Journal of Number Theory 170 (2017) 390–408

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Families of polynomials and their specializations

Arnaud Bodin [a], Pierre Dèbes [a,*], Salah Najib [b]

[a] *Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France*
[b] *Faculté Polydisciplinaire de Khouribga, Université Hassan 1er, BP 145, Hay Ezzaytoune, 25000 Khouribga, Maroc*

ARTICLE INFO

Article history:
Received 20 October 2015
Received in revised form 8 June 2016
Accepted 10 June 2016
Available online 20 August 2016
Communicated by D. Wan

MSC:
primary 12E05
secondary 11C08, 13P05, 12Y05

Keywords:
Polynomials
Specialization
Irreducibility
Newton polygon
Good reduction
Deformation

ABSTRACT

For a polynomial in several variables depending on some parameters, we discuss some results to the effect that for almost all values of the parameters the polynomial is irreducible. In particular we recast in this perspective some results of Grothendieck and of Gao.

0. Introduction

This paper is devoted to irreducibility questions for families of polynomials in several indeterminates $x_1, \ldots, x_\ell$ parametrized by further indeterminates $t_1, \ldots, t_s$. We assume

* Corresponding author.
E-mail addresses: Arnaud.Bodin@math.univ-lille1.fr (A. Bodin), Pierre.Debes@math.univ-lille1.fr (P. Dèbes), slhnajib@gmail.com (S. Najib).

http://dx.doi.org/10.1016/j.jnt.2016.06.023
0022-314X/

that $\ell \geqslant 2$ and the base field k is algebraically closed; the more arithmetic case $\ell = 1$ depends on the base field and involves different tools and techniques.

Set $\underline{t} = \{t_1, \ldots, t_s\}$, $\underline{x} = \{x_1, \ldots, x_\ell\}$ and consider a polynomial $F \in k[\underline{t}, \underline{x}]$, irreducible in $\overline{k(\underline{t})}[\underline{x}]$ (where $\overline{k(\underline{t})}$ is the algebraic closure of $k(\underline{t})$); F is said to be *generically irreducible*. The core question is about the irreducibility of the polynomials obtained by substituting elements $t_1^*, \ldots, t_s^* \in k$ for the corresponding parameters $t_1, \ldots, t_s$ – the *specializations of* F.

More specifically we wish to investigate the following problem, as explicitly as possible:

– when the generic irreducibility property is satisfied, show some boundedness results on the following set, which we call the *spectrum* of F:

$$\mathrm{sp}(F) = \{\underline{t}^* = (t_1^*, \ldots, t_s^*) \in k^s \mid F(\underline{t}^*, \underline{x}) \text{ is reducible in } k[\underline{x}]\},$$

and some density results for its complement,

– find some criteria for the generic irreducibility property to be satisfied and deduce some new specific examples.

A first approach rests on classical results of Noether and Bertini and a second one involves more combinatorial tools like the Newton polygon and the associated Minkowski theorem. We contribute to these approaches by implementing some ideas and results coming from connected areas, notably of Grothendieck (Arithmetic Geometry) and Gao (Polyhedral Combinatorics). This leads to new answers to the problem together with an improved and unified presentation of results from our previous papers [BDN09a,BDN09b] and other related papers. Those were concerned with special cases of the general situation considered here. In particular polynomials $f(x, y) - t$ and variants of those have been much studied and the word "spectrum" refers to the classical terminology used in this special case.

§1 briefly reviews the classical background and introduces our contribution, which is then detailed in §2 and §3.

1. The classical approaches and our contribution

1.1. The arithmetico-geometric approach

Fix $F \in k[\underline{t}, \underline{x}]$ and assume as above that it is generically irreducible.

1.1.1. Noether

Denote by $\mathcal{U}_F$ the open Zariski subset of all $\underline{t}^* \in k^s$ such that $\deg(F(\underline{t}^*, \underline{x})) = \deg_{\underline{x}} F(\underline{t}, \underline{x})$. The spectrum $\mathrm{sp}(F)$ is a proper Zariski closed subset of $\mathcal{U}_F$: there exist non-zero polynomials $h_1, \ldots, h_\nu \in k[\underline{t}]$ such that

$$\mathrm{sp}(F) \cap \mathcal{U}_F = \mathcal{Z}(h_1, \ldots, h_\nu) \cap \mathcal{U}_F \tag{1}$$

where $\mathcal{Z}(h_1, \ldots, h_\nu)$ denotes the zero set of $h_1, \ldots, h_\nu$. In other words, for $\underline{t}^* \in k^s$ such that $\deg(F(\underline{t}^*, \underline{x})) = \deg_{\underline{x}} F(\underline{t}, \underline{x})$,

(2) *$F(\underline{t}^*, \underline{x})$ is reducible in $k[\underline{x}]$ if and only if $h_m(\underline{t}^*) = 0$ for each $m = 1, \dots, \nu$.*

This is the classical Noether theorem (*e.g.* [Sch00, §3.1 theorem 32]) which follows from elimination theory. Namely recall that for a given degree d and a given number of indeterminates ℓ, if $(a_{\underline{i}})_{\underline{i} \in I_{\ell,d}}$ are indeterminates that correspond to the coefficients of a polynomial of degree d in ℓ indeterminates, then there exist finitely many homogeneous forms $\mathcal{N}_j(a_{\underline{i}})$ $(j = 1, \dots, D)$ in the $a_{\underline{i}}$ $(\underline{i} \in I_{\ell,d})$ and with coefficients in $\mathbb{Z}$ such that:

(3) *for a polynomial P of degree d in ℓ indeterminates and with coefficients $(a^*_{\underline{i}})_{\underline{i} \in I_{\ell,d}}$ in an algebraically closed field K (in such a way that $a^*_{\underline{i}}$ corresponds to $a_{\underline{i}}$), the polynomial P, if it is of degree d, is reducible in $K[\underline{x}]$ if and only if $\mathcal{N}_j(a^*_{\underline{i}}) = 0$, $j = 1, \dots, D$.*

Furthermore some subsequent works of Ruppert, Kaltofen, Gao and Chèze–Busé–Najib provide the following bounds for the degree of the *Noether forms* $\mathcal{N}_j$:

$$\begin{cases} \deg(\mathcal{N}_j) \leqslant d^2 - 1 & \text{if } k \text{ is of characteristic 0 [Rup86]} \\ & \text{or } p > d(d-1) \text{ [Gao03, th.2.3] [BCN11, th.1]} \\ \deg(\mathcal{N}_j) \leqslant 12 d^6 & \text{in general [Kal95]} \end{cases}$$

