QUALITATIVE THEORY OF DYNAMICAL SYSTEMS **2**, 285–300 (2004)
ARTICLE NO. 85

Algebraic Closure of a Rational Function

Jean Moulin Ollagnier

LIX, *École Polytechnique, F 91128 Palaiseau Cedex, FRANCE &*
UNIVERSITÉ PARIS XII–VAL DE MARNE, *Créteil, FRANCE*
E-mail: Jean.Moulin-Ollagnier@polytechnique.edu

We give a simple algorithm to decide if a non–constant rational fraction $R = P/Q$ in the field $\mathbb{K}(x) = \mathbb{K}(x_1, \ldots, x_n)$ in $n \geq 2$ variables over a field $\mathbb{K}$ of characteristic 0 can be written as a non–trivial composition $R = U(R_1)$, where R_1 is another n–variable rational fraction whereas U is a one–variable rational fraction which is not a homography.

More precisely, this algorithm produces a generator of the *algebraic closure of a rational fraction* in the field $\mathbb{K}(x)$.

Although our algorithm is simple (it uses only elementary linear algebra), its proof relies on a structure theorem: *the algebraic closure of a rational fraction is a purely transcendental extension of* $\mathbb{K}$ *of transcendence degree* 1.

Despite this theorem is a generalization of a result of Poincaré about the rational first integrals of polynomial planar vector fields, we found it useful to give a complete proof of it: our proof is as algebraic as possible and thus very different from Poincaré's original work.

1. INTRODUCTION

During the preparation of the paper [4], Andrzej Nowicki asked the very natural question

Please devise an algorithm to decide if a non–constant rational fraction $R = P/Q$ in the field $\mathbb{K}(x) = \mathbb{K}(x_1, \ldots, x_n)$, where the field $\mathbb{K}$ has characteristic 0, can be written as a composition $R = U(R_1)$, where $R_1 = P_1/Q_1$ is another n–variable rational fraction whereas $U = S/T$ is a one–variable rational fraction, a non–trivial one i. e. not a homography.

Our paper [4] indeed deals with polynomials instead of rational fractions; in this paper, we prove the correctness of our algorithm by using an important theorem of Zaks [16]. We tried to get rid of Zaks theorem in our proof, but to avoid it, we encountered the classical theorem of Lüroth; this remark could be the purpose of a short paper, that remains to be written.

In the two–variable case, if $R = P/Q$ is a rational fraction with coprime P and Q, then R is a *rational first integral* of the vector field $(PQ_y - QP_y)\partial_x + (QP_x - PQ_x)\partial_y$ or a rational first integral of the 1–form $Q\,dP - P\,dQ$; the above question is then related to the algebraic integration of differential equations developed by Poincaré [11, 12, 13].

Generally, in the many–variable case, a rational fraction $R = P/Q$ with coprime P and Q is a first integral or *a constant* of the 1–form $\omega = Q\,dP - P\,dQ$ which means that $\omega \wedge dR = 0$.

The *field of constants* of ω, i. e. the field of all Φ in $\mathbb{K}(x)$ such that $\omega \wedge d\Phi = 0$ then coincides with the algebraic closure of $\mathbb{K}(R)$ in $\mathbb{K}(x)$.

Characterizing this field thus answers the above mentioned question : this field of constants turns out to be generated over $\mathbb{K}$ by one element, which is transcendental over $\mathbb{K}$; moreover, every element of minimal *level* of the algebraic closure of $\mathbb{K}(R)$ in $\mathbb{K}(x)$ can then be chosen as a generator of it. This result we call the *structure theorem*. It is the key of our algorithm to produce *a generator of the algebraic closure of a rational fraction*.

We first prove the structure theorem when $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed. As rank conditions of linear systems are involved, it is thereafter possible to go back from the algebraic closure $\overline{\mathbb{K}}$ to the given base field $\mathbb{K}$.

Our proof will be algebraic. Besides the specific arguments, two main general facts are involved in it as important lemmas :

- Given a $\overline{\mathbb{K}}$–derivation δ of $\overline{\mathbb{K}}[x]$ and a positive integer m, there are only finitely many *cofactors* for all *Darboux polynomials* of total degree at most m.
- If P/Q is a non–constant rational fraction in $\overline{\mathbb{K}}(x)$ and if F is an *irreducible* Darboux polynomial of the *vector derivation* δ associated to the irreducible 1–form ω deduced from the exterior derivative of P/Q, then P/Q is an absolute constant in the quotient field of the domain $\overline{\mathbb{K}}[x]/(F)$.

These lemmas belong to the folklore of polynomial dynamical systems, but, for sake of completeness, we give a thorough description and a proof of them.

The present paper is then organized as follows:

- In Section 2, we recall all necessary definitions, global notations and so on. We ask the reader to forgive the maybe too didactic style of this section.
- In the next three sections (3,4,5), we deal with the "important algebraic general facts".
- Section 6 is devoted to the main structure theorem.
- In Section 7, we give the announced algorithm.

Remark that there exists an "Algebra membership algorithm" ([15], [3] Proposition C.2.3), which is based on the theory of Gröbner bases that can be used in connection with these topics.

2. PRELIMINARIES

2.1. Global notations

Throughout the paper we will keep the notations $\mathbb{K}$ for a given field of characteristic 0 and $\overline{\mathbb{K}}$ for its algebraic closure or to put emphasis on the fact that $\overline{\mathbb{K}}$ is algebraically closed.

Then $\mathbb{A} = \mathbb{K}[x] = \mathbb{K}[x_1, \ldots, x_n]$ stands for the polynomial ring in $n \geq 2$ variables over $\mathbb{K}$ (resp. $\overline{\mathbb{A}} = \overline{\mathbb{K}}[x] = \overline{\mathbb{K}}[x_1, \ldots, x_n]$); if we need the ring of polynomials in one variable over $\mathbb{K}$ or $\overline{\mathbb{K}}$, we will denote the indeterminate by t.

