A Groebner basis approach to solve a Conjecture of Nowicki

Joseph Khoury

Department of Mathematics and Statistics, University of Ottawa.
585 King Edward, Ottawa, Ontario, Canada,
K1N 6N5

Abstract

Let k be a field of characteristic zero, n any positive integer and let δ_n be the derivation $\sum_{i=1}^{n} X_i \frac{\partial}{\partial Y_i}$ of the polynomial ring $k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ in $2n$ variables over k. A Conjecture of Nowicki (Conjecture 6.9.10 in (8)) states the following

$$\ker \delta_n = k[X_1, \ldots, X_n, X_iY_j - X_jY_i;\ 1 \leq i < j \leq n]$$

in which case we say that δ_n is *standard*.

In this paper, we use the elimination theory of Groebner bases to prove that Nowicki's conjecture holds in the more general case of the derivation $D = \sum_{i=1}^{n} X_i^{t_i} \frac{\partial}{\partial Y_i}$, $t_i \in \mathbb{Z}_{\geq 0}$.

In (6), H. Kojima and M. Miyanishi argued that D is standard in the case where $t_i = t$ $(i = 1, \ldots n)$ for some $t \geq 3$. Although the result is true, we show in Section 4 of this paper that the proof presented in (6) is not complete.

Key words: Locally nilpotent derivations, Elimination theory.

1. Introduction

Throughout n is a positive integer, k is an algebraically closed field (unless it is used as an index as in T_k or T_{jk} in which case it stands for a positive integer).

From a geometric point of view, a locally nilpotent derivation d on the polynomial ring $k[X] := k[X_1, \ldots, X_n]$ determines an algebraic action of the additive group $(k, +)$ (viewed as an algebraic group called G_a) on the affine space $\mathbb{A}_k^n$ over k. Moreover, the ring of invariants of this action is $\ker d$.

Email address: jkhoury@uottawa.ca (Joseph Khoury).
URL: http://aix1.uottawa.ca/∼jkhoury (Joseph Khoury).

Preprint submitted to Elsevier *13 August 2008*

The study of locally nilpotent derivations and their kernels has a profound roots in other branches of mathematics like Lie theory, invariant theory, and differential equations. In particular, the question of finite generation of kernels of derivations on $k[X]$ is closely related to the famous fourteenth problem of Hilbert that can be stated as follows:

(*) If L is a subfield of $k(X)$ (the field of fractions of $k[X]$) containing k, is $L \cap k[X]$ a finitely generated k-algebra?

More precisely, if d is a k-derivation on $k[X]$ such that $A = \ker d$ is not a finitely generated k-algebra, then the field of fractions of A, $\mathrm{Frac}(A)$, is a counterexample to (*) since $\mathrm{Frac}(A) \cap k[X] = A$. In fact, most counterexamples of (*) found recently are constructed this way (see for example (2), (3)). Another example that illustrates the importance of finding generators of the kernel is in the proof (see (7)) of the fact that the hypersurface $x + x^2y + z^2 + t^3 = 0$ is not isomorphic to $\mathbb{C}^3$ in $\mathbb{C}^4$.

It is well known (see (9)) that if d is a linear k-derivation of $k[X]$ (see the terminology below), then $\ker d$ is finitely generated as a k-algebra. All the known proofs of this fact are not constructive in the sense that they don't give a complete description of the kernel. The derivation we consider in this paper is $D = \sum_{i=1}^{n} X_i^{t_i} \frac{\partial}{\partial Y_i}$ of the polynomial ring in $2n$ variables $k[X, Y] := k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$. Note that D is linear if $t_i = 1$ for all $i = 1, \ldots n$. However, if $t_i \geq 2$ for some i, even the finite generation of $\ker D$ is not clear. The main result of this paper gives a complete description of $\ker D$ for arbitrary n in terms of its generators over k. This solves a more general form of a Conjecture of Nowicki (Conjecture 6.9.10 in (8)).

1.1. *Terminology*

Let R be a UFD containing $\mathbb{Q}$, B be an R-algebra and $d : B \to B$ a derivation of B. The following terminologies will be used throughout this paper.

- If B is a polynomial ring in m variables over R, we write $B \cong R^{[m]}$.
- If $d(R) = 0$, then we say that d is an R-derivation of B.
- d is called *locally nilpotent* if for all $b \in B$, there exists $n \in \mathbb{N}$ such that $d^n(b) = 0$.
- If $B = R^{[m]}$, then an R-derivation $d : B \to B$ is called R-*elementary* (or simply *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:

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

  Note that if d is elementary, then it is in particular locally nilpotent.
- An R-derivation d of $B = R[Y_1, \ldots, Y_m] \cong R^{[m]}$ is called R-*linear* (or simply *linear*) if $d(Y_i)$ is a linear form (over R) in the Y_j's for all i.
- Given an R-elementary derivation $d = \sum_{i=1}^{m} a_i \frac{\partial}{\partial Y_i}$ of $B = R[Y_1, \ldots, Y_m] \cong R^{[m]}$, we say that d is *standard* if $\ker d = R[L_{ij},\ 1 \leq i < j \leq m]$ where $L_{ij} = \frac{a_i}{g_{ij}} Y_j - \frac{a_j}{g_{ij}} Y_i$ with:

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

  (Note that $R[L_{ij},\ 1 \leq i < j \leq m] \subseteq \ker d$)

- A locally nilpotent derivation d of B is called *fixed-point-free* if the ideal of B generated by the image of d is equal to B.

The following is the main result of this paper:

Theorem 1. *Let $n \in \mathbb{Z}_{>0}$ and $t_1, \ldots, t_n \in \mathbb{Z}_{\geq 0}$. Then the $k[X]$-elementary derivation*

$$D = \sum_{i=1}^{n} X_i^{t_i} \frac{\partial}{\partial Y_i}$$

of $k[X, Y]$ is standard.

The special case where all the t_i's are equal to 1 was considered by Nowicki in (8). Since, in that case, D is $k[X]$-linear, it is known (see (9)) that $\ker D$ is a finitely generated $k[X]$-algebra, but no set of generators is known for arbitrary n. Nowicki conjectured Theorem 1 in that case ($t_i = 1$ for all i), basing his conjecture on his consideration of the cases $n = 2, 3, 4$. On the other hand, it was argued in (6) that Theorem 1 holds in the case where $t_i = t$ ($i = 1, \ldots, n$) for some $t \geq 3$. However, we show that the proof presented in (6) has a gap. Note that in the case where $t_i \geq 2$ for some i (i.e, D is not linear), it is no longer evident that $\ker D$ is finitely generated as a k-algebra. In Section 2, we show that we can restrict ourselves to the linear case.

2. Restriction to the linear case

With the notations of Theorem 1, if $t_i = 0$ for some i then D is in particular fixed-point-free and hence standard by Theorem 6.1 in (5). Thus, we may assume that $t_i > 0$ for all i. Next, we show that it is enough to treat the linear case.

Proposition 2. *Let R be a ring, R' a subring of R such that R is a free R'-module. Then every polynomial ring $R[Y_1, \ldots, Y_t]$ over R is a free $R'[Y_1, \ldots, Y_t]$-module. Moreover, if $\mathcal{B}$ is a basis of R over R', then $\mathcal{B}$ is also a basis of $R[Y_1, \ldots, Y_t]$ over $R'[Y_1, \ldots, Y_t]$.*

Proof. Clearly, it is enough to assume that $t = 1$. Let $f = \sum a_i Y_1^i \in R[Y_1]$ ($a_i \in R$). Since each a_j can be written uniquely as $\sum \alpha_i b_i$ with $\alpha_i \in R'$ and $b_i \in \mathcal{B}$, then f can be written uniquely as a finite sum

$$f = \sum f_i(Y_1) b_i$$

where $f_i(Y_1) \in R'[Y_1]$ and $b_i \in \mathcal{B}$ for all i. This shows that $\mathcal{B}$ is a basis of $R[Y_1]$ over $R'[Y_1]$. $\square$

With assumptions and notations as in Proposition 2, let $D = \sum_{i=1}^{t} a_i \partial/\partial Y_i$ be an R-elementary derivation of $R[Y_1, \ldots, Y_t]$ such that $a_i \in R'$ for all i and let D' be the restriction of D to $R'[Y_1, \ldots, Y_t]$. We have the following.

