Analytic and Algebraic Geometry
Łódź University Press 2013, 57 – 79
http://dx.doi.org/10.18778/7969-017-6.06

RINGS OF CONSTANTS OF POLYNOMIAL DERIVATIONS AND p-BASES

PIOTR JĘDRZEJEWICZ

Abstract. We present a survey of results concerning p-bases of rings of constants with respect to polynomial derivations in characteristic $p > 0$. We discuss characterizations of rings of constants, properties of their generators and a general characterization of their p-bases. We also focus on some special cases: one-element p-bases, eigenvector p-bases and when a ring of constants is a polynomial graded subalgebra.

Introduction

In Section 1 we introduce the notation and definitions concerning derivations, rings of constants and p-bases. Then we discuss characterizations of rings of constants in Section 2 and we present some basic information on the number of generators for rings of constants of polynomial derivations in Section 3. For a wider panorama of contemporary differential algebra we refer to the book of Nowicki ([41]), and for problems connected with locally nilpotent derivations we refer to the book of Freudenburg ([10]).

Next two sections contain a general characterization of p-bases of rings of constants with respect to polynomial derivations, based on the author's paper [26]. In Section 4 we present generalizations of Freudenburg's lemma (Theorems 4.7 and 4.8). The main theorem (Theorem 5.4) and its motivations are presented in Section 5. In Section 6 (based on the results of [23] and [18]) we discuss analogies and differences between single generators of rings of constants in zero and positive characteristic, and we focus on some special cases. Section 7, based on [24], is devoted to specific properties of eigenvector p-bases (Theorem 7.2). Finally, in

2010 *Mathematics Subject Classification.* Primary 13N15, Secondary 13F20.
Key words and phrases. Polynomial, derivation, ring of constants, p-basis.

Section 8 (based on the paper [28], joint with Nowicki) we describe rings of constants of homogeneous polynomial derivations in positive characteristic, which are polynomial algebras.

1. Basic definitions and notation

Throughout this article, by a ring we mean a commutative ring with unity, and by a domain we mean a commutative ring with unity, without zero divisors. If K is a ring, then by $K[x_1, \ldots, x_n]$ we denote a polynomial K-algebra. If R is a domain, then by R_0 we denote its field of fractions.

Let A be a domain. By A^* we denote the set of all invertible elements of A. We call two elements $a, b \in A$ associated and denote it by $a \sim b$, if $a = bc$ for some $c \in A^*$. An element $a \in A$ is called square-free if $b^2 \nmid a$ for every $b \in A \setminus A^*$.

Let A be a domain of characteristic $p > 0$. Then

$$A^p = \{a^p;\ a \in A\}$$

is a subring of A. Let B a subring of A, containing A^p. An element $a \in A$ is called B-free if $b \nmid a$ for every $b \in B \setminus A^*$. If $A = k[x_1, \ldots, x_n]$ is a polynomial algebra over a field k of characteristic $p > 0$, then $k[x_1^p, \ldots, x_n^p]$-free elements are called shortly p-free.

If A is a domain of characteristic $p > 0$ and B is a subring of A, containing A^p, then for elements $f_1, \ldots, f_m \in A$ we define the following subring of A:

$$C_B(f_1, \ldots, f_m) = B_0(f_1, \ldots, f_m) \cap A = B_0[f_1, \ldots, f_m] \cap A.$$

Note that the equality $B_0(f_1, \ldots, f_m) = B_0[f_1, \ldots, f_m]$ can easily be proved directly, but it also follows from the fact that the field extension $B_0 \subset B_0(f_1, \ldots, f_m)$ is algebraic.

Let A be a ring. An additive map $d\colon A \to A$ satisfying the Leibniz rule

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

for $f, g \in A$, is called a derivation of A. The set

$$A^d = \{f \in A :\ d(f) = 0\}$$

is called the ring of constants of d; it is a subring of A. Moreover, if A is a field, then A^d is a subfield of A.

If A is a K-algebra, where K is a ring, then a K-linear derivation $d\colon A \to A$ is called a K-derivation. In this case A^d is a K-subalgebra of A. When K is a subring of A, d is a K-derivation if and only if $K \subset A^d$.

If d is a K-derivation of a polynomial algebra $K[x_1, \ldots, x_n]$, where K is a ring, then

$$d(f) = \frac{\partial f}{\partial x_1} d(x_1) + \ldots + \frac{\partial f}{\partial x_n} d(x_n)$$

for every $f \in K[x_1, \ldots, x_n]$.

On the other hand, for arbitrary polynomials $g_1, \ldots, g_n \in K[x_1, \ldots, x_n]$ there exists exactly one K-derivation d of $K[x_1, \ldots, x_n]$ such that

$$\begin{cases} d(x_1) &= g_1 \\ & \vdots \\ d(x_n) &= g_n \end{cases}$$

and this derivation is of the form

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

Let A be a domain. Then every derivation $d\colon A \to A$ can be uniquely extended to a derivation $\delta\colon A_0 \to A_0$, which is defined by the formula

$$\delta\left(\frac{f}{g}\right) = \frac{d(f)g - fd(g)}{g^2}$$

for $f, g \in A$, $g \neq 0$. If A is a K-domain (that is, a K-algebra and a domain), where K is a domain, and d is a K-derivation, then δ is a K_0-derivation.

If A is a domain of characteristic $p > 0$ and $d\colon A \to A$ is a derivation, then $d(a^p) = 0$ for every $a \in A$, so $A^p \subset A^d$. If A is also a K-algebra, where K is a domain of characteristic $p > 0$, and d is a K-derivation, then $KA^p \subset A^d$, so d is a KA^p-derivation. For example, if A is a polynomial K-algebra: $A = K[x_1, \ldots, x_n]$, where $\operatorname{char} K = p > 0$, then $A^p = K^p[x_1^p, \ldots, x_n^p]$ and $KA^p = K[x_1^p, \ldots, x_n^p]$.

Lemma 1.1. *Let K be a domain of characteristic $p > 0$, consider a polynomial $f \in K[x_1, \ldots, x_n]$. Then $f \in K[x_1^p, \ldots, x_n^p]$ if and only if $\frac{\partial f}{\partial x_i} = 0$ for $i = 1, \ldots, n$.*

Recall the definition of a p-basis. We restrict our interests to finite p-bases, see [35], 38.A, p. 269, for a definition of a p-basis of arbitrary cardinality.

Definition 1.2. *Let R be a domain of characteristic $p > 0$ and B a subring of R, containing R^p. Let $f_1, \ldots, f_m \in R$.*

a) *The elements $f_1, \ldots, f_m$ are called p-independent over B if the elements of the form $f_1^{\alpha_1} \ldots f_m^{\alpha_m}$, where $\alpha_1, \ldots, \alpha_m \in \{0, \ldots, p-1\}$, are linearly independent over B.*

b) *We say that the elements $f_1, \ldots, f_m$ form a p-basis of R over B if R is a free B-module with a basis of the form*

$$f_1^{\alpha_1} \ldots f_m^{\alpha_m},$$

where $\alpha_1, \ldots, \alpha_m \in \{0, \ldots, p-1\}$.

Note that the elements $f_1, \dots, f_m$ form a p-basis of R over B if and only if they are p-independent over B and generate R as a B-algebra. If the elements $f_1, \dots, f_m$ form a p-basis of R over B, then every element $f \in R$ can be presented in the form

$$f = \sum_{0 \leqslant \alpha_1, \dots, \alpha_m < p} a_\alpha f_1^{\alpha_1} \dots f_m^{\alpha_m},$$

where $a_\alpha \in B$, and this presentation is unique.

The notion of a p-basis is a specific positive characteristic analog of a transcendental basis. It fits into the same abstract notion of dependency, see [52], II.12, p. 97 and II.17, p. 129.

Example 1.3. *The elements $x_1, \dots, x_n$ form:*

a) *a p-basis of $K[x_1, \dots, x_n]$ over $K[x_1^p, \dots, x_n^p]$,*

b) *a p-basis of $k(x_1, \dots, x_n)$ over $k(x_1^p, \dots, x_n^p)$,*

c) *a p-basis of $K[[x_1, \dots, x_n]]$ over $K[[x_1^p, \dots, x_n^p]]$,*

where K is a domain, k is a field, $\operatorname{char} K = \operatorname{char} k = p > 0$.

Theorem 1.4. ([15], p. 180)
If M is a subfield of a field L of characteristic $p > 0$, such that $L^p \subset M$, then there exists a p-basis (possibly infinite) of L over M.

Various conditions for existence of p-bases of ring extensions have been studied for a long time (see, for example, [46] and its references).

