

Rings of constants for k -derivations in $k[x_1, \dots, x_n]$

By

Andrzej NOWICKI and Masayoshi NAGATA

In this note we give several remarks on the rings of constants for a family D of k -derivations in the rings of polynomials over a field k .

1. Preliminaries.

Let us recall at first ([1]) that if $k[x_1, \dots, x_n]$ is the ring of polynomials over a commutative ring k and $f_1, \dots, f_n \in k[x_1, \dots, x_n]$ then there exists a unique k -derivation d of $k[x_1, \dots, x_n]$ such that $d(x_1) = f_1, \dots, d(x_n) = f_n$. This derivation d is defined by

$$d(h) = (\partial h / \partial x_1) f_1 + \dots + (\partial h / \partial x_n) f_n,$$

for $h \in k[x_1, \dots, x_n]$.

Let k be a field, A a commutative k -algebra with 1, and D a family of k -derivations of A . We denote by A^D the set of constants of A with respect to D , that is,

$$A^D = \{a \in A; d(a) = 0 \text{ for any } d \in D\}.$$

If D has only one element d then we write A^d instead of $A^{(d)}$. It is clear that $A^D = \bigcap_{d \in D} A^d$.

The set A^D is a k -subalgebra of A containing k . If A is a field then A^D is a subfield of A containing k .

Assume now that A has no zero divisors and A_0 is the field of quotients of A . Denote by \bar{D} the set $\{\bar{d}; d \in D\}$, where \bar{d} is the k -derivation of A_0 defined by

$$\bar{d}(a/b) = (d(a)b - ad(b))b^{-2},$$

for $a, b \in A$ and $b \neq 0$. In this situation we have two subfields of A_0 :

$$(A^D)_0 = \text{the field of quotients of } A^D,$$

$$(A_0)^{\bar{D}} = \text{the field of constants of } A_0 \text{ with respect to } \bar{D}.$$

The following example shows that these subfields could be different

Example 1.1. Let $\text{char}(k)=0$ and let d be the k -derivation of $A=k[x, y]$ such that $d(x)=x$ and $d(y)=y$. Then $(A^d)_0 \neq (A_0)^{\bar{d}}$.

Proof. It is easy to show that $(A^d)_0=k$ and $x/y \in (A_0)^{\bar{d}} \setminus k$.

Proposition 1.2. If D is a family of k -derivations in a k -domain A then

- (1) $k \subseteq A^D \subseteq (A^D)_0 \subseteq (A_0)^{\bar{D}} \subseteq A_0$,
- (2) $(A^D)_0 \cap A = (A_0)^{\bar{D}} \cap A = A^D$.

The proof is straightforward.

2. The case $\text{char}(k)=0$.

In this section k is always a field of characteristic zero.

Lemma 2.1. If D is a family of k -derivations in a k -domain A then the ring A^D is integrally closed in A .

Proof. Let $a \in A$ be an integral element over A^D and let

$$a^n + c_1 a^{n-1} + \cdots + c_{n-1} a + c_n = 0,$$

where $c_1, \dots, c_n \in A^D$ and n is minimal. If $d \in D$ then

$$0 = d(0) = ud(a),$$

where $u = na^{n-1} + (n-1)c_1 a^{n-2} + \cdots + c_{n-1}$. Since $u \neq 0$ (because n is minimal and $\text{char}(k)=0$), $d(a)=0$ and hence, $a \in \bigcap_{d \in D} A^d = A^D$.

As an immediate consequence of Lemma 2.1 we obtain

Proposition 2.2. If D is a family of k -derivations of $A=k[x_1, \dots, x_n]$, where k is a field of characteristic zero, then the ring A^D is integrally closed in A . In particular A^D is normal.

Note the following well known ([3] p. 177)

Lemma 2.3. Let $L \subseteq K$ be a separable algebraic extension of fields. If d is an L -derivation of K then $d=0$.

This lemma implies

Proposition 2.4. If D is a non-zero family of k -derivations of $A=k[x_1, \dots, x_n]$, where k is a field of characteristic zero, then $\text{tr.deg}_k(A^D) \leq n-1$.