Lemma 3. *If $\mathcal{B}$ is a basis of R over R', then $\ker D$ is a free $\ker D'$-module with basis $\mathcal{B}$. In particular, if $G \subset R'[Y_1, \ldots, Y_t]$ generates $\ker D'$ as an R'-algebra, then G generates $\ker D$ as an R-algebra.*

Proof. Let $f \in R[Y_1, \ldots, Y_t]$ and write $f = \sum f_i b_i$ where $f_i \in R'[Y_1, \ldots, Y_t]$ and $b_i \in \mathcal{B}$. Since $b_i \in R$, we have that $D(f) = \sum D(f_i) b_i = \sum D'(f_i) b_i$. Therefore,

$$f \in \ker D \Leftrightarrow \forall i, D' f_i = 0 \Leftrightarrow \forall i, f_i \in \ker D'.$$

□

In our case, let $R = k[X_1, \ldots, X_n]$ and $R' = k[X_1^{t_1}, \ldots, X_n^{t_n}]$. Then R is a free R'-module with basis $\mathcal{B} = \{X_1^{s_1} \cdots X_n^{s_n};\ 0 \leq s_i < t_i,\ i = 1 \ldots n\}$, and $R' \cong k^{[n]}$. Now let $Z_i = X_i^{t_i}$, then the restriction D' of D to $R'[Y_1, \ldots, Y_n]$ is the derivation $\sum_{i=1}^n Z_i \partial / \partial Y_i$. If $\{Z_i Y_j - Y_i Z_j :\ 1 \leq i < j \leq n\}$ generates $\ker D'$ over R', then Lemma 3 implies that the same set generates $\ker D$ over R.

Thus the proof of Theorem 1 reduces to that of:

Theorem 4. *Let n be a positive integer. Then the derivation*

$$D = \sum_{i=1}^{n} X_i \frac{\partial}{\partial Y_i}$$

of the polynomial ring $k[X, Y]$ is standard.

Theorem 4 can be easily verified if $n = 1, 2$. The case $n = 3$ was treated in (8). This case follows also from the main result in (4). Hence we may (and will) assume in what follows that n is an integer greater than or equal to 4. Let $k[X, Y, T]$ denote the following polynomial ring in $\frac{n(n+5)}{2}$ variables over k:

$$k[X_1, \ldots, X_n, Y_1, \ldots, Y_n, T_1, \ldots, T_n, T_{ij} :\ 1 \leq i < j \leq n].$$

If $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, let $|\underline{\alpha}|$ denote the total degree of $\underline{\alpha}$ ($|\underline{\alpha}| = \sum_{i=1}^n \alpha_i$). If P is a monomial in $k[X, Y, T]$, we identify P with a vector $\underline{\alpha}_P \in \mathbb{Z}_{\geq 0}^{\frac{n(n+5)}{2}}$ and we define the total degree $|P|$ of P as being the total degree of $\underline{\alpha}_P$.

Let $<_{grevlex}$ denote the graded reversed lexicographic ordering on $k[X, Y, T]$ with

$$X_1 > \ldots > X_n > Y_1 > \ldots > Y_n > T_1 > \ldots > T_n > T_{ij}$$

for all i, j with $1 \leq i < j \leq n$ and

$$T_{ij} > T_{kl} \Longleftrightarrow \begin{cases} i < k \\ \text{or} \\ i = k \text{ and } j < l. \end{cases}$$

Let $<$ denote the $2n$-*elimination monomial ordering* on $k[X, Y, T]$. This is the monomial ordering on $k[X, Y, T]$ defined as follows: for any monomials P, P' in $k[X, Y]$ and M, M' in $k[T] := K[T_1, \ldots, T_n, T_{ij} :\ 1 \leq i < j \leq n]$:

$$PM < P'M' \Leftrightarrow \begin{cases} |P| < |P'| \\ \text{or} \\ |P| = |P'| \text{ and } PM <_{grevlex} P'M' \end{cases}$$

With respect to this monomial ordering, any monomial involving any of the X_i's or the Y_i's is greater than any monomial in $k[T]$.

Next, consider the ideal I of $k[X,Y,T]$ generated by the elements

$$X_1, T_i - X_i, T_{jk} - L_{jk}, \text{ for } 1 \leq i \leq n \text{ and } 1 \leq j < k \leq n.$$

Proposition 5. *With respect to the monomial ordering $<$ on $k[X,Y,T]$ defined above, a Groebner basis for the ideal I is given by the union of the following seven families of elements of $k[X,Y,T]$ (the underlined elements are the leading monomials):*

$$\mathcal{F}_1 = \{\underline{X_1}, \underline{T_1}\} \cup \{-T_i + \underline{X_i};\ 2 \leq i \leq n\}$$

$$\mathcal{F}_2 = \{T_i T_{1j} - \underline{T_j T_{1i}};\ 2 \leq i < j \leq n\}$$

$$\mathcal{F}_3 = \{T_{1i} + \underline{Y_1 T_i};\ 2 \leq i \leq n\}$$

$$\mathcal{F}_4 = \{T_{ij} + Y_i T_j - \underline{Y_j T_i};\ 2 \leq i < j \leq n\}$$

$$\mathcal{F}_5 = \{T_{ij} T_{kl} - T_{ik} T_{jl} + \underline{T_{il} T_{jk}};\ 1 \leq i < j < k < l \leq n\}$$

$$\mathcal{F}_6 = \{Y_i T_{jk} - Y_j T_{ik} + \underline{Y_k T_{ij}};\ 1 \leq i < j < k \leq n\}$$

$$\mathcal{F}_7 = \{T_i T_{jk} - T_j T_{ik} + \underline{T_k T_{ij}};\ 2 \leq i < j < k \leq n\}$$

3. Proof of Proposition 5

First we prove that the ideal I can be generated by $\bigcup_{i=1}^{7} \mathcal{F}_i$.

Lemma 6. *With the above notations, I is generated (as an ideal of $k[X,Y,T]$) by $G := \cup_{i=1}^{7} \mathcal{F}_i$.*

Proof. Let I_1 be the ideal of $k[X,Y,T]$ generated by G.
$\underline{I \subseteq I_1}$: Clearly, $T_i - X_i \in I_1$ for all $i \in \{1, \ldots, n\}$.

For $2 \leq i \leq n$, we have

$$\begin{aligned} T_{1i} - L_{1i} &= (T_{1i} + Y_1 T_i) - Y_1(T_i - X_i) - Y_i X_1 \\ &\in I_1. \end{aligned}$$

For $2 \leq i < j \leq n$, we have

$$
\begin{aligned}
T_{ij} - L_{ij} &= T_{ij} - X_iY_j + X_jY_i \\
&= (T_{ij} + Y_iT_j - Y_jT_i) + Y_j(T_i - X_i) - Y_i(T_j - X_j) \\
&\in I_1.
\end{aligned}
$$

$\underline{I_1 \subseteq I}$: This can be shown using the following identities:
1. $-T_i + X_i = -(T_i - X_i);\ 2 \leq i \leq n$ and $T_1 = (T_1 - X_1) + X_1$.