Given polynomials $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, where K is a ring, and $j_1, \dots, j_m \in \{1, \dots, n\}$, by $\operatorname{jac}_{j_1,\dots,j_m}^{f_1,\dots,f_m}$ we denote the Jacobian determinant of $f_1, \dots, f_m$ with respect to $x_{j_1}, \dots, x_{j_m}$. If $m = n$, then the Jacobian determinant of $f_1, \dots, f_n$ with respect to $x_1, \dots, x_n$ we denote by $\operatorname{jac}(f_1, \dots, f_n)$.

It is convenient to introduce the following notion of a differential gcd of polynomials $f_1, \dots, f_m \in K[x_1, \dots, x_n]$, where K is a UFD:

$$\operatorname{dgcd}(f_1, \dots, f_m) = \gcd\left(\operatorname{jac}_{j_1,\dots,j_m}^{f_1,\dots,f_m},\ j_1, \dots, j_m \in \{1, \dots, n\}\right).$$

We put $\operatorname{dgcd}(f_1, \dots, f_m) = 0$ if $\operatorname{jac}_{j_1,\dots,j_m}^{f_1,\dots,f_m} = 0$ for every $j_1, \dots, j_m$.

Note that $\operatorname{dgcd}(f_1, \dots, f_m)$ is defined up to a factor from K^*. We have

$$\operatorname{dgcd}(f) \sim \gcd\left(\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}\right)$$

for a single polynomial $f \in K[x_1, \dots, x_n]$ and

$$\operatorname{dgcd}(f_1, \dots, f_n) \sim \operatorname{jac}(f_1, \dots, f_n)$$

for n polynomials $f_1, \dots, f_n \in K[x_1, \dots, x_n]$.

From a generalized Laplace expansion we obtain the following ([26], Lemma 3.2).

Lemma 1.5. *Consider arbitrary pairwise different numbers $i_1, \ldots, i_r$ belonging to $\{1, \ldots, m\}$, where $1 \leqslant r \leqslant m$.*

a) *If* $\operatorname{dgcd}(f_{i_1}, \ldots, f_{i_r}) \neq 0$, *then* $\operatorname{dgcd}(f_{i_1}, \ldots, f_{i_r}) \mid \operatorname{dgcd}(f_1, \ldots, f_m)$.

b) *If* $\operatorname{dgcd}(f_{i_1}, \ldots, f_{i_r}) = 0$, *then* $\operatorname{dgcd}(f_1, \ldots, f_m) = 0$.

Recall the following known positive characteristic analog of the well known criterion of algebraic dependence in characteristic zero.

Lemma 1.6. *Let K be a domain of characteristic $p > 0$. Polynomials $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$ are p-dependent over $K[x_1^p, \ldots, x_n^p]$ if and only if $\operatorname{jac}_{j_1,\ldots,j_m}^{f_1,\ldots,f_m} = 0$ for every $j_1, \ldots, j_m \in \{1, \ldots, n\}$.*

2. Characterizations of rings of constants

Recall some characterizations of fields of constants with respect to derivations of fields. The case of characteristic zero was considered by Suzuki in [49] (Theorem 1) under the assumption of finite transcendence degree and genralized by Nowicki in [42], Theorem 4.2 (see also [41], Theorem 3.3.2).

Theorem 2.1. (Suzuki, Nowicki)
Let $K \subset L$ be an extension of fields of characteristic 0. A subfield $M \subset L$ such that $K \subset M$, is a field of constants of some K-derivation of L if and only if M is algebraically closed in L.

Similarly, in the positive characteristic case, Baer considered extensions of finite degree (see [15], IV.7, p. 185). Gerstenhaber proved the theorem in the general case in [12] (Remark at the end of Section 1) and, explicitly, in [13], Lemma 2.

Theorem 2.2. (Baer, Gerstenhaber)
Let $K \subset L$ be an extension of fields of characteristic $p > 0$ satisfying the condition $L^p \subset K$. Then every subfield $M \subset L$ such that $K \subset M$, is a field of constants of some K-derivation of L.

A characterization of rings of constants with respect to derivations of domains was obtained by Nowicki in [42], Theorem 5.4 (see also [41], Theorem 4.1.4).

Theorem 2.3. (Nowicki)
Let A be a finitely generated k-domain, where k is a field of characteristic zero. Let R be a k-subalgebra of A. The following conditions are equivalent:

(1) *R is the ring of constants of some k-derivation of A,*

(2) *R is integrally closed in A and $R_0 \cap A = R$.*

The author observed in [16] and, more generally, in [19], that analogous characterization (without the condition that R is integrally closed) holds in the positive characteristic case.

Theorem 2.4. ([16], Theorem 1.1, [19], Theorem 2.5)
Let A be a finitely generated K-domain, where K is a domain of characteristic $p > 0$. Let R be a subring of A. The following conditions are equivalent:

(1) *R is the ring of constants of some K-derivation of A,*

(2) *$KA^p \subset R$ and $R_0 \cap A = R$.*

The implications (1) $\Rightarrow$ (2) in Theorems 2.3 and 2.4 hold without the assumption A is finitely generated, and there are counter-examples to the reverse implications ([17], see Example 2.7 below).

Daigle noted ([5], 1.4) that the two conditions in (2) in Theorem 2.3 can be replaced by one condition of algebraic closedness (in the ring sense). The author observed in [22] that we can apply this condition to the positive characteristic case if we modify it to separable algebraic closedness. We call R separably algebraically closed in A, if each element of A, separably algebraic over R, belongs to R ([22], Definition 2.1).

Theorem 2.5. ([22], Theorem 3.1)
Let A be a finitely generated K-domain, where K is a domain (of arbitrary characteristic). Let R be a K-subalgebra of A. If $\operatorname{char} K = p > 0$, *we assume additionally that $A^p \subset R$ and we put $B = KA^p$. The following conditions are equivalent:*

(1) *R is the ring of constants of some K-derivation of A,*

(2) *R is separably algebraically closed in A,*

(3) *R is a maximal element in one of the following families of rings:*

$$\begin{cases} \Phi_m = \{R :\ K \subset R \subset A,\ \operatorname{tr\,deg}_K R \leqslant m\} & \text{if } \operatorname{char} A = 0, \\ \Psi_m = \{R :\ B \subset R \subset A,\ (R_0 : B_0) \leqslant p^m\} & \text{if } \operatorname{char} A = p > 0, \end{cases}$$

where $m = 0, 1, 2, \ldots$

Now, let A be a domain of characteristic $p > 0$ and let B be a subring of A, containing A^p. Consider arbitrary elements $f_1, \ldots, f_m \in A$. Recall a notation

$$C_B(f_1, \ldots, f_m) = B_0(f_1, \ldots, f_m) \cap A = B_0[f_1, \ldots, f_m] \cap A.$$

If A is finitely generated as a B-algebra, then $C_B(f_1, \ldots, f_m)$ is the smallest (with respect to inclusion) ring of constants of a B-derivation containing the elements $f_1, \ldots, f_m$. Under this assumption, the elements $f_1, \ldots, f_m$ form a p-basis (over B) of the ring of constants of some B-derivation if and only if $f_1, \ldots, f_m$ are p-independent over B and $C_B(f_1, \ldots, f_m) = B[f_1, \ldots, f_m]$.

Remark that the notion of the ring $C_k(f)$, for a polynomial f over a field k of characteristic 0, was introduced by Nowicki in [40].

Let k be a field of characteristic $p > 0$. Note that, if $f \notin k[x^p, y^p]$, then f is a one-element p-basis of $k[x^p, y^p, f]$.

Example 2.6. *Let d be a k-derivation of $k[x, y]$ such that*

$$\begin{cases} d(x) &= x \\ d(y) &= -y. \end{cases}$$

Then the polynomial xy is a (one-element) p-basis of $k[x, y]^d$:

$$k[x, y]^d = C_B(xy) = k[x^p, y^p, xy],$$

where $B = k[x^p, y^p]$.

The following example from [24] (Example 4.3), motivated by Examples 6, 7 from [17], shows that in Theorem 2.4 the assumption that A is finitely generated is necessary.

Example 2.7. *Let k be a field of characteristic $p > 0$, let $A = k[x_0, x_1, x_2, \dots]$ be a polynomial k-algebra, put $B = k[x_0^p, x_1^p, x_2^p, \dots]$. For $i = 1, 2, \dots$ put $f_i = x_i^{r_i} - x_0$, where $r_i > 1$ and $p \nmid r_i$. Consider the ring*

$$C_B(f_1, f_2, f_3, \dots) = B_0(f_1, f_2, f_3, \dots) \cap A.$$

Then:

a) *the polynomials $f_1, f_2, f_3, \dots$ form a p-basis of $C_B(f_1, f_2, f_3, \dots)$ over B,*

b) *$C_B(f_1, f_2, f_3, \dots)$ is not a ring of constants of any B-derivation of A.*

3. Generators of rings of constants

The case of characteristic zero. Let k be a field of characteristic 0.

