ACTA ARITHMETICA
147.3 (2011)

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

by

LAURENT BUSÉ (Sophia Antipolis), GUILLAUME CHÈZE (Toulouse) and
SALAH NAJIB (Brive)

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

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

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

It is customary to say that f is *non-composite* if it 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 states 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 if f is non-composite, then the cardinality of $\sigma(f)$ does not exceed $\deg(f) - 1$; 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.

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

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

with

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

2010 *Mathematics Subject Classification*: Primary 12E05; Secondary 11C08, 12Y05.
Key words and phrases: spectrum, GCD, Noether's theorem, Ostrowski's theorem, Bertini's theorem, composite rational function.

DOI: 10.4064/aa147-3-2 © Instytut Matematyczny PAN, 2011

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

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

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

Again, r is said to be *non-composite* if it 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 $\mu f^\sharp - \lambda g^\sharp = 0$, $(\mu : \lambda) \in \mathbb{P}^1_{\overline{\mathbb{K}}}$, 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 $d = 1$ or $n = 1$. 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 was obtained by Poincaré [18]. Poincaré's bound was improved by many writers: 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 irreducibility theorem given by W. Ruppert in [19].

In this article, we follow the strategy of [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 find that, under some suitable hypothesis, $\varphi(\mathrm{Spect}_{f,g})$ is equal to $\mathrm{Spect}_{\varphi(f),\varphi(g)}$. For two special situations, namely when $f, g \in \mathbb{Z}[\underline{X}]$ and φ is the reduction modulo a prime number p, or when $f, g \in \mathbb{K}[Z_1,\ldots,Z_s][\underline{X}]$ 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 we study the behavior of a composite rational function. More precisely we show that, under some suitable hypothesis, "f/g is composite over its coefficient field" if and only if "f/g is composite over any extension of its coefficient field". Thanks to the effective Noether irreducibility theorem, we then show that if r is a non-composite rational function with integer coefficients and p is a large prime, then r modulo p is also non-composite. An explicit lower bound is given for such a prime. Finally, with the same approach we also study the specialization of a non-composite rational function with coefficients in $\mathbb{K}[Z_1, \dots, Z_n]$ after the evaluation $Z_i = z_i \in \mathbb{K}$, $i = 1, \dots, n$. We end the paper with a Bertini-like result for non-composite rational functions.

Notation. If

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

then we set

$$H(f) = \max_{i_1,\dots,i_n} |c_{i_1,\dots,i_n}| \quad \text{and} \quad \|f\|_1 = \sum_{i_1,\dots,i_n} |c_{i_1,\dots,i_n}|.$$

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

For simplicity, given a ring morphism $\rho : A \to B$, we will still denote by ρ its canonical extensions to polynomials, $A[\underline{X}] \to B[\underline{X}]$, and to matrices, $\mathrm{Mat}_{p,q}(A) \to \mathrm{Mat}_{p,q}(B)$.

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

1.1. Noether reducibility forms. We recall some effective results about Noether forms that give a necessary and sufficient condition on the coefficients for 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, $d, n \geq 2$ and*

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

There exists a finite set of polynomials

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

such that

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

where F is the homogeneous polynomial $X_0^{\deg(f)} f(X_1/X_0, \dots, X_n/X_0)$. Furthermore,

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

If $\mathbb{K}$ has positive characteristic $p > d(d-1)$, then the above statement remains valid save that the Φ_t are now polynomials with coefficients in $\mathbb{F}_p$.

Proof. In characteristic zero the conclusion has been proved by Ruppert [19]. Gao [8, Lemma 2.4] showed that the conclusion is implied by the non-vanishing of a certain resultant. This covers the case of positive characteristic $p > d(d-1)$. ∎

It should be noticed that a similar theorem is true without any hypothesis on the characteristic of the ground field $\mathbb{K}$ (see e.g. [13, Theorem 7]), but then the estimates for the degrees and heights are much weaker than the ones given here.

1.2. GCDs of several polynomials under specialization. The following theorem is a classical result of elimination theory. Modern statements and proofs 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 degrees $d_1 \geq \cdots \geq d_n \geq 1$ 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)

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

does not have (maximal) rank $d_1 + d_2$.

