BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 59, No. 1, 2011

COMMUTATIVE ALGEBRA

A Characterization of One-Element p-Bases of Rings of Constants

by

Piotr JĘDRZEJEWICZ

Presented by Andrzej SKOWROŃSKI

Summary. Let K be a unique factorization domain of characteristic $p > 0$, and let $f \in K[x_1, \ldots, x_n]$ be a polynomial not lying in $K[x_1^p, \ldots, x_n^p]$. We prove that $K[x_1^p, \ldots, x_n^p, f]$ is the ring of constants of a K-derivation of $K[x_1, \ldots, x_n]$ if and only if all the partial derivatives of f are relatively prime. The proof is based on a generalization of Freudenburg's lemma to the case of polynomials over a unique factorization domain of arbitrary characteristic.

1. Introduction. Nowicki and Nagata in [10] considered various questions about the number of generators of rings of constants of derivations, both in zero and positive characteristic cases. In particular, they proved in [10, Proposition 4.1] that if k is a field of positive characteristic, then the ring of constants of an arbitrary k-derivation of the polynomial k-algebra $k[x_1, \ldots, x_n]$ is finitely generated over k. In [10, Proposition 4.2] they proved that if $\operatorname{char} k = 2$, then the ring of constants of a nonzero k-derivation of $k[x, y]$ is a $k[x^2, y^2]$-algebra generated by a single polynomial. They also gave a counter-example in the case of $\operatorname{char} k = p > 2$. It is natural to ask when the ring of constants of a k-derivation of $k[x_1, \ldots, x_n]$, where $\operatorname{char} k = p > 0$, is generated over $k[x_1^p, \ldots, x_n^p]$ by a single element.

The present author presented in [5] a discussion of sufficient conditions and necessary conditions for an element to be such a single generator of a ring of constants. In Theorem 2.3 of [5] the author proved that for a polynomial $f \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$, where K is a UFD of characteristic $p > 0$,

2010 *Mathematics Subject Classification*: Primary 13N15; Secondary 12E05.
Key words and phrases: derivation, ring of constants, p-basis.

DOI: 10.4064/ba59-1-3

the condition

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

is sufficient and the condition

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

is necessary. The conditions $(*)$ and $(**)$ are necessary and sufficient in the case of characteristic 2 ([5, Theorem 3.7]). The proof was based on the following analog of Freudenburg's lemma.

Proposition 1.1 ([5, 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 $g \mid \frac{\partial f}{\partial x_i}$ for $i = 1, \ldots, n$, then $g^2 \mid f + h$ for some $h \in K[x_1^2, \ldots, x_n^2]$.*

The original version of this lemma was presented by Freudenburg for two variables over $\mathbb{C}$ in [3].

Lemma 1.2 (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 $\partial f/\partial x$ and $\partial f/\partial y$. Then there exists $c \in \mathbb{C}$ such that g divides $f + c$.*

This fact was generalized to polynomials over an arbitrary algebraically closed field of characteristic zero by van den Essen, Nowicki and Tyc in [2, Proposition 2.1].

Proposition 1.3 (van den Essen, Nowicki, Tyc). *Let k be an algebraically closed field of characteristic zero. Let P 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 $\partial f/\partial x_i$ belongs to P, then there exists $c \in k$ such that $f + c \in P$.*

The natural analog of Freudenburg's lemma appeared to be, in general, false in characteristic $p > 2$ ([5]). The condition $(**)$ also turned out to be, in general, not sufficient.

In this article we generalize Freudenburg's lemma to polynomials over a UFD of arbitrary characteristic (Theorem 3.1). In positive characteristic it is a weaker version of this lemma than the one mentioned above. This enables us to obtain in Theorem 4.2 the equivalence of some conditions for f to be a single generator of the ring of constants of a derivation, in particular, we obtain the condition $(*)$.

2. Preliminaries. Throughout this paper by a ring we mean a commutative ring with unity and by a domain we mean a commutative ring with unity, without zero divisors.