Description (1) of $\mathrm{sp}(F)$ follows, as explained in [BDN09b, §2.3.1]: one can take for $h_1, \dots, h_\nu \in k[\underline{t}]$ the values of the Noether forms at the coefficients in $k[\underline{t}]$ of the polynomial F. The above bounds yield, in each case

$$(4) \qquad \deg_{t_i}(h_m) \leqslant \deg_{t_i}(F) \times \begin{cases} d^2 - 1 \\ 12 d^6 \end{cases} \qquad (i = 1, \dots, s,\ m = 1, \dots, \nu)$$

1.1.2. Bertini–Noether

Every non-zero polynomial h in the ideal $\langle h_1, \dots, h_\nu \rangle$ of $k[\underline{t}]$ has this Bertini–Noether property: for every $\underline{t}^* \in k^s$ such that $\deg(F(\underline{t}^*, \underline{x})) = \deg_{\underline{x}} F(\underline{t}, \underline{x})$,

(5) *if $h(\underline{t}^*) \neq 0$ then $F(\underline{t}^*, \underline{x})$ is irreducible in $k[\underline{x}]$.*

Taking for h one of the non-zero polynomials $h_1, \dots, h_\nu$ yields, for $s = 1$ and k of characteristic 0 or $p > d(d-1)$,

$$(6) \qquad \mathrm{card}(\mathrm{sp}(F) \cap \mathcal{U}_F) \leqslant (d^2 - 1) \deg_{t_1}(F)$$

More generally, if $s \geqslant 1$, we have this conclusion:

(7) *For every $i = 1, \dots, s$, the set of $t_i^* \in k$ such that the polynomial $F(t_1, \dots, t_{i-1}, t_i^*, t_{i+1}, \dots, t_s, \underline{x})$ is of degree d and reducible in the polynomial ring $\overline{k(t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_s)}[\underline{x}]$ is of cardinality $\leqslant (d^2 - 1) \deg_{t_i}(F)$.*

Consequently, the polynomial $F(\underline{t}^*, \underline{x})$ is irreducible in $k[\underline{x}]$ provided that
- $t_1^* \in k$ stays out of a certain finite set E_1 of cardinality $\leqslant d^2 \deg_{t_1}(F)$,
- $t_2^* \in k$ stays out of a certain finite set E_2 of cardinality $\leqslant d^2 \deg_{t_2}(F)$ (E_2 depending on t_1^*),
- ...

– $t_s^* \in k$ stays out of a certain finite set E_s of cardinality $\leqslant d^2 \deg_{t_s}(F)$ (E_s depending on $t_1^*, \dots, t_{s-1}^*$).

1.1.3. Grothendieck and our contribution

We offer an approach in which we replace elimination theory and the Noether theorem by the Grothendieck good reduction criterion for algebraic covers. We base it on [Dèb16] which revisits Grothendieck's work [Gro71,GM71] with a polynomial viewpoint.

For polynomials $F(\underline{t}, T, Y)$ with $\ell = 2$ indeterminates T, Y, monic in Y, which this approach is more naturally concerned with, we produce an explicit polynomial $\mathcal{B}_F \in k[\underline{t}]$, called the *bad prime divisor* of F, that has the Bertini–Noether property (5):

(Corollary 2.8) *Assume* $\mathrm{char}(k) = 0$. *If* $\underline{t}^* \in k^s$ *satisfies* $\mathcal{B}_F(\underline{t}^*) \neq 0$, *then the polynomial* $F(\underline{t}^*, T, Y) \in k[T, Y]$ *is irreducible in* $k[T, Y]$.

The polynomial $\mathcal{B}_F$ is directly computable from the coefficients of F through elementary operations, starting with the discriminant $\Delta_F \in k[\underline{t}][T]$ of F relative to Y (§2.2). This general bound for the degree of $\mathcal{B}_F$ follows:

(8) $\quad \deg_{t_i}(\mathcal{B}_F) \leqslant 16 d^5 \deg_{t_i}(F)$, $(i = 1, \dots, s)$.

It is not as good as (4); the advantage of $\mathcal{B}_F$ lies in its full explicitness (which may lead to better bounds in specific cases (see §2.2.6)) and in its arithmetic meaning, where the name "bad prime divisor" originates: if $\mathcal{B}_F(\underline{t}^*) \neq 0$, the distinct roots (in $\overline{k(\underline{t})}$) of Δ_F remain defined and distinct after specialization of $\underline{t}$ to $\underline{t}^* \in k^s$. The construction improves on [BDN09a, §3], which used a result of Zannier rather than the Grothendieck reduction theory.

We also explain how to get rid of the "monic" assumption in Corollary 2.8, to relax the condition on the characteristic of k and to pass from 2 to any number ℓ of indeterminates. We finally obtain a statement like Corollary 2.8 above but in the bigger generality. The polynomial $\mathcal{B}_F$ has to be adjusted but is still explicitly described (see §2.3 and Corollary 2.10).

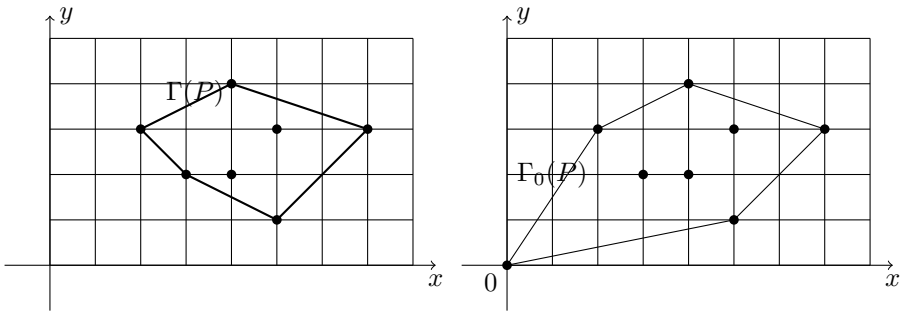
1.2. The more combinatorial approach

This second approach uses the Newton representation of polynomials as polyhedrons and the associated Minkowski irreducibility criterion. We will also review another related approach, based on the Bertini–Krull theorem and compare the two.