Recall the following theorem of Zariski ([51]).

Theorem 3.1. (Zariski)
Let L be a subfield of $k(x_1, \dots, x_n)$ containing k. If $\operatorname{tr\,deg}_k L \leqslant 2$, then the ring

$$L \cap k[x_1, \dots, x_n]$$

is finitely generated over k.

Nowicki and Nagata in [43] (Theorem 2.6) applied Zariski's theorem to rings of constants of derivations.

Theorem 3.2. (Nowicki, Nagata)
Let d be a k-derivation of $k[x_1, \dots, x_n]$. If $n \leqslant 3$, then $k[x_1, \dots, x_n]^d$ is finitely generated over k.

The following example was obtained by Kuroda in [30] and [31] (see [10], 7.6, p. 175). This example is very important in the context of Hilbert's Fourteenth Problem. It solved the Problem for ordinary derivations, while for locally nilpotent derivations the case of $n = 4$ remains open (we refer to [10] for details).

Example 3.3. (Kuroda)
Let d be a k-derivation of $k[x, y, z, t]$ such that

$$\begin{cases} d(x) &= x(4x^4 - y^4 - z^4) \\ d(y) &= y(4y^4 - x^4 - z^4) \\ d(z) &= z(4z^4 - x^4 - y^4) \\ d(t) &= -20x^3y^3z^3. \end{cases}$$

Then $k[x, y, z, t]^d$ is not a finitely generated k-algebra.

Nowicki and Strelcyn in [44] constructed examples of k-derivations with arbitrary finite (minimal) number of generators of rings of constants.

Example 3.4. (Nowicki, Strelcyn)
Let $n \geqslant 3$ and $r \geqslant 0$. Then r is the minimal number of generators of $k[x_1, \ldots, x_n]^d$ as a k-algebra, for the following k-derivation d.

a) *Let $r < n$. Consider a k-derivation d such that $d(x_i) = 0$ if $i \leqslant r$ and $d(x_i) = x_i$ if $i > r$. Then*

$$k[x_1, \ldots, x_n]^d = k[x_1, \ldots, x_r].$$

b) *Let $r \geqslant n$. Consider a k-derivation d such that*

$$\begin{cases} d(x_1) &= x_1 \\ d(x_2) &= x_2 \\ d(x_3) &= (n - r - 2)x_3 \\ d(x_i) &= 0 \ \text{for} \ i > 3. \end{cases}$$

Then

$$k[x_1, \ldots, x_n]^d = k[f_0, f_1, \ldots, f_{r-n+2}, x_4, \ldots, x_n],$$

where $f_j = x_1^j x_2^{r-n+2-j} x_3$ for $j = 0, \ldots, r - n + 2$.

Now, recall the following theorem of Zaks ([50]).

Theorem 3.5. (Zaks)
If R is a Dedekind subring of $k[x_1, \ldots, x_n]$ containing k, then $R = k[f]$ for some $f \in k[x_1, \ldots, x_n]$.

Using Zaks' theorem, Nowicki and Nagata proved ([43], Theorem 2.8, [41], Theorem 7.1.4, Corollary 7.1.5) the following.

Theorem 3.6. (Nowicki, Nagata)
If d is a k-derivation of $k[x_1, \ldots, x_n]$, such that $\operatorname{tr\,deg}_k k[x_1, \ldots, x_n]^d \leqslant 1$, then $k[x_1, \ldots, x_n]^d = k[f]$ for some $f \in k[x_1, \ldots, x_n]$.

Corollary 3.7. *If d is a nonzero k-derivation of $k[x,y]$, then $k[x,y]^d = k[f]$ for some $f \in k[x,y]$.*

Note also in this context Miyanishi's theorem ([36], see [10], Theorem 5.1, p. 108).

Theorem 3.8. (Miyanishi)
If d is a nonzero locally nilpotent k-derivation of $k[x,y,z]$, then $k[x,y,z]^d = k[f,g]$ for some algebraically independent $f, g \in k[x,y,z]$.

The case of positive characteristic. Now, let k be a field of characteristic $p > 0$.

Recall the results of Nowicki and Nagata ([43], Proposition 4.1, Proposition 4.2).

Theorem 3.9. (Nowicki, Nagata)
If d is a k-derivation of $k[x_1,\dots,x_n]$, then $k[x_1,\dots,x_n]^d$ is finitely generated as a $k[x_1^p,\dots,x_n^p]$-algebra.

Theorem 3.10. (Nowicki, Nagata)
If $\operatorname{char} k = 2$ and d is a nonzero k-derivation of $k[x,y]$, then there exists a polynomial $f \in k[x,y]$ such that $k[x,y]^d = k[x^2, y^2, f]$.

Nowicki and Nagata proved that, if $p > 2$, the ring of constants of the Euler's derivation in $k[x,y]$ is not of the form $k[x^p, y^p, f]$ for any polynomial $f \in k[x,y]$ ([43], Example 4.3). Li in [34] proved that in this case $p-1$ is the minimal number of generators of $k[x,y]^d$ as a $k[x^p,y^p]$-algebra.

Example 3.11. *Let d be a k-derivation of $k[x,y]$ such that*

$$\begin{cases} d(x) &= x \\ d(y) &= y. \end{cases}$$

Then, for $B = k[x^p, y^p]$ we have:

$$k[x,y]^d = C_B(x^{p-1}y) = k[x^p, x^{p-1}y, \dots, xy^{p-1}, y^p].$$

Li in [33] (Theorem) obtained the following generalization of Theorem 3.10 for arbitrary characteristic $p > 0$.

Theorem 3.12. (Li)
Let d be a nonzero k-derivation of $k[x,y]$. Then:

a) *$k[x,y]^d$ is a free $k[x^p,y^p]$-module of rank p or 1,*

b) *there exist $g_1,\dots,g_{p-1} \in k[x,y]$ such that $k[x,y]^d = k[x^p, y^p, g_1, \dots, g_{p-1}]$.*

Note also that Nowicki and Nagata gave an example of a derivation, which ring of constants is not a free module ([43], Example 4.6).

Example 3.13. *Let $n \geqslant 3$ and let d be a k-derivation of $k[x_1,\dots,x_n]$ such that $d(x_i) = x_i^p$ for $i = 1,\dots,n$. Then $k[x_1,\dots,x_n]^d$ is not a free $k[x_1^p,\dots,x_n^p]$-module.*

4. Freudenburg's lemma

The key preparatory fact for the main characterization of p-bases of rings of constants with respect to polynomial derivations (Theorem 5.4) is a positive characteristic generalization of the following lemma, obtained by Freudenburg in [9].

Lemma 4.1. (Freudenburg)
Given a polynomial $f \in \mathbb{C}[x,y]$, suppose $g \in \mathbb{C}[x,y]$ is an irreducible non-constant divisor of both $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$. Then there exists $c \in \mathbb{C}$ such that g divides $f + c$.

This lemma was generalized by van den Essen, Nowicki and Tyc in [8], Proposition 2.1.

Proposition 4.2. (van den Essen, Nowicki, Tyc)
Let k be an algebraically closed field of characteristic zero. Let Q be a prime ideal in $k[x_1,\ldots,x_n]$ and $f \in k[x_1,\ldots,x_n]$. If for each i the partial derivative $\frac{\partial f}{\partial x_i}$ belongs to Q, then there exists $c \in k$ such that $f - c \in Q$.

The following example from [8], Remark 2.4, shows that the condition that k is algebraically closed can not be dropped in the above theorem. We can, however, make a positive conclusion, as in point b).

Example 4.3. *Consider polynomials $f = x^3 + 3x$, $g = x^2 + 1 \in \mathbb{R}[x]$. Then g is irreducible, $g \mid f'$ and:*

a) *$g \nmid f - c$ for any $c \in \mathbb{R}$,*

b) *$g \mid f^2 + 4$, where $w(x) = x^2 + 4$ is irreducible.*

Note the following generalization of the Freudenburg's lemma for a UFD of arbitrary characteristic.

