Serdica
Mathematical Journal
Сердика
Математическо списание

Serdica Math. J. **30** (2004), 549–570

Serdica
Mathematical Journal

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

A NOTE ON ELEMENTARY DERIVATIONS

Joseph Khoury

Communicated by V. Drensky

Abstract. Let R be a UFD containing a field of characteristic 0, and $B_m = R[Y_1, \dots, Y_m]$ be a polynomial ring over R. It was conjectured in [5] that if D is an R-elementary monomial derivation of B_3 such that $\ker D$ is a finitely generated R-algebra then the generators of $\ker D$ can be chosen to be linear in the Y_i's. In this paper, we prove that this does not hold for B_4. We also investigate R-elementary derivations D of B_m satisfying one or the other of the following conditions:

(i) D is standard.

(ii) $\ker D$ is generated over R by linear constants.

(iii) D is fix-point-free.

(iv) $\ker D$ is finitely generated as an R-algebra.

(v) D is surjective.

(vi) The rank of D is strictly less than m.

2000 *Mathematics Subject Classification:* Primary: 14R10. Secondary: 14R20, 13N15.
Key words: Derivations, Hilbert fourteenth problem.

1. Introduction. In this paper, unless otherwise noted, k is a field of characteristic 0, R is a UFD containing k and B is an R-algebra which is a polynomial ring in a finite number of variables over R. If m is a positive integer, then $R^{[m]}$ means the polynomial ring in m variables over R. If $B \cong R^{[m]}$, then a *coordinate system* of B over R is an element $(Y_1, \ldots, Y_m) \in B^m$ satisfying $B = R[Y_1, \ldots, Y_m]$. Recall that a *derivation* $D : B \to B$ is an additive map satisying $D(xy) = D(x)y + xD(y)$ for all $x, y \in B$. If $D(R) = \{0\}$, then we say that D is an R-derivation of B. D is called *locally nilpotent* if for every $x \in B$, there exists $n \geq 0$ such that $D^n(x) = 0$.

Definition 1.1. *If $B = R^{[m]}$, then an R-derivation $D : B \to B$ is called* R-elementary *if there exists a coordinate system $(Y_1, \ldots, Y_m)$ of B over R such that $DY_i \in R$ for all i.*

In this case we have:

$$D = \sum_{i=1}^{m} a_i \frac{\partial}{\partial Y_i} \qquad \text{(where } a_i \in R\text{)}.$$

Definition 1.2. *Let $C = k^{[N]}$. A derivation $D : C \to C$ is* elementary *if, for some integers $m, n \geq 0$ such that $m + n = N$, there exists a coordinate system $(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ of C satisfying:*

$$k[X_1, \ldots, X_n] \subseteq \ker D \quad \textit{and} \quad \forall\, i, \quad DY_i \in k[X_1, \ldots, X_n].$$

In this case, D is $k[X_1, \ldots, X_n]$-elementary:

$$D = \sum_{i=1}^{m} a_i \frac{\partial}{\partial Y_i} \qquad \text{(where } a_i \in k[X_1, \ldots, X_n]\text{)}.$$

An immediate consequence of the above definition is that all elementary derivations are locally nilpotent.

Definition 1.3. *A derivation $D : B \longrightarrow B$ is called* irreducible *if the only principal ideal of B containing $D(B)$ is B itself. A locally nilpotent derivation D is called* fix-point-free *if the ideal of B generated by the image of D is equal to B. A* slice *of D is an element $s \in B$ such that $D(s) = 1$.*

It is clear that any surjective locally nilpotent derivation of B admits a slice. The converse is also true: if s is a slice of a locally nilpotent derivation D

of B and $y \in B$, let

$$x = \sum_{k=0}^{\infty} (-1)^k \frac{s^{k+1}}{(k+1)!} D^k(y)$$

then $x \in B$ since D is locally nilpotent and it is easy to verify that $D(x) = y$.

Knowing that a locally nilpotent derivation of a polynomial algebra admits a slice helps to understand the kernel of the derivation. More precisely, the following is a well known fact (see [8]).

Proposition 1.1. *If $D : C \to C$ is a locally nilpotent R-derivation of an R-algebra C with a slice s, then*

1. $C = A[s] = A^{[1]}$*, where* $A = \ker D$.
2. *The map*

$$\begin{array}{rccc} \zeta : & C & \longrightarrow & C \\ & x & \mapsto & \sum_{i \geq 0} \frac{1}{i!}(-s)^i D^i(x) \end{array}$$

is a homomorphism of R-algebras with image equal to $\ker D$*. In particular, if $C = R[Y_1, \dots, Y_m]$ then*

$$\ker D = R[\zeta(Y_1), \dots, \zeta(Y_m)].$$

R-derivations of B can be classified according to their *rank*:

Definition 1.4. *The* rank *of an R-derivation D of B is defined to the least integer s ($0 \leq s \leq n$) for which there exists a coordinate system $(X_1, \dots, X_n)$ of B over R satisfying $R[X_1, \dots, X_{n-s}] \subseteq$* $\ker D$*. In other words, rank D is the least number of partial derivatives of B needed to express D.*

Clearly, the rank of D is zero if and only if D is the zero derivation.

Definition 1.5. *Let $B = R[Y_1, \dots, Y_m]$ and consider an R-elementary derivation*

$$D = \sum_{i=1}^{m} a_i \, \partial_i \quad : \quad B \longrightarrow B$$

where $a_i \in R$ and $\partial_i = \partial / \partial Y_i$ for all i.

1. *Any element of* $\ker D$ *of the form*

$$r_1 Y_1 + \cdots + r_m Y_m \qquad (\textit{where } r_i \in R)$$

is said to be a linear constant *of D.*

2. *Given* $i, j \in \{1, \ldots, m\}$*, define* $L_{ij} = \dfrac{a_i}{g_{ij}} Y_j - \dfrac{a_j}{g_{ij}} Y_i$ *where:*

$$g_{ij} = \begin{cases} \gcd(a_i, a_j) & \text{if } a_i \neq 0 \text{ or } a_j \neq 0 \\ 1 & \text{if } a_i = 0 = a_j. \end{cases}$$

   It is clear that $L_{ij} \in \ker D$*,* $L_{ii} = 0$ *and* $L_{ji} = -L_{ij}$ *(for all* i, j*). We call the elements* L_{ij} *the* standard linear constants *of* D*.*

3. *If* $\ker D$ *is generated as an* R*-algebra by the standard linear constants, we say that* D *is a* standard *derivation.*

This paper investigates R-elementary derivations $D : R^{[m]} \to R^{[m]}$ satisfying one or the other of the following conditions:

(i) *D is standard.*

(ii) $\ker D$ *is generated over* R *by linear constants.*

(iii) *D is fix-point-free.*

(iv) $\ker D$ *is finitely generated as an* R*-algebra.*

(v) *D is surjective.*

(vi) $\operatorname{Rank} D < m$*.*

Studying the finite generation of the kernel of derivations of polynomial rings is closely related to the famous fourteenth's problem of Hilbert, that can be stated as follows

> If L is a subfield of $k(X_1, ..., X_n)$ (the quotient field of $k^{[n]}$), is $L \cap k[X_1, ..., X_n]$ a finitely generated k-algebra?

