ELSEVIER

Journal of Pure and Applied Algebra 156 (2001) 69–79

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

On some properties of elementary derivations in dimension six

Joseph Khoury

Department of Mathematics, University of Ottawa, 585 King Edward, Ottawa, Ont., Canada K1N 6N5

Received 20 April 1999; received in revised form 29 June 1999
Communicated by C.A. Weibel

Abstract

Given a UFD R containing the rationals, we study elementary derivations of the polynomial ring in three variables over R. A consequence of Theorem 2.1, is that the kernel of every elementary monomial derivation of $k^{[6]}$ (k is a field of characteristic zero) is generated over k by at most six elements. In particular, seven is the lowest dimension in which we can construct a counterexample to Hilbert fourteenth's problem of Robert's type (see, Roberts, J. Algebra 132 (1990) 461–473).

MSC: 13B10; 14L30; 14E09; 13A50

1. Introduction

Throughout, k denotes a field of characteristic zero.

It is a well-known fact (see for example [11]) that algebraic $\boldsymbol{G}_a$-actions on affine spaces $\boldsymbol{A}_k^n$ are equivalent to locally nilpotent k-derivations of $k^{[n]}$ (see Definition 2.1 below), the polynomial ring in n variables over k. An important question to look at, when studying a derivation of $k^{[n]}$, is whether or not its kernel is a finitely generated k-algebra. This question was answered positively by Nagata and Nowicki [9] in the case $n \leq 3$. In higher dimensions, many examples of locally nilpotent derivations having nonfinitely generated kernels have been found, and each of these examples represents a counterexample to the famous 14th problem of Hilbert, that can be stated as follows:

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

E-mail address: s060855@matrix.cc.uottowa.ca (J. Khoury).

0022-4049/01/$ - see front matter
PII: S0022-4049(99)00121-8

The first counterexample to Hilbert's problem was given by Nagata [8] in 1958 and it was in dimension 32. In 1993, Derksen [3] proved that Nagata's example can be realized as the kernel of a derivation of $k^{[32]}$. The same thing happened with the second counterexample to Hilbert's fourteenth found by Roberts in 1990 [10] in dimension seven, and which was used by Deveney and Finston [5] to show that the kernel of the derivation

$$D = X_1^{t+1}\frac{\partial}{\partial Y_1} + X_2^{t+1}\frac{\partial}{\partial Y_2} + X_3^{t+1}\frac{\partial}{\partial Y_3} + (X_1X_2X_3)^t\frac{\partial}{\partial Y_4}$$

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 $t \geq 2$.

In 1998, a counterexample in dimension six was constructed by Freudenburg [6] as the field of fractions of the kernel of the derivation

$$d = X_1^3\frac{\partial}{\partial Y_1} + X_2^3Y_1\frac{\partial}{\partial Y_2} + X_2^3Y_2\frac{\partial}{\partial Y_3} + X_1^2X_2^2\frac{\partial}{\partial Y_4}$$

of $k[X_1,X_2,Y_1,Y_2,Y_3,Y_4]$.

Then Daigle and Freudenburg [2] constructed a counterexample in dimension five as the field of fractions of the kernel of the derivation

$$T = X_1^3\frac{\partial}{\partial X_2} + X_2\frac{\partial}{\partial X_3} + X_3\frac{\partial}{\partial X_4} + X_1^2\frac{\partial}{\partial X_5}$$

of $k[X_1,X_2,X_3,X_4,X_5]$. This leaves Hilbert's problem open only in dimension four.

A closer look at Robert's example suggests that we study a special type of derivations of polynomial rings called *elementary derivations* (see [13] for important aspects of elementary derivations).

If $n,m \geq 1$, then a derivation D of the polynomial ring $B{:=}k[X_1,\ldots,X_n,Y_1,\ldots,Y_m]$ is called *elementary* if it is of the form

$$D = a_1(X_1,\ldots,X_n)\frac{\partial}{\partial Y_1} + \cdots + a_m(X_1,\ldots,X_n)\frac{\partial}{\partial Y_m},$$

where each a_i is in $k[X_1,\ldots,X_n]$. It is called *monomial* if it is of the form

$$D = b_1\frac{\partial}{\partial X_1} + \cdots + b_n\frac{\partial}{\partial X_n} + b_{n+1}\frac{\partial}{\partial Y_1} + \cdots + b_{n+m}\frac{\partial}{\partial Y_m}.$$

where each b_i is a monomial in $X_1,\ldots,X_n$, $Y_1,\ldots,Y_m$. This means that the counterexample found by Roberts is the field of fractions of $\ker D$ for some monomial elementary derivation D of $k^{[7]}$. Having in mind that every derivation with infinitely generated kernel yields a counterexample to Hilbert's 14th problem, we show that a counterexample to Hilbert's problem of Robert's type cannot be constructed in dimension six. Namely we will prove the following.

