

## CONSTANTS OF DERIVATIONS IN POLYNOMIAL RINGS OVER UNIQUE FACTORIZATION DOMAINS

M'HAMMED EL KAHOU

(Communicated by Bernd Ulrich)

ABSTRACT. A well-known theorem, due to Nagata and Nowicki, states that the ring of constants of any  $\mathcal{K}$ -derivation of  $\mathcal{K}[x, y]$ , where  $\mathcal{K}$  is a commutative field of characteristic zero, is a polynomial ring in one variable over  $\mathcal{K}$ . In this paper we give an elementary proof of this theorem and show that it remains true if we replace  $\mathcal{K}$  by any unique factorization domain of characteristic zero.

### 1. INTRODUCTION

Derivations over polynomial rings and their rings of constants are objects of great importance in many fields of pure and applied mathematics (see, e.g., [3] for an excellent account). A classical application of derivations theory is the study of various questions such as first integrals and invariant algebraic sets for ordinary polynomial differential systems over the reals or the complexes. Also, it is nowadays well known that derivations, especially locally nilpotent ones, are ubiquitous in the study of algebraic automorphisms of affine spaces and various questions surrounding this wide area (see, e.g., [5]).

Very often, the study of practical questions, arising for example from differential equations, leads to dealing with derivations over abstract rings, sometimes even nonreduced, of characteristic zero. One of the fundamental questions in this topic is to describe their rings of constants. For polynomials of the type  $\mathcal{K}[x, y]$ , where  $\mathcal{K}$  is a commutative field of characteristic zero, a remarkable theorem due to Nagata and Nowicki [4] states that the ring of constants of any  $\mathcal{K}$ -derivation  $\mathcal{X}$  of such a ring is of the form  $\mathcal{K}[h]$  where  $h$  is a polynomial (see, e.g., [2] for some applications of this result). The proof of this theorem, as given in [4], is based on two highly nontrivial results. The first one, due to Zariski [7], gives a partial answer to the Hilbert 14th problem. More precisely, it states that for any subfield  $\mathcal{L} \supseteq \mathcal{K}$  of  $\mathcal{K}(x_1, \dots, x_n)$  of transcendence degree at most 2 over  $\mathcal{K}$ , the ring  $\mathcal{L} \cap \mathcal{K}[x_1, \dots, x_n]$  is finitely generated over  $\mathcal{K}$ . The second result is due to Zaks, who proved in [6] that Dedekind subrings, containing  $\mathcal{K}$ , of the polynomial ring  $\mathcal{K}[x_1, \dots, x_n]$  are of the type  $\mathcal{K}[h]$ .

In this paper we show that the result of Nagata and Nowicki also holds if we replace the ground field  $\mathcal{K}$  by any unique factorization domain of characteristic

---

Received by the editors December 27, 2002 and, in revised form, April 1, 2003.  
2000 *Mathematics Subject Classification*. Primary 12H05, 13P10.  
*Key words and phrases*. Derivations, ring of constants.

zero. Our main argument for this aim is a quite elementary result of classical fields theory that we state in Theorem 3.1.

## 2. NOTATION AND BASIC RESULTS

Let  $\mathcal{A}$  be a commutative ring with unit. In case  $\mathcal{A}$  is a domain, we let  $\mathcal{F}$  be its fractions field. We denote by  $\mathcal{A}[w] = \mathcal{A}[w_1, \dots, w_n]$  the ring of polynomials in the variables  $w_1, \dots, w_n$  with coefficients in  $\mathcal{A}$ . By admissible ordering on  $\mathbb{N}^n$  we mean a total ordering  $\preceq$  on  $\mathbb{N}^n$  that satisfies the two following axioms:

- i)  $\forall \alpha \in \mathbb{N}^n \quad 0 \preceq \alpha$ ,
- ii)  $\forall \alpha, \beta, \gamma \in \mathbb{N}^n \quad (\alpha \preceq \beta \Rightarrow \alpha + \gamma \preceq \beta + \gamma)$ .

