

## A NOTE ON TRIANGULAR DERIVATIONS OF $\mathbf{k}[X_1, X_2, X_3, X_4]$

DANIEL DAIGLE AND GENE FREUDENBURG

(Communicated by Wolmer V. Vasconcelos)

ABSTRACT. For a field  $\mathbf{k}$  of characteristic zero, and for each integer  $n \geq 4$ , we construct a triangular derivation of  $\mathbf{k}[X_1, X_2, X_3, X_4]$  whose ring of constants, though finitely generated over  $\mathbf{k}$ , cannot be generated by fewer than  $n$  elements.

### 1. INTRODUCTION

Let  $\mathbf{k}$  be a field of characteristic zero. If  $R$  is a finitely generated  $\mathbf{k}$ -algebra, we write  $\#(R) = s$  to indicate that  $R$  can be generated by  $s$  elements but not by  $s - 1$ . The purpose of this note is to show:

**Theorem.** *Given any integer  $n \geq 3$ , there exists a triangular derivation  $\Delta$  of the polynomial ring  $\mathbf{k}[X_1, X_2, X_3, X_4]$  whose kernel satisfies  $n \leq \#(\ker \Delta) \leq n + 1$ .*

Equivalently, the theorem asserts that, given  $n \geq 3$ , there exists a triangular action of  $G_a = (\mathbf{k}, +)$  on  $\mathbb{A}^4$  whose ring of invariants satisfies  $n \leq \#\mathcal{O}(\mathbb{A}^4)^{G_a} \leq n + 1$ . The theorem is proved by constructing  $\Delta$  explicitly for  $n \geq 4$  (for  $n = 3$ , just use a partial derivative).

In contrast to our present result, the well-known theorem of Miyanishi [2] states that, for any locally nilpotent  $\mathbf{k}$ -derivation  $D$  of  $\mathbf{k}[X_1, X_2, X_3]$ ,  $\#(\ker D) = 2$ . At the other extreme, the authors recently found a triangular derivation of the ring  $\mathbf{k}[X_1, X_2, X_3, X_4, X_5]$  whose kernel is not finitely generated as a  $\mathbf{k}$ -algebra [1]. It is not known whether such kernels in dimension four are always finitely generated, even for triangular derivations.

### 2. PRELIMINARIES

A *triangular* derivation of  $\mathbf{k}[X_1, \dots, X_n]$  is a  $\mathbf{k}$ -derivation  $\Delta : \mathbf{k}[X_1, \dots, X_n] \rightarrow \mathbf{k}[X_1, \dots, X_n]$  satisfying  $\Delta(X_i) \in \mathbf{k}[X_1, \dots, X_{i-1}]$  for all  $i = 1, \dots, n$ .

An element of a submonoid  $\Gamma$  of  $(\mathbb{N}, +)$  is *primitive* if it is positive and cannot be written as the sum of two positive elements of  $\Gamma$ . It is easy to see that the set of primitive elements in  $\Gamma$  is a finite set which generates  $\Gamma$  and which is contained in every generating set.

The *support* of an element  $f = \sum_{i=0}^{\infty} a_i X^i$  of the power series ring  $\mathbf{k}[[X]]$  is  $\text{Supp}(f) = \{i \in \mathbb{N} \mid a_i \neq 0\}$ . Given a submonoid  $\Gamma$  of  $(\mathbb{N}, +)$ , the elements  $f$  of

---

Received by the editors March 25, 1999 and, in revised form, May 12, 1999.

2000 *Mathematics Subject Classification.* Primary 14R10; Secondary 14R20, 13N15.

*Key words and phrases.* Derivations, Hilbert fourteenth problem, additive group actions, invariants.

The first author's research was supported by NSERC Canada.

$\mathbf{k}[[X]]$  satisfying  $\text{Supp}(f) \subseteq \Gamma$  form a subalgebra of  $\mathbf{k}[[X]]$  which we denote  $\mathbf{k}[[\Gamma]]$ . We observe:

- If  $g_1, \dots, g_r \in \mathbf{k}[[\Gamma]]$  and  $P \in \mathbf{k}[[T_1, \dots, T_r]]$  satisfy  $\text{ord}(g_i) \geq 1$  for
- (1) all  $i$  and  $\text{ord}(P) \geq 2$ , then no primitive element of  $\Gamma$  belongs to the support of  $P(g_1, \dots, g_r)$ .

