Jędrzejewicz, P.
Osaka J. Math.
46 (2009), 223–234

ONE-ELEMENT p-BASES OF RINGS OF CONSTANTS OF DERIVATIONS

PIOTR JĘDRZEJEWICZ

(Received November 19, 2007, revised November 30, 2007)

Abstract

In this paper we present sufficient conditions and necessary conditions for a single element to form a p-basis of a ring of constants of a derivation. We consider some special cases, when these conditions are equivalent, and we analyze some counter-examples, when the equivalence does not hold.

Introduction

If A is a commutative ring with unity, then we denote by A^* the subset of all invertible elements of A. Two elements $a, b \in A$ are called associated if $a = bc$ for some $c \in A^*$, and we denote it by $a \sim b$.

Let K be a commutative ring with unity and let A be a K-algebra. A K-linear map $d\colon A \to A$ such that $d(fg) = d(f)g + f\,d(g)$ for every $f, g \in A$, is called a K-derivation of A. If $A = K[x_1, \ldots, x_n]$ is a polynomial K-algebra and d is a K-derivation of A, then for every $f \in K[x_1, \ldots, x_n]$ we have

$$d(f) = \frac{\partial f}{\partial x_1} \cdot d(x_1) + \cdots + \frac{\partial f}{\partial x_n} \cdot d(x_n).$$

If d is a K-derivation of a K-algebra A, then its kernel

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

is a K-subalgebra of A, called the ring of constants of d. If A is a K-domain of characteristic $p > 0$, then a ring of constants of a K-derivation is always a $K[A^p]$-algebra, where $A^p = \{a^p,\ a \in A\}$.

Throughout this paper A and B will be domains of characteristic $p > 0$, such that

$$A^p \subseteq B \subset A \quad \text{and} \quad B_0 \cap A = B.$$

As the main example we will consider a polynomial algebra $A = K[x_1, \ldots, x_n]$ and its subalgebra $B = K[x_1^p, \ldots, x_n^p]$, where K is a unique factorization domain of characteristic $p > 0$.

2000 Mathematics Subject Classification. Primary 13N15; Secondary 12H05, 12E05.

If R is a domain, then R_0 denotes the field of fractions of R. For arbitrary $f \in A$ we consider the subring

$$C(f) = B_0(f) \cap A,$$

where $B_0(f)$ is the subfield of A_0 generated over B_0 by f. It is easy to see that for each $f \in A$ the ring $R = C(f)$ satisfies the conditions

$$B \subseteq R \quad \text{and} \quad R_0 \cap A = R.$$

Note that if a subring R of A satisfies these conditions and the field extension $B_0 \subseteq R_0$ is of degree p, then $R = C(f)$ for every $f \in R \setminus B$. Moreover, if A is finitely generated over B, then subrings of A satisfying these conditions are exactly the rings of constants of B-derivations of A ([7], Theorem 2.5; [5], Theorem 1.1; see [11], Theorem 5.4 or [10], Theorem 4.1.4 for original arguments in characteristic zero).

Nowicki in [9] proved that if k is a field of characteristic 0, then the ring of constants of every nonzero k-derivation of the polynomial algebra $k[x, y]$ is of the form $k[f]$ for some polynomial $f \in k[x, y]$. The properties of such generators in the case of characteristic 0 were investigated by Nowicki and Nagata in [12] and by Ayad in [1]. The authors of [12] showed also that in the case of characteristic 2 rings of constants of nonzero k-derivations of $k[x, y]$ are of the form $k[x^2, y^2, f]$ for suitable f.

For example, if k is a field of characteristic 2 and $f = xy \in k[x, y]$, then

$$C(f) = k[x^2, y^2, xy] = B[f],$$

where $B = k[x^2, y^2]$. On the other side ([12], Example 4.3), if k is a field of characteristic 3 and $f = x^2y \in k[x, y]$, then

$$C(f) = k[x^3, y^3, x^2y, xy^2] \neq k[x^3, y^3, x^2y] = B[f],$$

where $B = k[x^3, y^3]$.

If a subring R of A is generated over B by a single element $f \notin B$, that is, $R = B[f]$, then R is a free B-module with a basis $1, f, \ldots, f^{p-1}$ (Lemma 1.1). In this situation we call f a one-element p-basis of R over B (Definition 1.2). Note that the existence of one-element p-basis of a ring with respect to localizations and the module of derivations was investigated by Ono in [13].

Our main question is, when f is a one-element p-basis of $C(f)$. The answers, under additional assumptions about some kind of homogeneity, were obtained by the author in [5] and [6], and generalized for eigenvectors of a derivation in [7]. In this paper we study one-element p-bases consisted of an arbitrary element without additional assumptions.