2. $T_iT_{1j} - T_jT_{1i} = T_{1j}(T_i - X_i) - T_{1i}(T_j - X_j) + X_i(T_{1j} - L_{1j}) - X_j(T_{1i} - L_{1i}) + X_1L_{ij};\ 2 \leq i < j \leq n.$

3. $T_{1i} + Y_1T_i = (T_{1i} - L_{1i}) + Y_iX_1 + Y_1(T_i - X_i);\ 2 \leq i \leq n.$

4. $T_{ij} + Y_iT_j - Y_jT_i = (T_{ij} - L_{ij}) + Y_i(T_j - X_j) - Y_j(T_i - X_i);\ 2 \leq i < j \leq n.$

5. $T_{ij}T_{kl} - T_{ik}T_{jl} + T_{il}T_{jk} = T_{kl}(T_{ij} - L_{ij}) - T_{jl}(T_{ik} - L_{ik}) + T_{jk}(T_{il} - L_{il}) + L_{ij}(T_{kl} - L_{kl}) - L_{ik}(T_{jl} - L_{jl}) - L_{il}(T_{jk} - L_{jk});\ 1 \leq i < j < k < l \leq n.$

6. $Y_iT_{jk} - Y_jT_{ik} + Y_kT_{ij} = Y_i(T_{jk} - L_{jk}) - Y_j(T_{ik} - L_{ik}) + Y_k(T_{ij} - L_{ij});$
$1 \leq i < j < k \leq n.$

7. $T_iT_{jk} - T_jT_{ik} + T_kT_{ij} = T_k(T_{ij} - L_{ij}) - T_j(T_{ik} - L_{ik}) + T_i(T_{jk} - L_{jk}) + L_{jk}(T_i - X_i) - L_{ik}(T_j - X_j) + L_{ij}(T_k - X_k);\ 2 \leq i < j < k \leq n.$

□

Next we show that G is indeed a Groebner basis for I with respect to the monomial ordering $<$ considered above. We will proceed as follows: given $i, j \in \{1, \ldots, 7\}$ (i and j not necessarily distinct), we consider two elements $f_i \in \mathcal{F}_i$ and $f_j \in \mathcal{F}_j$ and we prove that their S-polynomial

$$
S(f_i, f_j) := \frac{\mathrm{LCM}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_i)} f_i - \frac{\mathrm{LCM}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))}{\mathrm{LT}(f_j)} f_j
$$

is in standard form relative to G, i.e., $S(f_i, f_j) = \sum_{g \in G} a_g g$ with $a_g \in k[X, Y, T]$ and $a_g g \leq S(f_i, f_j)$ whenever $a_g \neq 0$. Here, $\mathrm{LT}(f)$, $\mathrm{LM}(f)$ denote the leading term and the leading monomial of f respectively (with respect to the above monomial ordering) for each $f \in [X, Y, T]$, and if $f, g \in k[X, Y, T]$ are such that $\mathrm{LT}(f) \leq \mathrm{LT}(g)$ we simply write $f \leq g$. This process will be denoted by case "$(\mathcal{F}_i, \mathcal{F}_j)$". To show that G is a Groebner basis of I, it is enough to verify that $S(f_i, f_j)$ is in standard form relative to G for each $f_i, f_j \in G$ satisfying $\gcd(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) = 1$ by Buchberger's first criterion. Also note that if $S(f_i, f_j)$ is in standard form relative to G, then so is $S(f_j, f_i)$ since $S(f_i, f_j) = -S(f_j, f_i)$.

As it turns out, case $(\mathcal{F}_5, \mathcal{F}_5)$ will play a crucial role in simplifying many of the cases $(\mathcal{F}_i, \mathcal{F}_j)$. So we start with this case.

3.1. Case $(\mathcal{F}_5, \mathcal{F}_5)$

In all what follows, T_{ij} should be treated as 0 when $i = j$.

Lemma 7. *$\mathcal{F}_5$ is a Groebner basis for the ideal it generates in $k[T_{ij};\ 1 \le i < j \le n]$ with respect to the above monomial order. Moreover, if $f, g \in \mathcal{F}_5$ then $S(f,g)$ has a standard representation with respect to $\mathcal{F}_5$ of the form $S(f,g) = \sum T_{ij}\rho_{ij}$ with*
(1) $\rho_{ij} \in \mathcal{F}_5$ and $T_{ij}\rho_{ij} \le S(f,g)$;
(2) $S(f,g)$ and each $T_{ij}\rho_{ij}$ are homogeneous and have the same total degree in terms of the T_{1k}'s.

Proof. Let

$$f = T_{ab}T_{cd} - T_{ac}T_{bd} + T_{ad}T_{bc}, \quad g = T_{ij}T_{kl} - T_{ik}T_{jl} + T_{il}T_{jk}$$
$$1 \le a < b < c < d \le n, \qquad 1 \le i < j < k < l \le n$$

be two *distinct* elements of $\mathcal{F}_5$. Since $\mathrm{LT}(f) = T_{ad}T_{bc}$ and $\mathrm{LT}(g) = T_{il}T_{jk}$, it is enough (by Buchberger's first criterion and the relation $S(f,g) = -S(g,f)$) to consider the following cases

$$(1)\ (a,d) = (i,l) \qquad (2)\ (a,d) = (j,k) \qquad (3)\ (b,c) = (j,k).$$

In case (1), $S(f,g) = T_{ab}T_{cd}T_{jk} - T_{ac}T_{bd}T_{jk} - T_{aj}T_{bc}T_{kd} + T_{ak}T_{bc}T_{jd}$. Using the relation $S(f,g) = -S(g,f)$, one can restrict to the following subcases:

$$(1.1)\ 1 \le a = i < b < c \le j < k < d = l \le n$$
$$(1.2)\ 1 \le a = i < b \le j < c \le k < d = l \le n$$
$$(1.3)\ 1 \le a = i < b < j < k < c < d = l \le n.$$

In all the above subcases, $\mathrm{LT}(S(f,g)) = -T_{ac}T_{bd}T_{jk}$. On the other hand, we have the following expressions of $S(f,g)$ in standard forms relative to $\mathcal{F}_5$ in each of the three subcases:

In case (1.1) :
$$\begin{aligned} S(f,g) = & -T_{kd}(T_{ab}T_{cj} - T_{ac}T_{bj} + T_{aj}T_{bc}) + T_{jd}(T_{ab}T_{ck} - T_{ac}T_{bj} + T_{ak}T_{bc}) \\ & -T_{ac}(T_{bj}T_{kd} - T_{bk}T_{jd} + T_{bd}T_{jk}) + T_{ab}(T_{cj}T_{kd} - T_{ck}T_{jd} + T_{cd}T_{jk}). \end{aligned}$$

In case (1.2) :
$$\begin{aligned} S(f,g) = & T_{kd}(T_{ab}T_{jc} - T_{aj}T_{bc} + T_{ac}T_{bj}) + T_{jd}(T_{ab}T_{ck} - T_{ac}T_{bk} + T_{ak}T_{bc}) \\ & -T_{ac}(T_{bj}T_{kd} - T_{bk}T_{jd} + T_{bd}T_{jk}) - T_{ab}(T_{jc}T_{kd} - T_{jk}T_{cd} + T_{jd}T_{ck}). \end{aligned}$$

In case (1.3) :
$$\begin{aligned} S(f,g) = & T_{kd}(T_{ab}T_{jc} - T_{aj}T_{bc} + T_{ac}T_{bj}) - T_{jd}(T_{ab}T_{kc} - T_{ak}T_{bc} + T_{ac}T_{bk}) \\ & -T_{ac}(T_{bj}T_{kd} - T_{bk}T_{jd} + T_{bd}T_{jk}) + T_{ab}(T_{jk}T_{cd} - T_{jc}T_{kd} + T_{jd}T_{kc}). \end{aligned}$$

In case (2), we have the only possibility:

$$1 \le i < a = j < b < c < k = d < l \le n,$$

in which case $S(f,g) = T_{il}T_{ab}T_{cd} - T_{il}T_{ac}T_{bd} - T_{ia}T_{bc}T_{dl} + T_{id}T_{al}T_{bc}$ with $T_{id}T_{al}T_{bc}$ as a leading term. The following shows a standard form of $S(f,g)$ relative to $\mathcal{F}_5$:

$$\begin{aligned} S(f,g) = &T_{cd}(T_{ia}T_{bl} - T_{ib}T_{al} + T_{il}T_{ab}) - T_{bd}(T_{ia}T_{cl} - T_{ic}T_{al} + T_{il}T_{ac}) \\ &+T_{al}(T_{ib}T_{cd} - T_{ic}T_{bd} + T_{id}T_{bc}) - T_{ia}(T_{bc}T_{dl} - T_{bd}T_{cl} + T_{bl}T_{cd}). \end{aligned}$$

To check that $S(f,g)$ is in standard form relative to $\mathcal{F}_5$ in case (3), we can clearly restrict ourselves to the following two cases:

$$(3.1)\ 1 \le a \le i < b = j < c = k < l \le d \le n$$

$$(3.2)\ 1 \le a \le i < b = j < c = k < d \le l \le n.$$

In both cases, $S(f,g) = T_{ab}T_{il}T_{cd} - T_{ac}T_{il}T_{bd} - T_{ad}T_{ib}T_{cl} + T_{ad}T_{ic}T_{bl}$ with $\mathrm{LT}(S(f,g)) = T_{ad}T_{ic}T_{bl}$. In case (3.1),

$$\begin{aligned} S(f,g) = &T_{bl}(T_{ai}T_{cd} - T_{ac}T_{id} + T_{ad}T_{ic}) - T_{cd}(T_{ai}T_{bl} - T_{ab}T_{il} + T_{al}T_{ib}) \\ &-T_{ib}(T_{ac}T_{ld} - T_{al}T_{cd} + T_{ad}T_{cl}) + T_{ac}(T_{ib}T_{ld} - T_{il}T_{bd} + T_{id}T_{bl}) \end{aligned}$$

