UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XLV
2007

GENERATORS OF RINGS OF CONSTANTS OF DERIVATIONS

by Piotr Jędrzejewicz

Abstract. The aim of this paper is to summarize some motivations and results concerning generators of rings of constants of derivations, especially in the positive characteristic case.

1. Preliminaries. Let k be a field of characteristic $p \geqslant 0$. Denote by $k[X]$ the polynomial algebra $k[x_1, \ldots, x_n]$ and by $k(X)$ the field of rational functions $k(x_1, \ldots, x_n)$. A k-linear mapping $d\colon k[X] \to k[X]$ is called a k-derivation of $k[X]$ if

$$d(fg) = fd(g) + gd(f)$$

for all $f, g \in k[X]$. For any $g_1, \ldots, g_n \in k[X]$ there exists the unique k-derivation d of $k[X]$ such that

$$d(x_1) = g_1,\ \ldots,\ d(x_n) = g_n.$$

This derivation is of the form

$$d = g_1 \frac{\partial}{\partial x_1} + \ldots + g_n \frac{\partial}{\partial x_n}.$$

If d is a k-derivation of $k[X]$, then, by $k[X]^d$, we denote the ring of constants of d:

$$k[X]^d = \{f \in k[X] :\ d(f) = 0\}.$$

Denote, by $k[X^p]$, the subalgebra $k[x_1^p, \ldots, x_n^p] \subseteq k[X]$ and, by $k(X^p)$, the subfield $k(x_1^p, \ldots, x_n^p) \subseteq k(X)$. In the case of $p = 0$ we put $x_i^p = 1$, so $k[X^p] = k$ and $k(X^p) = k$. For every k-derivation of $k[X]$ there is

$$k[X^p] \subseteq k[X]^d,$$

so $k[X]^d$ is a $k[X^p]$-algebra.

In [**11**] (see [**9**], 4.1) Nowicki obtained necessary and sufficient conditions for rings of constants of derivations in the case of characteristic zero. Analogical conditions in the case of positive characteristic are simpler (see [**2**], Theorem 1.1).

2. Some general facts about the number of generators. Assume first that $\operatorname{char} k = 0$. We know that not all rings of constants of polynomial derivations are finitely generated (Hilbert's XIV Problem). Moreover, in the case of $n \geqslant 3$, in [**14**] (see [**9**], 7.4), Nowicki and Strelcyn showed that every nonnegative integer can be the minimal number of generators of a ring of constants.

In the case of $n = 2$, in [**13**], Nowicki and Nagata showed that every nonzero k-derivation of $k[x, y]$ has the ring of constants of the form $k[f]$ for some $f \in k[x, y]$. The properties of such rings were discussed in [**10**] (see [**9**], 5.2, 7.1, 7.2). Note also Miyanishi's theorem ([**8**], see [**1**], p. 30) that every nonzero locally nilpotent k-derivation of $k[x, y, z]$ has the ring of constants of the form $k[f, g]$ for some algebraically independent $f, g \in k[x, y, z]$.

Now assume that $\operatorname{char} k = p > 0$. In this case all rings of constants of polynomial derivations are finitely generated ([**13**]). In [**13**] Nowicki and Nagata proved that if $p = 2$ and d is a nonzero k-derivation of $k[x, y]$, then $k[x, y]^d = k[x^p, y^p, f]$ for some $f \in k[x, y]$. They also showed that if $p > 2$ and

$$d = x \cdot \frac{\partial}{\partial x} + y \cdot \frac{\partial}{\partial y},$$

then $k[x, y]^d \neq k[x^p, y^p, f]$ for any $f \in k[x, y]$. In [**7**] Li proved that for this derivation, the minimal number of generators of $k[x, y]^d$, as a $k[x^p, y^p]$-algebra, is equal to $p - 1$. In [**6**] Li proved that for every nonzero k-derivation of $k[x, y]$ the minimal number of generators is not greater than $p - 1$.

3. Example: linear derivations with rings of constants being generated by linear forms. Now k is a field of characteristic $p \geqslant 0$. A k-derivation $d\colon k[X] \to k[X]$ such that

$$d(x_j) = a_{1j}x_1 + \ldots + a_{nj}x_n \text{ for } j = 1, \ldots, n,$$

where $a_{ij} \in k$ for $i, j = 1, \ldots, n$, is called a linear derivation of $k[X]$.