Deveney and Finston ([3]) used a couterexample to Hilbert's fourteenth problem found by Roberts in 1990 ([6]) to prove that the kernel of the elementary derivation

$$D = X_1^{t+1} \frac{\partial}{\partial Y_1} + X_2^{t+1} \frac{\partial}{\partial Y_2} + X_3^{t+1} \frac{\partial}{\partial Y_3} + (X_1 X_2 X_3)^t \frac{\partial}{\partial Y_4}$$

of $k[X_1, X_2, X_3, Y_1, Y_2, Y_3, Y_4]$ is not finitely generated as a k-algebra for any $t \geq 2$.

To prove that the invariant subalgebras of some derivations in this paper are finitely generated we will use the following tool we proved in [5].

Proposition 1.2 ([5, Lemma 2.2])**.** *Let* $E \subseteq A_0 \subseteq A \subseteq C$ *be integral domains, where* E *is a UFD. Suppose that some element* d *of* $E \backslash \{0\}$ *satisfies:*

- $(A_0)_d = A_d$
- *$pC \cap A_0 = pA_0$ for each prime divisor p of d, (in E)*

then $A_0 = A$.

Using our notations, E plays the role of R, A plays the role of $\ker D$, A_0 is a subalgebra of $\ker D$ (which is a candidate for $\ker D$) and C plays the role of B.

2. Unimodular rows and variables. Recall that an element $F \in B \cong R^{[m]}$ is called a *variable* of B over R if there exists a coordinate system $(F, F_2, \ldots, F_m)$ of B over R.

Given an element F of B, it is desirable to know if F is a variable over R. That question seems to be hard in general. In this section, we give a necessary and sufficient condition for a linear form to be a variable.

Definition 2.1. *Let A be a ring and n a positive integer. An element $(a_1, \ldots, a_n)$ of A^n is called* a unimodular row of length n over A *if $a_1b_1 + \ldots + a_nb_n = 1$ for some $b_1, \ldots, b_n \in A$. A unimodular row over A is called* extendible *if it is the first row of an invertible matrix over A. The ring A is called* Hermite *if every unimodular row over A is extendible.*

It is well known that Hermite rings include:

1. polynomial rings over a field
2. Formal power series over a field
3. Laurent polynomials over a field
4. Any PID
5. Any complex Banach Algebra with a contractible maximal ideal space.

A well-known example of a non Hermite ring is the following.

Example 2.1. (M. Hochster, [4]) Let $R = \mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1) = \mathbb{R}[x, y, z]$ (x, y, z are the images of X, Y, Z in R respectively), then (x, y, z) is a unimodular row over R which is not extendible. So R is not Hermite.

Clearly any extendible unimodular row is unimodular. The converse holds in case of length 2 by the following (obvious) proposition.

Proposition 2.1. *f A is an arbitrary ring (commutative with identity), then any unimodular row of length ≤ 2 over A is extendible.*

We relate now the notion of a "linear variable" with that of "extendible unimodular row". First, a lemma.

Lemma 2.1. *Let E be a domain, and $V = E[X_1, \dots, X_n]$ be a polynomial ring in n variables over E. If $\gamma = (F_1, \dots, F_n)$ is a coordinate system of V over E, then the determinant of the matrix*

$$A = \left(\frac{\partial F_i}{\partial X_j}\right)_{1 \leq i,j \leq n}$$

is a unit of E.

Proposition 2.2. *Let A be a domain, $(a_1, \dots, a_n) \in A^n$ and $B = A[Y_1, \dots, Y_n] = A^{[n]}$. Then the following conditions are equivalent:*

1. *The linear form $a_1Y_1 + \cdots + a_nY_n$ is a variable of B over A*

2. *$(a_1, \dots, a_n)$ is an extendible unimodular row of B over A.*

Proof. Assume first that $F = a_1Y_1 + \cdots + a_nY_n$ is a variable of B over A, then $B = A[F, F_2, \dots, F_n]$ for some elements $F_2, \dots, F_n$ of B. By Lemma **??**,

$$\det(\mathcal{M}) \in R^* \tag{1}$$

where

$$\mathcal{M} = \left(\frac{\partial F_i}{\partial Y_j}\right)_{1 \leq i,j \leq n}$$

(with $F = F_1$). Sending all the variables to 0 in $\mathcal{M}$ gives a matrix with entries in R and first row equal to $(a_1, \dots, a_n)$. Relation (1) shows that the determinant of this matrix is a unit in A and hence $(a_1, \dots, a_n)$ is an extendible unimodular row of B over A.

For the converse, suppose that $\mathcal{M}$ is an invertible matrix with entries in A and first row equal to $(a_1, \dots, a_n)$. Let $(F_2, \dots, F_n) \in B^{n-1}$ be such that

$$\mathcal{M}^{-1} \begin{bmatrix} F \\ F_2 \\ \vdots \\ F_n \end{bmatrix} = \begin{bmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{bmatrix}.$$

This implies that $A[F, F_2, \dots, F_n] \supseteq A[Y_1, \dots, Y_n]$. Since the other inclusion is clear, $B = A[F, F_2, \dots, F_n]$ and F is then a variable of B over A $\square$

3. Homogeneous derivations.

Definition 3.1. *Let $C = \bigoplus_i C_i$ be a $\mathbb{Z}$-graded or an $\mathbb{N}$-graded ring. A derivation $D : C \to C$ is called* homogeneous *of degree n if there exists an integer n such that $D(C_i) \subseteq C_{i+n}$ for all i.*

Consider the natural $\mathbb{N}$-grading on $B = R[Y_1, \dots, Y_m]$ where the degree of each element of R is zero and the degree of each of the variables in one. Every R-elementary derivation on B is then homogeneous of degree -1.

The following proposition will be used later in this paper.

Proposition 3.1. *Let $B = R[Y_1, \dots, Y_m]$ equipped with the natural $\mathbb{N}$-grading. If D is a homogeneous derivation of B that annihilates a variable of B over R, then D annihilates a variable of B over R which is a linear form in the Y_i's (over R).*

Proof. Suppose that $F \in \ker D$ is a variable of B over R. Without loss of generality, one can assume that the homogeneous part of degree 0 of F is zero. Write

$$F = F_{(1)} + F_{(2)} + \ldots + F_{(d)}$$

where d is the degree of F and $F_{(i)}$ is the homogeneous part of F of degree i. Choose $F_2, \dots, F_m \in B$ such that $B = R[F, F_2, \dots, F_m]$ and let

$$\mathcal{M} = \left(\frac{\partial F_i}{\partial Y_j} \right)_{1 \le i,j \le n}$$

(with $F = F_1$). Then $\mathcal{M}$ is invertible by Lemma 2.1. Setting all the Y_i's equal to zero in $\mathcal{M}$ gives an element of $\mathrm{GL}_m(R)$ whose first row is $(\alpha_1, \alpha_2, \dots, \alpha_m)$ where

$$F_{(1)} = \alpha_1 Y_1 + \alpha_2 Y_2 + \cdots + \alpha_m Y_m.$$

Proposition 2.2 shows that $F_{(1)}$ is a variable of B over R. On the other hand, the fact that D is homogeneous implies that each of the homogeneous components of F are in $\ker D$. In particular $F_{(1)} \in \ker D$. $\square$

4. Standard derivations.

We consider first the simple case of R-elementary derivations in dimension 2 (R is a UFD containing a field k).

