Final version published in *Communications in Algebra* **39** (2011), 3138-3150.

Monomial derivations

Jean Moulin Ollagnier[1] and **Andrzej Nowicki**[2]

[1]Laboratoire LIX, École Polytechnique, F 91128 Palaiseau Cedex, France
and : Université Paris XII, Créteil, France,
(e-mail : Jean.Moulin-Ollagnier@polytechnique.edu).

[2]N. Copernicus University, Faculty of Mathematics and Computer Science,
87-100 Toruń, Poland, (e-mail: anow@mat.uni.torun.pl).

Abstract

We present some general properties of monomial derivations of the polynomial ring $k[x_1, \dots, x_n]$, where k is a field of characteristic zero. The main result of this paper is a characterization of some large class of monomial derivations without Darboux polynomials. In particular, we present a full description of all monomial derivations of $k[x, y, z]$ which have no Darboux polynomials.

Key Words: Derivation; Darboux polynomial; Field of constants; Jouanolou derivation.

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

Introduction

Let k be a field of characteristic zero, $k[X] = k[x_1, \dots, x_n]$ be the polynomial ring in n variables over k, and $k(X) = k(x_1, \dots, x_n)$ be the field of quotients of $k[X]$.

Let us assume that d is a derivation of $k[X]$, We denote also by d the unique extension of d to $k(X)$, and we denote by $k(X)^d$ the field of rational constants of d, that is,

$$k(X)^d = \{\varphi \in k(X);\ d(\varphi) = 0\}.$$

[0]Corresponding author : Andrzej Nowicki, N. Copernicus University, Faculty of Mathematics and Computer Science, ul. Chopina 12/18, 87–100 Toruń, Poland. E-mail: `anow@mat.uni.torun.pl`.

We say that this field is trivial if $k(X)^d = k$. A polynomial $F \in k[X]$ is said to be a *Darboux polynomial* of d if $F \notin k$ and $d(F) = \Lambda F$ for some $\Lambda \in k[X]$. We say that d is *without Darboux polynomials* if d has no Darboux polynomials.

It is obvious that if d is without Darboux polynomials, then the field $k(X)^d$ is trivial. The opposite implication is, in general, not true. The derivation $\delta = x\partial_x + (x+y)\partial_y$ of $k[x,y]$ has trivial field of constants (see [15], [14]), and x is a Darboux polynomial of δ. In this paper we prove that such opposite implications is true for a large class of monomial derivations of $k[X]$. More precisely, we say that a derivation d of $k[X]$ is *monomial* if

$$d(x_i) = x_1^{\beta_{i1}} \cdots x_n^{\beta_{in}}$$

for $i = 1, \ldots, n$, where each β_{ij} is a nonnegative integer. In this case we say that d is *normal monomial* if $\beta_{11} = \beta_{22} = \cdots = \beta_{nn} = 0$ and $\omega_d \neq 0$, where ω_d is the determinant of the matrix $[\beta_{ij}] - I$, that is,

$$\omega_d = \begin{vmatrix} \beta_{11}-1 & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22}-1 & \ldots & \beta_{2n} \\ \vdots & \cdots & & \vdots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn}-1 \end{vmatrix}.$$

The main result of the paper is Theorem 4.2, which states that if d is a normal monomial derivation of $k[X]$, then d is without Darboux polynomials if and only if $k(X)^d = k$.

The fact that for some derivation d, the triviality of $k(X)^d$ implies that d is without Darboux polynomials, plays an important role in several papers concerning polynomial derivations. Let us mention some papers on Jouanolou derivations. By the *Jouanolou derivation* with integer parameters $n \geq 2$ and $s \geq 1$ we mean a normal monomial derivation $d : k[X] \to k[X]$ such that

$$d(x_1) = x_2^s,\ d(x_2) = x_3^s,\ \ldots,\ d(x_{n-1}) = x_n^s,\ d(x_n) = x_1^s.$$

We denote such a derivation by $J(n,s)$. If $n = 2$ or $s = 1$, then $J(n,s)$ has a nontrivial rational constant (see, for example, [13] or [8]). In 1979 Jouanolou, in [3], proved that the derivation $J(3,s)$, for every $s \geq 2$, has no nontrivial Darboux polynomial. Today we know several different proofs of this fact ([7], [1], [18], [13]). There exists a proof ([8]) that the same is true for $s \geq 2$ and for every prime number $n \geq 3$. There are also separate such proofs for $n = 4$ and $s \geq 2$ ([19], [9], [10]). In 2003 Żołądek ([19]) proved the same for all $n \geq 3$ and $s \geq 2$. Some of these proofs were reduced only to proofs that Jouanolou derivations have trivial fields of constants.

In [16] there is a full description of all monomial derivations of $k[x,y,z]$ with trivial field of constants. Using this description and several additional facts, we presented, in [12], full lists of homogeneous monomial derivations of degrees $s \leqslant 4$ (of $k[x,y,z]$) without Darboux polynomials. Now, thanks to the main result of this paper, we are ready to present such lists for arbitrary degree $s \geqslant 2$. All monomial derivations d with trivial field of constants, which are described in [16], are without Darboux polynomials if and only if $x_i \nmid d(x_i)$ for all $i = 1, \dots, n$.

1 Notations and preliminary facts

Throughout this paper k is a field of characteristic zero. If $\mu = (\mu_1, \dots, \mu_n)$ is a sequence of integers, then we denote by X^μ the rational monomial $x_1^{\mu_1} \cdots x_n^{\mu_n}$ belonging to $k(X)$. In particular, if $\mu \in \mathbb{N}^n$ (where $\mathbb{N}$ denote the set of nonnegative integers), then X^μ is an ordinary monomial of $k[X]$. Note the following well-known lemma.

