COLLOQUIUM MATHEMATICUM

VOL. 122 2011 NO. 1

AN ALGORITHM FOR COMPUTING THE KERNEL OF A LOCALLY FINITE HIGHER DERIVATION UP TO A CERTAIN DEGREE

BY

YUKI ITO and HIDEO KOJIMA (Niigata)

Abstract. This paper gives an algorithm for computing the kernel of a locally finite higher derivation on the polynomial ring $k[x_1, \ldots, x_n]$ up to a given bound.

1. Introduction. Derivations and their kernels play an important role in mathematics. See [8], [3], [1], [4] for excellent accounts. To study the kernel of a derivation, it is important to find generators of the kernel. There are several techniques to compute them. We recall some results. Van den Essen [2] gave an important algorithm which computes all generators of the kernel of a locally nilpotent derivation on a finitely generated k-algebra provided k is a field of characteristic zero and the kernel is finitely generated as a k-algebra. Later on, Maubach [5] gave an algorithm which computes generators of the kernel of a (not necessarily locally nilpotent) k-derivation on a polynomial ring $k[x_1, \ldots, x_n]$ up to a certain degree provided k is a field of characteristic zero. We note that, if k is a field of positive characteristic, then the kernel of a k-derivation on a finitely generated k-algebra is finitely generated (cf. [9, Proposition 4.1]). In this case, Okuda [10] gave an algorithm which computes the kernel.

In positive characteristic, locally finite higher derivations and the study of their kernels (for the definitions, see Section 2) play an important role. For example, the additive group scheme action on an affine algebraic variety $X = \mathrm{Spec}(A)$ defined over an algebraically closed field k can be interpreted in terms of a locally finite iterative higher derivation on the coordinate ring A of X. Recently, the kernels of locally finite iterative higher derivations have been studied by several authors. For example, Okuda [10] gave generators for the kernel of a locally finite iterative higher derivation with a slice, where a *slice* of a locally finite iterative higher derivation $\{D_n\}_{n\geq 0}$ is an element $s \in A$ such that $D_1(s) = 1$ and $D_i(s) = 0$ for every $i \geq 2$. Later on, by generalizing van den Essen's algorithm in [2], Tanimoto [11] gave an algorithm

2010 *Mathematics Subject Classification*: Primary 13N15; Secondary 13A50.
Key words and phrases: higher derivation, locally finite higher derivation

DOI: 10.4064/cm122-1-3

for computing the kernel of a locally finite iterative higher derivation provided the kernel is finitely generated. The outline of Tanimoto's algorithm is almost the same as van den Essen's, and heavily depends on Gröbner bases computations.

In this paper, we give an algorithm for computing generators of the kernel of a (not necessarily iterative) locally finite higher derivation up to a certain degree. In Section 2, we recall some elementary results on locally finite higher derivations and their kernels. Moreover, for a locally finite higher derivation D, we explain the concept of D-grading, which is a word-for-word translation of that in [5, Section 3]. In Section 3, we give an algorithm computing the kernel of a "w-homogeneous" locally finite higher derivation. In Section 4, we show how to extend the algorithm of Section 3 to all locally finite higher derivations. The outline of the algorithm mimics Maubach's algorithm in [5].

2. Preliminary results. Let k be a field of characteristic $p \geq 0$ and let A be a k-algebra.

DEFINITION 2.1. A *locally finite higher derivation* (abbreviated as an *lfhd*) on A is a set of k-linear endomorphisms $D = \{D_n\}_{n \geq 0}$ of A satisfying the following conditions:

(1) D_0 is the identity map of A.
(2) For any $a, b \in A$ and for any integer $n \geq 0$,
$$D_n(ab) = \sum_{i+j=n} D_i(a)D_j(b).$$
(3) For any $a \in A$, there exists an integer $n \geq 0$ such that $D_m(a) = 0$ for every integer $m \geq n$.

An lfhd $D = \{D_n\}_{n \geq 0}$ on A is said to be *iterative* if it satisfies the following additional condition:

(4) For any $i, j \geq 0$,
$$D_i \circ D_j = \binom{i+j}{i} D_{i+j}.$$

A locally finite iterative higher derivation is abbreviated as an lfihd.

The following lemma is clear from the definition of locally finite higher derivations (cf. [7, Lemma I.1.2 (p. 15)]).

