LINEAR DERIVATIONS WITH RINGS OF CONSTANTS
GENERATED BY LINEAR FORMS

BY

PIOTR JĘDRZEJEWICZ (Toruń)

Abstract. Let $k$ be a field. We describe all linear derivations $d$ of the polynomial algebra $k[x_1, \ldots, x_m]$ such that the algebra of constants with respect to $d$ is generated by linear forms: (a) over $k$ in the case of $\text{char } k = 0$, (b) over $k[x_1^p, \ldots, x_m^p]$ in the case of $\text{char } k = p > 0$.

Introduction. Throughout this paper $k$ is a field of characteristic $p \geq 0$. We denote by $k[X]$ the polynomial algebra $k[x_1, \ldots, x_m]$ with the natural grading $k[X] = \bigoplus_{j=0}^{\infty} k[X]_j$, where $k[X]_j$ is the subspace of forms of degree $j$. We also denote by $k[X^p]$ the subalgebra $k[x_1^p, \ldots, x_m^p]$, but in the case of $p = 0$ we assume $x_i^p = 1$, $i = 1, \ldots, m$, and $k[X^p] = k$. If $v_1, \ldots, v_n \in k[X]$, then we denote by $\langle v_1, \ldots, v_n \rangle_k$ the $k$-linear space spanned by $v_1, \ldots, v_n$. Throughout this paper we denote by $\mathbb{N}$ the set of nonnegative integers, and by $\mathbb{F}_p$ the prime subfield of $k$.

A $k$-linear mapping $d: k[X] \to k[X]$ is called a $k$-derivation of $k[X]$ if $d(fg) = fd(g) + gd(f)$ for all $f, g \in k[X]$. If $d$ is a $k$-derivation of $k[X]$, then we denote by $k[X]^d$ the ring of constants of $d$, that is, $k[X]^d = \{ f \in k[X] : d(f) = 0 \}$. Note that $k[X^p] \subseteq k[X]^d$, so $k[X]^d$ is a $k[X^p]$-algebra.

A mapping $d: k[X] \to k[X]$ is called a linear derivation if $d$ is a $k$-derivation of $k[X]$ and $d(k[X]_j) \subseteq k[X]_j$ for $j = 0, 1, 2, \ldots$. It is clear that a $k$-derivation $d$ of $k[X]$ is a linear derivation if and only if $d(x_j) = \sum_{i=1}^{m} a_{ij}x_i$ for $j = 1, \ldots, m$, where $a_{ij} \in k$ for $i, j = 1, \ldots, m$. A linear derivation $d$ is uniquely determined by the matrix $(a_{ij})$.

2000 Mathematics Subject Classification: Primary 12H05; Secondary 13N15.

Key words and phrases: linear derivation, ring of constants.
In the case of \( \text{char } k = 0 \), Nowicki ([2]) described the linear derivations of \( k[X] \) such that \( k[X]^d = k \). He also described such derivations satisfying the condition \( k(X)^d = k \), where \( k(X) \) is the field of rational functions. In this paper we consider the following, more general problem, concerning polynomial constants of linear derivations. Let \( 0 \leq r \leq m \). The problem is to describe all linear derivations \( d \) of \( k[X] \) such that

\[
\begin{align*}
\ k[X]^d &= k[y_1, \ldots, y_r, y_{r+1}^p, \ldots, y_m^p] \\
\end{align*}
\]

(i.e. \( k[X]^d = k[y_1, \ldots, y_r] \) in the case of \( p = 0 \)) for some \( k \)-linear basis \( y_1, \ldots, y_m \) of \( k[X]_1 \).

1. The Jordan case. In this section we consider a special case when the matrix \( (a_{ij}) \) of a linear derivation \( d \) of \( k[X] = k[x_1, \ldots, x_m] \) is already in the Jordan form

\[
\begin{pmatrix}
J_{m_1}(\varrho_1) & 0 & \cdots & 0 \\
0 & J_{m_2}(\varrho_2) & \cdots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & J_{m_s}(\varrho_s)
\end{pmatrix},
\]

\[
J_{m_i}(\varrho_i) = \begin{pmatrix}
\varrho_i & 1 & \cdots & 0 \\
0 & \varrho_i & \ddots & \vdots \\
\vdots & \ddots & \ddots & 1 \\
0 & \cdots & 0 & \varrho_i
\end{pmatrix}_{m_i},
\]

\( i = 1, \ldots, s \), where \( s \geq 1 \), \( m_1 \geq \cdots \geq m_s \), \( m_1 + \cdots + m_s = m \), and where \( \varrho_1, \ldots, \varrho_s \in k \).