In case (3.2),

$$\begin{aligned} S(f,g) = &T_{bl}(T_{ai}T_{cd} - T_{ac}T_{id} + T_{ad}T_{ic}) - T_{cd}(T_{ai}T_{bl} - T_{ab}T_{il} + T_{al}T_{ib}) \\ &+T_{ib}(T_{ac}T_{dl} - T_{ad}T_{cl} + T_{al}T_{cd}) - T_{ac}(T_{ib}T_{dl} - T_{id}T_{bl} + T_{il}T_{bd}) \end{aligned}$$

This shows that $S(f,g)$ is in standard form relative to $\mathcal{F}_5$ in case (3).

The last conclusion of the Lemma is clear from the above calculations. $\square$

3.2. *Cases* $(\mathcal{F}_5, \mathcal{F}_6)$, $(\mathcal{F}_5, \mathcal{F}_7)$, $(\mathcal{F}_6, \mathcal{F}_6)$ *and* $(\mathcal{F}_7, \mathcal{F}_7)$

We exploit the properties of the Groebner basis for the family $\mathcal{F}_5$ described in Lemma 7 above to avoid many unnecessary computations of S-polynomials.

Let $(J, <)$ be a finite totally ordered set (with at least four elements), let $m = \min J$ and $M = \max J$. Let $k[X,Y,T](J)$ be the polynomial ring

$$\begin{aligned} &k[X_m, \dots, X_M, Y_m, \dots, Y_M, T_m, \dots, T_M, T_{ij} : m \le i < j \le M] \\ &\qquad = k[\{X_i\}_{i\in J} \cup \{Y_i\}_{i\in J} \cup \{T_i\}_{i\in J} \cup \{T_{ij}\}_{i,j\in J,\ i<j}]. \end{aligned}$$

One can clearly extend the monomial ordering defined on $k[X,Y,T]$ above to a monomial ordering on $k[X,Y,T](J)$. Moreover, for each $i \in \{5,6,7\}$, one can define a family $\mathcal{F}_i(J) \subset k[Y,T](J)$ by replacing, in the definition of $\mathcal{F}_i$ given in the statement of Proposition 5, each occurrence of "1" by "m" and each occurrence of "n" by "M". Then a closer look at the result of Lemma 7 above shows that $\mathcal{F}_5(J)$ is a Groebner basis for the ideal it generates in $k[T_{ij} :\ m \le i < j \le M](J)$.

Now, let $J = \{1, 2, \ldots, n\}$, $J' = \{0, 1, \ldots, n\}$ and consider the homomorphisms of k-algebras:

$$\phi_1,\ \phi_2 : k[X, Y, T](J) \to k[X, Y, T](J'),\ \psi_1,\ \psi_2 : k[X, Y, T](J') \to k[X, Y, T](J)$$

where

- ϕ_1 is the identity on $k[X, T](J)$ and $\phi_1(Y_i) = T_{0i}$.
- ϕ_2 is the identity on $k[X, Y, T_{kl};\ 1 \leq k < l \leq n]$ and $\phi_2(T_i) = T_{0i}$.
- ψ_1 sends X_0, Y_0, T_0 to 0, it restricts to the identity on $k[X, Y, T](J) \subset k[X, Y, T](J')$ and $\psi_1(T_{0i}) = Y_i$ for $1 \leq i \leq n$.
- As for ψ_2, it also sends X_0, Y_0, T_0 to 0, restricts to the identity on $k[X, Y, T](J) \subset k[X, Y, T](J')$ but $\psi_2(T_{0i}) = T_i$ for $1 \leq i \leq n$.

Clearly $\psi_t \circ \phi_t$ is the identity on $k[X, Y, T](J)$ for $t = 1, 2$.

Consider the monomial orderings on $k[Y_i,\ T_i,\ T_{kl} :\ i,\ k,\ l \in J,\ k < l]$ and $k[T_{ij} : i < j \in J']$ induced by the elimination orderings on $k[X, Y, T](J)$ and $k[X, Y, T](J')$ defined above. Then we have the following easy Lemma:

Lemma 8. *Let $\alpha, \beta \in k[Y_i,\ T_i,\ T_{kl} :\ i,\ k,\ l \in J,\ k < l]$, $\lambda, \mu \in k[T_{ij} : i < j \in J']$ be four nonzero polynomials such that α and β are homogeneous and have the same totaldegree in the Y_i's (respectively in the T_i's), and λ, μ are homogeneous and have the same totaldegree in the T_{0i}'s. Then:*

(1) $\phi_1\left(LCM(\alpha, \beta)\right) = LCM(\phi_1(\alpha), \phi_1(\beta))$ (respectively $\phi_2\left(LCM(\alpha, \beta)\right) = LCM(\phi_2(\alpha), \phi_2(\beta))$)

(2) if $\alpha \leq \beta$, then $\phi_1(\alpha) \leq \phi_1(\beta)$ (respectively $\phi_2(\alpha) \leq \phi_2(\beta)$)

(3) if $\lambda \leq \mu$, then $\psi_i(\lambda) \leq \psi_i(\mu)$ for $i = 1, 2$.

As a Corollary, we have

Lemma 9. *Let $f, g \in \mathcal{F}_5(J) \cup \mathcal{F}_6(J) \cup \mathcal{F}_7(J)$ then for $i = 1, 2$:*

$$\phi_i\left(S(f, g)\right) = S\left(\phi_i(f), \phi_i(g)\right).$$

Proof. This is a direct consequence of the definition of $S(f, g)$, of the homogeneousness of elements of the families $\mathcal{F}_6(J), \mathcal{F}_7(J)$ and the above Lemma. □

Using the properties of ϕ_i and ψ_i and the results of Lemma 7, one no longer needs to carry out the computations of $S(f, g)$ in the cases $(\mathcal{F}_5, \mathcal{F}_6)$, $(\mathcal{F}_5, \mathcal{F}_7)$, $(\mathcal{F}_6, \mathcal{F}_6)$ and $(\mathcal{F}_7, \mathcal{F}_7)$. Here is why:

Let $f \in \mathcal{F}_5(J) \cup \mathcal{F}_6(J)$, $g \in \mathcal{F}_6(J)$. We want to show that $S(f, g)$ is in standard form relative to G. Since $\phi_1(f)$, $\phi_1(g) \in \mathcal{F}_5(J')$, then Lemma 7 above shows that

$$S\left(\phi_1(f), \phi_1(g)\right) = \sum T_{ij} \rho_{ij} \tag{1}$$

where $0 \leq i < j \leq n$, $\rho_{ij} \in \mathcal{F}_5(J')$ and

$$T_{ij} \rho_{ij} \leq S\left(\phi_1(f), \phi_1(g)\right) \tag{2}$$

with $T_{ij}\rho_{ij}$ and $S(\phi_1(f), \phi_1(g))$ are homogeneous and have the same totaldegree in terms of the T_{0k}'s. Applying ψ_1 to relation (1), we get (by Lemmas 8 and 9):

$$S(f,g) = \sum \psi_1(T_{ij})\psi_1(\rho_{ij}) \tag{3}$$

with $\psi_1(T_{ij}) \in k[Y, T_{ij} : 1 \leq i < j \leq n]$ and $\psi_1(\rho_{ij}) \in \mathcal{F}_5(J) \cup \mathcal{F}_6(J)$. Moreover, Lemma 8 applied to relation (2) gives that

$$\psi_1(T_{ij})\psi_1(\rho_{ij}) \leq S(f,g). \tag{4}$$

Now relations (3) and (4) show that $S(f,g)$ is in standard form relative to G.