Given an admissible ordering  $\preceq$  on  $\mathbb{N}^n$  and a polynomial  $f = \sum_{\alpha} c_{\alpha} w^{\alpha}$  in  $\mathcal{A}[w]$ , we let the leading monomial  $\text{Lm}(f, \preceq)$  of  $f$  with respect to  $\preceq$  be  $w^{\beta}$  where  $\beta$  is the greatest element in the set  $\{\alpha ; c_{\alpha} \neq 0\}$ . The coefficient  $c_{\beta}$  is called the leading coefficient of  $f$  with respect to  $\preceq$  and denoted by  $\text{Lc}(f, \preceq)$ .

If  $\mathcal{A}$  is a domain and  $f, g$  are polynomials in  $\mathcal{A}[w]$  we have the equalities

$$\begin{aligned} \text{Lm}(fg, \preceq) &= \text{Lm}(f, \preceq)\text{Lm}(g, \preceq), \\ \text{Lc}(fg, \preceq) &= \text{Lc}(f, \preceq)\text{Lc}(g, \preceq). \end{aligned}$$

Assume that  $\mathcal{A}$  is a domain and let  $x = x_1, \dots, x_n$  be a list of indeterminates over  $\mathcal{A}[w]$ . Let us denote by  $\mathcal{P}$  the maximal ideal of  $\mathcal{F}(w)[x]$  generated by the polynomials  $x_1 - w_1, \dots, x_n - w_n$ . Given a subring  $\mathcal{B}$  of  $\mathcal{F}(w)$  we let  $\mathcal{P}_{\mathcal{B}}$  be the intersection of  $\mathcal{P}$  and  $\mathcal{B}[x]$ . For any ideal  $\mathcal{I}$  of  $\mathcal{F}[x]$  we let  $\dim \mathcal{I}$  be the Krull dimension of the ring  $\mathcal{F}[x]/\mathcal{I}$ .

Given an  $\mathcal{A}$ -derivation  $\mathcal{X}$  of  $\mathcal{A}[w]$  we let  $\mathcal{A}[w]^{\mathcal{X}}$  be the  $\mathcal{A}$ -subalgebra of constants of  $\mathcal{X}$ . When  $\mathcal{A}$  is a domain, the  $\mathcal{A}$ -derivation can uniquely be extended to  $\mathcal{F}(w)$ , and we let  $\mathcal{F}(w)^{\mathcal{X}}$  be its subfield of constants.

**Lemma 2.1.** *Let  $\mathcal{A}$  be a domain with fractions field  $\mathcal{F}$ . Let  $\mathcal{A}_1$  be a subring of  $\mathcal{A}[w]$  containing  $\mathcal{A}$ , and let  $\mathcal{F}_1$  be a subfield of  $\mathcal{F}(w)$  containing  $\mathcal{F}$ . Then the following assertions hold:*

- i)  $\text{trdeg}_{\mathcal{F}} \mathcal{F}_1 + \dim \mathcal{P}_{\mathcal{F}_1} = n$ ,
- ii) *the ideal  $\mathcal{P}_{\mathcal{A}_1}$  is generated by the system  $\{f(x) - f(w) ; f(w) \in \mathcal{A}_1\}$ .*

*Proof.* i) Let us consider the  $\mathcal{F}_1$ -algebra homomorphism defined by

$$\begin{aligned} \phi : \mathcal{F}_1[x] &\longrightarrow \mathcal{F}(w) \\ p(w, x) &\longmapsto p(w, w). \end{aligned}$$

Clearly, the kernel of  $\phi$  is  $\mathcal{P}_{\mathcal{F}_1}$ , and therefore  $\mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1}$  and  $\text{Im}(\phi)$  are isomorphic as  $\mathcal{F}_1$ -algebras and, in particular, as  $\mathcal{F}$ -algebras. This proves that

$$(2.1) \quad \text{trdeg}_{\mathcal{F}} \mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1} = \text{trdeg}_{\mathcal{F}} \text{Im}(\phi).$$