Proposition 4.4. ([21], Theorem 3.1)
Let K be a UFD, let Q be a prime ideal of $K[x_1,\ldots,x_n]$. Consider a polynomial $f \in K[x_1,\ldots,x_n]$ such that $\frac{\partial f}{\partial x_i} \in Q$ for $i = 1,\ldots,n$.

a) *If $\operatorname{char} K = 0$, then there exists an irreducible polynomial $w(x) \in K[x]$ such that $w(f) \in Q$.*

b) *If $\operatorname{char} K = p > 0$, then there exist $b, c \in K[x_1^p,\ldots,x_n^p]$ such that $\gcd(b,c) \sim 1$, $b \notin Q$ and $bf + c \in Q$.*

Now, let K be a UFD of characteristic $p > 0$.

Lemma 4.5. *Let $f \in K[x_1,\ldots,x_n]$ and let $g \in K[x_1,\ldots,x_n]$ be an irreducible polynomial. If $g \mid f$ and $g \mid \frac{\partial f}{\partial x_i}$ for every i, then $g^2 \mid f$ or $g \in K[x_1^p,\ldots,x_n^p]$.*

In the case of a principal ideal in positive characteristic we obtain from Proposition 4.4 the following equivalence.

Corollary 4.6. *Consider a polynomial $f \in K[x_1, \ldots, x_n]$ and an irreducible polynomial $g \in K[x_1, \ldots, x_n]$. The following conditions are equivalent:*

(1) $g \mid \frac{\partial f}{\partial x_i}$ *for* $i = 1, \ldots, n$,

(2) *there exist* $b, c \in K[x_1^p, \ldots, x_n^p]$ *such that* $g \nmid b$, $\gcd(b, c) \sim 1$ *and*

$$\begin{cases} g^2 \mid bf + c & \text{if } g \notin K[x_1^p, \ldots, x_n^p], \\ g \mid bf + c & \text{if } g \in K[x_1^p, \ldots, x_n^p]. \end{cases}$$

Now we are going to present generalizations of Freudenburg's lemma for an arbitrary number of polynomials instead of one. Theorem 4.7 is a generalization of Proposition 4.4 b), and Theorem 4.8 is a generalization of Corollary 4.6.

Theorem 4.7. ([26], Proposition 3.5)
Let $A = K[x_1, \ldots, x_n]$ be a polynomial K-algebra, where K is a UFD of characteristic $p > 0$. Put $B = K[x_1^p, \ldots, x_n^p]$. Let $f_1, \ldots, f_m \in A$, $m \geqslant 1$, and let Q be a prime ideal of A. If $\operatorname{jac}_{j_1,\ldots,j_m}^{f_1,\ldots,f_m} \in Q$ *for every $j_1, \ldots, j_m \in \{1, \ldots, n\}$, then there exist $i \in \{1, \ldots, m\}$ and*

$$b, c \in B[f_1, \ldots, \widehat{f_i}, \ldots, f_m],$$

$b \notin Q$, such that $bf_i + c \in Q$.

Proof. (Sketch.)
Consider the factor algebra $\overline{A} = A/Q$ and denote $\overline{f} = f + Q$ for an element $f \in A$, and by $\overline{T}$ the canonical homomorphic image in $\overline{A}$ of a subring $T \subset A$.

If $\operatorname{jac}_{j_1,\ldots,j_m}^{f_1,\ldots,f_m} \in Q$ for every $j_1, \ldots, j_m \in \{1, \ldots, n\}$, then the rank of the matrix

$$\begin{bmatrix} \overline{\partial f_1/\partial x_1} & \overline{\partial f_1/\partial x_2} & \cdots & \overline{\partial f_1/\partial x_n} \\ \overline{\partial f_2/\partial x_1} & \overline{\partial f_2/\partial x_2} & \cdots & \overline{\partial f_2/\partial x_n} \\ \vdots & \vdots & & \vdots \\ \overline{\partial f_m/\partial x_1} & \overline{\partial f_m/\partial x_2} & \cdots & \overline{\partial f_m/\partial x_n} \end{bmatrix}$$

over the field $(\overline{A})_0$ is less than m. From the linear dependence of the rows of this matrix we infer that:

$(*)$ there exist $s_1, \ldots, s_m \in A$, where $s_i \notin Q$ for some $i \in \{1, \ldots, m\}$, such that $s_1 d(f_1) + \ldots + s_m d(f_m) \in Q$ for every K-derivation d of A.

Now, denote $R_i = B[f_1, \ldots, \widehat{f_i}, \ldots, f_m]$. For every $\overline{R_i}$-derivation δ of $\overline{A}$ there exists a K-derivation d of A such that $\delta(\overline{f}) = \overline{d(f)}$ for every $f \in A$ ([21], Lemma 3.2). Then, by $(*)$, $d(f_i) \in Q$, so $\delta(\overline{f_i}) = \overline{0}$. Hence, $\overline{f_i}$ belongs to $(\overline{R_i})_0 \cap \overline{A}$ – the smallest ring of constants of any $\overline{R_i}$-derivation of $\overline{A}$, so there exist $b, c \in R_i$ such that $\overline{b} \neq \overline{0}$ and $\overline{f_i} = -\frac{\overline{c}}{\overline{b}}$. □

Theorem 4.8. ([26], Theorem 3.6)
Let K be a UFD of characteristic $p > 0$. Let $A = K[x_1, \ldots, x_n]$, put $B = K[x_1^p, \ldots, x_n^p]$. Consider arbitrary polynomials $f_1, \ldots, f_m \in A$, where $m \geqslant 1$, and denote

$$R_i = B[f_1, \ldots, \widehat{f_i}, \ldots, f_m]$$

for $i = 1, \ldots, m$, and, if $m > 1$,

$$R_{ij} = B[f_1, \ldots, \widehat{f_i}, \ldots, \widehat{f_j}, \ldots, f_m]$$

for $i, j = 1, \ldots, m$, such that $i \neq j$.

Then $\operatorname{dgcd}(f_1, \ldots, f_m)$ *is divisible by an irreducible polynomial $g \in A$ if and only if at least one of the following conditions holds:*

(i) $g \notin B$ *and* $g^2 \mid bf_i + c$ *for some* $i \in \{1, \ldots, m\}$ *and* $b, c \in R_i$ *such that* $g \nmid b$,

(ii) $g \in B$ *and* $g \mid bf_i + c$ *for some* $i \in \{1, \ldots, m\}$ *and* $b, c \in R_i$ *such that* $g \nmid b$,

(iii) $g \mid b_1 f_i + c_1$ *and* $g \mid b_2 f_j + c_2$ *for some* $i, j \in \{1, \ldots, m\}$, $i \neq j$, *and* $b_1, b_2, c_1, c_2 \in R_{ij}$ *such that* $g \nmid b_1$ *and* $g \nmid b_2$.

Proof. (Sketch.)
($\Rightarrow$) If $\operatorname{dgcd}(f_1, \ldots, f_m)$ is divisible by an irreducible polynomial $g \in A$, then $\operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_m} \in (g)$ for every $j_1, \ldots, j_m \in \{1, \ldots, n\}$. Hence, by Theorem 4.7, $bf_i + c = gh$ for some $i \in \{1, \ldots, m\}$, $b, c \in R_i$ such that $g \nmid b$, and $h \in A$.

The condition (i) holds if $g \notin B$ and $g \mid h$, and the condition (ii) holds if $g \in B$, so we assume that $g \notin B$ and $g \nmid h$. Applying, for arbitrary $j_1, \ldots, j_m \in \{1, \ldots, n\}$, the Jacobian derivation d_i defined by

$$d_i(f) = \operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_{i-1}, f, f_{i+1}, \ldots, f_m},$$

we infer that $g \mid \operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_{i-1}, g, f_{i+1}, \ldots, f_m}$. Then the condition $(*)$ from the proof of Theorem 4.7 holds for polynomials $f_1, \ldots, f_{i-1}, g, f_{i+1}, \ldots, f_m$, where (one can show that) $g \nmid s_j$ for some $j \neq i$, so since $\overline{g} = \overline{0}$, we obtain that $\overline{f_j} \in (\overline{R_{ij}})_0$. Recall that $\overline{f_i} \in (\overline{R_i})_0$, but $R_i = R_{ij}[f_j]$, so $\overline{f_i} \in (\overline{R_{ij}})_0$, and then (iii) holds.

($\Leftarrow$) If $bf_i + c = g^2 h$ for some irreducible polynomial $g \in A \setminus B$, some $h \in A$ and $b, c \in R_i$ such that $g \nmid b$, then we apply the derivation d_i defined above, and obtain that $g \mid \operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_m}$ for arbitrary $j_1, \ldots, j_m \in \{1, \ldots, n\}$, so $g \mid \operatorname{dgcd}(f_1, \ldots, f_m)$. We proceed similarly, if (ii) holds.

