Generators of rings of constants for some diagonal derivations in polynomial rings

by

Andrzej Nowicki

Institute of Mathematics, N. Copernicus University
87–100 Toruń, Poland (e-mail: anow@pltumk11.bitnet).

and

Jean – Marie Strelcyn

Département de Mathématiques, Université de Rouen,
URA CNRS 1378, B.P.118, 76134 Mont Saint Aignan Cedex, France
and
Laboratoire Analyse, Géométrie et Applications, URA CNRS 742,
Institut Galilée, Département de Mathématiques, Avenue J. – B. Clément,
93430 Villetaneuse, France (e-mail: strelcyn@math.univ-paris13.fr).

Abstract

Let $K$ be a field of characteristic zero. We show that if $n \geq 3$, given $r \geq 0$ there exists a diagonal $K$-derivation of $K[x_1, \ldots, x_n]$ such that the minimal number of generators over $K$ of the ring of constants is equal to $r$.

1. Introduction. Let $K$ be a field of characteristic zero and $R = K[x_1, \ldots, x_n]$ the polynomial ring over $K$.

Let $d$ be a $K$-derivation of $R$ and $R^d$ its ring of constants, that is,

$$R^d = \{ w \in R; d(w) = 0 \}.$$

If $R^d \neq K$ and $R^d$ is finitely generated over $K$ then we denote by $\gamma(d)$ the minimal number of polynomials from $R \setminus K$ which generate $R^d$ over $K$. Moreover we assume that $\gamma(d) = 0$ iff $R^d = K$, and $\gamma(d) = \infty$ iff $R^d$ is not finitely generated over $K$.

In a recent paper [1] Derksen show that the Nagata’s counterexample [3] to the fourteenth problem of Hilbert can be put in the form $R^d$ for some derivation $d$ with
The aim of this note is to prove the following

**Theorem 1** If \( n \geq 3 \) and \( r \geq 0 \) then there exists a diagonal \( K \)-derivation of \( R = K[x_1, \ldots, x_n] \) such that \( \gamma(d) = r \).

**2. Proof.** Let us start with the following two simple remarks:

(a) If \( d(x_1) = x_1, \ldots, d(x_n) = x_n \) then \( \gamma(d) = 0 \).

(b) Let \( 1 \leq r < n \) and \( d(x_1) = \ldots = d(x_r) = 0, d(x_{r+1}) = x_{r+1}, \ldots, d(x_n) = x_n \).

Then \( \gamma(d) = r \).

Consequently, in the remaining part of the proof we will assume that \( r \geq n \).

Define \( m = n - 3 \) and \( p = r - n + 2 = r - m - 1 \); \( p \geq 2 \).

Let \( x = x_1, y = x_2, z = x_3 \) and if \( n > 3, y_1 = x_4, \ldots, y_m = x_n \).

To prove our theorem let us consider a \( K \)-derivation of \( R \) defined as follows:

\[
\begin{align*}
d(x) &= x, \quad d(y) = y, \quad d(z) = -pz \\
d(y_1) &= \ldots = d(y_m) = 0.
\end{align*}
\]

and, if \( n > 3 \),

\[
\begin{align*}
d(y_1) &= \ldots = d(y_m) = 0.
\end{align*}
\]

Consider now \( r \) polynomials \( f_0, f_1, \ldots, f_{p+m} \):

\[
f_0 = x^p z, \quad f_1 = x^{p-1} y^i z, \ldots, \quad f_i = x^{p-1} y^i z, \ldots, \quad f_{p-1} = x^1 y^{p-1} z, \quad f_p = y^p z
\]

which are defined for every \( n \geq 3 \) and

\[
f_{p+1} = y_1, \quad f_{p+2} = y_2, \ldots, \quad f_{p+m} = y_m
\]

when \( n > 3 \).

If \( n = 3 \) then \( R = K[x, y, z] \) and \( p + 1 = r \). If \( n > 3 \) then \( R = K[x, y, z, y_1, \ldots, y_m] \) and \( p + 1 + m = r \).