Indeed, let  $\gamma \in \text{Supp} P(g_1, \dots, g_r)$ ; then  $\gamma$  must be in the support of some monomial  $g_1^{i_1} \cdots g_r^{i_r}$  with  $i_1 + \cdots + i_r \geq 2$ , so  $\gamma$  is the sum of  $i_1 + \cdots + i_r$  elements of  $\bigcup_{i=1}^r \text{Supp}(g_i) \subseteq \Gamma \setminus \{0\}$  and hence is not primitive.

**Lemma 1.** *Let  $\Gamma$  be a submonoid of  $(\mathbb{N}, +)$ , let  $e_1 < \cdots < e_h$  be the primitive elements of  $\Gamma$ , let  $R = \mathbf{k}[X^{e_1}, \dots, X^{e_h}]$  and let  $T$  be an indeterminate over  $R$ . Then:*

$$\#(R) = h \quad \text{and} \quad \#(R[T]) = h + 1.$$

*Proof.* Given  $f \in R[T]$ , let  $f(0) \in \mathbf{k}[X]$  be the result of evaluating  $f$  at  $T = 0$ , and let  $\text{ord}(f) \in \mathbb{N} \cup \{\infty\}$  be the  $X$ -order of  $f(0)$ , i.e., the largest  $s \geq 0$  such that  $X^s$  divides  $f(0)$  in  $\mathbf{k}[X]$ . Note that  $\#(R) = h$  is a consequence of  $\#(R[T]) = h + 1$ , so it suffices to prove the latter.

Assume that  $\#(R[T]) \neq h + 1$ ; then  $R[T]$  can be generated by  $h$  elements, say  $R[T] = \mathbf{k}[f_1, \dots, f_h]$ . We begin by showing that, replacing if necessary the generating set  $\{f_1, \dots, f_h\}$  by another one with the same cardinality  $h$ , we may arrange that  $\text{ord}(f_j) = e_j$  for all  $j = 1, \dots, h$ . To see this, consider an integer  $i$  satisfying  $1 \leq i \leq h$  and

(2) 
$$\text{ord}(f_j) = e_j, \quad \text{for all } j < i$$

(this certainly holds for  $i = 1$ ). Observe that every element of  $\Gamma$  strictly less than  $e_i$  belongs to the monoid generated by  $\{e_1, \dots, e_{i-1}\}$ ; hence, replacing each  $f_j$  (with  $j \geq i$ ) by  $f_j$  plus a suitable polynomial in  $(f_1, \dots, f_{i-1})$ , we may arrange that  $\text{ord}(f_j) \geq e_i$  for all  $j \geq i$ . After relabelling, we obtain that  $f_i, \dots, f_h$  satisfy

$$e_i \leq \text{ord}(f_i) \leq \text{ord}(f_{i+1}) \leq \cdots \leq \text{ord}(f_h).$$

Since  $X^{e_i} \in R[T]$ , we may write

$$X^{e_i} = \lambda_1 f_1 + \cdots + \lambda_h f_h + P(f_1, \dots, f_h),$$

where  $\lambda_j \in \mathbf{k}$ ,  $P \in \mathbf{k}[T_1, \dots, T_h]$  (the  $T_j$  are indeterminates) and where every monomial occurring in  $P(T_1, \dots, T_h)$  has degree at least two. Now  $P(f_1, \dots, f_h)|_{T=0} = P(f_1(0), \dots, f_h(0)) = \sum_j \mu_j X^{\gamma_j}$ , where  $\mu_j \in \mathbf{k}$  and  $\gamma_j \in \Gamma$ , but none of these  $\gamma_j$  can be a primitive element of  $\Gamma$  by (1). It follows that  $\lambda_j = 0$  for all  $j < i$ ; also,  $\text{ord}(f_i) = e_i$ , so we arranged that (2) holds for a larger value of  $i$ . Thus we may arrange that