Let \( n_1 = 1 \) and \( n_i = m_1 + \cdots + m_{i-1} + 1 \) for \( i = 2, \ldots, s \). Then \( d(x_{n_i}) = \varrho_i x_{n_i} \) and \( d(x_{n_i+l}) = x_{n_i+l-1} + \varrho_i x_{n_i+l} \) for \( l = 1, \ldots, m_i - 1 \), whenever \( m_i > 1 \).

Let

\[
I = \{1, \ldots, s\}, \quad I_0 = \{i \in I : \varrho_i = 0\}.
\]

We denote by \( d|_{k[X]_1} \) the restriction of \( d \) to \( k[X]_1 \). The kernel of \( d|_{k[X]_1} \) is \( k \)-linearly spanned by all the elements of the form \( x_{n_i} \), where \( i \in I_0 \), that is,

\[
k[X]^d \cap k[X]_1 = \langle x_{n_i} : i \in I_0 \rangle_k.
\]

This implies the following fact.

**Proposition 1.1.** Assume that \( k[X]^d = k[y_1, \ldots, y_r, y_{r+1}^p, \ldots, y_m^p] \) for some \( k \)-linear basis \( y_1, \ldots, y_m \) of \( k[X]_1 \). Then \( \langle y_1, \ldots, y_r \rangle_k = \langle x_{n_i} : i \in I_0 \rangle_k \) and \( k[X]^d \) is generated over \( k[X]^p \) by the elements \( x_{n_i} \), where \( i \in I_0 \), that is,

\[
k[X]^d = k[X]^p[x_{n_i} : i \in I_0].
\]

The aim of this section is to prove the following theorems.

**Theorem 1.2.** Let \( p = 0 \). The equality \( k[X]^d = k[x_{n_i} : i \in I_0] \) holds if and only if the following three conditions are satisfied:

1. the system \( (\varrho_i : i \in I \setminus I_0) \) is linearly independent over \( \mathbb{N} \),
Theorem 1.3. Let \( p > 0 \). The equality \( k[X]^d = k[X^p]|_{x_{i^+}^p \equiv x_i} \) holds if and only if the following three conditions are satisfied:

1. The system \( (g_i; i \in I \setminus I_0) \) is linearly independent over \( \mathbb{F}_p \),
2. \( m_1 \leq 2 \) or \( m_1 = 3, p = 2 \),
3. \( m_2 = 1 \).

Let \( \lambda_1, \ldots, \lambda_m \) be the diagonal elements of the matrix of \( d \), that is, \( \lambda_{n_i} = \cdots = \lambda_{n_i + m_i - 1} = g_i \) for \( i = 1, \ldots, s \). Obviously, \( d = d_D + d_N \), where \( d_D \) and \( d_N \) are the linear derivations defined by:

\[
\begin{align*}
d_D(x_j) &= \lambda_j x_j & \text{for} & \ j = 1, \ldots, m, \\
d_N(x_j) &= \begin{cases} 0 & \text{for} & j = n_1, \ldots, n_s, \\
x_j-1 & \text{for} & j \neq n_1, \ldots, n_s. \end{cases}
\end{align*}
\]

We see that

\[
d_D(x_1^{l_1} \ldots x_m^{l_m}) = (l_1 \lambda_1 + \cdots + l_m \lambda_m)x_1^{l_1} \ldots x_m^{l_m},
\]

\[
d_N(x_1^{l_1} \ldots x_m^{l_m}) = \sum_{j \neq n_1, \ldots, n_s} l_j x_1^{l_j-1} x_j^{-1} \ldots x_m^{l_m}.
\]

Proposition 1.4. \( k[X]^d = k[X]^{d_N} \cap k[X]^{d_D} \).

Proof. In the case of \( p = 0 \) this fact is well known ([4, Corollary 2.3] or [3, Corollary 9.4.4]). Assume that \( p > 0 \).