LEMMA 2.2. *Let $D = \{D_n\}_{n \geq 0}$ be a set of endomorphisms of A, where D_0 is the identity map. Then the following conditions are equivalent to each other:*

(1) *D is an lfhd on A.*

(2) *The mapping* $\varphi_D : A \to A[[t]]$, *where* $A[[t]]$ *is the formal power series ring in one variable* t *over* A, *given by* $\varphi_D(a) = \sum_{i\geq 0} D_i(a)t^i$, *is a homomorphism of* k*-algebras and* $\operatorname{Im}\varphi_D \subset A[t]$, *where* $A[t]$ *is the polynomial ring in one variable* t *over* A.

We call the mapping φ_D *as in* (2) *the homomorphism associated to an lfhd* D.

We now define the kernel of an lfhd. For an lfhd $D = \{D_n\}_{n\geq 0}$ on A, we define $A^D := \{a \in A \mid D_n(a) = 0 \text{ for every } n > 0\}$. It is clear that A^D is a k-subalgebra of A. We call it the *kernel* of D. We note that, for an element $a \in A$, $a \in A^D$ if and only if $\varphi_D(a) = a$, where φ_D is the homomorphism associated to D (cf. Lemma 2.2).

We shall give the concept of D-grading which is a word-for-word translation of that in [5, Section 3], where Maubach defines a D-grading for a k-derivation D. From now on, we assume that $A = k[x_1, \ldots, x_n]$ is a polynomial ring in n variables over k. We denote the set of all non-negative integers by $\mathbb{Z}_{\geq 0}$. Let $w \in (\mathbb{Z}_{\geq 0})^n$ be a non-zero vector. Then we can define a function on monomials $X^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ on A by

$$\deg(X^\alpha) = \langle \alpha, w \rangle,$$

where $\alpha = (\alpha_1, \ldots, \alpha_n)$ is a vector of $(\mathbb{Z}_{\geq 0})^n$ and $\langle \, , \rangle$ is the usual inner product. By using the degree function deg, we define

$$A_m := \operatorname{span}_k\{X^\alpha \mid \deg(X^\alpha) = m\}.$$

Then $A = \bigoplus_{n\geq 0} A_n$ is a well-defined grading. We can extend the degree function deg on elements of A_n: if $0 \neq F \in A_n$, then we define $\deg(F) = n$.

Definition 2.3. Assume that A has a well-defined grading $A = \bigoplus_n A_n$ given by a function deg coming from a w-grading. Let $D = \{D_n\}_{n\geq 0}$ be an lfhd on A. Then D is said to be *homogeneous* of degree m with respect to the grading if, for all non-negative integers v, i and for all $F \in A_v$, we have $D_i(F) \in A_{v-im}$. Conversely, if D is homogeneous of degree m with respect to the grading, then the grading is said to be a D*-homogeneous grading* of degree m.

We recall the notion of a combined grading given in [5, Section 3].

Definition 2.4. Let q be a positive integer and let $w_1, \ldots, w_q \in (\mathbb{Z}_{\geq 0})^n$. Then the associated $(\mathbb{Z}_{\geq 0})^q$-grading "grad" on A is defined by

$$\operatorname{grad}(X^\alpha) := (\langle \alpha, w_1 \rangle, \ldots, \langle \alpha, w_q \rangle).$$

Such a grading is called a *combined grading* if each $\deg_{w_i}$ is a D-homogeneous grading of degree m_i. In this case, the lfhd D is said to be homogeneous of degree $\overline{m} = (m_1, \ldots, m_q)$ with respect to grad.

3. Homogeneous kernel algorithm. In this section, we describe an algorithm computing a minimal set of generators of the kernel of a homogeneous lfhd. The outline of this algorithm mimics Maubach's algorithm in [5, Section 5]. In fact, all the definitions, assumptions and lemmas in this section are word-for-word translations of those in [5, Section 5]. Moreover, all the lemmas in this section can be proved by using the same arguments as in [5, Section 5]. For the reader's convenience, we reproduce the proofs.

Definition 3.1. Let q be a positive integer and let $v = (v_1, \dots, v_q)$ and $w = (w_1, \dots, w_q)$ be elements of $(\mathbb{Z}_{\geq 0})^q$. We write $w \leq v$ if $w_i \leq v_i$ for any $i = 1, \dots, q$. We also write $w < v$ if $w \leq v$ and $w \neq v$.

Now, let k be a field of characteristic $p \geq 0$, $A = k[x_1, \dots, x_n]$ the polynomial ring in n variables over k, and $D = \{D_n\}_{n \geq 0}$ an lfhd on A.

Assumptions. In this section, we assume that the ring A has a grading such that

$$A = \bigoplus_{v \in (\mathbb{Z}_{\geq 0})^q} A_v$$

and

$$\dim_k A_v < \infty$$

for any $v \in (\mathbb{Z}_{\geq 0})^q$ and that D is homogeneous of degree $\overline{m} = (m_1, \dots, m_q)$ with respect to this grading.