1.2.1. Newton–Minkowski

The Newton representation identifies monomials $x_1^{i_1} \cdots x_\ell^{i_\ell}$ with the corresponding ℓ-tuples $(i_1, \dots, i_\ell) \in \mathbb{R}^\ell$. Given a polynomial $P \in k[\underline{x}]$, define its *support* $\mathrm{supp}(P)$ as the set of monomials appearing in P with a non-zero coefficient and the *Newton polyhedron* $\Gamma(P)$ of P as the convex closure in $\mathbb{R}^\ell$ of $\mathrm{supp}(P)$. Also define $\Gamma_0(P)$ to be the convex

closure of $\mathrm{supp}(P) \cup \{0\}$. For example, the polynomial $P(x,y) = x^2y^3 + x^3y^2 + x^4y^2 + x^4y^4 + x^5y^3 + x^7y^3$ has the following Newton polygons $\Gamma(P)$ and $\Gamma_0(P)$:



The Minkowski theorem is this irreducibility criterion, where the sum $A + B$ of the two subsets A and B of $\mathbb{R}^\ell$ is $A + B = \{a + b \mid a \in A, b \in B\}$:

(9) *If $P = P_1 \cdot P_2$, with $P_1, P_2 \in k[\underline{x}]$, then $\Gamma(P) = \Gamma(P_1) + \Gamma(P_2)$. Consequently, if $\Gamma(P)$ is not summable, then P is irreducible in $k[\underline{x}]$,*

where we say that $\Gamma(P)$ is *summable* if it writes as the sum $A + B$ of two convex subsets A and B with integral vertices (in $\mathbb{N}^\ell$), each of them having at least two points. The converse is false: $(x - y + 1)(x + y + 1) + 1$ is irreducible but its Newton polygon is summable as it is also that of $(x - y + 1)(x + y + 1)$.

1.2.2. Our perspective

The Minkowski theorem can be viewed as follows. Suppose given a non-summable convex subset $\Gamma \subset \mathbb{R}^\ell$ with a set $\mathcal{V}_\Gamma$ of vertices contained in $\mathbb{N}^\ell$. Consider the polynomial obtained by summing all the monomials $t_{\underline{i}}\, x_1^{i_1} \cdots x_\ell^{i_\ell}$ where $\underline{i} = (i_1, \ldots, i_\ell)$ ranges over all the set $\mathcal{I}_\Gamma$ of all monomials inside Γ and the corresponding $t_{\underline{i}}$ are indeterminates, forming a set $\underline{t}_\Gamma$. Denote this polynomial by F_Γ, which is in $k[\underline{t}_\Gamma, \underline{x}]$.

(10) *F_Γ is generically irreducible and even satisfies this stronger irreducibility property: $F_\Gamma(\underline{t}^*_\Gamma, \underline{x})$ is irreducible in $k[\underline{x}]$, for every specialization $\underline{t}^*_\Gamma$ such that $t^*_{\underline{i}} \neq 0$ if $\underline{i} \in \mathcal{V}_\Gamma$.*

The condition on the specialization $\underline{t}^*_\Gamma$ indeed assures that the Newton polyhedron of $F_\Gamma(\underline{t}^*_\Gamma, \underline{x})$ is Γ. This yields this combinatorial version of the Bertini–Noether conclusion.

Proposition 1.1. *Let $F(\underline{t}, \underline{x}) \in k[\underline{t}, \underline{x}]$ be a polynomial with Newton polyhedron Γ (as a polynomial in $\underline{x}$). Denote its coefficients by $h_{\underline{i}}(\underline{t})$ ($\underline{i} \in \mathcal{I}_\Gamma$). If Γ is not summable then $F(\underline{t}^*, \underline{x})$ is irreducible in $k[\underline{x}]$ for every specialization $\underline{t}^*$ such that $h_{\underline{i}}(\underline{t}^*) \neq 0$ for each $\underline{i} \in \mathcal{V}_\Gamma$. Consequently, inequalities* (6), (7) *from §1.1.2 hold with $(d^2 - 1)\deg_{t_i}(F)$ replaced by $\mathrm{card}(\mathcal{V}_\Gamma)\deg_{t_i}(F)$.*

1.2.3. Bertini–Krull, Gao and our contribution

There exist efficient criteria and algorithms to decide whether a given convex set is summable, notably in a series of papers by Gao *et al.* [Gao01,GL01,ASGL04]. We use them in §3.2 to produce some new classes of generically irreducible polynomials.

The polynomial F_Γ from (10) is linear in the parameters $t_{\underline{i}}$ and we will focus on this special situation. That is: we will assume F is of the form

$$F = P(\underline{x}) - t_1 Q_1(\underline{x}) - \cdots - t_s Q_s(\underline{x}) \tag{11}$$

with $P, Q_1, \ldots, Q_s \in k[\underline{x}]$, which can be viewed as a *deformation* of the polynomial P by the polynomials $Q_1, \ldots, Q_s$. Here is an example of a result that can be deduced from Gao's criteria.

(Corollary 3.4) *Let $P, Q \in k[\underline{x}]$ such that*

(α) $\Gamma(P)$ is contained in a hyperplane $H \subset \mathbb{R}^\ell$ not passing through the origin,

(β) the coordinates of all the vertices of $\Gamma(P)$ are relatively prime,

(γ) $Q(0, \ldots, 0) \neq 0$, $\Gamma(Q) \subset \Gamma_0(P)$ and no monomial of Q is a vertex of $\Gamma(P)$.

Then the polynomial $F = P - tQ$ is generically irreducible and even has this stronger property: $P - t^*Q$ is irreducible in $k[\underline{x}]$ for every $t^* \in k \setminus \{0\}$.

For example, if p, q, r are 3 relatively prime positive integers, the polynomial

$$F(t, x, y, z) = x^p + y^q + z^r + t\,(\sum\nolimits_{\frac{i}{p}+\frac{j}{q}+\frac{k}{r}<1} a_{i,j,k} x^i y^j z^k\,) \quad \text{with } a_{0,0,0} \neq 0$$

satisfies the conclusion of Corollary 3.4 (as shown in Example 3.7, condition $a_{0,0,0} \neq 0$ can in fact be removed). Note further that the assumptions on P, Q in Corollary 3.4 only depend on the Newton polyhedrons $\Gamma(P)$ and $\Gamma(Q)$.

Before getting to applications of Gao's results, we review in §3.1 a more classical approach for polynomials as in (11), based on the Bertini–Krull theorem. The special case $P - tQ$ has been much studied due to its connection with the indecomposability and the spectrum of the rational function P/Q. The even more special case $Q = 1$ is of particular interest since a famous theorem of Stein provides an optimal bound for the cardinality of $\mathrm{sp}(P - t)$ which is sharper than the Bertini–Noether bound. This bound issue leads us to discuss to what extent the spectrum of a rational function can be prescribed. Finally we review and compare with Gao's results some results of [BDN09b] concerned with the special case of (11) that $Q_1, \ldots, Q_s$ are monomials, for which the Bertini–Krull theorem is also a main ingredient.