The same arguments applied to $f \in \mathcal{F}_5(J) \cup \mathcal{F}_7(J)$, $g \in \mathcal{F}_7(J)$ with ϕ_1, ψ_1 replaced by ϕ_2, ψ_2 respectively shows that $S(f,g)$ is in standard form relative to G in this case as well.

3.3. The other cases

In this subsection, we investigate the other cases $(\mathcal{F}_i, \mathcal{F}_j)$ necessary to complete the proof of Proposition 5. As mentioned above, we only need to consider cases where Buchberger's first criterion does not apply.

<u>Case $(\mathcal{F}_2, \mathcal{F}_2)$</u>

Let

$$\begin{aligned} &f = T_iT_{1j} - T_jT_{1i}, \quad && g = T_aT_{1b} - T_bT_{1a} \\ &2 \leq i < j \leq n, && 2 \leq a < b \leq n \end{aligned}$$

be two *distinct* elements of $\mathcal{F}_2$. By Buchberger's first criterion, it is enough to consider the following cases

$$(1)\, j = b \;\; (2)\, i = a.$$

In case (1), it is enough to consider the case

$$2 \leq i < a < j = b \leq n,$$

for which we get

$$\begin{aligned} S(f,g) &= -T_{1a}T_iT_{1j} + T_aT_{1i}T_{1j} \\ &= -T_{1j}(T_iT_{1a} - T_aT_{1i}). \end{aligned}$$

In case (2), we may restrict to

$$2 \leq i = a < j < b \leq n$$

and one can verify that

$$\begin{aligned} S(f,g) &= -T_iT_bT_{1j} + T_iT_jT_{1b} \\ &= T_i(T_jT_{1b} - T_bT_{1j}). \end{aligned}$$

In both cases, $S(f,g)$ is in standard form relative to G.

Case $(\mathcal{F}_2, \mathcal{F}_3)$

Let

$$f = T_iT_{1j} - T_jT_{1i} \in \mathcal{F}_2, \quad g = T_{1a} + Y_1T_a \in \mathcal{F}_3$$
$$2 \le i < j \le n, \qquad 2 \le a \le n.$$

The leading monomials of f and g are relatively prime except when $a = j$. In this case,

$$\begin{aligned} S(f,g) &= -Y_1T_iT_{1j} - T_{1i}T_{1j} \\ &= -T_{1j}(T_{1i} + Y_1T_i). \end{aligned}$$

Case $(\mathcal{F}_2, \mathcal{F}_4)$

Let

$$f = T_iT_{1j} - T_jT_{1i} \in \mathcal{F}_2, \quad g = T_{ab} + Y_aT_b - Y_bT_a \in \mathcal{F}_4$$
$$2 \le i < j \le n, \qquad 2 \le a < b \le n.$$

The leading monomials of f and g are relatively prime except when $a = j$. In this case,

$$\begin{aligned} S(f,g) &= -Y_bT_iT_{1j} + T_{jb}T_{1i} + Y_jT_bT_{1i} \\ &= (T_{1i}T_{jb} - T_{1j}T_{ib} + T_{1b}T_{ij}) + T_{1j}(T_{ib} - Y_bT_i + Y_iT_b) \\ &+ T_b(Y_1T_{ij} + Y_jT_{1i} - Y_iT_{1j}) - T_{ij}(T_{1b} + Y_1T_b). \end{aligned}$$

Case $(\mathcal{F}_2, \mathcal{F}_5)$

Let

$$f = T_iT_{1j} - T_jT_{1i} \in \mathcal{F}_2, \quad g = T_{ab}T_{cd} - T_{ac}T_{bd} + T_{ad}T_{bc} \in \mathcal{F}_5$$
$$2 \le i < j \le n, \qquad 1 \le a < b < c < d \le n.$$

The only case where the leading monomials of f and g are not relatively prime is when $a = 1$ and $i = d$. In this case

$$\begin{aligned} S(f,g) &= -T_dT_{1j}T_{bc} - T_jT_{1b}T_{cd} + T_jT_{1c}T_{bd} \\ &= -T_d(T_{1b}T_{cj} - T_{1c}T_{bj} + T_{1j}T_{bc}) - T_{1b}(T_cT_{dj} - T_dT_{cj} + T_jT_{cd}) \\ &+ T_{1c}(T_bT_{dj} - T_dT_{bj} + T_jT_{bd}) - T_{dj}(T_bT_{1c} - T_cT_{1b}). \end{aligned}$$

Case $(\mathcal{F}_2, \mathcal{F}_6)$

Let

$$f = T_iT_{1j} - T_jT_{1i} \in \mathcal{F}_2, \quad g = Y_aT_{bc} - Y_bT_{ac} + Y_cT_{ab} \in \mathcal{F}_6$$
$$2 \le i < j \le n, \qquad 1 \le a < b < c \le n.$$

Only the case $a = 1$, $i = b$ needs to be considered. Two subcases arise:

$$(1.1)\ \ 2 \le i = b < j \le c \le n$$
$$(1.2)\ \ 2 \le i = b < c < j \le n.$$

In both cases, $S(f,g) = -Y_c T_b T_{1j} - Y_1 T_j T_{bc} + Y_b T_j T_{1c}$.

In case (1.1), the leading term of $S(f,g)$ is $-Y_c T_b T_{1j}$ and

$$\begin{aligned} S(f,g) = & -T_b(Y_1 T_{jc} - Y_j T_{1c} + Y_c T_{1j}) + Y_1(T_b T_{jc} - T_j T_{bc} + T_c T_{bj}) \\ & + T_{1c}(T_{bj} + Y_b T_j - Y_j T_b) - T_{bj}(T_{1c} + Y_1 T_c). \end{aligned}$$

In case (1.2), the leading term of $S(f,g)$ is $Y_b T_j T_{1c}$. Moreover

$$\begin{aligned} S(f,g) = & \, T_b(Y_1 T_{cj} - Y_c T_{1j} + Y_j T_{1c}) - Y_1(T_b T_{cj} - T_c T_{bj} + T_j T_{bc}) \\ & + T_{1c}(T_{bj} + Y_b T_j - Y_j T_b) - T_{bj}(T_{1c} + Y_1 T_c). \end{aligned}$$

This shows that $S(f,g)$ is in standard form relative to G.

Case $(\mathcal{F}_2, \mathcal{F}_7)$

Let

$$\begin{aligned} & f = T_i T_{1j} - T_j T_{1i} \in \mathcal{F}_2, \quad && g = T_a T_{bc} - T_b T_{ac} + T_c T_{ab} \in \mathcal{F}_7 \\ & 2 \le i < j \le n, && 2 \le a < b < c \le n. \end{aligned}$$

The leading monomials of f and g are relatively prime except when $j = c$ in which case we have the three possibilities:

$$\begin{aligned} &(1)\, 2 \le i \le a < b < c = j \le n \\ &(2)\, 2 \le a < i \le b < c = j \le n \\ &(3)\, 2 \le a < b < i < c = j \le n. \end{aligned}$$

In all the above three cases, $S(f,g) = -T_i T_{1c} T_{ab} - T_a T_{1i} T_{bc} + T_b T_{1i} T_{ac}$ with leading term equals to $-T_i T_{1c} T_{ab}$. In case (1),

$$\begin{aligned} S(f,g) = & -T_i(T_{1a} T_{bc} - T_{1b} T_{ac} + T_{1c} T_{ab}) + T_{bc}(T_i T_{1a} - T_a T_{1i}) \\ & - T_{ac}(T_i T_{1b} - T_b T_{1i}). \end{aligned}$$

In case (2),

$$\begin{aligned} S(f,g) = & -T_i(T_{1a} T_{bc} - T_{1b} T_{ac} + T_{1c} T_{ab}) - T_{bc}(T_a T_{1i} - T_i T_{1a}) \\ & - T_{ac}(T_i T_{1b} - T_b T_{1i}). \end{aligned}$$

In case (3),

$$\begin{aligned} S(f,g) = & -T_i(T_{1a} T_{bc} - T_{1b} T_{ac} + T_{1c} T_{ab}) - T_{bc}(T_a T_{1i} - T_i T_{1a}) \\ & + T_{ac}(T_b T_{1i} - T_i T_{1b}). \end{aligned}$$

These are expressions of $S(f,g)$ in standard form relative to G in each of the above three cases.