Definition 3.2. For $v \in (\mathbb{Z}_{\geq 0})^q$, we set

$$B_v := \bigoplus_{w \leq v} A_w \quad \text{and} \quad B_v^- := \bigoplus_{w < v} A_w.$$

Definition 3.3. We fix $v \in (\mathbb{Z}_{\geq 0})^q$. For a finite set $\mathcal{F} := \{F_1, \dots, F_s\} \subset A$, we set $k[\mathcal{F}] := k[F_1, \dots, F_s]$, the k-subalgebra of A generated by $F_1, \dots, F_s$. For each $i = 1, \dots, s$, we set $\mathcal{F}_i := \mathcal{F} \setminus \{F_i\}$.

(1) A finite set $\mathcal{F} = \{F_1, \dots, F_s\} \subset B_v$ is called *good for* $v \in (\mathbb{Z}_{\geq 0})^q$ if:
- each F_i belongs to A_w for some $w \leq v$;
- $k[\mathcal{F}] \cap B_v = A^D \cap B_v$;
- for any i $(1 \leq i \leq s)$, $F_i \notin k[\mathcal{F}_i]$.

(2) A finite set $\mathcal{F} = \{F_1, \dots, F_s\} \subset B_v^-$ is called *good for* v^- if:
- each F_i belongs to A_w for some $w < v$;
- $k[\mathcal{F}] \cap B_v^- = A^D \cap B_v^-$;
- for any i $(1 \leq i \leq s)$, $F_i \notin k[\mathcal{F}_i]$.

For any $v \in (\mathbb{Z}_{\geq 0})^q$ and $n \geq 0$, we denote the restriction of D_n to A_v by $D_n|_v$. Note that $D_n|_v$ is a k-linear map from A_v to $A_{v - n\overline{m}}$ for any $v \in (\mathbb{Z}_{\geq 0})^q$ and $n \geq 0$.

LEMMA 3.4. *For any $v \in (\mathbb{Z}_{\geq 0})^q$, there exists a positive integer M such that*

$$A^D \cap A_v = \bigcap_{i\geq 1} \ker(D_i|_v) = \bigcap_{i\geq 1}^{M} \ker(D_i|_v).$$

Proof. Since A_v is a finite-dimensional k-vector space, there exists a positive integer M such that $D_j|_v = 0$ for any $j > M$. Then

$$\bigcap_{i\geq 1} \ker(D_i|_v) = \bigcap_{i\geq 1}^{M} \ker(D_i|_v).$$

We now prove the first equality in the statement. If $G \in A^D \cap A_v$, then $G \in A_v$ and $D_i|_v(G) = D_i(G) = 0$ for any $i \geq 1$. Hence $G \in \bigcap_{i\geq 1} \ker(D_i|_v)$. Conversely, if $G \in \bigcap_{i\geq 1} \ker(D_i|_v)$, then $G \in A_v$ and $D_i(G) = D_i|_v(G) = 0$ for any $i \geq 1$. Hence, $G \in A^D \cap A_v$. ∎

LEMMA 3.5. *Let $v \in (\mathbb{Z}_{\geq 0})^q$. Assume that we have finite sets $\mathcal{F}_w \subset A_w$ for all $w < v$ such that, for any $u < v$, $\bigcup_{w\leq u} \mathcal{F}_w$ is a good set for u. Then $\bigcup_{w<v} \mathcal{F}_w$ is good for v^-.*

Proof. Set $\mathcal{F} := \bigcup_{w<v} \mathcal{F}_w$. It suffices to prove the following:

(i) $k[\mathcal{F}] \cap B_v^- = A^D \cap B_v^-$.
(ii) If $F_i \in \mathcal{F}$, then $F_i \notin k[\mathcal{F}_i]$, where $\mathcal{F}_i = \mathcal{F} \setminus \{F_i\}$ (cf. Definition 3.3).

We first prove (i). By the hypothesis, for any $u < v$, we have $k[\mathcal{F}] \cap B_u = A^D \cap B_u \subset A^D \cap B_v^-$. So, $k[\mathcal{F}] \cap B_v^- \subseteq A^D \cap B_v^-$. Conversely, let $G \in A^D \cap B_v^-$. Split G into homogeneous parts $G = \sum_h G_h$. For any positive integer i, $0 = D_i(G) = D_i(\sum_h G_h) = \sum_h D_i(G_h)$. Since $D_i(G_h) \in A_{h-i\overline{m}}$, we have $D_i(G_h) = 0$ for any $i > 0$. So, $G_h \in A^D$ for any h. Since $\operatorname{grad}(G_h) = h$ $(< v)$, we have $G_h \in k[\mathcal{F}]$ for any h. Thus, $G = \sum_h G_h \in k[\mathcal{F}]$. Hence, $k[\mathcal{F}] \cap B_v^- \supseteq A^D \cap B_v^-$.