The motivation for studying rings of constants of linear derivations came from the following results in the case of $\operatorname{char} k = 0$:

– the well known description of linear derivations of $k[X]$ with trivial ring of constants, i.e., such that $k[X]^d = k$,

– the description of linear derivations of $k(X)$ with trivial field of constants, i.e., such that $k(X)^d = k$ (Nowicki, [**12**]).

General Questions:

1. When is $k[X]^d$ a polynomial k-algebra?

2. When is $k(X)^d$ a field of rational functions?

The answers to these questions are, in general, not known, so we can try to find them in some special cases.

Specific Questions:

1. When is $k[X]^d = k[y_1, \dots, y_r, y_{r+1}^p, \dots, y_n^p]$ for some k-linear basis $y_1, \dots, y_n$ of $kx_1 + \ldots + kx_n$ (i.e., $k[X]^d = k[y_1, \dots, y_r]$ in the case of $p = 0$)?

2. When is $k(X)^d = k(y_1, \dots, y_r, y_{r+1}^p, \dots, y_n^p)$ for some k-linear basis $y_1, \dots, y_n$ of $kx_1 + \ldots + kx_n$?

Theorem ([**4**]). *Answer for Question 2: if and only if the matrix (a_{ij}) has one of the following Jordan forms.*

– In the case of $p > 0$:

$$\begin{pmatrix} \rho_1 & & 0 \\ & \ddots & \\ 0 & & \rho_n \end{pmatrix}, \quad \begin{pmatrix} \begin{pmatrix} \rho_1 & 1 \\ 0 & \rho_1 \end{pmatrix} & & & 0 \\ & \rho_2 & & \\ & & \ddots & \\ 0 & & & \rho_{n-1} \end{pmatrix}, \quad \underbrace{\begin{pmatrix} \begin{pmatrix} \rho_1 & 1 & 0 \\ 0 & \rho_1 & 1 \\ 0 & 0 & \rho_1 \end{pmatrix} & & & 0 \\ & \rho_2 & & \\ & & \ddots & \\ 0 & & & \rho_{n-2} \end{pmatrix}}_{\text{only } p=2},$$

where nonzero ρ_i are linearly independent over $\mathbb{F}_p$ (the prime subfield).

– In the case of $p = 0$:

$$\begin{pmatrix} J(\rho_1) & & & & & 0 \\ & \ddots & & & & \\ & & J(\rho_m) & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix}, \quad \begin{pmatrix} J(\rho_1) & & & & & & 0 \\ & \ddots & & & & & \\ & & J(\rho_m) & & & & \\ & & & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 0 \end{pmatrix},$$

where $\rho_1, \dots, \rho_m \neq 0$ are linearly independent over $\mathbb{Z}_{\geqslant 0}$ and $J(\varrho_i)$ is a Jordan block with eigenvalue ϱ_i.

4. Example: monomial derivations in two variables with a single generator of the ring of constants. When we think about effective methods for computing rings of constants of derivations, then the main tool is van den Essen's [**1**] algorithm for computing generators for locally nilpotent derivations in the case of $p = 0$, when the ring of constants is finitely generated. Okuda in

[**15**] adapted this algorithm for arbitrary derivations in the case of $p > 0$. As an example he computed generators for monomial derivations in two variables in the cases of $p = 2$ and $p = 3$.

We here develop a different approach, because, for arbitrary p, we want to find all monomial derivations with rings of constants generated by exactly one element.

Let k be a field of characteristic $p > 0$. Let m, n, r, s be nonnegative integers, $m, n \not\equiv -1 \pmod{p}$, and let $\alpha, \beta \in k \setminus \{0\}$. Consider the following examples:

$$\begin{cases} d_1(x) = \alpha x^{rp}, \\ d_1(y) = \beta y^{sp}, \end{cases} \qquad k[x,y]^{d_1} = k[x^p, y^p, \beta x y^{sp} - \alpha x^{rp} y],$$

$$\begin{cases} d_2(x) = \alpha x, \\ d_2(y) = -\alpha y, \end{cases} \qquad k[x,y]^{d_2} = k[x^p, y^p, xy],$$