$$\text{ord}(f_j) = e_j \quad \text{for all } j = 1, \dots, h.$$

Since  $T \in R[T]$ , we may write

(3) 
$$T = \lambda'_1 f_1 + \cdots + \lambda'_h f_h + P'(f_1, \dots, f_h),$$

where  $\lambda'_j \in \mathbf{k}$ ,  $P' \in \mathbf{k}[T_1, \dots, T_h]$ , and where every monomial occurring in  $P'(T_1, \dots, T_h)$  has degree at least two. Evaluating (3) at  $T = 0$  shows that  $\lambda'_j = 0$  for all  $j$  (as before,  $P'(f_1(0), \dots, f_h(0))$  can't produce a term  $X^{e_j}$ , by (1)). On

the other hand, each  $f_j$  evaluated at  $X = 0$  is an element of  $T\mathbf{k}[T]$ . Thus, evaluating the equation  $T = P'(f_1, \dots, f_h)$  at  $X = 0$  yields  $T = T^2Q(T)$  for some  $Q(T) \in \mathbf{k}[T]$ . This is a contradiction, so  $\#(R[T]) = h + 1$  cannot be false.  $\square$

**Lemma 2.** *Let  $h, p, q$  be positive integers. If  $\gcd(p, q) = 1$ , then the ideal*

$$(T_0^q - T_1^p, T_1^q - T_2^p, \dots, T_{h-1}^q - T_h^p)$$

*of  $\mathbf{k}[T_0, \dots, T_h]$  is prime.*

*Proof.* Consider the ideals  $\mathfrak{p} = (T_0^q - T_1^p, \dots, T_{h-1}^q - T_h^p)$  of  $\mathbf{k}[T_0, \dots, T_h]$  and  $\mathfrak{p}' = (T_0^q - T_1^p, \dots, T_{h-2}^q - T_{h-1}^p)$  of  $\mathbf{k}[T_0, \dots, T_{h-1}]$ . By induction, we may assume that  $\mathfrak{p}'$  is prime. This allows us to identify  $R' = \mathbf{k}[T_0, \dots, T_{h-1}]/\mathfrak{p}'$  with  $\mathbf{k}[X^{e_0}, \dots, X^{e_{h-1}}]$ , where  $X$  is an indeterminate and  $e_j = p^{h-j}q^j$ . Let  $K'$  be the field of fractions of  $R'$  and note that  $K' = \mathbf{k}(X^p)$ . Since  $\mathbf{k}[T_0, \dots, T_h]/\mathfrak{p} \cong R'[T_h]/(T_h^p - \theta^q)$ , where  $\theta = T_{h-1} + \mathfrak{p}' \in R'$ , it suffices to show that  $T_h^p - \theta^q$  is an irreducible element of  $K'[T_h]$ ; for this, it's enough to verify that  $(\theta^q)^{i/p} \notin K'$  for all  $i = 1, \dots, p - 1$ . But  $\theta = X^{e_{h-1}}$ , so  $(\theta^q)^{i/p} = X^{iq^h} \notin \mathbf{k}(X^p)$  for all  $i = 1, \dots, p - 1$ .  $\square$

The following is a well-known fact about extracting roots in a power series ring.

**Lemma 3.** *Let  $q$  be a positive integer,  $R$  a domain containing  $\mathbb{Q}$ ,  $W$  an indeterminate over  $R$  and  $\sigma$  an element of  $R[[W]]$  with constant term equal to 1 (i.e.,  $\sigma = 1 + s_1W + s_2W^2 + \dots$  where  $s_i \in R$ ). Then there exists a unique  $\rho \in R[[W]]$  satisfying  $\rho^q = \sigma$  and having constant term equal to 1.*

**Lemma 4.** *Let  $h \geq 2$  be an integer and  $p, q$  prime numbers such that  $p^2 < q$ . Then there exist  $f_0, \dots, f_h \in \mathbf{k}[W, X]$  satisfying:*

- (i)  $f_j(0, X) = X^{p^{h-j}q^j}$  for all  $j$  such that  $0 \leq j \leq h$ ;
- (ii)  $f_{j+1} \equiv \frac{f_{j-1}^q - f_j^p}{W} \pmod{W^{h-j}}$  for all  $j$  such that  $0 < j < h$ ;
- (iii)  $f_{h-1}^q - f_h^p = 0$ .