Proposition 4.1. *Every R-elementary derivation of $R^{[2]}$ is standard.*

Proof. Let $B = R[Y_1, Y_2] = R^{[2]}$, and $D = a_1 \dfrac{\partial}{\partial Y_1} + a_2 \dfrac{\partial}{\partial Y_2}$ an R-elementary derivation of B. We may clearly assume that D is irreducible; i.e., a_1 and a_2 are relatively prime in R. Using Proposition 1.2, we will show that $\ker D = R[a_1Y_1 - a_2Y_2]$.

Let $F = a_1Y_2 - a_2Y_1$ and $R_0 = R[F]$. Then, $R_0 \subseteq \ker D$ and $(R_0)_{a_1} = (\ker D)_{a_1}$.
Let p be a prime divisor of a_1, and let $x \in pB \cap R_0$; we show that $x \in pR_0$, the inclusion $pR_0 \subseteq pB \cap R_0$ being clear. For this, write $x = \Phi(F)$ for some $\Phi \in R[T] = R^{[1]}$ then the image $\overline{\Phi} \in \overline{R}[T]$ of Φ (where $\overline{R} = R/pR$) is in the kernel of the epimorphism

$$\alpha : \overline{R}[T] \longrightarrow \overline{R}[\overline{F}]$$

sending T to $\overline{F}$. Since $\overline{F}$ is transcendental over $\overline{R}$, α is an isomorphism. Consequentely, $\overline{\Phi} = 0$ and $x \in pR_0$. $\square$

The implications $(i) \Longrightarrow (ii)$ and $(i) \Longrightarrow (iv)$ above (see the introduction) are true by the definition of standard derivations. By proposition 4.1, the $k[X_1, X_2]$-elementary derivation

$$X_1 \frac{\partial}{\partial Y_1} + X_2 \frac{\partial}{\partial Y_2} \tag{2}$$

of $k[X_1, X_2, Y_1, Y_2]$ is standard. Clearly, this derivation is not fix-point-free and consequently not surjective. This shows that $(i) \Longrightarrow (iii)$ and $(i) \Longrightarrow (v)$ are false in general. For the implication $(i) \Longrightarrow (vi)$, note that the derivation (2) above does not annihilate a variable of $k[X_1, X_2, Y_1, Y_2]$ over $k[X_1, X_2]$. Indeed, if $F \in k[X_1, X_2, Y_1, Y_2]$ is a variable of $k[X_1, X_2, Y_1, Y_2]$ over $k[X_1, X_2]$ such that $D(F) = 0$, then we may assume that $F = \alpha_1Y_1 + \alpha_2Y_2$ for some unimodular row (α_1, α_2) over $k[X_1, X_2]$ (Proposition 3.1). But the fact that $D(F) = 0$ implies that

$$X_1\alpha_1 + X_2\alpha_2 = 0$$

and hence the ideal generated by α_1 and α_2 in $k[X_1, X_2]$ is included in the ideal generated by X_1 and X_2. This contradicts the fact that (α_1, α_2) is a unimodular row. We conclude that the rank of D is 2 and that the implication $(i) \Longrightarrow (vi)$ is false.

5. The case where $\ker D$ is generated by linear constants.

The following theorem gives a counterexample "of rank m" to the implication $(ii) \Rightarrow (i)$ above.

Theorem 5.1. *The kernel of the elementary derivation*

$$D = (X_1^2 - X_2X_3)\frac{\partial}{\partial Y_1} + (X_2^2 - X_1X_3)\frac{\partial}{\partial Y_2} + (X_3^2 - X_1X_2)\frac{\partial}{\partial Y_3}$$

of $B = k[X_1, X_2, X_3, Y_1, Y_2, Y_3]$ is generated by two linear constants (in fact it is a polynomial ring in two variables over $k[X_1, X_2, X_3]$) but D is not standard. Moreover the rank of D over $k[X_1, X_2, X_3]$ is 3.

Proof. Let $a_1 = X_1^2 - X_2X_3$, $a_2 = X_2^2 - X_1X_3$, $a_3 = X_3^2 - X_1X_2$, and let $R = k[X_1, X_2, X_3]$. Then a_1, a_2, a_3 are pairwise relatively prime elements of R. Consider the two elements of B

$$f = X_3Y_1 + X_1Y_2 + X_2Y_3, \quad g = X_2Y_1 + X_3Y_2 + X_1Y_3$$

and the usual standard linear constants

$$\begin{array}{rcrcl} L_1 & = & a_3Y_2 - a_2Y_3 & = & X_3^2Y_2 - X_1X_2Y_2 - X_2^2Y_3 + X_1X_3Y_3 \\ L_2 & = & -a_3Y_1 + a_1Y_3 & = & -X_3^2Y_1 + X_1X_2Y_1 + X_1^2Y_3 - X_2X_3Y_3 \\ L_3 & = & a_2Y_1 - a_1Y_2 & = & X_2^2Y_1 - X_1X_3Y_1 - X_1^2Y_2 + X_2X_3Y_2. \end{array}$$

It is immediate that $D(f) = D(g) = 0$ and that the following relations are true

$$L_1 = -X_2f + X_3g, \quad L_2 = -X_2f + X_1g, \quad L_3 = -X_1f + X_2g.$$

Let $R_0 := R[f, g]$, then $R[L_1, L_2, L_3] \subseteq R_0$. It is easy to see that $(R[L_1, L_2, L_3])_{a_3} = (\ker D)_{a_3}$, so $(R_0)_{a_3} = (\ker D)_{a_3}$. We will show that $\ker D = R[f, g]$; so, it is enough (Proposition 1.2) to show that $a_3B \cap R_0 \subseteq a_3R_0$. Let $\overline{R} = R/a_3R$ and consider the ring homomorphism

$$\phi : \overline{R}[T_1, T_2] \longrightarrow \overline{R}[\overline{f}, \overline{g}]$$

sending T_1 to $\overline{f}$ and T_2 to $\overline{g}$. We claim that ϕ is an isomorphism. Indeed, since the elements $\overline{f}$ and $\overline{g}$ are not algebraic over $\overline{R}$, the transcendence degree of $\overline{R}[\overline{f}, \overline{g}]$ over $\overline{R}$ is either one or two. If it is one, then $\overline{f}, \overline{g}$ are linearly dependent over $K := \mathrm{qt}(\overline{R})$ and so there exists an $\overline{\alpha} \in \mathrm{qt}(\overline{R})^*$ such that $x_3 = \overline{\alpha}x_2$, $x_1 = \overline{\alpha}x_3$, $x_2 = \overline{\alpha}x_1$ (where x_i is the image of X_i in $\overline{R}$); in particular, $x_2^2 = x_1x_3$ in $\overline{R}$ and so

$$X_2^2 = X_1X_3 + (X_3^2 - X_1X_2)\Upsilon$$

for some $\Upsilon \in R$. This is absurd. Thus, $\mathrm{trdeg}_{\overline{R}}\overline{R}[\overline{f}, \overline{g}] = 2$, and so the height of $\ker \phi$ is zero. This shows that ϕ is injective, and hence an isomorphism. To finish the proof, consider an element $x = \Phi(f, g) = a_3b$ of $a_3B \cap R_0$ ($\Phi \in R[T_1, T_2]$ and

$b \in B$). Then the image $\overline{\Phi}$ of Φ in $\overline{R}[T_1, T_2]$ is in the kernel of ϕ, and consequently it is zero, so $\Phi = a_3 h$ for some $h \in R[T_1, T_2]$, and hence $x = \Phi(f, g) \in a_3 R_0$ as desired. We conclude that $\ker D = R[f, g]$.