We now prove (ii). Let $F_i \in \mathcal{F}$. Then F_i is homogeneous and $\operatorname{grad}(F_i) < v$. Set $u := \operatorname{grad}(F_i)$ and $\tilde{\mathcal{F}} := \bigcup_{w\leq u} F_w$. Then $F_i \in \mathcal{F} \cap B_u = \tilde{\mathcal{F}}$. Suppose that $F_i \in k[\mathcal{F}_i]$. Since $F_i \in B_u$, we have $F_i \in k[\mathcal{F}_i] \cap B_u$. Then $F_i \in k[\tilde{\mathcal{F}} \setminus \{F_i\}]$, which is a contradiction because $\tilde{\mathcal{F}}$ is a good set for u. ∎

LEMMA 3.6. *The empty set is good for $v = (0,\dots,0)$. Namely, $A_{(0,\dots,0)} = k$.*

Proof. It is clear that $k \subset A_{(0,\dots,0)}$. Assume that there exists an element $a \in A_{(0,\dots,0)} \setminus k$. Then $\{a, a^2, a^3, \dots\}$ is a k-linearly independent subset of $A_{(0,\dots,0)}$. This is a contradiction because $A_{(0,\dots,0)}$ is finite-dimensional. ∎

LEMMA 3.7. *Let $v \in (\mathbb{Z}_{\geq 0})^q$. Suppose that we have finite sets $\mathcal{F}_w \subset A_w$ for all $w < v$ such that $\bigcup_{w<v} \mathcal{F}_w$ is a good set for v^-. Then we can construct a finite set $\mathcal{F}_v \subset A_v$ such that $\bigcup_{w\leq v} \mathcal{F}_w$ is a good set for v.*

Proof. Set $\mathcal{F} := \bigcup_{w<v} \mathcal{F}_w$. Since $\dim_k A_v < \infty$, $k[\mathcal{F}] \cap A_v$ is a finite-dimensional k-vector space. Set $s := \#\mathcal{F}$ and $I := \{\alpha = (\alpha_1, \dots, \alpha_s) \in (\mathbb{Z}_{\geq 0})^s \mid \mathcal{F}^\alpha := F_1^{\alpha_1} \cdots F_s^{\alpha_s} \in A_v\}$, where we write $\mathcal{F}$ as $\mathcal{F} = \{F_1, \dots, F_s\}$. Then

$$k[\mathcal{F}] \cap A_v = \sum_{\alpha \in I} k\mathcal{F}^\alpha,$$

so $\{\mathcal{F}^\alpha\}_{\alpha \in I}$ is a generating set of $k[\mathcal{F}] \cap A_v$. As I is a finite set, we can take (and calculate) a subset J of I such that $\{\mathcal{F}_\alpha\}_{\alpha \in J}$ is a k-basis of $k[\mathcal{F}] \cap A_v$. Then $\dim_k(k[\mathcal{F}] \cap A_v) = \#J$. Now we compute $\bigcap_{i \geq 1} \ker(D_i|_v)$, which is a k-subspace of A_v because every $D_i|_v$ is a k-linear map from A_v to $A_{v-i\overline{m}}$. Since $k[\mathcal{F}] \cap A_v$ is a k-subspace of $A^D \cap A_v = \bigcap_{i \geq 1} \ker(D_i|_v)$, $\{\mathcal{F}^\alpha\}_{\alpha \in J}$ are independent elements in $\bigcap_{i \geq 1} \ker(D_i|_v)$. We can take a finite set $\mathcal{F}_v = \{G_1, \dots, G_t\}$ for which $\{\mathcal{F}^\alpha\}_{\alpha \in J} \cup \mathcal{F}_v$ forms a k-basis of $\bigcap_{i \geq 1} \ker(D_i|_v)$. Then

$$\bigcap_{i \geq 1} \ker(D_i|_v) = \Big(\bigoplus_{\alpha \in J} k\mathcal{F}^\alpha\Big) \oplus \Big(\bigoplus_{i=1}^{t} kG_i\Big). \tag{3.1}$$

Here we note that $t = \#\mathcal{F}_v = \dim_k(\bigcap_{i \geq 1} \ker(D_i|_v)) - \dim_k(k[\mathcal{F}] \cap A_v)$ and $\mathcal{F}_v \subset A_v$. Now, for i $(1 \leq i \leq t)$, we set $\mathcal{F}_{v,i} := \mathcal{F}_v \setminus \{G_i\}$. We prove the following claim.