We present necessary conditions and sufficient conditions for an element f to be a one-element p-basis of a ring of constants of a derivation in the case of positive characteristic. We consider various levels of generality. In Theorem 1.4 we deal with an

arbitrary domain, in Theorem 1.5 with a UFD, and in Theorem 2.3 with a polynomial algebra over a UFD. We prove that in the latter case the condition

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

is sufficient and the condition

$$\gcd\left(f + h, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) \sim 1 \quad \text{for every} \quad h \in K[x_1^p, \ldots, x_n^p]$$

is necessary.

In the case of characteristic 2 we prove that these conditions are equivalent. We conclude it from the characteristic 2 version of the following Freudenburg's lemma, presented (for two variables over $\mathbb{C}$) in [4] and generalized in [3].

Lemma ([4], Lemma; [3], Proposition 2.1). *Given a polynomial $f \in k[x_1, \ldots, x_n]$, where k is an algebraically closed field of characteristic zero, suppose $g \in k[x_1, \ldots, x_n]$ is an irreducible non-constant divisor of $\partial f/\partial x_i$ for $i = 1, \ldots, n$. Then there exists $c \in k$ such that g divides $f + c$.*

Actually, the thesis of the above lemma can be strengthened such that g^2 divides $f + c$ ([3]). We can observe a similar fact in positive characteristic, see Lemma 2.1.

In the last section we discuss some counter-examples to a version of this lemma in the case of $p > 2$.

1. The case of an arbitrary domain

In this section A is a domain of characteristic $p > 0$ and B is a subring containing A^p, such that $B_0 \cap A = B$.

We start from some basic observations.

Lemma 1.1. *For an arbitrary element $f \in A \setminus B$ the following holds*:

a) $B_0(f) = B_0[f]$,

b) *the elements* $1, f, \ldots, f^{p-1}$ *are linearly independent over* B_0,

c) *the ring* $B[f]$ *is a free* B*-module with a basis* $1, f, \ldots, f^{p-1}$.

Proof. a) One can easily show this directly, but this also follows from the algebraic dependence of f over B_0 ([14], Theorem 2, p. 56).

b) The field $B_0(f)$ is a purely inseparable extension of B_0 and, by a), the elements $1, f, \ldots, f^{p-1}$ span $B_0(f)$ over B_0. Thus $[B_0(f) : B_0] = p^e$ for some e ([14], Corollary 3, p. 68) and $1 < [B_0(f) : B_0] \leqslant p$, so $[B_0(f) : B_0] = p$.

c) This follows from b), because $f^p \in B$. □

The definition of a p-basis of a ring extension can be found in [8], p. 269. We are interested in rings with one-element p-bases, that is, rings of the form presented in c) in the previous lemma.

DEFINITION 1.2. If a subring R of A is a free B-module with a basis $1, f, \ldots, f^{p-1}$ for some $f \in A$, then f is called a one-element p-basis of R over B.

The next lemma will be useful in the rest of this section. Recall that A, B are domains of characteristic $p > 0$, such that $A^p \subseteq B \subset A$ and $B_0 \cap A = B$.

Lemma 1.3. *For an arbitrary element $f \in A \setminus B$ the following conditions are equivalent*:
(i) *f is a one-element p-basis of $C(f)$,*
(ii) *$C(f) = B[f]$,*
(iii) *for every $w_0, w_1, \ldots, w_{p-1} \in B_0$, if*

$$w_0 + w_1 f + \cdots + w_{p-1} f^{p-1} \in A,$$

then $w_0, w_1, \ldots, w_{p-1} \in B$.

Proof. The equivalence (i) $\Leftrightarrow$ (ii) follows from Lemma 1.1 c).

(ii) $\Rightarrow$ (iii) Assume that $C(f) = B[f]$ and consider $w_0, w_1, \ldots, w_{p-1} \in B_0$ such that $g = w_0 + w_1 f + \cdots + w_{p-1} f^{p-1} \in A$. Then $g \in B_0[f] \cap A$, so, by the assumption, $g \in B[f]$, that is, $g = v_0 + v_1 f + \cdots + v_{p-1} f^{p-1}$ for some $v_0, v_1, \ldots, v_{p-1} \in B$. Hence $w_i = v_i$ for each i, because $1, f, \ldots, f^{p-1}$ are linearly independent over B_0 by Lemma 1.1 b).

(iii) $\Rightarrow$ (ii) Assume that (iii) holds. Obviously $B[f] \subseteq B_0(f) \cap A = C(f)$. Now, take an arbitrary element $g \in C(f)$. By Lemma 1.1 a) $C(f) = B_0[f] \cap A$, so $g = w_0 + w_1 f + \cdots + w_{p-1} f^{p-1}$ for some $w_0, w_1, \ldots, w_{p-1} \in B_0$. Then $w_0, w_1, \ldots, w_{p-1} \in B$ by (iii), and $g \in B[f]$. □

Note that the assumption $B_0 \cap A = B$ in the above lemma is important. Without this condition Lemma 1.3, in general, is not true, as shown by the following example. (The author thanks the referee for this example.)