Theorem 1.1. *The kernel of any elementary monomial derivation of $k^{[6]}$ is generated by at most six linear elements in the Y_i's.*

Note that both derivations d and T are monomial, but not elementary.

Elementary derivations of polynomial rings over k were studied in detail in [13], where it was shown that the kernel of any elementary derivation of B is a finitely generated k-algebra in the case where $n+m \leq 5$. Also it was shown in [13] that if $n \geq 3$ and $m \geq 4$, then the kernel of any derivation of Robert's type is not a finitely generated k-algebra. It remains the case where $m=3$ and $n \geq 3$ about which little is known (see Question 4.3 in [13]). Theorem 1.1 gives then new information about this case. In fact in Section 2, we will prove a result (see Theorem 2.1) for the case $m=3$ in the more general case where B is a polynomial ring over a UFD.

All rings in this paper are commutative and have an identity element. If A is a ring, the notation $B = A^{[n]}$ means that B is isomorphic to a polynomial ring in n variables over A. If $A \subset B$ are rings, we say that A is *factorially closed* in B if, for $x, y \in B$, $xy \in A \setminus \{0\}$ implies that $x, y \in A$.

2. Elementary derivations of $R[Y_1, Y_2, Y_3]$

Definition 2.1. Let B be a domain containing the rationals.

(1) A *derivation* of B is a map $D : B \to B$ satisfying $D(x+y) = D(x) + D(y)$ and $D(xy) = xD(y) + yD(x)$ for all $x, y \in B$.

(2) The derivation D is called *locally nilpotent* if for every $x \in B$, there exists $n \geq 0$ such that $D^n(x) = 0$.

(3) If A is a subalgebra of B, then D is called an *A-derivation* if $D(a) = 0$ for all $a \in A$.

(4) A derivation D of B is called *irreducible* if the only principal ideal of B containing $D(B)$ is B.

Definition 2.2. If $B = R[Y_1, \ldots, Y_m]$ is a polynomial ring in m variables over a domain R, then a derivation D of B is called *R-elementary* if it is of the form

$$D = \sum_{i=1}^{m} a_i \partial_i$$

for some $a_i \in R$ and where ∂_i means the partial derivative with respect to Y_i.

With the notations of Definition 2.2, it is easy to see that an R-elementary derivation of B is locally nilpotent and an R-derivation. Also, if R is a UFD, then the R-elementary derivation $D = \sum_{i=1}^{m} a_i \partial_i$ of B is irreducible if and only if the elements $a_1, \ldots, a_m$ of R are relatively prime.

For a list of basic facts about locally nilpotent derivations we refer the reader to Section 1.1 in [1].

For the main theorem of this section, let R be a UFD which is finitely generated k-algebra, and $B = R[Y_1, Y_2, Y_3] = R^{[3]}$. If a_1, a_2, a_3 are relatively prime elements of R, define $g_i := \gcd(a_j, a_k)$ for $i = 1, 2, 3$ and $\{i, j, k\} = \{1, 2, 3\}$, and fix the three elements of B

$$L_1 = \frac{a_3}{g_1} Y_2 - \frac{a_2}{g_1} Y_3, \quad L_2 = -\frac{a_3}{g_2} Y_1 + \frac{a_1}{g_2} Y_3, \quad L_3 = \frac{a_2}{g_3} Y_1 - \frac{a_1}{g_3} Y_2$$

with the understanding that $g_i = 1$ and $L_i = 0$ when $a_i = a_k = 0$. Then we have the following easy lemma.

Lemma 2.1. (1) *g_1, g_2, g_3 are pairwise relatively prime in R.*
(2) *If $\{i,j,k\} = \{1,2,3\}$, then $g_i g_j$ is a divisor of a_k in R.*
(3) *Write $a_k = \alpha_k g_i g_j$ for $\{i,j,k\} = \{1,2,3\}$, then $\alpha_1, \alpha_2, \alpha_3$ are pairwise relatively prime in R.*
(4) *$L_i \in \ker D$ for all $i \in \{1,2,3\}$ where D is the elementary derivation $a_1\partial_1 + a_2\partial_2 + a_3\partial_3$ of B.*

Proof. Left to the reader. □

The main theorem in this section is the following.

