DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NIJMEGEN The Netherlands

An algorithm to compute the kernel of a derivation up to a certain degree

Stefan Maubach

Report No. 98.. (November 1998)

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF NIJMEGEN
Toernooiveld
6525 ED Nijmegen
The Netherlands

Abstract

An algorithm is described which computes generators of the kernel of derivations on $k[X_1, \ldots, X_n]$ up to a previously given bound. For w-homogeneous derivations it is shown that if the algorithm computes a generating set for the kernel then this set is minimal.

1 Introduction

Derivations and the study of their kernels play a crucial role in many problems. For example the famous Hilbert 14 problem was solved by examining kernels of certain derivations (see [Freudenburg], [Daigle,Freudenburg], [Deveney,Finston]). Also a proof of the fact that the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$ is not isomorphic to $\mathbb{C}^3$ uses kernels of derivations (see [Derksen], [Makar-Limanov]). For more problems about derivations (and their kernels) we refer to the excellent account in [Nowicki].

Hence it is often important to find generators of the kernel. For locally nilpotent derivations there are two algorithms in the literature. The first one was given in [Tan] who only considered linear derivations. (derivations on $k[X_1, \ldots, X_n]$ for which each $D(X_i)$ is linear.) The most important one is given in [Essen]. This algorithm computes all generators of the kernel of any locally nilpotent derivation on just any integral $\mathbb{Q}$-algebra provided the kernel is finitely generated. If one has an infinitely generated kernel, the algorithm never stops. However, a big offset of this algorithm is that it is very inefficient and time consuming since it heavily depends on Gröbner bases computations. For computational purposes the ESSEN-algorithm is often useless due to this flaw.

The new algorithm described in this article can be used to compute generators up to a certain degree of the kernel of any k-derivation (not necessarily locally nilpotent). In section 5 we will describe the new algorithm on "w-homogeneous" derivations. In section 6 we show how to extend the algorithm on all derivations.

The algorithm does not use Gröbner bases but linear algebra instead. This makes it much more efficient. How this algorithm works is described in section 5. In section 7 an example of the algorithm is given and the efficiency of this algorithm is compared to the algorithm in [Essen]; the differences are probably largely in favor of the new algorithm.

In section 8 it is proved that the algorithm provides a minimal number of generators for w-homogeneous derivations.

This algorithm is in fact an application of a very useful grading theory: the concept of D-gradings. These gradings are constructed given a certain derivation, and a lot of questions concerning this derivation can be solved by the use of this theory. This is described in section 3. An example of how these gradings can be used is in section 4. More examples of this can be found in [Maubach2].

In section 2 some notations are summed up which are used throughout the paper.

2 Notations and introduction

In this article the following notations are used:

- $A = k[X_1, \ldots, X_p]$, the polynomial ring in p variables, where k is a field of characteristic zero.
- By "$H \in A$ a monomial" we mean : H is of the form $X_1^{\alpha_1} \cdots X_p^{\alpha_p}$ where $\alpha_i \in \mathbb{N}$. Sometimes we use the same word for $c \cdot X_1^{\alpha_1} \cdots X_p^{\alpha_p}$ where $c \in k, c \neq 0$, but this won't give rise to any misunderstandings.
- Given $\{F_1, \ldots, F_q\} \subset A$ a finite subset of A, we denote $\{F_1, \ldots, F_q\}$ by $\{F\}$ and $k[F_1, \ldots, F_q]$ by $k[F]$. Define $\hat{F_i} := \{F_1, \ldots, F_{i-1}, F_{i+1}, \ldots, F_q\}$ (even if $F_i = F_j$ some $j \neq i$). Furthermore, $\{F_v\}$ means a subset of generators of the kernel of a derivation homogeneous of degree v; if $v = (v_1, \ldots, v_n)$ we will write $A_{(v_1,\ldots,v_n)}$ for A_v.
- If $F_1, \ldots, F_q \in A$ and $\alpha \in \mathbb{N}^q$ we write F^α for $F_1^{\alpha_1} \cdots F_q^{\alpha_q}$
- D is a k-derivation on A. (See below for a definition.)
- By a grading we mean a decomposition of A of the form $A = \oplus_{\sigma \in \mathbb{N}^q} A_\sigma$ for some $q \in \mathbb{N}^*$ such that for each $\sigma \in \mathbb{N}$ A_σ is a k-vectorspace and $A_\sigma A_\tau \subseteq A_{\sigma+\tau}$ for all $\sigma, \tau \in \mathbb{N}^k$.
- We say "F is homogeneous of degree σ" (with respect to a grading) if $F \in A_\sigma$.
- The symbol "$\subset$" is reserved to "strictly included". For "included" the symbol "$\subseteq$" is used.