Lemma 1.1 ([2], [16]). *Let $a_1 = (a_{11}, \dots, a_{1n}), \dots, a_n = (a_{n1}, \dots, a_{nn})$ be elements of $\mathbb{Z}^n$, and let A denote the $n \times n$ matrix $[a_{ij}]$. If $\det A \neq 0$, then the rational monomials $X^{\alpha_1}, \dots, X^{\alpha_n}$ are algebraically independent over k.*

Assume now that $\beta_1, \dots, \beta_n \in \mathbb{N}^n$ and consider a monomial derivation $d : k[X] \to k[X]$ of the form

$$d(x_1) = X^{\beta_1}, \quad \dots, \quad d(x_n) = X^{\beta_n}.$$

Put $\beta_1 = (\beta_{11}, \dots, \beta_{1n}), \dots, \beta_n = (\beta_{n1}, \dots, \beta_{nn})$, where each β_{ij} is a nonnegative integer, and let $A = [a_{ij}]$ denote the matrix $[\beta_{ij}] - I$, where I is the $n \times n$ identity matrix. Let us recall (see Introduction) that we denote by ω_d the determinant of the matrix A. Put

$$y_1 = \frac{d(x_1)}{x_1}, \quad \dots, \quad y_n = \frac{d(x_n)}{x_n}.$$

Then $y_1 = X^{a_1}, \dots, y_n = X^{a_n}$, where each a_i, for $i = 1, \dots, n$, is equal to $(a_{i1}, \dots, a_{in})$. It is easy to check that

$$d(y_i) = y_i(a_{i1}y_1 + \cdots + a_{in}y_n),$$

for all $i = 1, \dots, n$. This implies, in particular, that $d(R) \subseteq R$, where R is the smallest k-subalgebra of $k(X)$ containing $y_1, \dots, y_n$. Observe that if $\omega_d \neq 0$, then (by Lemma 1.1) the elements $y_1, \dots, y_n$ are algebraically independent over k. Thus, if $\omega_d \neq 0$, then $R = k[Y] = k[y_1, \ldots, y_n]$ is a polynomial ring over k in n variables, and we have a new derivation $\delta : k[Y] \to k[Y]$ such that

$$\delta(y_1) = y_1(a_{11}y_1 + \cdots + a_{1n}y_n), \quad \cdots, \quad \delta(y_n) = y_n(a_{n1}y_1 + \cdots + a_{nn}y_n).$$

The derivation δ is the restriction of d to $k[Y]$. We call δ the *factorisable derivation associated with* d. The concept of factorisable derivation associated with a derivation was introduced by Lagutinskii in [5] and this concept was intensively studied in [8], [16] and [17]

We will say (as in [11], [9] and [16]) that a Darboux polynomial $F \in k[Y] \smallsetminus k$ of δ is *strict* if F is not divisible by any of the variables $y_1, \ldots, y_n$. Let us recall, from [16], the following proposition.

Proposition 1.2 ([16]). *Let $d : k(X) \to k(X)$ be a monomial derivation such that $\omega_d \neq 0$, and let $\delta : k[Y] \to k[Y]$ be the factorisable derivation associated with d. Then the following conditions are equivalent.*

(1) $k(X)^d \neq k$.

(2) $k(Y)^\delta \neq k$.

(3) *The derivation δ has a strict Darboux polynomial.*

2 The field extension $\mathbf{k(Y) \subset k(X)}$

In this section we present some preparatory properties of the field extension $k(Y) \subset k(X)$. We use mostly the same notations as in Section 1.

Let us assume that $a_1 = (a_{11}, \ldots, a_{1n}), \ldots, a_n = (a_{n1}, \ldots, a_{nn})$ are elements belonging to $\mathbb{Z}^n$, and let A denote the $n \times n$ matrix $[a_{ij}]$. Put

$$N = |\det A|,$$

and assume that $N \geqslant 1$. Let $X = \{x_1, \ldots, x_n\}$ be a set of variables over k, and let $Y = \{y_1, \ldots, y_n\}$, where each y_i is the rational monomial $X^{a_i} = x_1^{a_{i1}} \cdots x_n^{a_{in}}$, for $i = 1, \ldots, n$.

Since $\det A \neq 0$, the matrix A is invertible over $\mathbb{Q}$. This means that there exists an $n \times n$ matrix $A' = \left[a'_{ij}\right]$ such that each a'_{ij} is an integer, and

$$AA' = A'A = NI,$$

where I is the $n \times n$ identity matrix.

Look at the field extension $k(Y) \subset k(X)$. Since $\det A \neq 0$, this extension is (by Lemma 1.1) algebraic. But $k(X)$ is finitely generated over k, so the extension $k(Y) \subset k(X)$ is finite. We will show, in the next section, that if the field k is algebraically closed, then this extension is Galois. In this section we prove several lemmas and propositions which are needed for our proof of this fact.

We denote by $k\langle[Y]\rangle$ the ring of fractions of the polynomial ring $k[Y] = k[y_1, \dots, y_n]$ by the multiplicatively closed subset $\{y_1^{m_1} \cdots y_n^{m_n};\ m_a, \dots, m_n \in \mathbb{N}\}$. This ring is of course a subring of the field $k(Y)$. Every nonzero element of $k\langle[Y]\rangle$ is of the form $Y^u h$, where $Y^u = y_1^{u_1} \cdots y_n^{u_n}$ with $u_1, \dots, u_n \in \mathbb{Z}$, and h is a strict polynomial belonging to $k[Y]$, that is, $0 \neq h \in k[Y]$ and h is not divisible by any of the variables $y_1, \dots, y_n$.

Lemma 2.1. *The monomials $x_1^N, \dots, x_n^N$ belong to $k\langle[Y]\rangle$. Thus, all polynomials in $k[X]$ are integral over $k\langle[Y]\rangle$.*

Proof. For every $i = 1, \dots, n$, we have $x_i^N = \prod_{j=1}^{n} y_j^{a'_{ij}} \in k\langle[Y]\rangle$. $\square$

The next lemma is obvious.