Theorem 2.1. *Let R be a UFD which is a finitely generated k-algebra, and let $B = R[Y_1, Y_2, Y_3] = R^{[3]}$. Let $D = a_1\partial_1 + a_2\partial_2 + a_3\partial_3$ be an irreducible R-elementary derivation of B (i.e. $\gcd(a_1, a_2, a_3) = 1$) and let g_i, α_i, L_i $(i = 1,2,3)$ be as above. Assume that $a_3 \neq 0$ and that for every prime divisor p of a_3, the ring $\bar{R} := R/pR$ is a UFD. Then* $\ker D = R[L_1, L_2, L_3]$ *if and only if* $\gcd(\overline{\alpha_1}, \overline{\alpha_2}, \overline{\alpha_3}) = 1$ in $\bar{R}$ *for every prime divisor p* of a_3.

Remark 2.1. With the notations of Theorem 2.1, if only one of the a_i's, say a_3, is zero, then Theorem 2.4 of [1] implies that the kernel of the derivation $a_1\partial_1 + a_2\partial_2$ of $R[Y_1, Y_2]$ is $R[a_1Y_2 - a_2Y_1] = R[L_3]$, and so $\ker D = R[L_3, Y_3] = R[L_1, L_2, L_3]$ (since in this case $L_1 = -Y_3$ and $L_2 = Y_3$). If two of the a_i's are equal to zero, say $a_1 = a_2 = 0$, then clearly $\ker D = R[Y_1, Y_2] = R[L_1, L_2, L_3]$ (since $L_1 = Y_2$, $L_2 = -Y_1$ and $L_3 = 0$ in this case). So if one at least of the a_i's is zero, $\ker D = R[L_1, L_2, L_3]$.

The proof of Theorem 2.1 requires the following fact (see also the algorithm of van den Essen in [12]):

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 $E \setminus \{0\}$ satisfies*:
- $(A_0)_d = (A)_d$
- *$pC \cap A_0 = pA_0$ for each prime divisor p of d,*
  then $A_0 = A$.

Proof. The assumption $pC \cap A_0 = pA_0$ implies (by an easy induction argument) that if q is a finite product of prime factors of d, then $qC \cap A_0 = qA_0$. In particular, $d^nC \cap A_0 = d^nA_0$ for all $n \geq 0$. Now if $y \in A$, then $d^n y \in A_0$ for some $n \geq 0$, so $d^n y \in d^nC \cap A_0 = d^nA_0$ and $y \in A_0$. □

Another result needed for the proof of Theorem 2.1 is the following.

Proposition 2.1. *Let $a_1,\dots,a_m$, $m \geq 1$ be elements of a UFD E containing the rationals, and let A be the kernel of the corresponding E-elementary derivation $D = a_1\partial_1 + \cdots + a_m\partial_m$ of $C := E[Y_1,\dots,Y_m]$. Fix $i \in \{1,\dots,m\}$ such that $a_i \neq 0$ and consider the E-algebra A_i generated by the $m-1$ elements*

$$L_{ij} := \frac{a_i}{g_{ij}}Y_j - \frac{a_j}{g_{ij}}Y_i, \quad j \in \{1,\dots,m\} \setminus \{i\},$$

where $g_{ij} = \gcd(a_i,a_j)$. Then $(A)_{a_i} = (A_i)_{a_i}$.

Proof. For the proof, we may clearly assume that $i = 1$ (so $a_1 \neq 0$). Note that if $i \neq j$, then $D(L_{ij}) = 0$ and hence $A_1 := E[L_{1j}\colon j > 1] \subseteq A$. Let $S := \{a_1^n;\ n \geq 0\}$, then S is a multiplicatively closed subset of $E \subseteq A$, and hence D induces a locally nilpotent derivation $S^{-1}D : S^{-1}C \to S^{-1}C$ (defined by the quotient rule of derivation) satisfying $A_{a_1} = S^{-1}A = \ker S^{-1}D$. On the other hand, Y_1/a_1 is a slice for $S^{-1}D$ (i.e., $S^{-1}D(Y_1/a_1) = 1$) and it is a well-known fact (see for example Lemma 2.1 of [4]) that $\ker S^{-1}D$ is equal to $\operatorname{im}\zeta$ where ζ is the homomorphism

$$S^{-1}C \to S^{-1}C$$

$$c \mapsto \sum_{j \geq 0} \frac{1}{j!}\left(-\frac{Y_1}{a_1}\right)^j (S^{-1}D)^j(c).$$

We have $\zeta(Y_1) = 0$ and, for $i > 1$, $\zeta(Y_i) = Y_i - (a_i/a_1)Y_1 = (g_{1i}/a_1)L_{1i}$, where g_{1i}/a_1 is a unit of E_{a_1}. So, $A_{a_1} = \operatorname{im}\zeta = E_{a_1}[L_{12},\dots,L_{1m}] = (A_1)_{a_1}$, which proves the proposition. □

Corollary 2.1. *With the notion of Theorem* 2.1, $(\ker D)_{a_i} = (R[L_1,L_2,L_3])_{a_i}$ *for any* $i \in \{1,2,3\}$.