2.2. Level

As the word *degree*, which is sometimes used with this meaning, could be confusing, it is convenient to call the maximum of the *total degrees* of two *coprime* polynomials P and Q the *level* of the non–zero rational fraction $R = P/Q$:

$$\mathrm{lev}(R) \;=\; \max(\deg(P), deg(Q)).$$

This definition is valid for any number of variables; the level enjoys interesting properties connected with the present subject :

- The level of a polynomial is equal to its total degree: $\mathrm{lev}(P) = \deg(P)$.
- $\mathrm{lev}(R) = 0$ if and only if $R \in \mathbb{K}^*$.
- For a univariate U, $\mathrm{lev}(U) = 1$ if and only if U is a homography and, more generally, $\mathrm{lev}(U(R)) \;=\; \mathrm{lev}(U \circ R) \;=\; \mathrm{lev}(U) \cdot \mathrm{lev}(R)$.

2.3. Derivations

A $\mathbb{K}$–*derivation* δ of the polynomial ring $\mathbb{A} = \mathbb{K}[x]$ is a $\mathbb{K}$–linear map from $\mathbb{A}$ to itself that satisfies the Leibniz rule for the product

$$\forall [f, g] \in \mathbb{A}^2,\; \delta(f \cdot g) \;=\; g \cdot \delta(f) + f \cdot \delta(g). \tag{1}$$

The same definition of a $\mathbb{K}$–derivation can be given for any $\mathbb{K}$–algebra.

In the case of a polynomial ring in n variables, the n *partial derivatives* $\partial_i \;=\; \partial/\partial(x_i)$ are derivations and moreover they constitute a basis of the $\mathbb{A}$–module of all $\mathbb{K}$–derivations from $\mathbb{A}$ to $\mathbb{A}$.

It is then convenient to consider the n–tuple of them as a *vector derivation* from $\mathbb{A}$ to the free module $\Lambda_1(\mathbb{A}^n)$.

The image df of an element f of $\mathbb{A}$ by this n–tuple is called the *exterior derivative* of f or simply its *derivative*.

Every $\mathbb{K}$–derivation δ from $\mathbb{A}$ to $\mathbb{A}$ is then completely and uniquely given by coupling the *vector field* V, which is the n–tuple $V = [\delta(x_1), \ldots, \delta(x_n)]$ of $\Lambda^1(\mathbb{A}^n)$ with the derivative, which is a 1–form :

$$\forall f \in \mathbb{A},\ \delta(f) \ = < V, df > = \sum_{i=1}^{n} \delta(x_i) \cdot \partial_i(f). \tag{2}$$

Refer to [1] for a general study of derivations and differentials.

A $\mathbb{K}$–derivation δ from $\mathbb{A}$ to $\mathbb{A}$ has a unique extension to the quotient field $\mathbb{K}(x)$ of $\mathbb{A}$ as a $\mathbb{K}$–derivation of $\mathbb{K}(x)$ and there is no trouble to denote this extension by the same δ.

It is also a classical fact that a $\mathbb{K}$–derivation of a field extension $\mathbb{L}$ of $\mathbb{K}$ can be extended in a unique way to become a $\mathbb{K}$–derivation of an *algebraic* extension $\mathbb{L}_1$ of $\mathbb{L}$ [8].

2.4. Algebraic and functional closure of a rational fraction

Let R be a element of $\mathbb{K}(x_1, \ldots, x_n) \setminus \mathbb{K}$. Its exterior derivative dR is not the 0–vector

We will say that a rational fraction Φ is *functionally parallel* to R if $d\Phi$ is a multiple of dR by some element of $\mathbb{K}(x)$; we will denote this fact by $d\Phi \,//\, dR$.

Clearly, the set of all rational fractions that are functionally parallel to a given $R \in \mathbb{K}(x) \setminus \mathbb{K}$ constitute a subfield of $\mathbb{K}(x)$, the *functional closure* $\mathcal{FC}(R)$ of R in $\mathbb{K}(X)$.

It could also be interesting to consider the functional closure of R in a larger field like $\overline{\mathbb{K}}(x)$; there will be no confusion in using the same symbol $\mathcal{FC}(R)$.

On the other hand, the set of all rational fractions that are algebraic over $\mathbb{K}(R)$ for a given $R \in \mathbb{K}(x) \setminus \mathbb{K}$ constitute a subfield of $\mathbb{K}(x)$, the *algebraic closure* $\mathcal{AC}(R)$ of R.

Here also, it could also be interesting to consider the algebraic closure of R in a larger field like $\overline{\mathbb{K}}(x)$; there will be no confusion either in using the same symbol $\mathcal{AC}(R)$.

If $R = U(\Phi)$ with a univariate U, then $dR = U'(\Phi)\, d\Phi$ and Φ is functionally parallel to R. In the same situation, Φ is algebraic over R.

This is not surprising according to the next proposition for which we need the following slight generalization of Lemma 2.5 of [4].

Lemma 1. *Let $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \mathbb{K}_2$ be fields of characteristic 0 such that the extension $\mathbb{K}_1 \subset \mathbb{K}_2$ is algebraic. Let δ be some $\mathbb{K}_0$–vector derivation of $\mathbb{K}_1$*

whose field of constants is exactly $\mathbb{K}_0$*. If* $\mathbb{K}_0$ *is algebraically closed in* $\mathbb{K}_2$*, the field of constants of the unique extension of* δ *to* $\mathbb{K}_2$ *is also* $\mathbb{K}_0$*.*

Proof. There is no difficulty to change a scalar derivation for a vector one in the proof of [4]. ▌

PROPOSITION 2. *Let* R *be a element of* $\mathbb{K}(x_1, \ldots, x_n)\backslash\mathbb{K}$*. The functional closure of* R *is equal to its algebraic closure.*

Proof. Let $R = P/Q$ where P and Q are coprime polynomials in $\mathbb{K}[x]$. Denote by ω the 1–form $\omega = Q\,dP - P\,dQ$ and consider the $\mathbb{K}$–vector derivation δ_ω defined on $\mathbb{K}(x)$ by $\delta_\omega(F) = \omega \wedge dF$ for a $F \in \mathbb{K}(x)$.