2. The Grothendieck arithmetico-geometric approach

This section elaborates on §1.1.3. §2.1 explains the reduction to the situation of $\ell = 2$ indeterminates. §2.2 introduces the bad prime divisor and the Grothendieck approach. Finally, §2.3 conjoins §2.1 and §2.2.

The general notation introduced in §1 is retained.

2.1. Reduction to the situation $\ell = 2$

The main result of this subsection is the following statement. For more generality, several polynomials $F_1, \dots, F_h$ replace the single polynomial F from §1.

The following additional notation is needed. Given a polynomial P in the indeterminates $\underline{y} = (y_1, \dots, y_N)$ with coefficients in some integral domain and $B = (b_{ij})_{1 \leqslant i,j \leqslant N}$ a $N \times N$-matrix with entries in the same domain, set

$$P(B \cdot \underline{y}) = P(\sum_{j=1}^{N} b_{1j} y_j, \dots, \sum_{j=1}^{N} b_{Nj} y_j)$$

Theorem 2.1. *Let $F_1, \dots, F_h \in k[\underline{t}, \underline{x}]$, assumed to be irreducible in $\overline{k(\underline{t})}[\underline{x}]$ and $\kappa \subset k$ be an infinite subfield. There is a matrix $B = (b_{ij})_{i,j} \in \mathrm{GL}_\ell(\kappa)$ such that the polynomial $F_i(\underline{t}, B \cdot \underline{x})$, which is of the form*

$$F_i(t_1, \dots, t_s, \sum_{j=1}^{\ell} b_{1j} x_j, \dots, \sum_{j=1}^{\ell} b_{\ell j} x_j) \qquad (i = 1, \dots, h)$$

is irreducible in $\overline{k(\underline{t}, x_1, \dots, x_{\ell-2})}[x_{\ell-1}, x_\ell]$ and satisfies the degree condition $\deg_{x_{\ell-1}, x_\ell}(F_i(\underline{t}, B \cdot \underline{x})) = \deg_{\underline{x}}(F_i(\underline{t}, \underline{x}))$.

Remark 2.2. If $F_1, \dots, F_h$ are only irreducible in $k(\underline{t})[\underline{x}]$, the same conclusion holds with these adjustments: B should be a matrix $B = (b_{ij})_{i,j} \in \mathrm{GL}_{s+\ell}(\kappa)$ that applies to the $s + \ell$ indeterminates $t_1, \dots, t_s, x_1, \dots, x_\ell$; the resulting polynomial $F_i(B \cdot (\underline{t}, \underline{x}))$ is of the form

$$F_i(\beta_1(\underline{x}) + \tau_1(\underline{t}), \dots, \beta_{s+\ell}(\underline{x}) + \tau_{s+\ell}(\underline{t})) \qquad (i = 1, \dots, h)$$

for some κ-linear forms $\beta_1(\underline{x}), \dots, \beta_{s+\ell}(\underline{x}) \in \kappa[\underline{x}]$ and $\tau_1(\underline{t}), \dots, \tau_{s+\ell}(\underline{t}) \in \kappa[\underline{t}]$.

The main tool in the proof of Theorem 2.1 is Proposition 2.3 below. Let A be an integral domain with fraction field K and let $\underline{y} = \{y_1, \dots, y_N\}$, $\underline{z} = \{z_1, \dots, z_M\}$ be two sets of indeterminates with $N \geqslant 2$, $M \geqslant 1$.

Proposition 2.3. *Let $\kappa \subset A$ be an infinite subfield and $P_1, \dots, P_h \in A[\underline{z}, \underline{y}]$ be h polynomials, irreducible in $\overline{K}[\underline{z}, \underline{y}]$. There exists a matrix $B = (b_{ij})_{i,j} \in \mathrm{GL}_{M+N}(\kappa)$ such that for $i = 1, \dots, h$,*

(a) *the polynomial $P_i(B \cdot (\underline{z}, \underline{y}))$, which is of the form*

$$P_i(\beta_1(\underline{y}) + \tau_1(\underline{z}), \dots, \beta_{M+N}(\underline{y}) + \tau_{M+N}(\underline{z}))$$

for some κ-linear forms $\beta_1(\underline{y}), \dots, \beta_{M+N}(\underline{y}) \in \kappa[\underline{y}]$

and some κ-linear forms $\tau_1(\underline{z}), \dots, \tau_{M+N}(\underline{z}) \in \kappa[\underline{z}]$,

is irreducible in $\overline{K(\underline{z})}[\underline{y}]$,

(b) *furthermore* $\deg_{\underline{y}}(P_i(B \cdot (\underline{z}, \underline{y}))) = \deg_{\underline{z},\underline{y}}(P_i)$.

Remark 2.4. There are several variants of Proposition 2.3 in the literature: [Sch76, ch5, theorem 3d] for 1 polynomial ($h = 1$) and 1 parameter ($M = 1$), [Kal95, lemma 7] for $h = 1$, [Naj05, proposition 1] for $M = 1$. Our version has several polynomials and several parameters and the produced matrix has coefficients in any given infinite subfield of the ring A.

Theorem 2.1 corresponds to the following special case of Proposition 2.3: $\underline{z} = (x_1, \dots, x_{\ell-2})$, $\underline{y} = (x_{\ell-1}, x_\ell)$ and $A = k[\underline{t}]$ while Remark 2.2 corresponds to the special case: $\underline{z} = (t_1, \dots, t_s, x_1, \dots, x_{\ell-2})$, $\underline{y} = (x_{\ell-1}, x_\ell)$ and $A = k$.

Proof of Proposition 2.3. Proposition 2.3 is a generalization of [Naj05, proposition 1], which corresponds to the special situation: $\underline{z} = z_1$ and $\kappa = A = K$.

First we generalize [Naj05, proposition 1] to the situation "$\kappa \subset A$ infinite" (but still with $\underline{z} = z_1$). This only requires to adjust the proof of [Naj05]: the matrices that are constructed there with coefficients in K can be chosen with coefficients in κ, the main point being that κ is infinite. The core of the proof is the Matsusaka–Zariski theorem [FJ04, proposition 10.5.2].