The inclusion \( k[X]^{d_N} \cap k[X]^{d_D} \subseteq k[X]^d \) is clear. To prove the reverse inclusion, suppose that \( d(f) = 0 \) for some \( f \in k[X] \). Let \( l \) be a positive integer such that \( p^l \geq m \), where \( m = \dim_k k[X]_1 \). Then \( (d_N|_{k[X]})^p = 0 \), so \( d_N^p = 0 \), and we have \( d_D^p (f) = d^p (f) = 0 \).

It is easy to see that all the monomials of the form \( x_1^{l_1} \ldots x_m^{l_m} \) such that \( l_1 \lambda_1 + \cdots + l_m \lambda_m = 0 \) form a \( k \)-linear basis of \( k[X]^{d_D} \), and all the monomials of the form \( x_1^{l_1} \ldots x_m^{l_m} \) such that \( l_1 \lambda_1^p + \cdots + l_m \lambda_m^p = 0 \) form a \( k \)-linear basis of \( k[X]^{d_D^p} \). Since \( l_1 \lambda_1^p + \cdots + l_m \lambda_m^p = (l_1 \lambda_1 + \cdots + l_m \lambda_m)^p \) for every \( l_1, \ldots, l_m \in \mathbb{Z} \), we have \( k[X]^{d_D^p} = k[X]^{d_D} \). This implies that \( d_D(f) = 0, \) so \( d_N(f) = d(f) - d_D(f) = 0, \) and finally \( f \in k[X]^{d_N} \cap k[X]^{d_D} \).

Note the following useful proposition.

Proposition 1.5. Let \( K \) be a domain of characteristic \( p \geq 0 \). Let \( \delta \) be a \( K \)-derivation of \( K[x_1, \ldots, x_m] \) such that \( \delta(x_i) = 0 \) for \( i \leq r \) and \( \delta(x_i) = \mu_i x_i \) for \( i > r \), where \( \mu_{r+1}, \ldots, \mu_m \in K \setminus \{0\} \) are linearly independent (over \( \mathbb{F}_p \) in the case of \( p > 0 \), over \( \mathbb{N} \) in the case of \( p = 0 \)). Then \( K[x_1, \ldots, x_m]^\delta = K[x_1, \ldots, x_r, x_{r+1}^p, \ldots, x_m^p] \).
Proof. It is enough to observe that \(d(x_1^l_1 \ldots x_m^l_m) = (l_{r+1}\mu_{r+1} + \cdots + l_m\mu_m)x_1^{l_1} \ldots x_m^{l_m}\) for every \(l_1, \ldots, l_m \geq 0\), so \(K[x_1, \ldots, x_m]^\delta\) is a free \(K\)-module and the monomials \(x_1^{l_1} \ldots x_m^{l_m}\) such that \(l_{r+1}\mu_{r+1} + \cdots + l_m\mu_m = 0\) form a basis of this module. ■

Recall that \(I = \{1, \ldots, s\}\) and \(I_0 = \{i \in I : \varrho_i = 0\}\). Let \(J = \{1, \ldots, m\}\) and \(J_0 = \{j \in J : \lambda_j = 0\}\).

Proof of Theorem 1.2. (\(\Rightarrow\)) (1) Assume that the system \((\varrho_i; i \in I \setminus I_0)\) is linearly dependent over \(\mathbb{N}\). Then there exist \(l_1, \ldots, l_s \in \mathbb{N}\) such that \(l_1\varrho_1 + \cdots + l_s\varrho_s = 0\) and \(l_j > 0\) for some \(j \in I \setminus I_0\). In this case \(x_1^{l_1} \ldots x_n^{l_s} \in k[X]^d \setminus k[x_n; i \in I_0]\).

(2) The condition \(m_i \geq 3\) for some \(i \in I_0\) means that \(d(x_n_i) = 0\), \(d(x_{n_i+1}) = x_{n_i}\) and \(d(x_{n_i+2}) = x_{n_i+1}\). Then \(x_{n_i+1} - 2x_n x_{n_i+2} \in k[X]^d \setminus k[x_n; i \in I_0]\).

(3) The condition \(m_i, m_j \geq 2\) for some \(i, j \in I_0\), \(i \neq j\) means that \(d(x_n_i) = 0\), \(d(x_{n_i+1}) = x_{n_i}\), \(d(x_{n_j}) = 0\) and \(d(x_{n_j+1}) = x_{n_j}\). Then \(x_{n_i} x_{n_j+1} - x_{n_i+1} x_{n_j} \in k[X]^d \setminus k[x_n; i \in I_0]\).