Clearly, $\delta_\omega(F) = 0$ if and only if dF is a multiple of ω, i. e. a multiple of dR. Thus, the functional closure of R is the kernel of the vector derivation δ_ω: $\mathcal{FC}(R) = \mathbb{K}(x)^{\delta_\omega}$.

As $R \notin \mathbb{K}$, there exists a partial derivative of R, say $\partial_n(R)$, such that $\partial_n(R) \neq 0$.

Let now M be the algebraic closure of R: $M = \mathcal{AC}(R)$. The field $M(x_1, \ldots, x_{n-1})$ is a purely transcendental extension of M, $\mathbb{K}(x)$ is an algebraic extension of it whereas M is algebraically closed in $\mathbb{K}(x)$.

According to the previous Lemma 1, the field of constants of δ_ω in $\mathbb{K}(x)$ is M, which is the sought result, as soon as we can prove that the field of constants of δ_ω in the intermediate field $M(x_1, \ldots, x_{n-1})$ is M.

Let us compute $\delta_\omega(\Phi(x_1, \ldots, x_{n-1})$, where Φ is a $n-1$ variable rational fraction with coefficients in M :

$$\delta_\omega(\Phi(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{n-1} \Phi'_i\,(\omega \wedge dx_i),$$

where Φ'_i is the partial derivative in $M(x_1, \ldots, x_{n-1})$.

Since $\delta_n(R) \neq 0$, the $\omega \wedge dx_i$ are linearly independent over $\mathbb{K}(x)$. Consequently, if $\delta_\omega(\Phi) = 0$, then all Φ'_i are 0 and then $\Phi \in M$. ▌

2.5. Darboux polynomials and constants of vector derivations

Let δ from $\mathbb{A}$ to $\mathbb{A}^m$ be a vector derivation i. e. an m–tuple of scalar derivations.

A non–zero polynomial $F \in \mathbb{A}$ is said to be a *Darboux polynomial* of δ if there exists a $\Lambda \in \mathbb{A}^m$ such that $\delta(F) = F\Lambda$. In this case, Λ is unique and it is called the *cofactor* of F for the derivation δ.

We have been used for a long time to paying attention to such polynomials in connection with the theory of integrability of vector fields initiated by Darboux himself [2].

The essential first properties of Darboux polynomials are the following.

• The product of two Darboux polynomials is a Darboux polynomial and the cofactor of the product is the sum of the cofactors.
• Conversely, if the product FG of two coprime polynomials is a Darboux polynomial, then F and G are Darboux polynomials.
• If $F^\alpha, \alpha \in \mathbb{N}^\star$, is a Darboux polynomial then F itself is a Darboux polynomial (this is a point where the characteristic 0 plays a role).

When δ is extended to a vector derivation from $\mathbb{K}(x)$ to $\mathbb{K}(x)^m$, a rational fraction $R \in \mathbb{K}(x) \setminus \mathbb{K}$ is said to be a *constant* of δ if $\delta(R) = 0$. In this case, its numerator and denominator are Darboux polynomials for δ *with the same cofactor*.

3. ABSOLUTE RELATIVE CONSTANTS

The aim of this section is to show, when the base field $\overline{\mathbb{K}}$ is algebraically closed, that a non–constant rational fraction P/Q in $\overline{\mathbb{K}}(x)$ becomes an *absolute constant*, i. e. an element of $\overline{\mathbb{K}}$, *relatively* to F, i. e. in the quotient field of the domain $\overline{\mathbb{K}}[x]/(F)$, where F is an irreducible Darboux polynomial of some precise vector derivation built from the Pfaffian form $Q\,dP - P\,dQ$.

Proposition 3. *Let $\overline{\mathbb{K}}$ be an algebraically closed field and let $\mathbb{A} = \overline{\mathbb{K}}[x]$ be the polynomial ring in n variables over $\overline{\mathbb{K}}$. Let P and Q be coprime elements in $\overline{\mathbb{K}}[x]$ such that $Q\,dP - P\,dQ = \phi\,\omega \neq 0$, where ω is an irreducible 1–form in $\Lambda^1(\mathbb{A}^n)$ [ϕ is the greatest common diviosr of the coefficients of $Q\,dP - P\,dQ$].*

Let then δ_ω be the $\overline{\mathbb{K}}$–vector derivation from $\mathbb{A}$ to $\Lambda^2(\mathbb{A}^n)$ defined by $\delta_\omega(f) = \omega \wedge df$.

If F be an irreducible Darboux polynomial of δ_ω, then there exists a pair $[\alpha, \beta] \neq [0, 0]$ in $\overline{\mathbb{K}}^2$ such that F divides $\alpha P + \beta Q$.

Proof. If F divides Q, we take $[\alpha, \beta] = [0, 1]$.

Otherwise, consider the non–zero images $\overline{P}$ and $\overline{Q}$ of P and Q in the quotient domain $\overline{\mathbb{K}}[x]/(F)$. Let then $c = \overline{P}/\overline{Q}$ be their quotient in the quotient field $\overline{\mathbb{K}}_F$ of $\overline{\mathbb{K}}[x]/(F)$.