This generalized [Naj05, proposition 1], applied to the situation of Proposition 2.3, provides a matrix $B_1 \in \mathrm{GL}_{M+N}(\kappa)$ such that $P_i(B_1 \cdot (\underline{z}, \underline{y}))$ is irreducible in $\overline{k(z_1)}[z_2, \dots, z_M, y_1, \dots, y_N]$ and satisfies the degree condition

$$\deg_{z_2,\dots,z_M,\underline{y}}(P_i(B_1 \cdot (\underline{z}, \underline{y}))) = \deg_{\underline{z},\underline{y}}(P_i) \ (i = 1, \dots, h).$$

Apply next the generalized [Naj05, proposition 1] to the polynomials $P_i(B_1 \cdot (\underline{z}, \underline{y}))$, $i = 1, \dots, h$, viewed as polynomials in the indeterminates $z_2, \dots, z_M, \underline{y}$ and to the same infinite subfield κ (of the coefficient field $k(z_1)$ of these polynomials). This provides a matrix $B_2 \in \mathrm{GL}_{M+N-1}(\kappa)$ which we make a matrix $B_2 \in \mathrm{GL}_{M+N}(\kappa)$ by letting it be the identity on the missing coordinate z_1 and is such that the polynomial $P_i(B_1 B_2 \cdot (\underline{z}, \underline{y}))$ is irreducible in $\overline{k(z_1, z_2)}[z_3, \dots, z_M, \underline{y}]$ and satisfies $\deg_{z_3,\dots,z_M,\underline{y}}(P_i(B_1 B_2 \cdot (\underline{z}, \underline{y}))) = \deg_{\underline{z},\underline{y}}(P_i)$ $(i = 1, \dots, h)$. Iterating this process leads to the desired statement. □

2.2. The bad prime divisor and the Grothendieck approach

This subsection is based on [Dèb16]. The context there is that of polynomials $F \in A[T, Y]$ with coefficients in a Dedekind domain A, with $A = \mathbb{Z}$ and $A = k[t]$ as typical examples. Here we focus on the situation $A = k[\underline{t}]$, which is not a Dedekind domain if $s \geqslant 2$. We can however specialize one by one the parameters $t_1, \dots, t_s$ so as to work at each step with the ring $A = k(t_1, \dots, t_i)[t_{i+1}]$ which is a Dedekind domain (see §2.2.4).

Let A be an integral domain with fraction field K and $F \in A[T,Y]$ be a polynomial, irreducible in $\overline{K}[T,Y]$. Up to switching Y and T, one may assume that $n = \deg_Y(F) \geqslant 1$. Assume further $n \geqslant 2$; the remaining case $n = 1$ is trivial (see Remark 2.6). Set $m = \deg_T(F)$; $m \geqslant 1$. Assume A is of characteristic 0 or $p > (2n^2 - n)m$. Paragraphs §2.2.1–2.2.3 recall from [Dèb16] the construction of the bad prime divisor and its Bertini–Noether property.

2.2.1. Preliminary reduction to a monic polynomial

First reduce to the situation where F is monic in Y by replacing

$$F(T,Y) = F_0 Y^n + F_1 Y^{n-1} + \cdots + F_n$$
$$\text{with } F_0, F_1, \ldots, F_n \in A[T],$$
$$\text{by}$$
$$Q(T,Y) = F_0^{n-1} F(T, \frac{Y}{F_0}) = Y^n + F_1 Y^{n-1} + \cdots + F_0^{n-1} F_n$$

We have $\deg_Y(Q) = n$ and $\deg_T(Q) \leqslant nm$, so $p > (2\deg_Y(Q) - 1)\deg_T(Q)$ in the case $p > 0$. Consequently the polynomial Q, as a polynomial in Y, has only simple roots in $\overline{K(T)}$ and so do the irreducible factors in $K[T]$ of its discriminant w.r.t. Y, as polynomials in T; they have only simple roots in $\overline{K}$. This is a starting hypothesis in [Dèb16].

2.2.2. Definition of the bad prime divisor

Assume from now on, in addition to $F \in A[T,Y]$, irreducible in $\overline{K}[T,Y]$, that F is monic in Y, $n = \deg_Y(F) \geqslant 2$, $m = \deg_T(F) \geqslant 1$, that the characteristic of A is 0 or $p > (2n-1)m$ and that A is integrally closed.

Denote the *discriminant* of F relative to Y by

$$\Delta_F = \mathrm{disc}_Y(F)$$

We have $\Delta_F \in A[T]$ and $\Delta_F \neq 0$. Consider the *reduced discriminant*:

$$\Delta_F^{\mathrm{red}} = (\Delta_{F,0})^{\rho} \prod_{i=1}^{\rho} (T - \tau_i)$$

where $\Delta_{F,0}$ is the leading coefficient of Δ_F and $\tau_1, \ldots, \tau_\rho$ are the distinct roots of Δ_F in $\overline{K}$. From [Dèb16, lemma 2.1], we have $\Delta_F^{\mathrm{red}} \in A[T]$ and

$$\Delta_F^{\mathrm{red}} = \Delta_{F,0}^{\rho-1} \frac{\Delta_F}{\gcd(\Delta_F, \Delta_F')}$$

where the gcd is calculated in the ring $K[T]$ and made to be monic by multiplying by the suitable non-zero constant. Furthermore the discriminant of this reduced discriminant:

$$\mathrm{disc}(\Delta_F^{\mathrm{red}}) = (\Delta_{F,0})^{2\rho(\rho-1)} \prod_{1\leqslant i\neq j\leqslant \rho} (\tau_j - \tau_i)$$

is an element of A and is non-zero as by construction $\Delta_F^{\mathrm{red}}(T)$ has no multiple root in $\overline{K}$. Define then an element $\mathcal{B}_F$ by

$$\mathcal{B}_F = \Delta_{F,0} \cdot \mathrm{disc}(\Delta_F^{\mathrm{red}})$$

We have $\mathcal{B}_F \in A$ and $\mathcal{B}_F \neq 0$.

Definition 2.5. The maximal ideals $\mathfrak{p} \subset A$ that contain $\mathcal{B}_F$ are called the *bad primes* of $F \in A[T,Y]$ and $\mathcal{B}_F$ is called the *bad prime divisor*. Maximal ideals $\mathfrak{p} \subset A$ that are not bad are said to be *good*.

Remark 2.6. In the case $\deg_Y(P) = 1$, $\deg_T(P) \leqslant 1$, the construction leads to $\mathcal{B}_F = 1$. All maximal ideals $\mathfrak{p} \subset A$ are good and the main result, Theorem 2.7 below, trivially holds.

2.2.3. The main result

In addition to the assumptions of §2.2.2, assume that A is a Dedekind domain. Let $\mathcal{G}$ be the Galois group of the splitting field of F over $\overline{K}(T)$.