Next we prove that D is not standard. To see this, it is enough to notice that f is homogeneous of degree 2 in the X_i's and the Y_j's while each standard linear constant is homogeneous of degree 3. In other words, $f \in \ker D \backslash R[L_1, L_2, L_3]$ where L_1, L_2, L_3 are the standard linear constants of D.

We finish by proving that the rank of D over $k[X_1, X_2, X_3]$ is 3. Suppose on the contrary that $\operatorname{rank} D < 3$, then D annihilates a variable F of $k[X_1, X_2, X_3, Y_1, Y_2, Y_3]$ over $k[X_1, X_2, X_3]$. By Propostion 3.1, we may assume that $F = \alpha_1 Y_1 + \alpha_2 Y_2 + \alpha_3 Y_3$ for some unimodular row $(\alpha_1, \alpha_2, \alpha_3)$ of $k[X_1, X_2, X_3]$. Since $D(F) = 0$, we have

$$(X_1^2 - X_2 X_3)\alpha_1 + (X_2^2 - X_1 X_3)\alpha_2 + (X_3^2 - X_1 X_2)\alpha_3 = 0. \tag{3}$$

Sending the variables X_2, X_3 to 0 in (3) simultaneously shows that $\alpha_1(X_1, 0, 0) = 0$, so $\alpha_1 \in (X_1, X_2, X_3)k[X_1, X_2, X_3]$; similarly, $\alpha_2, \alpha_3 \in (X_1, X_2, X_3)k[X_1, X_2, X_3]$ and this contradicts the fact that $1 \in (\alpha_1, \alpha_2, \alpha_3)k[X_1, X_2, X_3]$. $\square$

Remark 5.1. The main result in [5] treats the case of elementary derivations $D = \sum_{i=1}^{3} a_i \dfrac{\partial}{\partial Y_i}$ of $R[Y_1, Y_2, Y_3]$ where for some $i \in \{1, 2, 3\}$, R/pR is a UFD for every prime divisor p of a_i. With the notation of Theorem 5.1, each a_i is prime and $R/a_i R$ is not a UFD.

Remark 5.2. The above theorem shows that the condition "fix-point-free" of Theorem 6.1 below is not superfluous. The Theorem also gives an example of a derivation satisfying condition (*ii*) above but neither of the conditions (*iii*), (*v*) and (*vi*) (clearly, D is not fix-point-free and hence not surjective).

The above theorem can be used to construct counterexamples to the implication (*ii*) $\Longrightarrow$ (*i*) of derivations D satisfying "$\operatorname{rank} D < n$". First some notations. Let m and n be two positive integers such that $m < n$, $B_n = R[Y_1, \ldots, Y_n]$, $B_m = R[Y_1, \ldots, Y_m]$. Let $D = \sum_{i=1}^{m} a_i \dfrac{\partial}{\partial Y_i}$ be an R-elementary derivation of B_m.

Proposition 5.1. *D is standard as an R-elementary derivation of B_m if and only if it is standard as an R-elementary derivation of B_n.*

Proof. Consider D as a derivation of B_n. The following two facts finish the proof:

- The standard linear constants of D are the L_{ij}'s (as defined above) with $1 \leq i < j \leq m$ and $Y_{m+1}, \ldots, Y_n$.

- $\ker D = C[Y_{m+1}, \dots, Y_n]$ where C is the kernel of D as a derivation of B_m. $\square$

We prove next that the implication $(ii) \Longrightarrow (iv)$ is true in the case of a noetherian ring. Namely, we have the following proposition.

Proposition 5.2. *Let R be a noetherian domain of characteristic zero, $B = R[Y_1, \dots, Y_m]$ and $D = \sum_{i=1}^{m} a_i \frac{\partial}{\partial Y_i}$ an R-elementary derivation of B. If $\ker D$ is generated over R by linear forms, then it is a finitely generated R-algebra.*

Proof. Let M be the set of all linear constants of D, then clearly M is an R-module. If $D = \sum_{i=1}^{m} a_i \frac{\partial}{\partial Y_i}$ where $a_i \in R$, then it is clear that M is isomorphic as an R-module to the submodule

$$N = \left\{ (\alpha_1, \dots, \alpha_m) \in R^m;\ \begin{pmatrix} a_1 & \dots & a_m \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = 0 \right\}$$

of R^m. Since R is noetherian, R^m is noetherian and N is finitely generated R-module. $\square$

6. Fix-point-free *R*-elementary derivations. Let C be an integral domain containing $\mathbb{Q}$, and let $D : C \longrightarrow C$ be a locally nilpotent derivation. It is well-known that there is an associated $\mathbf{G}_a$-action, $\alpha : \mathbf{G}_a \times \operatorname{Spec} C \to \operatorname{Spec} C$, and it turns out that the set of fixed points of α is the closed subset $V(I)$ of $\operatorname{Spec} C$, where I denotes the ideal (DC) of C generated by DC (the image of D). In particular, α is fix-point-free if and only if $(DC) = C$. This motivates the definition of fix-point-free derivation given in Definition 1.3.

Obviously, if a derivation of B admits a slice then it is fix-point-free. It is well-known that the converse is not true in general. The following proposition proves, among other things, that the converse holds for elementary derivations.

Proposition 6.1. *Let R be a domain containing $\mathbb{Q}$. If $B = R[Y_1, \dots, Y_m] = R^{[m]}$, and $D : B \to B$ an R-elementary derivation, then:*

1. *If D is fix-point-free, then it admits a slice. Moreover, $\ker D$ can be generated by m linear constants.*

2. *If D is fix-point-free and R is Hermite, then there exists a coordinate system $(Z_1, \dots, Z_m)$ of B over R related to $(Y_1, \dots, Y_m)$ by a linear change of variables, such that $D = \partial/\partial Z_m$.*

Proof. Write $D = \sum_{i=1}^{m} a_i \partial_i$ where $a_i \in R$ and $\partial_i = \partial/\partial Y_i$. If D is fix-point-free then $1 \in (DY_1, \dots, DY_m)$ so $\sum_{i=1}^{m} a_i r_i = 1$ for some $(r_1, \dots, r_m) \in R^m$. Consequently, $s = \sum_{i=1}^{m} r_i Y_i$ is a slice of D and by Proposition 1.1, $B = A[s] = A^{[1]}$ where $A = \ker D$. Also, Proposition 1.1 shows that $\ker D = R[\zeta(Y_1), \dots, \zeta(Y_m)]$ where ζ is the homomorphism of R-algebras:

$$\begin{array}{cccc} \zeta : & B & \longrightarrow & B \\ & x & \mapsto & \sum_{i \geq 0} \frac{1}{i!}(-s)^i D^i(x) \end{array}.$$

In particular, each $\zeta(Y_i)$ is a linear constant.

If R is a Hermite ring, then $(r_1 \dots r_m)$ is extendible, i.e., it is the first row of a matrix $U \in \mathrm{Gl}_m(R)$ and it follows that s is a variable of B over R by Proposition 2.2. A closer look at the proof of Proposition 2.2 shows that we can write $B = R[s_1, \dots, s_{m-1}, s]$ for some linear forms $s_1, \dots, s_{m-1}$ of B. For $1 \leq i \leq m-1$, take $Z_i = \zeta(s_i)$ then Z_i is a linear form in the Y_i's and by Propostion 1.1 (using $\zeta(s) = 0$) we get that $A = R[Z_1, \dots, Z_{m-1}]$. Let $Z_m = s$, then by Proposition 2.2 again $B = A[Z_m] = R[Z_1, \dots, Z_m]$, and $D = \partial/\partial Z_m$. Note that $(Z_1, \dots, Z_m)$ is a coordinate system of B over R related to $(Y_1, \dots, Y_m)$ by a linear change of variables. $\square$

Remark 6.1. Proposition 6.1 shows in particular that if $D : B \to B$ is fix-point-free elementary derivation of B, then D is surjective (since it has a slice) and $\ker D$ is finitely generated over R by m linear constants.