$$\begin{cases} d_3(x) = \alpha y^n, \\ d_3(y) = \beta x^m, \end{cases} \qquad k[x,y]^{d_3} = k[x^p, y^p, (n+1)\beta x^{m+1} - (m+1)\alpha y^{n+1}],$$

$$\begin{cases} d_4(x) = \alpha x^{rp} y^n, \\ d_4(y) = \beta, \end{cases} \qquad k[x,y]^{d_4} = k[x^p, y^p, (n+1)\beta x - \alpha x^{rp} y^{n+1}],$$

$$\begin{cases} d_5(x) = 0, \\ d_5(y) = \beta, \end{cases} \qquad k[x,y]^{d_5} = k[x^p, y^p, x],$$

$$\begin{cases} d_6(x) = \alpha, \\ d_6(y) = \beta x^m y^{sp}, \end{cases} \qquad k[x,y]^{d_6} = k[x^p, y^p, \beta x^{m+1} y^{sp} - (m+1)\alpha y],$$

$$\begin{cases} d_7(x) = \alpha, \\ d_7(y) = 0, \end{cases} \qquad k[x,y]^{d_7} = k[x^p, y^p, y].$$

THEOREM ([**3**]). *A k-derivation d of $k[x,y]$ such that*

$$\begin{cases} d(x) = \alpha x^t y^u, \\ d(y) = \beta x^v y^w, \end{cases}$$

where $\alpha, \beta \in k$, has the ring of contants of the form $k[x^p, y^p, f]$, where $f \in k[x,y] \setminus k[x^p, y^p]$, if and only if $d = x^j y^l \cdot d_i$, where $j, l \geqslant 0$, $i \in \{1, 2, \ldots, 7\}$.

This theorem is a special case of a more general one, concerning derivations, which are homogeneous with respect to weights, because every monomial derivation is homogeneous with respect to a suitable weight vector.

5. Derivations in positive characteristic, homogeneous with respect to weights. Let $\gamma = (\gamma_1, \ldots, \gamma_n) \in k^n \setminus \{(0, \ldots, 0)\}$. For every $r \in k$ denote by $k[X]^{\gamma}_{(r)}$ the k-linear span of all monomials $x_1^{l_1} \ldots x_n^{l_n}$ such that

$$l_1\gamma_1 + \ldots + l_n\gamma_n = r.$$

A k-derivation d of $k[X]$ will be called γ-homogeneous of degree s, where $s \in k$, if $d(k[X]^{\gamma}_{(r)}) \subseteq k[X]^{\gamma}_{(r+s)}$ for every $r \in k$.

Theorem ([**3**]). *Let* $\operatorname{char} k = p > 0$, $f \in k[x,y] \setminus k[x^p, y^p]$ *and* d *be a nonzero* γ*-homogeneous* k*-derivation of* $k[x,y]$*. Then* $k[x,y]^d = k[x^p, y^p, f]$ *if and only if*

$$gcd\,(d(x), d(y))^{-1} \cdot d = a \cdot \frac{\partial f}{\partial y} \cdot \frac{\partial}{\partial x} - a \cdot \frac{\partial f}{\partial x} \cdot \frac{\partial}{\partial y}$$

for some $a \in k \setminus \{0\}$.

Note that γ-homogeneous polynomials of γ-degree 0 play a special role, because if $d(f) = 0$ for some $f \in k[x,y]^{\gamma}_{(0)} \setminus k[x^p, y^p]$ and a nonzero k-derivation d of $k[x,y]$, then

$$k[x,y]^d = k[x,y]^{\gamma}_{(0)}.$$

The equality $k[x,y]^{\gamma}_{(0)} = k[x^p, y^p, f]$, where $\gamma = (\lambda, \mu)$, holds in the following three cases only:

- $\lambda + \mu = 0$, $f = axy + g$,
- $\lambda = 0$, $f = ax + g$,
- $\mu = 0$, $f = ay + g$,

where $a \in k \setminus \{0\}$ and $g \in k[x^p, y^p]$.

6. More generators. If $\operatorname{char} k = p > 0$ and d is a nonzero k-derivation of $k[X]$, then

$$k[X]^d = k(x_1^p, \ldots, x_n^p, f_1, \ldots, f_m) \cap k[X] = k(X^p)[f_1, \ldots, f_m] \cap k[X]$$

for some $f_1, \ldots, f_m \in k[X]$, $m < n$.