Lemma 2.2. *The field $k(Y)$ does not change if we use the following elementary transformations of rows of the matrix A.*

(1) *The interchange of two rows.*

(2) *The multiplication of one row by -1.*

(3) *The addition of an integer multiple of one row to another row.*

Moreover, in each of these transformations the number N does not change.

Applying the above elementary transformations, the Euclidean algorithm and a standard procedure, we may assume that the matrix A has the following lower-triangular form

$$(*) \qquad a = \begin{bmatrix} m_1 & 0 & 0 & \cdots & 0 \\ a_{21} & m_2 & 0 & \cdots & 0 \\ a_{31} & a_{32} & m_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & m_n \end{bmatrix},$$

where $m_1, \dots, m_n$ are positive integer, $m_1 \cdots m_n = N$, and each a_{ij} is a nonnegative integer smaller than m_j.

Note the following well-known lemma (see, for example, [6]).

Lemma 2.3. *Let $L[t]$ be a polynomial ring in one variable t over a field L. Let φ be a nonzero polynomial, belonging to $L[t]$, of degree $m \geqslant 1$. Then $L(\varphi) \subset L(t)$ is a finite field extension, and $(L(t) : L(\varphi)) = m$.*

Now we may prove the following proposition.

Proposition 2.4. *Let $a_1 = (a_{11}, \dots, a_{1n}), \dots, a_n = (a_{n1}, \dots, a_{nn})$ are elements belonging to $\mathbb{Z}^n$, and let A denote the $n \times n$ matrix $[a_{ij}]$. Put $N = |\det A|$, and assume that $N \geqslant 1$. Let $X = \{x_1, \dots, x_n\}$ be a set of variables over a field k, and let $Y = \{y_1, \dots, y_n\}$, where each y_i, for $i = 1, \dots, n$, is the rational monomial $X^{a_i} = x_1^{a_{i1}} \cdots x_n^{a_{in}}$. Then the dimension of the linear space $k(X)$ over $k(Y)$ is equal to N, that is, $(k(X) : k(Y)) = N$.*

Proof. It follows from Lemma 2.2 that we only need to consider the case where the matrix A is of the form $(*)$. Let $M_0 = k(Y) = k(y_1, \dots, y_n)$ and

$$M_i = k(x_1, x_2, \dots, x_{i-1}, y_i, y_{i+1}, \dots, y_n),\ i = 1, \dots, n.$$

In particular, $M_1 = k(x_1, y_2, y_3, \dots, y_n)$ and $M_n = k(x_1, \dots, x_n) = k(X)$. Then we have the tower of fields:

$$k(Y) = M_0 \subset M_1 \subset \cdots \subset M_n = k(X).$$

Let $i \in \{1, \dots, n\}$ and denote by L_i the field $k(x_1, \dots, x_{i-1}, y_{i+1}, \dots, y_n)$. Then we have:

$$\begin{aligned} M_{i-1} &= k\left(x_1, \dots, x_{i-1}, y_i, \dots, y_n\right) = L_i(y_i) = L_i\left(x_1^{a_{i1}} \cdots x_{i-1}^{a_{i,i-1}} x_i^{m_i}\right) = L_i\left(x_i^{m_i}\right) \\ &\subset L_i(x_i) = k(x_1, \dots, x_i, y_{i+1}, \dots, y_n) = M_i. \end{aligned}$$

It is obvious that x_i is algebraically independent over L_i. Thus, Lemma 2.3 implies that $(L_i(x_i) : L_i(x_i^{m_i})) = m_i$, that is, for every $i = 1, \dots, n$, we have the equality $(M_i : M_{i-1}) = m_i$. Hence,

$$\begin{aligned} (k(X) : k(Y)) &= (M_n : M_0) = (M_n : M_{n-1})\,(M_{n-1} : M_{n-2}) \cdots (M_1 : M_0) \\ &= m_n m_{n-1} \cdots m_1. \end{aligned}$$

But $m_n m_{n-1} \cdots m_1 = N$, so $(k(X) : k(Y)) = N$. $\square$

There exists another proof of the above proposition. Consider the free abelian group $\mathbb{Z}^n$ and the subgroup of it generated by the rows of the matrix A. The quotient of them is finite. Take a system B of representatives of all the classes. The family (X^β), where β runs in B, is a basis of $K(X)$ as a vector space over $K(Y)$. It is well-known that the order of the above quotient group is equal to N. Thus, $(k(X) : k(Y)) = N$.

In this second proof we considered the subgroup of $\mathbb{Z}^n$ generated by rows. The same is true for the subgroup generated by columns, and a proof is clear. Let us note:

Proposition 2.5. *In the above notation, let H be the subgroup of the free abelian group $\mathbb{Z}^n$ generated by the columns of the matrix A. Then the quotient group of them is finite, and its order is equal to N.*

3 The group of automorphisms

Throughout this section we assume that the field k is algebraically closed.

Let $a_1 = (a_{11}, \dots, a_{1n}), \dots, a_n = (a_{n1}, \dots, a_{nn})$ be elements belonging to $\mathbb{Z}^n$, and let A denote the $n \times n$ matrix $[a_{ij}]$. Put $N = |\det A|$, and assume that $N \geqslant 1$. Let $X = \{x_1, \dots, x_n\}$ be a set of variables over k, and let $Y = \{y_1, \dots, y_n\}$, where each y_i is the rational monomial $X^{a_i} = x_1^{a_{i1}} \cdots x_n^{a_{in}}$, for $i = 1, \dots, n$.

We denote by $\mathrm{Aut}(k(X)/k(Y))$ the Galois group of the field extension $k(Y) \subset k(X)$. Every element σ of $\mathrm{Aut}(k(X)/k(Y))$ is a $k(Y)$-automorphism of the field $k(X)$, that is, $\sigma : k(X) \to k(X)$ is a field automorphism such that $\sigma(b) = b$ for every $b \in k(Y)$. Let $|\mathrm{Aut}(k(X)/k(Y))|$ denote the order of $\mathrm{Aut}(k(X)/k(Y))$. Since always

$$|\mathrm{Aut}(k(X)/k(Y))| \leqslant (k(X) : k(Y))$$

(see [6]) and $(k(X) : k(Y)) = N$ (by Proposition 2.4), the group $\mathrm{Aut}(k(X)/k(Y))$ is finite. We will show that $|\mathrm{Aut}(k(X)/k(Y))| = N$, that is, that the field extension $k(Y) \subset k(X)$ is Galois.

