Noether's forms for the study of non-composite rational functions and their spectrum

Laurent Busé, Guillaume Chèze, Salah Najib

NOETHER'S FORMS FOR THE STUDY OF NON-COMPOSITE RATIONAL FUNCTIONS AND THEIR SPECTRUM

LAURENT BUSÉ, GUILLAUME CHÈZE, AND SALAH NAJIB

Abstract. In this paper, the spectrum and the decomposability of a multivariate rational function are studied by means of the effective Noether's irreducibility theorem given by Ruppert in [19]. With this approach, some new effective results are obtained. In particular, we show that the reduction modulo p of the spectrum of a given integer multivariate rational function r coincides with the spectrum of the reduction of r modulo p for p a prime integer greater or equal to an explicit bound. This bound is given in terms of the degree, the height and the number of variables of r. With the same strategy, we also study the decomposability of r modulo p. Some similar explicit results are also provided for the case of polynomials with coefficients in $A = \mathbb{K}[\underline{Z}]$.

Introduction

Consider a non-constant polynomial $f \in \mathbb{K}[X_1, \ldots, X_n]$, $n \geq 2$, where $\mathbb{K}$ is a field. Denoting by $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$, the *spectrum* of f is the set

$$\sigma(f) := \{\lambda \in \overline{\mathbb{K}} : f - \lambda \text{ is reducible in } \overline{\mathbb{K}}[X_1, \ldots, X_n]\} \subset \overline{\mathbb{K}}.$$

We recall that a polynomial $f(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$ is said to be absolutely irreducible if it is irreducible in $\overline{\mathbb{K}}[X_1, \ldots, X_n]$.

It is customary to say that f is *non-composite* if f cannot be written in the form $u(h(\underline{X}))$ with $h(\underline{X}) \in \mathbb{K}[\underline{X}]$, $u(t) \in \mathbb{K}[t]$ and $\deg(u) \geq 2$. A famous theorem of Bertini gives that f is non-composite if and only if $\sigma(f)$ is finite; see for instance [20, Theorem 37]. Furthermore, Stein proved in [22] that the cardinality of $\sigma(f)$ is at most equal to $\deg(f) - 1$; see also [17, 16, 7, 12].

Recently in [4], A. Bodin, P. Dèbes, and S. Najib have studied the behavior of the spectrum of a polynomial via a ring morphism. Here we generalize this study to the spectrum of a rational function and we give explicit bounds.

Suppose given two non-constant relatively prime polynomials f and g in the polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$, $n \geq 2$. The *spectrum* of the rational function $r = f/g \in \mathbb{K}(X_1, \ldots, X_n)$ is the set

$$\sigma(f, g) := \{(\lambda : \mu) \in \mathbb{P}^1_{\overline{\mathbb{K}}} : \mu f^\sharp - \lambda g^\sharp \text{ is reducible in } \overline{\mathbb{K}}[X_0, X_1, \ldots, X_n]\} \subset \mathbb{P}^1_{\overline{\mathbb{K}}}$$

with

$$f^\sharp := X_0^{\deg(r)} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right),\ g^\sharp := X_0^{\deg(r)} g\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right),$$

Date: June 16, 2009.

Key words and phrases. Spectrum, GCD, Noether's theorem, Ostrowski's theorem, Bertini's theorem, composite rational function.

where $\deg(r) := \max(\deg(f), \deg(g))$. That is to say,

$$\sigma(f,g) := \{(\lambda:\mu) \in \mathbb{P}^1_{\overline{\mathbb{K}}} \ : \ \mu f - \lambda g \quad \text{is reducible in} \quad \overline{\mathbb{K}}[X_1,\ldots,X_n] \\ \text{or} \ \deg \mu f - \lambda g < \deg r\}.$$

In a more geometric terminology, $\sigma(f,g)$ counts the number of reducible hypersurfaces in the pencil of hypersurfaces defined by the equations $\mu f - \lambda g = 0$ with $(\lambda:\mu) \in \mathbb{P}^1_{\overline{\mathbb{K}}}$.

Again, r is said to be *non-composite* if r cannot be written in the form $u(h(\underline{X}))$ with $h(\underline{X}) \in \mathbb{K}(\underline{X})$ and $u(t) \in \mathbb{K}(t)$, $\deg(u) \geq 2$. Actually, $\sigma(f,g)$ is finite if and only if r is non-composite and if and only if the pencil of projective algebraic hypersurfaces $\mu f^\sharp - \lambda g^\sharp = 0$, $(\mu:\lambda) \in \mathbb{P}^1_{\mathbb{K}}$, has its general element irreducible (see for instance [10, Chapitre 2, Théorème 3.4.6] or [3, Theorem 2.2] for detailed proofs). Notice that the study of $\sigma(f,g)$ is trivial if $d = 1$, and $n = 1$. Therefore, throughout this paper we will always assume that $d \geq 2$, and $n \geq 2$.

The study of the spectrum is related to the computation of the number of reducible curves in a pencil of algebraic plane curves. This problem has been widely studied. As far as we know, the first related result has been given by Poincaré [18]. Poincaré's bound was improved by a lot of works, see e.g. [19, 16, 23, 1, 3]. In [5] the authors study the number (counted with multiplicity) of reducible curves in a pencil of algebraic plane curves. The method used relies on an effective Noether's irreducibility theorem given by W. Ruppert in [19].

In this article, we follow the same strategy as in [5] using in addition basic results of elimination theory. More precisely, in the first section we give some preliminaries which are used throughout this work. In the second section, we show that the spectrum consists of the roots of a particular homogeneous polynomial denoted $\mathrm{Spect}_{f,g}$. If φ is a morphism then we get, under some suitable hypothesis, that $\varphi(\mathrm{Spect}_{f,g}) = \mathrm{Spect}_{\varphi(f),\varphi(g)}$. For two special situations, namely $f, g \in \mathbb{Z}[\underline{X}]$, and φ is the reduction modulo a prime number p, or $f, g \in \mathbb{K}[Z_1,\ldots,Z_s][\underline{X}]$, and φ sends Z_i to $z_i \in \mathbb{K}$, we give explicit results in terms of the degree, the height and the number of variables of f/g.

In the last section of this article we study the behavior of a composite rational function. More precisely we show, under some suitable hypothesis, that "f/g is composite over its coefficients field" if and only if "f/g is composite over any extension of its coefficients field". Thanks to the effective Noether's irreducibility theorem, we then show that if r is a non-composite rational function with integer coefficients and p is a "big enough" prime, then r modulo p is also non-composite. An explicit lower bound is given for such an integer p. Finally, with the same approach we also study the reduction of a non-composite rational function with coefficients in $\mathbb{K}[Z_1,\ldots,Z_n]$ after the specialization $Z_i = z_i \in \mathbb{K}$, $i = 1,\ldots,n$. We end the paper by showing that after a generic linear change of variables, a non-composite rational function remains non-composite.