Case $(\mathcal{F}_3, \mathcal{F}_3)$

Let

$$f = T_{1i} + Y_1 T_i, \quad g = T_{1a} + Y_1 T_a$$
$$2 \le i \le n, \qquad 2 \le a \le n.$$

be two distinct elements of $\mathcal{F}_3$. We can clearly assume that $2 \le a < i \le n$ in which case $S(f,g) = T_a T_{1i} - T_i T_{1a} \in \mathcal{F}_2$. In particular, $S(f,g)$ is in standard form relative to G.

Case $(\mathcal{F}_3, \mathcal{F}_4)$

Let

$$f = T_{1i} + Y_1 T_i \in \mathcal{F}_3, \quad g = T_{ab} + Y_a T_b - Y_b T_a \in \mathcal{F}_4$$
$$2 \le i \le n, \qquad 2 \le a < b \le n.$$

The only case where the leading monomials of f and g are not relatively prime is when $i = a$. In this case

$$\begin{aligned} S(f,g) &= Y_b T_{1a} + Y_1 T_{ab} + Y_1 Y_a T_b \\ &= Y_a(T_{1b} + Y_1 T_b) + (Y_1 T_{ab} - Y_a T_{1b} + Y_b T_{1a}). \end{aligned}$$

Case $(\mathcal{F}_3, \mathcal{F}_7)$

Let

$$f = T_{1i} + Y_1 T_i \in \mathcal{F}_3, \quad g = T_a T_{bc} - T_b T_{ac} + T_c T_{ab} \in \mathcal{F}_7$$
$$2 \le i \le n, \qquad 1 \le a < b < c \le n.$$

When $i = c$, one has

$$\begin{aligned} S(f,g) &= T_{1c} T_{ab} - Y_1 T_a T_{bc} + Y_1 T_b T_{ac} \\ &= T_{ac}(T_{1b} + Y_1 T_b) + (T_{1a} T_{bc} - T_{1b} T_{ac} + T_{1c} T_{ab}) \\ &\quad - T_{bc}(T_{1a} + Y_1 T_a). \end{aligned}$$

Case $(\mathcal{F}_4, \mathcal{F}_4)$

Let

$$f = T_{ij} + Y_i T_j - Y_j T_i, \quad g = T_{ab} + Y_a T_b - Y_b T_a$$
$$2 \le i < j \le n, \qquad 2 \le a < b \le n$$

be two distinct elements of $\mathcal{F}_4$. The leading monomials of f and g are relatively prime except in either one of the following two cases:

$$(1)\, i = a \ \ (2)\, j = b.$$

In case (1), we may assume $1 \le i = a < j < b \le n$. In this case $S(f,g) = -Y_a Y_b T_j + Y_a Y_j T_b + Y_j T_{ab} - Y_b T_{aj}$ and one can easily verify that

$$S(f,g) = -(Y_a T_{jb} - Y_j T_{ab} + Y_b T_{aj}) + Y_a(T_{jb} + Y_j T_b - Y_b T_j).$$

In case (2), we may assume $1 \le i < a < j = b \le n$, in which case $S(f,g) = Y_a T_i T_b - Y_i T_a T_b + T_i T_{ab} - T_a T_{ib}$. Also, one can verify that

$$S(f,g) = (T_iT_{ab} - T_aT_{ib} + T_bT_{ia}) - T_b(T_{ia} + Y_iT_a - Y_aT_i).$$

Case $(\mathcal{F}_4, \mathcal{F}_6)$

Let

$$f = T_{ij} + Y_iT_j - Y_jT_i \in \mathcal{F}_4, \quad g = Y_aT_{bc} - Y_bT_{ac} + Y_cT_{ab} \in \mathcal{F}_6$$
$$2 \le i < j \le n, \qquad 1 \le a < b < c \le n.$$

The leading monomials of f and g are relatively prime except in the case where $j = c$. Three subcases are possible:

$$(1)\ 2 \le i \le a < b < c = j \le n$$
$$(2)\ 1 \le a < i \le b < c = j \le n$$
$$(3)\ 1 \le a < b < i < c = j \le n.$$

In all these cases $S(f,g) = -T_{ic}T_{ab} - Y_iT_cT_{ab} - Y_aT_iT_{bc} + Y_bT_iT_{ac}$ with leading term equals to $-Y_iT_cT_{ab}$. In case (1),

$$\begin{aligned} S(f,g) = &-(T_{ia}T_{bc} - T_{ib}T_{ac} + T_{ic}T_{ab}) - Y_i(T_aT_{bc} - T_bT_{ac} + T_cT_{ab}) \\ &- T_{ac}(T_{ib} + Y_iT_b - Y_bT_i) + T_{bc}(T_{ia} + Y_iT_a - Y_aT_i). \end{aligned}$$

In case (2),

$$\begin{aligned} S(f,g) = &(T_{ai}T_{bc} - T_{ab}T_{ic} + T_{ac}T_{ib}) - Y_i(T_aT_{bc} - T_bT_{ac} + T_cT_{ab}) \\ &- T_{ac}(T_{ib} + Y_iT_b - Y_bT_i) - T_{bc}(T_{ai} + Y_aT_i - Y_iT_a). \end{aligned}$$

In case (3),

$$\begin{aligned} S(f,g) = &(T_{ai}T_{bc} - T_{ab}T_{ic} + T_{ac}T_{ib}) - Y_i(T_aT_{bc} - T_bT_{ac} + T_cT_{ab}) \\ &+ T_{ac}(T_{bi} + Y_bT_i - Y_iT_b) - T_{bc}(T_{ai} + Y_aT_i - Y_iT_a). \end{aligned}$$

This proves that $S(f,g)$ is in standard form relative to G in this case.

Case $(\mathcal{F}_4, \mathcal{F}_7)$

Let

$$f = T_{ij} + Y_iT_j - Y_jT_i \in \mathcal{F}_4, \quad g = T_aT_{bc} - T_bT_{ac} + T_cT_{ab} \in \mathcal{F}_7$$
$$2 \le i < j \le n, \qquad 1 \le a < b < c \le n.$$

The leading monomials of f and g are relatively prime except in the case where $i = c$. This leaves us with one possibility:

$$1 \le a < b < c = i < j \le n.$$

In this case, $S(f,g) = -T_{ab}T_{cj} - Y_cT_jT_{ab} - Y_jT_aT_{bc} + Y_jT_bT_{ac}$ with $-Y_cT_jT_{ab}$ as leading term. Moreover, the following is a representation of $S(f,g)$ in standard form relative to G.

$$S(f,g) = -T_{ac}(T_{bj} + Y_bT_j - Y_jT_b) - (T_{ab}T_{cj} - T_{ac}T_{bj} + T_{aj}T_{bc})$$
$$+ T_{bc}(T_{aj} + Y_aT_j - Y_jT_a) - T_j(Y_aT_{bc} - Y_bT_{ac} + Y_cT_{ab}).$$

Case $(\mathcal{F}_6, \mathcal{F}_7)$

Let

$$f = Y_aT_{bc} - Y_bT_{ac} + Y_cT_{ab} \in \mathcal{F}_6, \quad g = T_iT_{jk} - T_jT_{ik} + T_kT_{ij} \in \mathcal{F}_7$$
$$1 \le a < b < c \le n, \qquad 1 \le i < j < k \le n$$

Since $\mathrm{LT}(f) = Y_cT_{ab}$ and $\mathrm{LT}(g) = T_kT_{ij}$, it is enough to consider the following case

$$1 \le a = i < b = j < c \le k \le n.$$

In this case, $S(f,g) = Y_aT_kT_{bc} - Y_bT_kT_{ac} - Y_cT_aT_{bk} + Y_cT_bT_{ak}$ has $-Y_bT_kT_{ac}$ as a leading term. On the other hand, the following shows that $S(f,g)$ is in standard form relative to G:

$$S(f,g) = -Y_b(T_aT_{ck} - T_cT_{ak} + T_kT_{ac}) - T_{ak}(T_{bc} - Y_bT_c + Y_cT_b)$$
$$+ T_{bc}(T_{ak} + Y_aT_k - Y_kT_a) + T_a(Y_bT_{ck} - Y_cT_{bk} + Y_kT_{bc}).$$

This finishes the proof of Proposition 5.