As $\overline{\mathbb{K}}$ is algebraically closed, to show that c belongs to $\overline{\mathbb{K}}$, which gives the conclusion, it suffices to show that c is an absolute constant in $\overline{\mathbb{K}}_F$ which means that $\delta(c) = 0$ for every $\overline{\mathbb{K}}$–derivation of $\overline{\mathbb{K}}_F$. Indeed, an absolute constant is algebraic over $\overline{\mathbb{K}}$, hence belongs to it.

Up to a factor, a $\overline{\mathbb{K}}$–derivation of $\overline{\mathbb{K}}_F$ is the extension to $\overline{\mathbb{K}}_F$ of a $\overline{\mathbb{K}}$–derivation of $\overline{\mathbb{K}}[x]/(F)$.

Then it suffices to prove, for every $\overline{\mathbb{K}}$–derivation δ of $\overline{\mathbb{K}}[x]/(F)$ that

$$\overline{Q}^2\,\delta\left(\frac{\overline{P}}{\overline{Q}}\right) = \overline{Q}\delta(\overline{P}) - \overline{P}\delta(\overline{Q}) = 0.$$

Now, every $\overline{\mathbb{K}}$–derivation δ of $\overline{\mathbb{K}}[x]/(F)$ is given by a (non–unique) $\overline{\mathbb{K}}$–derivation of $\mathbb{A}$ for which F is a Darboux polynomial; there is no trouble to denote by the same δ such a preimage.

We have thus to prove that $Q\,\delta(P)\;-\;P\,\delta(Q)$ belongs to the ideal (F) for any $\overline{\mathbb{K}}$–derivation δ of $\mathbb{A}$ for which F is a Darboux polynomial.

Such a derivation is given by

$$\delta(g)\;=\;\sum_{i=1}^{i=n}\delta(x_i)\,g_i,$$

where g_i stands for the partial derivative of the polynomial g with respect to x_i.

As $Q\,dP - P\,dQ = \phi\,\omega$, it suffices to prove that $<\delta,\omega> = \sum_{i=1}^{i=n}\delta(x_i)\,\omega_i$ belongs to the ideal (F), where the ω_i are the coordinates of ω.

Recall that F is a Darboux polynomial for δ_ω which means in this case that there exists polynomials $\Lambda_{i,j}$ for all pairs of integers $1\le i\,,\,j\le n$ such that

$$\forall[i,j],\;1\le i\,,\,j\le n,\;\omega_i\,F_j\,-\omega_j\,F_i\;=\;F\,\Lambda_{i,j}. \tag{3}$$

From the previous equality (3), summing $\delta(x_j)\,(\omega_i\,F_j\;-\omega_j\,F_i)$ over all j gives

$$\forall i,\;1\le i\le n,\;\;\omega_i\,\delta(F)\;-\;F_i\,.<\delta,\omega>=\;F\sum_j\delta(x_j)\Lambda_{i,j} \tag{4}$$

As $\delta(F)$ belongs to (F), all products $F_i\,.<\delta,\omega>$ also belong to the ideal (F). As F is irreducible, F and a partial derivative F_i are coprime for some i, it follows that $<\delta,\omega>$ itself has to belong to the ideal (F). ▌

4. FINITENESS OF COFACTORS

In this section we describe a folklore result and we give a proof of it in algebraic terms.

PROPOSITION 4. *Let δ be a scalar $\overline{\mathbb{K}}$–derivation of $\overline{\mathbb{A}}=\overline{\mathbb{K}}[x_1,\ldots,x_n]$ and m be a positive integer. Then the set of cofactors of all Darboux polynomials of δ of total degree at most m is finite.*

Proof.

Some notations.

The $\overline{\mathbb{K}}$–derivation δ is completely and uniquely given by the $\delta_i := \delta(x_i)$. Let s be the maximum of the total degrees of the polynomials $\delta(x_i)$.

We denote by $T_{n,m}$ the set of all n–tuples $\alpha = [\alpha_1, \ldots, \alpha_n]$ of nonnegative integers with a "total degree" $|\alpha| = \alpha_1 + \cdots + \alpha_n \le m$ and, as usual, x^α stands for the product of powers $x_1^{\alpha_1}.\cdots.x_n^{\alpha_n}$.

The symbol $\sharp E$ will stand for the number of elements of a finite set E.

Every polynomial $\delta_i = \delta(x_i)$ can be written as

$$\delta_i = \sum_{\alpha \in T_{n,s}} \delta_{i,\alpha}\, x^\alpha \tag{5}$$

whereas a polynomial F of total degree at most m can be written as

$$F = \sum_{\alpha \in T_{n,m}} F_\alpha\, x^\alpha. \tag{6}$$

A linear algebra problem.

Let F be a non–zero Darboux polynomial of total degree at most m of δ and let Λ be its cofactor:

$$\sum_{i=1}^{i=n} \delta_i \frac{\partial F}{\partial x_i} = \Lambda\, F. \tag{7}$$

The polynomial cofactor Λ has a total degree at most $s-1$ and thus can be written as

$$\Lambda = \sum_{\alpha \in T_{n,s-1}} \Lambda_\alpha\, x^\alpha. \tag{8}$$

The Darboux relation (7) can be expanded as

$$\begin{array}{l} \left(\sum_{\alpha\in T_{n,s-1}} \Lambda_\alpha x^\alpha\right)\left(\sum_{\beta \in T_{n,m}} F_\beta x^\beta\right) \\ \quad -\sum_{i=1}^{i=n}\left(\sum_{\alpha \in T_{n,s}} \delta_{i,\alpha} x^\alpha\right)\left(\sum_{\beta\in T_{n,m},\beta_i>0} \beta_i F_\beta x^{\beta-\epsilon_i}\right) = 0. \end{array} \tag{9}$$

In the previous formula (9), ϵ_i stands for the n–tuple $[0, \ldots, 1, \ldots, 0]$ of $T_{n,1}$ whose all coordinates are 0 except the i–th one which is equal to 1.