3 Special gradings on a ring: D-gradings

The concept of w-gradings is well-known: if we have a polynomial ring A (in p variables) and a vector $0 \neq w \in \mathbb{N}^p$ then we can define a function on monomials X^α by

$$deg(X^\alpha) = < \alpha, w >$$

where $<,>$ is the usual inner product on $\mathbb{N}^p$. If we now define

$$A_n := \text{span}_k\{X^\alpha \mid deg(X^\alpha) = n\}$$

then $A = \oplus A_n$ is a well-defined grading. (It is easy to check that $A_n A_m \subseteq A_{n+m}$.) We can extend deg on elements of A_n: if $0 \neq F \in A_n$ then define $deg(F) = n$.

Definition 3.1. Assume we have on A a derivation D (not necessarily locally nilpotent) and a grading given by a function 'deg' coming from a w-grading. Let $m \in \mathbb{Z}$. We call such a grading a D-homogeneous grading of degree m if $D(A_n) \subseteq A_{n-m}$ for all n. We may also split them into 3 groups:

If $m = 0$ then we call the grading a D-invariant grading.
If $m < 0$ then we call the grading a D-increasing grading.
If $m > 0$ then we call the grading a D-decreasing grading.

Notice that "F is homogeneous with respect to the grading" means something completely different from "D is homogeneous with respect to the grading". The first sentence says that $F \in A_n$ for some n, and the second one says that there exists some m such that for all n and all $F \in A_n$ we have $D(F) \in A_{n-m}$.

We have an easy method to check if a grading is D-homogeneous with respect to a given D.

Lemma 3.2. *Let D be any derivation on A. Assume that A has a grading $\oplus A_n$. Then the grading is D-homogeneous of degree m iff $D(X_i)$ is homogeneous with respect to the grading and $deg(D(X_i)) = deg(X_i) - m$ for all i with $D(X_i) \neq 0$.*

Proof. $\Rightarrow$ is obvious. So assume that $D(X_i)$ is homogeneous and that $deg(X_i) = deg(D(X_i)) - m$ for all i with $D(X_i) \neq 0$. We have to prove that this implies $D(A_n) \subseteq A_{n-m}$. Suppose $F \in A_n$. If $D(F) = 0$ then $D(F) \in A_{n-m}$. So assume $D(F) \neq 0$. We will prove $D(F) \in A_{n-m}$. Let $F = \sum c_\alpha X^\alpha$. So we have $deg(X^\alpha) = n$ for every α with $c_\alpha \neq 0$.

$$\begin{aligned} D(F) = &\ D(\textstyle\sum c_\alpha X^\alpha) \\ = &\ \textstyle\sum D(c_\alpha X^\alpha) \\ = &\ \textstyle\sum \sum_{i=1}^{p} c_\alpha \alpha_i X^{\alpha - e_i} D(X_i). \end{aligned}$$

Since $D(F) \neq 0$ there exist i with $c_\alpha \alpha_i X^{\alpha - e_i} D(X_i) \neq 0$. For all such i we have

$$\begin{aligned} deg(c_\alpha \alpha_i X^{\alpha - e_i} D(X_i)) = &\ deg(X^{\alpha - e_i} D(X_i)) \\ = &\ deg(X^\alpha) - deg(X_i) + deg(D(X_i)) \\ \text{(assumption)} = &\ n - deg(X_i) + deg(X_i) - m \\ = &\ n - m. \end{aligned}$$

So $F \in A_{n-m}$. □

Definition 3.3. Let D be a derivation on A. To $w_1, \ldots, w_k \in \mathbb{N}^p$ associate an $\mathbb{N}^k$-grading "*grad*" on A: $grad(X^\alpha) := (< w_1, \alpha >, \ldots, < w_k, \alpha >)$. We call such a grading a *combined grading* if each deg_{w_i} is D-homogeneous.

Keep in mind that these functions *grad*, *deg*, etc. are NOT defined on A. One can only write down '$grad(F)$' if one knows F to be homogeneous with respect to *grad*.

4 Example

In this section an example is shown of how these special gradings are defined and what one can do with it. First some definitions are necessary:

Definition 4.1. $A := k[X, Y, Z, T]$, $D := Y^a \partial_X + Z^b \partial_Y + T^c \partial_Z$ $(a, b, c \in \mathbb{N})$.

Let $m \in \mathbb{Z}$. We'll try to find a D-homogeneous grading of degree m. Assuming one has a D-homogeneous grading of degree m on A, denoted deg, then

$$
\begin{array}{rll}
(*) \quad deg(X^\alpha Y^\beta Z^\gamma T^\delta) = deg(& D(X^\alpha Y^\beta Z^\gamma T^\delta)) - m \\
= deg(& \alpha X^{\alpha-1} Y^{\beta+a} Z^\gamma T^\delta + \\
& \beta X^\alpha Y^{\beta-1} Z^{\gamma+b} T^\delta + \\
& \gamma X^\alpha Y^\beta Z^{\gamma-1} T^{\delta+c} &) - m
\end{array}
$$