EXAMPLE. Let $A = k[x, y, y^2/x]$, $B = k[x^3, y^3, y^2/x]$, where k is a field of characteristic 3. Let $f = xy$. Then $B_0(f) = B_0$ and $B_0 \cap A = k[x^3, y^3, y^2/x, xy] = B[f]$. Meanwhile, $x^2/y, x/y^2 \notin B$ and $x^2/y - (x/y^2) \cdot xy = 0 \in A$.

The following theorem presents a sufficient condition and a necessary condition for f to form a p-basis of $C(f)$ over B. The proof of the implication (i) $\Rightarrow$ (ii) is motivated by the proof of Lemma 2.6 in [2].

Theorem 1.4. *Let A be a domain of characteristic $p > 0$ and B a subring of A, containing A^p, such that $B_0 \cap A = B$. Let $f \in A \setminus B$. Consider the following conditions*:

(i) $d(f) = 1$ *for some B-derivation d of A,*

(ii) $C(f) = B[f]$,

(iii) *for every $h \in B$ the element $f + h$ is not divisible by a square of any element from $A \setminus A^*$, nor by any element from $B \setminus A^*$.*

Then we have the following implications:

$$\text{(i)} \Rightarrow \text{(ii)} \Rightarrow \text{(iii)}.$$

Proof. (i) $\Rightarrow$ (ii) Suppose that the condition (i) holds, but $C(f) \neq B[f]$. Then, by Lemma 1.3, there exist $w_0, w_1, \ldots, w_{p-1} \in B_0$ such that $w_0 + w_1 f + \cdots + w_{p-1} f^{p-1} \in A$ and $w_i \notin B$ for some i. Let l be the least nonnegative integer such that $w_0 + w_1 f + \cdots + w_l f^l \in A$ for some $w_0, w_1, \ldots, w_l \in B_0$, where $w_i \notin B$ for some i. Of course $0 < l < p$. Moreover, $w_l \notin B$ by the minimality of l. Let d be a B-derivation of A such that $d(f) = 1$ and let d_0 be the extension of d to a B_0-derivation of A_0, defined by $d_0(g/h) = (d(g)h - g\,d(h))/h^2$. Then $d_0(w_0 + w_1 f + \cdots + w_l f^l) = (w_1 + 2w_2 f + \cdots + l w_l f^{l-1})\,d(f)$, so $w_1 + 2w_2 f + \cdots + l w_l f^{l-1} \in A$, and we have a contradiction with the minimality of l.

(ii) $\Rightarrow$ (iii) This is a special case of Proposition 3.3 a) in [7], just remember that $C(f) = C(f + h)$ and $B[f] = B[f + h]$. □

If A is a unique factorization domain, then the condition (i) of Theorem 1.4 can be replaced by a weaker one.

Theorem 1.5. *Let A be a UFD of characteristic $p > 0$ and B a subring of A, containing A^p, such that $B_0 \cap A = B$. Let $f \in A \setminus B$. If all elements of the form $d(f)$, where d is a B-derivation of A, have no common noninvertible divisors, then $C(f) = B[f]$.*

Proof. Similarly like in the proof of Theorem 1.4, we obtain that $(w_1 + 2w_2 f + \cdots + l w_l f^{l-1})\,d(f) = d_0(w_0 + w_1 f + \cdots + w_l f^l) \in A$ for every B-derivation d. Since, by the assumption, the elements of the form $d(f)$ have no common noninvertible divisors, hence $w_1 + 2w_2 f + \cdots + l w_l f^{l-1} \in A$. □

The following example shows that if A is not a UFD, then this weaker condition may be not sufficient.

EXAMPLE. Let k be a field of characteristic $p > 0$, let $K = k[a, b]/(a^3 - b^2)$, $A = K[x, y]$, $B = K[x^p, y^p]$, and let $f = bx + a^2 y$. The elements $\partial f/\partial x = b$ and $\partial f/\partial y = a^2$ have no common noninvertible divisors, so all the elements of the form

$d(f)$ have no common noninvertible divisors. On the other hand, $(a/b)\cdot f = ax + by \in A$ and $a/b \notin B$, so $C(f) \neq B[f]$ by Lemma 1.3.

2. The case of a polynomial algebra

In this section we consider a polynomial algebra $A = K[x_1, \ldots, x_n]$ over a unique factorization domain K of characteristic $p > 0$, and a subalgebra $B = K[x_1^p, \ldots, x_n^p]$.

The following two lemmas are analogical to some well-known facts from characteristic zero.