The crucial step in the proof of Theorem 2.1 is the following lemma.

Lemma 2.3. *With the notations of Theorem* 2.1, if $p \in R$ *is a prime element such that* $\bar{R} := R/pR$ *is a UFD, then* $pB \cap R[L_1,L_2,L_3] = pR[L_1,L_2,L_3]$ *if and only if the elements* $\bar{\alpha}_1,\bar{\alpha}_2,\bar{\alpha}_3$ *of* $\bar{R}$ *are relatively prime.*

Proof. If one of the a_i's is zero, then Remark 2.1 implies that $\ker D = R[L_1,L_2,L_3]$ and hence $R[L_1,L_2,L_3]$ is a factorially closed subring of B and so the equality $pB \cap R[L_1,L_2,L_3] = pR[L_1,L_2,L_3]$ is true. On the other hand, it is easy to see that one of the α_i's is invertible in this case, and so $\gcd(\bar{\alpha}_1,\bar{\alpha}_2,\bar{\alpha}_3) = 1$. Thus, we may, and will assume that $a_i \neq 0$ for all i.

Let $R_0 = R[L_1,L_2,L_3] \subseteq \ker D$. Assume first that $\bar{\alpha}_1,\bar{\alpha}_2,\bar{\alpha}_3$ are relatively prime in $\bar{R}$, we need to prove that $pB \cap R_0 \subseteq pR_0$ (the other inclusion being clear). To see this, consider the ring homomorphism

$$\phi : \bar{R}[S,T,U] \to \bar{R}[\bar{L}_1,\bar{L}_2,\bar{L}_3],$$

sending S,T,U to $\bar{L}_1,\bar{L}_2,\bar{L}_3$, respectively, and let $\wp$ be the kernel of ϕ.

Claim. *$\wp = \bar{q}\bar{R}[S,T,U]$ where $\bar{q} = \bar{\alpha}_1 S + \bar{\alpha}_2 T + \bar{\alpha}_3 U$.*

Indeed, modulo p we have that $\bar{L}_1 = \overline{\alpha_3 g_2} Y_2 - \overline{\alpha_2 g_3} Y_3$, $\bar{L}_2 = -\overline{\alpha_3 g_1} Y_1 + \overline{\alpha_1 g_3} Y_3$, $\bar{L}_3 = \overline{\alpha_2 g_1} Y_1 - \overline{\alpha_1 g_2} Y_2$ and since $\overline{\alpha_1 L_1} + \overline{\alpha_2 L_2} + \overline{\alpha_3 L_3} = 0$ in $\bar{R}$ (in fact $\alpha_1 L_1 + \alpha_2 L_2 + \alpha_3 L_3 = 0$ in R), then $\mathrm{trdeg}_{\bar{R}} \bar{R}[\bar{L}_1, \bar{L}_2, \bar{L}_3] = 2$. Hence the height of $\wp$ is one, and $\wp$ is a principal ideal of $\bar{R}[S,T,U]$ since $\bar{R}$ is a UFD. Consider the element $\bar{q} = \bar{\alpha}_1 S + \bar{\alpha}_2 T + \bar{\alpha}_3 U \in \bar{R}[S,T,U]$, then clearly $\phi(\bar{q}) = 0$, and since $\gcd(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = 1$ by assumption, $\bar{q}$ is irreducible. Thus $\wp = \bar{q}\bar{R}[S,T,U]$ as claimed.

From the claim, it follows easily that the kernel of the homomorphism

$$\psi : R[S,T,U] \to R[L_1, L_2, L_3] \to \bar{R}[\bar{L}_1, \bar{L}_2, \bar{L}_3]$$

is the ideal $(\alpha_1 S + \alpha_2 T + \alpha_3 U, p)$ of $R[S,T,U]$. Now we prove the inclusion $pB \cap R_0 \subseteq pR_0$. Let $x \in pB \cap R_0$ and choose $\Phi \in R[S,T,U]$ and $b \in B$ such that $x = pb = \Phi(L_1, L_2, L_3)$, then clearly $\Phi \in \ker(\psi)$ and hence we can write $\Phi = (\alpha_1 S + \alpha_2 T + \alpha_3 U)\Phi_1 + p\Phi_2$ for some $\Phi_1, \Phi_2 \in R[S,T,U]$. This shows that $x = p\Phi_2(L_1, L_2, L_3) \in pR_0$.