The 0 polynomial on the left–hand side of (9) of total degree at most $m + s - 1$ can be expanded as

$$\sum_{\alpha \in T_{n,m+s-1}} \left[\sum_{\beta \in T_{n,m}} M_{\alpha,\beta}\, F_\beta\right] x^\alpha = 0, \tag{10}$$

where the coefficient $M_{\alpha,\beta}$ of the matrix is

$$M_{\alpha,\beta} \;=\; \sum_{\gamma+\beta=\alpha} \Lambda_\gamma \;-\; \sum_{1\le i\le n,\beta_i>0} \beta_i \left(\sum_{\gamma+\beta=\alpha+\epsilon_i} \delta_{i,\gamma} \right). \tag{11}$$

Then there exists a non–zero Darboux polynomial of total degree at most m with a cofactor Λ for δ if and only if the linear system in the unknowns $\{F_\alpha, \alpha \in T_{n,m}\}$ given by the matrix M has a non–zero solution.

A necessary and sufficient condition for that is that all minor determinants of maximal order ($\sharp\, T_{n,m}$) of M vanish.

A polynomial algebra problem.

All previous determinants are homogeneous polynomials in the variables Λ_α and $\delta_{i,\beta}$ together, they have the same degree $\sharp\, T_{n,m}$ and their coefficients are integers.

Let us denote by $\mathcal{D}_M$ the set of all these polynomials.

For every $\Delta \in \mathcal{D}_M$, Δ^+ denote the homogeneous part of Δ of degree $\sharp\, T_{n,m}$ in the Λ_α only. Equivalently, we obtain Δ^+ by evaluating Δ when all $\delta_{i,\beta}$ vanish.

For combinatorial reasons, Δ^+ may be the 0 polynomial for some Δ of $\mathcal{D}_M$. Among all elements of $\mathcal{D}_M$, let us select those for which Δ^+ is not the 0 polynomial in the unknowns Λ_α and denote by $\overline{\mathcal{D}}_M$ the set of them. That all Δ of $\overline{\mathcal{D}}_M$ vanish is a necessary (but maybe not sufficient) condition for Λ to be a cofactor.

Consider now the special case of the above matrix M where all $\delta_{i,\alpha}$ vanish. This corresponds to the special case of the Darboux relation (7) for the 0 derivation:

$$\Lambda F \;=\; 0. \tag{12}$$

The only possibility for the cofactor is then $\Lambda = 0 : \forall \alpha \in T_{n,s-1}, \Lambda_\alpha = 0$.

On the other hand, a necessary and sufficient condition is that the tuple Λ_α of unknowns is a zero of the set of homogeneous polynomials $\{\Delta^+,\, \Delta \in \overline{\mathcal{D}}_M\}$.

For the elements of $\overline{\mathcal{D}}_M$ considered as non–homogeneous polynomials in the Λ_α, Δ^+ is the leading form. Thus, the only common zero of all these leading forms is the 0–tuple.

It is now a general fact that a family of polynomials over an algebraically closed field *without zero at infinity* has only a finite number of zeroes. We discuss this elementary but important result in the next section. ∎

Corollary 5. *Let δ be a scalar or vector $\mathbb{K}$–derivation of the $\mathbb{K}$–algebra $\mathbb{A} := \mathbb{K}[x_1, \ldots, x_n]$ and m be a positive integer. Then the set of cofactors of all Darboux polynomials of δ of total degree at most m is finite.*

Proof. The finiteness result of Proposition 4, which is true for a scalar $\overline{\mathbb{K}}$–derivation, is also true for a scalar $\mathbb{K}$–derivation.

Cofactors with coefficients in $\mathbb{K}$ are cofactors with coefficients in $\overline{\mathbb{K}}$.

Then, a cofactor of a vector derivation from $\mathbb{A}$ to some finitely generated free module over $\mathbb{A}$ has coordinates that are cofactors of scalar derivations and the finiteness result also holds for vector $\mathbb{K}$–derivations. ∎

5. IDEALS WITH A FINITE NUMBER OF ZEROES

Let us consider the following situation :

- $\overline{\mathbb{A}} = \overline{\mathbb{K}}[x]$ is the polynomial ring in n variables over an algebraically closed field $\overline{\mathbb{K}}$,
- $[f_1, \ldots, f_s]$ is a finite set of polynomials in $\overline{\mathbb{A}}$,
- there is no common zero for all f_i at infinity, which means that the finite set of homogeneous polynomials $[\overline{f_1}, \cdots, \overline{f_s}]$, where $\overline{f}$ stands for the homogeneous component of highest total degree of a polynomial f, has only the trivial common zero : $[x_1 = 0, \ldots, x_n = 0]$.

Then, the f_i have only a finite number of common zeroes in the affine space, namely

- there is only a finite number of n–tuples $[x_1, \ldots, x_n]$ in $\overline{\mathbb{K}}^n$ at which all f_i vanish.

This classical fact is a consequence of Hilbert's Nullstellensatz and arguments for it can be found in many places [5, 6, 9, 10, 14]. The result itself can be found in [9] as the last assumption of theorem 3.2 in it. Let us give nevertheless some general idea of its proof.

Let $\mathcal{I}$ be the ideal generated in $\overline{\mathbb{A}}$ by the f_i. This ideal has a finite number of zeroes if and only if the quotient ring $\overline{\mathbb{A}}/\mathcal{I}$ has a finite dimension as a $\overline{\mathbb{K}}$–vector space ([5], Corollary 4 p. 23, for instance).

For every total degree d, consider the finite–dimensional $\overline{\mathbb{K}}$–vector space $\overline{\mathbb{B}}_d$ of all homogeneous polynomials of degree d in $\overline{\mathbb{B}} = \overline{\mathbb{K}}[x_0, x_1, \ldots, x_n]$ and the the finite–dimensional $\overline{\mathbb{K}}$–vector space $\overline{\mathcal{I}}_d$ of all of them which belong to $\mathcal{I}$ (when evaluated at $x_0 = 1$).