must hold. Hence, if for all $\alpha, \beta, \gamma, \delta \in \mathbb{N}$ we have $deg(X^\alpha Y^\beta Z^\gamma T^\delta) = \alpha w_1 + \beta w_2 + \gamma w_3 + \delta w_4$ it follows that for all $\alpha, \beta, \gamma, \delta \in \mathbb{N}$:

$$
\begin{array}{rcl}
(**) \quad \alpha w_1 + \beta w_2 + \gamma w_3 + \delta w_4 = & (\alpha - 1) w_1 + (\beta + a) w_2 + \gamma w_3 + \delta w_4 - m \\
= & \alpha w_1 + (\beta - 1) w_2 + (\gamma + b) w_3 + \delta w_4 - m \\
= & \alpha w_1 + \beta w_2 + (\gamma - 1) w_3 + (\delta + c) w_4 - m
\end{array}
$$

holds. This is true iff $0 = -w_1 + a w_2 - m = -w_2 + b w_3 - m = -w_3 + c w_4 - m$. Hence $w = -m(ab + a + 1, b + 1, 1, 0) + w_4(abc, bc, c, 1)$. Let us choose $m = 0, w_4 = 1$ to find a D-invariant grading and let us choose $m = -1, w_4 = 0$ to find a D-decreasing grading of degree -1. So we define $deg_2(X^\alpha Y^\beta Z^\gamma T^\delta) =< (\alpha, \beta, \gamma, \delta), (abc, bc, c, 1) >$, which induces a D-invariant grading; $deg_1(X^\alpha Y^\beta Z^\gamma T^\delta) =< (\alpha, \beta, \gamma, \delta), (ab+a+1, b+1, 1, 0) >$, which induces a D-decreasing grading. Hence by the previous chapter one obtains: $grad := (deg_2, deg_1)$ which induces a combined grading on A.

The next theorem is a nice example of how things work with D-invariant gradings.

Lemma 4.2. *Let $D_1 := Y^a \partial_X + Z^b \partial_Y + S \partial_Z$ and $D_2 := Y^a \partial_X + Z^b \partial_Y + T^c \partial_Z$. If $ker(D_1)$ is finitely generated, then $ker(D_2)$ is as well.*

Proof. Suppose $ker(D_1) = k[F_1, \ldots, F_n] \subseteq k[X, Y, Z, S]$.
Consider the substitution homomorphism $\phi : k[X, Y, Z, S] \longrightarrow k[X, Y, Z, T]$ sending S to T^c and leaving the elements of $k[X, Y, Z]$ invariant. Then it is easy to prove that $D_2 \circ \phi = \phi \circ D_1$.
We will prove that $ker(D_2) = k[T][\phi(F_1), \ldots, \phi(F_n)]$. Define deg_2 in $k[X, Y, Z, S]$ in the same way as above (replace S by T). Suppose $G \in ker(D_2)$. Write $G = \sum_{i=0}^{c-1} G_i$ where every monomial H appearing in G_i has $deg_2(H) = i \bmod (c)$. For such H the following statement holds:

$$deg_2(H) = deg_2(X^\alpha Y^\beta Z^\gamma T^\delta) \equiv c(\ldots) + \delta \equiv \delta \text{mod}(c).$$

So $G_i/T^i \in k[X, Y, Z, T^c]$. Hence we can define $\phi^{-1}(G_i/T^i)$ (and even define $\phi^{-1} D_2(G_i/T^i)$). Furthermore, $D_2(G_i) = 0$ because we have divided everything into groups of the same D-invariant degree. Now we have:

$$
\begin{array}{rrl}
& 0 = & D_2(\frac{G_i}{T^i}) \\
\Leftrightarrow & 0 = & \phi^{-1} D_2(\frac{G_i}{T^i}) \\
& = & \phi^{-1} D_2 \phi \phi^{-1}(\frac{G_i}{T^i}) \\
& = & D_1 \phi^{-1}(\frac{G_i}{T^i}).
\end{array}
$$

Hence

$$\begin{array}{rrl} & \phi^{-1}\frac{G_i}{T^i} \in & k[F_1,\ldots,F_n] \\ \Leftrightarrow & \frac{G_i}{T^i} \in & \phi(k[F_1,\ldots,F_n]) \\ & = & k[\phi(F_1),\ldots,\phi(F_n)]. \end{array}$$

Hence $G_i \in T^i k[\phi(F_1),\ldots,\phi(F_n)] \subset k[T][\phi(F_1),\ldots,\phi(F_n)]$. So $G = \sum_{i=0}^{c-1} G_i \in k[T][\phi(F_1),\ldots,\phi(F_n)]$, and this is what we needed. □

So this last lemma states that one can choose $c = 1$ for computational purposes.

Remark: in [Maubach2] it is proved that the derivation D_2 (and hence D_1) have finitely generated kernel. A stronger result is obtained: triangular k-derivations over $k[X_1, X_2, X_3, X_4]$ which map each X_i to a monomial have a kernel which is generated over k by at most four elements.