If $g \mid b_1 f_i + c_1$ and $g \mid b_2 f_j + c_2$ for some irreducible polynomial g, $i \neq j$ and $b_1, b_2, c_1, c_2 \in R_{ij}$ such that $g \nmid b_1$ and $g \nmid b_2$, then $g \mid \operatorname{dgcd}(b_1 f_i + c_1, b_2 f_j + c_2)$, so

$$g \mid \operatorname{dgcd}(f_1, \ldots, b_1 f_i + c_1, \ldots, b_2 f_j + c_2, \ldots, f_m)$$

by Lemma 1.5. Then we show that

$$\operatorname{dgcd}(f_1, \ldots, b_1 f_i + c_1, \ldots, b_2 f_j + c_2, \ldots, f_m)$$

$$= b_1 b_2 \operatorname{dgcd}(f_1, \ldots, f_i, \ldots, f_j, \ldots, f_m)$$

and obtain the conclusion: $g \mid \operatorname{dgcd}(f_1, \ldots, f_m)$. □

Let us remark that the zero characteristic analog of Theorem 4.8 for $m = n$ ([25], Theorem 4.1) is connected with a characterization of Keller maps and an equivalent formulation of the Jacobian Conjecture.

5. A characterization of p-bases of rings of constants

A characterization of p-bases of the whole polynomial algebra $k[x_1, \ldots, x_n]$ was obtained by Nousiainen in [39], see Niitsuma, [37] or [38].

Theorem 5.1. (Nousiainen)
Given polynomials $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$, where k is a field of characteristic $p > 0$, the following conditions are equivalent:

(1) *there exist k-derivations $d_1, \ldots, d_n$ of $k[x_1, \ldots, x_n]$ such that $d_i(f_j) = \delta_{ij}$ (the Kronecker delta) for $i, j = 1, \ldots, n$,*

(2) *there exist k-derivations $d_1, \ldots, d_n$ of $k[x_1, \ldots, x_n]$ such that $\det(d_i(f_j)) \in k \setminus \{0\}$,*

(3) *the Jacobian matrix $\left[\dfrac{\partial f_i}{\partial x_j}\right]$ is invertible,*

(4) *$k[x_1, \ldots, x_n] = k[x_1^p, \ldots, x_n^p, f_1, \ldots, f_n]$,*

(5) *the polynomials $f_1, \ldots, f_n$ form a p-basis of $k[x_1, \ldots, x_n]$ over $k[x_1^p, \ldots, x_n^p]$.*

Note that Lang and Mandal obtained in [32], Theorem 2.2, some other equivalent conditions in terms of Jacobian derivations.

Nousiainen's theorem is connected with the positive characteristic version of the Jacobian Conjecture formulated by Adjamagbo ([1], see [7], 10.3.16, p. 261).

Conjecture 5.2. *Let $f_1, \ldots, f_n \in \mathbb{F}_p[x_1, \ldots, x_n]$. If $\operatorname{jac}(f_1, \ldots, f_n) \in \mathbb{F}_p \setminus \{0\}$ and p does not divide the degree of the field extension $\mathbb{F}_p(f_1, \ldots, f_n) \subset \mathbb{F}_p(x_1, \ldots, x_n)$, then $\mathbb{F}_p[f_1, \ldots, f_n] = \mathbb{F}_p[x_1, \ldots, x_n]$.*

Theorem 5.3. (Adjamagbo, [1], see [7], 10.3.17, p. 261)
If the above conjecture is true for all $n \geqslant 1$ and all primes p, then the Jacobian Conjecture is true.

Now we present a general theorem about p-bases of rings of constants of polynomial derivations. In the case $m = n$ it extends the Nousiainen's theorem with the condition (3) below.

Theorem 5.4. ([26], Theorem 4.4)
Let K be a UFD of characteristic $p > 0$, let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$, where $m \in \{1, \ldots, n\}$. Denote: $B = K[x_1^p, \ldots, x_n^p]$, $R_i = B[f_1, \ldots, \widehat{f_i}, \ldots, f_m]$ for $i = 1, \ldots, m$, and $R_{ij} = B[f_1, \ldots, \widehat{f_i}, \ldots, \widehat{f_j}, \ldots, f_m]$ for $i, j = 1, \ldots, m$, such that $i \neq j$.

The following conditions are equivalent:

(1) $\operatorname{dgcd}(f_1, \ldots, f_m) \sim 1$,

(2) *the polynomials $f_1, \ldots, f_m$ form a p-basis of the ring of constants of some K-derivation,*

(3) *the polynomial $bf_i + c$ is square-free and B-free for every $i \in \{1, \ldots, m\}$ and $b, c \in R_i$ such that $\gcd(b, c) \sim 1$, and, if $m > 1$, then $\gcd(b_1 f_i + c_1, b_2 f_j + c_2) \sim 1$ for every $i, j \in \{1, \ldots, m\}$, $i \neq j$, and $b_1, b_2, c_1, c_2 \in R_{ij}$ such that $\gcd(b_1, c_1) \sim 1$ and $\gcd(b_2, c_2) \sim 1$.*

Proof. (Sketch.)
(1) $\Rightarrow$ (2) Assume that $\operatorname{dgcd}(f_1, \ldots, f_m) \sim 1$. By Lemma 1.6, $f_1, \ldots, f_m$ are p-independent over B. We will show that for every $b \in B \setminus \{0\}$ and $a_\alpha \in B$, $0 \leqslant \alpha_1, \ldots, \alpha_m < p$, the following holds:

$(*)$ if $b \mid \sum_{0 \leqslant \alpha_1, \ldots, \alpha_m < p} a_\alpha f_1^{\alpha_1} \ldots f_m^{\alpha_m}$, then $b \mid a_\alpha$ for every $\alpha_1, \ldots, \alpha_m \in \{0, \ldots, p-1\}$.

Denote by s the maximal sum $\alpha_1 + \ldots + \alpha_m$ such that $a_\alpha \neq 0$. If $s = 0$, $(*)$ holds. Assume that $s > 0$ and $(*)$ holds for $s - 1$. Let $b \mid \sum_{0 \leqslant \alpha_1, \ldots, \alpha_m < p} a_\alpha f_1^{\alpha_1} \ldots f_m^{\alpha_m}$. Applying, for each i, the Jacobian derivation d_i defined by

$$d_i(f) = \operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_{i-1}, f, f_{i+1}, \ldots, f_m},$$

we obtain that $b \mid \sum_{0 \leqslant \alpha_1, \ldots, \alpha_m < p} \alpha_i a_\alpha f_1^{\alpha_1} \ldots f_i^{\alpha_i - 1} \ldots f_m^{\alpha_m} \operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_m}$. Then

$$b \mid \sum_{0 \leqslant \alpha_1, \ldots, \alpha_m < p} \alpha_i a_\alpha f_1^{\alpha_1} \ldots f_i^{\alpha_i - 1} \ldots f_m^{\alpha_m},$$

because $\gcd\left(\operatorname{jac}_{j_1, \ldots, j_m}^{f_1, \ldots, f_m},\ j_1, \ldots, j_m \in \{1, \ldots, n\}\right) \sim 1$, and it is enough to use the induction hypotheses.

Now, observe that any element of the ring

$$C_B(f_1, \ldots, f_m) = B_0[f_1, \ldots, f_m] \cap A$$

is the form $\sum_{0 \leqslant \alpha_1, \ldots, \alpha_m < p} \frac{a_\alpha}{b} f_1^{\alpha_1} \ldots f_m^{\alpha_m}$, where $b \in B \setminus \{0\}$, $a_\alpha \in B$, so, by $(*)$, it belongs to $B[f_1, \ldots, f_m]$.

(2) $\Rightarrow$ (3) Assume that $f_1, \ldots, f_m$ form a p-basis of the ring $R = C_B(f_1, \ldots, f_m)$.

If $g^2 \mid bf_i + c$ for some $i \in \{1, \dots, m\}$, $b, c \in R_i$ such that $\gcd(b, c) \sim 1$, and a noninvertible polynomial g, then one can show that the polynomial $\frac{1}{g^p} \cdot (bf + c)^{p-1}$ belongs to R and does not belong to $B[f_1, \dots, f_m]$.

If $g \mid bf_i + c$ for some $i \in \{1, \dots, m\}$, $b, c \in R_i$ such that $\gcd(b, c) \sim 1$, and a noninvertible polynomial $g \in B$, then $\frac{bf+c}{g} \in R \setminus B[f_1, \dots, f_m]$.