*Proof.* Define  $f_h = X^{q^h}$  and  $f_{h-1} = X^{pq^{h-1}}$ . Suppose that  $f_h, \dots, f_i \in \mathbf{k}[W, X]$  have been defined (where  $0 < i < h$ ) and satisfy (i)–(iii) and

$$(4) \quad X^{p^{h-j}q^j} \mid f_j \quad (i \leq j \leq h).$$

Note that the assumption  $p^2 < q$  implies that  $f_i^p + Wf_{i+1}$  is divisible by  $X^{p^{h-i+1}q^i}$ ; define

$$\sigma = \frac{f_i^p + Wf_{i+1}}{X^{p^{h-i+1}q^i}} \in \mathbf{k}[W, X] \subset \mathbf{k}[X][[W]]$$

and note that  $\sigma$  has the form  $\sigma = 1 + s_1W + s_2W^2 + \dots$  (with  $s_j \in \mathbf{k}[X]$ ). By Lemma 3, we may consider  $\rho = 1 + r_1W + r_2W^2 + \dots \in \mathbf{k}[X][[W]]$  (with  $r_j \in \mathbf{k}[X]$ ) such that  $\rho^q = \sigma$ . Then  $\tilde{f}_{i-1} := X^{p^{h-i+1}q^{i-1}}\rho \in \mathbf{k}[X][[W]]$  satisfies

$$\frac{\tilde{f}_{i-1}^q - f_i^p}{W} = f_{i+1} \quad \text{and} \quad X^{p^{h-i+1}q^{i-1}} \mid \tilde{f}_{i-1}$$

so, if  $f_{i-1} \in \mathbf{k}[W, X]$  is a suitable truncation of  $\tilde{f}_{i-1}$ , then  $f_h, \dots, f_{i-1}$  satisfy (i)–(iii) and (4). So we are done by induction.  $\square$

3. THE EXAMPLES

Given an integer  $h \geq 2$ , we construct a triangular derivation  $\Delta : \mathbf{k}[W, X, Y, Z] \rightarrow \mathbf{k}[W, X, Y, Z]$  whose kernel satisfies  $h + 2 \leq \#(\ker \Delta) \leq h + 3$ .

Choose prime numbers  $p, q$  satisfying  $p^2 < q$ ; consider  $f_0, \dots, f_h \in \mathbf{k}[W, X]$  as in Lemma 4 and define  $F_0 = f_0 + YW^{h+1}$ ,  $F_1 = f_1 + ZW^h$  and

$$F_{i+1} = \frac{F_{i-1}^q - F_i^p}{W} \quad (1 \leq i \leq h).$$

Let  $A = \mathbf{k}[W, F_0, \dots, F_{h+1}]$ . We have to prove the following two claims:

(5)  $h + 2 \leq \#(A) \leq h + 3;$

$A$  is the kernel of some triangular derivation

(6)  $\Delta : \mathbf{k}[W, X, Y, Z] \rightarrow \mathbf{k}[W, X, Y, Z].$

We begin by showing that

(7)  $F_j = f_j + b_j W^{h+1-j} \quad (0 \leq j \leq h + 1),$

where  $b_j \in \mathbf{k}[W, X, Y, Z]$  and  $b_j(0, X, Y, Z) \notin \mathbf{k}[X]$ , and where we define  $f_{h+1} = 0$ . We proceed by induction and note that the assertion is clear for  $j \leq 1$ . Assume that (7) holds for  $0 \leq j \leq i$ , for some  $i$  such that  $1 \leq i \leq h$ . Then  $F_i = f_i + b_i W^{h+1-i}$  and  $F_{i-1} = f_{i-1} + b_{i-1} W^{h+2-i}$ , so

$$\begin{aligned} F_{i-1}^q - F_i^p &= (f_{i-1} + b_{i-1} W^{h+2-i})^q - (f_i + b_i W^{h+1-i})^p \\ &= (f_{i-1}^q - f_i^p) - p f_i^{p-1} b_i W^{h+1-i} + \varepsilon_1 W^{h+2-i} \end{aligned}$$

for some  $\varepsilon_1 \in \mathbf{k}[W, X, Y, Z]$ . Write  $\frac{f_{i-1}^q - f_i^p}{W} = f_{i+1} + \varepsilon_2 W^{h-i}$ , with  $\varepsilon_2 \in \mathbf{k}[W, X]$ ; then dividing  $(F_{i-1}^q - F_i^p)$  by  $W$  gives