Proof. Let $s = \text{tr.deg}_k(A^D)$, $K=k(x_1, \dots, x_n)$ and $L=(A_0)^{\bar{D}}$. It is clear that $s \leq n$. Suppose now that $s=n$. Then $L \subseteq K$ is a separable algebraic field extension. If $d \in D$ then \bar{d} is an L -derivation of K so, by Lemma 2.3, $\bar{d}=0$ and hence $d=0$; that is, $D=0$ and we have a contradiction to our assumption.

Now let us recall a result due to Zariski ([9], see [5] p. 41)

Zariski's Theorem 2.5. Let k be a field and let L be a subfield of $k(x_1, \dots, x_n)$

containing k . If $\text{tr.deg}_k(L) \leq 2$ then the ring $L \cap k[x_1, \dots, x_n]$ is finitely generated over k .

As a consequence of the Zariski's Theorem, Propositions 2.4 and 1.2(2) we obtain the following

Theorem 2.6. *Let D be a family of k -derivations of the polynomial ring $k[x_1, \dots, x_n]$ over a field k of characteristic zero. If $n \leq 3$ then there exist polynomials $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ such that $k[x_1, \dots, x_n]^D = k[f_1, \dots, f_s]$.*

The next result is due to Zaks ([8], see also [2]).

Zaks' Theorem 2.7. *Let k be a field. If R is a Dedekind subring of $k[x_1, \dots, x_n]$ containing k then there exist a polynomial $f \in k[x_1, \dots, x_n]$ such that $R = k[f]$.*

By Zaks' Theorem and Theorem 2.6 we have

Theorem 2.8. *Let $\text{char}(k) = 0$ and let D be a non-zero family of k -derivations of $k[x, y]$. Then there exists a polynomial $f \in k[x, y]$ such that $k[x, y]^D = k[f]$.*

Proof. Let $R = k[x, y]^D$ and $s = \text{tr.deg}_k(R)$. We know, by Proposition 2.4, that $s \leq 1$. If $s = 0$ then $R = k$, so $R = k[f]$, where for example $f = 1$. If $s = 1$ then, by Proposition 2.2 and Theorem 2.6, R is a Dedekind subring of $k[x, y]$ containing k and hence, by Zaks' Theorem, $R = k[f]$, for some $f \in k[x, y]$.

3. Closed polynomials in characteristic zero.

Consider the following family \mathcal{M} of subrings in $k[x_1, \dots, x_n]$:

$$\mathcal{M} = \{k[f]; f \in k[x_1, \dots, x_n] \setminus k\}.$$

If $\text{char}(k) = 0$ and $k[f] \subseteq k[g]$, for some polynomials $f, g \in k[x_1, \dots, x_n] \setminus k$, then $\deg(f) > \deg(g)$ and hence, we see that in the family \mathcal{M} there exist maximal elements.

We shall say that a polynomial $f \in k[x_1, \dots, x_n] \setminus k$ is *closed* if the ring $k[f]$ is integrally closed in $k[x_1, \dots, x_n]$.

Lemma 3.1. *Let $\text{char}(k) = 0$ and $f \in k[x_1, \dots, x_n] \setminus k$. Then f is closed if and only if the ring $k[f]$ is a maximal element in \mathcal{M} .*

Proof. Let f be closed and assume that $k[f] \subseteq k[g]$ for some $g \in k[x_1, \dots, x_n]$. Then $f \in k[g]$, that is,

$$f = a_s g^s + \dots + a_1 g + a_0,$$

for some $a_0, \dots, a_s \in k$ with $a_s \neq 0$. Hence

$$g^s + a_s^{-1} a_{s-1} g^{s-1} + \dots + a_s^{-1} a_1 g + (a_s^{-1} a_0 - f) = 0$$

and hence g is integral over $k[f]$. Since $k[f]$ is integrally closed in $k[x_1, \dots, x_n]$, $k[f] = k[g]$ and we see that $k[f]$ is maximal in \mathcal{M} .