Remark 6.2. In the above proposition, R needs not to be a UFD. It suffices that R is any domain containing the rationals.

We prove next that "fix-point-free" implies "standard" in the easy case where the image under D of one of the Y_i's is a unit. Namely:

Proposition 6.2. *Let $R \supseteq \mathbb{Q}$ be a UFD, $B = R[Y_1, \dots, Y_m] = R^{[m]}$ and $D : B \to B$ an R-elementary derivation. If $DY_i \in R^*$ for some i, then* $\ker D$ *is generated by $m-1$ standard linear constants.*

Proof. We may assume that $DY_1 \in R^*$. Define $s = (DY_1)^{-1} Y_1$, then s is a slice of D and consequently the map $B \overrightarrow{\zeta} B$ defined by $\xi(x) = \sum_{j \geq 0} \dfrac{1}{j!}(-s)^j D^j(x)$ is a homomorphism of R-algebras with image equal to $\ker D$. Thus $\ker D = R[\zeta(Y_1), \dots, \zeta(Y_m)]$ and we are done since $\zeta(Y_j) = Y_j - (DY_j)s = L_{1,j}$ for each j. $\square$

We prove now the main result of this section.

Theorem 6.1. *Let $R \supseteq \mathbb{Q}$ be a UFD, $B = R[Y_1, \ldots, Y_m] = R^{[m]}$ and $D : B \to B$ an R-elementary derivation. If D is fix-point-free, then it is standard.*

Proof. By Proposition 6.1,

$$\ker D = R[\xi(Y_1), \ldots, \xi(Y_m)],$$

where each $\xi(Y_i) = Y_i - a_i s$ is a linear constant. We obtain:

(4) $\ker D$ is generated as an R-algebra by m linear constants.

So it suffices to show that each linear constant is a linear combination (over R) of the standard linear constants. In other words, we have to show that the R-module $T(D)$ is trivial, where:

$$\begin{aligned} \mathrm{LC}(D) &= \textit{set of linear constants of } D \text{ (an } R\text{-submodule of } \ker D), \\ \mathrm{SLC}(D) &= R\textit{-submodule of } \mathrm{LC}(D) \text{ generated by the standard linear constants}, \\ T(D) &= \mathrm{LC}(D)/\mathrm{SLC}(D). \end{aligned}$$

Let $\mathfrak{m}$ be a maximal ideal of R and consider the derivation $D_{\mathfrak{m}} : B_{\mathfrak{m}} \to B_{\mathfrak{m}}$ obtained by localization at the set $R \backslash \mathfrak{m}$. Now $R_{\mathfrak{m}}$ is a UFD, $B_{\mathfrak{m}} = R_{\mathfrak{m}}[Y_1, \ldots, Y_m] = R_{\mathfrak{m}}^{[m]}$ and $D_{\mathfrak{m}} = \sum_{i=1}^{m} a_i \partial_i$ is an $R_{\mathfrak{m}}$-elementary derivation. Since D is fix-point-free, we have $(a_1, \ldots, a_m)R \nsubseteq \mathfrak{m}$ so, for some i, a_i is a unit of $R_{\mathfrak{m}}$. By Proposition 6.2, $D_{\mathfrak{m}}$ is standard, so $T(D_{\mathfrak{m}}) = 0$. It is immediate that $\mathrm{LC}(D_{\mathfrak{m}}) = \mathrm{LC}(D)_{\mathfrak{m}}$ and $\mathrm{SLC}(D_{\mathfrak{m}}) = \mathrm{SLC}(D)_{\mathfrak{m}}$, so $T(D_{\mathfrak{m}}) = T(D)_{\mathfrak{m}}$ and we have shown:

$$T(D)_{\mathfrak{m}} = 0 \quad \textit{for all maximal ideals } \mathfrak{m} \text{ of } R.$$

We conclude that $T(D) = 0$ and the result follows. □

So far we have shown that the implications $(iii) \Longrightarrow (i)$, $(iii) \Longrightarrow (ii)$, $(iii) \Longrightarrow (iv)$ and $(iii) \Longrightarrow (v)$ are all true. By Proposition 6.1, we also know that $(iii) \Longrightarrow (vi)$ is true in the case of Hermite rings. In this case, we can actually say a lot more: the rank of the derivation is one and hence it is "conjugate to a partial derivative".

If R is not Hermite, we don't know if $(iii) \Longrightarrow (vi)$ is true or not. However, the following gives an example of a fix-point-free elementary derivation which is not "conjugate to a partial derivative" of B.

Proposition 6.3. *Let* $R = \mathbb{R}[x, y, z]$ *be as in Example* 2.1 *above, and let* $B = R[Y_1, Y_2, Y_3] \cong R^{[3]}$. *Let* $D = x\frac{\partial}{Y_1} + y\frac{\partial}{Y_2} + z\frac{\partial}{Y_3}$. *Then* D *is fix-point-free* R*-elementary derivation of* B *satisfying* $\operatorname{rank} D \geq 2$.

P r o o f. Let $s = xY_1 + yY_2 + zY_3 \in B$, then $D(s) = x^2 + y^2 + z^2 = 1$ in R, and s is then a slice of D. In particular D is fix-point-free, and $B = A[s] \cong A^{[1]}$ where $A = \ker D$. We prove next that $\operatorname{rank} D \geq 2$. Clearly $\operatorname{rank} D \neq 0$, so it suffices to show that $\operatorname{rank} D \neq 1$. Assume that $rankD = 1$, then one can find a coordinate system (F, G, H) of B over R such that $D = \Phi(F, G, H)\frac{\partial}{\partial H}$ for some $\Phi \in R^{[3]}$. Clearly, $A = R[F, G]$ and so $B = A[s] = \mathbb{R}[F, G, s]$. Thus, s is a variable of B over R. By Prosition 2.2, (x, y, z) is an extendible unimodular row. This is a contradiction (see Example 2.1) □

7. The case where ker D is finitely generated as an R-algebra. It was conjectured in [5] that if D is an R-elementary monomial derivation of $R[Y_1, Y_2, Y_3]$ such that $\ker D$ is a finitely generated R-algebra then the generators of $\ker D$ can be chosen to be linear in the Y_i's. In this section we prove that this is not always the case. Theorem 7.1 gives a counterexample to the implications $(iv) \Longrightarrow (i)$, $(iv) \Longrightarrow (ii)$, $(iv) \Longrightarrow (iii)$.

Theorem 7.1. *The kernel of the derivation*

$$D = X_1^2\frac{\partial}{\partial Y_1} + X_2^2\frac{\partial}{\partial Y_2} + X_3^2\frac{\partial}{\partial Y_3} + X_2X_3\frac{\partial}{\partial Y_4}$$

of $k[X_1, X_2, X_3, Y_1, Y_2, Y_3, Y_4] \cong k^{[7]}$ *is a finitely generated* $k[X_1, X_2, X_3]$*-algebra which cannot be generated over* $k[X_1, X_2, X_3]$ *by linear forms in the* Y_i*'s.*

To that end we will use Proposition 1.2 and the elimination theory of Groebner bases. Regarding Groebner bases, S-polynomials and Buchberger's criteria, the reader may refer to ([1]).