$$\begin{aligned} F_{i+1} &= (f_{i+1} + \varepsilon_2 W^{h-i}) - p f_i^{p-1} b_i W^{h-i} + \varepsilon_1 W^{h+1-i} \\ &= f_{i+1} + (\varepsilon_2 - p f_i^{p-1} b_i + \varepsilon_1 W) W^{h-i}, \end{aligned}$$

which proves (7). (In particular, the  $F_j$ 's are polynomials.)

Let  $\pi : \mathbf{k}[W, X, Y, Z] \rightarrow \mathbf{k}[X, Y, Z]$  be the surjective  $\mathbf{k}$ -homomorphism defined by

$$W \mapsto 0, \quad X \mapsto X, \quad Y \mapsto Y, \quad Z \mapsto Z.$$

Then (7) implies that  $\pi(A) = \mathbf{k}[X^{e_0}, \dots, X^{e_h}, \tau]$ , where  $e_i = p^{h-i} q^i$  and where  $\tau$  is transcendental over  $\mathbf{k}(X)$ . Let  $R = \mathbf{k}[X^{e_0}, \dots, X^{e_h}]$ ; since  $R[\tau]$  is a homomorphic image of  $A$ ,  $\#(A) \geq \#(R[\tau])$ ; since  $\#(R[\tau]) = h + 2$  by Lemma 1, (5) holds. Define a derivation  $\Delta : \mathbf{k}[W, X, Y, Z] \rightarrow \mathbf{k}[W, X, Y, Z]$  by

(8) 
$$\Delta = \begin{vmatrix} \frac{\partial}{\partial X} & \frac{\partial}{\partial Y} & \frac{\partial}{\partial Z} \\ \frac{\partial F_0}{\partial X} & \frac{\partial F_0}{\partial Y} & \frac{\partial F_0}{\partial Z} \\ \frac{\partial F_1}{\partial X} & \frac{\partial F_1}{\partial Y} & \frac{\partial F_1}{\partial Z} \end{vmatrix}.$$

Then  $\Delta Z = -W^{h+1} \frac{\partial f_1}{\partial X}$ ,  $\Delta Y = -W^h \frac{\partial f_0}{\partial X}$ ,  $\Delta X = W^{2h+1}$  and  $\Delta W = 0$ , so  $\Delta$  is a triangular derivation of  $\mathbf{k}[W, X, Y, Z]$ . It is clear that  $\mathbf{k}[W, F_0, F_1] \subseteq \ker \Delta$ , so  $A \subseteq \ker \Delta$ ; let us now argue that  $\ker \Delta \subseteq A_W$ . Write  $B = \mathbf{k}[W, X, Y, Z]$ ; since

$$B_W \supseteq A_W[X] \supseteq \mathbf{k}[W, W^{-1}, X, F_0, F_1] = \mathbf{k}[W, W^{-1}, X, Y, Z] = B_W,$$

$B_W$  is a polynomial ring over  $A_W$ . On the other hand,  $(\ker \Delta)_W$  contains  $A_W$  and is the kernel of the nonzero derivation  $\Delta_W : B_W \rightarrow B_W$ , so  $(\ker \Delta)_W = A_W$  and

we have shown that  $A \subseteq \ker \Delta \subset A_W$ . So, in order to prove (6), there remains only to prove

$$(9) \quad A \cap WB = WA.$$

It is easy to see that the proof of (9) reduces to that of the following: if  $T_0, \dots, T_{h+1}$  are indeterminates and  $\psi \in \mathbf{k}[T_0, \dots, T_{h+1}]$ , then  $\psi(F_0, \dots, F_{h+1}) \in WB$  implies  $\psi(F_0, \dots, F_{h+1}) \in WA$ . Write  $\psi = \sum_{n \geq 0} \psi_n T_{h+1}^n$  with  $\psi_n \in \mathbf{k}[T_0, \dots, T_h]$ . Then

$$0 = \pi(\psi(F_0, \dots, F_{h+1})) = \sum_{n \geq 0} \psi_n(X^{e_0}, \dots, X^{e_h})\tau^n,$$