Claim. *The set $\mathcal{F} \cup \mathcal{F}_v = \bigcup_{w \leq v} \mathcal{F}_w$ is good for v, namely:*

(1) $A^D \cap B_v = k[\mathcal{F} \cup \mathcal{F}_v] \cap B_v$.
(2) (a) $G_i \notin k[\mathcal{F} \cup \mathcal{F}_{v,i}]$ *for any* i $(1 \leq i \leq t)$ *and* (b) $F_i \notin k[\mathcal{F}_i \cup \mathcal{F}_v]$ *for any* i $(1 \leq i \leq s)$.

Proof. (1) The "$\supseteq$" part is clear since $k[\mathcal{F} \cup \mathcal{F}_v] \subset A^D$. To prove "$\subseteq$", let $H \in A^D \cap B_v$. We decompose H into homogeneous components and set $H := H_1 + H_2$, where $H_2 \in B_v^-$ and $H_1 \in A_v$. For any $i \geq 1$, $0 = D_i(H) = D_i(H_1) + D_i(H_2)$. Since $D_i(H_1) \in A_{v-i\overline{m}}$ and $D_i(H_2) \in B^-_{v-i\overline{m}}$, we have $D_i(H_1) = D_i(H_2) = 0$. As $\mathcal{F}$ is good for v^-, $H_2 \in k[\mathcal{F}] \cap B_v^- \subset k[\mathcal{F} \cup \mathcal{F}_v] \cap B_v$. We infer from (3.1) that

$$\begin{aligned}
H_1 &\in A^D \cap A_v \ \Big(= \bigcap_{i \geq 1} \ker(D_i|_v)\Big) \\
&= \Big(\bigoplus_{\alpha \in J} k\mathcal{F}^\alpha\Big) \oplus \Big(\bigoplus_{i=1}^{t} kG_i\Big) \\
&= (k[\mathcal{F}] \cap A_v) \oplus (k[\mathcal{F}_v] \cap A_v) \\
&= k[\mathcal{F} \cup \mathcal{F}_v] \cap A_v \\
&\subset k[\mathcal{F} \cup \mathcal{F}_v] \cap B_v.
\end{aligned}$$

Therefore, $H = H_1 + H_2 \in k[\mathcal{F} \cup \mathcal{F}_v] \cap B_v$.

(2) We prove (a). From the proof of (1), we have

$$k[\mathcal{F} \cup \mathcal{F}_v] \cap A_v = \Big(\bigoplus_{\alpha \in J} k\mathcal{F}^\alpha\Big) \oplus \Big(\bigoplus_{i=1}^{t} kG_i\Big).$$

Since $\{\mathcal{F}^\alpha\}_{\alpha \in J} \cup \mathcal{F}_v$ is a k-basis of $\bigcap_{i \geq 1} \ker(D_i|_v) = k[\mathcal{F} \cup \mathcal{F}_v] \cap A_v$, we have $G_i \notin (\bigoplus_{\alpha \in J} k\mathcal{F}^\alpha) \oplus (\bigoplus_{j \neq i} kG_j)$. Hence, for any i $(1 \leq i \leq t)$,

$$\begin{aligned} G_i \notin & \Big(\bigoplus_{\alpha \in J} k\mathcal{F}^\alpha\Big) \oplus \Big(\bigoplus_{j \neq i} kG_j\Big) \\ &= k[\mathcal{F}] \cap A_v \oplus k[\mathcal{F}_{v,i}] \cap A_v = k[\mathcal{F} \cup \mathcal{F}_{v,i}] \cap A_v. \end{aligned}$$

Since $G_i \in A_v$, we have $G_i \notin k[\mathcal{F} \cup \mathcal{F}_{v,i}]$.

To prove (b), suppose to the contrary that $F_i \in k[\mathcal{F}_i \cup \mathcal{F}_v]$ for some i $(1 \leq i \leq s)$. Then there exists a polynomial P of $(s-1)+t$ variables over k satisfying $P(\mathcal{F}_i \cup \mathcal{F}_v) = P(F_1, \ldots, F_{i-1}, F_{i+1}, \ldots, F_s, G_1, \ldots, G_t) = F_i$. Set $w := \operatorname{grad}(F_i)$. Then $w < v$. Comparing degrees in the equation $F_i = P(\mathcal{F}_i \cup \mathcal{F}_v)$ shows that P is a polynomial in the $\mathcal{F}_i$ because $\operatorname{grad}(G_j) > w$ for any j, $1 \leq j \leq t$. Then $F_i \in k[\mathcal{F}_i]$, which is a contradiction. ∎

The proof of Lemma 3.7 is thus completed. ∎

By the above lemmas, we obtain the following algorithm for computing generators of the kernel of a homogeneous lfhd up to a certain degree.