(\(\Leftarrow\)) Assume that conditions (1)–(3) hold.

We have \(d_N(x_j) = 0\) for \(j \in J_0\) and \(d_N(x_j) = \lambda_j x_j\) for \(j \in I \setminus J_0\), where \(\lambda_j = \varrho_i \neq 0\), \(n_i \leq j < n_i + m_i\), \(i \in I \setminus I_0\). The system \((\lambda_j; j \in J \setminus J_0)\) is linearly independent over \(\mathbb{N}\), because \((\varrho_i; i \in I \setminus I_0)\) is, so \(k[X]^d N = k[x_j; j \in J_0]\) by Proposition 1.5.

Let \(d_N'\) be the restriction of \(d_N\) to \(k[x_j; j \in J_0]\). Then, by Proposition 1.4, \(k[X]^d = (k[X]^d N)^d N = k[x_j; j \in J_0]^d N\). If \(m_{i_0} = 2\) for some \(i_0 \in I_0\), then it is easy to see that \(k[x_j; j \in J_0]^d N = k[x_j; j \in J_0 \setminus \{m_{i_0+1}\}] = k[x_n; i \in I_0]\).

If \(m_i = 1\) for every \(i \in I_0\), then \(d_N' = 0\), so \(k[x_j; j \in J_0]^d N = k[x_j; j \in J_0] = k[x_n; i \in I_0]\). ■

Proof of Theorem 1.3. (\(\Rightarrow\)) (1) Assume that the system \((\varrho_i; i \in I \setminus I_0)\) is linearly dependent over \(\mathbb{F}_p\). Then there exist nonnegative integers \(l_1, \ldots, l_s < p\) such that \(l_1\varrho_1 + \cdots + l_s\varrho_s = 0\) and \(l_j > 0\) for some \(j \in I \setminus I_0\). In this case \(x_1^{l_1} \ldots x_n^{l_s} \in k[X]^d \setminus k[X^p][x_n; i \in I_0]\).

(2) The condition \(m_1 \geq 3\) means that \(d(x_1) = \varrho_1 x_1\), \(d(x_2) = x_1 + \varrho_1 x_2\) and \(d(x_3) = x_2 + \varrho_1 x_3\). Then for \(p > 2\) we have \(x_1^{p-2} x_2^2 - 2x_1^{p-1} x_3 \in k[X]^d \setminus k[X^p][x_n; i \in I_0]\).

The condition \(m_1 \geq 4\) means that \(d(x_1) = \varrho_1 x_1\), \(d(x_2) = x_1 + \varrho_1 x_2\), \(d(x_3) = x_2 + \varrho_1 x_3\) and \(d(x_4) = x_3 + \varrho_1 x_4\). Then for \(p = 2\) we have \(x_1^3 x_4 + x_1^2 x_2 x_3 + x_1 x_2^2 \in k[X]^d \setminus k[X^p][x_n; i \in I_0]\).

(3) The condition \(m_2 \geq 2\) means that \(d(x_1) = \varrho_1 x_1\), \(d(x_2) = x_1 + \varrho_1 x_2\), \(d(x_{m_1+1}) = \varrho_2 x_{m_1+1}\) and \(d(x_{m_1+2}) = x_{m_1+1} + \varrho_2 x_{m_1+2}\). Then \(x_1^{p-1} x_2 x_{m_1+1} - x_1 x_{m_1+1} x_{m_1+2} \in k[X]^d \setminus k[X^p][x_n; i \in I_0]\).
(⇐) Assume that conditions (1)–(3) hold.

Let \(d'_D\) be the restriction of \(d_D\) to \(k[X^p][x_{n_1}, \ldots, x_{n_s}]\). Recall that \(J = \{1, \ldots, m\}\). Consider the set \(J' = J \setminus \{n_1, \ldots, n_s\}\). Let \(K = k[x_j^p; j \in J']\).

We see that \(d'_D\) is a \(K\)-derivation of \(K[x_{n_1}, \ldots, x_{n_s}] = k[X^p][x_{n_1}, \ldots, x_{n_s}]\) such that \(d'_D(x_{n_i}) = g_i x_{n_i}\), where \(g_i = 0\) for \(i \in I_0\), \(g_i \neq 0\) for \(i \in I \setminus I_0\) and the system \((g_i; i \in I \setminus I_0)\) is linearly independent over \(\mathbb{F}_p\). Proposition 1.5 implies that \(k[X^p][x_{n_1}, \ldots, x_{n_s}]^{d'_D} = k[X^p][x_{n_i}; i \in I_0]\). This ends the proof if \(m_1 = 1\).