Proposition 3.1. *Every $k(Y)$-automorphism of $k(X)$ is diagonal. More precisely, if σ is a $k(Y)$-automorphism of $k(X)$, then*

$$\sigma(x_1) = \varepsilon_1 x_1, \quad \dots, \quad \sigma(x_n) = \varepsilon_n x_n,$$

for some elements $\varepsilon_1, \dots, \varepsilon_n$ which are N-th roots of unity.

Proof. Let $\sigma : k(X) \to k(X)$ be a $k(Y)$-automorphism, and let $i \in \{1, \dots, n\}$. Consider the element $b_i = x_i^N$. We know (see Lemma 2.1) that $b_i \in k(Y)$. Hence $\sigma(x_i)^N = \sigma(x_i^N) = \sigma(b_i) = b_i$, and hence $\sigma(x_i)$ is a root of the polynomial $f_i(t) = t^N - b_i$ belonging to the polynomial ring $k(Y)[t]$. The polynomial $f_i(t)$ has N roots: $x_i = u_0 x_i, u_1 x_i, \dots, u_{N-1} x_i$, where $u_0, \dots, u_{N-1}$ are the all N-th roots of unity. Thus, there exists an N-th root $\varepsilon_i \in \{u_0, \dots, u_{N-1}\}$ such that $\sigma(x_i) = \varepsilon_i x_i$. $\square$

Let ε be a fixed primitive N-th root of 1.

Let $b_1, \dots, b_n$ be arbitrary elements of the ring $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$, and let

$$b = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

The column b belongs to the abelian group $(\mathbb{Z}_N)^n$. Consider the k-automorphism $\sigma_b : k(X) \to k(X)$ defined by

$$\sigma_b(x_i) = \varepsilon^{b_i} x_i, \quad \text{for } \ i = 1, \dots, n.$$

This automorphism is a $k(Y)$-automorphism if and only if $\sigma_b(y_i) = y_i$, that is, if $\sigma_b\left(X^{a_i}\right) = X^{a_i}$ for all $i = 1, \dots, n$. But each $\sigma_b\left(X^{a_i}\right)$ is equal to $\varepsilon^{a_{i1}b_1 + \cdots + a_{in}b_n} X^{a_i}$, so $\sigma_b\left(X^{a_i}\right) = X^{a_i} \iff a_{i1}b_1 + \cdots + a_{in}b_n = 0$ in $\mathbb{Z}_N$. This means that σ_b is a $k(Y)$-automorphism if and only if the matrix product Ab equals zero in $(\mathbb{Z}_N)^n$.

Let us denote by h the group homomorphism from $(\mathbb{Z}_N)^n$ to $(\mathbb{Z}_N)^n$ defined by

$$h(b) = Ab, \quad \text{for all } \ b \in (\mathbb{Z}_N)^n.$$

As a consequence of Proposition 3.1 and the above facts we obtain the following proposition.

Proposition 3.2. *The order of the Galois group* $\mathrm{Aut}(k(X)/k(Y))$ *is equal to the order of the group* $Ker\, h$.

It is easy to show that the groups $\mathrm{Aut}(k(X)/k(Y))$ and $\ker h$ are isomorphic, but we do not need this fact.

Proposition 3.3. *If the field k is algebraically closed, then the field extension $k(Y) \subset k(X)$ is Galois.*

Proof. Let $f : \mathbb{Z}^n \to \mathbb{Z}^n$, $g : \mathbb{Z}^n \to \mathbb{Z}^n$, $\eta : \mathbb{Z}^n \to (\mathbb{Z}_N)^n$ be homomorphisms of $\mathbb{Z}$-modules defined by

$$f(U) = NU, \quad g(U) = AU, \quad \eta(U) = U \bmod N,$$

for every column $U \in \mathbb{Z}^n$. Then we have the following commutative diagram of $\mathbb{Z}$-modules and $\mathbb{Z}$-homomorphisms.

$$\begin{array}{ccccccccc}
 & & \mathbb{Z}^n & \xrightarrow{f} & \mathbb{Z}^n & \xrightarrow{\eta} & (\mathbb{Z}_N)^n & \longrightarrow & 0 \\
 & & \downarrow g & & \downarrow g & & \downarrow h & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{f} & \mathbb{Z}^n & \xrightarrow{\eta} & (\mathbb{Z}_N)^n & &
\end{array}$$

where the two rows are exact. The homomorphism $h : (\mathbb{Z}_N)^n \to (\mathbb{Z}_N)^n$ is the same as before. We will use the snake lemma (see, for example [6])

It is possible to complete it in a unique way in a commutative diagram with exact rows and columns :

$$
\begin{array}{ccccccccc}
 & & \operatorname{Ker} g & \xrightarrow{f_1} & \operatorname{Ker} g & \xrightarrow{\eta_1} & \operatorname{Ker} h & & \\
 & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle k} & & \\
 & & \mathbb{Z}^n & \xrightarrow{f} & \mathbb{Z}^n & \xrightarrow{\eta} & (\mathbb{Z}_N)^n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\
0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{f} & \mathbb{Z}^n & \xrightarrow{\eta} & (\mathbb{Z}_N)^n & & \\
 & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle r} & & \\
 & & \operatorname{Coker} g & \xrightarrow{f_2} & \operatorname{Coker} g & \xrightarrow{\eta_2} & \operatorname{Coker} h & &
\end{array}
$$