In particular, given a field $\mathbb{L}$ and a ring morphism $\rho : A \to \mathbb{L}$, $\rho(f_1), \ldots, \rho(f_n)$ have a common root in the projective line over $\overline{\mathbb{L}}$ if and only if $\rho(\varphi)$ does not have (maximal) rank $d_1 + d_2$.

This theorem allows us to control the behavior of GCDs of several polynomials with coefficients in a UFD 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, let $f_1, \ldots, f_n$ be $n \geq 2$ non-zero homogeneous polynomials in $A[U,V]$ and let $\rho : A \to \mathbb{L}$ be a ring morphism into a field $\mathbb{L}$. Let $\alpha \in A$ be the leading coefficient of $\gcd(f_1, \ldots, f_n) \in A[U,V]$. There exists a finite collection $(c_i)_{i \in I}$ of computable elements in A with the following property: if $\rho(c_i) \neq 0$ for some $i \in I$ then*

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

Proof. Set $g_\rho = \gcd(\rho(f_1), \ldots, \rho(f_n)) \in \mathbb{L}[U,V]$, which is a monic polynomial, and $g = \gcd(f_1, \ldots, f_n) \in A[U,V]$. For all $i = 1, \ldots, n$ there exists a

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

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 $\rho(g)$ 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 by $(c_i)_{i\in I}$ 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: when $A = \mathbb{Z}$ and ρ is the reduction modulo p, and when $A = \mathbb{K}[Z_1,\dots,Z_s]$ and $\rho : A \to \mathbb{K}$ is an evaluation morphism. Our next task is to detail Corollary 3 in these two situations.

Proposition 4. *Let $f_1,\dots,f_n \in \mathbb{Z}[U,V]$ be $n \geq 2$ homogeneous polynomials of positive degree and set*

$$d = \max_i \deg(f_i), \qquad H = \max_i H(f_i).$$

(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 primes*

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

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

$$\overline{\alpha}^p \cdot \gcd(\overline{f}_1^p,\dots,\overline{f}_n^p) = \overline{\gcd(f_1,\dots,f_n)}^p \in \mathbb{F}_p[U,V]$$

for all primes

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

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

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

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

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

Therefore, one of these minors remains non-zero modulo p, and Theorem 2 implies that $\overline{f}_1^p, \dots, \overline{f}_n^p$ do not have a common root in the projective line over an algebraically closed field extension of $\mathbb{F}_p$. We deduce that $\overline{f}_1^p, \dots, \overline{f}_n^p$ 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 the notation introduced in its proof. For all $i = 1, \dots, n$ 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 $\rho(h_1), \dots, \rho(h_n)$ do not have a homogeneous common factor of positive degree in $\mathbb{F}_p[U,V]$. Now, for all $i = 1, \dots, n$ we have $\deg(h_i) \leq d$. Moreover, Mignotte's bound [24, Corollary 6.33] implies that $H(h_i) \leq (d+1)^{1/2} 2^d H$. Therefore, applying (i) we deduce that the claimed equality holds if

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

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])

$$\overline{\gcd(f_1, f_2)}^p = \overline{\alpha} \cdot \gcd(\overline{f}_1, \overline{f}_2) \in \mathbb{F}_p[U,V] \tag{1.1}$$

if and only if $p \nmid \operatorname{Res}(h_1, h_2) \in \mathbb{Z}$, where $f_i = \gcd(f_1, f_2)h_i$, $i = 1, 2$, and $\operatorname{Res}(h_1, h_2)$ 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 $\underline{Z} := (Z_1, \dots, Z_s)$.

Proposition 5. *Let $f_1, \dots, f_n$ 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, let $\rho : \mathbb{K}[\underline{Z}] \to \mathbb{K}$ be a ring morphism and assume that all coefficients of $f_1, \dots, f_n$ 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 non-zero 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 non-zero elements in $\mathbb{K}[\underline{Z}]$ of degree $\leq 2dk$ such that if $\rho(q_i)$, $i \in I$, are not all zero, then*

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

Proof. Analogous to the proof of Proposition 4. $\blacksquare$

2. Study of the spectrum of a rational function. Let A be a UFD, $\mathbb{K}$ be its fraction field and $r = f/g \in \mathbb{K}(X_1, \ldots, X_n)$ be a rational function such that $f, g \in A[X_1, \ldots, X_n]$ 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