5 An algorithm to compute minimal sets of generators of kernels of some derivations

This section will describe the algorithm on a special class of derivations.

Convention: By v, w we will denote elements in $\mathbb{N}^q$.

Definition 5.1. Write $w \le v$ for $v, w \in \mathbb{N}^q$ if the i-th coordinate of w is smaller than or equal to the i-th coordinate of v for all i. We also write $w < v$ when $w \le v$ and $w \ne v$.

Assume that our ring A has a grading such that

$$A := \bigoplus_{v\in\mathbb{N}^q} A_v$$

and D is a derivation homogeneous with respect to this grading.

Definition 5.2.

$$B_v := \bigoplus_{w\le v} A_w$$

and

$$B_v^- := \bigoplus_{w<v} A_w.$$

Definition 5.3. We call $\{F\} = \{F_1,\ldots,F_s\} \subseteq B_v$ a "good set" for $v \in \mathbb{N}^q$ when:

(1) each $F_i \in A_w$ for some $w \le v$,
(2) $k[F] \cap B_v = ker(D) \cap B_v$,
(3) for every i one has $F_i \notin k[\hat{F_i}]$.

We also define $\{F\} \subseteq B_v^-$ a "good set for v^-" when:

(1) each $F_i \in A_w$ for some $w < v$,
(2) $k[F] \cap B_v^- = ker(D) \cap B_v^-$,
(3) for every i one has $F_i \notin k[\hat{F_i}]$.

Problem: construct algebraic generators for $ker(D)$. More precisely: compute a (preferably minimal) finite set $\{F\} := \{F_1, F_2, \ldots, F_n\} \subset A$ such that $ker(D) \supset k[F]$ and $F_i \notin k[\hat{F_i}]$ for all i.

The algorithm's purpose: We will give an algorithm to find such algebraic generators *up to a certain degree*. However, we are not able to use the algorithm for just any (locally nilpotent) derivation D on A. In addition we need:

Assumption: A is equipped with a *combined grading* consisting of $q \geq 1$ D-homogeneous gradings of degree m_i. (Hence $A = \oplus A_v$, $v \in \mathbb{N}^q$.) Furthermore we assume that $dim_k(A_v) < \infty$ for all v, so we're dealing with finite dimensional k-vector spaces only.

Definition 5.4. We denote by D_v for $v \in \mathbb{N}^q$ the restriction of D to A_v. Then by the assumptions on the grading *grad* we have $D(A_v) \subseteq A_{v-\bar{m}}$ where $\bar{m} = (m_1, \ldots, m_q)$, ($m_i$ as in "Assumption") and D_v can be seen as a linear map from the finite dimensional vector space A_v to the finite dimensional vector space $A_{v-\bar{m}}$.

Lemma 5.5. $ker(D_v) = ker(D) \cap A_v$.

Proof. ($\supseteq$) If $F \in ker(D) \cap A_v$ then $F \in A_v$ and hence $D(F) = D_v(F) = 0$ and $F \in ker(D)$. ($\subseteq$) If $F \in ker(D_v)$ then $F \in A_v$ and $D(F) = 0$. □

Input of the algorithm:

- $\{X_1, \ldots, X_p\}$, the generators of the k-algebra A.
- D a k-derivation on A.
- a combined grading $A := \oplus_{v \in \mathbb{N}^q} A_v$, denoted by *grad*, which of course depends on D. (This combined grading must satisfy the assumptions above.)
- $b \in \mathbb{N}^q$, the degree as where to stop calculating.

Output: generators $F_1, \ldots, F_s \in B_b$ such that $\{F_1, \ldots, F_s\}$ is a good set for b. More precisely:
(1) each $F_i \in A_v$ for some $v < b$.
(2) $k[F_1, \ldots, F_s] \cap B_b = ker(D) \cap B_b$ and
(3) $F_i \notin k[\hat{F_i}]$.

The algorithm is based on the following induction step:

Lemma 5.6. *Let $v \in \mathbb{N}^q$. Suppose we have finite sets $\{F_w\} \subset A_w$ for all $w < v$ such that $\bigcup_{w<v}\{F_w\}$ is a good set for v^-. Then we can construct a finite set $\{F_v\} \subset A_v$ such that $\bigcup_{w\leq v}\{F_w\}$ is a good set for v.*

Before we will prove this lemma we show that it gives us the needed tool to calculate good sets.