Assume now that $k[f]$ is a maximal element in \mathcal{M} and denote by E the integral closure of $k[f]$ in $k[x_1, \dots, x_n]$. Then E is a Dedekind subring of

$k[x_1, \dots, x_n]$ containing k so, by Theorem 2, 7, $E = k[h]$, for some $h \in k[x_1, \dots, x_n]$. Now, by the maximality of $k[f]$ in \mathcal{M} , $k[f] = k[h] = E$ and so, f is closed.

Proposition 3.2. *Let D be a family of k -derivations in $A = k[x_1, \dots, x_n]$, where k is a field of characteristic zero. If the ring A^D is finitely generated over k (for example, if $n \leq 3$) then $A^D = k$ or there exist closed polynomials $f_1, \dots, f_s \in A$ such that $A^D = k[f_1, \dots, f_s]$.*

Proof. Assume that $A^D \neq k$ and let $A^D = k[h_1, \dots, h_s]$ for some $h_1, \dots, h_s \in A - k$. Let f_1, \dots, f_s be polynomials in $A \setminus k$ such that $k[h_i] \subseteq k[f_i]$ and $k[f_i]$ is a maximal element in \mathcal{M} , for $i = 1, \dots, s$. Then there exist polynomials $u_1(t), \dots, u_s(t) \in k[t]$ such that $h_i = u_i(f_i)$, for $i = 1, \dots, s$. We may assume that the polynomials $u_1(t), \dots, u_s(t)$ have minimal degrees. Now, using the same argument as in the proof of Lemma 2.1, we see that $f_1, \dots, f_s \in A^D$. Hence $k[f_1, \dots, f_s] \subseteq A^D = k[h_1, \dots, h_s] \subseteq k[f_1, \dots, f_s]$, that is, $A^D = k[f_1, \dots, f_s]$ and, by Lemma 3.1, f_1, \dots, f_s are closed.

Proposition 3.3. *Let D be a non-zero family of k -derivations in $k[x, y]$, where k is a field of characteristic zero. Denote $R = k[x, y]^D$. If $f \in R \setminus k$, then R is the integral closure of the ring $k[f]$ in $k[x, y]$.*

Proof. If $f \in R \setminus k$ then $R \neq k$ and, by Theorem 2.8 and Proposition 3.2, $R = k[h]$, for some closed polynomial $h \in k[x, y]$. Hence $k[f] \subseteq k[h]$, $k[h]$ is integrally closed in $k[x, y]$ and $k[h]$ is integral over $k[f]$. This means that $R = k[h]$ is the integral closure of $k[f]$ in $k[x, y]$.

Theorem 3.4. *Let k be a field of characteristic zero and let A be a subring of $k[x, y]$ containing k , such that A is integrally closed in $k[x, y]$. If $\text{Krull-dim}(A) \leq 1$ then there exists a k -derivation d of $k[x, y]$ such that $A = k[x, y]^d$.*

Proof. Let $s = \text{Krull-dim}(A)$. If $s = 0$ then $A = k$ and we have $A = k[x, y]^d$, where, for example, d is such k -derivation of $k[x, y]$ that $d(x) = x$ and $d(y) = y$.

Assume that $s = 1$. Then A is a Dedekind subring of $k[x, y]$ containing k (see [2] Theorem 1) hence, by Theorem 2.7, $A = k[h]$ for some closed polynomial $h \in k[x, y] \setminus k$. Consider k -derivation d of $k[x, y]$ such that $d(x) = \partial h / \partial y$, $d(y) = -\partial h / \partial x$. Then $h \in k[x, y]^d \setminus k$ and we see, by Proposition 3.3, that $A = k[x, y]^d$.

4. The case $\text{char}(k) = p > 0$.

Throughout this section k is a field of characteristic $p > 0$.

Denote $A = k[x_1, \dots, x_n]$, $R = k[x_1^p, \dots, x_n^p]$. It is well known that A is a free R -module on the basis (p -basis)

$$\{x_1^{i_1} \cdots x_n^{i_n}; i_1 < p, \dots, i_n < p\}$$

and hence, in particular, A is a noetherian R -module.