Consider the following elements of $\ker D$

$$L_{12} = X_1^2Y_2 - X_2^2Y_1 \qquad L_{13} = X_1^2Y_3 - X_3^2Y_1$$
$$L_{14} = X_1^2Y_4 - X_2X_3Y_1 \qquad L_{24} = X_2Y_4 - X_3Y_2$$
$$L_{34} = X_3Y_4 - X_2Y_3$$
$$f = X_1^2Y_4^2 - X_1^2Y_2Y_3 + X_3^2Y_1Y_2 + X_2^2Y_1Y_3 - 2X_2X_3Y_1Y_4.$$

We will prove that $\ker D = k[X_1, X_2, X_3, f, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}]$. For this, let $k[X, Y, T]$ denote the polynomial ring

$$k[X_1, X_2, X_3, Y_1, Y_2, Y_3, Y_4, T_1, T_2, T_3, T_4, T_{12}, T_{13}, T_{14}, T_{24}, T_{34}]$$

in 16 variables and let I be the ideal of $k[X,Y,T]$ generated by the elements

$$T_1 - X_1, T_2 - X_2, T_3 - X_3, T_4 - f, T_{12} - L_{12}, T_{13} - L_{13}, \\ T_{14} - L_{14}, T_{24} - L_{24}, T_{34} - L_{34}, X_1.$$

The next lemma gives a Groebner basis for the ideal I. The elements of this basis will be used in computing the generators of $\ker D$. The proof of the lemma is left to the reader.

Lemma 7.1. *A Groebner basis for I with respect to the lexicographic order on $k[X,Y,T]$ with*

$$X_1 > X_2 > X_3 > Y_1 > \ldots > Y_4 > T_1 > \ldots > T_4 > T_{12} > T_{13} > T_{14} > T_{24} > T_{34}$$

is given by the elements
$g_1 = -T_2 + X_2$
$g_2 = -T_3 + X_3$
$g_3 = X_1$
$g_4 = Y_1 T_2^2 + T_{12}$
$g_5 = Y_1 T_3^2 + T_{13}$
$g_6 = Y_1 T_2 T_3 + T_{14}$
$g_7 = T_1$
$g_8 = -Y_4 T_2 + T_{24} + T_3 Y_2$
$g_9 = Y_3 T_2 - Y_4 T_3 + T_{34}$
$g_{10} = Y_2 T_{13} + Y_3 T_{12} - 2Y_4 T_{14} + T_4$
$g_{11} = -T_3 T_{12} + T_{14} T_2$
$g_{12} = T_2 T_{13} - T_3 T_{14}$
$g_{13} = T_4 + Y_1 T_3 T_{24} + Y_3 T_{12} - Y_4 T_{14}$
$g_{14} = -Y_2 T_{14} + Y_1 T_2 T_{24} + Y_4 T_{12}$
$g_{15} = Y_1 T_2 T_{34} - Y_3 T_{12} + Y_4 T_{14}$
$g_{16} = -Y_3 T_{14} + Y_1 T_3 T_{34} + Y_4 T_{13}$
$g_{17} = T_3 Y_3 T_{12} - T_3 Y_4 T_{14} + T_{14} T_{34}$
$g_{18} = Y_3 T_{12} T_{34} + Y_3 T_{14} T_{24} - Y_4 T_{13} T_{24} - Y_4 T_{14} T_{34} + T_4 T_{34}$
$g_{19} = -T_{14}^2 + T_{12} T_{13}$
$g_{20} = -T_{14} T_{34} + T_3 T_4 - T_{13} T_{24}$
$g_{21} = T_2 T_4 - T_{14} T_{24} - T_{12} T_{34}$
$g_{22} = -T_{13} Y_4 T_3 + T_{13} T_{34} + Y_3 T_3 T_{14}$
$g_{23} = Y_1 T_{24}^2 - Y_2 Y_3 T_{12} - Y_2 T_4 + Y_4^2 T_{12}$
$g_{24} = Y_1 T_{24} T_{34} + Y_3 Y_2 T_{14} + Y_4 T_4 - Y_4^2 T_{14}$
$g_{25} = T_{14}^2 Y_2 - 2Y_4 T_{14} T_{12} + T_4 T_{12} + Y_3 T_{12}^2$

$g_{26} = Y_1T_{34}^2 + Y_3^2T_{12} - 2Y_3Y_4T_{14} + Y_4^2T_{13}$
$g_{27} = T_{34}Y_2T_{14} - T_{34}Y_4T_{12} - T_{24}Y_3T_{12} + T_{24}Y_4T_{14}$
$g_{28} = T_{13}Y_3T_{14}T_{24} + Y_3T_{34}T_{14}^2 - Y_4T_{13}^2T_{24} - T_{13}Y_4T_{14}T_{34} + T_{13}T_4T_{34}.$

We prove next that $\ker D = k[X_1, X_2, X_3, f, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}]$.

Let $k[T]$ and $k[X,Y]$ denote respectively the polynomial rings $k[T_1, T_2, T_3, T_4, T_{12}, T_{13}, T_{14}, T_{24}, T_{34}]$ and $k[X_1, X_2, X_3, Y_1, Y_2, Y_3, Y_4]$. Let $A_0 = k[X_1, X_2, X_3, f, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}]$, then $A_0 \subseteq \ker D$ and $(A_0)_{X_i} = (\ker D)_{X_i}$ for $i = 1, 2, 3$. By Proposition 1.2, it is enough to show that $X_1k[X,Y] \cap A_0 \subseteq X_1A_0$ (the other inclusion being obvious). So let $x \in X_1k[X,Y] \cap A_0$ and choose $z \in k[X,Y]$, $\Phi \in k[T]$ such that $x = \Phi(X_1, X_2, X_3, f, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}) = X_1z$. This means that Φ is in the kernel of the homomorphism

$$\theta : k[T] \xrightarrow{\psi} A_0 \hookrightarrow k[X,Y] \xrightarrow{\pi} k[X,Y]/(X_1)$$

where π is the canonical epimorphism and ψ sends T_i to X_i, $i = 1, 2, 3$, T_4 to f and T_{jk} to L_{jk}. Also, consider the homomorphism

$$\kappa : k[X,Y,T] \xrightarrow{\sigma} k[X,Y] \xrightarrow{\pi} k[X,Y]/(X_1)$$

where σ is the homomorphism sending X_i to X_i, Y_i to Y_i ($i = 1, 2, 3, 4$), T_i to X_i ($i = 1, 2, 3$), T_4 to f, and T_{ij} to L_{ij}. It is clear that θ is the restriction of κ to $k[T]$ and hence

$$\ker\theta = \ker\kappa \cap k[T]. \tag{5}$$

We claim that $\ker\kappa$ is the ideal I (considered above) of $k[X,Y,T]$ generated by the elements

$$X_1, T_1 - X_1, T_2 - X_2, T_3 - X_3, T_4 - f, T_{12} - L_{12}, T_{13} - L_{13},$$
$$T_{14} - L_{14}, T_{24} - L_{24}, T_{34} - L_{34}.$$

Indeed, let $\Gamma = (\gamma_1, \ldots, \gamma_{16})$ be the 16-tuple

$$(X_1, X_2, X_3, Y_1, Y_2, Y_3, Y_4, T_1 - X_1, T_2 - X_2, T_3 - X_3, T_4 - f,$$
$$T_{12} - L_{12}, T_{13} - L_{13}, T_{14} - L_{14}, T_{24} - L_{24}, T_{34} - L_{34}).$$

Clearly, Γ is a coordinate system of $k[X,Y,T]$, that is

$$k[X,Y,T] = k[\gamma_1, \ldots, \gamma_{16}].$$

The domain and codomain of κ are respectively $k[\Gamma]$ and $k[\gamma_1,\dots,\gamma_7]/(\gamma_1)$ and κ is defined by

$$\kappa(\gamma_i)=\begin{cases} 0, & \text{if } i=1 \text{ or } i>7\\ \gamma_i+(\gamma_i), & \text{if } 2\le i\le 7.\end{cases}$$

So we have

$$\ker\kappa=\langle\gamma_1,\gamma_8,\gamma_9,\dots,\gamma_{16}\rangle=I,$$

and the claim is proved.