Let K be a domain. We denote by K_0 the field of fractions of K, and by K^* the set of all invertible elements of K. Two polynomials $f, g \in K[x_1, \ldots, x_n]$ are called *associated* if $f = ag$ for some $a \in K^*$; we then write $f \sim g$. A polynomial $f \in K[x_1, \ldots, x_n]$ is called *square-free* if it is not divisible by a square of any polynomial from $K[x_1, \ldots, x_n] \setminus K^*$. If K is a domain of characteristic $p > 0$, then a polynomial $f \in K[x_1, \ldots, x_n]$ is called *p-free* if it is not divisible by any polynomial from $K[x_1^p, \ldots, x_n^p] \setminus K^*$.

Let K be a ring and let A be a K-algebra. A K-linear map $d\colon A \to A$ is called a *K-derivation* of A if $d(fg) = d(f)g + fd(g)$ for every $f, g \in A$. The kernel of a K-derivation d is called the *ring of constants* of d and is denoted by A^d.

If the K-algebra A is a domain of characteristic $p > 0$, then $A^p = \{a^p;\ a \in A\}$ is a subring of A. Denote by KA^p the K-submodule of A generated by A^p and observe that KA^p is a K-subalgebra of A. The ring of constants of every K-derivation of A is a KA^p-subalgebra of A. In particular, the ring of constants of every K-derivation of $K[x_1, \ldots, x_n]$ is a $K[x_1^p, \ldots, x_n^p]$-subalgebra of $K[x_1, \ldots, x_n]$.

Recall some definitions and facts from [4].

Definition 2.1. Let A be a domain of characteristic $p \geq 0$, and let R be a subring of A. If $p = 0$, we put $T^p = 1$ and $R_0[T^p] = R_0$. An element $a \in A$ is called *separably algebraic* over R if $w(a) = 0$ for some irreducible polynomial $w(T) \in R_0[T] \setminus R_0[T^p]$. The set of all elements of A separably algebraic over R is called the *separable algebraic closure* of R in A and is denoted by $\overline{R}^A$.

Proposition 2.2. *Let A be a domain of characteristic $p > 0$. Let R be a subring of A such that $A^p \subseteq R$. Then $\overline{R}^A = R_0 \cap A$.*

The following theorem from [4] concerns rings of constants of K-derivations, where K is a domain. It is a generalization of Nowicki's characterization ([9, Theorem 5.4], [8, Theorem 4.1.4]) and Daigle's observation ([1, Theorem 1.4]); see also [6, Theorem 1.1].

Theorem 2.3. *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 $\operatorname{char} K = p > 0$, assume additionally that $A^p \subseteq R$. The following conditions are equivalent:*

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

(2) $\overline{R}^A = R$.

The following corollary of the above theorem will be useful in the proof of Theorem 3.1.

Corollary 2.4. *Let A be a finitely generated K-domain, where K is a domain. Then the smallest (with respect to inclusion) ring of constants of a K-derivation of A is of the form $\overline{B}^A$, where:*

(a) *B is the canonical homomorphic image of K in A if* $\operatorname{char} K = 0$,
(b) *$B = KA^p$ if* $\operatorname{char} K = p > 0$.

In particular, for $\operatorname{char} K = p > 0$, the smallest ring of constants containing a given element $f \in A$ is of the form

$$\overline{B[f]}^A = B_0(f) \cap A = B_0[f] \cap A,$$

where $B = KA^p$.

The general definition of a p-basis can be found, for example, in [7, p. 269]. In this paper we deal only with the one-element case.

Definition 2.5. Let A, B be domains of characteristic $p > 0$ such that $A^p \subseteq B$, and let R be a subring of A. An element $f \in A$ is called a *one-element p-basis* of R over B if R is a free B-module with basis $1, f, \ldots, f^{p-1}$.

The following fact is an adaptation of Lemma 1.3 from [5]. It will be useful in the proof of Theorem 4.2.

Lemma 2.6. *Let K is a domain of characteristic $p > 0$. For an arbitrary polynomial $f \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$ put*

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

Then the following conditions are equivalent:

(i) *$K[x_1^p, \ldots, x_n^p, f]$ is the ring of constants of a K-derivation,*
(ii) *f is a one-element p-basis of $C(f)$,*
(iii) *$C(f) = K[x_1^p, \ldots, x_n^p, f]$,*
(iv) *for every $w_0, w_1, \ldots, w_{p-1} \in K(x_1^p, \ldots, x_n^p)$, if*

$$w_0 + w_1 f + \cdots + w_{p-1} f^{p-1} \in K[x_1, \ldots, x_n],$$

then $w_0, w_1, \ldots, w_{p-1} \in K[x_1^p, \ldots, x_n^p]$.