Homogeneous Kernel Algorithm

Input:

- $\{x_1, \ldots, x_n\}$: the generators of the polynomial ring A in n variables over k.
- $A := \bigoplus_{v \in (\mathbb{Z}_{\geq 0})^q} A_v$: a combined grading of A denoted by grad, which satisfies the above assumptions.
- D: a homogeneous lfhd on A of degree $\overline{m}$ with respect to the grading.
- $b \in (\mathbb{Z}_{\geq 0})^q$: the degree indicating 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.

By using the same argument as in the proof of [5, Theorem 8.1], we obtain the following result.

Proposition 3.8. *Assume that the preceding algorithm produces the set $\mathcal{F} = \{F_1, \ldots, F_s\}$ which is good for b and that $A^D = k[\mathcal{F}]$. If A^D is expressed as $A^D = k[G_1, \ldots, G_t]$ for some G_i, then $s \leq t$.*

We give an example.

EXAMPLE 3.9. Let k be a field of characteristic $p \neq 2$ and $A = k[x, y, z]$. Let $\varphi : A \to A[t]$ be the k-algebra homomorphism given by

$$\varphi(x) = x + yt + \frac{z}{2}t^2, \quad \varphi(y) = y + zt, \quad \varphi(z) = z.$$

By Lemma 2.2, we have an lfhd $D = \{D_n\}_{n\geq 0}$ such that $\varphi_D = \varphi$. The lfhd D is homogeneous of degree 0 with respect to the usual grading. Now we find a good set for $b = 2$. We use the same notation as above. We can easily see that $\mathcal{F}_0 = \emptyset$, $\mathcal{F}_1 = \{z\}$ and $A_2 \cap A^D = \mathrm{span}_k\{x^2, xy, xz, y^2, yz, z^2\} \cap \bigcap_{i=1}^4 \ker D_i$. Since D_1 can be expressed as

$$D_1 = y\frac{\partial}{\partial x} + z\frac{\partial}{\partial y},$$

it is easy to see that $A_2 \cap \ker D_1 = \mathrm{span}_k\{xz - \frac{1}{2}y^2, z^2\}$. Since $xz - \frac{1}{2}y^2, z^2 \in A^D$, we have $A_2 \cap A^D = \mathrm{span}_k\{xz - \frac{1}{2}y^2, z^2\}$. Then $\mathcal{F}_2 = \{xz - \frac{1}{2}y^2\}$ and so $\{z, xz - \frac{1}{2}y^2\}$ is a good set for $b = 2$.

4. Algorithm for a non-homogeneous lfhd. In this section, we describe an algorithm to find generators of the kernel of a non-homogeneous lfhd by making it homogeneous. The outline of this algorithm is almost the same as Maubach's algorithm in [5, Section 6].

Let k be a field and $A = k[x_1, \dots, x_n]$. On A, we consider the usual grading deg defined by $\deg(x_1^{a_1} \cdots x_n^{a_n}) = a_1 + \cdots + a_n$. Let $D = \{D_n\}_{n\geq 0}$ be an lfhd on A and let $\varphi_D : A \to A[t]$ be the homomorphism associated to D (cf. Lemma 2.2). Then there exists a positive integer M such that $D_j(x_i) = 0$ for any i $(1 \leq i \leq n)$ and $j > M$. Then we define integers $\{N_j\}_{j\geq 1}$ satisfying the following conditions:

$$N_1 \geq \max_{1\leq j\leq M}\left\{\max_{1\leq i\leq n} \frac{\deg(D_j(x_i)) + j - 1}{j}\right\},$$
$$N_j = jN_1 - (j-1) = j(N_1 - 1) + 1 \quad (j > 1).$$

We introduce one new variable z. Let $\psi : A \to A[z, z^{-1}]$ be the homogeneization map defined by

$$\psi(f(x_1, \dots, x_n)) = f(x_1/z, \dots, x_n/z)$$

for $f(x_1, \dots, x_n) \in A$. We denote by π the substitution homomorphism $A[z] \to A$ sending z to 1.