Notations. If

$$f(X_1,\ldots,X_n) = \sum_{i_1,\ldots,i_n} c_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \in \mathbb{Z}[X_1,\ldots,X_n]$$

then we set $H(f) = \max_{i_1,\ldots,i_n} |c_{i_1,\ldots,i_n}|$ and $\|f\|_1 = \sum_{i_1,\ldots,i_n} |c_{i_1,\ldots,i_n}|$. The field with p elements $\mathbb{Z}/p\mathbb{Z}$ is denoted by $\mathbb{F}_p$. Given a polynomial $f \in \mathbb{Z}[\underline{X}]$ and a prime

integer $p \in \mathbb{Z}$, we will use the notation $\overline{f}^p$ for the reduction of f modulo p, that is to say, the class of f in $\mathbb{F}_p[\underline{X}]$. Finally, for any field $\mathbb{K}$ we denote by $\overline{\mathbb{K}}$ (one of) its algebraic closure.

1. Preliminaries

This section is devoted to the statement of some algebraic properties that are deeply rooted to elimination theory.

1.1. **Noether's reducibility forms.** We recall some effective results about the Noether's forms that give a necessary and sufficient condition on the coefficients of a polynomial to be absolutely irreducible. We refer the reader to [21, 20, 13, 19] for different types of such forms.

Theorem 1. *Let $\mathbb{K}$ be a field of characteristic zero, $d \geq 2$, $n \geq 2$ and*

$$f(X_1, \ldots, X_n) = \sum_{0 \leq e_1 + \cdots + e_n \leq d} c_{e_1,\ldots,e_n} X_1^{e_1} \ldots X_n^{e_n} \in \mathbb{K}[X_1, \ldots, X_n].$$

There exists a finite set of polynomials:

$$\Phi_t(\ldots, C_{e_1,\ldots,e_n}, \ldots) \in \mathbb{Z}[\ldots, C_{e_1,\ldots,e_n}, \ldots]$$

such that

$$\begin{aligned} \forall t, \Phi_t(\ldots, c_{e_1,\ldots,e_n}, \ldots) = 0 &\iff f \text{ is reducible in } \overline{\mathbb{K}}[X_1, \ldots, X_n] \text{ or } \deg(f) < d, \\ &\iff F(X_0, \ldots, X_n) \text{ is reducible in } \overline{\mathbb{K}}[X_0, \ldots, X_n], \end{aligned}$$

where F is the homogeneous polynomial $X_0^{\deg(f)} f\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)$. Furthermore,

$$\deg \Phi_t \leq d^2 - 1 \text{ and } \|\Phi_t\|_1 \leq d^{3d^2-3}\left(\binom{n+d}{n} 2^d\right)^{d^2-1}.$$

If $\mathbb{K}$ has positive characteristic $p > d(d-1)$, the coefficients of the Φ_t's above are to be taken modulo p.

Proof. In characteristic zero this theorem has been proved by Ruppert [19]. Actually Gao showed in [8] that this theorem is also true in positive characteristic p providing $p > d(d-1)$. This improvement of original Ruppert's result is contained in [8, Lemma 2.4] where it is explained that the non-vanishing of a certain resultant guaranties the statement of this theorem. □

It should be noticed that the above theorem is true without any hypothesis on the characteristic of the ground field $\mathbb{K}$, see e.g. [13, Theorem 7], but then the degrees and the heights of these forms are with no comparison with the ones given here.

1.2. **GCDs of several polynomials under specialization.** The following theorem is a classical and old result taken from elimination theory. Modern statements and proofs of this result can be found in [11, §2.10] and [14, Corollaire of Théorème 1].

Theorem 2. *Let A be a domain and $f_1, \ldots, f_n$ be $n \geq 2$ homogeneous polynomials in $A[U, V]$ of degree $d_1 \geq \cdots \geq d_n \geq 1$ respectively. The polynomials $f_1, \ldots, f_n$*

have a common root in the projective line over the algebraic closure of the fraction field of A if and only if the multiplication map[1]

$$\bigoplus_{i=1}^{n} A[U,V]_{d_1+d_2-d_i-1} \xrightarrow{\varphi} A[U,V]_{d_1+d_2-1} : (g_1,\dots,g_n) \mapsto \sum_{i=1}^{n} g_i f_i$$

does not have (maximal) rank d_1+d_2.

In particular, given a field $\mathbb{L}$ and a ring morphism $\rho : A \to \mathbb{L}$, $\rho(f_1),\dots,\rho(f_n)$ have a common root in the projective line over $\overline{\mathbb{L}}$ if and only if $\rho(\varphi)$ does not have (maximal) rank d_1+d_2 (notice that we also denoted by ρ its canonical extensions to some suitable matrix and polynomial rings).

This theorem allows to control the behavior of GCDs of several polynomials with coefficients in a UFD ring under specialization. Hereafter, we will always assume that polynomial GCDs over a field are taken to be monic with respect to a certain monomial order (e.g. the lexicographical order).

Corollary 3. *Let A be a UFD, $f_1,\dots,f_n$ be $n \geq 2$ nonzero homogeneous polynomials in $A[U,V]$ and suppose given a ring morphism $\rho : A \to \mathbb{L}$ where $\mathbb{L}$ is a field. Let $\alpha \in A$ be the leading coefficient of $\gcd(f_1,\dots,f_n) \in A[U,V]$. There exists a finite collection of algorithmically computable elements $(c_i)_{i\in I}$ in A with the following property: if $\rho(c_i) \neq 0$ for some $i \in I$ then*

$$\rho(\gcd(f_1,\dots,f_n)) = \rho(\alpha)\gcd(\rho(f_1),\dots,\rho(f_n)) \in \mathbb{L}[U,V].$$

Proof. Set $g_\rho = \gcd(\rho(f_1),\dots,\rho(f_n)) \in \mathbb{L}[U,V]$, which is a monic polynomial, and $g = \gcd(f_1,\dots,f_n) \in A[U,V]$. For all $i = 1,\dots,n$ there exists a polynomial $h_i \in A[U,V]$ such that $f_i = gh_i$. It follows that $\rho(f_i) = \rho(g)\rho(h_i)$ and hence that $\rho(g)$ divides g_ρ. Furthermore, $h_1,\dots,h_n$ have no homogeneous common factor of positive degree in $A[U,V]$, so by Theorem 2 there exists a multiplication map, say φ, with the property that $\rho(h_1),\dots,\rho(h_n)$ have no homogeneous common factor in $\mathbb{L}[U,V]$ if the rank of $\rho(\varphi)$ is maximal. Denoting $(c_i)_{i\in I}$ the collection of maximal minors of a matrix of φ, the fact that the rank of $\rho(\varphi)$ is not maximal is equivalent to the fact that $\rho(c_i) = 0$ for all $i \in I$. Therefore, we deduce that $\rho(g)$ and g_ρ are equal in $\mathbb{L}[U,V]$ up to an invertible element if $\rho(c_i) \neq 0$ for some $i \in I$. Since g_ρ is monic by convention, the claimed equality is obtained by comparison of the leading coefficients. □

In this paper we will be mainly interested in two particular cases, namely the case where $A = \mathbb{Z}$ and ρ is the reduction modulo p, and the case where $A = \mathbb{K}[Z_1,\dots,Z_s]$ and $\rho : A \to \mathbb{K}$ is an evaluation morphism. Our next task is to detail Corollary 3 in these two particular situations.