Moreover, there exists a unique $\mathbb{Z}$-homomorphism v from $\operatorname{Ker} h$ to $\operatorname{Coker} g$ such that the following long sequence is exact :

$$\operatorname{Ker} g \xrightarrow{f_1} \operatorname{Ker} g \xrightarrow{\eta_1} \operatorname{Ker} h \xrightarrow{v} \operatorname{Coker} g \xrightarrow{f_2} \operatorname{Coker} g \xrightarrow{\eta_2} \operatorname{Coker} h.$$

Observe that $f_2 : \operatorname{Coker} g \to \operatorname{Coker} g$ is indeed the zero map. Let $U \in \mathbb{Z}^n$. Since $AA' = NI$ (see Section 2), we have $NU = A \cdot (A'U) = g(A'U)$. Thus, every element of the form NU, where $U \in \mathbb{Z}^n$, belongs to $\operatorname{Im} g$. Now, if $U + \operatorname{Im} g$ is an arbitrary element from $\operatorname{Coker} g$, then

$$f_2 (U + \operatorname{Im} g) = f_2 p(U) = qf(U) = q(NU) = NU + \operatorname{Im} g = 0 + \operatorname{Im} g,$$

and this means that $f_2 = 0$. Note also that the assumption $\det A \neq 0$ implies that g is injective, so $\operatorname{Ker} g = 0$.

Thus, the following short sequence is exact:

$$0 \longrightarrow \operatorname{Ker} h \xrightarrow{v} \operatorname{Coker} g \xrightarrow{0} ,$$

that is, the abelian groups $\operatorname{Ker} h$ and $\operatorname{Coker} g$ are isomorphic.

The image of g is the subgroup of $\mathbb{Z}^n$ generated by the columns of the matrix A. We know, by Proposition 2.5, that the quotient group of them is finite, and its order is equal to N. Thus, the cardinality of $\operatorname{Coker} g$ is equal to N. Moreover, the cardinality of $\operatorname{Ker} h$ is equal to the order of the group $Aut(k(X)/k(Y))$ (see Proposition 3.2). Therefore, $|Aut(k(X)/k(Y))| = N = (k(X) : k(Y))$, and so the extension $k(Y) \subset k(X)$ is Galois. □

In the above proposition we assumed that the field k is algebraically closed. Without this assumption the field extension $k(Y) \subset k(X)$ is not Galois, in general. For example, the field extension $\mathbb{Q}(x^3) \subset \mathbb{Q}(x)$ is not Galois.

4 The main results

Let $d : k[X] \to k[X]$ be a monomial derivation of the form

$$d(x_1) = X^{\beta_1}, \quad \dots, \quad d(x_n) = X^{\beta_n},$$

where $\beta_1 = (\beta_{11}, \dots, \beta_{1n}), \dots, \beta_n = (\beta_{n1}, \dots, \beta_{nn})$, are sequences of nonnegative integers. Let as recall (see Introduction), that d is called *normal* if $\beta_{11} = \beta_{22} = \dots = \beta_{nn} = 0$ and the determinant ω_d is nonzero.

We will say that d is *special*, if either d is without Darboux polynomials or all irreducible Darboux polynomials of d belong to the set $\{x_1, \dots, x_n\}$. In other words, if a monomial derivation d of $k[X]$ is special and $f \in k[X] \smallsetminus k$ is a Darboux polynomial of d, then f is a monomial, that is, $f = ax_1^{m_1} \cdots x_n^{m_n}$ for some $0 \neq a \in k$ and some nonnegative integers $m_1, \dots, m_n$ such that $\sum m_i \geqslant 1$.

Now we are ready to prove the main result of this paper.

Theorem 4.1. *Let d be a monomial derivation of a polynomial ring $k[X] = k[x_1, \dots, x_n]$, where k is a field of characteristic zero. If $\omega_d \neq 0$ then d is special if and only if the field $k(X)^d$ is trivial.*

Proof. Denote by $y_1, \dots, y_n$ the rational monomials $\frac{d(x_1)}{x_1}, \dots, \frac{d(x_n)}{x_n}$, respectively, and let $k(Y)$ denote the field $k(y_1, \dots, y_n)$. Since $\omega_d \neq 0$, we have the finite field extension $k(Y) \subset k(X)$ with $(k(X) : k(Y)) = N$, where $N = |\omega_d|$.

$\Longrightarrow$. Assume that d is special and let φ be a nonzero element of $k(X)$ such that $d(\varphi) = 0$. Let $\varphi = \frac{f}{g}$, where $f, g \in k[X] \smallsetminus \{0\}$ with $\gcd(f, g) = 1$. Then $d(f)g = fd(g)$, so $d(f) = \lambda f$, $d(g) = \lambda g$ for some $\lambda \in k[X]$. Thus, if $f \notin k$, then f is a Darboux polynomial of d. The same for g. The assumption that d is special implies that

$$f = ax_1^{u_1} \cdots x_n^{u_n}, \quad g = bx_1^{v_1} \cdots x_n^{v_n},$$

for some nonzero $a, b \in k$ and some nonnegative integers $u_1, \dots, u_n, v_1, \dots, v_n$. Moreover, $\frac{d(f)}{f} = \frac{d(g)}{g} = \lambda$. Observe that

$$\begin{aligned} \tfrac{d(f)}{f} &= u_1\tfrac{d(x_1)}{x_1} + \dots + u_n\tfrac{d(x_n)}{x_n} &= u_1y_1 + \dots + u_ny_n, \\ \tfrac{d(g)}{g} &= v_1\tfrac{d(x_1)}{x_1} + \dots + v_n\tfrac{d(x_n)}{x_n} &= v_1y_1 + \dots + v_ny_n. \end{aligned}$$

So, we have the equality $u_1y_1 + \dots + u_ny_n = v_1y_1 + \dots + v_ny_n$. We know, by Lemma 1.1, that the elements $y_1, \dots, y_n$ are algebraically independent.