If $\mathfrak{p} \subset A$ is a prime ideal, denote the residue field $A/\mathfrak{p}$ by $\kappa_\mathfrak{p}$, the reduction map by $s_\mathfrak{p} : A \to \kappa_\mathfrak{p}$, the localized ring of A by $\mathfrak{p}$ by $A_\mathfrak{p}$ and the polynomial obtained by reducing the coefficients of P by $s_\mathfrak{p}(P)$.

Theorem 2.7 *(theorem 2.6 of [Dèb16]). Let $\mathfrak{p} \subset A$ be a good prime of F such that $|\mathcal{G}| \notin \mathfrak{p}$. Then we have these two conclusions:*

(Good Behavior) *We have $\mathcal{B}_{s_\mathfrak{p}(F)} = s_\mathfrak{p}(\mathcal{B}_F) \neq 0$.*

(Good Reduction) *The polynomial $s_\mathfrak{p}(F)$ is irreducible in $\overline{\kappa_\mathfrak{p}}[T,Y]$.*

Condition $\mathcal{B}_{s_\mathfrak{p}(F)} = s_\mathfrak{p}(\mathcal{B}_F) \neq 0$ rephrases as saying that no distinct roots τ_i and τ_j of Δ_F meet modulo $\mathfrak{p}$ and none of the roots τ_i meets ∞ modulo $\mathfrak{p}$.

2.2.4. Specializations in families of polynomials

Take $A = k[\underline{t}]$ and consider a polynomial $F \in k[\underline{t}][T,Y]$ as in §2.2.2. The bad prime divisor $\mathcal{B}_F$ is an element of $k[\underline{t}]$ and the bad primes are the s-tuples $\underline{t}^* = (t_1^*, \ldots, t_s^*)$ such that $\mathcal{B}_F(\underline{t}^*) = 0$.

Theorem 2.7 cannot be applied directly if $s \geqslant 2$ as $A = k[\underline{t}]$ is not a Dedekind domain but can be applied to F viewed in $k(t_1, \ldots, t_{s-1})[t_s][T,Y]$. It is readily checked that the bad prime divisor relative to $k(t_1, \ldots, t_{s-1})[t_s]$ is the same as relative to the smaller ring $k[t_1, \ldots, t_s]$. Hence it is the polynomial $\mathcal{B}_F$ in $k[t_1, \ldots, t_s]$ introduced above.

From the assumptions, k is of characteristic 0 or $p > (2n-1)m \geqslant n$. Therefore, as $|\mathcal{G}|$ divides $n!$, p cannot divide $|\mathcal{G}|$ and $|\mathcal{G}|$ is in no prime ideal $\mathfrak{p}$ of $k[\underline{t}]$. Let $t_s^* \in k$ such

that $\mathcal{B}_F(t_1,\dots,t_{s-1},t_s^*) \neq 0$. From Theorem 2.7, $F(t_1,\dots,t_{s-1},t_s^*,T,Y)$ is irreducible in $\overline{k(t_1,\dots,t_{s-1})}[T,Y]$ and its bad prime divisor is $\mathcal{B}_F(t_1,\dots,t_{s-1},t_s^*) \in k[t_1,\dots,t_{s-1}]$. Theorem 2.7 can then be applied to $F(t_1,\dots,t_{s-1},t_s^*,T,Y)$ to specialize t_{s-1}. An inductive argument finally leads to this conclusion:

Corollary 2.8. *If $(t_1^*,\dots,t_s^*) \in k^s$ satisfies $\mathcal{B}_F(t_1^*,\dots,t_s^*) \neq 0$, then the polynomial $F(t_1^*,\dots,t_s^*,T,Y) \in k[T,Y]$ is irreducible in $k[T,Y]$.*

2.2.5. Reduction modulo p

The unifying context "$F \in A[T,Y]$ with A a Dedekind domain" also allows the special case $F \in \mathbb{Z}[T,Y]$ and the prime $\mathfrak{p}$ is a prime number p. In this situation the bad prime divisor $\mathcal{B}_F$ is a non-zero integer, the bad primes are the prime numbers dividing $\mathcal{B}_F$ and Theorem 2.7 yields this effective version of Ostrowski's theorem:

Corollary 2.9. *If p is a prime number not dividing $\mathcal{B}_F$ nor $|\mathcal{G}|$, then the reduced polynomial $\overline{F}$ is irreducible in $\overline{\mathbb{F}_p}[T,Y]$.*

2.2.6. Explicitness of $\mathcal{B}_F$

In the two typical situations $A = k[\underline{t}]$ and $A = \mathbb{Z}$, one can explicitly bound the bad prime divisor $\mathcal{B}_F$. However as already alluded to in §1.1.3, the bounds are big and do not improve on previously known ones. On the other hand, one can compute the exact value of $\mathcal{B}_F$ for specific polynomials *via* a simple computer program, which may be more precise in some cases.

For example, many bounds have been given in the situation $A = \mathbb{Z}$ over the years (Schmidt [Sch76], Kaltofen [Kal95], Ruppert [Rup86,Rup99], Zannier [Zan97], Gao–Rodrigues [GR03]), the best one being the last one by Gao–Rodrigues who proved that an absolutely irreducible polynomial $F(T,Y) = \sum_{i,i} a_{ij}T^iY^j \in \mathbb{Z}[T,Y]$ remains irreducible modulo every prime

$$p > (\sqrt{m^2+n^2}\ ||F||_2)^{2\tau-3}$$

where $m = \deg_T(F)$, $n = \deg_Y(F)$, $||F||_2 = \sqrt{\sum_{i,j} a_{ij}^2}$ and τ is the number of integral points inside the Newton polygon of F [GR03, theorem 1].

For $F(T,Y) = Y^3 - 6T^2 + TY - 2$, Gao–Rodrigues concludes to irreducibility modulo every prime $p > 13^{11/2} \cdot 42^{11/2}$. On the other hand, we obtain $\mathcal{B}_F = 2^{16} \cdot 3^{19} \cdot 431 \cdot 433$, which is bigger but only the prime divisors of $\mathcal{B}_F$ should be tested. It can be checked that F is irreducible modulo 5 for example (though 5 is smaller than the Gao–Rodrigues bound), that F is reducible modulo the prime 2, which divides $\mathcal{B}_F$, and is irreducible modulo 3 although 3 divides $\mathcal{B}_F$; the bad prime divisor is not optimal.

Similar comments apply to the situation $A = k[\underline{t}]$. We refer to [Dèb16, §4.2] for the estimate $\deg_{t_i}(\mathcal{B}_F) \leqslant 16d^5 \deg_{t_i}(F)$ given in §1.1.3. For $F(t,T,Y) = T^2Y + 2TY^2 + Y^3 +$

$3T+3Y+t$ (in case $A=\mathbb{Q}[t]$), one obtains $\mathcal{B}_F = t^2\cdot(t-1)^3\cdot(t+1)^3$. It can be checked that $F(2,T,Y)$ is irreducible, $F(0,T,Y)$ is reducible and $F(1,T,Y)$ is irreducible.