If \(m_1 = 2\), then it is easy to see that \(k[X]^{d_N} = k[x_1, x_2^p, x_3, \ldots, x_m] = k[X^p][x_{n_1}, \ldots, x_{n_s}]\). If \(p = 2\) and \(m_1 = 3\), then it is easy to see that \(k[X]^{d_N} = k[x_1, x_2^p, x_3^p, x_4, \ldots, x_m] = k[X^p][x_{n_1}, \ldots, x_{n_s}]\). In both cases, by Proposition 1.4, \(k[X]^d = (k[X]^{d_N})^{d_D} = k[X^p][x_{n_i}; i \in I_0]\).

2. Some facts about graded algebras. In this section by a graded \(k\)-algebra we mean a \(k\)-algebra with a \(\mathbb{Z}\)-grading \(A = \bigoplus_{j=0}^\infty A_j\). Nonzero elements of \(A_j\) are called homogeneous of degree \(j\).

Note the following well known fact.

**Lemma 2.1.** Let \(B = \bigoplus_{j=0}^\infty B_j\) be a graded commutative \(k\)-algebra, \(B_0 = k\), and \(M = \bigoplus_{j > 0} B_j\). Let \(f_1, \ldots, f_n \in M\).

(a) If \(B = k[f_1, \ldots, f_n]\), then \(M/M^2 = \langle f_1 + M^2, \ldots, f_n + M^2 \rangle_k\).

(b) If \(f_1, \ldots, f_n\) are homogeneous elements and \(M/M^2 = \langle f_1 + M^2, \ldots, f_n + M^2 \rangle_k\), then \(B = k[f_1, \ldots, f_n]\). ■

The original version of this lemma ([1, II.3.2]) was formulated as an equivalence of three conditions under the assumptions that \(k = \mathbb{C}\) and \(f_1, \ldots, f_n\) are homogeneous elements. However, the proof is valid for an arbitrary field \(k\) and the implication in (a) is true for arbitrary \(f_1, \ldots, f_n \in M\).

If elements \(f_1, \ldots, f_n\) generate the \(k\)-algebra \(B\), with \(n\) smallest possible, then we say that \(f_1, \ldots, f_n\) form a minimal system of generators of \(B\). Using the previous lemma we can easily establish the following proposition.

**Proposition 2.2.** Let \(B = \bigoplus_{j=0}^\infty B_j\) be a graded commutative \(k\)-algebra with \(B_0 = k\) and let \(C_j = \sum_{l=1}^{j-1} B_l \cdot B_{j-l}\) for \(j > 1\), \(C_1 = 0\), \(C_0 = k\).

(a) Homogeneous elements \(f_1, \ldots, f_n\) form a minimal system of generators of \(B\) if and only if for every \(j\) the residue classes modulo \(C_j\) of all the elements \(f_i\) of degree \(j\) form a basis of the \(k\)-linear space \(B_j/C_j\).

(b) Let \(k \subseteq k'\) be a field extension. Denote by \(B'\) the graded \(k'\)-algebra \(k' \otimes_k B\). Let \(C'_j = \sum_{l=1}^{j-1} B'_l \cdot B'_{j-l}\) for \(j > 1\), \(C'_1 = 0\), \(C'_0 = k'\). Then \(\dim_k B_j/C_j = \dim_{k'} B'_j/C'_j\) for every \(j\). Moreover, if homogeneous
elements $f_1, \ldots, f_n$ form a minimal system of generators of the $k$-algebra $B$, then the elements $1 \otimes f_1, \ldots, 1 \otimes f_n$ form a minimal system of generators of the $k'$-algebra $B'$.

Proof. (a) Let $M = \bigoplus_{j>0} B_j$. Then $M^2 = \bigoplus_{j>0} C_j$. Lemma 2.1 implies that the elements $f_1, \ldots, f_n$ generate the $k$-algebra $B$ if and only if their residue classes modulo $M$ generate the linear space $M/M^2 \simeq \bigoplus_j B_j/C_j$. So $f_1, \ldots, f_n$ form a minimal system of generators of $B$ if and only if for every $j$ the residue classes modulo $C_j$ of all the elements $f_i$ of degree $j$ form a basis of $B_j/C_j$.