Lemma 5.7. *Let $v \in \mathbb{N}^q$. Suppose we have finite sets $\{F_w\} \subset A_w$ for all $w < v$ such that for all $u < v$: $\bigcup_{w\leq u}\{F_w\}$ is a good set for u. Then $\bigcup_{w<v}\{F_w\}$ is a good set for v^-.*

Proof. Write $\{F\} := \bigcup_{w<v}\{F_w\}$. We need to prove
(1) $k[F] \cap B_v^- = ker(D) \cap B_v^-$.
(2) if $F_i \in \{F\}$ then $F_i \notin k[\hat{F}_i]$.
(1): "$\subseteq$" is trivial. "$\supseteq$": Let $G \in ker(D)$ and suppose $G \in B_v^-$. Split G into homogeneous parts: $G = \sum G_h$. Then $0 = D(G) = D(\sum G_h) = \sum D(G_h)$ thus $D(G_h) = 0$ and hence $G_h \in ker(D)$. So $grad(G_h)$ is defined and $< v$. Thus $G_h \in k[F]$. Hence $G = \sum G_h \in k[F]$.
(2): Let $F_i \in \{F\}$. Then F_i is homogeneous and $grad(F_i) < v$. Let $u := grad(F_i)$. Then $F_i \in \{F\} \cap B_u = \bigcup_{w\leq u}\{F_w\}$. Write $\widetilde{F} := \bigcup_{w\leq u}\{F_w\}$. Suppose $F_i \in k[\hat{F}]$. Then since $F_i \in B_u$ we have $F_i \in k[\hat{F}] \cap B_u$. But then $F_i \in k[\hat{\widetilde{F}}]$. But this states by definition that $\widetilde{F}$ is not a good set for u. Contradiction. ☐

By these last two lemma's we can calculate good sets for any vector v if we have a good set for $A_{(0,\ldots,0)}$.

Lemma 5.8. *A good set for $A_{(0,\ldots,0)}$ is the empty set ($A_{(0,\ldots,0)} = k$).*

Proof. Of course $A_{(0,\ldots,0)} \supseteq k$. Now suppose $A_{(0,\ldots,0)} \neq k$. Then take $a \in A_{(0,\ldots,0)}$ for which $a \notin k$. Then $a, a^2, a^3, \ldots \in A_{(0,\ldots,0)}$. But then $\{1, a, a^2, \ldots\}$ is a k-independent subset of $A_{(0,\ldots,0)}$ and thus $A_{(0,\ldots,0)}$ not finite dimensional. But by assumption, however, A_v finite dimensional for any v. Contradiction, so $A_{(0,\ldots,0)} = k$ and hence $ker(D) \cap A_{(0,\ldots,0)} = k$. So the empty set is a good set for $A_{(0,\ldots,0)}$. ☐

It suffices to prove lemma 5.6. The following proof is in fact a description of the algorithm.

Proof. (of lemma 5.6.) Write $\{F\} = \bigcup_{w<v}\{F_w\}$.
$k[F] \cap A_v$ is a finite dimensional k-vector space. It is spanned by all F^α for which $F^\alpha \in A_v$. Let $s := \#F$.

$$I := \{\alpha \in \mathbb{N}^s \mid F^\alpha \in A_v\}.$$

Then we know:

$$(*) \quad k[F] \cap A_v = \sum_{\alpha\in I} k \cdot F^\alpha.$$

We did write "$\sum$" and not "$\oplus$" since we don't know that $\cup_{\alpha\in I}\{F^\alpha\}$ is an independent set over k. But, of course we can take (and calculate!) a subset J of I for which

$$k[F]\cap A_v=\bigoplus_{\alpha\in J}k\cdot F^\alpha.$$

Hence $dim_k(k[F]\cap A_v)=\#J$. Now we compute $ker(D_v)$. (This is easy since it is a linear k-map from a finite dimensional k-vectorspace to a finite dimensional k-vectorspace.) Since $k[F]\cap A_v\subseteq ker(D)\cap A_v$ we have (by lemma 5.5)

$$k[F]\cap A_v\subseteq ker(D)\cap A_v=ker(D_v).$$

Hence $\oplus_{\alpha\in J}k{\cdot}F^\alpha\subseteq ker(D_v)$. Thus $\{F^\alpha|\alpha\in J\}$ are independent elements in $ker(D_v)$. Now choose $\{F_v\}\subset ker(D_v)$ for which $\{F^\alpha;\alpha\in J\}\cup\{F_v\}$ forms a k-linear basis of $ker(D_v)$. So

$$ker(D_v)=\Big(\bigoplus_{\alpha\in J}k\cdot F^\alpha\Big)\oplus\Big(\bigoplus_{f\in\{F_v\}}k\cdot f\Big).$$

Note that $\#\{F_v\}=dim_k(ker(D_v))-dim_k(k[F]\cap A_v)<\infty$ and that $\{F_v\}$ is a set of polynomials homogeneous of degree v. Then we claim: $\{F,F_v\}$ is a good set for v. For this we need two (in fact three) things to be true :

(1) $ker(D)\cap B_v=k[F,F_v]\cap B_v$
(2)(a) $F_{v,i}\notin k[F,\hat{F}_{v,i}]$, and (2)(b) $F_i\notin k[\hat{F}_i,F_v]$.