3.4. The proof of Theorem 4

In (4), the following tool for finite generation of the kernel of a locally nilpotent derivation was given. We include the proof for the reader's benefit.

Proposition 10. ***(Lemma 2.2**, (4)) 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 $A_0 = A$.

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 $n \ge 0$. Now if $y \in A$, then $d^ny \in A_0$ for some $n \ge 0$, so $d^ny \in d^nC \cap A_0 = d^nA_0$ and $y \in A_0$. $\square$

With the notations of Proposition 10, E plays the role of $k[X]$, 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 $k[X,Y]$.

Let $A_0 = k[X_1, \ldots, X_n, L_{ij} : 1 \le i < j \le n]$. Then $A_0 \subseteq \ker D$ and $(A_0)_{X_i} = (\ker D)_{X_i}$ for $i = 1, \ldots, n$. By Proposition 10, 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 $x = \Phi(X_1, \ldots, X_n, L_{ij} : 1 \le i < j \le n) = X_1z$. This means that Φ is in the kernel of the homomorphism

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

where π is the canonical epimorphism and ϵ sends T_i to X_i, $i = 1, \ldots, n$ and T_{jk} to L_{jk}, $1 \le j < k \le n$. 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, T_i to X_i, Y_i to Y_i $(i = 1, \ldots, n)$ 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

$$X_1, T_i - X_i, T_{jk} - L_{jk}, \text{ for } 1 \le i \le n \text{ and } 1 \le j < k \le n.$$

Indeed, let $N = \frac{n(n+5)}{2}$, and let $\Gamma = (\gamma_1, \ldots, \gamma_N)$ be the N-tuple

$$(X_1, \ldots, X_n, Y_1, \ldots, Y_n, T_1 - X_1, \ldots, T_n - X_n, T_{12} - L_{12}, \ldots, T_{n,n-1} - L_{n,n-1}),$$

then Γ is clearly a coordinate system of $k[X, Y, T]$ (that is $k[X, Y, T] = k[\gamma_1, \ldots, \gamma_N]$). Let $\lambda : k[\gamma_1, \ldots, \gamma_N] \to k[\gamma_2, \ldots, \gamma_{2n}]$ be the homomorphism of k-algebras defined by the following commutative diagram

$$\begin{array}{lll} k[X,Y,T] & \xrightarrow{\kappa} & k[X,Y]/(X_1) \cong k[\gamma_1, \ldots, \gamma_{2n}]/(\gamma_1) \\ \downarrow\cong & & \downarrow\cong \\ k[\Gamma] & \xrightarrow{\lambda} & k[\gamma_2, \ldots, \gamma_{2n}]. \end{array}$$

So

$$\lambda(\gamma_i) = \begin{cases} \gamma_i & \text{if } 2 \le i \le 2n \\ 0 & \text{if } i = 1 \text{ or } i > 2n \end{cases}$$

This means that $\ker\lambda = \ker\kappa = \langle \gamma_1, \gamma_{2n+1}, \gamma_{2n+2}, \ldots, \gamma_N \rangle = I$, and the claim is proved. Since $G = \cup_{i=1}^7 \mathcal{F}_i$ is a Groebner basis for the ideal I, the elimination theory together with (5) implies in particular that the set

$$\mathcal{H} := \{T_1\} \cup \mathcal{F}_2 \cup \mathcal{F}_5 \cup \mathcal{F}_7$$

generates $\ker\theta$ as an ideal of $k[T]$ and hence

$$\Phi = \sum (\xi_i h_i(T)) + T_1\rho(T) \tag{6}$$

for $\xi_i, \rho \in k[T]$ and $h_i \in \mathcal{F}_2 \cup \mathcal{F}_5 \cup \mathcal{F}_7$. On the other hand, one can easily verify the following identities:

$X_i L_{1j} - X_j L_{1i} = X_1 L_{ij} \in X_1 A_0$, $2 \le i < j \le n$

$L_{ij} L_{kl} - L_{ik} L_{jl} + L_{il} L_{jk} = 0$, $1 \le i < j < k < l \le n$

$X_i L_{jk} - X_j L_{ik} + X_k L_{jk} = 0$, $1 \le i < j < k \le n$.

This means that $x = \Phi(X, L) \in X_1 A_0$, and the theorem is proved.

4. On the proof of (6)

We start with a sufficient condition for the G_a-invariant subring to be finitely generated over k given by H. Kojima and M. Miyanishi in (6). First some notation. Let C be a noetherian domain, $A = \sum_{n\geq 0} A^n$ a finitely generated graded C-algebra which is an integral domain. Let $\delta : A \to A$ be a locally nilpotent C-derivation of A which is homogeneous of degree -1; that is $\delta(A^{n+1}) \subseteq A^n$ for each $n > 0$. Let A_0 and A_1 be the subrings $\delta^{-1}(0)$ and $(\delta^2)^{-1}(0)$ of A, respectively. Let $R = A[T]$ be a polynomial in one variable over A, $c \in C\backslash\{0\}$ and let $R_0 = \Delta^{-1}(0)$ where Δ denote the locally nilpotent C-derivation $c\frac{\partial}{\partial T} + \delta$ of R. Write $\delta(A_1) \cap C = \sum_{i=1}^{r} \delta(u_i)C$ with $u_i \in A_1$ and let $c_i v_i = \delta(u_i)T - cu_i$ for some $c_i \in C$ and $v_i \in R$, where c_i is a factor of $\delta(u_i)$ and c. Let $R' = A_0[v_1, \ldots, v_r]$, then R' is a graded subalgebra of R, which one can regard as a graded ring by setting $R^n = \sum_{i+j=n} A^i T^j$ with $\deg T = 1$.

Theorem 11. *(**Theorem 1.1**, (6)) With the above notations and assumptions, we assume further that:*
- *(1) A_0 is finitely generated over C;*
- *(2) depth$_\wp R \geq 2$ and depth$_\wp R' \geq 2$ for every $\wp \in Spec\, C$ with $\wp \supseteq \delta(A_1) \cap C$.*

Then $R' = R_0$. Hence R_0 is finitely generated over C.

This tool for finite generation of R_0 is then used to prove the following

Theorem 12. *(**Theorem 1.2**, (6)) Let $m \geq 2$, let $A = k[X_1, \ldots, X_m, Y_1, \ldots, Y_m]$ be a polynomial ring in $2m$ variables and let $\Delta = \sum_{i=1}^{m} X_i^{t+1}\partial/\partial Y_i$ be a locally nilpotent k-derivation of A, where $t \geq 2$. Then the invariant subring $A_0 := \Delta^{-1}(0)$ is given as*

$$A_0 = k[X_1, \ldots, X_m, X_i^{t+1}Y_j - X_j^{t+1}Y_i : 1 \leq i < j \leq m]$$

$$\cong \frac{k[X_1, \ldots, X_m, U_{ij} : 1 \leq i < j < k \leq m]}{(X_i^{t+1}U_{jk} - X_j^{t+1}U_{ik} + X_k^{t+1}U_{ij} : 1 \leq i < j < k \leq m)}.$$

Here, in the second presentation of the ring A_0, we adjoin variables U_{ij} to the polynomial ring $k[X_1, \ldots, X_m]$ for all possible pairs (i, j) with $1 \leq i < j \leq m$ and consider the residue ring modulo the ideal generated by the elements

$$X_i^{t+1}U_{jk} - X_j^{t+1}U_{ik} + X_k^{t+1}U_{ij}$$

for all possible triplets (i, j, k) with $1 \leq i < j < k \leq m$.

In what follows we show that the proof of the above theorem, as it is given in (6), fails at one stage. We begin by describing roughly the proof of the theorem propsed in (6). In our argument we use $m = 4$ for simplicity.