For any d, the multiplication by x_0 is a $\overline{\mathbb{K}}$–linear map from the quotient space $\overline{\mathbb{B}}_d/\overline{\mathcal{I}}_d$ to the next one $\overline{\mathbb{B}}_{d+1}/\overline{\mathcal{I}}_{d+1}$.

This map is clearly injective; the key assumption that there is no common zero at infinity implies that it is also surjective for a large enough d. Indeed, according to the Nullstellensatz, for large enough d, all monomials of total degree d in $x_1, \ldots, x_n$ belong to $\overline{\mathcal{I}}_d$.

Thus, the dimension of $\overline{\mathbb{A}}_d/\overline{\mathcal{I}}_d$ becomes constant.

The quotient ring $\overline{\mathbb{A}}/\mathcal{I}$ is a subspace of the inductive limit of the previous inductive system of quotients and thus has a finite dimension as a $\overline{\mathbb{K}}$–vector space.

6. THE MAIN THEOREM

As we said in the introduction, the proof of our algorithm depends on a structure result, which is a generalization of some considerations of Poincaré about the rational integration of polynomial planar vector fields.

THEOREM 6. *Let R belong to $\mathbb{K}(x) \setminus \mathbb{K}$. Then the algebraic/functional closure of R in $\mathbb{K}(x)$ is a purely transcendental extension of transcendence degree 1; every element S of it with minimal positive level is a generator: $\mathcal{AC}(R) = \mathcal{FC}(R) = \mathbb{K}(S)$.*

Proof.

The 1–form ω and the vector derivation δ_ω.

Let us write $R = P/Q$, where P and Q are coprime polynomials in $\mathbb{A} = \mathbb{K}[x_1, \ldots, x_n]$. A rational fraction $R_1 = P_1/Q_1$ belongs to $\mathcal{FC}(R)$ if and only if dR_1 is a multiple of the non–zero 1–form $Q\,dP - P\,dQ$.

This 1–form can be written as $\phi\omega$, where ω is irreducible, which means that the greatest common divisor of all its components is 1.

Consider now the vector derivation δ_ω defined by $\delta_\omega(F) = \omega \wedge dF$.

Clearly, $\omega \wedge (Q\,dP - P\,dQ) = 0$. This means that $Q\,\omega \wedge dP = P\,\omega \wedge dQ$; as P and Q are coprime, P divides $\omega \wedge dP$ and Q divides $\omega \wedge dQ$ and they are Darboux polynomials of δ_ω with the same cofactor $\rho_0 \in \Lambda_2(\mathbb{A}^n)$.

Moreover, as $Q\,dP - P\,dQ = \phi\,\omega$, $(Q\,dP - P\,dQ) \wedge dQ = \phi\,\omega \wedge dQ = \phi\,Q\,\rho_0$. and $dP \wedge dQ = \phi\rho_0$.

A fraction $R_1 = P_1/Q_1$ belongs to $\mathcal{FC}(R)$ if and only if

$$\omega \wedge (Q_1\,dP_1 - P_1\,dQ_1) = 0 \quad \text{as an element of } \Lambda_2(\mathbb{A}^n). \tag{13}$$

In this case P_1 and Q_1, that are assumed to be coprime, are Darboux polynomials of the vector derivation δ_ω with the same cofactor $\rho(P_1) = \rho(Q_1) \in \Lambda_2(\mathbb{A}^n)$.

Darboux polynomials of δ_ω with prescribed cofactor.

Given a level l and a 2–form ρ, denote by $\mathcal{D}(\omega, l, \rho)$ the $\mathbb{K}$–vector space of all polynomials in $\mathbb{K}[x]$ of degree at most l that are Darboux polynomials of δ_ω with the cofactor ρ. In the same way, $\overline{\mathbb{K}}$ being the algebraic closure of $\mathbb{K}$, denote by $\overline{\mathcal{D}}(\omega, l, \rho)$ the $\overline{\mathbb{K}}$–vector space of all polynomials in $\overline{\mathbb{K}}[x]$ of degree at most l that are Darboux polynomials of δ_ω with the cofactor ρ. The dimension of these two vector spaces over different fields is the same, as it it given by a rank condition of a linear system like (11); denote this dimension by $\dim(\omega, l, \rho)$.

The functional closure in $\mathbb{K}(x)$, minimal level.

Denote by l_1 (resp. by l_2) the minimal level for which there exists a functionally parallel rational fraction $R_2 = P_2/Q_2$ of such level in $\mathbb{K}(x)$ (resp. in $\overline{\mathbb{K}}(x)$). R_2 is defined up to a homography.

We don't know yet that $l_2 = l_1$, we have only $l_2 \leq l_1$.

Let then $\rho_2 \in \Lambda_2(\overline{\mathbb{A}}^n)$ be the common cofactor of the coprime P_2 and Q_2 for δ_ω [we don't know yet that $\rho_2 \in \Lambda_2(\mathbb{A}^n)$].

The key point to prove is that $\dim(\omega, l_2, \rho_2) = 2$.

Let us first show that there is a finite number of reducible elements in the vector space $\overline{\mathcal{D}}(\omega, l_2, \rho_2)$ or more accurately in the corresponding projective space.

Indeed, if there are infinitely many reducible elements in it, according to the finiteness of cofactors (Corollary 5), among all irreducible factors of all the previous Darboux polynomials, we will have two non–proportional Darboux polynomials with the same cofactor and a common level strictly less than l_2; their quotient would then be an element of the functional closure with a smaller level.