Where $\hat{F}_{v,i}$ is defined as follows: if $\{F_v\}$ is$\{G_1,\ldots,G_n\}$ then write $\hat{F}_{v,i}:=\{G_1,\ldots,G_{i-1},G_{i+1},\ldots,G_n\}$.
Proof of (1): "$\supseteq$" is O.K. "$\subseteq$": take $G\in ker(D)\cap B_v$. Decompose G into homogeneous components and let $G:=G_1+G_2$ where $G_2\in B_v^-$ and $G_1\in A_v$. Then

$$0=D(G)=D(G_1)+D(G_2)$$

hence $D(G_1)=0$ and $D(G_2)=0$. By hypothesis $G_2\in k[F]\cap B_v^-\subseteq k[F,F_v]\cap B_v$. Furthermore

$$\begin{aligned}G_1\in\ & ker(D)\cap A_v\\ =\ & \Big(\textstyle\bigoplus_{\alpha\in J}k\cdot F^\alpha\Big)\oplus\Big(\bigoplus_{f\in\{F_v\}}k\cdot f\Big)\\ =\ & k[F]\cap A_v\oplus k[F_v]\cap A_v\\ =\ & k[F,F_v]\cap A_v\\ \subseteq\ & k[F,F_v]\cap B_v\end{aligned}$$

thus

$$G=G_1+G_2\in k[F,F_v]\cap B_v.$$

Proof of (2)(a): We know

$$k[F,F_v]\cap A_v=\Big(\bigoplus_{\alpha\in J}k\cdot F^\alpha\Big)\oplus\Big(\bigoplus_{f\in\{F_v\}}k\cdot f\Big).$$

So $F_{v,i}$ is independent of the other terms and hence

$$\begin{aligned} F_{v,i} \notin \Big(\bigoplus_{\alpha \in J} k \cdot F^{\alpha}\Big) \oplus \Big(\bigoplus_{F_{v,i} \neq f \in \{F_v\}} k \cdot f\Big) \\ = \quad k[F] \cap A_v \oplus k[\hat{F}_{v,i}] \cap A_v \\ = \quad k[F, \hat{F}_{v,i}] \cap A_v. \end{aligned}$$

Since $F_{v,i} \notin k[F, \hat{F}_{v,i}] \cap A_v$ and $F_{v,i} \in A_v$ we have $F_{v,i} \notin k[F, \hat{F}_{v,i}]$.
Proof of (2)(b): Suppose $F_i \in k[\hat{F}_i, F_v]$. Then there is a polynomial $P(\hat{F}_i, F_v)$ which equals F_i. Let $w = grad(F_i)$. Then $w < v$. Comparing degrees in the equation $F_i = P(\hat{F}_i, F_v)$ gives us that P is in fact a polynomial in the $\{\hat{F}_i\}$ since the $\{F_v\}$ have too high degree. But by hypothesis $F_i \notin k[\hat{F}_i]$. Contradiction, hence $F_i \notin k[\hat{F}_i, F_v]$.
So now (1), (2)(a), (2)(b) all hold. These are the exact requirements for $\{F, F_v\}$ to be a good set for v, which was what we needed to prove. □

Remark 5.9. If one wants to check if one has all generators of the kernel there is an easy method to do that using the algorithm in [Essen]. (Put all generators found in the algebra R_0 and check if $R_0 = R_1$, where R_0 and R_1 are as in [Essen]). More about this in the second part of section 7.

6 Applying the algorithm to non-homogeneous derivations

In this section we describe how the algorithm can easily be used on any derivation by making it homogeneous. Let $D = \sum_{i=1}^{p} a_i \partial_i$ be a derivation on A. Introduce one new variable Z and extend D to the Laurent polynomial ring $A[Z, Z^{-1}]$ by defining $D(Z) = 0$. Let $\varphi : A \longrightarrow A[Z, Z^{-1}]$ be the homogenization map sending $f(X_1, \ldots, X_p) \in A$ to $f(X_1/Z, \ldots, X_p/Z)$. By π we denote the substitution homomorphism $A[Z, Z^{-1}] \longrightarrow A$ sending Z to 1. On A we consider the "usual" grading "deg" defined by $deg(X^{\alpha}) = \alpha_1 + \ldots + \alpha_p$. For $0 \neq g \in A$ we put $g^* := Z^{deg(g)} \varphi(g) \in A[Z]$. Obviously $\pi(g^*) = g$. Furthermore one easily verifies that

$$(*) \quad \partial_i(\varphi(g)) = \frac{1}{Z} \varphi(\partial_i g) \text{ for all } g \in A.$$

On $A[Z]$ we define the *homogenization* $\widetilde{D}$ of D by $\widetilde{D} := \sum_{i=1}^{p} Z^d \varphi(a_i) \partial_i$ where $d = max(deg(a_1), \ldots, deg(a_p))$.