Proposition 4. *Suppose given $n \geq 2$ homogeneous polynomials $f_1,\dots,f_n \in \mathbb{Z}[U,V]$ of positive degree and set $d = \max_i \deg(f_i)$, $H = \max_i H(f_i)$.*

(i) *If $f_1,\dots,f_n$ have no (homogeneous) common factor of positive degree in $\mathbb{Z}[U,V]$, then $\overline{f_1}^p,\dots,\overline{f_n}^p$ have no (homogeneous) common factor of positive degree in $\mathbb{F}_p[U,V]$ for all prime integer*

$$p > d^d H^{2d}.$$

[1] the notation $A[U,V]_d$, $d \in \mathbb{N}$, stands for the free A-module of homogeneous polynomials of degree d.

(ii) *Denoting by* $\alpha \in \mathbb{Z}$ *the leading coefficient of* $\gcd(f_1, \ldots, f_n) \in \mathbb{Z}[U, V]$*, we have*

$$\overline{\alpha}^p.\gcd(\overline{f_1}^p, \ldots, \overline{f_n}^p) = \overline{\gcd(f_1, \ldots, f_n)}^p \in \mathbb{F}_p[U, V]$$

for all prime integer

$$p > d^d(d+1)^d 2^{2d^2} H^{2d}.$$

Proof. Denote by $d_1 \geq d_2 \geq \ldots \geq d_n \geq 1$ the degree of $f_1, \ldots, f_n$ respectively. Observe that $d = d_1$. By Theorem 2, the hypothesis implies that the multiplication map

$$\oplus_{i=1}^n A[U, V]_{d_1+d_2-d_i-1} \to A[U, V]_{d_1+d_2-1} : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^n g_i f_i$$

has maximal rank $d_1 + d_2$. Using Hadamard's inequality [24, Theorem 16.6] we obtain that the absolute value of each $(d_1 + d_2)$-minor of the matrix of the above multiplication map is bounded above by

$$(\sqrt{dH^2})^{d_1+d_2} = d^{\frac{d_1+d_2}{2}} H^{d_1+d_2} \leq d^d H^{2d}.$$

Therefore, one of these minors remains non-zero modulo p and Theorem 2 implies that $\overline{f_1}^p, \ldots, \overline{f_n}^p$ do not have a common root in the projective line over an algebraically closed field extension of $\mathbb{F}_p$. We deduce that $\overline{f_1}^p, \ldots, \overline{f_n}^p$ do not have a homogeneous common factor of positive degree in $\mathbb{F}_p[U, V]$ and (i) is proved.

To prove (ii) we use Corollary 3 and take again the notation of its proof. For all $i = 1, \ldots, n$ there exists a homogeneous polynomial $h_i \in \mathbb{Z}[U, V]$ such that $f_i = gh_i$ and we know that the claimed equality holds if $\varphi(h_1), \ldots, \varphi(h_n)$ does not have a homogeneous common factor of positive degree in $\mathbb{F}_p[U, V]$. Since for all $i = 1, \ldots, n$ we have $\deg(h_i) \leq d$ and $H(h_i) \leq (d+1)^{\frac{1}{2}} 2^d H$ by Mignotte's bounds [24, Corollary 6.33] and (i) imply that the above condition is satisfied if

$$p > e^{d \ln(d)} \left[(d+1)^{\frac{1}{2}} 2^d H\right]^{2d} = e^{d \ln(d)} (d+1)^d 2^{2d^2} H^{2d}.$$

□

It should be noticed that a result similar to (i) has been proved in [26, last paragraph of page 136] but with a larger bound for the prime integer p, namely $e^{2nd^2} H^{2d}$. Also, to convince the reader that the bound given in (ii) is not too rough, we mention that in the case $n = 2$ it is not difficult to see that (see for instance [24, Theorem 6.26] or [25, §4.4])

$$\overline{\gcd(f_1, f_2)}^p = \overline{\alpha}.\gcd(\overline{f_1}, \overline{f_2}) \in \mathbb{F}_p[U, V] \tag{1.1}$$

if and only if $p \nmid \mathrm{Res}(h_1, h_2) \in \mathbb{Z}$, where $f_i = \gcd(f_1, f_2)h_i$, $i = 1, 2$ and $\mathrm{Res}(h_1, h_2)$ is the resultant of h_1 and h_2. Therefore, it appears necessary to bound $H(h_i)$, $i = 1, 2$, in terms of $H(f_i)$, $i = 1, 2$.

Now, we turn to the second case of application of Corollary 3. For that purpose, we introduce a new set of indeterminates $\underline{Z} := Z_1, \ldots, Z_s$.

Proposition 5. *Let* $f_1, \ldots, f_n$ *be* $n \geq 2$ *polynomials in* $\mathbb{K}[\underline{Z}][U, V]$ *that are homogeneous with respect to the variables* U, V *of degree* d *with coefficients in* $\mathbb{K}[\underline{Z}]$*. Also, suppose given a ring morphism* $\rho : \mathbb{K}[\underline{Z}] \to \mathbb{K}$ *and assume that all coefficients of* $f_1, \ldots, f_n$ *are polynomials in* $\mathbb{K}[\underline{Z}]$ *of degree* $\leq k$*.*

(i) *If $f_1, \dots, f_n$ have no (homogeneous) common factor of positive degree in $\mathbb{K}[\underline{Z}][U,V]$, then there exists a finite collection $(p_i)_{i\in I}$ of nonzero elements in $\mathbb{K}[\underline{Z}]$ of degree $\leq 2dk$ such that $\rho(f_1), \dots, \rho(f_n)$ have no (homogeneous) common factor of positive degree in $\mathbb{K}[U,V]$ if $\rho(p_i)$, $i \in I$, are not all zero.*

(ii) *Denoting by $\alpha \in \mathbb{K}[\underline{Z}]$ the leading coefficient of* $\gcd(f_1, \dots, f_n) \in \mathbb{K}[\underline{Z}][U,V]$ *as a homogeneous polynomial in the variables U, V, there exists a finite collection $(q_i)_{i\in I}$ of nonzero elements in $\mathbb{K}[\underline{Z}]$ of degree $\leq 2dk$ such that*

$$\rho(\alpha).\gcd(\rho(f_1), \dots, \rho(f_n)) = \rho(\gcd(f_1, \dots, f_n)) \in \mathbb{K}[X]$$

if $\rho(q_i)$, $i \in I$, are not all zero.