Since  $\mathcal{F}_1 \supset \mathcal{F}$ , we have  $\text{Im}(\phi) \supset \mathcal{F}[w]$  and therefore  $\text{trdeg}_{\mathcal{F}} \text{Im}(\phi) = n$ . On the other hand, we have the  $\mathcal{F}$ -algebra extension  $\mathcal{F} \subset \mathcal{F}_1 \subset \mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1}$  which gives the relation

$$(2.2) \quad \text{trdeg}_{\mathcal{F}} \mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1} = \text{trdeg}_{\mathcal{F}} \mathcal{F}_1 + \text{trdeg}_{\mathcal{F}_1} \mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1}.$$

Since  $\mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1}$  is an affine ring over  $\mathcal{F}_1$  we have

$$(2.3) \quad \text{trdeg}_{\mathcal{F}_1} \mathcal{F}_1[x]/\mathcal{P}_{\mathcal{F}_1} = \dim \mathcal{P}_{\mathcal{F}_1}.$$

Gathering the equalities (2.1), (2.2) and (2.3) we get the claimed equality.

ii) Let  $g(w, x) \in \mathcal{P}_{\mathcal{A}_1}$ , and write  $g(w, x) = \sum_{\alpha} g_{\alpha}(w)x^{\alpha}$  with  $g_{\alpha}(w) \in \mathcal{A}_1$ . On the first hand, let us notice that  $f(x) - f(w) \in \mathcal{P}_{\mathcal{A}_1}$  for any  $f(w) \in \mathcal{A}_1$ . On the other hand, we have  $g(w, x) - \sum_{\alpha} (g_{\alpha}(w) - g_{\alpha}(x))x^{\alpha} = \sum_{\alpha} g_{\alpha}(x)x^{\alpha}$  and therefore  $h(x) = \sum_{\alpha} g_{\alpha}(x)x^{\alpha} \in \mathcal{P}_{\mathcal{A}_1}$ . This last relation implies that  $h(w) = 0$ , and so  $h = 0$  according to the fact that  $w_1, \dots, w_n$  are algebraically independent over  $\mathcal{A}$ .  $\square$

3. THE MAIN RESULT AND SOME APPLICATIONS

In this section we state the principal result of this paper. We then apply it to show that the Nagata-Nowicki theorem also holds if we take a unique factorization domain of characteristic zero as a ground ring instead of a field. The extension to unique factorization domains is not new. A proof of it, which builds on the case of a field, is given in [1].

**Theorem 3.1.** *Let  $\mathcal{A}$  be a unique factorization domain with fractions field  $\mathcal{F}$ , and let  $\mathcal{F}_1 \supset \mathcal{F}$  be a subfield of  $\mathcal{F}(w)$  with transcendence degree 1 over  $\mathcal{F}$ . Then there exists  $h \in \mathcal{A}[w]$  such that  $\mathcal{F}_1 \cap \mathcal{A}[w] = \mathcal{A}[h]$ .*

*Proof.* If  $\mathcal{A}_1 = \mathcal{F}_1 \cap \mathcal{A}[w]$  equals  $\mathcal{A}$ , we just choose  $h = 1$  and we are done. Thus we may assume, without loss of generality, that  $\mathcal{A} \subsetneq \mathcal{A}_1$ , i.e.,  $\mathcal{A}_1$  contains a nonconstant polynomial.