(b) For every $j > 1$ we have a canonical $k'$-linear isomorphism

$$
\sum_{l=1}^{j-1} (k' \otimes_k B_i) \cdot (k' \otimes_k B_{j-l}) \simeq k' \otimes_k \sum_{l=1}^{j-1} B_i \cdot B_{j-l},
$$

that is, $C'_j \simeq k' \otimes_k C_j$. This implies that $\dim_k B_j/C_j = \dim_{k'} B'_j/C'_j$.

Let $f_{i_1}, \ldots, f_{i_s}$ be all the elements $f_i$ of degree $j$. By (a), the residue classes modulo $C_j$ of $f_{i_1}, \ldots, f_{i_s}$ form a $k$-linear basis of $B_j/C_j$. Then the residue classes of $1 \otimes f_{i_1}, \ldots, 1 \otimes f_{i_s}$ form a $k'$-linear basis of $B'_j/C'_j$. Again by (a), the elements $1 \otimes f_1, \ldots, 1 \otimes f_n$ form a minimal system of generators of the $k'$-algebra $B'$.

Note the following immediate consequence of Lemma 2.1 and Proposition 2.2(a).

Corollary 2.3. If $B$ is generated by $n$ elements (not necessarily homogeneous), then $B$ is generated by some $n$ homogeneous elements.

Proof. Let $M$ and $C_j$ be defined as in Lemma 2.1 and Proposition 2.2. It is enough to observe that $M/M^2 \simeq \bigoplus_{j=0}^\infty B_j/C_j$, so $\sum_{j=0}^\infty \dim_k B_j/C_j \leq n$.

Now we will prove the following proposition.

Proposition 2.4. Let $k \subseteq k'$ be an extension of fields of arbitrary characteristic $p \geq 0$, let $B$ be a graded subalgebra of $k[X]$ and $B' = k' \otimes_k B$ the corresponding subalgebra of $k'[X]$. Let $r \in \{0, 1, \ldots, m\}$. Then the following conditions are equivalent:

(i) $B = k[y_1, \ldots, y_r, y_{r+1}^p, \ldots, y_m^p]$ for some $k$-linear basis $y_1, \ldots, y_m$ of $k[X]_1$,

(ii) $B' = k'[z_1, \ldots, z_r, z_{r+1}^p, \ldots, z_m^p]$ for some $k'$-linear basis $z_1, \ldots, z_m$ of $k'[X]_1$.

Proof. (i)$\Rightarrow$(ii) is obvious.

(ii)$\Rightarrow$(i). Assume that $B' = k'[z_1, \ldots, z_r, z_{r+1}^p, \ldots, z_m^p]$ for some $k'$-linear basis $z_1, \ldots, z_m$ of $k'[X]_1$. Let $C_j$ and $C'_j$ be defined as in Proposition 2.2.
Let \( p = 0 \). The elements \( z_1, \ldots, z_r \) form a minimal system of generators of the \( k' \)-algebra \( B' \), so \( \dim_{k'} B'_j = r \) and \( \dim_{k'} B'_j/C'_j = 0 \) for \( j > 1 \) by Proposition 2.2(a). Proposition 2.2(b) implies that \( \dim_k B_1 = r \) and \( \dim_k B_j/C_j = 0 \) for \( j > 1 \). Let \( y_1, \ldots, y_r \) be a \( k \)-linear basis of \( B_1 \). Then \( y_1, \ldots, y_r \) form a minimal system of generators of the \( k \)-algebra \( B \) (Proposition 2.2(a)), so \( B = k[y_1, \ldots, y_r] \).

Now let \( p > 0 \). Using similar arguments to those for \( p = 0 \), we show that the elements \( y_1, \ldots, y_r \) of a \( k \)-linear basis of \( B_1 \) together with some elements \( t_{r+1}, \ldots, t_m \in B_p \) form a minimal system of generators of the \( k \)-algebra \( B \). We can enlarge \( \{y_1, \ldots, y_r\} \) to a basis \( \{y_1, \ldots, y_m\} \) of \( k[X]_1 \). Let \( V = k[y_1, \ldots, y_r]_p + \langle y^p_{r+1}, \ldots, y^p_m \rangle_k \). Then \( V \subseteq B_p \), but we see that \( \dim_k V = \dim_k B_p \), so \( V = B_p \), that is, \( k[y_1, \ldots, y_r]_p + \langle y^p_{r+1}, \ldots, y^p_m \rangle_k = k[y_1, \ldots, y_r]_p + \langle t_{r+1}, \ldots, t_m \rangle_k \). This implies that \( B = k[y_1, \ldots, y_r, y^p_{r+1}, \ldots, y^p_m] \).