If D is a family of k -derivations of A then $R \subseteq A^D$ and so, A^D is an R -submodule of A . Therefore we have

Proposition 4.1. *If D is a family of k -derivations of $A = k[x_1, \dots, x_n]$, where k is a field of characteristic $p > 0$, then there exist polynomials $f_1, \dots, f_s \in A$ such that*

$$A^D = k[x_1^D, \dots, x_n^D, f_1, \dots, f_s].$$

If $\text{char}(k)=2$ and $n=2$ then the following proposition shows (if $D \neq 0$ and s is as in Proposition 4.1) that $s=1$.

Proposition 4.2. *Let k be a field of characteristic two and let D be a non-zero family of k -derivations in $k[x, y]$. Then there exists a polynomial $f \in k[x, y]$ such that $k[x, y]^D = k[x^2, y^2, f]$.*

Proof. If $k[x, y]^D = k[x^2, y^2]$, then $k[x, y]^D = k[x^2, y^2, f]$, where $f=1$. Assume that $k[x, y]^D \neq k[x^2, y^2]$. Let f_1, \dots, f_s be as in Proposition 4.1, and let $f_i = a_i x + b_i y + c_i xy + u_i$, where $a_i, b_i, c_i, u_i \in k[x^2, y^2]$, for $i=1, \dots, s$.

We may assume that

- (1) f_1, \dots, f_s do not belong to $k[x^2, y^2]$,
- (2) $u_1 = \dots = u_s = 0$.

Moreover, we may assume that

- (3) there is no elements $v_i \in k[x^2, y^2] \setminus k$ such that $v_i \mid f_i$, for $i=1, \dots, s$.

In fact, if for example $f_1 = vg$, where $v \in k[x^2, y^2] \setminus k$ and $g \in k[x, y]$, then for any $d \in D$, $0 = d(f_1) = vd(g)$, that is, $d(g) = 0$ and hence $g \in k[x, y]^D$ and we have $k[x, y]^D = k[x^2, y^2, g, f_2, \dots, f_s]$.

Denote by L the field $k(x^2, y^2)[f_1, \dots, f_s]$ and let $m = [L : k(x^2, y^2)]$. Then $m=4, 2$ or 1 . If $m=4$ then $L = k(x, y)$ and we have a contradiction to the assumption that $D \neq 0$. If $m=1$, then $k[x, y]^D = k[x^2, y^2]$.

Assume now that $m=2$. Then $L = k(x^2, y^2)[f_i]$, for some $i=1, \dots, s$ (since $k(x^2, y^2)[f_i]$ is a two-dimensional subspace of L over $k(x^2, y^2)$), and, in particular, we have $af_1 = bf_2 + c$, where a and b are non-zero elements in $k[x^2, y^2]$ and $c \in k[x^2, y^2]$. But $c=0$, by (2), hence $af_1 = bf_2$. Let $u = \gcd(a, b)$, $a = ua'$, $b = ub'$, for $a', b' \in k[x, y]$. Then $a'f_1 = b'f_2$, $\gcd(a', b')=1$ and it is easy to show that $k \setminus \{0\} \subset k[x^2, y^2]$. This implies that $a' \mid f_2$, $b' \mid f_1$ so, by (3), a' and b' belong to $k \setminus \{0\}$. Therefore $f_1 = cf_2$, for some $c \in k \setminus \{0\}$ and we have

$$k[x, y]^D = k[x^2, y^2, f_2, f_3, \dots, f_s].$$

Repeating the above argument we see that $k[x, y]^D = k[x^2, y^2, f_s]$.

If $\text{char}(k)=p>2$ then the assertion of Proposition 4.2 is not true, in general.

Example 4.3. *Let $\text{char}(k)=p>2$ and let d be the k -derivation of $k[x, y]$ such that $d(x)=x$, and $d(y)=y$. Then there is no polynomial $f \in k[x, y]$ such that $k[x, y]^d = k[x^p, y^p, f]$.*