According to Lemma 2.1 i), we have  $\dim \mathcal{P}_{\mathcal{F}_1} = n - 1$ . Since, moreover,  $\mathcal{P}_{\mathcal{F}_1}$  is prime, it is principal, i.e., generated by a single polynomial, say  $f(w, x)$ . Let us choose an admissible ordering  $\preceq$  on  $\mathbb{N}^n$  and write

$$f(w, x) = \sum_{\alpha} c_{\alpha}(w)x^{\alpha}.$$

Let  $x^{\beta} = \text{Lm}(f, \preceq)$ , and notice that  $\beta \neq 0$  since  $f(w, x)$  is nonconstant. On the other hand, even if it means dividing  $f(w, x)$  by  $c_{\beta}(w)$  we may assume that  $c_{\beta}(w) = 1$ . Let us write  $c_{\alpha}(w) = \frac{a_{\alpha}(w)}{b_{\alpha}(w)}$  with  $a_{\alpha}(w), b_{\alpha}(w) \in \mathcal{A}[w]$ , and let  $\ell(w)$  be the least common multiple of the  $b_{\alpha}(w)$ 's. We can therefore write

$$(3.1) \quad f(w, x) = \frac{1}{\ell(w)}(\ell(w)x^{\beta} + \sum_{\alpha \prec \beta} d_{\alpha}(w)x^{\alpha})$$

where the  $d_{\alpha}(w)$ 's are polynomials in  $\mathcal{A}[w]$ . If we let  $d(w)$  be the greatest common divisor of  $\ell(w)$  and the  $d_{\alpha}(w)$ 's, then  $d(w)$  divides  $\ell(w)$ , say  $\ell(w) = c(w)d(w)$ , and the equation (3.1) reduces to

$$(3.2) \quad f(w, x) = \frac{f_1(w, x)}{c(w)}$$

where  $f_1(w, x)$  is a primitive polynomial in  $\mathcal{A}[w][x]$  and its leading coefficient with respect to  $\preceq$  is  $c(w)$ .

Let  $g(w)$  be a nonconstant polynomial in  $\mathcal{A}_1$ , and notice that  $g(w) - g(x)$  belongs to  $\mathcal{P}_{\mathcal{F}_1}$ . Since  $\mathcal{F}_1$  contains  $\mathcal{F}$  we may assume, without loss of generality, that  $g(w)$  is primitive. Therefore, there exists  $g_1(w, x) \in \mathcal{F}_1[x]$  such that

$$(3.3) \quad g(w) - g(x) = g_1(w, x)f(w, x).$$

We can write  $g_1(w, x)$  in the form

$$(3.4) \quad g_1(w, x) = \frac{a(w)}{b(w)}g_2(w, x)$$

where  $a(w), b(w) \in \mathcal{A}[w]$  are co-primes and  $g_2(w, x) \in \mathcal{A}[w][x]$  is primitive. Now taking into account this last equality, the relation (3.3) reduces to

$$(3.5) \quad b(w)c(w)(g(w) - g(x)) = a(w)g_2(w, x)f_1(w, x).$$

Comparing the contents in both sides of this last equality, and taking into account the fact that  $g(x)$  is primitive, we get  $b(w)c(w) = a(w)$ , which means that  $b(w)$  divides  $a(w)$  and therefore  $b(w)$  is a unit in  $\mathcal{A}[w]$  according to the fact that  $a(w)$  and  $b(w)$  are co-primes. Without loss of generality, we may assume that  $b(w) = 1$ . This implies that  $a(w) = c(w)$ , and simplifying by it in the equation (3.5) we get

$$(3.6) \quad g(w) - g(x) = g_2(w, x)f_1(w, x).$$

This gives the equality  $\text{Lc}(g, \preceq) = -\text{Lc}(g_2, \preceq)\text{Lc}(f_1, \preceq) = -\text{Lc}(g_2, \preceq)c(w)$ , and therefore both  $c(w)$  and  $\text{Lc}(g_2, \preceq)$  are constants in  $\mathcal{A}$ . This implies according to (3.2), (3.4) and the assumption  $\mathcal{F} \subset \mathcal{F}_1$  that  $f_1(w, x)$  and  $g_2(w, x)$  lie in  $\mathcal{A}_1[x]$ .