If $g \mid b_1 f_i + c_1$ and $g \mid b_2 f_j + c_2$ for some $i, j \in \{1, \dots, m\}$, $i \neq j$, $b_1, b_2, c_1, c_2 \in R_{ij}$ such that $\gcd(b_1, c_1) \sim 1$, $\gcd(b_2, c_2) \sim 1$ and a noninvertible polynomial g, then $\frac{1}{g^p} \cdot (b_1 f_i + c_1)^{p-1}(b_2 f_j + c_2) \in R \setminus B[f_1, \dots, f_m]$.

$\neg(1) \Rightarrow \neg(3)$ If $g \mid \operatorname{dgcd}(f_1, \dots, f_m)$ for irreducible polynomial g, then at least one of the conditions (i), (ii), (iii) of Theorem 4.8 holds. Now, if $bf_i + c$ is divisible by g or by g^2, it is enough to take h – a product of g and all (if any) irreducible factors of b, which do not divide c, and then $bf_i + c + h^p$ remains being divisible by g, resp. by g^2, but $\gcd(b, c + h^p) \sim 1$. □

6. Closed polynomials and one-element p-bases

The properties of single generators of rings of constants were studied by many authors.

Theorem 6.1. (Nowicki, Nagata, Ayad, Arzhantsev, Petravchuk)
Let k be a field, let $f \in k[x_1, \dots, x_n] \setminus k$. Denote by $\overline{k}$ the algebraic closure of k. Consider the following conditions:

(1) *$k[f]$ is the ring of constants of some k-derivation of $k[x_1, \dots, x_n]$,*

(2) *$k[f]$ is integrally closed in $k[x_1, \dots, x_n]$,*

(3) *$k[f]$ is a maximal element (with respect to inclusion) of the family $\{k[g];\ g \in k[x_1, \dots, x_n]\}$,*

(4) *for some $c \in \overline{k}$ the polynomial $f + c$ is irreducible over $\overline{k}$,*

(5) *for all but finitely many $c \in \overline{k}$ the polynomial $f + c$ is irreducible over $\overline{k}$.*

a) *If $\operatorname{char} k = 0$, then the conditions* (1) – (5) *are equivalent.*

b) *If k is a perfect field, then the conditions* (2) – (5) *are equivalent.*

c) *For arbitrary field the conditions* (2) *and* (3) *are equivalent.*

Nowicki and Nagata proved the equivalence of the conditions (1), (2) and (3) in characteristic zero ([40], Theorem 2.1; [41], Proposition 5.2.1; [43], Lemma 3.1). Ayad added the condition (4) in $\operatorname{char} k = 0$ ([3], Théorème 8, Remarque), based on the theorem of Płoski ([47], see [48], 3.3, Corollary 1, p. 220), and observed that the

equivalence (2) $\Leftrightarrow$ (3) holds also for $\operatorname{char} k = p > 0$. Arhzantsev and Petravchuk ([2], Theorem 1) considered the case of a perfect field and added the condition (5).

Note also that Nowicki and Nagata in [40] and [43] defined a closed polynomial in characteristic zero as a polynomial f satisfying the condition (3) above.

Now, let k be a field of characteristic $p > 0$.

Consider the following families of subrings of $k[x_1, \ldots, x_n]$:

$$\begin{aligned}
\mathcal{A} &= \{k[g];\ g \in k[x_1, \ldots, x_n]\},\\
\mathcal{B} &= \{k[x_1^p, \ldots, x_n^p, g];\ g \in k[x_1, \ldots, x_n]\},\\
\mathcal{C} &= \{R \subset k[x_1, \ldots, x_n] :\ k[x_1^p, \ldots, x_n^p] \subset R,\ (R_0 : k(x_1^p, \ldots, x_n^p)) = p\},
\end{aligned}$$

where $(L : K)$ denotes the degree of a field extension $K \subset L$.

The family $\mathcal{A}$ plays its role in characteristic zero, the family $\mathcal{B}$ is a natural positive characteristic analog, since rings of constants are $k[x_1^p, \ldots, x_n^p]$-algebras. The family $\mathcal{C}$, however, has the property that its maximal elements are rings of constants (see Theorem 2.5).

Note that we do not have any implication, in general, between the maximality of respective rings in $\mathcal{A}$ and in $\mathcal{B}$ ([23], Examples 2.1, 2.2), and even the maximality in $\mathcal{C}$ does not imply, in general, the maximality in $\mathcal{A}$. Moreover, the maximality in $\mathcal{B}$ does not imply, in general, the maximality in $\mathcal{C}$ ([23], Example 2.3). The only implication is that if an element of $\mathcal{B}$ is maximal in $\mathcal{C}$, then it is also maximal in $\mathcal{B}$.

Example 6.2. a) *Put $f_1 = x_1^p x_2$. Then the ring $k[f_1]$ is maximal in $\mathcal{A}$, and the ring $k[x_1^p, \ldots, x_n^p, f_1]$ is not maximal in $\mathcal{B}$.*

b) *Put $f_2 = x_1 + x_1^p$. Then the ring $k[x_1^p, \ldots, x_n^p, f_2]$ is maximal in $\mathcal{B}$ and in $\mathcal{C}$, and the ring $k[f_2]$ is not maximal in $\mathcal{A}$.*

c) *Put $f_3 = x_1^{p-1} x_2$. Then the ring $k[x_1^p, \ldots, x_n^p, f_3]$ is maximal in $\mathcal{B}$, and is not maximal in $\mathcal{C}$.*

Now we are going to analyze a characterization of single generators of rings of constants. In order to understand better the condition (3) in Theorem 6.4 below, observe the following positive characteristic analog of a known property of polynomials. Recall that k denotes a field of characteristic $p > 0$.

Lemma 6.3. *Consider a polynomial $f \in k[x_1, \ldots, x_n] \setminus k[x_1^p, \ldots, x_n^p]$. Then*

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) \sim 1$$

if and only if f is square-free and p-free.

From Theorem 5.4 in the case of $m = 1$ we have the following.

Theorem 6.4. ([21], Theorem 4.2)
Let $f \in k[x_1, \ldots, x_n] \setminus k[x_1^p, \ldots, x_n^p]$. The following conditions are equivalent:

(1) $\gcd\left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) \sim 1$,

(2) *$k[x_1^p, \ldots, x_n^p, f]$ is the ring of constants of a k-derivation,*

(3) *for every $b, c \in k[x_1^p, \ldots, x_n^p]$ such that $\gcd(b, c) \sim 1$, the polynomial $bf + c$ is square-free and p-free.*

It is easy to see that

$$\gcd\left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) \mid d(f)$$

for every k-derivation d of $k[x_1, \ldots, x_n]$ and a polynomial $f \in k[x_1, \ldots, x_n] \setminus k[x_1^p, \ldots, x_n^p]$. If $d(f) = cf$ for some $c \in k \setminus \{0\}$, then

$$\gcd\left(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) \sim \gcd\left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right).$$

Hence, we obtain the following fact.

Corollary 6.5. *Let $f \in k[x_1, \ldots, x_n] \setminus k[x_1^p, \ldots, x_n^p]$. Assume that $d(f) = cf$ for some $c \in k \setminus \{0\}$. Then $k[x_1^p, \ldots, x_n^p, f]$ is a ring of constants of a k-derivation if and only if the polynomial f is square-free and p-free.*

Finally, observe a list of monomial derivations in two variables with one-element p-bases of rings of constants. The motivation was connected with the paper of Okuda ([45]), who adapted van den Essen's algorithm ([6], see [7], 1.4, p. 37) to positive characteristic. Recall that k denotes a field of characteristic $p > 0$.

Example 6.6. ([18], Example 13)
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:

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

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

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

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

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

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

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

Theorem 6.7. ([18], Theorem 16)
Let d be a monomial k-derivation of $k[x,y]$:

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

where $\alpha, \beta \in k$. Then

$$k[x,y]^d = k[x^p, y^p, f]$$

for some $f \in k[x,y] \setminus k[x^p, y^p]$ if and only if $d = x^j y^l \cdot d_i$, where $j, l \geqslant 0$, $i \in \{1, 2, \ldots, 7\}$, and the derivation d_i is as in Example 6.6.

7. Eigenvector p-bases

Recall the Moore's determinant (see, for example, [14], Corollary 1.3.7, p. 8).