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

where

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

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

$$V f^\sharp(X_0, \ldots, X_n) - U g^\sharp(X_0, \ldots, X_n) \in A[U,V][X_0, X_1, \ldots, X_n].$$

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 $(\lambda : \mu) \in \mathbb{P}^1_{\overline{\mathbb{K}}}$ we have

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

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

$$\rho(\mathrm{Spect}_{f,g}) = \gamma \cdot \mathrm{Spect}_{\rho(f),\rho(g)} \qquad \text{for some } \gamma \in \mathbb{L} \setminus \{0\}.$$

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

2.1. Spectrum and reduction modulo p

THEOREM 6. *Let $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ with $\gcd(f,g) = 1$. Set $d = \deg(f/g) = \max(\deg(f), \deg(g))$. For all primes $p > \mathcal{B}$ with*

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

where

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

we have

$$\overline{\mathrm{Spect}}^p_{f,g} = \kappa \cdot \mathrm{Spect}_{\overline{f}^p, \overline{g}^p}$$

in the polynomial ring $\mathbb{F}_p[U,V]$ for some $\kappa \in \mathbb{F}_p \setminus \{0\}$.

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

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

and

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

It follows that

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

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

$$\overline{\mathrm{Spect}_{f,g}(U,V)}^p = \overline{\gcd(\Phi_t(Vf^\sharp - Ug^\sharp))}^p = \kappa\cdot \gcd(\overline{\Phi_t(Vf^\sharp - Ug^\sharp)}^p)$$

if $p > \mathcal{B}$, for some $\kappa \in \mathbb{F}_p \setminus \{0\}$, and therefore

$$\overline{\mathrm{Spect}_{f,g}(U,V)}^p = \kappa\cdot \mathrm{Spect}_{\overline{f}^p,\overline{g}^p}(U,V)$$

by Theorem 1. ∎

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

Corollary 7. *In the notation of Theorem 6, if $\sigma(f,g)=\emptyset$ then $\sigma(\overline{f}^p,\overline{g}^p)=\emptyset$ for all primes $p>\mathcal{B}$.*

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

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

Theorem 8. *Let $f,g\in\mathbb{K}[Z_1,\dots,Z_s][X_1,\dots,X_n]$ with $\deg_{\underline{Z}}(f)\le k$, $\deg_{\underline{Z}}(g)\le k$, $\deg_{\underline{X}}(f)\le d$ and $\deg_{\underline{X}}(g)\le d$. Given $\underline{z} := (z_1,\dots,z_s)\in\mathbb{K}^s$, denote by $\mathrm{ev}_{\underline{z}}$ the ring morphism $\mathbb{K}[Z_1,\dots,Z_s]\to\mathbb{K}$ that sends Z_i to z_i for all $i=1,\dots,s$. There exists a finite collection of non-zero 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*

$$\mathrm{ev}_{\underline{z}}(\mathrm{Spect}_{f,g}) = \kappa\cdot\mathrm{Spect}_{\mathrm{ev}_{\underline{z}(f)},\mathrm{ev}_{\underline{z}(g)}} \qquad \textit{for some } \kappa\in\mathbb{K}\setminus\{0\}.$$

Proof. We consider again Noether's forms $(\Phi_t(Vf^\sharp - Ug^\sharp))_{t\in T}$. By construction, $\deg_{\underline{Z}}(\Phi_t(Vf^\sharp - Ug^\sharp))\le (d^2-1)k$ and $\deg_{U,V}(\Phi_t(Vf^\sharp - Ug^\sharp))\le$

$d^2 - 1$. Therefore, Proposition 5 yields 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

$$\mathrm{ev}_{\underline{z}}(\mathrm{Spect}_{f,g}) = \kappa \cdot \mathrm{Spect}_{\mathrm{ev}_{\underline{z}(f)},\mathrm{ev}_{\underline{z}(g)}} \qquad \text{for some } \kappa \in \mathbb{K}\setminus\{0\}$$

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 Lemma that we recall.

LEMMA 9 (Zippel–Schwartz). *Let $P \in A[X_1,\dots,X_n]$ 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*

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

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

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

$$\sigma(\mathrm{ev}_{\underline{z}(f)}, \mathrm{ev}_{\underline{z}(g)}) = \emptyset$$

with probability at least $1 - 2(d^2-1)^3k^2/|S|$.