Good Question: When is $k[X]^d = k[x_1^p, \ldots, x_n^p, f_1, \ldots, f_m]$?

Theorem ([**5**]). *Let* k *be a field of characteristic* $p > 0$ *and* $f_1, \ldots, f_m \in k[X]$ *be eigenvectors of some* k*-derivation of* $k[X]$ *with eigenvalues being linearly independent over* $\mathbb{F}_p$*. Then:*

a) $k(X^p)[f_1, \ldots, f_m] \cap k[X]$ *is a free* $k[x_1^p, \ldots, x_n^p]$*-module with a basis*

$$\left\{ \frac{f_1^{\alpha_1} \ldots f_m^{\alpha_m}}{g_\alpha};\ 0 \leqslant \alpha_1, \ldots, \alpha_m < p \right\},$$

where g_α *is the least common multiple of all divisors of* $f_1^{\alpha_1} \ldots f_m^{\alpha_m}$*, belonging to* $k[x_1^p, \ldots, x_n^p]$*.*

b) $k(X^p)[f_1, \ldots, f_m] \cap k[X] = k[x_1^p, \ldots, x_n^p, f_1, \ldots, f_m]$ *if and only if* $f_1, \ldots, f_m$ *are pairwise coprime and have no multiple factors and no factors from* $k[X^p] \setminus k$*.*

Let us conclude with some "effective methods" questions.

Specific Question: Given $f_1, \dots, f_m \in k[X]$, $p > 0$. Can we compute generators of the $k[X^p]$-algebra

$$k(X^p)[f_1, \dots, f_m] \cap k[X]?$$

General Questions:

1. Given $f_1, \dots, f_m \in k[X]$. Can we compute generators of the k-algebra

$$k(f_1, \dots, f_m) \cap k[X],$$

if it is finitely generated?

2. Can we prove that such algorithm does not exist?

References

1. van den Essen A., *Polynomial automorphisms and the Jacobian Conjecture*, Birkhäuser, Basel, 2000.
2. Jędrzejewicz P., *Rings of constants of p-homogeneous polynomial derivations*, Comm. Algebra, **31** (2003), 5501–5511.
3. Jędrzejewicz P., *On rings of constants of derivations in two variables in positive characteristic*, Coll. Math., **106** (2006), 109–117.
4. Jędrzejewicz P., *Linear derivations with rings of constants being generated by linear forms*, to appear.
5. Jędrzejewicz P., *Eigenvector p-bases of rings of constants of derivations*, to appear.
6. Li W., *Remarks on rings of constants of derivations*, Proc. Amer. Math. Soc., **107** (1989), 337–340.
7. Li W., *Remarks on rings of constants of derivations II*, Comm. Algebra, **20** (1992), 2191–2194.
8. Miyanishi M., *Normal affine subalgebras of a polynomial ring*, in: *Algebraic and Topological Theories*, Kinokuniya, Tokyo, 1985, 37–51.
9. Nowicki A., *Polynomial derivations and their rings of constants*, UMK, Toruń, 1994.
10. Nowicki A., *On the jacobian equation $J(f, g) = 0$ for polynomials in $k[x, y]$*, Nagoya Math. J., **109** (1988), 151–157.
11. Nowicki A., *Rings and fields of constants for derivations in characteristic zero*, J. Pure Appl. Algebra, **96** (1994), 47–55.
12. Nowicki A., *On the nonexistence of rational first integrals for systems of linear differential equations*, Linear Algebra Appl., **235** (1996), 107–120.
13. Nowicki A., Nagata M., *Rings of constants for k-derivations in $k[x_1, \dots, x_n]$*, J. Math. Kyoto Univ., **28** (1988), 111–118.
14. Nowicki A., Strelcyn J.-M., *Generators of rings of constants for some diagonal derivations in polynomial rings*, J. Pure Appl. Algebra, **101** (1995), 207–212.
15. Okuda S.-I., *Kernels of derivations in positive characteristic*, Hiroshima Math. J., **34** (2004), 1–19.

Received September 30, 2006

Toruń, Poland