Hence, $u_1 = v_1, \ \ldots, \ u_n = v_n$. This means that $\varphi = \frac{f}{g} = \frac{a}{b} \in k$. We proved that if d is special then $k(X)^d = k$.

$\Longleftarrow$. Assume that $k(X)^d = k$. Let $\overline{k}$ denote the algebraic closure of k, and $\overline{d}$ be the derivation of $\overline{k}[X]$ such that $\overline{d}(x_i) = d(x_i)$ for all $i = 1, \ldots, n$. Then $\overline{k}(X)^{\overline{d}} = \overline{k}$ (see [15]). Thus, for a proof that d is special, we may assume that the field k is algebraically closed.

Denote by G the group $\operatorname{Aut}(k(X)/k(Y))$. We know that G is finite and $|G| = N$ (Proposition 3.3).

Observe that if σ is a $k(Y)$-automorphism of $k(X)$, then $\sigma d \sigma^{-1} = d$. In fact, for every $i \in \{1, \ldots, n\}$, $\sigma(x_i) = \varepsilon_i x_i$ for some unit root ε_i (by Proposition 3.1), and we have the equalities

$$\sigma d(x_i) = \sigma(x_i y_i) = \sigma(x_i) y_i = \varepsilon_i x_i y_i = \varepsilon_i d(x_i) = d(\varepsilon x_i) = d\sigma(x_i),$$

which imply that $\sigma d = d\sigma$, that is, $\sigma d \sigma^{-1} = d$.

Let us suppose that $f \in k[X] \smallsetminus k$ is a Darboux polynomial of d. Let $d(f) = \lambda f$, where $\lambda \in k[X]$. Consider two polynomials F and Λ defined by

$$F = \prod_{\sigma \in G} \sigma(f), \quad \Lambda = \sum_{\sigma \in G} \sigma(\lambda).$$

Since every automorphism σ is diagonal (Proposition 3.1), F and Λ belong to $k[X]$. In particular, f divides F in $k[X]$. Moreover, the equalities $\sigma d \sigma^{-1} = d$ imply that

$$d(F) = \Lambda F.$$

The polynomials F and Λ are invariant with respect to G, that is, $\sigma(F) = F$ and $\sigma(\Lambda) = \Lambda$ for every $\sigma \in G$. But the extension $k(Y) \subset k(X)$ is Galois (Proposition 3.3), so F, Λ belong to $k(Y)$. Therefore,

$$\delta(F) = \Lambda F,$$

where δ is the factorisable derivation associated with d (see Section 1). Let us recall (see Lemma 2.1) that $k[X]$ is integral over $k\langle[Y]\rangle$. Thus, the polynomials F, Λ belong to $k(Y)$ and they are integral over $k\langle[Y]\rangle$.

The ring $k\langle[Y]\rangle$ is a ring of fractions of the polynomial ring $k[Y]$, which is a unique factorization domain (UFD). This means, that $k\langle[Y]\rangle$ is also UFD (see, for example, [4]), and so, the domain $k\langle[Y]\rangle$ is integrally closed. Therefore, the polynomials F and Λ belong to $k\langle[Y]\rangle$. In particular,

$$F = Y^u h,$$

where $Y^u = y_1^{u_1} \cdots y_n^{u_n}$ with $u_1, \dots, u_n \in \mathbb{Z}$, and h is a nonzero strict polynomial belonging to $k[Y]$. Now, from the equality $\delta(F) = \Lambda F$, we obtain that $\delta(h) = wh$, for some $w \in k[Y]$. Thus, if $h \notin k$, then we have a contradiction with Proposition 1.2. Therefore, F is a rational monomial with respect to variables $y_1, \dots, y_n$. But every y_i is a rational monomial in $x_1, \dots, x_n$, so F is a rational monomial in $x_1, \dots, x_n$. Moreover, $F \in k[X] \smallsetminus k$, so $F = ax_1^{m_1} \cdots x_n^{m_n}$ for some $0 \neq a \in k$ and nonnegative integers $m_1, \dots, m_n$. This implies that the polynomial f is also a monomial, because f divides F.

We proved that, if f is a Darboux polynomial of d, then f is a monomial. This means that the derivation d is special. □

In the above theorem we assumed only that d is a monomial derivation of $k[X]$ with $w_d \neq 0$. Assume now that d satisfies the additional condition "$x_i \nmid d(x_i)$ for all $i = 1, \dots, n$". Then, as an immediate consequence of Theorem 4.1 we have the following theorem.

Theorem 4.2. *Let d be a normal monomial derivation of a polynomial ring $k[X] = k[x_1, \dots, x_n]$, where k is a field of characteristic zero. Then d is without Darboux polynomials if and only if the field $k(X)^d$ is trivial.*

In Theorems 4.1 and 4.2 the monomial derivation d is monic, that is, all the polynomials $d(x_1), \dots, d(x_n)$ are monomials with coefficients 1. The next result shows that our theorems are valid also for arbitrary nonzero coefficients.

Theorem 4.3. *Let d be a derivation of a polynomial ring $k[X] = k[x_1, \dots, x_n]$, where k is a field of characteristic zero. Assume that*

$$d(x_i) = a_i x_1^{\beta_{i1}} \cdots x_n^{\beta_{in}}$$

for $i = 1, \dots, n$, where each a_i is a nonzero element from k, and each β_{ij} is a nonnegative integer. Denote by A the $n \times n$ matrix $[\beta_{ij}] - I$, and let $w_d = \det A$. If the determinant ω_d is nonzero, then the following two conditions are equivalent.