For the same reason, there is only one direction at most in $\overline{\mathcal{D}}(\omega, l_2, \rho_2)$ of degree strictly smaller than l_2. If there is such a one, take Q_2 as this one by performing a suitable homography on R_2.

Now, according to Proposition 3, every irreducible element of $\overline{\mathcal{D}}(\omega, l_2, \rho_2)$ of degree l_2 divides $\alpha P_2 + \beta Q_2$; then, for degree reasons, it belongs to the $\overline{\mathbb{K}}$–vector space $VS(P_2, Q_2)$ they generate.

Similarly, an element of $\overline{\mathcal{D}}(\omega, l_2, \rho_2)$ of degree strictly less than l_2 is a multiple of Q_2 and belongs to $VS(P_2, Q_2)$.

The set–theoretic difference $\overline{\mathcal{D}}(\omega, l_2, \rho_2) \setminus VS(P_2, Q_2)$ is contained in the finite union of the one–dimensional vector spaces generated by reducible elements of $\overline{\mathcal{D}}(\omega, l_2, \rho_2)$.

The field $\overline{\mathbb{K}}$ is infinite and this difference is empty.

$\overline{\mathcal{D}}(\omega, l_2, \rho_2)$ is then equal to $VS(P_2, Q_2)$ and $\dim(\omega, l_2, \rho_2) = 2$.

The functional closure in $\overline{\mathbb{K}}(x)$*, conclusion.*

According to Proposition 3, every irreducible Darboux polynomial of δ_ω divides some $\alpha P_2 + \beta Q_2$ and its degree is at most l_2.

Among *irreducible* Darboux polynomials of δ_ω (in $\overline{\mathbb{K}}[x]$), we thus distinguish the *regular* ones that are the irreducible elements $\alpha P_2 + \beta Q_2$ of the pencil and the *small* ones, that are factors of reducible elements of the pencil.

There is a finite number of small ones, up to scalar multiplication.

Now, if P_3/Q_3 is functionally parallel to P/Q and belongs to $\overline{\mathbb{K}}(x)$, then we can find two independent linear combinations $S_3 = \alpha P_3 + \beta Q_3$, $T_3 = \gamma P_3 + \delta Q_3$ of P_3 and Q_3 that are not divisible by any small Darboux polynomial.

The Darboux polynomials S_3 and T_3 thus factor into irreducible Darboux polynomials that are regular $\lambda_i P_2 + \mu_i Q_2$ of $VS(P_2, Q_2)$.

Then, as products of elements of $VS(P_2, Q_2)$, S_3 and T_3 are homogeneous polynomials in $\overline{\mathbb{K}}[P_2, Q_2]$. Since the cofactors of S_3 and T_3 are equal, they are homogeneous polynomials *of the same degree* in $\overline{\mathbb{K}}[P_2, Q_2]$ and so are P_3 and Q_3 themselves as linear combinations of them.

As a by–product, the cofactor of P_3 and Q_3 is $\mathrm{lev}(P_3/Q_3)/l_2$ times the cofactor of P_2 and Q_2.

Thus, the functional closure of P/Q in $\overline{\mathbb{K}}(x)$ is generated by one element P_2/Q_2.

Moreover, $\mathrm{lev}(P_2/Q_2)$ divides $\mathrm{lev}(P/Q)$ and the common cofactor ρ_2 of P_2 and Q_2 belongs to $\Lambda_2(\mathbb{A}^n)$, which will allow us to describe the functional closure in $\mathbb{K}(x)$ itself.

Back to the functional closure in $\mathbb{K}(x)$*.*

As a $\mathbb{K}$–vector space, $\mathcal{D}(\omega, l_2, \rho_2)$ has dimension 2 and we can find an element of the functional closure of P/Q in $\mathbb{K}(x)$ with level l_2, hence $l_1 = l_2$.

This means that P_2 and Q_2 can be chosen in $\mathbb{K}[x]$.

It is not difficult to show that if a polynomial $P_3 \in \mathbb{K}[x]$ is a homogeneous polynomial in $\overline{\mathbb{K}}[P_2, Q_2]$ with P_2 and Q_2 in $\mathbb{K}[x]$, then P_3 is in fact a homogeneous polynomial in $\mathbb{K}[P_2, Q_2]$. ▮

Proposition 7. *In the above situation,* $\frac{\dim(\omega, l_2, \rho_2) - 1}{l_2} = \frac{\dim(\omega, l_0, \rho_0) - 1}{l_0}$.

Proof. Elements of $\mathcal{D}(\omega, l_0, \rho_0)$ are the homogeneous two–variable polynomials of degree l_0/l_2 in P_2 and Q_2; they constitute a $\mathbb{K}$–vector space of dimension $l_0/l_2 + 1$. ▮

6.1. The special case of polynomials

Our main theorem 6 holds in the particular case where the non–constant rational fraction R is a polynomial, $R = P/1$.

Let P_2/Q_2 be a generator of $\mathcal{AC}(P/1) = \mathcal{FC}(P/1)$.

Then P and 1 are both homogeneous polynomials of the same degree k of P_2 and Q_2 with coefficients in $\mathbb{K}$.

This implies that some linear combination of P_2 and Q_2 belongs to $\mathbb{K}^*$. Then we can use a homography to produce a polynomial generator of the previous functional/algebraic closure of P.

Moreover, the cofactor involved in the proof is 0 is this particular case. We thus find again a result (Lemma 2.5) of [4] : the integral closure of a non–constant polynomial f in $\mathbb{K}[x]$ is a polynomial ring $\mathbb{K}[h]$ for some polynomial h.

7. THE ALGORITHM

7.1. The algorithm

The announced algorithm then goes as follows.

INPUT : Let P and Q be coprime polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.
- Compute the level l of $R = P/Q$.
- Compute the irreducible 1–form ω from $Q\,dP \,-\, P\,dQ$.
- Compute the common cofactor ρ of P and Q for the derivation δ_ω.
- Compute the dimension $d = \dim(\omega, l, \rho)$.