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 $q_ic(\underline{z}) \neq 0$ for some $i \in I$, where $(q_i)_{i\in I}$ is the collection of polynomials in Theorem 8, then $\mathrm{Spect}_{\mathrm{ev}_{\underline{z}(f)},\mathrm{ev}_{\underline{z}(g)}} \in \mathbb{K}$. ∎

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 $r(X_1,\dots,X_n) \in \mathbb{K}(X_1,\dots,X_n)$ is closely related to the indecomposability of r over $\overline{\mathbb{K}}$. After recalling this link, we will study the indecomposability of rational functions.

THEOREM 11. *Let $\mathbb{K}$ be a field of characteristic $p \ge 0$. Let $r = f/g \in \mathbb{K}(X_1,\dots,X_n)$ 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 $\overline{\mathbb{K}}[X_1,\dots,X_n]$ for all $\lambda \in \overline{\mathbb{K}}$ such that* $\deg(f-\lambda g) = \deg(r)$,
(iii) *$f(X_1,\dots,X_n) - Tg(X_1,\dots,X_n)$ is reducible in $\overline{\mathbb{K}(T)}[X_1,\dots,X_n]$.*

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)⇔(ii): See [3, Theorem 2.2].

(ii)⇒(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 implies that $f-Tg$ is reducible in $\overline{\mathbb{K}(T)}[X_1,\dots,X_n]$.

(iii)⇒(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 $\overline{\mathbb{K}}[X_1,\dots,X_n]$. ∎

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

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

Proof. Obviously, if r is composite over $\mathbb{K}$ then it 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 $h\in\overline{\mathbb{K}}(X_1,\dots,X_n)$. We have $u=u_1/u_2$ where $u_1,u_2\in\overline{\mathbb{K}}[T]$, and $h=h_1/h_2$ is reduced and non-composite with $h_1,h_2\in\overline{\mathbb{K}}[X_1,\dots,X_n]$. We are going to show that there exist $U\in\mathbb{K}(T)$ and $H\in\mathbb{K}(X_1,\dots,X_n)$ such that $r=U(H)$.

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

Step 1: *One can suppose that* $\mathrm{lc}(f)=1$, $\mathrm{lc}(g)=1$ *and* $\mathrm{mdeg}(f)\succ\mathrm{mdeg}(g)$. Indeed, to satisfy the first condition, we just have to take $f/\mathrm{lc}(f)$ and $g/\mathrm{lc}(g)$. Then, for the second condition, 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 $\mathbb{K}$.

Step 2: *One can suppose that* $\mathrm{lc}(h_1)=1$, $\mathrm{lc}(h_2)=1$ *and* $\mathrm{mdeg}(h_1)\succ\mathrm{mdeg}(h_2)$. This actually follows by the same trick as 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 $v(T)=u(1/T)$.

Step 3: *One can suppose that* $h_1(0,\dots,0)=0$ *and* $h_2(0,\dots,0)\neq 0$. Indeed, if $h_2(0,\dots,0)\neq 0$ then we can consider

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

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

$$\begin{aligned}&h_2(X_1,\dots,X_n)\\&\quad=c_0(X_1,\dots,X_{n-1})+c_1(X_1,\dots,X_{n-1})X_n+\dots+c_d(X_1,\dots,X_{n-1})X_n^d\end{aligned}$$

with $c_i(X_1,\dots,X_{n-1})\in\overline{\mathbb{K}}[X_1,\dots,X_{n-1}]$ and $h_2(x_1,\dots,x_n)=0$ for all $(x_1,\dots,x_n)\in\mathbb{K}^n$. Then, for any $(x_1,\dots,x_{n-1})\in\mathbb{K}^{n-1}$, $h_2(x_1,\dots,x_{n-1},X_n)\in\overline{\mathbb{K}}[X_n]$ has degree $\leq d$ and at least p distinct roots in $\mathbb{K}$. It follows that $h_2(x_1,\dots,x_{n-1},X_n)$ is the null polynomial and hence

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

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

Step 4: $h_2(X_1,\dots,X_n)\in\mathbb{K}[X_1,\dots,X_n]$. To show this, we are going to prove that if r, h_1 and h_2 satisfy the hypothesis of the previous steps then $h_2\in\mathbb{K}[X_1,\dots,X_n]$.