Lemma 6.1. $\pi(ker(\widetilde{D})) = ker(D)$

Proof. ($\supseteq$:) Let $g \in ker(D)$. Then $\sum a_i \partial_i(g) = 0$, so by $(*)$ $\sum \varphi(a_i) Z \partial_i(\varphi(g)) = 0$ i.e. $\widetilde{D}(\varphi(g)) = 0$. So $\widetilde{D}(g^*) = 0$. Since $g = \pi(g^*)$ we get $g \in \pi(ker(\widetilde{D}))$. So $\pi(ker(\widetilde{D})) \supseteq ker(D)$.
($\subseteq$:) Let $h \in ker(\widetilde{D})$. Then $Z^d \sum \varphi(a_i) \partial_i(h) = 0$. Applying π gives $\sum a_i \partial_i(\pi(h)) = 0$ i.e. $\pi(h) \in ker(D)$. So $\pi(ker(\widetilde{D})) \subseteq ker(D)$. □

Now one can easily verify that $\widetilde{D}$ matches the requirements of the algorithm, using the "usual" grading $grad := deg$ on $A[Z]$ as the needed "combined grading". Hence we can find generators for $ker(D)$ by calculating generators for $ker(\widetilde{D})$.

Remark: Perhaps a flaw in this extension is that the algorithm can not compute a minimal set of generators. Perhaps under some extreme conditions $ker(\widetilde{D})$ could be not finitely generated while $ker(D)$ is.

7 Example of the algorithm and efficiency.

Let us consider the derivation on $An := k[X_1, \ldots, X_n]$ given by

$$D_n := X_{n-1}\partial_{X_n} + X_{n-2}\partial_{X_{n-1}} + \ldots + X_1\partial_{X_2}.$$

We can easily construct a D_n-invariant and a D_n-decreasing grading on An and combine them in a grading $grad$ defined by

$$grad(X^\alpha) = (< p, \alpha >, < q, \alpha >)$$

where $p = (1, \ldots, 1)$ and $q = (0, 1, \ldots, n-2, n-1)$. We are going to consider this derivation for $n = 5$ and write $A := A5$ for notational reasons. Also we denote A_v as the collection of all polynomials of $grad(F) = v$, and $\{F_v\}$ means the set of generators of degree equal to v. Also $\{F_v^-\}$ is the set of generators of degree smaller than v. Easy to check is that $A_{(n,m)}$ is finite dimensional over k for all n, m, hence the algorithm will work on this derivation with this grading. Suppose we already know that $\{F_{(1,0)}\} = \{X_1\}$ and that $\{F_{(0,0)}\} = \{F_{(2,0)}\} = \{F_{(0,1)}\} = \{F_{(1,1)}\} = \{F_{(2,1)}\} = \{F_{(0,2)}\} = \{F_{(1,2)}\} = \{\}$. (This is easily deduced.) Now we want to find a good set for the vector $(2, 2)$ using the technique described in the proof of lemma 5.6. Easy to see is that $A_{(2,2)} = kX_3X_1 + kX_2^2$, $A_{(2,1)} = kX_3$. Furthermore $D_v(A_{(2,2)}) \subseteq A_{(2,1)}$ so the linear map $D_v : A_{(2,2)} \longrightarrow A_{(2,1)}$ needs to be considered. The kernel of this map is, as one easily sees, a linear space L generated by $X_3X_1 - \frac{1}{2}X_2^2$. The generating set for $(2, 2)^-$ is $\{F^-_{(2,2)}\} = \{t\}$. So we need to check if there are elements of L in $k[F^-_{(2,2)}]$, hence we need to check if there are elements of L in $k[F^-_{(2,2)}] \cap A_{(2,2)} = \{0\}$. Hence we get $dim(L) - dim(\{0\}) = 1$ new generator(s). So $\{F_{(2,2)}\} = \{X_3X_1 - \frac{1}{2}X_2^2\}$.

Now about efficiency. All calculations are done on a SUN ENTERPRISE 4000 (Ultrasparc 170 MHz) using the MAGMA computer algebra system. The algorithm calculates within 22 seconds the generators up to grad (10,10). These are all generators, as can be checked by the method in remark 5.9 within 2 seconds. [1] If one uses the algorithm in [Essen] then one has to wait for 3902 seconds (65 minutes) until the answer is given! This is an incredible decrease of 99.3 % !!

[1] This is not always this extremely fast: but anyway a lot faster than only applying the ESSEN-algorithm.

8 Minimality of the generators

Assume that we have $\{F_1, \ldots, F_p\}$ given by the algorithm in section 5 as generators of $ker(D)$. (So we have used the algorithm and concluded in some way that they generate the complete kernel, for example by remark 5.9.)