Lemma 2.1. *Let $f \in K[x_1, \ldots, x_n]$ and let g be a prime element of $K[x_1, \ldots, x_n]$, not belonging to $K[x_1^p, \ldots, x_n^p]$. If $g \mid f$ and $g \mid \partial f/\partial x_i$ for every i, then $g^2 \mid f$.*

Proof. Let $f = g^r h$, where $r \geqslant 1$, $h \in K[x_1, \ldots, x_n]$, $g \nmid h$. Then $\partial f/\partial x_i = g^{r-1}(r(\partial g/\partial x_i)h + g\partial h/\partial x_i)$ for each i. By the assumption $\partial g/\partial x_i \neq 0$ for some i, so $g \nmid \partial g/\partial x_i$, because $\partial g/\partial x_i$ has lower degree with respect to x_i than g. This implies that, if $p \nmid r$, then $g \nmid r(\partial g/\partial x_i)h$, so $g^{r-1} \mid \partial f/\partial x_i$ and $g^r \nmid \partial f/\partial x_i$, hence $r \geqslant 2$. Note also that, if $p \mid r$, then obviously $r \geqslant 2$. □

Lemma 2.2. *Let $f \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$. 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 not divisible by a square of any polynomial from $K[x_1, \ldots, x_n] \setminus K^*$, nor by any polynomial from $K[x_1^p, \ldots, x_n^p] \setminus K^*$.

Proof. ($\Rightarrow$) It is easy to see that if $g^2 \mid f$ for some $g \in K[x_1, \ldots, x_n] \setminus K^*$ or $g \mid f$ for some $g \in K[x_1^p, \ldots, x_n^p] \setminus K^*$, then $g \mid \partial f/\partial x_i$ for every i.

($\Leftarrow$) Assume that $\gcd(f, \partial f/\partial x_1, \ldots, \partial f/\partial x_n) \nsim 1$ and consider a prime element $g \in K[x_1, \ldots, x_n] \setminus K^*$ such that $g \mid f$ and $g \mid \partial f/\partial x_i$ for every i. If $g \notin K[x_1^p, \ldots, x_n^p]$, then $g^2 \mid f$ by the previous lemma. □

The following theorem presents a sufficient condition and a necessary condition for a polynomial f to be a one-element p-basis of $C(f)$. The implication (i) $\Rightarrow$ (ii) is a positive characteristic analog of Proposition 14 in [1].

Theorem 2.3. *Let K be a UFD of characteristic $p > 0$, let $f \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$. Consider the following conditions*:

(i) $\gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$,

(ii) $C(f) = K[x_1^p, \ldots, x_n^p, f]$,

(iii) $\gcd(f + h, \partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$ *for every* $h \in K[x_1^p, \ldots, x_n^p]$.

Then we have the following implications:

$$\text{(i)} \Rightarrow \text{(ii)} \Rightarrow \text{(iii)}.$$

Proof. (i) $\Rightarrow$ (ii) If $\gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$, then, obviously, all elements of the form $d(f)$, where d is a K-derivation of $K[x_1, \ldots, x_n]$, have no common non-invertible divisors, so $C(f) = K[x_1^p, \ldots, x_n^p, f]$ by Theorem 1.5.

(ii) $\Rightarrow$ (iii) Assume that $C(f) = K[x_1^p, \ldots, x_n^p, f]$. Then, by Theorem 1.4, for every $h \in K[x_1^p, \ldots, x_n^p]$, the polynomial $f + h$ is not divisible by a square of any polynomial from $K[x_1, \ldots, x_n] \setminus K^*$, nor by any polynomial from $K[x_1^p, \ldots, x_n^p] \setminus K^*$, so $\gcd(f + h, \partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$ by Lemma 2.2. □

The rest of this paper is devoted to partial answers to the following two questions.

Question I. When are the conditions (i) and (ii) of Theorem 2.3 equivalent?

In Theorem 3.7 we will give an affirmative answer to the above question in the case of characteristic $K = 2$. Moreover, it is easy to see that the equivalence (i) $\Leftrightarrow$ (ii) holds in Theorem 2.3 for arbitrary characteristic in the case of one variable. Namely, for $f \in K[x]$ the condition (i) means that $f = ax + b$ for some $a \in K^*$, $b \in K[x^p]$. And this is equivalent to (ii), because $C(f) = K[x]$.

Question II. When are the conditions (i) and (iii) of Theorem 2.3 equivalent?

The answer to this question is obviously affirmative if $\gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n) \mid f + h$ for some $h \in K[x_1^p, \ldots, x_n^p]$. This is the case when $d(f) = f$ for some K-derivation d of $K[x_1, \ldots, x_n]$ (compare [7], Theorem 4.4 with a single eigenvector), in particular, if K is a field and f is homogeneous of a nonzero degree with respect to any weight vector ([6], Proposition 2). Another situations when we have an affirmative answer to Question II will be presented in the next section.