Proof. Suppose that $k[x, y]^d = k[x^p, y^p, f]$, for some $f \in k[x, y]$, and consider the monomials $x^{p-1}y$ and xy^{p-1} . We see that these monomials belong to $k[x, y]^d$. Therefore

$$x^{p-1}y = u(f) \text{ and } xy^{p-1} = v(f),$$

for some polynomials $u(t), v(t) \in k[x^p, y^p][t]$, and we have

$$-x^{p-2}y = (\partial/\partial x)(x^{p-1}y) = u'(f)(\partial f/\partial x)$$

$$\begin{aligned}
x^{p-1} &= (\partial/\partial y)(x^{p-1}y) = u'(f)(\partial f/\partial y) \\
y^{p-1} &= (\partial/\partial x)(xy^{p-1}) = v'(f)(\partial f/\partial x) \\
-xy^{p-2} &= (\partial/\partial y)(xy^{p-1}) = v'(f)(\partial f/\partial y),
\end{aligned}$$

where $u'(t)$, $v'(t)$ are derivatives of $u(t)$ and $v(t)$, respectively. This implies, in particular, that $u'(f) = ax^{p-2}$, for some $a \in k \setminus \{0\}$. Hence $x^{p-2} \in k[x^p, y^p, f] = k[x, y]^d$. But it is a contradiction, because $d(x^{p-2}) = -2x^{p-3} \neq 0$.

Observe that if $n=2$ and $p=2$ then, by Proposition 4.2, every ring of constants is a free $k[x^p, y^p]$ -module. Now we shall show that it is also true for an arbitrary $p > 0$ and $D = \{d\}$.

Theorem 4.4. *Let k be a field of characteristic $p > 0$ and d a k -derivation of $k[x, y]$. Then the ring $k[x, y]^d$ is a free $k[x^p, y^p]$ -module.*

Before the proof of Theorem 4.4 we recall a few facts for M -sequences in regular local rings (see [6]).

Let R be a commutative ring and M a non-zero R -module. We denote by $\text{hd}(M)$ the projective dimension of M . An element $r \in R$ is called a zero divisor with respect to M if there is a nonzero element m of M such that $rm = 0$.

Assume now that R is a regular local ring with the maximal ideal \mathfrak{m} and $M \neq 0$ is a finitely generated R -module.

We say that a sequence t_1, \dots, t_n of elements of \mathfrak{m} is an M -sequence if t_i is not a zero divisor with respect to $M / \sum_{j=1}^{i-1} t_j M$, for each $i=1, \dots, n$. It is known (see [6] p.97) that all maximal M -sequences have the same length, this length we denote by $s(M)$.

Note the following theorem which is due to Auslander, Buchsbaum and Serre (see [6] p.98)

Theorem 4.5. *Let (R, \mathfrak{m}) be a regular local ring and M a finitely generated R -module different from zero. Then*

$$\text{hd}(M) = \text{Krull-dim}(R) - s(M).$$

Proof of Theorem 4.4. Denote $R = k[x^p, y^p]$, $A = k[x, y]$, $M = d(A)$, $K = k[x, y]^d$ and consider the following exact sequence of R -modules:

$$(1) \quad 0 \longrightarrow K \longrightarrow A \xrightarrow{d} M \longrightarrow 0.$$

Let \mathfrak{m} be a maximal ideal of R . Then the sequence (1) induces the exact sequence of $R_{\mathfrak{m}}$ -modules:

$$(2) \quad 0 \longrightarrow K_{\mathfrak{m}} \longrightarrow A_{\mathfrak{m}} \xrightarrow{d_{\mathfrak{m}}} M_{\mathfrak{m}} \longrightarrow 0.$$

Since $R_{\mathfrak{m}}$ is a regular local ring and $M_{\mathfrak{m}}$ is a finitely generated $R_{\mathfrak{m}}$ -module different from zero, we have (by Theorem 4.5)

$$\text{hd}(M_{\mathfrak{m}}) = 2 - s(M_{\mathfrak{m}}).$$

But M_m is contained in the ring A_m which is an integral domain and so, $s(M_m) \geq 1$. Therefore $hd(M_m) \leq 1$ and hence, by the sequence (2) (since A_m is a free R_m -module), $hd(K_m) = 0$ and we have $hd(K) = \sup_m hd(M_m) = 0$. This implies that K is a projective R -module and hence, by [7] (see [4]), $K = k[x, y]^d$ is a free $k[x^p, y^p]$ -module.