Proof. Completely similar to the proof of Proposition 4. □

2. Study of the spectrum of a rational function

Let A be a UFD, $\mathbb{K}$ be its fraction field and suppose given a rational function $r = f/g \in \mathbb{K}(X_1, \dots, X_n)$ with $f, g \in A[X_1, \dots, X_n]$ and $\gcd(f,g) = 1$. Set $d := \deg(r) = \max(\deg(f), \deg(g))$. We recall that, by definition, the *spectrum* of r is the set

$$\sigma(f,g) := \{(\lambda : \mu) \in \mathbb{P}^1_{\overline{\mathbb{K}}} : \mu f^\sharp - \lambda g^\sharp \text{ is reducible in } \overline{\mathbb{K}}[X_0, X_1, \dots, X_n]\} \subset \mathbb{P}^1_{\overline{\mathbb{K}}}$$

where

$$f^\sharp := X_0^{\deg(r)} f\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right),\ g^\sharp := X_0^{\deg(r)} g\left(\frac{X_1}{X_0}, \dots, \frac{X_n}{X_0}\right).$$

Assume that $\sigma(f,g)$ is finite and denote by $\Phi_t(U,V)$ the Noether's reducibility forms associated to the polynomial

$$Vf^\sharp(X_0, \dots, X_n) - Ug^\sharp(X_0, \dots, X_n) \in A[U,V][X_0, X_1, \dots, X_n].$$

These forms are all homogeneous polynomials in $A[U,V]$ by construction. We will denote their GCD by $\mathrm{Spect}_{f,g}(U,V) \in A[U,V]$. By Theorem 1, for all $(\lambda : \mu) \in \mathbb{P}^1_K$ we have

$$\mathrm{Spect}_{f,g}(\lambda : \mu) = 0 \iff (\lambda : \mu) \in \sigma(f,g).$$

As an immediate consequence of Corollary 3, we have the following property. Given a morphism $\rho : A \to \mathbb{L}$, where $\mathbb{L}$ is a field, there exists a non-zero element c of A such that if $\rho(c) \neq 0$ then

$$\rho(\mathrm{Spect}_{f,g}) = \mathrm{Spect}_{\rho(f),\rho(g)}$$

up to multiplication by a non-zero element in $\mathbb{L}$.

In what follows, we will investigate this property in two particular cases of interest: the case where $A = \mathbb{Z}$ and ρ is the reduction modulo p, and the case where $A = \mathbb{K}[Z_1, \dots, Z_s]$ and $\rho : A \to \mathbb{K}$ is an evaluation morphism.

2.1. Spectrum and reduction modulo p.

Theorem 6. *Suppose given f, g two multivariate polynomials in $\mathbb{Z}[X_1, \dots, X_n]$ such that* $\gcd(f,g) = 1$. *Set $d = \deg(f/g) = \max(\deg(f), \deg(g))$. For all prime integer $p > \mathcal{B}$ with*

$$\mathcal{B} = 2^{2(d^2-1)^2} d^{2d^2-2} (d^2-1)^{d^2-1} \mathcal{H}^{2d}$$

where

$$\mathcal{H} = d^{3d^2-3}\left(\binom{n+d}{n} 2^d\right)^{d^2-1} \binom{d^2-1}{\lfloor (d^2-1)/2 \rfloor} \max\left(H(f), H(g)\right)^{d^2-1}$$

we have

$$Spect_{\overline{f}^p,\overline{g}^p} = \kappa.\overline{Spect_{f,g}}^p$$

in the polynomial ring $\mathbb{F}_p[U,V]$ *with* $0 \neq \kappa \in \mathbb{F}_p$.

Proof. From the definition of $Spect_{f,g}(U,V)$, this is a consequence of Theorem 1. Indeed, straightforward computations show that

$$H(\Phi_t(Vf^\sharp - Ug^\sharp)) \leq \|\Phi_t\|_1 H\big((Vf^\sharp - Ug^\sharp)^{d^2-1}\big)$$

and

$$H\big((Vf^\sharp - Ug^\sharp)^{d^2-1}\big) \leq \binom{d^2-1}{\lfloor (d^2-1)/2 \rfloor} \max\big(H(f), H(g)\big)^{d^2-1}.$$

It follows

$$H(\Phi_t(Vf^\sharp - Ug^\sharp)) \leq \\ d^{3d^2-3}\Big(\binom{n+d}{n}2^d\Big)^{d^2-1}\binom{d^2-1}{\lfloor (d^2-1)/2 \rfloor} \max\big(H(f), H(g)\big)^{d^2-1}.$$

Now, applying Proposition 4 with degree d^2-1 and height H_1 we obtain that

$$\overline{Spect_{f,g}(U,V)}^p = \overline{\gcd\big(\Phi_t(Vf^\sharp - Ug^\sharp)\big)}^p = \kappa.\gcd\big(\overline{\Phi_t(Vf^\sharp - Tg^\sharp)}^p\big)$$

if $p > \mathcal{B}$, where $0 \neq \kappa \in \mathbb{F}_p$, and therefore that

$$\overline{Spect_{f,g}(U,V)}^p = \kappa.Spect_{\overline{f}^p,\overline{g}^p}(U,V)$$

by Theorem 1. □

As a consequence of this theorem we obtain an analog of Ostrowski's result. The classical Ostrowski's theorem asserts that if a polynomial f is absolutely irreducible then $\overline{f}^p$ is absolutely irreducible providing p is big enough. In our context we get the

Corollary 7. *Under the notations of Theorem 6, if* $\sigma(f,g) = \emptyset$ *then* $\sigma(\overline{f}^p, \overline{g}^p) = \emptyset$ *for all prime integer* p *such that* $p > \mathcal{B}$.

Before moving on, we mention that our strategy can be used similarly to deal with the case of polynomials in $A[X_1,\ldots,X_n]$ and reduction modulo a prime ideal in A.