3. An analog of Freudenburg's lemma. In this section we prove the following analog of the lemma of Freudenburg.

Theorem 3.1. *Let K be a UFD, and let P be a prime ideal of the polynomial algebra $K[x_1, \ldots, x_n]$. Consider a polynomial $f \in K[x_1, \ldots, x_n]$ such that $\partial f / \partial x_i \in P$ for $i = 1, \ldots, n$.*

(a) *If* $\operatorname{char} K = 0$, *then there exists an irreducible polynomial $W(T) \in K[T]$ such that $W(f) \in P$.*
(b) *If* $\operatorname{char} K = p > 0$, *then there exist $b, c \in K[x_1^p, \ldots, x_n^p]$ such that* $\gcd(b, c) \sim 1$, *$b \notin P$ and $bf + c \in P$.*

The proof is based on the following observation.

Lemma 3.2. *Let K be a domain, let I be an ideal of $K[x_1,\dots,x_n]$ and let δ be a K-derivation of the factor algebra $A = K[x_1,\dots,x_n]/I$. Then there exists a K-derivation d of $K[x_1,\dots,x_n]$ such that $\delta(\overline{f}) = \overline{d(f)}$ for every $f \in k[x_1,\dots,x_n]$, where $\overline{f}$ denotes the coset of f in A.*

Proof. Put $\delta(\overline{x_i}) = \overline{h_i}$, where $h_i \in K[x_1,\dots,x_n]$, for $i = 1,\dots,n$. Define a K-derivation d of $K[x_1,\dots,x_n]$ such that $d(x_i) = h_i$ for $i = 1,\dots,n$. Then, by a straightforward computation, one can verify that $\delta(\overline{f}) = \overline{d(f)}$ for every $f \in k[x_1,\dots,x_n]$. ∎

Now we can prove Theorem 3.1.

Proof of Theorem 3.1. Note that if d is a K-derivation of $K[x_1,\dots,x_n]$, then

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

so $d(f) \in P$.

Consider the factor algebra $A = K[x_1,\dots,x_n]/P$. Since P is a prime ideal, A is a domain. If δ is an arbitrary K-derivation of A, then, by Lemma 3.2, there exists a K-derivation d of $K[x_1,\dots,x_n]$ such that $\delta(\overline{f}) = \overline{d(f)} = \overline{0}$, since $d(f) \in P$. We conclude that $\overline{f}$ belongs to the ring of constants of every K-derivation of A.

If $\operatorname{char} K = 0$, then, by Corollary 2.4(a), $\overline{f} \in \overline{B}^A$, where B is the canonical homomorphic image of K in A. Hence $U(\overline{f}) = \overline{0}$ for some polynomial $U(T) \in B_0[T] \setminus B_0$. Let $U(T) = \overline{a_n}T^n + \cdots + \overline{a_1}T + \overline{a_0}$, where $a_n,\dots,a_1,a_0 \in K_0$, and put $W(T) = a_nT^n + \cdots + a_1T + a_0$. We may assume that the polynomial $W(T)$ belongs to $K[T]$ and is irreducible in $K[T]$. We deduce that $W(f) \in P$.

If $\operatorname{char} K = p > 0$, then $\overline{f} \in (KA^p)_0 \cap A$, by Corollary 2.4(b) and Proposition 2.2. Therefore $\overline{b} \cdot \overline{f} = \overline{-c}$ for some $b, c \in K[x_1^p,\dots,x_n^p]$, $b \notin P$, where we may assume that $\gcd(b,c) \sim 1$. We infer that $bf + c \in P$. ∎

In a special case when P is a principal ideal, we obtain a stronger result.