We mention a construction of Busé–Chèze for polynomials $F=P(T,Y)-tQ(T,Y)\in k[t,T,Y]$ [BC11, theorems 8 and 10]: building on a method of Ruppert, they produce a matrix with entries in $k[t]$ with the property that the points $t^*\in k$ where the rank drops are exactly those for which $P(T,Y)-t^*Q(T,Y)$ is reducible. They deduce a polynomial $B(t)$ which plays the role of our polynomial $\mathcal{B}_F$. For our example above, they obtain $B(t)=t^3$ whose root 0 is indeed the unique spectral value of F. Their method extends to more general situations which include our example above in situation $A=\mathbb{Z}$ for which they obtain $B=6$.

2.3. Conjoining §2.1 and §2.2

In our original situation, we have a polynomial $F\in k[\underline{t},\underline{x}]$ assumed to be irreducible in $\overline{k(\underline{t})}[\underline{x}]$. Assume further that k is of characteristic 0 or $p>2\deg(F)^3$.

Corollary 2.10. *There is a non-zero polynomial $\widetilde{\mathcal{B}}_F(\underline{t},\underline{x})\in k[\underline{t},\underline{x}]$, explicitly constructed in the proof, with the following property. For every $\underline{t}^*\in k^s$ such that $\widetilde{\mathcal{B}}_F(\underline{t}^*,\underline{x})\neq 0$ (in $k[\underline{x}]$), the polynomial $F(\underline{t}^*,\underline{x})$ is irreducible in $k[\underline{x}]$.*

Proof. The number of indeterminates $x_1,\dots,x_\ell$ being $\ell\geqslant 2$, we may assume $\deg_{x_j}(F)\geqslant 1$ for $j=\ell-1,\ell$. Set $T=x_{\ell-1}$, $Y=x_\ell$, $A=k[\underline{t},x_1,\dots,x_{\ell-2}]$ and $K=\mathrm{Frac}(A)$. From Theorem 2.1, there is a matrix $B\in\mathrm{GL}_\ell(k)$ such that the polynomial

$$F(\underline{t},B\cdot\underline{x})$$

is in $A[T,Y]$ and is irreducible in $\overline{K}[T,Y]$. The assumption on the characteristic of k guarantees that the one made on the characteristic of A in §2.2 is satisfied. Apply §2.2.1 to make F monic in Y. Denote then its bad prime divisor by $\widetilde{\mathcal{B}}_F$; it is a non-zero element of $k[\underline{t},x_1,\dots,x_{\ell-2}]\subset k[\underline{t},\underline{x}]$.

Let $\underline{t}^*\in k^s$ such that $\widetilde{\mathcal{B}}_F(\underline{t}^*,\underline{x})\neq 0$ (in $k[\underline{x}]$). The set of $(\ell-2)$-tuples $(x_1^*,\dots,x_{\ell-2}^*)\in k^{\ell-2}$ such that $\widetilde{\mathcal{B}}_F(\underline{t}^*,x_1^*,\dots,x_{\ell-2}^*)=0$ is a proper Zariski closed subset $\mathcal{Z}\subset k^{\ell-2}$. From Corollary 2.8, for every $(x_1^*,\dots,x_{\ell-2}^*)\in k^{\ell-2}\setminus\mathcal{Z}$, the polynomial obtained from $F(\underline{t},B\cdot\underline{x})$ by specializing $\underline{t}$ to $\underline{t}^*$ and x_k to x_k^* for $k=1,\dots,\ell-2$, is irreducible in $k[T,Y]$. *A fortiori* the polynomial obtained by only specializing $\underline{t}$ to $\underline{t}^*$ is irreducible in $k[\underline{x}]$. This polynomial is $F(\underline{t}^*,B\cdot\underline{x})$. The result follows as the matrix B is invertible. □

Thanks to the generality of Theorem 2.1, Corollary 2.10 extends to the situation of several polynomials $F_1,\dots,F_h$: $\widetilde{\mathcal{B}}_F$ should be replaced by the product $\widetilde{\mathcal{B}}_{F_1}\cdots\widetilde{\mathcal{B}}_{F_h}$ for some matrix B working for all $F_1,\dots,F_h$; the two indeterminates x_i which play the role of T and Y may however differ.

3. Combinatorial approach to irreducibility criteria

The central aim of this section is to provide some generic irreducibility criteria; it elaborates on §1.2.3. §3.1 first reviews the approach based on the Bertini–Krull theorem. §3.2 is devoted to applications of the more recent Gao criteria for non-summability of polyhedrons.

In this section we assume that F is of the form

$$F(\underline{t},\underline{x}) = P(\underline{x}) - t_1 Q_1(\underline{x}) - \cdots - t_s Q_s(\underline{x})$$

that is, is a linear deformation of the polynomial $P \in k[\underline{x}]$ by the polynomials $Q_1,\ldots,Q_s \in k[\underline{x}]$.

3.1. The Bertini–Krull approach

The Bertini–Krull theorem is a very explicit *iff* criterion for a polynomial $F(\underline{t},\underline{x})$ as above to be generically irreducible. We refer to [Sch00, theorem 37] for the precise statement. We recall below two applications (§3.1.1 and §3.1.2).

3.1.1. Pencil of two polynomials

Assume further that $s = 1$, that is:

$$F(t,\underline{x}) = P(\underline{x}) - tQ(\underline{x})$$

with $\max(\deg(P),\deg(Q)) \geqslant 1$. The Bertini–Krull theorem relates the generic irreducibility of F to the indecomposability of the rational function P/Q. Recall that P/Q is said to be *decomposable* in $k(\underline{x})$ if there exist $A,B \in k[\underline{x}]$, $B \neq 0$ and $h,g \in k[u]$ with $g \neq 0$ and $\max(\deg g,\deg h) \geqslant 2$ such that

$$\frac{P}{Q} = \frac{h}{g}\left(\frac{A}{B}\right).$$[1]

Then we have

(1) *$F(t,\underline{x}) = P(\underline{x}) - tQ(\underline{x})$ is generically irreducible if and only if P/Q is indecomposable.*

In the special "polynomial situation", *i.e.* $Q = 1$, the condition "P indecomposable in $k(\underline{x})$" is equivalent to "P indecomposable in $k[\underline{x}]$", *i.e.* P does not write $P(\underline{x}) = h(A(\underline{x}))$ with $A \in k[\underline{x}]$ and $h \in k[u]$ with $\deg h \geqslant 2$. This follows from results due to Gordan and Noether in characteristic 0 and Igusa and Schinzel in general [Sch00, theorems 3 and 4].