Lemma 7.1. *Let k be a field of characteristic $p > 0$, let $c_1, \ldots, c_m \in k$, $m > 1$. Then*

$$\begin{vmatrix} c_1 & c_1^p & \cdots & c_1^{p^{m-1}} \\ c_2 & c_2^p & \cdots & c_2^{p^{m-1}} \\ \vdots & \vdots & & \vdots \\ c_m & c_m^p & \cdots & c_m^{p^{m-1}} \end{vmatrix} = \prod_{i=1}^{m} \prod_{\alpha_1, \ldots, \alpha_{i-1} \in \mathbb{F}_p} (\alpha_1 c_1 + \ldots + \alpha_{i-1} c_{i-1} + c_i).$$

Recall also a notation

$$\operatorname{dgcd}(f_1, \ldots, f_m) = \gcd\left(\operatorname{jac}^{f_1, \ldots, f_m}_{j_1, \ldots, j_m},\ j_1, \ldots, j_m \in \{1, \ldots, n\}\right).$$

The following theorem, taking into consideration Theorem 5.4, is motivated by Corollary 6.5.

Theorem 7.2. ([24], Theorem 3.2)
Let k be a field of characteristic $p > 0$, consider polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \setminus \{0\}$, where $m > 1$. Assume that $f_1, \ldots, f_m$ are eigenvectors of some k-derivation of $k[x_1, \ldots, x_n]$ and their eigenvalues are linearly independent over the prime subfield $\mathbb{F}_p$. Then $f_1, \ldots, f_m$ are p-independent over $k[x_1^p, \ldots, x_n^p]$, and the following conditions are equivalent:

(1) *$k[x_1^p, \ldots, x_n^p, f_1, \ldots, f_m]$ is the ring of constants of some k-derivation,*

(2) $f_1, \dots, f_m$ *are pairwise coprime, square-free and p-free,*

(3) $\operatorname{dgcd}(f_1, \dots, f_m) \sim 1$,

(4) $\operatorname{dgcd}(f_{i_1}, f_{i_2}) \sim 1$ *for every* $i_1 \neq i_2$.

Proof. (Sketch.)
Let Δ be a k-derivation such that $\Delta(f_i) = c_i f_i$, where $c_i \in k$ for $i = 1, \dots, m$, and $c_1, \dots, c_m$ are linearly independent over $\mathbb{F}_p$. Consider k-derivations $d_j = \Delta^{p^{j-1}}$, $j = 1, \dots, m$.

Consider the matrix

$$M = \begin{bmatrix} d_1(f_1) & d_2(f_1) & \cdots & d_m(f_1) \\ d_1(f_2) & d_2(f_2) & \cdots & d_m(f_2) \\ \vdots & \vdots & & \vdots \\ d_1(f_m) & d_2(f_m) & \cdots & d_m(f_m) \end{bmatrix}.$$

We have $d_j(f_i) = c_i^{p^{j-1}} f_i$ for $i, j \in \{1, \dots, m\}$, so $\det M = c f_1 \dots f_m$, where c is the value of the Moore's determinant from Lemma 7.1, $c \in k$. Since $c_1, \dots, c_m$ are linearly independent over $\mathbb{F}_p$, we have $c \neq 0$ and $\det M \neq 0$.

On the other hand, one can show that

$$\det M = \sum_{j_1, \dots, j_m \in \{1, \dots, n\}} d_1(x_{j_1}) \dots d_m(x_{j_m}) \operatorname{jac}^{f_1, \dots, f_m}_{j_1, \dots, j_m},$$

so $f_1, \dots, f_m$ are p-independent over $k[x_1^p, \dots, x_n^p]$ by Lemma 1.6. Moreover, we obtain that

$$\operatorname{dgcd}(f_1, \dots, f_m) \mid f_1 \dots f_m.$$

$\neg(3) \Rightarrow \neg(2)$ Assume that $\operatorname{dgcd}(f_1, \dots, f_m)$ is divisible by an irreducible polynomial $g \in k[x_1, \dots, x_n]$. Then $g \mid f_i$ for some i.

Now we change in the matrix M the derivation d_m to $d'_m = \frac{\partial}{\partial x_l}$, where $l \in \{1, \dots, n\}$, and expand its determinant with respect to the last column. Again, using Lemma 7.1, we obtain the divisibility

$$\operatorname{dgcd}(f_1, \dots, f_m) \mid \sum_{j=1}^{m} (-1)^{m+j} c_j f_1 \dots f_{j-1} \frac{\partial f_j}{\partial x_l} f_{j+1} \dots f_m,$$

where $c_j \in k \setminus \{0\}$. Hence, $g \mid f_1 \dots f_{i-1} \frac{\partial f_i}{\partial x_l} f_{i+1} \dots f_m$, so $g \mid f_j$ for some $j \neq i$ or $g \mid \frac{\partial f_i}{\partial x_l}$ for $l = 1, \dots, n$, and then, by Lemma 4.5, $g^2 \mid f_i$ or $g \in k[x_1^p, \dots, x_n^p]$.

$(4) \Rightarrow (2)$ For every $i_1 \neq i_2$, if $\operatorname{dgcd}(f_{i_1}, f_{i_2}) \sim 1$, then f_{i_1} and f_{i_2} are coprime, square-free and p-free by the implication $(1) \Rightarrow (3)$ of Theorem 5.4 (for $m = 2$).

The implications (1) $\Rightarrow$ (2) and (3) $\Rightarrow$ (1) follow directly from Theorem 5.4. The implication (3) $\Rightarrow$ (4) follows from Lemma 1.5. $\square$

8. Rings of constants of homogeneous derivations

The motivation to describe rings of constants of homogeneous derivations being polynomial algebras, comes from the following theorem.

Theorem 8.1. (Ganong, Daigle)
Let k be a field of characteristic $p > 0$, let A and R be polynomial k-algebras in two variables such that $A^p \subsetneqq R \subsetneqq A$. Then there exist $x, y \in A$ such that $A = k[x, y]$ and $R = k[x, y^p]$.

The above theorem was proved by Ganong in [11], in the case of algebraically closed field k and then by Daigle in [4] in the general case. Note also that Kimura and Niitsuma in [29] proved that, in the case of a perfect field k of characteristic $p > 0$, under these assumptions, A has a p-basis over R and R has a p-basis over A^p.

Nowicki and the author generalized the above theorem to n variables in the homogeneous case.

Theorem 8.2. ([28], Theorem 3.1, [27], Theorem 2.2)
Let p be a prime number. Let k be a field (of arbitrary characteristic) and let $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ be homogeneous polynomials such that

$$k[x_1^p, \ldots, x_n^p] \subset k[f_1, \ldots, f_n].$$

a) *If* $\operatorname{char} k \neq p$, *then*

$$k[f_1, \ldots, f_n] = k[x_1^{l_1}, \ldots, x_n^{l_n}]$$

for some $l_1, \ldots, l_n \in \{1, p\}$.

b) *If* $\operatorname{char} k = p$, *then*

$$k[f_1, \ldots, f_n] = k[y_1, \ldots, y_m, y_{m+1}^p, \ldots, y_n^p]$$

for some $m \in \{0, 1, \ldots, n\}$ and some k-linear basis $y_1, \ldots, y_n$ of $\langle x_1, \ldots, x_n \rangle$.

For proofs, we refer to two articles joint with Nowicki. The article [27] contains the proof of the above theorem. The article [28] contains a theorem about (polynomial graded) subalgebras containing $k[x_1^{p_1}, \ldots, x_n^{p_n}]$, where $p_1, \ldots, p_n$ are arbitrary prime numbers ([28], Theorem 2.1).

A k-derivation d of $k[x_1, \ldots, x_n]$ is called homogeneous of degree r if $d(x_i)$, if nonzero, is a homogeneous polynomial of degree $r + 1$ for $i = 1, \ldots, n$. In this case, for every homogeneous polynomial $f \in k[x_1, \ldots, x_n]$ of degree s, the polynomial $d(f)$, if nonzero, is homogeneous of degree $r+s$. The ring of constants of a homogeneous derivation is a graded subalgebra. As a consequence of Theorem 8.2 we obtain.

Theorem 8.3. ([28], Theorem 4.1)
Let d be a homogeneous k-derivation of $k[x_1,\dots,x_n]$, where k is a field of characteristic $p>0$. Then $k[x_1,\dots,x_n]^d$ is a polynomial k-algebra if and only if

$$(*) \qquad k[x_1,\dots,x_n]^d = k[y_1,\dots,y_m,y_{m+1}^p,\dots,y_n^p]$$

for some $m\in\{0,1,\dots,n\}$ and some k-linear basis $y_1,\dots,y_n$ of $\langle x_1,\dots,x_n\rangle$.

A homogeneous k-derivation of $k[x_1,\dots,x_n]$ of degree 0 is called linear. In this case a restriction of d to $\langle x_1,\dots,x_n\rangle$ is a k-linear endomorphism. The author obtained in [20], Theorem 3.2, a description of linear derivations with rings of constants of the form $(*)$ above. Finally, we have the following.