Since  $f_1(w, x) \in \mathcal{P}_{\mathcal{F}_1} \subset \mathcal{P}$ , we have  $f_1(w, w) = 0$ , and in particular  $f_1(0, 0) = 0$ . This proves that  $f_1(w, 0)$  is either equal to zero or nonconstant.

By substituting 0 to  $x$  in the relation (3.6) we get

$$(3.7) \quad g(w) = g_2(w, 0)f_1(w, 0) + g(0)$$

with  $g_2(w, 0), f_1(w, 0) \in \mathcal{A}_1$ . This last equality and the fact that  $g(w)$  is non-constant show that  $f_1(w, 0) \neq 0$ , and thus it is nonconstant. This proves that  $\deg(g_2(w, 0)) < \deg(g(w))$ . By using induction on  $\deg(g(w))$  we deduce that  $g(w)$  is a polynomial with coefficients in  $\mathcal{A}$  in terms of  $f_1(w, 0)$ .  $\square$

As an immediate consequence of Theorem 3.1 we have the following extension of the Nagata and Nowicki theorem [4].

**Corollary 3.2.** *Let  $\mathcal{A}$  be a unique factorization domain of characteristic zero, and let  $\mathcal{X}$  be a nonzero  $\mathcal{A}$ -derivation of  $\mathcal{A}[w_1, w_2]$ . Then there exists  $h \in \mathcal{A}[w_1, w_2]$  such that  $\mathcal{A}[w_1, w_2]^{\mathcal{X}} = \mathcal{A}[h]$ .*

*Proof.* Without loss of generality, we may assume that  $\mathcal{A}[w_1, w_2]^{\mathcal{X}} \supsetneq \mathcal{A}$ . If  $\mathcal{F}$  is the fractions field of  $\mathcal{A}$ , then taking into account the fact that  $\mathcal{F}$  is of characteristic zero and  $\mathcal{X} \neq 0$ , the field  $\mathcal{F}(w_1, w_2)^{\mathcal{X}}$  is of transcendence degree 1 over  $\mathcal{F}$  and  $\mathcal{A}[w_1, w_2]^{\mathcal{X}} = \mathcal{F}(w_1, w_2)^{\mathcal{X}} \cap \mathcal{A}[w_1, w_2]$ . This proves the claimed result according to Theorem 3.1.  $\square$

## REFERENCES

- [1] J. Berson. *Derivations on polynomial rings over a domain*, Master's thesis, University of Nijmegen, Nijmegen, The Netherlands, 1999.
- [2] A. van den Essen. *Polynomial automorphisms and the Jacobian conjecture*, Progress in Math., vol. 190, Birkhäuser Verlag, Basel, 2000. MR **2001j**:14082
- [3] A. Nowicki. *Polynomial derivations and their rings of constants*. N. Copernicus University Press, Toruń, 1994.
- [4] A. Nowicki and M. Nagata. *Rings of constants for  $k$ -derivations in  $k[x_1, \dots, x_n]$* . J. Math. Kyoto Univ., 28:111–118, 1988. MR **89b**:13009
- [5] P. van Rossum. *Tackling problems on affine space with locally nilpotent derivations on polynomial rings*. Ph.D. thesis, University of Nijmegen, The Netherlands, 2001.

- [6] A. Zaks. *Dedekind subrings of  $k[x_1, \dots, x_n]$  are rings of polynomials.* Israel J. Math., 9:285–289, 1971. MR **43**:6191
- [7] O. Zariski. *Interprétations algébrique-géométriques du quatorzième problème de Hilbert.* Bull. Sci. Math., 78:155–168, 1954. MR **16**:398c

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCES SEMLALIA, CADI AYYAD UNIVERSITY,  
P.O. BOX 2390, MARRAKECH, MOROCCO  
*E-mail address:* `elkahoui@ucam.ac.ma`