Using the elimination theory, we know that the set $\Sigma=\{g_7,g_{11},g_{12},g_{19},g_{20},g_{21}\}$ generates the ideal $I\cap k[T]$ of $k[T]$. Hence,

$$\Phi=\sum\xi_i h_i(T) \tag{6}$$

where $\xi_i\in k[T]$ and $h_i\in\{g_7,g_{11},g_{12},g_{19},g_{20},g_{21}\}$. On the other hand, one can easily verify the following identities:

$$\begin{array}{rclcl}
\psi(g_7) & = & X_1 & & \\
\psi(g_{11}) & = & -X_3L_{12}+X_2L_{14} & = & X_1^2L_{24}\\
\psi(g_{12}) & = & -X_3L_{14}+X_2L_{13} & = & -X_1^2L_{34}\\
\psi(g_{19}) & = & -L_{14}^2+L_{12}L_{13} & = & X_1^2f\\
\psi(g_{20}) & = & -L_{14}L_{34}+X_3f-L_{13}L_{24} & = & 0\\
\psi(g_{21}) & = & X_2f-L_{14}L_{24}-L_{12}L_{34} & = & 0.
\end{array}$$

This means that $x=\Phi(X_1,X_2,X_3,L_{12},L_{13},L_{14},L_{24},L_{34},f)\in X_1A_0$, and consequentely

$$\ker D=k[X_1,X_2,X_3,f,L_{12},L_{13},L_{14},L_{24},L_{34}].$$

The next two lemmas show that $\ker D$ cannot be generated over $k[X_1,X_2,X_3]$ by linear forms in the Y_i's.

Lemma 7.2. *With the above notation, if L is an element of $\ker D$ of the form*

$$L=\alpha_1Y_1+\cdots+\alpha_4Y_4$$

for some $\alpha_1,\dots,\alpha_4\in k[X_1,X_2,X_3]$, then

$$L\in k[X_1,X_2,X_3,L_{12},L_{13},L_{14},L_{24},L_{34}].$$

P r o o f. If L is a linear form in the Y_i's over $k[X1, X2, X3]$ in $\ker D$, then L has the form

$$L = \alpha_1 Y_1 + \alpha_2 Y_2 + \alpha_3 Y_3 + \alpha_4 Y_4$$

where $\alpha_i \in k[X_1, X_2, X_3]$ $i \in \{1, 2, 3, 4\}$. Since $L \in \ker D$, we have

$$\alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2 + \alpha_4 X_2 X_3 = 0. \tag{7}$$

Let $\phi = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \alpha_3 X_3^2$, then equation (7) shows that both X_2 and X_3 are divisors of ϕ. Taking equation (7) modulo X_2 gives that

$$X_1^2 \alpha_{12} + X_3^2 \alpha_{32} = 0 \tag{8}$$

where $\alpha_{12} = \alpha_1 \mid_{X_2=0}$ and $\alpha_{32} = \alpha_3 \mid_{X_2=0}$. Since X_1 and X_3 are relatively prime, equation (8) implies that $\alpha_1 = -X_3^2 \beta_{32} + X_2 \beta_1$ and $\alpha_3 = X_1^2 \beta_{32} + X_2 \beta_3$ for some $\beta_1, \beta_3 \in k[X_1, X_2, X_3]$ and β_{32} in $k[X_1, X_3]$. After simplification we find

$$\phi = X_1^2 X_2 \beta_1 + X_2 X_3^2 \beta_3 + \alpha_2 X_2^2. \tag{9}$$

Since X_3 is a divisor of ϕ, equation (9) implies that

$$X_1^2 X_2 \beta_1 \mid_{X_3=0} + X_2^2 \alpha_2 \mid_{X_3=0} = 0.$$

Consequently, $\alpha_2 = X_1^2 u + X_3 v$ and $\beta_1 = -X_2 u + X_3 w$ for some $u \in k[X_1, X_2]$ and $v, w \in k[X_1, X_2, X_3]$. Replacing these values of α_2 and β_1 in the expression (9) of ϕ, we get

$$\phi = X_2 X_3 (X_1^2 w + X_3 \beta_3 + X_2 v)$$

and consequently $\alpha_4 = -\phi/(X_2 X_3) = -(X_1^2 w + X_3 \beta_3 + X_2 v)$. Hence,

$$\begin{aligned}
\alpha_1 &= -X_2^2 u - X_3^2 \beta_{32} + X_2 X_3 w \\
\alpha_2 &= X_1^2 u + X_3 v \\
\alpha_3 &= X_1^2 \beta_{32} + X_2 \beta_3 \\
\alpha_4 &= -(X_1^2 w + X_3 \beta_3 + X_2 v)
\end{aligned}$$

and so

$$\begin{aligned}
L &= \alpha_1 Y_1 + \alpha_2 Y_2 + \alpha_3 Y_3 + \alpha_4 Y_4 \\
&= u(X_1^2 Y_2 - X_2^2 Y_1) + \beta_{32}(X_1^2 Y_3 - X_3^2 Y_1) \\
&+ v(X_3 Y_2 - X_2 Y_3) - w(X_1^2 Y_4 - X_2 X_3 Y_1) \\
&+ \beta_3 (X_2 Y_3 - X_3 Y_2) \\
&\in k[X_1, X_2, X_3, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}]. \quad \square
\end{aligned}$$

Lemma 7.3. *With the above notation,*

$$f \notin k[X_1, X_2, X_3, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}].$$