2.2. Spectrum of a rational function with coefficients in $\mathbb{K}[\underline{Z}]$.

Theorem 8. *Let* f,g *be two polynomials in* $\mathbb{K}[Z_1,\ldots,Z_s][X_1,\ldots,X_n]$ *such that* $\deg_{\underline{Z}}(f) \leq k$, $\deg_{\underline{Z}}(g) \leq k$, $\deg_{\underline{X}}(f) \leq d$ *and* $\deg_{\underline{X}}(g) \leq d$. *Given* $\underline{z} := (z_1,\ldots,z_s) \in \mathbb{K}^s$, *denote by* $\mathrm{ev}_{\underline{z}}$ *the ring morphism* $\mathbb{K}[Z_1,\ldots,Z_s] \to \mathbb{K}$ *that sends* Z_i *to* z_i *for all* $i = 1,\ldots,s$. *There exists a finite collection of nonzero polynomials in* $\mathbb{K}[\underline{Z}]$, *say* $(q_i)_{i\in I}$, *of degree smaller than* $2(d^2-1)^2k$ *with the property that: if* $\mathrm{ev}_{\underline{z}}(q_i) \in \mathbb{K}$ *are not all zero then*

$$ev_{\underline{z}}(\mathrm{Spect}_{f,g}) = \kappa.\mathrm{Spect}_{ev_{\underline{z}}(f),ev_{\underline{z}}(g)}$$

where $0 \neq \kappa \in \mathbb{K}$.

Proof. We consider again Noether's forms $(\Phi_t(Vf^\sharp - Ug^\sharp))_{t\in T}$. By construction we have $\deg_{\underline{Z}}(\Phi_t(Vf^\sharp - Ug^\sharp)) \leq (d^2-1)k$ and $\deg_{U,V}(\Phi_t(Vf^\sharp - Ug^\sharp)) \leq d^2-1$. Therefore, Proposition 5 shows the existence of a finite collection of polynomials $(q_j)_{j\in J}$ in $\mathbb{K}[\underline{Z}]$ of degree smaller than $2(d^2-1)^2k$ with the property that

$$ev_{\underline{z}}(\mathrm{Spect}_{f,g}) = \kappa.\mathrm{Spect}_{ev_{\underline{z}(f)},ev_{\underline{z}(g)}}$$

where $0 \neq \kappa \in \mathbb{K}$, if $\mathrm{ev}_{\underline{z}}(q_j) \neq 0$ for some $j \in J$. □

This result has the following probabilistic corollary that follows from the well known Zippel-Schwartz's Lemma that we recall.

Lemma 9 (Zippel-Schwartz)**.** *Let $P \in A[X_1,\ldots,X_n]$ be a polynomial of total degree d, where A is an integral domain. Let S be a finite subset of A. For a uniform random choice of x_i in S we have*

$$\mathcal{P}\Big(\{P(\underline{x}) = 0 \mid x_i \in S\}\Big) \leq d/|S|,$$

where $|S|$ denotes the cardinal of S and $\mathcal{P}$ the probability.

Corollary 10. *With the notations of Theorem 8, let S be a finite subset of $\mathbb{K}$ with $|S|$ elements. If $\sigma(f,g) = \emptyset$ then for a uniform random choice of the z_i's in S we have*

$$\sigma(ev_{\underline{z}(f)}, ev_{\underline{z}(g)}) = \emptyset$$

with probability at least $1 - \dfrac{2(d^2-1)^3k^2}{|S|}$.

Proof. As $\sigma(f,g) = \emptyset$, $\mathrm{Spect}_{f,g} =: c(\underline{Z})$ is a non-zero polynomial in $\mathbb{K}[\underline{Z}]$ of degree less than $k(d^2-1)$. Therefore, if $q_i c(\underline{z}) \neq 0$ for some $i \in I$, where $(q_i)_{i\in I}$ is the collection of polynomials in Theorem 8, then $\mathrm{Spect}_{ev_{\underline{z}(f)},ev_{\underline{z}(g)}} \in \mathbb{K}$. □

3. Indecomposability of rational functions

In the previous section we have studied the spectrum of a rational function. It turns out that the spectrum of $r(X_1,\ldots,X_n) \in \mathbb{K}(X_1,\ldots,X_n)$ is deeply related to the indecomposability of r over $\overline{\mathbb{K}}$. After recalling this link, we will study indecomposability of rational functions.

Theorem 11. *Let $\mathbb{K}$ be a field of characteristic $p \geq 0$. Let $r = f/g \in \mathbb{K}(X_1,\ldots,X_n)$ be a non-constant reduced rational function. The following are equivalent:*

(i) *r is composite over $\overline{\mathbb{K}}$,*
(ii) *$f - \lambda g$ is reducible in $\overline{\mathbb{K}}[X_1,\ldots,X_n]$ for all $\lambda \in \overline{\mathbb{K}}$ such that* $\deg(f-\lambda g) = \deg(r)$,
(iii) *the polynomial $f(X_1,\ldots,X_n) - Tg(X_1,\ldots,X_n)$ is reducible in the polynomial ring $\overline{\mathbb{K}(T)}[X_1,\ldots,X_n]$.*

Remark 12. We recall that this kind of result is already known for the polynomial case (see for instance [6, Lemma 7]).

Proof of Theorem 11. (i) $\iff$ (ii): see [3, Theorem 2.2].

(ii) $\Rightarrow$ (iii): statement (ii) means that for all $\lambda \in \overline{\mathbb{K}}$ such that $\deg(f-\lambda g) = \deg r$, we have $\Phi_t(f-\lambda g) = 0$ for all t. Then $\Phi_t(f - Tg)$ has an infinite number of roots in $\overline{\mathbb{K}}$ and thus $\Phi_t(f-Tg) = 0$ for all t. This gives $f - Tg$ is reducible in $\overline{\mathbb{K}(T)}[X_1,\ldots,X_n]$.

(iii) $\Rightarrow$ (ii): statement (iii) means that $\Phi_t(f - Tg) = 0 \in \mathbb{K}[T]$ for all t. Hence, if $\lambda \in \overline{\mathbb{K}}$ is such that $\deg(f - \lambda g) = \deg r$, we can conclude thanks to Theorem 1 that $f - \lambda g$ is reducible in $\overline{\mathbb{K}}[X_1, \ldots, X_n]$. □

The following theorem shows that under some hypothesis, r is composite over $\mathbb{K}$ if and only if r is composite over $\overline{\mathbb{K}}$. Therefore, we will sometimes say hereafter that r is composite instead of r is composite over its coefficients field.

Theorem 13. *Let $\mathbb{K}$ be a perfect field of characteristic $p = 0$ or $p \geq d^2$ and let $r = f/g \in \mathbb{K}(X_1, \ldots, X_n)$, $n \geq 2$, be a non-constant reduced rational function of degree d. Then, r is composite over $\mathbb{K}$ if and only if r is composite over $\overline{\mathbb{K}}$.*

Proof. Obviously, if r is composite over $\mathbb{K}$ then r is composite over any extension of $\mathbb{K}$ and thus over $\overline{\mathbb{K}}$. So, suppose that $r = u(h)$ with $\deg(u) \geq 2$, $u \in \overline{\mathbb{K}}(T)$ and $h \in \overline{\mathbb{K}}(X_1, \ldots, X_n)$. We set $u = u_1/u_2$ where $u_1, u_2 \in \overline{\mathbb{K}}[T]$ and $h = h_1/h_2$ is reduced and non-composite with $h_1, h_2 \in \overline{\mathbb{K}}[X_1, \ldots, X_n]$. We are going to show that there exist $U \in \mathbb{K}(T)$ and $H \in \mathbb{K}(X_1, \ldots, X_n)$ such that $r = U(H)$.