Let us observe that these polynomials belong to \( R^d \). Indeed; if \( 0 \leq i \leq p \) then

\[
d(f_i) = d(x^{p-i} y^i z) = (p - i + i - p)x^{p-i} y^i z = 0
\]

and if \( i = p + j \geq p \), then \( d(f_i) = d(y_j) = 0 \).

2
Lemma 1 The polynomials \( f_0, \ldots, f_{r-1} \) generate \( R^d \) over \( K \).

Proof. Let \( w \in R \) be such that \( d(w) = 0 \). First let us consider the case when \( w \in K[x, y, z] \). Thus

\[ w = \sum a_{ijk} x^i y^j z^k \]

with all \( a_{ijk} \in K \). Since \( d \) is diagonal then all monomials \( x^i y^j z^k \) from the above sum are such that \( d(x^i y^j z^k) = 0 \). Let us pick such a monomial \( w_0 = x^i y^j z^k \). Then \( i + j = pk \). Let \( a, b, u, v \) be the nonnegative integers such that

\[ i = ap + u, \quad j = bp + v, \quad u < p, \quad v < p. \]

Then either \( u + v = 0 \), or \( u + v = p \). If \( u + v = 0 \), then \( k = a + b \) and consequently

\[ w_0 = x^i y^j z^k = x^{ap} y^{bp} z^{a+b} = (x^p z)^a (y^p z)^b = f_0 f_p^b. \]

If \( u + v = p \), then \( k = a + b + 1 \) which implies

\[ w_0 = x^i y^j z^k = x^{ap+u} y^{bp+v} z^{a+b+1} = (x^u y^v z)(x^p z)^a (y^p z)^b = f_v f_p f_0. \]

Therefore, if \( w \in K[x, y, z] \) and \( d(w) = 0 \), then \( w \in K[f_0, \ldots, f_p] \).

Assume now that \( w \in R = K[x, y, z, y_1, \ldots, y_m] \). Then

\[ w = \sum a_{i1 \ldots im} y_1^{i_1} \ldots y_m^{i_m} \]

where all coefficients \( a_{i1 \ldots im} \) belong to \( K[x, y, z] \). Since \( d(w) = 0 \) we have

\[ 0 = d(w) = \sum d(a_{i1 \ldots im}) y_1^{i_1} \ldots y_m^{i_m}, \]

and hence \( d(a_{i1 \ldots im}) = 0 \). From the first step of our proof, we know that \( a_{i1 \ldots im} \in K[f_0, \ldots, f_p] \) and therefore \( w \in K[f_0, \ldots, f_p, y_1, \ldots, y_m] = K[f_0, \ldots, f_{r-1}]. \)

Now we will prove that \( \{ f_0, \ldots, f_{r-1} \} \) is a minimal set of generators of \( R^d \).

For this aim suppose that for some \( s < r \) there exist polynomials \( g_1, \ldots, g_s \) such that \( R^d = K[g_1, \ldots, g_s] \). Then \( K[f_0, \ldots, f_{r-1}] = K[g_1, \ldots, g_s] \) so that there exist polynomials \( \alpha_0, \ldots, \alpha_{r-1} \in K[u_1, \ldots, u_s] \) such that

\[ f_i = \alpha_i(g_1, \ldots, g_s) \]

for \( i = 0, 1, \ldots, r - 1 \). Moreover there exist polynomials \( \beta_1, \ldots, \beta_s \in K[v_0, \ldots, v_{r-1}] \) such that

\[ g_j = \beta_j(f_0, \ldots, f_{r-1}) \]

for \( j = 1, \ldots, s \).