Proposition 3.3. *Let K be a UFD. Consider $f, g \in K[x_1,\dots,x_n] \setminus K$ such that g is irreducible and g divides $\partial f/\partial x_i$ for $i = 1,\dots,n$. If* $\operatorname{char} K = p > 0$, *assume additionally that $f, g \notin K[x_1^p,\dots,x_n^p]$.*

(a) *If* $\operatorname{char} K = 0$, *then there exists an irreducible polynomial $W(T) \in K[T]$, such that g^2 divides $W(f)$.*
(b) *If* $\operatorname{char} K = p > 0$, *then there exist $b, c \in K[x_1^p,\dots,x_n^p]$ such that g^2 divides $bf + c$, g does not divide b and* $\gcd(b,c) \sim 1$.

Proof. (a) Applying Theorem 3.1 to the prime ideal $P = (g)$, we obtain $W(f) = gh$ for some $h \in K[x_1,\dots,x_n]$. Since $g \notin K$, we have $\frac{\partial g}{\partial x_i} \neq 0$ for some i, and then $g \nmid \frac{\partial g}{\partial x_i}$. Taking the partial derivative with respect to x_i of both sides of the equality $W(f) = gh$ we obtain

$$W'(f)\frac{\partial f}{\partial x_i} = h\frac{\partial g}{\partial x_i} + g\frac{\partial h}{\partial x_i},$$

so $g \mid h\frac{\partial g}{\partial x_i}$. Hence $g \mid h$ and $g^2 \mid W(f)$.

(b) We use the same arguments as in case (a) with a polynomial $W(T) = bT + c \in K'[T]$, where $K' = K[x_1^p, \ldots, x_n^p]$. ∎

Note that as a consequence of the above proposition we obtain a characterization of polynomials with relatively prime partial derivatives. In the case of characteristic zero we have the following theorem.

Theorem 3.4. *Let K be a field of characteristic* 0, *and let $f \in K[x_1, \ldots, x_n] \setminus K$. The following conditions are equivalent:*

(i) $\gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$,
(ii) *for every irreducible polynomial $W(T) \in K[T]$, the polynomial $W(f)$ is square-free.*

4. One-element p-bases. In this section we obtain a characterization of one-element p-bases of rings of constants of K-derivations of $K[x_1, \ldots, x_n]$, where K is a UFD of characteristic $p > 0$.

If $f = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$, where $a_{i_1,\ldots,i_n} \in K$, then we set

$$f_{(p)} = \sum_{\substack{i_1,\ldots,i_n \geq 0 \\ p|i_1,\ldots,p|i_n}} a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}.$$

We can improve Proposition 3.3 from [5] in the following way.

Proposition 4.1. *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 $g \mid \frac{\partial f}{\partial x_i}$ for $i = 1, \ldots, n$, then $g \mid f - f_{(p)}$.*

Proof. By [5, Proposition 3.3], under these assumptions we have $g \mid f + h$ for some $h \in K[x_1^p, \ldots, x_n^p]$, so $f + h = gw$, where $w \in K[x_1, \ldots, x_n]$. Since $g \in K[x_1^p, \ldots, x_n^p]$, it is easy to check that $(gw)_{(p)} = gw_{(p)}$. Then $f_{(p)} + h = (f+h)_{(p)} = gw_{(p)}$, and we obtain $f - f_{(p)} = g(w - w_{(p)})$, that is, $g \mid f - f_{(p)}$. ∎

Now, we can prove the main theorem.

Theorem 4.2. *Let K be a UFD of characteristic $p > 0$, let $f \in K[x_1, \ldots, x_n] \setminus K[x_1^p, \ldots, x_n^p]$. The following conditions are equivalent:*

(i) $\gcd(\partial f/\partial x_1, \ldots, \partial f/\partial x_n) \sim 1$,
(ii) *$K[x_1^p, \ldots, x_n^p, f]$ is the ring of constants of a K-derivation,*
(iii) *for every $b, c \in K[x_1^p, \ldots, x_n^p]$ such that $b \neq 0$ and $\gcd(b, c) \sim 1$, the polynomial $bf + c$ is square-free and p-free,*
(iv) *the polynomial $f - f_{(p)}$ is p-free and, for every $b, c \in K[x_1^p, \ldots, x_n^p]$ such that $b \neq 0$ and $\gcd(b, c) \sim 1$, the polynomial $bf + c$ is square-free.*

Proof. The implication (i)$\Rightarrow$(ii) was proved in [5, Theorem 2.3]. The implication (iii)$\Rightarrow$(iv) is obvious.