Let $\lambda\in\mathbb{K}$ be such that $\deg(f+\lambda g)=\deg(r)=d$. Since r is composite over $\overline{\mathbb{K}}$, it follows that $f+\lambda g$ 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 Steps 1 and 2, $\mathrm{lc}(f+\lambda g)=1$ and $\mathrm{lc}(h_1+\lambda_i h_2)=1$ 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 by using Bertini's Theorem; see for instance [5, proof of Theorem 13] or [3]).

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

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

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

$$(\star)\qquad\begin{aligned}h_1+\lambda_1h_2&=\tau(h_1)+\tau(\lambda_{i_1})\tau(h_2),\\h_1+\lambda_2h_2&=\tau(h_1)+\tau(\lambda_{i_2})\tau(h_2).\end{aligned}$$

Thus, $(\lambda_1-\lambda_2)h_2=(\tau(\lambda_{i_1})-\tau(\lambda_{i_2}))\tau(h_2)$. As $\mathrm{lc}(h_2)=1$, 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 $h_2 \in \mathbb{K}[X_1, \dots, X_n]$ because $\mathbb{K}$ is a perfect field.

STEP 5: $h_1 \in \mathbb{K}[X_1, \dots, X_n]$. Indeed, $(\star)$ and the hypothesis $h_1(0, \dots, 0) = 0$ (see Step 3) imply that $\lambda_1 h_2(0, \dots, 0) = \tau(\lambda_{i_1}) h_2(0, \dots, 0)$. As $h_2(0, \dots, 0) \neq 0$ (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 obviously remains true when we take any extension of $\mathbb{K}$ instead of $\overline{\mathbb{K}}$. Also, observe that the conclusion of this theorem is false for univariate [2] ($n = 1$) rational functions; see [9, Example 5]. Finally, we mention that if $p \leq d^2$ and the field $\mathbb{K}$ is not perfect then the conclusion is also false. Indeed, in [2, p. 27] one can find the following counterexample: $f(X, Y) = X^p + bY^p = (X + \beta Y)^p$, 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 there).

Theorems 11 and 13 yield

COROLLARY 15.

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

Corollary 15 clearly implies several results about the indecomposability of r. For instance, if $r = f/g$ is a non-composite rational function where $f, g \in \mathbb{Z}[X_1, \dots, X_n]$, and p is a prime greater than $H(\operatorname{Spect}_{f,g})$ and the bound $\mathcal{B}$ of Theorem 6, then $\overline{r}^p$ is non-composite. Indeed, $\overline{\operatorname{Spect}}^p_{f,g} = \operatorname{Spect}_{\overline{f}^p, \overline{g}^p} \neq 0$ in $\mathbb{F}_p[U, V]$ 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 $\Phi_t(Uf - Vg)$'s. But if r is supposed to be non-composite then there exists a t_0 such that $\Phi_{t_0}(Uf - Vg) \neq 0$. In this case it is enough to study the behavior 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 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 and set*

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

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

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

Proof. Thanks to Theorem 11, we know 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 $\overline{\Phi}^p_{t_0}(\overline{f}^p - T\overline{g}^p) \neq 0$ (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 functions 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 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*

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

Proof. Assume that r is non-composite over $\mathbb{K}(\underline{Z})$. Then, by Theorem 11, $f - Tg$ is irreducible in $\overline{\mathbb{K}(\underline{Z}, T)}[\underline{X}]$. 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 $a_D(\underline{z}) \neq 0$ the rational function $r(\underline{z}, \underline{X})$ is non-composite. Furthermore Theorem 1 gives $\deg_{\underline{Z}}(a_i) \leq k(d^2 - 1)$. 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 $f(X, Y, Z) = (XY)^2 + Z$. It 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 $z \in \mathbb{K}$.

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 $r = f/g \in \mathbb{K}(X_1, \ldots, X_n)$ be a reduced non-composite rational function. For 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 $1 - (3d(d-1) + 1)/|S|$ where d is the degree of r.