Let $\varphi_{\tilde{D}} : A[z] \to A[z][t]$ be the k-algebra homomorphism defined by

$$\varphi_{\tilde{D}}(x_i) = x_i + \sum_{j=1}^{M} z^{N_j}\psi(D_j(x_i))t^j \quad (i = 1, \dots, n),$$
$$\varphi_{\tilde{D}}(z) = z.$$

It is then clear that $\varphi_{\tilde{D}}(f)|_{t=0} = f$ for any $f \in A[z]$. By Lemma 2.2, $\varphi_{\tilde{D}}$ defines an lfhd $\tilde{D} = \{\tilde{D}_n\}_{n\geq 0}$ on $A[z]$ such that $\varphi_{\tilde{D}}(f) = \sum_{n\geq 0} \tilde{D}_n(f)t^n$ for any $f \in A[z]$.

LEMMA 4.1. *On $A[z] = k[x_1, \ldots, x_n, z]$, consider the usual grading* deg *defined by* $\deg(x_1^{a_1} \cdots x_n^{a_n} z^b) = a_1 + \cdots + a_n + b$. *Then the lfhd $\tilde{D} = \{\tilde{D}_n\}_{n\geq 0}$ defined as above is homogeneous of degree $-(N_1 - 1)$ with respect to* deg.

Proof. For any $1 \leq i \leq n$ and $j \geq 1$, $\tilde{D}_j(x_i)$ is either the zero polynomial or a homogeneous polynomial of degree $N_j = j(N_1 - 1) + 1$. So, for any homogeneous polynomial $f \in A[z]$ and for any integer $j \geq 0$, $\tilde{D}_j(f)$ is either the zero polynomial or a homogeneous polynomial of degree $\deg f + j(N_1 - 1)$. ∎

We call the lfhd $\tilde{D}$ the *homogeneization* of D.

LEMMA 4.2 (cf. [5, Lemma 6.1]). *Let $A[z]^{\tilde{D}}$ be the kernel of the lfhd $\tilde{D}$ on $A[z]$. Then*

$$\pi(A[z]^{\tilde{D}}) = A^D.$$

Proof. Naturally, we can extend the morphism $\pi : A[z] \to A$ to a k-algebra homomorphism $\pi' : A[z][t] \to A[t]$ by setting $\pi'(t) = t$. Then we have

$$\pi'(\varphi_{\tilde{D}}(x_i)) = \pi'\Big(x_i + \sum_{j=1} z^{N_j}\psi(D_j(x_i))t^j\Big) = x_i + \sum_{j=1} D_j(x_i)t^j = \varphi_D(\pi(x_i))$$

for any $i = 1, \ldots, n$ and $\pi'(\varphi_{\tilde{D}}(z)) = \pi'(z) = 1 = \varphi_D(\pi(z))$. Hence, $\pi' \circ \varphi_{\tilde{D}} = \varphi_D \circ \pi$ as a homomorphism from $A[z]$ to $A[t]$. Let $h \in A[z]^{\tilde{D}}$. Then $\varphi_{\tilde{D}}(h) = h \in A[z]$ and so $\pi(h) = \pi'(\varphi_{\tilde{D}}(h)) = \varphi_D(\pi(h))$. Since $\pi(h) \in A$, we conclude that $\pi(h) \in A^D$. Hence, $\pi(A[z]^{\tilde{D}}) \subset A^D$.

Conversely, let $g \in A^D$. Then $\varphi_D(g) = g \in A$. Since $g = \varphi_D(g) = \varphi_D(\pi(z^{\deg g}\psi(g))) = \pi'(\varphi_{\tilde{D}}(z^{\deg g}\psi(g))) \in A$ and since $\tilde{D}_j(z^{\deg g}\psi(g))$ is homogeneous for any $j \geq 0$, we know that $\varphi_{\tilde{D}}(z^{\deg g}\psi(g)) \in A[z]$. Then $z^{\deg g}\psi(g) \in A[z]^{\tilde{D}}$ and so $g = \pi(z^{\deg g}\psi(g)) \in \pi(A[z]^{\tilde{D}})$. Hence, $A^D \subset \pi(A[z]^{\tilde{D}})$. ∎

By Lemma 4.1, $\tilde{D}$ satisfies the requirements of the algorithm of Section 3, with the usual grading deg on $A[z]$ as the combined grading. By Lemma 4.2, we can find generators for A^D by calculating those for $A[z]^{\tilde{D}}$.