(ii)$\Rightarrow$(iii). Assume that $K[x_1^p, \dots, x_n^p, f]$ is the ring of constants of some K-derivation of $K[x_1, \dots, x_n]$ and consider $b, c \in K[x_1^p, \dots, x_n^p]$ such that $b \neq 0$ and $\gcd(b, c) \sim 1$. If $h \mid bf + c$ for some $h \in K[x_1^p, \dots, x_n^p] \setminus K^*$, then $(b/h)f + c/h \in K[x_1, \dots, x_n]$, where $b/h, c/h \in K(x_1^p, \dots, x_n^p)$. By Lemma 2.6 we deduce that $b/h, c/h \in K[x_1^p, \dots, x_n^p]$, so $h \mid b$ and $h \mid c$, a contradiction.

Suppose that $g^2 \mid bf + c$ for some $g \in K[x_1, \dots, x_n] \setminus K^*$. If $p = 2$, then $g^2 \in K[x_1^p, \dots, x_n^p]$, and this is the case we have just considered. Assume that $p > 2$ and put $r = (p+1)/2$. Note that $g^p \mid g^{2r}$ and $g^{2r} \mid (bf + c)^r$, so $g^p \mid (bf + c)^r$. We have $(bf + c)^r = b^r f^r + \dots + c^r$, so $(b^r/g^p)f^r + \dots + c^r/g^p \in K[x_1, \dots, x_n]$. Since $r < p$, we deduce by Lemma 2.6 that $b^r/g^p, c^r/g^p \in K[x_1^p, \dots, x_n^p]$, so $g \mid b$ and $g \mid c$, a contradiction.

$\neg$(i)$\Rightarrow$ $\neg$(iv). Assume that $\gcd(\partial f/\partial x_1, \dots, \partial f/\partial x_n) \nsim 1$ and consider an irreducible polynomial $g \in K[x_1, \dots, x_n]$ such that $g \mid \frac{\partial f}{\partial x_i}$ for $i = 1, \dots, n$. If g belongs to $K[x_1^p, \dots, x_n^p]$, then $g \mid f - f_{(p)}$ by Proposition 4.1. If g does not belong to $K[x_1^p, \dots, x_n^p]$, then, by Proposition 3.3, $g^2 \mid bf + c$ for some $b, c \in K[x_1^p, \dots, x_n^p]$ such that $b \neq 0$ and $\gcd(b, c) \sim 1$. In both cases condition (iv) does not hold. ∎

References

[1] D. Daigle, *Locally nilpotent derivations*, lecture notes for the September School of Algebraic Geometry (Łukęcin, 2003) (unpublished), aix1.uottawa.ca/˜ddaigle/.

[2] A. van den Essen, A. Nowicki and A. Tyc, *Generalizations of a lemma of Freudenburg*, J. Pure Appl. Algebra 177 (2003), 43–47.

[3] G. Freudenburg, *A note on the kernel of a locally nilpotent derivation*, Proc. Amer. Math. Soc. 124 (1996), 27–29.

[4] P. Jędrzejewicz, *A note on rings of constants of derivations in integral domains*, Colloq. Math. 122 (2011), 241–245.

[5] —, *One-element p-bases of rings of constants of derivations*, Osaka J. Math. 46 (2009), 223–234.

[6] —, *Rings of constants of p-homogeneous polynomial derivations*, Comm. Algebra 31 (2003), 5501–5511.

[7] H. Matsumura, *Commutative Algebra*, 2nd ed., Benjamin, Reading, MA, 1980.

[8] A. Nowicki, *Polynomial derivations and their rings of constants*, Nicolaus Copernicus University, Toruń, 1994, www.mat.umk.pl/˜anow/.

[9] —, *Rings and fields of constants for derivations in characteristic zero*, J. Pure Appl. Algebra 96 (1994), 47–55.

[10] A. Nowicki and M. Nagata, *Rings of constants for k-derivations in* $k[x_1, \dots, x_n]$, J. Math. Kyoto Univ. 28 (1988), 111–118.

Piotr Jędrzejewicz
Faculty of Mathematics and Computer Science
Nicolaus Copernicus University
87-100 Toruń, Poland
E-mail: pjedrzej@mat.umk.pl

Received January 10, 2011 (7810)