Theorem 8.4. ([28], Corollary 4.2)
Let d be a linear derivation of $k[x_1,\dots,x_n]$, where k is a field of characteristic $p>0$. Then $k[x_1,\dots,x_n]^d$ is a polynomial k-algebra if and only if the Jordan matrix of the endomorphism $d|_{\langle x_1,\dots,x_n\rangle}$ has one of the following forms:

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

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

Acknowledgements. The author would like to thank Professor Andrzej Nowicki for many helpful remarks that improved this article.

References

[1] K. Adjamagbo, *On separable algebras over a UFD and the Jacobian Conjecture in any characteristic*, in: *A. van den Essen (ed.), Automorphisms of Affine Spaces, Proceedings of the conference "Invertible Polynomial Maps", July 4–8, 1994*, Curaçao, Caribbean Mathematics Foundation, Kluwer Academic Publishers, 1995.

[2] I.V. Arzhantsev, A.P. Petravchuk, *Closed polynomials and saturated subalgebras of polynomial algebras*, Ukrainian Math. J. 59 (2007), 1783–1790.

[3] M. Ayad, *Sur les polynômes $f(X,Y)$ tels que $K[f]$ est intégralement fermé dans $K[X,Y]$*, Acta Arith. 105 (2002), 9–28.

[4] D. Daigle, *Plane Frobenius sandwiches of degree p*, Proc. Amer. Math. Soc. 117 (1993), 885–889.

[5] D. Daigle, *Locally nilpotent derivations*, *Lecture notes for the "September School" of Algebraic Geometry*, Łukęcin, Poland, September 2003 (unpublished), aix1.uottawa.ca/~ddaigle/.

[6] 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.
[7] A. van den Essen, *Polynomial automorphisms and the Jacobian Conjecture*, Birkhäuser Verlag, Basel, 2000.
[8] A. van den Essen, A. Nowicki, A. Tyc, *Generalizations of a lemma of Freudenburg*, J. Pure Appl. Algebra 177 (2003), 43–47.
[9] G. Freudenburg, *A note on the kernel of a locally nilpotent derivation*, Proc. Amer. Math. Soc. 124 (1996), 27–29.
[10] G. Freudenburg, *Algebraic theory of locally nilpotent derivations*, Encyclopaedia of Mathematical Sciences 136, Springer Verlag, Berlin, 2006.
[11] R. Ganong, *Plane Frobenius sandwiches*, Proc. Amer. Math. Soc. 84 (1982), 474–478.
[12] M. Gerstenhaber, *On the Galois theory of inseparable extensions*, Bull. Amer. Math. Soc. 70 (1964), 561–566.
[13] M. Gerstenhaber, *On infinite inseparable extensions of exponent one*, Bull. Amer. Math. Soc. 71 (1965), 878–881.
[14] D. Goss, *Basic structures of function field arithmetic*, Springer, Berlin, 1996.
[15] N. Jacobson, *Lectures in abstract algebra*, vol. III, D. Van Nostrand, Princeton, 1964.
[16] P. Jędrzejewicz, *Rings of constants of p-homogeneous polynomial derivations*, Comm. Algebra 31 (2003), 5501–5511.
[17] P. Jędrzejewicz, *A note on characterizations of rings of constants with respect to derivations*, Colloq. Math. 99 (2004), 51–53.
[18] P. Jędrzejewicz, *On rings of constants of derivations in two variables in positive characteristic*, Colloq. Math. 106 (2006), 109–117.
[19] P. Jędrzejewicz, *Eigenvector p-bases of rings of constants of derivations*, Comm. Algebra 36 (2008), 1500–1508.
[20] P. Jędrzejewicz, *Linear derivations with rings of constants generated by linear forms*, Colloq. Math. 113 (2008), 279–286.
[21] P. Jędrzejewicz, *A characterization of one-element p-bases of rings of constants*, Bull. Pol. Acad. Sci. Math. 59 (2011), 19–26.
[22] P. Jędrzejewicz, *A note on rings of constants of derivations in integral domains*, Colloq. Math. 122 (2011), 241–245.
[23] P. Jędrzejewicz, *Positive characteristic analogs of closed polynomials*, Cent. Eur. J. Math. 9 (2011), 50–56.
[24] P. Jędrzejewicz, *Jacobian conditions for p-bases*, Comm. Algebra 40 (2012), 2841–2852.
[25] P. Jędrzejewicz, *A characterization of Keller maps*, J. Pure Appl. Algebra 217 (2013), 165–171.
[26] P. Jędrzejewicz, *A characterization of p-bases of rings of constants*, Cent. Eur. J. Math. 11 (2013), 900–909.
[27] P. Jędrzejewicz, A. Nowicki, *Subalgebras of polynomial algebras containing prime powers of variables*, in: *Materiały na XXXII Konferencję Szkoleniową z Geometrii Analitycznej i Algebraicznej Zespolonej*, Łódź, 2011, 11–21.
[28] P. Jędrzejewicz, A. Nowicki, *Polynomial graded subalgebras of polynomial algebras*, Comm. Algebra 40 (2012), 2853–2866.
[29] T. Kimura, H. Niitsuma, *A note on p-basis of a polynomial ring in two variables*, SUT J. Math. 25 (1989), 33–38.
[30] S. Kuroda, *A counterexample to the Forteenth Problem of Hilbert in dimension four*, J. Algebra 279 (2004), 126–134.

[31] S. Kuroda, *Fields defined by locally nilpotent derivations and monomials*, J. Algebra 293 (2005), 395–406.
[32] J. Lang, S. Mandal, *On Jacobian n-tuples in characteristic p*, Rocky Mountain J. Math. 23 (1993), 271–279.
[33] W. Li, *Remarks on rings of constants of derivations*, Proc. Amer. Math. Soc. 107 (1989), 337–340.
[34] W. Li, *Remarks on rings of constants of derivations II*, Comm. Algebra 20 (1992), 2191–2194.
[35] H. Matsumura, *Commutative algebra*, 2nd ed., Benjamin, Reading, 1980.
[36] M. Miyanishi, *Normal affine subalgebras of a polynomial ring*, in: *Algebraic and Topological Theories*, Kinokuniya, Tokyo, 1985, 37–51.
[37] H. Niitsuma, *Jacobian matrix and p-basis*, TRU Math. 24 (1988), 19–34.
[38] H. Niitsuma, *Jacobian matrix and p-basis*, in: *Topics in algebra*, 185–188, Banach Center Publ. 26, part 2, PWN, Warszawa 1990.
[39] P. Nousiainen, *On the Jacobian Problem* (thesis), Pennsylvania State University, 1982.
[40] A. Nowicki, *On the Jacobian equation $J(f,g)=0$ for polynomials in $k[x,y]$*, Nagoya Math. J. 109 (1988), 151–157.
[41] A. Nowicki, *Polynomial derivations and their rings of constants*, Nicolaus Copernicus University, Toruń, 1994, www.mat.umk.pl/~anow/.
[42] A. Nowicki, *Rings and fields of constants for derivations in characteristic zero*, J. Pure Appl. Algebra 96 (1994), 47–55.
[43] 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.
[44] A. Nowicki, J.-M. Strelcyn, *Generators of rings of constants for some diagonal derivations in polynomial rings*, J. Pure Appl. Algebra 101 (1995), 207–212.
[45] S.-I. Okuda, *Kernels of derivations in positive characteristic*, Hiroshima Math. J. 34 (2004), 1–19.
[46] T. Ono, *A note on p-bases of a regular affine domain extension*, Proc. Amer. Math. Soc. 136 (2008), 3079–3087.
[47] A. Płoski, *On the irreducibility of polynomials in several complex variables*, Bull. Polish Acad. Sci. Math. 39 (1991), 241–247.
[48] A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, 2000.
[49] S. Suzuki, *Some types of derivations and their applications to field theory*, J. Math. Kyoto Univ. 21 (1981), 375–382.
[50] A. Zaks, *Dedekind subrings of $k[x_1,\ldots,x_n]$ are rings of polynomials*, Israel J. Math., 9 (1971), 285–289.
[51] O. Zariski, *Interprétations algébrico-géométriques du quatorzième problème de Hilbert*, Bull. Sci. Math., 78 (1954), 155–168.
[52] O. Zariski, P. Samuel, *Commutative algebra*, vol. I, D. Van Nostrand, New York, 1958.

Faculty of Mathematics and Computer Science, Nicolaus Copernicus University, ul. Chopina 12/18, 87-100 Toruń

E-mail address: pjedrzej@mat.umk.pl