Denote \( F = (f_0, \ldots, f_{r-1}) \) and \( G = (g_1, \ldots, g_s) = (\beta_1(F), \ldots, \beta_s(F)) \). Then in the ring \( R \) the following identities are satisfied:

\[ f_i = \alpha_i(G) = \alpha_i(\beta_1(F), \ldots, \beta_s(F)), \]

where all coefficients \( \alpha_{i1 \ldots im} \) belong to \( K[f_0, \ldots, f_{r-1}] \). Therefore \( d(G) = 0 \) and consequently \( d(F) = 0 \) as well. This contradicts the minimality of \( \{ f_0, \ldots, f_{r-1} \} \) as the minimal set of generators of \( R^d \).
for \( i = 0, 1, \ldots, r - 1 \), that is,

\[ F = (\alpha \circ \beta)(F), \]

where \( \alpha = (\alpha_0, \ldots, \alpha_{r-1}) \) and \( \beta = (\beta_1, \ldots, \beta_s) \).

Let us introduce the notations:

\[ \omega = (0, 0, 1, 0, \ldots, 0) \in K^n, \]

\[ A_{ik} = \frac{\partial \alpha_i}{\partial u_k}(G), \quad B_{kq} = \frac{\partial \beta_k}{\partial v_q}(F), \quad a_{ik} = A_{ik}(\omega), \quad b_{kq} = B_{kq}(\omega), \]

for any \( i, q = 0, 1, \ldots, r - 1 \) and \( k = 1, \ldots, s \).

Moreover define

\[ C_{iq} = \sum_{k=1}^{s} A_{ik} B_{kq}, \quad c_{iq} = C_{iq}(\omega) = \sum_{k=1}^{s} a_{ik} b_{kq}, \]

where \( i, q = 0, 1, \ldots, r - 1 \).

Finally let us introduce the matrices:

\[ A = [a_{ik}], \quad B = [b_{kq}], \quad C = [c_{iq}], \]

where \( 0 \leq i \leq r - 1, \quad 1 \leq k \leq s \) and \( 0 \leq q \leq r - 1 \).

By \( \delta_{iq} \) we denote usual Kronecker delta.

Now, using the above notations we will prove the following two lemmas.

**Lemma 2** If \( 0 \leq i \leq r - 1 \) and \( p + 1 \leq q \leq r - 1 \) then \( c_{iq} = \delta_{iq} \).

**Proof.** Differentiating the identity \( F = (\alpha \circ \beta)(F) \) one obtains that

\[ \frac{\partial f_i}{\partial x_j} = \sum_{l=0}^{r-1} C_{il} \frac{\partial f_l}{\partial x_j} \]  \hspace{1cm} (1)

for \( i = 0, 1, \ldots, r - 1 \) and \( j = 1, \ldots, n \).

Let \( q \) be as in our lemma and denote

\[ t = q - p, \quad j_0 = t + 3. \]

Then \( t > 0, \ j_0 > 3 \) and by virtue of our choice of \( f_0, \ldots, f_{r-1} \) we see that \( f_q = y_t = x_{j_0} \), so \( \frac{\partial f_q}{\partial x_{j_0}} = 1 \) and, if \( i \neq q \), then \( \frac{\partial f_i}{\partial x_{j_0}} = 0 \), that is,

\[ \frac{\partial f_i}{\partial x_{j_0}} = \delta_{iq}. \]  \hspace{1cm} (2)

Therefore, by (1) and (2):

\[ C_{iq} = C_{iq} \cdot 1 = C_{iq} \frac{\partial f_q}{\partial x_{j_0}} = \sum_{l=0}^{r-1} C_{il} \frac{\partial f_l}{\partial x_{j_0}} = \frac{\partial f_i}{\partial x_{j_0}} = \delta_{iq}, \]

and consequently \( c_{iq} = C_{iq}(\omega) = \delta_{iq} \).
Lemma 3 If $0 \leq i \leq p$ and $1 \leq q \leq p$ then $c_{iq} = \delta_{iq}$.