Proof. If $f \in k[X_1, X_2, X_3, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}]$, we can choose a polynomial Φ in

$$E := k[X_1, X_2, X_3, U_1, U_2, U_3, U_4, U_5]$$

such that

$$f = \Phi(X_1, X_2, X_3, L_{12}, L_{13}, L_{14}, L_{24}, L_{34}). \tag{10}$$

Consider the $\mathbb{N}^2$-grading on $k[X, Y]$ defined by declaring $k \subseteq k[X, Y]_{(0,0)}$ and $\deg(X_i) = (1, 0)$, $\deg(Y_j) = (0, 1)$ for $i \in \{1, 2, 3\}$ and $j \in \{1, 2, 3, 4\}$. Also define a similar $\mathbb{N}^2$-grading on E by $k \subseteq E_{(0,0)}$ and $\deg(X_i) = (1, 0)$, $\deg(U_j) = (2, 1)$ for $j \in \{1, 2, 3\}$, and $\deg(U_4) = \deg(U_5) = (1, 1)$. Write

$$\Phi = \Phi_{d_1} + \Phi_{d_2} + \cdots \Phi_{d_r}$$

where Φ_{d_i} is the homogeneous component of Φ of degree $d_i \in \mathbb{N}^2$. Since the elements $L_{12}, L_{13}, L_{14}, L_{24}, L_{34}$ are all homogeneous with respect to the $\mathbb{N}^2$-grading on $k[X, Y]$ defined above, it is easy to check that

$$\Phi_{d_i}(X_1, X_2, X_3, L_{12}, L_{13}, L_{14}, L_{24}, L_{34})$$

is either zero or homogeneous of degree d_i, for all $i \in \{1, \ldots, r\}$. Also, since f is a homogeneous element of degree $(2, 2)$ of $k[X, Y]$, equation (10) implies that

$$f = \Phi_{(2,2)}(X_1, X_2, X_3, L_{12}, L_{13}, L_{14}, L_{24}, L_{34})$$

and this can only happen if

$$f = aL_{24}^2 + bL_{34}^2 + cL_{24}L_{34} \tag{11}$$

for some $a, b, c \in k$. Indeed, a homogeneous element of degree $(2, 2)$ of E can only be a linear combination of U_4^2, U_5^2 and U_4U_5 because of the degrees of the X_i's and the U_i's defined above.

Now equation (11) implies that $f \in k[X_2, X_3, Y_2, Y_3, Y_4]$, which is absurd. $\square$

Theorem 7.1 is now a direct consequence of the above two lemmas.

8. The property of being elementary. Let $B = R^{[m]}$, where R is a UFD containing the rationals; given an irreducible locally nilpotent derivation D of B, can we determine whether D is R-elementary? (That is, can we decide whether there exists a coordinate system $(Y_1, \dots, Y_m)$ of B over R satisfying $DY_i \in R$ for all i?)

An answer in general seems to be hard. The present section answers the question in the case where R is a PID and $m = 2$.

We start with two well known facts:

Proposition 8.1 ([2]). *Let R be a UFD containing $\mathbb{Q}$ and let $D \neq 0$ be a locally nilpotent R-derivation of $B = R[Y_1, Y_2] \cong R^{[2]}$. Then there exists $P \in B$ and $\alpha \in \ker D$ such that* $\ker D = R[P]$ *and* $D = \alpha \left(P_{Y_2} \dfrac{\partial}{\partial Y_1} - P_{Y_1} \dfrac{\partial}{\partial Y_2} \right)$.

Proposition 8.2 ([7]). *Let R be a $\mathbb{Q}$-algebra, let $P \in B = R[Y_1, Y_2] \cong R^{[2]}$ and define $\Delta_P = P_{Y_2} \dfrac{\partial}{\partial Y_1} - P_{Y_1} \dfrac{\partial}{\partial Y_2} : B \to B$. Then the following are equivalent.*

1. *P is a variable of B over R*
2. *D is locally nilpotent, has a slice and* $\ker D = R[P]$.

Lemma 8.1. *Let R be PID containing $\mathbb{Q}$, $B = R^{[m]}$ and $D : B \to B$ an irreducible R-derivation. The following are equivalent:*

1. *D is R-elementary*
2. *$D = \partial/\partial Z_1$ for some coordinate system $(Z_1, \dots, Z_m)$ of B over R.*

Proof. If D is R-elementary, then there exists a coordinate system $(Y_1, \dots, Y_m)$ of B over R satisfying $DY_i \in R$ for all i. Let $a_i = DY_i$ for each i. Since R is a PID, $(a_1, \dots, a_m)B$ is a principal ideal of B and it follows that $(a_1, \dots, a_m)B = B$ by the irreducibility of D; so D is fix-point-free. As R is Hermite (every PID is Hermite), Proposition 6.1 implies that condition (2) holds. The converse is clear. $\square$

Proposition 8.3. *Let R be PID containing $\mathbb{Q}$, $B = R^{[2]}$ and $D : B \to B$ an irreducible R-derivation. The following are equivalent:*

1. *D is R-elementary*
2. *D is locally nilpotent and fix-point-free.*

P r o o f. By Lemma 8.1, it is clear that (1) implies (2). If (2) holds, let (Y_1, Y_2) be any coordinate system of B over R; then Propositions 8.1 and 8.2 imply that, for some variable P of B over R, we have $\ker D = R[P]$ and $D = P_{Y_2}\dfrac{\partial}{\partial Y_1} - P_{Y_1}\dfrac{\partial}{\partial Y_2}$. Choose Q such that $B = R[P, Q]$, then $D(Q) \in R^*$ and $D(P) = 0 \in R$, so D is R-elementary. $\square$

Example 8.1. Choose $f(X) \in k[X]$ and $g(X, Y) \in k[X, Y]$ such that

$$\gcd(f(X), g(X, Y)) = 1$$

and let D be the k-derivation of $k[X, Y, Z]$ defined by

$$D(X) = 0, \quad D(Y) = f(X), \quad D(Z) = g(X, Y)\ .$$

Then D is an irreducible locally nilpotent $k[X]$-derivation of $k[X, Y, Z]$. By Proposition 8.3, D is $k[X]$-elementary if and only if

$$(f(X), g(X, Y))k[X, Y] = k[X, Y].$$

We conclude with the following:

Proposition 8.4. *If R is a PID containing $\mathbb{Q}$, then any nonzero R-elementary derivation of $B = R[Y_1, \ldots, Y_m]$ is standard.*

P r o o f. Let $D = \sum_{i=1}^{m} a_i \dfrac{\partial}{\partial Y_i}$ be such a derivation of B ($a_i \in R$ for all i). Write $D = \alpha D'$ where $\alpha \in B$ and $D' : B \to B$ is an irreducible derivation. Note that $\alpha D'(Y_i) \in R$ for all i; it follows that $\alpha \in R$ and that D' is R-elementary. By Lemma 8.1, D' is standard and hence D is also standard. $\square$

REFERENCES

[1] D. Cox, J. Little, D. O'Shea. Ideals, Varieties, and Algorithms. Springer-Verlag, New York, 1992.

[2] D. Daigle, G. Freudenburg. Locally nilpotent derivations over a UFD and an application to rank two locally nilpotent derivations of $k[X_1, \ldots, X_n]$. *J. Algebra*, **204** (1998), 353–371.

[3] J. Deveney, D. Finston. G_a actions on $\mathbf{C}^3$ and $\mathbf{C}^7$. *Comm. Algebra* **22**, *15* (1994), 6295–6302.

[4] M. Hochster. Nonuniqueness of coefficient rings in a polynomial ring. *Proc. Amer. Math. Soc.* **34**, *1* (1972), 81–82.

[5] J. Khoury. On some properties of locally nilpotent derivations in dimension six. *J. Pure Appl. Algebra* **156/1** (2001), 69–79.

[6] P. Roberts. An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth Problem. *J. Algebra* **132** (1990) 461–473.

[7] Arno van den Essen, Peter van Rossum. Coordinates in two variables over a $\mathbb{Q}$-algebra. *Trans. Amer. Math. Soc.* **356** (2004), 1691–1703.

[8] D. Wright. On the jacobian conjecture. *Illinois J. Mathematics* **25** (1981), 423–440.

Department of Mathematics and Statistics
University of Ottawa
585 King Edward Ave.
Ottawa, ON K1N 6N5
Canada
email: `jkhoury@matrix.cc.uottawa.ca`

Received June 18, 2004
Revised July 26, 2004