The next example shows that if $n \geq 3$ then the assertion of Theorem 4.4 is not true, in general.

Example 4.6. Let $\text{char}(k) = p > 0$, $n \geq 3$, and let d be the k -derivation of $k[x_1, \dots, x_n]$ such that $d(x_i) = x_i^p$, for $i = 1, \dots, n$. Then the ring $k[x_1, \dots, x_n]^d$ is not a free $k[x_1^p, \dots, x_n^p]$ -module.

Proof. Denote $R = k[x_1^p, \dots, x_n^p]$, $A = k[x_1, \dots, x_n]$, $M = d(A)$ and $K = A^d$. Let \mathfrak{m} be the maximal ideal of R generated by x_1^p, \dots, x_n^p and consider the exact sequences (1) and (2) as in the proof of Theorem 4.4. We shall show that $s(M_m) = 1$.

Let $t_1 = x_1^p/1, \dots, t_n = x_n^p/1$. The elements t_1, \dots, t_n generate the maximal ideal $\mathfrak{m}R_m$. Observe that t_1 is not a zero divisor with respect to M_m , and $t_1 \in M_m \setminus t_1 M_m$ (since $1 \notin M$). If u is an arbitrary element of $\mathfrak{m}R_m$, then $u = a_1 t_1 + \dots + a_n t_n$, for some $a_1, \dots, a_n \in R_m$ and we have

$$\begin{aligned} u &= a_1 d_m(x_1/1) + \dots + a_n d_m(x_n/1) \\ &= d_m(a_1(x_1/1) + \dots + a_n(x_n/1)), \end{aligned}$$

that is, $u \in M_m$ and hence, $t_1 u \in t_1 M_m$.

Therefore t_1 is a maximal M_m -sequence and hence (since all maximal M_m -sequences have the same length), $s(M_m) = 1$. Now, by Theorem 4.5, $hd(M_m) = n - 1 \geq 2$ and hence, $hd(K_m) \geq 1$. This implies that $hd(K) = \sup hd(K_m) \geq 1$, that is, $K = k[x_1, \dots, x_n]^d$ is not a free $k[x_1^p, \dots, x_n^p]$ -module.

Remark 4.7. Using the same argument as in the proof of Example 4.6 we may prove that if $n \geq 3$ and $d(x_i) = x_{v(i)}^p$, where v is a permutation of $\{1, \dots, n\}$, then the ring $k[x_1, \dots, x_n]^d$ is not a free $k[x_1^p, \dots, x_n^p]$ -module.

INSTITUTE OF MATHEMATICS
COPERNICUS UNIVERSITY
TORUN, Poland
and
DEPARTMENT OF MATHEMATICS
SHINSHU UNIVERSITY
and
DEPARTMENT OF MATHEMATICS
KYOTO UNIVERSITY

References

- [1] N. Bourbaki, *Elements de Mathématique, Algèbre Commutative*, Chapter 2, Herman, Paris, 1961.
- [2] P. Eakin, A note on finite dimensional subrings of polynomial rings, *Proc. Amer. Math. Soc.*, **31** (1972), 75–80.
- [3] N. Jacobson, *Lectures in Abstract Algebra*, Vol. 3, Van Nostrand, Princeton, N.J., 1964.
- [4] T.Y. Lam, *Serre's Conjecture*, *Lect. Notes in Math.*, 635, 1978.
- [5] M. Nagata, *Lectures on the Fourteenth Problem of Hilbert*, Tata Institute of Fundamental Research, Bombay, 1965.
- [6] M. Nagata, *Local Rings*, Interscience Tracts in Pure and Appl. Math., No. 13, Interscience. New York, 1972.
- [7] C.S. Seshadri, Triviality of vector bundles over the affine space K^2 , *Proc. Nat'l. Acad. Sci. U.S.A.*, **44** (1958), 456–458.
- [8] A. Zaks, Dedekind subrings of $k[x_1, \dots, x_n]$ are rings of polynomials, *Israel J. Math.*, **9**(1971), 285–289.
- [9] O. Zariski, Interpretations algebrico-geometriques du quatorzieme probleme de Hilbert, *Bull. Sci. Math.*, **78** (1954), 155–168.