Proof. Let $d_x = \frac{\partial}{\partial x}$, $d_y = \frac{\partial}{\partial y}$. Given a natural number $t \geq 2$ we define $M_t$ as the ideal in $R$ generated by all elements of the form

$$d_x^a d_y^b (f_k), \text{ where } k = 0, 1, \ldots, p \text{ and } 1 \leq a + b \leq t - 1.$$ 

It is clear that $d_x(M_t) \subseteq M_{t+1}$ and $d_y(M_t) \subseteq M_{t+1}$. Moreover every element from $M_p$ is of the form $zh$, where $h \in R$ is such that $h(\omega) = 0$.

By successive differentiations of the identity $F = (\alpha \circ \beta)(F)$ one easily sees (see (1)) that, for $a \geq 0$, $b \geq 0$, $a + b > 0$ and $0 \leq k \leq p$,

$$d_x^a d_y^b (f_k) = \sum_{l=0}^{r-1} C_{kl} d_x^a d_y^b (f_l) + E_{k,a,b},$$

where $E_{k,a,b} \in M_{a+b}$. From the above identity and Lemma 2 one deduces that

$$d_x^a d_y^b (f_k)(\omega) = \sum_{l=0}^{p} c_{kl} d_x^a d_y^b (f_l)(\omega), \quad (3)$$

because every element of the ideal $M_{a+b}$ vanishes at $\omega$. Now, observe that if $0 \leq k, q \leq p$ then

$$d_x^{p-q} d_y^q (f_k) = (p - q)! q! \delta_{kq} z. \quad (4)$$

Therefore, by (3) and (4), one obtains that

$$(p - q)! q! \delta_{kq} = d_x^{p-q} d_y^q (f_k)(\omega)$$

$$= \sum_{l=0}^{p} c_{kl} d_x^{p-q} d_y^q (f_l)(\omega)$$

$$= (p - q)! q! c_{kq}$$

and consequently $c_{iq} = \delta_{iq}$.

Now we can conclude the proof of our theorem. By Lemmas 1 and 2, the matrix $C$ is invertible. Let $D = C^{-1}A$. Then $D$ is an $r \times s$ matrix and $I = DB$, where $I$ is the $r \times r$ identity matrix. Therefore there exist two $K$-linear mappings $B : K^r \rightarrow K^s$, $D : K^s \rightarrow K^r$ such that $D \circ B = id$. Then $B$ is injective, but it is a contradiction because $s < r$. This proves that $\{f_0, \ldots, f_{r-1}\}$ is a minimal set of generators of $R^d$ over $K$, that is, $\gamma(d) = r$.

3. Remark. In the proof we never used the assumption that $\{g_i\}, \{f_j\}, \{\alpha_k\}$ are polynomials. Note that the same proof gives the following
Proposition Let $K$ be the field of real or of complex numbers. Let $n, p$ be natural numbers such that $n \geq 3$ and $2 \leq p \leq n$. Denote $x = (x_1, \ldots, x_n)$ and let
\[
\begin{align*}
 f_i(x) &= x_i^{p-i}x_2x_3, \quad \text{for } 0 \leq i \leq p, \\
 f_i(x) &= x_{n-p+i}, \quad \text{for } p+1 \leq i \leq p+n-3.
\end{align*}
\]
If $g_1, \ldots, g_s \in C^\infty(K^n)$ and $f_i = \alpha_i(g_1, \ldots, g_s)$, $g_j = \beta_j(f_0, \ldots, f_{p+n-3})$, for some functions
\[
\begin{align*}
\alpha_i &\in C^\infty(K^s), \quad 0 \leq i \leq p+n-3, \\
\beta_j &\in C^\infty(K^{p+n-2}), \quad 1 \leq j \leq s,
\end{align*}
\]
then $s \geq r$.

If $K$ is the field of real numbers instead of $C^\infty$ functions it suffices to consider functions of class $C^p$.

Acknowledgments. The first version of this paper was written when the second author was a guest at Department of Mathematics of Toruń University. It was completed during the stay of the first author at the Department of Mathematics of Rouen University as visiting professor. Both Departments are acknowledged for their hospitality and excellent working conditions.

References