Next, we prove the other direction. Assume that $pB \cap R_0 = pR_0$, we show that $\gcd(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = 1$ in $\bar{R}$. Let $g \in R$ be such that $\bar{g} = \gcd(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3)$ in $\bar{R}$ and write $\bar{\alpha}_i = \bar{\beta}_i \bar{g}$ for some $\beta_i \in R$, and $\gcd(\bar{\beta}_1, \bar{\beta}_2, \bar{\beta}_3) = 1$ in $\bar{R}$. Also, choose $\zeta_i \in R$ such that

$$\alpha_i = \beta_i g + \zeta_i p \tag{1}$$

for $i \in \{1,2,3\}$. Now since $\overline{\alpha_1 L_1} + \overline{\alpha_2 L_2} + \overline{\alpha_3 L_3} = 0$, then either $\bar{g} = 0$ or $\overline{\beta_1 L_1} + \overline{\beta_2 L_2} + \overline{\beta_3 L_3} = 0$. If, $\bar{g} = 0$, then $g = rp$ for some $r \in R$, and Eq. (1) implies that $p | \alpha_i$ for all i, which gives a contradiction to the fact that the α_i's are relatively prime (Lemma 2.1). We deduce that $\beta_1 L_1 + \beta_2 L_2 + \beta_3 L_3 \in pB \cap R_0 = pR_0$. Choose $\Phi \in R[S,T,U]$ such that $\beta_1 L_1 + \beta_2 L_2 + \beta_3 L_3 = p\Phi(L_1, L_2, L_3)$ and write $\Phi = \Phi_0 + \Phi_1 + \cdots + \Phi_n$ where Φ_i is the homogeneous component of Φ of degree i. Since each L_i is homogeneous of degree 1, then each $\Phi_i(L_1, L_2, L_3)$ is also homogeneous of degree i, and this means that $\Phi_i(L_1, L_2, L_3) = 0$ for all $i \neq 1$. Thus, $\beta_1 L_1 + \beta_2 L_2 + \beta_3 L_3 = p\Phi(L_1, L_2, L_3) = p(\gamma_1 L_1 + \gamma_2 L_2 + \gamma_3 L_3)$ where $\gamma_i \in R$ for all i and this gives the equation

$$(\beta_1 - p\gamma_1)L_1 + (\beta_2 - p\gamma_2)L_2 + (\beta_3 - p\gamma_3)L_3 = 0.$$

Let $\lambda_i := \beta_i - p\gamma_i$ for all $i \in \{1,2,3\}$, then we have the equations

$$\lambda_1 L_1 + \lambda_2 L_2 + \lambda_3 L_3 = 0, \tag{2}$$

$$\alpha_1 L_1 + \alpha_2 L_2 + \alpha_3 L_3 = 0. \tag{3}$$

Let K be the field of fractions of R, then clearly L_i, L_j are linearly independent over K as vectors of the K-vector space

$$V = \{P \in K[Y_1, Y_2, Y_3] \mid P \text{ is homogeneous of degree one}\}.$$

Also, since $\bar{\beta}_i \neq 0$ for at least one $i \in \{1,2,3\}$ (otherwise, the β_i's would not be relatively prime), we deduce that $\lambda_i \neq 0$ for at least one i. Assume that $\lambda_1 \neq 0$, then from Eqs. (2) and (3) above we can deduce that

$$\frac{\alpha_2}{\alpha_1} L_2 + \frac{\alpha_3}{\alpha_1} L_3 = \frac{\lambda_2}{\lambda_1} L_2 + \frac{\lambda_3}{\lambda_1} L_3$$

as elements of V. This gives the two equations

$$\alpha_i\lambda_1 = \alpha_1\lambda_i, \quad i = 2,3. \tag{4}$$

Now since α_1, α_i are relatively prime for $i = 2,3$ (Lemma 2.1), then Eq. (4) shows that α_i divides λ_i for $i = 1,2,3$, and Eq. (4) implies that $\lambda_i = \mu\alpha_i$ for $i = 1,2,3$, where $\mu = \lambda_1/\alpha_1 \in R$. Hence $\beta_i - p\gamma_i = \mu\alpha_i = \mu(\beta_i g + \zeta_i p)$ for all $i = 1,2,3$. In other words, $\bar{\beta}_i(1 - \overline{\mu g}) = 0$ for all $i \in \{1,2,3\}$. Choose i such that $\bar{\beta}_i \neq 0$, then $\overline{\mu g} = 1$ and hence $\bar{g} \in \bar{R}^*$. This shows that $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3$ are relatively prime in $\bar{R}$ and the lemma is proved. □

The main theorem of this section can now be deduced easily from the above lemma.