3. Some special cases

In this section we observe the cases when the conditions (i), (ii) and (iii) of Theorem 2.3 are equivalent. More precisely, in Propositions 3.1, 3.3, 3.5 and 3.6 we present conditions, which are stronger than the negation of (i), and which imply the negation of (iii). Such implications have the form of simpler versions of the Freudenburg's lemma ([4], [3]) in positive characteristic. The first one is obtained when a prime factor has some special form.

Proposition 3.1. *Let K be a UFD of characteristic $p > 0$. Let $f \in K[x_1, \ldots, x_n]$ and let $g \in K[x_1, \ldots, x_n]$ be a polynomial of the form $g = x_j + r$, where $r \in K[x_1, \ldots,$*

$x_{j-1}, x_{j+1}, \ldots, x_n]$, *for some* j. *If* $g \mid \partial f/\partial x_i$ *for* $i = 1, \ldots, n$, *then* $g^2 \mid f + h$ *for some* $h \in K[x_1^p, \ldots, x_n^p]$.

Proof. We may assume that $j = 1$, that is, $g = x_1 + r$, where $r \in K[x_2, \ldots, x_n]$. By easy induction on the degree of f with respect to x_1 we obtain that $f = ag + b$ for some $a \in K[x_1, \ldots, x_n]$, $b \in K[x_2, \ldots, x_n]$, so $\partial f/\partial x_1 = (\partial a/\partial x_1)g + a$ and $\partial f/\partial x_i = (\partial a/\partial x_i)g + a(\partial g/\partial x_i) + \partial b/\partial x_i$ for $i > 1$. From these equalities we deduce that if $g \mid \partial f/\partial x_i$ for each i, then $g \mid a$ and $g \mid \partial b/\partial x_i$ for $i > 1$. Since $\partial b/\partial x_i$ is of degree 0 with respect to x_1, hence $\partial b/\partial x_i = 0$ for each $i > 1$, so $b \in K[x_2^p, \ldots, x_n^p]$. Finally, $g^2 \mid f + h$ for $h = -b$. □

The other particular version is obtained when we consider a factor (not necessarily prime) from the subalgebra generated by p-th powers of variables. We need the following obvious lemma.

Lemma 3.2. *Let* K *be a domain of characteristic* $p > 0$ *and let* $f \in K[x]$, $f = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}$, *where* $a_i \in K[x^p]$ *for* $i = 0, 1, \ldots, p-1$. *If* $b \in K[x^p]$ *and* $b \mid f$, *then* $b \mid a_i$ *for* $i = 0, 1, \ldots, p-1$.

Proposition 3.3. *Let* K *be a UFD of characteristic* $p > 0$. *Let* $f \in K[x_1, \ldots, x_n]$ *and* $g \in K[x_1^p, \ldots, x_n^p]$. *If* $g \mid \partial f/\partial x_i$ *for* $i = 1, \ldots, n$, *then* $g \mid f + h$ *for some* $h \in K[x_1^p, \ldots, x_n^p]$.

Proof. Induction. Let $n = 1$, $f \in K[x]$, $f = a_0 + a_1 x + \cdots + a_{p-1}x^{p-1}$, where $a_i \in K[x^p]$ for $i = 0, 1, \ldots, p-1$. Consider an polynomial $g \in K[x^p]$ such that $g \mid \partial f/\partial x$. Since $\partial f/\partial x = a_1 + \cdots + (p-1)a_{p-1}x^{p-2}$, hence $g \mid a_i$ for $i = 1, \ldots, p-1$, by Lemma 3.2. Then $g \mid f - a_0$.

Now, let $n > 1$ and assume that the statement holds for $n - 1$. Consider polynomials $f \in K[x_1, \ldots, x_n]$ and $g \in K[x_1^p, \ldots, x_n^p]$ such that $g \mid \partial f/\partial x_i$ for $i = 1, \ldots, n$. Put $K_n = K[x_1, \ldots, x_{n-1}]$. Since $g \mid \partial f/\partial x_n$, hence $g \mid f - h_0$ for some $h_0 \in K_n[x_n^p]$, by the case of $n = 1$. Then obviously $g \mid \partial f/\partial x_i - \partial h_0/\partial x_i$ for $i = 1, \ldots, n-1$, because $g \in K[x_1^p, \ldots, x_n^p]$, so $g \mid \partial h_0/\partial x_i$. Put $K' = K[x_n^p]$. By the induction assumption for $h_0 \in K'[x_1, \ldots, x_{n-1}]$ we obtain that $g \mid h_0 + h$ for some $h \in K'[x_1^p, \ldots, x_{n-1}^p]$, so finally, $g \mid f + h$. □

The next proposition is especially useful in the case of characteristic $K = 2$. First, note the following consequence of Lemma 1.2 in [7].