The notation $\mathrm{mdeg}(f)$ denotes the multi-degree of f associated to a given monomial order $\prec$ and $lc(f)$ denotes the leading coefficient of f associated to $\prec$.

First step: we claim that one can suppose that $lc(f) = 1$, $lc(g) = 1$ and $\mathrm{mdeg}(f) \succ \mathrm{mdeg}(g)$. Indeed, to satisfy the first condition, we just have to take $f/lc(f)$ and $g/lc(g)$. Then, for the second conditon, if $\mathrm{mdeg}(f) \prec \mathrm{mdeg}(g)$ we take g/f, and if $\mathrm{mdeg}(f) = \mathrm{mdeg}(g)$ we set $F = f$, $G = f - g$ and take F/G. Indeed, f/g is composite over $\mathbb{K}$ if and only if F/G is composite over $\mathbb{K}$.

Second step: we claim that one can suppose that $lc(h_1) = 1$, $lc(h_2) = 1$ and $\mathrm{mdeg}(h_1) \succ \mathrm{mdeg}(h_2)$. This actually follows from the same trick that we use in the first step. We just have to remark that if $r = u(h_1/h_2)$ then $r = v(h_2/h_1)$ with $v(T) = u(1/T)$.

Third step: one can suppose that $h_1(0, \ldots, 0) = 0$ and $h_2(0, \ldots, 0) \neq 0$. Indeed, if $h_2(0, \ldots, 0) \neq 0$ then we can consider

$$H_1 = h_1 - \left(\frac{h_1(0, \ldots, 0)}{h_2(0, \ldots, 0)}\right) h_2$$

and $H_2 = h_2$. Then we can write $r = v(H_1/H_2)$ with H_1 and H_2 satisfying the above conditions and the ones of the second step.

Now, if $h_2(0, \ldots, 0) = 0$ then a change of coordinates $r(X_1 - a_1, \ldots, X_n - a_n)$, with $(a_1, \ldots, a_n) \in \mathbb{K}^n$ such that $h_2(a_1, \ldots, a_n) \neq 0$, gives the desired result. So we just have to show that there exists such an element $(a_1, \ldots, a_n) \in \mathbb{K}^n$ if $p \geq d^2$ (it is clear if $p = 0$). To do this, we observe that $\deg h_2 \leq d < p$ and proceed by contradiction.

Assume that

$$h_2(X_1, \ldots, X_n) = \\ c_0(X_1, \ldots, X_{n-1}) + c_1(X_1, \ldots, X_{n-1})X_n + \cdots + c_d(X_1, \ldots, X_{n-1})X_n^d$$

with $c_i(X_1, \ldots, X_{n-1}) \in \overline{\mathbb{K}}[X_1, \ldots, X_{n-1}]$, is such that

$$\forall (x_1, \ldots, x_n) \in \mathbb{K}^n,\ h_2(x_1, \ldots, x_n) = 0.$$

Then, given $(x_1, \ldots, x_{n-1}) \in \mathbb{K}^{n-1}$ we have that $h_2(x_1, \ldots, x_{n-1}, X_n) \in \overline{\mathbb{K}}[X_n]$ has degree $\leq d$ and at least p distinct roots in $\mathbb{K}$. It follows that $h_2(x_1, \ldots, x_{n-1}, X_n)$ is the null polynomial and hence that

$$\forall i = 0, \ldots, d, \forall (x_1, \ldots, x_{n-1}) \in \mathbb{K}^{n-1}, c_i(x_1, \ldots, x_{n-1}) = 0.$$

Now, since $c_i(X_1, \ldots, X_{n-1})$ has also degree $\leq d$, we can continue this process in the same way to end with the conclusion that $h_2 = 0$ in $\overline{\mathbb{K}}[X_1, \ldots, X_n]$.

Fourth step: we claim that $h_2(X_1, \ldots, X_n) \in \mathbb{K}[X_1, \ldots, X_n]$. To show this, we are going to prove that if r, h_1 and h_2 satisfies the hypothesis of the previous steps then $h_2 \in \mathbb{K}[X_1, \ldots, X_n]$.

Let $\lambda \in \mathbb{K}$ such that $\deg(f - \lambda g) = \deg r = d$. Since r is composite over $\overline{\mathbb{K}}$ then $f - \lambda g$ is reducible over $\overline{\mathbb{K}}$ by Theorem 11, and we have:

$$f + \lambda g = \alpha \prod_{i=1}^{m} (h_1 + \lambda_i h_2),$$

where λ_i are the roots of $u_1 + \lambda u_2 = \alpha \prod_{i=1}^{m} (T - \lambda_i)$, see the proof of [3, Corollary 2.4]. Thanks to step 1 and 2, $lc(f + \lambda g) = 1$ and $lc(h_1 + \lambda_i h_2) = 1$ so that $\alpha = 1$. As h_1/h_2 is non-composite we can find $\lambda \in \mathbb{K}$ such that for all i, $h_1 + \lambda_i h_2$ is irreducible over $\overline{\mathbb{K}}$ because $|\sigma(h_1, h_2)| \leq d^2 - 1$ and $p = 0$ or $p > d^2$ (the bound $|\sigma(h_1, h_2)| \leq d^2 - 1$ is proved for any field in the bivariate case in [16] and its extension to the multivariate case is easily obtained using Bertini's Theorem; see for instance [5, Proof of Theorem 13] or [3].)

Now let $\tau \in \mathit{Galois}(\mathbb{L}/\mathbb{K})$, where $\mathbb{L}$ is the field generated by all the coefficients of u_1, u_2, h_1, h_2, we have:

$$f - \lambda g = \tau(f - \lambda g) = \prod_{i=1}^{m} \big(\tau(h_1) + \tau(\lambda_i)\tau(h_2)\big).$$

As $lc\big(\tau(h_1) + \tau(\lambda_i)\tau(h_2)\big) = 1$ and $\tau(h_1) + \tau(\lambda_i)\tau(h_2)$ is also irreducible over $\overline{\mathbb{K}}$, we can write:

$$\begin{aligned} h_1 + \lambda_1 h_2 &= \tau(h_1) + \tau(\lambda_{i_1})\tau(h_2), \qquad (\star) \\ h_1 + \lambda_2 h_2 &= \tau(h_1) + \tau(\lambda_{i_2})\tau(h_2). \end{aligned}$$

Thus, $(\lambda_1 - \lambda_2)h_2 = (\tau(\lambda_{i_1}) - \tau(\lambda_{i_2}))\tau(h_2)$. As $lc(h_2) = 1$, we deduce that $(\lambda_1 - \lambda_2) = \tau(\lambda_{i_1}) - \tau(\lambda_{i_2})$ and then $h_2 = \tau(h_2)$. This implies that $h_2 \in \mathbb{K}[X_1, \ldots, X_n]$ because $\mathbb{K}$ is a perfect field.