Proof of Theorem 2.1. If $\ker D = R[L_1, L_2, L_3]$, then in particular, $R[L_1, L_2, L_3]$ is factorially closed in B (as the kernel of a locally nilpotent derivation of B). Let p be a prime divisor of a_3 and let $x \in pB \cap R[L_1, L_2, L_3]$, and write $x = pb$ for some $b \in B$, then $b \in R[L_1, L_2, L_3]$ since the latter is factorially closed, and so $pB \cap R[L_1, L_2, L_3] = pR[L_1, L_2, L_3]$. Then Lemma 2.3 gives that gcd $(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = 1$. Conversely, assume that for each prime divisor p of a_3, the elements $\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3$ of $\bar{R} := R/pR$ are relatively prime, then by Lemma 2.3, $pB \cap R[L_1, L_2, L_3] = pR[L_1, L_2, L_3]$ for all prime divisors p of a_3. By Corollary 2.1 and Lemma 2.2, we deduce that $\ker D = R[L_1, L_2, L_3]$. □

An important consequence of the above theorem is the following.

Corollary 2.2. *If $R = k[X_1, \ldots, X_n]$ is a polynomial ring in n variables ($n \geq 1$) over k, then the kernel of any elementary monomial derivation of $R[Y_1, Y_2, Y_3]$ is equal to $R[L_1, L_2, L_3]$.*

Proof. Let $D = a_1\partial_1 + a_2\partial_2 + a_3\partial_3$ be an elementary monomial derivation of $B = R[Y_1, Y_2, Y_3]$. We may assume that D is irreducible and (by Remark 2.1) that $a_i \neq 0$ for all i. Let α_i, L_i be as above. For any $i \in \{1, \ldots, n\}$, we can choose $j \neq k$ such that α_j, α_k are not divisible by X_i (since the α_i's are pairwise relatively prime). This means that

$$\alpha_j, \alpha_k \in k[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n] \cong k[X_1, \ldots, X_n]/(X_i)$$

and therefore the α_i's are relatively prime modulo X_i for any i. The corollary follows now from Theorem 2.1. □

Note that the elementary derivations encountered in this section satisfy the following conjecture.

Conjecture. *If the kernel of an R-elementary derivation D of $B = R[Y_1, Y_2, Y_3]$ is a finitely generated R-algebra, then the generators of* $\ker D$ *can be chosen to be linear in the Y_i's.*

3. Elementary monomial derivations in dimension six

The purpose of this section is to prove Theorem 1.1.

Let $B := k[X_1,\dots,X_n,\ Y_1,\dots,Y_m], n,\ m \geq 1,\ n+m=6,\ R=k[X_1,\dots,X_n]$ and D the R-elementary derivation $a_1\partial_1+\cdots+a_m\partial_m$ of B ($a_i \in R$ and ∂_i is the partial derivative with respect to Y_i).

For the proof of Theorem 1.1, we will consider several cases. It is known [13] that if $n=1,2,4,5$, then the kernel of any elementary derivation D of B is a finitely generated k-algebra. If in addition we assume that D is monomial, then we will show that its kernel is generated by at most six elements that are linear in the Y_i's. As for the case $n=m=3$, even the fact that the kernel is a finitely generated k-algebra seems to be a new result. Note also that for the proof of the Theorem 1.1 we may clearly assume that the derivation D is irreducible. Also, if $a_i=\alpha_i X_1^a X_2^b X_3^c$ for some $\alpha_i \in k^*$, and $a,b,c \in \mathbf{N}$, then we may assume that $\alpha_i=1$. We start with a proposition.