Recall the following fact.

**Proposition** ([3, 5.1.1], [2, 2.1]). Let \( k \subseteq k' \) be a field extension and let \( d \) be a \( k \)-derivation of a \( k \)-algebra \( A \). Denote by \( i \) the inclusion \( A^d \rightarrow A \). Then \( d' = 1 \otimes d \) is a \( k' \)-derivation of the \( k' \)-algebra \( A' = k' \otimes_k A \) and \( (1 \otimes i)(k' \otimes_k A^d) = A'^{d'} \).

The way of reducing an arbitrary linear derivation to its Jordan form is given in the following corollary of the above proposition and Proposition 2.4.

**Corollary 2.5.** If \( d \) is a \( k \)-derivation of \( k[X] \) and \( d' \) is a \( k' \)-derivation of \( k'[X] \) such that \( d'(x_i) = d(x_i) \) for \( i = 1, \ldots, m \), then the following conditions are equivalent:

(i) \( k[X]_d^d = k[y_1, \ldots, y_r, y^p_{r+1}, \ldots, y^p_m] \) for some \( k \)-linear basis \( y_1, \ldots, y_m \) of \( k[X]_1 \);

(ii) \( k'[X]_d^d = k'[z_1, \ldots, z_r, z^p_{r+1}, \ldots, z^p_m] \) for some \( k' \)-linear basis \( z_1, \ldots, z_m \) of \( k'[X]_1 \).

**3. The general case.** Now let \( d \) be a linear derivation of \( k[X] \). Using Corollary 2.5 for the algebraic closure \( \overline{k} \) of \( k \), Proposition 1.1 and Theorems 1.2 and 1.3 for the Jordan matrix of the endomorphism \( d|_{k[X]} \) over \( \overline{k} \), we obtain the following theorems.

**Theorem 3.1.** Let \( d \) be a linear derivation of \( k[X] \), where \( k \) is a field of characteristic 0. Then

\[
k[X]^d = k[y_1, \ldots, y_r]
\]

for some linearly independent homogeneous polynomials \( y_1, \ldots, y_m \) of degree 1 if and only if the Jordan matrix of \( d|_{k[X]} \) satisfies the following conditions.

(1) There are exactly \( r \) Jordan blocks with zero eigenvalues.
Nonzero eigenvalues of different Jordan blocks are pairwise different and linearly independent over $\mathbb{N}$.

At most one Jordan block with zero eigenvalue has dimension greater than 1, and if such a block exists, it is of dimension 2.

**Theorem 3.2.** Let $d$ be a linear derivation of $k[X]$, where $k$ is a field of characteristic $p > 0$. Then

$$k[X]^d = k[y_1, \ldots, y_r, y_{r+1}^p, \ldots, y_m^p]$$

for some $k$-linear basis $y_1, \ldots, y_m$ of $k[X]$ if and only if the Jordan matrix of $d|_{k[X]}$ satisfies the following conditions.

1. There are exactly $r$ Jordan blocks with zero eigenvalues.
2. Nonzero eigenvalues of different Jordan blocks are pairwise different and linearly independent over $\mathbb{F}_p$.
3. At most one Jordan block has dimension greater than 1, and if such a block exists, then its dimension is 2 in the case of $p > 2$, and 2 or 3 for $p = 2$.

Note that all the rings of constants mentioned in Theorems 3.1 and 3.2 are polynomial $k$-algebras. It is well known that in the case of char $k = 0$ there exist linear derivations of $k[X]$ with rings of constants being polynomial $k$-algebras not generated by linear forms. Let us end with the following question.

**Question.** Does there exist a linear derivation of $k[X]$, where char $k = p > 0$, such that $k[X]^d$ is a polynomial $k$-algebra not of the form mentioned in Theorem 3.2?

**REFERENCES**


Faculty of Mathematics and Computer Science
Nicolaus Copernicus University
Chopina 12/18
87-100 Toruń, Poland
E-mail: pjedrzej@mat.uni.torun.pl

*Received 13 September 2007; revised 6 February 2008*