Let $D = k[X_1, X_2, X_3, X_4, Y_1, Y_2, Y_3]$. Then with the notation of Theorem 12, $A = D[Y_4]$, and $\Delta = \delta + X_4^{t+1}\frac{\partial}{\partial Y_4}$ where $\delta = \sum_{i=1}^{3} X_i^{t+1}\frac{\partial}{\partial Y_i}$. In (6), the authors used an induction hypothesis to assume that the kernel D_0 of δ has the form described in the theorem. Since we are using a specific value for m, we can use a result from (4) to assume that $D_0 = k[X_1, X_2, X_3, X_4, X_i^{t+1}Y_j - X_j^{t+1}Y_i : 1 \leq i < j \leq 3]$ and the isomorphism

$$D_0 \cong k[X_1, X_2, X_3, X_4, U_{12}, U_{13}, U_{23}]/(X_1^{t+1}U_{23} - X_2^{t+1}U_{13} + X_3^{t+1}U_{12}) \tag{7}$$

follows easily. Write

$$D_0 = k[x_1, x_2, x_3, u_{12}, u_{13}, u_{23}][X_4]$$

where x_i, u_{kl} are the images in D_0 of X_i and U_{kl}: $1 \leq i \leq 3$, $1 \leq k < l \leq 3$ respectively.

For the passage from $m = 3$ to $m = 4$, the authors used Theorem 11 to show that A_0 is isomorphic to

$$A' := D_0[X_i^{t+1}Y_4 - X_4^{t+1}Y_i : 1 \leq i \leq 3].$$

To achieve this, the authors needed to know that the following quotient ring:

$$B := D_0[U_1, U_2, U_3]/(X_i^{t+1}U_j - X_j^{t+1}U_i + X_4^{t+1}\overline{U_{ij}} : 1 \leq i < j \leq 3)$$

is isomorphic to A' via the natural D_0-homomorphism $\phi : B \to A'$ sending U_i to $X_i^{t+1}Y_4 - X_4^{t+1}Y_i$ $(1 \leq i \leq 3)$. Clearly ϕ is onto, and to show that it is injective, the authors argued first that B is an integral domain and then use the relation

$$\text{height}(\ker \phi) + \dim(B/\ker \phi) = \dim B$$

together with the fact that $\dim A' = \dim B$ to deduce that $\ker \phi = 0$. So, the only detail that remains to be checked is the fact that B is indeed a domain. To do this, the authors argued that the image x_4 of X_4 in B is a nonzero divisor of B and that the quotient ring B/x_4B is a domain. In the following subsection, we prove that B is not a domain.

4.1. Proof of the fact that B is not a domain

Let $k[X][Y][U_1, U_2, U_3]$ be the polynomial ring in eleven variables over k, where $X = \{X_1, X_2, X_3, X_4\}$, $Y = \{Y_1, Y_2, Y_3, Y_4\}$ are the sets of variables. For each $i, j \in \{1, 2, 3, 4\}$, we set

$$L_{i,j} = X_i^{t+1}Y_j - X_j^{t+1}Y_i, \;\; M_{i,j} = X_i^{t+1}Y_j - X_j^{t+1}Y_i + X_4^{t+1}L_{i,j}.$$

Then $B = S/P$ where

$$S = k[X][L_{1,2}, L_{1,3}, L_{23}][U_1, U_2, U_3]$$

and P is the ideal of S generated by $M_{1,2}$, $M_{1,3}$ and $M_{2,3}$. Consider the homomorphism of $k[X, Y]$-algebras

$$\phi' : k[X, Y][U_1, U_2, U_3] \to k[X, Y][L_{1,4}, L_{2,4}, L_{3,4}]$$

defined by $\phi'(U_i) = L_{i,4}$ for $i = 1, 2, 3$. In view of the relations:

$$L_{2,3} = X_1^{-t-1}(X_2^{t+1}L_{1,3} - X_3^{t+1}L_{1,2}), \;\; L_{i,4} = X_1^{-t-1}(X_i^{t+1}L_{1,4} - X_4^{t+1}L_{1,i})$$

for $i = 2, 3$, we know that the transcendence degree of

$$\phi'(S) = k[X][L_{1,2}, L_{1,3}, L_{2,3}][L_{1,4}, L_{2,4}, L_{3,4}]$$

over k is seven. Here, the transcendence degree of a k-domain R is defined to be the transcendence degree of the field of fractions of R over k. Clearly, $\phi'(S)$ is isomorphic to $S/(S \cap \ker \phi')$. It follows that

$$\phi'(M_{i,j}) = X_i^{t+1} L_{j,4} - X_j^{t+1} L_{i,4} + X_4^{t+1} L_{i,j} = 0$$

for $1 \leq i < j \leq 3$, so P is contained in the prime ideal $S \cap \ker \phi'$. Hence, X_1 is not in P since $\phi'(X_1) \neq 0$. Thus, the image x_1 of X_1 in B is not zero.
Now suppose to the contrary that B is a domain, then in particular P is a prime ideal of S. Moreover

$$\begin{aligned} B \subseteq B[x_1^{-1}] = S[X_1^{-1}]/P' &\cong k[X][X_1^{-1}, L_{1,2}, L_{1,3}, L_{2,3}, U_1] \\ &= k[X][X_1^{-1}, L_{1,2}, L_{1,3}, U_1], \end{aligned}$$

where P' is the ideal of $S[X_1^{-1}]$ generated by

$$X_1^{-t-1} M_{1,i} = U_i - (X_1^{-1} X_i)^{t+1} U_1 + (X_1^{-1} X_4)^{t+1} L_{1,i}$$

for $i = 2, 3$. From this, we know that the transcendence degree of B is seven. Consequently, we must have $P = S \cap \ker \phi'$, since the transcendence degree of $S/(S \cap \ker \phi')$ is also seven. A direct computation shows that

$$f := Y_1 M_{2,3} - Y_2 M_{1,3} + Y_3 M_{1,2} = -L_{2,3} U_1 + L_{1,3} U_2 - L_{1,2} U_3.$$

Hence, $f \in S \cap \ker \phi'$. We show that f does not belong to P by contradiction. Note that the monomial $Y_1 X_2^{t+1} U_3$ appears in f with a nonzero coefficient. Suppose that $f = f_1 M_{2,3} + f_2 M_{1,3} + f_3 M_{1,2}$ for some $f_1, f_2, f_3 \in S$. Then $Y_1 X_2^{t+1} U_3$ must appear in $f_1 X_2^{t+1} U_3$ or $f' := -f_1 X_3^{t+1} U_2 + f_1 X_4^{t+1} L_{2,3} + f_2 M_{1,3} + f_3 M_{1,2}$. It is easy to check that each monomial appearing in f' is divisible by one of $X_1^{t+1}, X_3^{t+1}, X_4^{t+1}, U_1$ and U_2 in $k[X][Y][U_1, U_2, U_3]$, while $Y_1 X_2^{t+1} U_3$ is not. Hence $Y_1 X_2^{t+1} U_3$ appears in $f_1 X_2^{t+1} U_3$. This implies that the monomial Y_1 appears in f_1. However, it follows from the definition of S that the monomial Y_1 does not appear in any element of S, a contradiction. Thus, f does not belong to P, and so we get that $P \neq S \cap \ker \phi'$. This is a contradiction.

This proves that B is not a domain.

Acknowledgment. The simple proof of the fact that B is not a domain appearing in the last section is due to the referee of this paper. In the original version of the paper, the author proved that B/x_4B was not a domain, but was not sure about the fact that B itself is a domain. The author would also like to thank the referee for his many valuable comments and suggestions.

References

[1] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and algorithmes*, New York: Springer-Verlag, 1996.

[2] D. Daigle, G. Freudenburg, *A counterexample to Hilbert's Fourtennth Problem in dimension five*, J. Algebra, **221** (1999), 528-535.

[3] G. Freudenburg, *A counterexample to Hilbert's Fourtennth Problem in dimension six*, Transformation Groups **5** (2000), 61-71.

[4] J. Khoury, *On some properties of locally nilpotent derivations in dimension six*, Journal of Pure and Applied Algebra, **156/1** (2001), 69-79.

[5] J. Khoury, *A note on elementary derivations*, Serdica Math. J. **30**, 549-570.

[6] H. Kojima, M. Miyanishi, *On Robert's counterexample to the fourteenth problem of Hilbert*, Journal of Pure and applied algebra, **122** (1997), 277-292.

[7] L. Makar-Limanov, *More on the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$, or a $\mathbb{C}^3$ like threefold which is not $\mathbb{C}^3$*, Israel J. Math. **96** (1996), 419-429.

[8] A. Nowicki, *Polynomial derivations and their rings of constants*, Wydawnictwo Uniwersytetu Mikolaja Kopernika, Torun 1994.

[9] R. Weitzenbock, *Über die invaranten Gruppen*, Acta. Math., **58** (1932), 231-293.