Lemma 3.4. *Let* K *be a UFD of characteristic* $p > 0$. *Let* g *be a prime element of* $K[x]$, $g \notin K[x^p]$, $g \mid a$, *where* $a \in K[x^p]$. *Then* $g^p \mid a$.

Proposition 3.5. *Let K be a UFD of characteristic $p > 0$. Let $f \in K[x_1, \ldots, x_n]$ be a polynomial such that $\partial^2 f/\partial x_i^2 = 0$ for $i = 1, \ldots, n$, let g be a prime element of $K[x_1, \ldots, x_n]$, such that $\partial g/\partial x_i \neq 0$ for $i = 1, \ldots, n$. If $g \mid \partial f/\partial x_i$ for $i = 1, \ldots, n$, then $g^p \mid f + h$ for some $h \in K[x_1^p, \ldots, x_n^p]$.*

Proof. Put $K_i = K[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ for $i = 1, \ldots, n$. The assumptions imply that $\partial f/\partial x_i \in K_i[x_i^p]$ and $g \in K_i[x_i] \setminus K_i[x_i^p]$ for each i, so, if $g \mid \partial f/\partial x_i$, then $g^p \mid \partial f/\partial x_i$ by Lemma 3.4. Since $g^p \in K[x_1^p, \ldots, x_n^p]$, hence the statement follows from Proposition 3.3. □

The characteristic 2 version of the Freudenburg's lemma is the following.

Proposition 3.6. *Let K be a UFD of characteristic 2. Let $f \in K[x_1, \ldots, x_n]$ and let g be a prime element of $K[x_1, \ldots, x_n]$, not belonging to $K[x_1^2, \ldots, x_n^2]$. If $g \mid \partial f/\partial x_i$ for $i = 1, \ldots, n$, then $g^2 \mid f + h$ for some $h \in K[x_1^2, \ldots, x_n^2]$.*

Proof. Induction. Let $n = 1$, let $f \in K[x]$, $f = ax + b$, where $a, b \in K[x^2]$. Consider a prime divisor g of $\partial f/\partial x = a$ such that $g \notin K[x^2]$. Then $g^2 \mid a$ by Lemma 3.4, so $g^2 \mid f - b$.

Now, let $n > 1$ and assume that the statement holds for $n - 1$. Consider polynomials $f, g \in K[x_1, \ldots, x_n]$ such that g is prime, $g \notin K[x_1^2, \ldots, x_n^2]$ and $g \mid \partial f/\partial x_i$ for $i = 1, \ldots, n$. From Proposition 3.5 we know that the statement is true if $\partial g/\partial x_i \neq 0$ for every i, because $\partial^2 f/\partial x_i^2 = 0$ in characteristic 2.

Now assume that $\partial g/\partial x_j = 0$ for some j, for example, $\partial g/\partial x_n = 0$. Then $g \in K_n[x_n^2]$, where $K_n = K[x_1, \ldots, x_{n-1}]$. Put $f_n = f - x_n(\partial f/\partial x_n)$, so also $f_n \in K_n[x_n^2]$. For each i, since $g \mid \partial f/\partial x_i$ and $\partial g/\partial x_n = 0$, hence $g \mid (\partial/\partial x_n)(\partial f/\partial x_i)$. For $i < n$ we have $\partial f_n/\partial x_i = \partial f/\partial x_i - x_n(\partial^2 f/\partial x_i \partial x_n)$, so $g \mid \partial f_n/\partial x_i$.

Put $K' = K[x_n^2]$. Observe that $f_n, g \in K'[x_1, \ldots, x_{n-1}]$, g is prime in $K'[x_1, \ldots, x_{n-1}]$, $g \notin K'[x_1^2, \ldots, x_{n-1}^2]$. By the induction assumption, since $g \mid \partial f_n/\partial x_i$ for every $i < n$, hence $g^2 \mid f_n + h$ for some $h \in K'[x_1^2, \ldots, x_{n-1}^2]$, that is, $h \in K[x_1^2, \ldots, x_n^2]$. Then $g \mid f + h$, because $g \mid \partial f/\partial x_n$, and finally, by Lemma 2.1, we obtain that $g^2 \mid f + h$. □

Now we obtain, in the case of characteristic 2, the equivalence of sufficient and necessary conditions for a polynomial f to be a one-element p-basis of $C(f)$.

Theorem 3.7. *If K is a UFD of characteristic 2 and $f \in K[x_1, \ldots, x_n] \setminus K[x_1^2, \ldots, x_n^2]$, then the following conditions are equivalent*:

(i) $\gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$,

(ii) $C(f) = K[x_1^2, \ldots, x_n^2, f]$,

(iii) $\gcd(f + h, \partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$ *for every* $h \in K[x_1^2, \ldots, x_n^2]$,

(iv) *for every* $h \in K[x_1^2, \ldots, x_n^2]$ *the polynomial* $f + h$ *is not divisible by any polynomial from* $K[x_1^2, \ldots, x_n^2] \setminus K^*$.