TEST : If $d = 2$ then $\boxed{P/Q}$ generates its algebraic closure
else $\dim(\omega, \frac{l}{d-1}, \frac{\rho}{d-1}) = 2$.

OUTPUT : any pair $[P_2, Q_2]$ of independent elements of the corresponding $\mathbb{K}$–vector space gives the sought generator $\boxed{P_2/Q_2}$.

Proof. This is a consequence of theorem 6 and of its proof. ▮

7.2. Reconstruction

In order to complete the previous algorithm, it remains to produce the homogeneous two–variable polynomials of degree k expressing P and Q in P_2 and Q_2 which amounts to giving the element U of $\mathbb{K}(t)$ such that $R = P/Q = U(P_2/Q_2)$.

From an algorithmic point of view, this task is a special case of a procedure that decides if a polynomial $F \in \mathbb{K}[x]$ is a homogeneous polynomial of degree k of two polynomials G and H of $\mathbb{K}[x]$ and produces the $B \in \mathbb{K}_k[u, v]$ such that $F = B(G, H)$ if the answer is "yes". This is a special case because we know the answer and want to compute B.

This *reconstruction* algorithm is only valid if $dG \wedge dH \neq 0$. The basic remark is the following : if $F = B(G, H)$, then $dF = \partial_u(B)(G, H)\, dG + \partial_v(B)(G, H)\, dH$ and $k\, B(G, H) = G\, \partial_u(B)(G, H) + H\, \partial_v(B)(G, H)$ according to Euler's identity.

Here are the headlines of such an algorithm.

• If $k = 0$, F is a homogeneous polynomial of degree 0 of G and H if and only if F is a constant.
∘ If F is not a constant, the answer is "no";
∘ if F is a constant, the answer is "yes" and $B = F$.
• If $k \geq 1$, there is *at most* one way to write dF as a linear combination $F_1\, dG + F_2\, dH$ with F_1 and F_2 in $\mathbb{K}(x)$.
∘ If this is not possible, then F is not a function of G and H and the answer is "no".
∘ If this is possible, F_1 and F_2 have to be polynomials otherwise the answer is "no".
∘ In the case where F_1 and F_2 are polynomials, we have to check *recursively* if both of them are homogeneous polynomials of G and H of degree $k - 1$.
∗ If the recursive answer is "no", then the answer is "no".
∗ If the recursive answer is "yes", we receive polynomials B_1, B_2: the answer is "yes" and the sought B is $B(G, H) = (1/k).(GB_1(G, H) + HB_2(G, H))$.

When the rational fraction R is a (homographical transform of a) polynomial, the previous reconstruction algorithm cannot be applied as the wegde product $dG \wedge dH$ is 0.

The special simple algorithm given in [4] has to be used in place of it.

ACKNOWLEDGMENTS

It is great pleasure for me to thank Andrzej Nowicki (University of Toruń) and Andrzej Maciejewski (University of Zielona Góra) for their friendly attention to the unfinished previous versions of this work and the anonymous referee for her/his very pertinent remarks.

REFERENCES

1. N. Bourbaki, *Algèbre chap.* 4*, Polynômes et fractions rationnelles* Hermann, Paris (1967).
2. G. Darboux, *Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré,* Bull. Sc. Math. 2ème série **2** (1878), 60–96, 123–144, 151–200.
3. A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture,* Progress in Mathematics, Birkhaüser Verlag, Basel, Boston, Berlin (2000).
4. A. van den Essen, J. Moulin Ollagnier & A. Nowicki, *Rings of constants of the form $k[f]$,* Preprint (2005).
5. W. Fulton, *Algebraic Curves–An introduction to algebraic geometry,* Addison–Wesley Publishing Company, Inc. (1989).
6. Gedes et al., *Algorithms for Computer Algebra,* Kluwer Academic Publishers, Boston, Dordrecht, London (1995).
7. J.-P. Jouanolou, *Equations de Pfaff algébriques,* Lect. Notes in Math. **708**, Springer–Verlag, Berlin (1979).
8. I. Kaplansky, *An Introduction to Differential Algebra,* Hermann, Paris (1976).
9. D. Lazard, *Résolution des systèmes d'équations algébriques,* Theoretical Computer Science **15** (1981), 77–110.
10. B. Mishra, *Algorithmic Algebra,* Springer–Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, Hong Kong, Barcelona, Budapest (1993).
11. H. Poincaré, *Sur l'intégration algébrique des équations différentielles,* C. R. Acad. Sc. Paris **112** (1891), 761–764; reprinted in Œuvres, tome III, Gauthier–Villars, Paris (1965), 32–34.
12. H. Poincaré, *Sur l'intégration algébrique des équations différentielles du premier ordre et du premier degré,* Rendic. Circ. Matem. Palermo **5** (1891), 161–191; reprinted in Œuvres, tome III, Gauthier–Villars, Paris (1965), 35–58.
13. H. Poincaré, *Sur l'intégration algébrique des équations différentielles du premier ordre et du premier degré,* Rendic. Circ. Matem. Palermo **11** (1897), 193–239; reprinted in Œuvres, tome III, Gauthier–Villars, Paris (1965), 59–94.
14. I. Shafarevich, *Basic Algebraic Geometry,* Springer–Verlag, Berlin, Heidelberg, New–York (1977).
15. D. Shannon & M. Sweedler, *Using Gröbner bases to determine algebra membership, split surjective homomorphisms determine birational equivalence,* J. Symbolic Computation, **6** (1988), 267–273.
16. A. Zaks, *Dedekind subrings of $k[x_1, \dots, x_n]$ are rings of polynomials*, Israel J. of Mathematics, **9** (1971), 285–289.