Theorem 8.1. *The algorithm given in section 5 gives* minimal *generators in the sense that if $k[F_1, \ldots, F_p] = k[G_1, \ldots, G_q]$ for some G_i then we must have $q \geq p$.*

Proof. We may assume that $G_1(0) = \ldots = G_q(0) = 0$ by replacing '$G_i(X)$' by '$G_i(X) - G_i(0)$' if necessary. Let $\mathfrak{m} := (F_1, \ldots, F_n)$. $k[F_1, \ldots, F_p]/\mathfrak{m}$ is isomorphic to the field k, and the F_i are homogeneous; hence $\mathfrak{m}$ is a homogeneous maximal ideal. Since $G_i \in k[F_1, \ldots, F_p]$ we have $G_i = P(F_1, \ldots, F_p) + c$ for some $c \in k$ and some polynomial $P(T) \in k[T_1, \ldots, T_p]$ having no constant term. But since $F_j(0) = 0$ all j and $G_i(0) = 0$ we have $c = 0$. Hence $G_i \in \mathfrak{m}$, so $\mathfrak{m} \supset (G_1, \ldots, G_q)$. In the same way we can also prove $(G_1, \ldots, G_q) \supset \mathfrak{m}$ hence $\mathfrak{m} = (G_1, \ldots, G_q)$.
Now consider $\mathfrak{m}/\mathfrak{m}^2$. This is a k-vector space. It is generated by the $\bar{F}_i := F_i \mod \mathfrak{m}$; namely if $g \in \mathfrak{m}$, then

$$g = P(F_1, \ldots, F_d) = \lambda_1 F_1 + \ldots + \lambda_d F_d + \sum_{|\beta| \geq 2} \lambda_\beta F^\beta. \;\; \lambda_i, \lambda_\beta \in k$$

Since each F^β with $|\beta| \geq 2$ belongs to $\mathfrak{m}^2$ we get $\bar{g} = \sum \lambda_i \bar{F}_i$.
Now we claim that these generators $\bar{F}_i$ also form a basis; suppose

$$\bar{F}_i = \lambda_1 \bar{F}_1 + \ldots + \lambda_{i-1} \bar{F}_{i-1} + \lambda_{i+1} \bar{F}_{i+1} + \ldots + \lambda_p \bar{F}_p.$$

Then

$$F_i = \lambda_1 F_1 + \ldots + \lambda_{i-1} F_{i-1} + \lambda_{i+1} F_{i+1} + \ldots + \lambda_p F_p + \sum \lambda_\beta F^\beta.$$

Let us take the homogeneous part of $grad(F_i)$ in this equation. Since all F_j are homogeneous of nonzero degree themselves we get an expression of F_i in the other F_j's which satisfy $grad(F_j) \leq grad(F_i)$. But this is in contradiction with the assumption that the F_i's are found by the algorithm ,which means that they should satisfy the properties of a "good set". Hence the $\bar{F}_i$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$; thus $dim(\mathfrak{m}/\mathfrak{m}^2) = p$. Now since $(G_1, \ldots, G_q) = \mathfrak{m}$ the $\bar{G}_i$ generate the vector space $\mathfrak{m}/\mathfrak{m}^2$. Since $dim(\mathfrak{m}/\mathfrak{m}^2) = p$ we need at least p generators. Hence q should be larger or equal to p. ☐

9 Acknowledgements

The author has been assisted in writing the paper by several persons. He would like to thank:
Peter van Rossum, for programming the algorithm and for some very stimulating discussions;
Arno van den Essen, for pointing out the general case which has become section 6,

and of course for doing a lot of corrective work;
Thank you very much!

References:

[Daigle,Freudenburg] D.Daigle and G.Freudenburg, A counterexample to Hilbert's Fourteenth problem in dimension five, preprint 1999.

[Derksen] H.Derksen, More on the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$, preprint 1995.

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

[Essen] A. van den Essen, An algorithm to compute the invariant ring of a G_a-action on an affine variety, J. Symb. Comp.; 1993, 16, 551-555.

[Freudenburg] G. Freudenburg, A counterexample to Hilbert's Fourteenth Problem in dimension six, preprint 1998.

[Makar-Limanov], On the hypersurface $x + x^2y + z^2 + t^3 = 0$ in $\mathbb{C}^4$, to appear in Israel J. of Math.

[Maubach1] S.Maubach, Triangular monomial derivations on $k[X_1, X_2, X_3, X_4]$ have kernel generated by at most four elements, Report No.9822 (Oct. 1998) Dep. of math. Univ. of Nijmegen

[Maubach2] S.Maubach, Hilbert 14 and related subjects, master thesis, 1998, Dep. of math. Univ. of Nijmegen

[Nowicki] A.Nowicki, Polynomial derivations and their ring of constants, Univ.Mikol. Kopern. Toruń, 1994, ISBN 83-231-0543-X

[Tan] L.Tan, An algorithm for explicit generators of the invariants of the basic G_a-actions. Comm. in Algebra 17(3), 1989, 565-572.