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) were obtained in Theorem 2.3. The implication (iii) $\Rightarrow$ (i) follows from Propositions 3.3 and 3.6. And the equivalence (iii) $\Leftrightarrow$ (iv) follows from Lemma 2.2, because, in the case of characteristic 2, a square of a polynomial from $K[x_1, \ldots, x_n] \setminus K^*$ belongs to $K[x_1^2, \ldots, x_n^2] \setminus K^*$. □

4. Some examples for $p > 2$

In this section we analyze some counter-examples to the "$p > 2$" version of Proposition 3.6.

Let K be a UFD of characteristic $p > 2$. We are looking for pairs of polynomials (f, g) such that $f, g \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$, satisfying the following conditions:

$$(*) \qquad \begin{cases} g \quad \text{is a prime element of} \quad K[x_1, \ldots, x_n], \\ g \mid \dfrac{\partial f}{\partial x_i} \quad \text{for} \quad i = 1, \ldots, n, \\ g \nmid f + h \quad \text{for every} \quad h \in K[x_1^p, \ldots, x_n^p]. \end{cases}$$

Of course, every pair (f, g) satisfying $(*)$ is a counter-example to the "$p > 2$" version of Proposition 3.6. On the other side, all counter-examples satisfy $(*)$, because for $g \notin K[x_1^p, \ldots, x_n^p]$, if $g \mid \partial f/\partial x_i$ for $i = 1, \ldots, n$ and $g^2 \nmid f + h$ for every $h \in K[x_1^p, \ldots, x_n^p]$, then $g \nmid f + h$ (Lemma 2.1).

We will consider a special case, when $g \sim \gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n)$. In this case f is a counter-example to the implication (iii) $\Rightarrow$ (i) in Theorem 2.3. The following examples have been found using a computer.

EXAMPLE. Let K be a UFD of characteristic 3. The following pairs of polynomials (f_j, g_j) satisfy the condition $(*)$:

$$\begin{array}{lll} f_1 = x^5 + x^2 + x, & g_1 = x^4 + x - 1, & f_1, g_1 \in \mathbb{F}_3[x], \\ f_2 = x^5 + xy^3, & g_2 = x^4 - y^3, & f_2, g_2 \in K[x, y], \\ f_3 = x^3y^2 + x^4y + x^5 + y^4 - xy^3, & g_3 = x^4 - x^3y + y^3, & f_3, g_3 \in K[x, y], \\ f_4 = x^5y + x^2y^4 + xy^5, & g_4 = x^4 + xy^3 - y^4, & f_4, g_4 \in \mathbb{F}_3[x, y]. \end{array}$$

The fact, that each g_j is prime, could be verified by hand, but the last condition of $(*)$ is obtained by the following lemma.

Lemma 4.1. *Let $f \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$, where K is a UFD of characteristic $p > 0$. Assume that $g \sim \gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n)$ is a prime element of $K[x_1, \ldots, x_n]$, not belonging to $K[x_1^p, \ldots, x_n^p]$. Let $\partial f/\partial x_i = u_i g$, $u_i \in K[x_1, \ldots, x_n]$, for $i = 1, \ldots, n$. If $u_i \notin (g, \partial g/\partial x_i)$ for some i, then $g \nmid f + h$ for every $h \in K[x_1^p, \ldots, x_n^p]$.*

Proof. Suppose that $g \mid f + h$ for some $h \in K[x_1^p, \ldots, x_n^p]$. Then $g^2 \mid f + h$ by Lemma 2.1, so $f + h = g^2 s$ for some $s \in K[x_1, \ldots, x_n]$. Hence $\partial f/\partial x_i = 2g(\partial g/\partial x_i)s + g^2(\partial s/\partial x_i)$, so $u_i = 2s(\partial g/\partial x_i) + (\partial s/\partial x_i)g$, that is, $u_i \in (g, \partial g/\partial x_i)$. □

Actually, the examples f_1 and f_4 are not very valuable, they just show that in general we need g to be irreducible over the algebraic closure of K (when K is a field), like in the characteristic zero case ([3], Remark 2.4). So it is remarkable that, as we observed in Proposition 3.6, the Freudenburg's lemma in the case of characteristic 2 is valid over any UFD, we do not even need K to be a field!

One can see that our examples are not so arbitrary. Note that the polynomial f_1 is of one variable, but f_2 in some sense is also of one variable, since it belongs to $K[x, y^3] = K'[x]$, where $K' = K[y^3]$. And f_3 is the same, because $f_3 \in K[z, t^3]$ for a linear change of coordinates: $z = x - y$, $t = x + y$. This is the reason why f_1, f_2, f_3 are not counter-examples to the implication (ii) $\Rightarrow$ (i) in Theorem 2.3.