Proposition 3.1. *Let R be a UFD containing the rationals, $a_1,\dots,a_m \in R$, and let D be the R-elementary derivation $a_1\partial/\partial Y_1+\cdots+a_m\partial/\partial Y_m$ of $B := R[Y_1,\dots,Y_m]$. If $a_i \in R^*$ for some i, then $\ker D$ is generated by $m-1$ elements linear in $Y_1,\dots,Y_m$ (in fact $\ker D$ is a polynomial ring in $m-1$ variables over R).*

Proof. We may clearly assume that $a_1=1$. In this case consider the elements

$$f_1=a_2Y_1-Y_2,\quad f_2=a_3Y_1-Y_3,\dots,f_{m-1}=a_mY_1-Y_m$$

of B. Clearly $A' := R[f_1,\dots,f_{m-1}] \subseteq C := \ker D$, and since $Y_j=a_jY_1-f_{j-1}$ for all $j \geq 2$, we can easily see that $B=A'[Y_1]$. Since $A' \subseteq C \subset B$ and C is algebraically closed in B, it follows that $A'=C$. $\square$

Corollary 3.1. *Theorem 1.1 is true if $n=1$ or if $a_i=1$ for some i.*

Proof. If $n=1$, then $D=X_1^{n_1}\partial_1+\cdots+X_1^{n_5}\partial_5$, and by the irreducibility of D we may assume that $a_1=1$ and we are done by the above proposition. $\square$

By Corollary 2.2, Theorem 1.1 is true in the case $n=m=3$. We study next the case $n=2$, $m=4$. In this case, we will prove a more general result (the generalization is due to D. Daigle). Namely we have the following.

Theorem 3.1. *If $R=k[U,V]=k^{[2]}$ and $a_1,\dots,a_m,\ m \geq 1$ are monomials in U,V (not all zero), then the kernel of the elementary derivation $D=\sum_{i=1}^m a_i\partial_i$ of $B=R[Y_1,\dots,Y_m]$ is a polynomial ring in $m-1$ variables over R. Moreover, the $m-1$ generators of $\ker D$ can be chosen to be of the form $b_iY_i-b_jY_j$ where $1 \leq i<j \leq m$ and $b_i,b_j \in R$.*

The proof uses Lemma 3.1 (see below) which holds in the following more general situation: R is a UFD, $B=R[Y_1,\dots,Y_m]$ and $D: B \to B$ an R-elementary derivation of

B, i.e., of the form

$$D=\sum_{i=1}^{m} a_i\partial_i,$$

where $a_i \in R$ and ∂_i means the partial derivative with respect to Y_i. Also, for each pair $(i,j) \in \mathbf{N}^2$ with $1 \le i < j \le m$, define

$$L_{i,j}=\begin{cases} \left(\frac{a_j}{\gcd(a_i,a_j)}\right) Y_i-\left(\frac{a_j}{\gcd(a_i,a_j)}\right) Y_j & \text{if } a_i \neq 0 \text{ or } a_j \neq 0,\\ 0 & \text{if } a_i=a_j=0. \end{cases}$$

Then clearly $L_{i,j} \in \ker D$. For any integer $k \ge 0$, we say that "D has the property $P(k)$" if $D=0$ or $\ker D$ can be generated (as R-algebra) by k-elements of the $L_{i,j}$'s. With these notations, we have the following.

Lemma 3.1. *Suppose that for some $i \in \{1,\dots,m\}$, we have*
1. *The restriction D_i of D to $B_i=R[Y_1,\dots,Y_{i-1},\ Y_{i+1},\dots,Y_m]$ has the property $P(k)$;*
2. *$a_j \mid a_i$ for some $j \neq i$,*

then D has the property $P(k+1)$.

Proof. If $D=0$, there is nothing to prove, so we may assume $D \neq 0$ and consequently, we may choose $j \neq i$ such that $a_j \neq 0$ and $a_j \mid a_i$. Then the element $L=Y_i-a_i/a_j\,Y_j$ belongs to $\ker D$ and clearly $B=B_i[L]$, so $\ker D=(\ker D_i)[L]$ and D has the property $P(k+1)$. $\square$

Proof of Theorem 3.1. We proceed by induction on m, the case $m=1$ being obvious. By the induction hypothesis and Lemma 3.1, we may assume that a_i does not divide a_j whenever $i \neq j$; in particular $a_i \neq 0$ for all i so, multiplying each a_i (or rather Y_i) by a unit if necessary, we may assume that $a_i=U^{u_i}V^{v_i}$ for all i. We may also relabel the Y_i's in such a way that

$$u_1 > \cdots > u_m \quad \text{and} \quad v_1 < \cdots < v_m.$$

Note that $L_{i,j}=V^{v_j-v_i}\,Y_i-U^{u_i-u_j}\,Y_j$, where L_{ij} is as above. Let $A=R[L_{i,i+1}:1 \le i \le m-1]$, we will show that $\ker D=A$.