where  $\tau = \pi(F_{h+1})$  is transcendental over  $\mathbf{k}(X)$ , and consequently  $\psi_n \in \ker \varphi$  for all  $n$ , where  $\varphi : \mathbf{k}[T_0, \dots, T_h] \rightarrow \mathbf{k}[X]$  is the  $\mathbf{k}$ -homomorphism which maps  $T_i$  to  $X^{e_i}$ . By Lemma 2,  $\ker \varphi = (T_0^q - T_1^p, \dots, T_{h-1}^q - T_h^p)$ , so  $\psi_n = \sum_{j=1}^h \alpha_j (T_{j-1}^q - T_j^p)$  for some  $\alpha_j \in \mathbf{k}[T_0, \dots, T_h]$ . Then

$$\begin{aligned} \psi_n(F_0, \dots, F_h) &= \sum_{j=1}^h \alpha_j(F_0, \dots, F_h)(F_{j-1}^q - F_j^p) \\ &= \sum_{j=1}^h \alpha_j(F_0, \dots, F_h)WF_{j+1} \in WA. \end{aligned}$$

So (9) holds and, consequently,  $\ker(\Delta) = A$ . So (5) and (6) are proved.

**Example.** We exhibit a triangular derivation  $\Delta$  of  $\mathbf{k}[W, X, Y, Z]$  whose kernel cannot be generated by five elements over  $\mathbf{k}$ . Let  $p = 2, q = 5$  and  $h = 4$  and, following the proof of Lemma 4, successively define  $f_4, f_3, f_2, f_1, f_0$  by:<sup>1</sup>

$$\begin{aligned} f_4 &= X^{625}, \quad f_3 = X^{250}, \quad f_2 = X^{100} + \frac{1}{5} X^{225}W, \\ f_1 &= X^{40} + \left(\frac{2}{25} X^{165} + \frac{1}{5} X^{90}\right)W + \left(-\frac{3}{625} X^{290} - \frac{8}{125} X^{215} - \frac{2}{25} X^{140}\right)W^2 \end{aligned}$$

and

$$\begin{aligned} f_0 &= X^{16} + \left(\frac{2}{25} X^{66} + \frac{1}{5} X^{36} + \frac{4}{125} X^{141}\right)W \\ &+ \left(-\frac{92}{3125} X^{191} - \frac{23}{625} X^{116} - \frac{42}{15625} X^{266} + \frac{9}{625} X^{161} - \frac{8}{125} X^{86} - \frac{2}{25} X^{56}\right)W^2 \\ &+ \left(\frac{408}{78125} X^{241} + \frac{68}{15625} X^{166} + \frac{666}{390625} X^{316} + \frac{328}{15625} X^{211} + \frac{132}{3125} X^{136}\right. \\ &\quad \left.+ \frac{36}{625} X^{106} - \frac{72}{78125} X^{286} - \frac{28}{3125} X^{181} + \frac{6}{125} X^{76} + \frac{244}{1953125} X^{391}\right)W^3. \end{aligned}$$

Define  $\Delta$  as in (8) or, equivalently, by

$$\Delta W = 0, \quad \Delta X = W^9, \quad \Delta Y = -W^4 \frac{\partial f_0}{\partial X} \quad \text{and} \quad \Delta Z = -W^5 \frac{\partial f_1}{\partial X}.$$

Then, by (5) and (6), we have  $6 \leq \#(\ker \Delta) \leq 7$ .

<sup>1</sup>Note that the  $f_j$ 's are not unique.

## REFERENCES

1. D. Daigle, G. Freudenburg, *A counterexample to Hilbert's Fourteenth Problem in dimension five*, ppt 1999 (9 pages)
2. M. Miyanishi, *Normal affine subalgebras of a polynomial ring*, in: Algebraic and Topological Theories – to the Memory of Dr. Takehiko Miyata, Kinokuniya, Tokyo (1985) 37-51 CMP 91:10

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF OTTAWA, OTTAWA, CANADA  
K1N 6N5

*E-mail address:* `daniel@mathstat.uottawa.ca`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN INDIANA, EVANSVILLE, INDIANA  
47712

*E-mail address:* `freudenb@usi.edu`