Last step: we claim that $h_1 \in \mathbb{K}[X_1, \ldots, X_n]$. Indeed, $(\star)$ and the hypothesis $h_1(0, \ldots, 0) = 0$ (see step 3) implies that $\lambda_1 h_2(0, \ldots, 0) = \tau(\lambda_{i_1})h_2(0, \ldots, 0)$. As $h_2(0, \ldots, 0) \neq 0$ (by step 3 again), we get $\lambda_1 = \tau(\lambda_{i_1})$. Then $(\star)$ means that $h_1 = \tau(h_1)$ and this concludes the proof because $\mathbb{K}$ is a perfect field. □

Remark 14. First, notice that the above result remains obviously true when we take any extension of $\mathbb{K}$ instead of $\overline{\mathbb{K}}$. Also, observe that this theorem is false for univariate[2] ($n = 1$) rational function; see [9, Example 5]. Finally, mention that if $p \leq d^2$ and the field $\mathbb{K}$ is not perfect then the theorem is also false. Indeed, in [2, page 27] one can find the following counterexample: $f(X, Y) = X^p + bY^p =$

[2]Recall that a non-constant univariate rational function $r(X) \in \mathbb{K}(X)$ is called composite over a field $\mathbb{K}$ if $r(X) = u(h(X))$, where $u,\ h \in \mathbb{K}(X)$ such that $\deg(u) \geq 2$ and $\deg(h) \geq 2$.

$(X+\beta Y)^p$, with $b \in \mathbb{K} \setminus \mathbb{K}^p$ and $\beta^p = b$, is composite in $\mathbb{K}(\beta)$ (which is clear) but non-composite in $\mathbb{K}$ (which is proved in loc. cit.).

Theorem 11 and Theorem 13 yield the

Corollary 15.

$$\begin{aligned} r = f/g \text{ is non-composite} &\iff \operatorname{Spect}_{f,g}(T) \neq 0 \text{ in } \mathbb{K}[T] \\ &\iff \sigma(f,g) \text{ is finite.} \end{aligned}$$

Corollary 15 clearly implies several results about the indecomposability of r. For instance, if $r = f/g$ is a non-composite rational function where $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$, and p is a prime integer bigger than $H(\operatorname{Spect}_{f,g})$ and the bound $\mathcal{B}$ of Theorem 6, then $\overline{r}^p$ is non-composite. Indeed, $\overline{\operatorname{Spect}_{f,g}}^p = \operatorname{Spect}_{\overline{f}^p,\overline{g}^p} \neq 0$ in $\mathbb{F}_p[T]$, for all $p > \mathcal{B}$.

With this strategy we could deduce several similar results but the bounds obtained in this way can be improved. Indeed, when we use the polynomial Spect we have to study the gcd of the $\Phi_t(f - Tg)$'s. But if r is supposed to be non-composite then there exits an index t_0 such that $\Phi_{t_0}(f - Tg) \neq 0$. In this case it is enough to study the behaviour of one polynomial instead of the gcd of several polynomials. Thus, in what follows we are going to study the indecomposability of a rational function using Noether's forms.

3.1. **Reduction modulo p.**

Theorem 16. *Let $r = f/g \in \mathbb{Z}(\underline{X})$ be a non-constant reduced and non-composite rational function. If*

$$p > \mathcal{H} = d^{3d^2-3}\left(\binom{n+d}{n}2^d\right)^{d^2-1}\binom{d^2-1}{\lfloor (d^2-1)/2 \rfloor}\max\big(H(f), H(g)\big)^{d^2-1},$$

then $\overline{r}^p$ is non-composite and $\overline{f}^p$, $\overline{g}^p$ are coprime.

Proof. Thanks to Theorem 11, we have that $f - Tg$ is irreducible in $\overline{\mathbb{Q}(T)}[X_1, \ldots, X_n]$. Therefore, there exists t_0 such that $\Phi_{t_0}(f - Tg) \neq 0$ in $\mathbb{Z}[T]$. Now, if $p > \mathcal{H}$ then $\overline{\Phi_{t_0}}^p(\overline{f}^p - T\overline{g}^p) \neq 0$ (see the proof of Theorem 6). This means that $\overline{f}^p - T\overline{g}^p$ is irreducible in $\overline{\mathbb{F}_p(T)}[X_1, \ldots, X_n]$ and hence $\overline{r}^p$ is non-composite by Theorem 11. Of course, $\overline{f}^p$ and $\overline{g}^p$ are coprime because otherwise $\overline{f}^p - T\overline{g}^p$ cannot be irreducible. □

3.2. **Indecomposability of rational function with coefficients in $\mathbb{K}[\underline{Z}]$.**

Theorem 17. *Let d and k be positive integers, $\mathbb{K}$ be a perfect field of characteristic 0 or $p \geq d^2$, $r = f/g \in \mathbb{K}[\underline{Z}](\underline{X})$ be a non-constant reduced rational function with $0 < \deg_{\underline{X}}(r) \leq d$, $0 < \deg_{\underline{Z}}(r) \leq k$ and let S be a finite subset of $\mathbb{K}$.*

If r is non-composite over $\mathbb{K}(\underline{Z})$ then for a uniform random choice of z_i in S we have

$$\mathcal{P}\Big(\{r(z_1, \ldots, z_s, \underline{X}) \text{ is non-composite over } \mathbb{K} \mid z_i \in S\}\Big) \geq 1 - k(d^2-1)/|S|,$$

where $|S|$ denotes the cardinal of S and $\mathcal{P}$ the probability.