(1) *Either d is without Darboux polynomials or all irreducible Darboux polynomials of d belong to the set $\{x_1, \dots, x_n\}$.*

(2) *The field $k(X)^d$ is trivial.*

Proof. It is clear (see the proof of Theorem 4.1) that we may assume that the field k is algebraically closed. Consider the matrices

$$E_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \quad \dots, \quad E_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}, \quad U = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix}.$$

Since $\det A \neq 0$, for every $i \in \{1, \ldots n\}$ there exists a unique solution $[\gamma_{i1}, \ldots, \gamma_{in}]^T \in \mathbb{Q}^n$ of the matrix equation $AU = E_i$. Let

$$\varepsilon_i = \left(a_1^{-1}\right)^{\gamma_{1i}} \left(a_2^{-1}\right)^{\gamma_{2i}} \cdots \left(a_n^{-1}\right)^{\gamma_{ni}},$$

for $i = 1, \ldots, n$, and let $\tau : k(X) \to k(X)$ be the diagonal automorphism defined by $\tau(x_i) = \varepsilon_i x_i$ for all $i = 1, \ldots, n$. Put $D = \tau d \tau^{-1}$. Then it is easy to check that

$$D(x_i) = x_1^{\beta_{i1}} \cdots x_n^{\beta_{in}}$$

for all $i = 1, \ldots, n$. Thus, the derivations d and D are equivalent and they have the same matrix A. Now the statement is a consequence of Theorem 4.1. □

5 Monomial derivations in three variables

In the case of a ring of polynomials in two variables, it is easy to show that every monomial derivation of has a Darboux polynomial (see, for example, [16]). On the contrary, in three variables, various possibilities exist. Moreover, additional facts can be shown in this *smallest general case*; this is the reason of the present Section.

Let us consider $k[x, y, z]$, the polynomial ring in three variables over a field k (of characteristic zero). Let d be a monomial derivation of $k[x, y, z]$ of the form

$$(*) \qquad d(x) = y^{p_2} z^{p_3}, \quad d(y) = x^{q_1} z^{q_3}, \quad d(z) = x^{r_1} y^{r_2},$$

where $p_2, p_3, q_1, q_3, r_1, r_2$ are nonnegative integers. In this case

$$\omega_d = \begin{vmatrix} -1 & p_2 & p_3 \\ q_1 & -1 & q_3 \\ r_1 & r_2 & -1 \end{vmatrix} = -1 + p_2 q_3 r_1 + p_3 q_1 r_2 + r_1 p_3 + r_2 q_3 + p_2 q_1.$$

If $\omega_d \neq 0$, then we know (by Theorem 4.2) that d is without Darboux polynomials if and only if $k(x, y, z)^d = k$. All monomial derivations of $k[x, y, z]$, with trivial field of constants, are described in [16]. So, the problem of existence of Darboux polynomials has a full solution for monomial derivations of $k[x, y, z]$ with nonzero determinant.

There exist monomial derivations d of $k[x, y, z]$ for which $\omega_d = 0$. Let us look at the following example.

Example 5.1. *Let $d(x) = 1$, $d(y) = x^a z$, $d(z) = x^b y$, where $a \neq b$ are nonnegative integers. Then $\omega_d = 0$, $k(x, y, z)^d = k$, and d is without Darboux polynomials.*

Proof. It is obvious that $\omega_d = \begin{vmatrix} -1 & 0 & 0 \\ a & -1 & 1 \\ b & 1 & -1 \end{vmatrix} = 0$. Using [16] we easily deduce that $k(x, y, z)^d = k$. There is only a problem with Darboux polynomials. The determinant ω_d is equal to 0, so we cannot use Theorem 4.2.

For a proof that d is without Darboux polynomial consider the new monomial derivation $D = yd$. The determinant of this new derivation is nonzero:

$$\omega_D = \begin{vmatrix} -1 & 1 & 0 \\ a & 0 & 1 \\ b & 2 & -1 \end{vmatrix} = a + b + 2 \neq 0.$$

Moreover, $k(x, y, z)^D = k(x, y, z)^d = k$. Hence, we know, by Theorem 4.1, that every Darboux polynomial of D is a monomial.

Let us suppose that $f \in k[x, y, z] \smallsetminus k$ is a Darboux polynomial of d. Let $d(f) = \lambda f$, where $\lambda \in k[x, y, z]$. Then

$$D(f) = yd(f) = (y\lambda)f,$$

so f is a Darboux polynomial of D, and so, f is a monomial. Let $f = cx^p y^q z^r$, where $0 \neq c \in k$ and p, q, r are nonnegative integers. Since $f \notin k$, at least one of the numbers p, q, r is greater than zero. This means that at least one of the variables x, y, z is a Darboux polynomial of d (every factor of a Darboux polynomial is a Darboux polynomial). But it is a contradiction, because $x \nmid d(x)$, $y \nmid d(y)$ and $z \nmid d(z)$. Thus, we proved that d is without Darboux polynomials. □

We would like to find an example of a monomial derivation d of the form $(*)$ such that $\omega_d = 0$, $k(x, y, z)^d = k$ and d has a Darboux polynomial. But it is impossible. For every derivation d of the form $(*)$ we may use the same trick as in the proof of Example 5.1. Instead of derivation d we may consider the new derivations: xd, yd, zd. If $\omega_d = 0$, then at least one of the determinants ω_{xd}, ω_{yd}, ω_{zd} is nonzero. It is a consequence of the following lemma.

Lemma 5.2. *Let M be a 3×4 matrix of the form*

$$M = \begin{bmatrix} -1 & p_2 & p_3 & 1 \\ q_1 & -1 & q_3 & 1 \\ r_1 & r_2 & -1 & 1 \end{bmatrix},$$

where $p_2, p_3, q_1, q_3, r_1, r_2$ are nonnegative integers. Then the rank of M is equal to 3.