The common property of f_1, f_2, f_3 is that $\partial f/\partial x \mid \partial f/\partial y$. We can generalize these examples in the following way.

Proposition 4.2. *Let K be a UFD of characteristic $p > 2$ and let $f \in K[x_1, \ldots, x_n]$ be a polynomial with zero coefficients of x_{i_0} and $x_{i_0}^2$ for some i_0. Assume additionally that $\partial f/\partial x_{i_0}$ is a prime element of $K[x_1, \ldots, x_n]$, not belonging to $K[x_1^p, \ldots, x_n^p]$, such that $\partial f/\partial x_{i_0} \mid \partial f/\partial x_j$ for every j. Then the pair (f, g), where $g = \partial f/\partial x_{i_0}$, satisfies* $(*)$.

Proof. By Lemma 4.1 it is enough to prove that $1 \notin (g, \partial g/\partial x_{i_0})$. Since f has zero coefficients of x_{i_0} and $x_{i_0}^2$, hence g and $\partial g/\partial x_{i_0}$ have no constant terms, so $(g, \partial g/\partial x_{i_0}) \subseteq (x_1, \ldots, x_n)$. □

The polynomial f_4 from our examples does not fit in with the above proposition, because it is homogeneous of degree 6 and the relation between its partial derivatives is of the form $x(\partial f/\partial x) + y(\partial f/\partial y) = 0$ (note that f_4 is neither a counter-example to the implication (ii) $\Rightarrow$ (i) in Theorem 2.3, see [5], Proposition 4.4, when K is a field). We can generalize this example in the following way.

Proposition 4.3. *Let K be a UFD of characteristic $p > 2$. Let $a, b \in K[x^p, y^p]$ be polynomials without constant terms, such that $g = ax^{p-2} + by^{p-2}$ is a prime element of $K[x, y]$. Then, for $f = ax^{p-1}y - bxy^{p-1}$, the pair (f, g) satisfies* $(*)$.

Proof. We have $a, b \in (x^p, y^p)$, so $(g, \partial g/\partial x) \subseteq (x^p, y^p)$. But $\partial f/\partial x = -yg$ and $-y \notin (x^p, y^p)$, so the statement follows from Lemma 4.1. □

Note that for $p > 3$ the condition that a and b have no constant terms may be omitted in the above proposition.

Finally, let us emphasize that it is not clear whether the counter-examples discussed in this section are in some sense special and the "$p > 2$" version of Proposition 3.6, as well as the implication (iii) $\Rightarrow$ (i) in Theorem 2.3, holds under some natural additional assumption. Remark also that we do not know any counter-example

to the implication (ii) $\Rightarrow$ (i) in Theorem 2.3. It seems to be possible that this implication holds.

ACKNOWLEDGEMENTS. The author would like to thank the referee for constructive remarks.

References

[1] 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.
[2] D. Daigle and G. Freudenburg: *Locally nilpotent derivations over a UFD and an application to rank two locally nilpotent derivations of $k[X_1, \ldots, X_n]$*, J. Algebra **204** (1998), 353–371.
[3] A. van den Essen, A. Nowicki and A. Tyc: *Generalizations of a lemma of Freudenburg*, J. Pure Appl. Algebra **177** (2003), 43–47.
[4] G. Freudenburg: *A note on the kernel of a locally nilpotent derivation*, Proc. Amer. Math. Soc. **124** (1996), 27–29.
[5] P. Jędrzejewicz: *Rings of constants of p-homogeneous polynomial derivations*, Comm. Algebra **31** (2003), 5501–5511.
[6] P. Jędrzejewicz: *On rings of constants of derivations in two variables in positive characteristic*, Colloq. Math. **106** (2006), 109–117.
[7] P. Jędrzejewicz: *Eigenvector p-bases of rings of constants of derivations*, Comm. Algebra **36** (2008), 1500–1508.
[8] H. Matsumura: Commutative Algebra, second edition, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
[9] A. Nowicki: *On the Jacobian equation $J(f, g) = 0$ for polynomials in $k[x, y]$*, Nagoya Math. J. **109** (1988), 151–157.
[10] A. Nowicki: Polynomial Derivations and Their Rings of Constants, Nicolaus Copernicus University, Toruń, 1994.
[11] A. Nowicki: *Rings and fields of constants for derivations in characteristic zero*, J. Pure Appl. Algebra **96** (1994), 47–55.
[12] 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.
[13] T. Ono: *A note on p-bases of rings*, Proc. Amer. Math. Soc. **128** (2000), 353–360.
[14] O. Zariski and P. Samuel: Commutative Algebra, volume I, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958.

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