EXAMPLE 4.3. Let k be a field of characteristic $p \neq 2$ and $A = k[x, y]$. Let D be an lfhd on A such that $\varphi_D(x) = x + yt + \frac{1}{2}t^2$ and $\varphi_D(y) = y + t$, where $\varphi_D : A \to A[t]$ is the homomorphism associated to D. With the same notation as above, we may set $N_j = 1$ for any integer $j \geq 1$. Then the homogeneization $\tilde{D}$ of D satisfies

$$\varphi_{\tilde{D}}(x) = x + yt + \frac{z}{2}t^2, \quad \varphi_{\tilde{D}}(y) = y + zt, \quad \varphi_{\tilde{D}}(z) = z.$$

That is, $\tilde{D}$ is the same as the lhfd D in Example 3.9. By Example 3.9, we know that $\{z, xz - \frac{1}{2}y^2\}$ is a good set fo $b = 2$ (cf. Definition 3.3). Let $A = \bigoplus_{v \in \mathbb{Z}_{\geq 0}} A_v$ be the usual grading of A. From the proof of Lemma 4.2, we get

$$k[\pi(z), \pi(xz - y^2/2)] \cap \bigoplus_{v \leq 2} A_v = k[x - y^2/2] \cap \bigoplus_{v \leq 2} A_v = A^D \cap \bigoplus_{v \leq 2} A_v.$$

5. Appendix—Kernel-check algorithm. In [6, p. 32], Maubach gives an abbreviated version of van den Essen's algorithm in [2]. He calls the algorithm the *kernel-check algorithm.* Similarly, we have an abbreviated version of Tanimoto's algorithm in [11]. The algorithm stated below is a word-for-word translation of the kernel-check algorithm.

Let R be a PID, let $A = R[a_1, \ldots, a_n]$ be a finitely generated R-algebra and let $D = \{D_n\}_{n \geq 0}$ be a non-trivial lfihd. Let $\sigma \in A$ satisfy:

(1) $\sigma \notin A^D$.
(2) $\deg_t \varphi_D(\sigma) = \min\{\deg_t(\varphi_D(f)) \mid f \in A \setminus A^D\}$.

Then σ is called a *local slice* of D (cf. [11, p. 2285]). Let c be the leading coefficient of $\varphi_D(\sigma)$ as a polynomial in one variable t. We note that $c \in A^D$ (cf. [11, Section 1]). Suppose a finite set $\{f_1, \ldots, f_m\} \subset A^D$ is given. Then the algorithm proceeds in the following two steps.

Step 1. Find generators $P_1, \ldots, P_s$ for the ideal

$$J = \{P \in R^{[m]} \mid P(f_1, \ldots, f_m) \in cA\},$$

where $R^{[m]}$ denotes the polynomial ring in m variables over R. (We can calculate generators of J by using for example the theory of Gröbner bases.)

Step 2. If $c^{-1}P_i(f_1, \ldots, f_m) \in R[f_1, \ldots, f_m]$ for each $i = 1, \ldots, s$, then the output is yes; otherwise, it is no.

Acknowledgements. The authors would like to thank Professor Ryuji Tanimoto for giving us the first version of his paper [11] and useful comments. The authors would also like to thank the referee for useful suggestions to improve the paper.

REFERENCES

[1] D. Daigle, *Locally nilpotent derivations*, Lecture Notes for the 26th Autumn School of Algebraic Geometry, Łukęcin, 2003.

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

[3] —, *Polynomial Automorphisms and the Jacobian Conjecture*, Progr. Math. 190, Birkhäuser, Basel, 2000.

[4] G. Freudenburg, *Algebraic Theory of Locally Nilpotent Derivations*, Encyclopaedia Math. Sci. 136, Springer, 2006.

[5] S. Maubach, *An algorithm to compute the kernel of a derivation up to a certain degree*, J. Symbolic Comput. 29 (2000), 959–970.

[6] —, *Polynomial endomorphisms and kernels of derivations*, Ph.D. thesis, Univ. Nijmegen, 2003.

[7] M. Miyanishi, *Lectures on Curves on Rational and Unirational Surfaces*, Tata Institute of Fundamental Research, Springer, Berlin, 1978.

[8] A. Nowicki, *Polynomial Derivations and their Rings of Constants*, Uniwersytet Mikołaja Kopernika, Toruń, 1994.

[9] A. Nowicki and M. Nagata, *Rings of constants for k-derivations in $k[x_1, \ldots, x_n]$*, J. Math. Kyoto Univ. 28 (1988), 111–118.

[10] S. Okuda, *Kernels of derivations in positive characteristic*, Hiroshima Math. J. 34 (2004), 1–19.

[11] R. Tanimoto, *An algorithm for computing the kernel of a locally finite iterative higher derivation*, J. Pure Appl. Algebra 212 (2008), 2284–2297.

Yuki Ito
Graduate School of Science and Technology
Niigata University
Niigata 950-2181, Japan

Hideo Kojima
Department of Information Engineering
Faculty of Engineering
Niigata University
Niigata 950-2181, Japan
E-mail: kojima@ie.niigata-u.ac.jp

Received 7 November 2009;
revised 23 February 2010 (5296)