Proof. Assume that r is non-composite over $\mathbb{K}(\underline{Z})$. Then, by Theorem 11, we have that $f - Tg$ is irreducible in $\overline{\mathbb{K}(\underline{Z})}[\underline{X}]$. Thus there exists t_0 such that $\Phi_{t_0}(f - Tg) \neq 0$ in $\mathbb{K}[\underline{Z}][T]$. We can write $\Phi_{t_0}(f - Tg) = \sum_{i=0}^{D} a_i T^i$ with $a_i \in \mathbb{K}[\underline{Z}]$ and $a_D \neq 0 \in$

$\mathbb{K}[\underline{Z}]$. Therefore, for all $\underline{z} \in \mathbb{K}^s$ such that $a_D(\underline{z}) \neq 0$ we have $r(\underline{z}, \underline{X})$ is non-composite. Furthermore Theorem 1 gives $\deg_Z a_i \leq k(d^2-1)$. Then, Lemma 9 applied to $a_D(\underline{Z})$ gives the desired result. □

Remark 18. Theorem 17 is false with the hypothesis "r is non-composite over $\mathbb{K}$" instead of "r is non-composite over $\mathbb{K}(\underline{Z})$". Indeed, take $n = 2$ and $s = 1$ and consider the polynomial $f(X, Y, Z) = (XY)^2 + Z$. This polynomial is non-composite over $\mathbb{K}$ (because $\deg_Z(f) = 1$) but $f(X, Y, z) = (XY)^2 + z$ is composite over $\mathbb{K}$ for all value $z \in \mathbb{K}$.

3.3. **A reduction from n to two variables.** We give the following Bertini like result.

Theorem 19. *Let $\mathbb{K}$ be a perfect field of characteristic 0 or $p \geq d^2$, S be a finite subset of $\mathbb{K}$ and let $r = f/g \in \mathbb{K}(X_1, \ldots, X_n)$ be a reduced non-composite rational function.*

For a uniform random choices of the u_i's, v_i's and w_i's in S, the rational function

$$\tilde{r}(X, Y) = r(u_1X + v_1Y + w_1, \ldots, u_nX + v_nY + w_n) \in \mathbb{K}[X, Y].$$

is non-composite with probability at least $1 - \big(3d(d-1)+1\big)/|S|$ where d is the degree of r.

Proof. As we did before, we study $f - Tg$. This polynomial is irreducible over $\overline{\mathbb{K}(T)}$ by Theorem 11. Then we apply the effective Bertini's Theorem given in [15, Corollary 8] to this polynomial. We obtain that $\tilde{f}(X, Y) - T\tilde{g}(X, Y)$ is irreducible in $\overline{\mathbb{K}(T)}[X, Y]$ with a probability at least $1 - \big(3d(d-1)+1\big)/|S|$. Then by Theorem 11 yields the desired result about $\tilde{r}$. □

4. Acknowledgment

During the preparation of this paper, the third author was supported by Abdus Salam center (ICTP, Trieste) and after by Max-Planck Institut (Bonn). He wish to thank Pierre Dèbes for encouragements and comments, as well as Enrico Bombieri and Umberto Zannier for their discussions in the beginning of this work.

References

[1] Shreeram S. Abhyankar, William J. Heinzer, and Avinash Sathaye. Translates of polynomials. In *A tribute to C. S. Seshadri (Chennai, 2002)*, Trends Math., pages 51–124. Birkhäuser, Basel, 2003.
[2] Mohamed Ayad. Sur les polynômes $f(X, Y)$ tels que $K[f]$ est intégralement fermé dans $K[X, Y]$. *Acta Arith.*, 105(1):9–28, 2002.
[3] A. Bodin. Reducibility of rational functions in several variables. *Israel J. Math.*, to appear, 2008.
[4] A. Bodin, P. Dèbes, and S. Najib. On indecomposable polynomials and their spectrum. *Acta Arith.*, 2009. To appear.
[5] L. Busé and G. Chèze. On the total order of reducibility of a pencil of algebraic plane curves. Preprint, 2008.
[6] G. Chèze and S. Najib. indecomposability of polynomials via jacobian matrix. Preprint, 2007.
[7] Ewa Cygan. Factorization of polynomials. *Bull. Polish Acad. Sci. Math.*, 40(1):45–52, 1992.
[8] Shuhong Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72(242):801–822 (electronic), 2003.
[9] Jaime Gutierrez and David Sevilla. Building counterexamples to generalizations for rational functions of Ritt's decomposition theorem. *J. Algebra*, 303(2):655–667, 2006.

[10] J. P. Jouanolou. *Équations de Pfaff algébriques*, volume 708 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979.
[11] J. P. Jouanolou. Idéaux résultants. *Adv. in Math.*, 37(3):212–238, 1980.
[12] Shulim Kaliman. Two remarks on polynomials in two variables. *Pacific J. Math.*, 154(2):285–295, 1992.
[13] Erich Kaltofen. Effective Noether irreducibility forms and applications. *J. Comput. System Sci.*, 50(2):274–295, 1995. 23rd Symposium on the Theory of Computing (New Orleans, LA, 1991).
[14] Daniel Lazard. Algèbre linéaire sur $K[X_1, \cdots, X_n]$, et élimination. *Bull. Soc. Math. France*, 105(2):165–190, 1977.
[15] Grégoire Lecerf. Improved dense multivariate polynomial factorization algorithms. *J. Symbolic Comput.*, 42(4):477–494, 2007.
[16] Dino Lorenzini. Reducibility of polynomials in two variables. *J. Algebra*, 156(1):65–75, 1993.
[17] Salah Najib. Une généralisation de l'inégalité de Stein-Lorenzini. *J. Algebra*, 292(2):566–573, 2005.
[18] Henri Poincaré. Sur l'intégration algébrique des équations différentielles du premier ordre. *Rend. Circ. Mat. Palermo*, 5:161–191, 1891.
[19] Wolfgang Ruppert. Reduzibilität Ebener Kurven. *J. Reine Angew. Math.*, 369:167–191, 1986.
[20] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.
[21] Wolfgang M. Schmidt. *Equations over finite fields. An elementary approach*. Springer-Verlag, Berlin, 1976. Lecture Notes in Mathematics, Vol. 536.
[22] Yosef Stein. The total reducibility order of a polynomial in two variables. *Israel J. Math.*, 68(1):109–122, 1989.
[23] Angelo Vistoli. The number of reducible hypersurfaces in a pencil. *Invent. Math.*, 112(2):247–262, 1993.
[24] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.
[25] Chee Keng Yap. *Fundamental problems of algorithmic algebra*. Oxford University Press, New York, 2000.
[26] Umberto Zannier. On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$. *Arch. Math. (Basel)*, 68(2):129–138, 1997.

INRIA, Galaad, 2004 route des Lucioles, B.P. 93, Sophia Antipolis, 06902,
E-mail address: Laurent.Buse@inria.fr

Institut de Mathmatiques de Toulouse, Universit Paul Sabatier Toulouse 3, MIP Bt 1R3, 31 062 TOULOUSE cedex 9, France
E-mail address: guillaume.cheze@math.ups-tlse.fr

Max-Planck Institut für Mathematik. Vivatsgasse 7, Bonn 53111. Germany
E-mail address: najib@mpim-bonn.mpg.de, salah.najib@math.univ-lille1.fr