Proof. As before, we study $f - Tg$. This polynomial is irreducible over $\overline{\mathbb{K}(T)}$ by Theorem 11. We apply to this polynomial Lemma 7 in [13] and the effective Bertini Theorem given in [15, Corollary 8]. We find that $\tilde{f}(X,Y) - T\tilde{g}(X,Y)$ is irreducible in $\overline{\mathbb{K}(T)}[X,Y]$ with probability at least $1-(3d(d-1)+1)/|S|$. Then Theorem 11 yields the desired result about $\tilde{r}$. ∎

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

References

[1] S. S. Abhyankar, W. J. Heinzer, and A. Sathaye, *Translates of polynomials*, in: A tribute to C. S. Seshadri (Chennai, 2002), Trends Math., Birkhäuser, Basel, 2003, 51–124.

[2] M. Ayad, *Sur les polynômes $f(X,Y)$ tels que $K[f]$ est intégralement fermé dans $K[X,Y]$*, Acta Arith. 105 (2002), 9–28.

[3] A. Bodin, *Reducibility of rational functions in several variables*, Israel J. Math. 164 (2008), 333–347.

[4] A. Bodin, P. Dèbes, and S. Najib, *Indecomposable polynomials and their spectrum*, Acta Arith. 139 (2009), 79–100.

[5] L. Busé and G. Chèze, *On the total order of reducibility of a pencil of algebraic plane curves*, arXiv:0812.4706, 2008.

[6] G. Chèze and S. Najib, *Indecomposability of polynomials via jacobian matrix*, J. Algebra 324 (2010), 1–11.

[7] E. Cygan, *Factorization of polynomials*, Bull. Polish Acad. Sci. Math. 40 (1992), 45–52.

[8] S. H. Gao, *Factoring multivariate polynomials via partial differential equations*, Math. Comp. 72 (2003), 801–822 (electronic).

[9] J. Gutierrez and D. Sevilla, *Building counterexamples to generalizations for rational functions of Ritt's decomposition theorem*, J. Algebra 303 (2006), 655–667.

[10] J.-P. Jouanolou, *Équations de Pfaff algébriques*, Lecture Notes in Math. 708, Springer, Berlin, 1979.

[11] —, *Idéaux résultants*, Adv. Math. 37 (1980), 212–238.

[12] S. Kaliman, *Two remarks on polynomials in two variables*, Pacific J. Math. 154 (1992), 285–295.

[13] E. Kaltofen, *Effective Noether irreducibility forms and applications*, J. Comput. System Sci. 50 (1995), 274–295.

[14] D. Lazard, *Algèbre linéaire sur $K[X_1, \ldots, X_n]$, et élimination*, Bull. Soc. Math. France 105 (1977), 165–190.

[15] G. Lecerf, *Improved dense multivariate polynomial factorization algorithms*, J. Symbolic Comput. 42 (2007), 477–494.

[16] D. Lorenzini, *Reducibility of polynomials in two variables*, J. Algebra 156 (1993), 65–75.

[17] S. Najib, *Une généralisation de l'inégalité de Stein–Lorenzini*, ibid. 292 (2005), 566–573.

[18] H. Poincaré, *Sur l'intégration algébrique des équations différentielles du premier ordre*, Rend. Circ. Mat. Palermo 5 (1891), 161–191.

[19] W. Ruppert, *Reduzibilität ebener Kurven*, J. Reine Angew. Math. 369 (1986), 167–191.

[20] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia Math. Appl. 77, Cambridge Univ. Press, Cambridge, 2000.

[21] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, Berlin, 1976.

[22] Y. Stein, *The total reducibility order of a polynomial in two variables*, Israel J. Math. 68 (1989), 109–122.

[23] A. Vistoli, *The number of reducible hypersurfaces in a pencil*, Invent. Math. 112 (1993), 247–262.

[24] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 2nd ed., Cambridge Univ. Press, Cambridge, 2003.

[25] C. K. Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford Univ. Press, New York, 2000.

[26] U. Zannier, *On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$*, Arch. Math. (Basel) 68 (1997), 129–138.

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

Guillaume Chèze
Institut de Mathématiques de Toulouse
Université Paul Sabatier Toulouse 3
MIP Bât. 1R3
31062 Toulouse Cedex 9, France
E-mail: guillaume.cheze@math.ups-tlse.fr

Salah Najib
Université de Limoges
IUT du Limousin
7 rue Jules Vallès
19100 Brive, France
E-mail: najibm@voila.fr

Received on 16.6.2009
and in revised form on 15.12.2010 (6060)