A simple calculation shows that

$$L_{i,j}=U^{u_i-u_{i+1}}\,L_{i+1,j}+\,V^{v_j-v_{i+1}}\,L_{i,i+1},$$

whenever $j-i>1$. In particular, $L_{i,j}$ belongs to the R-module generated by $L_{i+1,j}$ and $L_{i,i+1}$, and hence to the R-module generated by the set $\{L_{i,i+1} \mid 1 \le i \le m-1\}$. This shows that $L_{i,j} \in A$ for all i,j satisfying $i<j$. Also, it follows from Proposition 2.1 that $A_U=(\ker D)_U$ (by the irreducibility of D, we can find $i \in \{1,\dots,m\}$ such that $a_i=U^{\mu}$ for some $\mu \ge 1$), and consequently, it suffices (by Theorem 2.1) to prove that

$$A \cap UB=UA. \tag{5}$$

Clearly, $UA \subseteq A \cap UB$. Conversely, let $x \in A \cap UB$ and write $x=\Phi(L_{1,2},\dots,L_{m-1,m})$, where $\Phi \in R[T_1,\dots,T_{m-1}]$ is a polynomial in $m-1$ variables. Let $\bar{R}=R/UR$,

$\bar{B} = B/UB = \bar{R}[Y_1,\dots,Y_m]$ and let us take the images via $B \to \bar{B}$. Since $x \mapsto 0$ and $L_{i,i+1} \mapsto V^{v_{i+1}-v_i}Y_i$, this gives

$$\bar{\Phi}(V^{v_2-v_1}Y_1,\dots,V^{v_m-v_{m-1}}Y_{m-1}) = 0$$

and consequently $\bar{\Phi} = 0$. This means that each coefficient of Φ is divisible by U, and so $x \in UA$ and Eq. (5) is proved. $\square$

In particular, Theorem 3.1 shows that D has the property $P(m-1)$, and this means that if $n=2$ and $m=4$, then $\ker D$ is generated over k by at most five linear elements in the Y_i's. It remains now to consider the cases $n=4$, $m=2$ and $n=5$, $m=1$. In the first case, the derivation has the form $D = a_1\partial_1 + a_2\partial_2$, where $a_i \in k[X_1,\dots,X_4]$ and in this case, Proposition 4.1 of [13] shows that the kernel of D is $k[X_1,\dots,X_4, a_2Y_1 - a_1Y_2]$. In the case where $n=5$, $m=1$, it is easy to verify that the kernel is simply $k[X_1,\dots,X_5]$. This finishes the proof of Theorem 1.1.

Remark. One can easily notice the similarity between the main result of this paper and Maubach's result in [7].

Acknowledgements

I wish to thank Daniel Daigle of the university of Ottawa for his significant help on clarifying many aspects and tools used in this paper and on reshaping some of the proofs and hence saving me a great deal of embarassment.

References

[1] D. Daigle, G. Freudenburg, Locally nilpotent derivations over a UFD and an application to rank two locally nilpotent derivations of $k[X_1,\dots,X_n]$, J. Algebra 204 (1998) 353–371.
[2] D. Daigle, G. Freudenburg, A counterexample to Hilbert's fourteenth problem in dimension five, J. Algebra, to appear.
[3] H. Derksen, The kernel of a derivation, J. Pure Appl. Algebra 84 (1993) 13–16.
[4] J. Deveney, D. Finston, Fields of G_a invariants are ruled, Canad. Math. Bull 37 (1994) 37–41.
[5] J. Deveney, D. Finston, G_a actions on $\boldsymbol{C}^3$ and $\boldsymbol{C}^7$, Comm. Algebra 22 (15) (1994) 6295–6302.
[6] G. Freudenburg, A counterexample to Hilbert's Fourteenth Problem in dimension six, Transform. Groups, to appear.
[7] S. Maubach, Triangular monomial derivations on $k[X_1,X_2,X_3,X_4]$ have kernel generated by at most four elements, J. Pure Appl. Algebra 153 (2) (2000) 165–170.
[8] M. Nagata, On the fourteenth problem of Hilbert, Proceedings of the International Congress Mathematico, 1958, New York, Cambridge University Press, Cambridge, 1966, pp. 459–462.
[9] M. Nagata, A. Nowicki, Rings of constants for k-derivations in $k[X_1,\dots,X_n]$, J. Math. Kyoto Univ. 28 (1) (1988) 111–118.
[10] 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.
[11] D. Snow, Unipotent Actions on Affine Spaces, Topological Methods in Algebraic Transformation Groups, Birkhauser, Boston, 1989.

[12] A. van den Essen, An algorithm to compute the invariant ring of a G_a-action on an affine variety, J. Symbolic Comput. 16 (1993) 551–555.

[13] A. van den Essen, T. Janssen, Kernels of elementary derivations, University of Nijmegen, Report No. 9548, Nijmegen, The Netherlands, 1995.