Proof. Denote by $\omega_0,\ \omega_1,\ \omega_2,\ \omega_3$, the determinants

$$\begin{vmatrix} -1 & p_2 & p_3 \\ q_1 & -1 & q_3 \\ r_1 & r_2 & -1 \end{vmatrix}, \quad \begin{vmatrix} 1 & p_2 & p_3 \\ 1 & -1 & q_3 \\ 1 & r_2 & -1 \end{vmatrix}, \quad \begin{vmatrix} -1 & 1 & p_3 \\ q_1 & 1 & q_3 \\ r_1 & 1 & -1 \end{vmatrix}, \quad \begin{vmatrix} -1 & p_2 & 1 \\ q_1 & -1 & 1 \\ r_1 & r_2 & 1 \end{vmatrix},$$

respectively, and suppose that $\operatorname{rank} M < 3$. Then $\omega_0 = \omega_1 = \omega_2 = \omega_3 = 0$. Let us calculate:

$$\begin{array}{rcl} 0 = \omega_0 & = & -1 + p_2q_3r_1 + p_3q_1r_2 + p_3r_1 + q_3r_2 + p_2q_1, \\ 0 = \omega_1 & = & 1 + p_2q_3 + p_3r_2 + p_2 + p_3 - q_3r_2, \\ 0 = \omega_2 & = & 1 + q_3r_1 + p_3q_1 + q_1 + q_3 - p_3r_1, \\ 0 = \omega_2 & = & 1 + p_2r_1 + q_1r_2 + r_1 + r_2 - p_2q_1. \end{array}$$

From these equalities we obtain the inequalities: $1 \geqslant p_3r_1 + q_3r_2 + p_2q_1$, $q_3r_2 \geqslant 1$, $p_3r_1 \geqslant 1$, $p_2q_1 \geqslant 1$, and we have a contradiction:

$$1 \geqslant p_3r_1 + q_3r_2 + p_2q_1 \geqslant 1 + 1 + 1 = 3.$$

Therefore, $\operatorname{rank} M = 3$. □

As a consequence of the above facts we obtain the following theorem.

Theorem 5.3. *Let d be a monomial derivation of the polynomial ring $k[x, y, z]$, where k is a field of characteristic zero. Assume that*

$$d(x) = y^{p_2}z^{p_3}, \quad d(y) = x^{q_1}z^{q_3}, \quad d(z) = x^{r_1}y^{r_2},$$

where $p_2, p_3, q_1, q_3, r_1, r_2$ are nonnegative integers. Then d is without Darboux polynomials if and only if $k(x, y, z)^d = k$.

We do not know if a similar statement is true for 4 (and more) variables. Of course if we have additional assumption that the determinant ω_d is nonzero, then it is true, by Theorem 4.2. What happens if $\omega_d = 0$? If the number of variables is greater than 3, then does not exist an analogy of Lemma 5.2. Look at the monomial derivation d of $k[x, y, z, t]$ defined by

$$d(x) = t^2, \quad d(y) = zt, \quad d(z) = y^2, \quad d(t) = xy.$$

Here $\omega_d = 0$, and the determinant of every monomial derivation of the form gd, where g is a monomial in x, y, z, t, is also equal to zero. What is the field $k(x, y, z, t)^d$? Does the derivation d has Darboux polynomials? We do not know answers for these questions. There exists a big number of such examples of monomial derivations.

References

[1] D. Cerveau, A. Lins-Neto, Holomorphic foliations in CP(2) having an invariant algebraic curve, Ann. Inst. Fourier 41 (4) (1991) 883 - 903.

[2] N. Jacobson, Lectures in abstract algebra. Vol. III: Theory of fields and Galois theory, D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto, Ont.-London-New York, 1964.

[3] J.-P. Jouanolou, Équations de Pfaff algébriques, Lect. Notes in Math. 708, Springer-Verlag, Berlin, 1979.

[4] I. Kaplansky, Commutative Rings, The University of Chicago Press, Chicago and London, 1974.

[5] M.N. Lagutinskii, On the question of the simplest form of a system of ordinary differential equations (in Russian), Mat. Sb. 27 (1911) 420 - 423.

[6] S. Lang, Algebra, Second Edition, Addison–Wesley Publ. Comp. 1984.

[7] A. Lins-Neto, Algebraic solutions of polynomial differential equations and foliations in dimension two, in "Holomorphic dynamics", Lect. Notes in Math. 1345, 193 - 232, Springer-Verlag, Berlin, 1988.

[8] A. Maciejewski, J. Moulin Ollagnier, A. Nowicki, J.-M. Strelcyn, Around Jouanolou non-integrability theorem, Indagationes Mathematicae 11 (2000) 239 - 254.

[9] A. Maciejewski, J. Moulin Ollagnier, A. Nowicki, Generic polynomial vector fields are not integrable, Indag. Math. (N.S.) 15 (1) (2004) 55 - 72.

[10] A. Maciejewski, J. Moulin Ollagnier, A. Nowicki, Correction to: "Generic polynomial vector fields are not integrable", Indag. Math. (N.S.) 18 (2) (2007) 245 - 249.

[11] J. Moulin Ollagnier, Liouvillian integration of the Lotka-Volterra system, Qual. Theory Dyn. Syst. 2 (2001) 307 - 358.

[12] J. Moulin Ollagnier, A. Nowicki, Derivations of polynomial algebras without Darboux polynomials, J. Pure Appl. Algebra 212 (2008) 1626 - 1631.

[13] J. Moulin Ollagnier, A. Nowicki, J.-M. Strelcyn, On the non-existence of constants of derivations: The proof of a theorem of Jouanolou and its development, Bull. Sci. Math. 119 (1995) 195 - 233.

[14] A. Nowicki, Polynomial derivations and their rings of constants, N. Copernicus University Press, Toruń, 1994.

[15] A. Nowicki, On the non-existence of rational first integrals for systems of linear differential equations, Linear Algebra and Its Applications, 235 (1996) 107 - 120.

[16] A. Nowicki, J. Zieliński, Rational constants of monomial derivations, J. Algebra, 3002(2006) 387 - 418.

[17] J. Zieliński, Factorizable derivations and ideals of relations, Communications in Algebra, 35(2007) 983 - 997.

[18] H. Żołądek, On algebraic solutions of algebraic Pfaff equations, Studia Math. 114 (1995) 117 - 126.

[19] H. Żołądek, Multi-dimensional Jouanolou system, J. reine angew. Math. 556 (2003) 47 - 78.