[1] There is also a notion of decomposability for rational functions in one indeterminate. Definitions, problems, tools and techniques are however different although there is a Hilbert like specialization theorem proved in [BCD12] which provides a bridge between indecomposable polynomials in several indeterminates and those in one indeterminate.

Many articles have been devoted to the spectrum $\mathrm{sp}(P - tQ)$ in the indecomposable situation. We briefly recall the main questions and results in the next paragraphs.

On the cardinality The general Bertini–Noether bound (6) from §1 gives this inequality, when k is of characteristic 0 or $p > d(d-1)$:

(2) $\quad \mathrm{card}(\mathrm{sp}(P - tQ)) \leqslant d^2 - 1 \quad$ with $d = \max(\deg P, \deg Q)$.

We refer to [Bod08] for more details on this bound in the missing cases.

Ruppert shows further in [Rup86] that the Hesse cubic pencil

$$P(x,y) - tQ(x,y) = x^3 + y^3 + (1+x+y)^3 - 3t\ xy(1+x+y)$$

reaches the maximal possible value for $d = 3$ if spectral values are counted with multiplicity. That is, the following is checked: $\mathrm{sp}(P - tQ) = \{1, j, j^2, \infty\}$ (where $1, j, j^2$ are the cubic roots of 1)[2]; for each $t^* \in \mathrm{sp}(P - tQ)$, the curve $P(x,y) - t^*Q(x,y) = 0$ breaks into 3 lines; if the multiplicity $2 = 3 - 1$ is affected to each of the elements of $\mathrm{sp}(P - t^*Q)$, then $4 \times 2 = 8 = d^2 - 1$. Furthermore Nguyen asserts [Ngu11] that if the spectrum is counted with multiplicities as above, the Hesse cubic pencil is the only example that reaches the extremal value $d^2 - 1$ (for any $d \geqslant 3$).

Another interesting statement from [Ngu11] is that when $k = \mathbb{C}$, if $P(x,y) = 0$ and $Q(x,y) = 0$ are smooth plane curves, then

$$\mathrm{card}(\mathrm{sp}(P - tQ)) \leqslant 3d - 3$$

Furthermore, if $F = x(y^{d-1} - 1) + \lambda(x^{d-1} - 1) + \mu(x^{d-1} - y^{d-1})$ (with $d \geqslant 3$) is viewed as a polynomial in x, y, parametrized by (λ, μ) in the plane k^2, and $P - tQ$ is obtained by restricting (λ, μ) in some t-line, then, generically, the pencil $P - tQ$ realizes the bound $3d - 3$.

A major result about this issue remains *Stein's theorem* for polynomials:

(3) *If* $P \in k[\underline{x}]$ *is indecomposable, then* $\mathrm{card}(\mathrm{sp}(P - t)) < \deg(P)$.

This was first established by Stein [Ste89] in two variables and in characteristic 0, then extended to all characteristics by Lorenzini [Lor93] and finally generalized to more variables by Najib [Naj05].

On the spectrum itself It can be shown that generically a polynomial $P(\underline{x})$ is indecomposable and for $\deg(P) > 2$ or $\ell > 2$, the spectrum $\mathrm{sp}(P - t)$ is empty [BDN09a, proposition 2.2]. The question arises then as to whether other finite sets occur as spectra (within Stein's limitations). Najib [Naj04] answers positively to this question. He shows that

[2] The value ∞ can be moved to a finite point by a change of coordinates.

(4) *for any finite subset* $\mathcal{S} \subset k$*, there exists an indecomposable polynomial* $P \in k[\underline{x}]$ *such that* $\mathrm{sp}(P(\underline{x}) - t) = \mathcal{S}$.

He can further fix in advance all but one of the irreducible factors of the polynomials $P(\underline{x}) - t^*$ with $t^* \in \mathcal{S}$ and arrange for Stein's inequality to be an equality for P. For example, for every degree $d \geqslant 2$ and given $d-1$ points $t_1^*, \dots, t_{d-1}^* \in k$, he can construct an indecomposable polynomial $P(x, y)$ of degree d such that $P(x, y) - t_i^*$ is divisible by $x - t_i^*$, $i = 1, \dots, d-1$. Due to Stein's inequality, this already implies that $\mathcal{S}$ exactly equals $\{t_1^*, \dots, t_{d-1}^*\}$. Such a polynomial $P(x, y)$ can be made explicit: take

$$P(x, y) = y(x - t_1^*)(x - t_2^*) \dots (x - t_{d-1}^*) + x.$$

Furthermore some converse is stated in [Ngu11]: a degree d polynomial in two variables with a spectrum of cardinality $d-1$ is, up to some change of variables, the polynomial P above.

We end this discussion with open questions.

Problem. Given an integer $d \geqslant 1$ and a degree d polynomial $Q \in k[\underline{x}]$,

(a) find a polynomial $P \in k[\underline{x}]$ of degree $\leqslant d$ such that P/Q is indecomposable and for which the Bertini–Noether inequality (2) from §3.1.1 is an equality;

(b) given a finite subset $\mathcal{S} \subset k$ of cardinality $\leqslant d^2 - 1$, find a polynomial $P \in k[\underline{x}]$ such that $\deg(P) \leqslant d$, P/Q indecomposable and $\mathrm{sp}(P(\underline{x}) - tQ(\underline{x})) = \mathcal{S}$.

For (b), the method from [Naj04] generalizes to construct a polynomial P such that $\deg(P) \leqslant d$, P/Q indecomposable and $\mathrm{sp}(P(\underline{x}) - tQ(\underline{x}))$ contains any prescribed subset $\mathcal{S}$ of $d-1$ elements. However the Bertini–Noether bound (2) for rational functions is not sharp enough (as is the Stein bound (3) for polynomials) to conclude that the containment is an equality.

3.1.2. Deformation by monomials

Consider the general case

$$F(\underline{t}, \underline{x}) = P(\underline{x}) - t_1 Q_1(\underline{x}) - \dots - t_s Q_s(\underline{x})$$

of a deformation by s polynomials but assume that $Q_1, \dots, Q_s$ are monomials. [BDN09b] shows how to handle this situation with the Bertini–Krull theorem. The following statements are two selected generic irreducibility criteria from [BDN09b], which can be compared to the results of next subsection given by the more combinatorial approach.

Theorem 3.1. *Let* $F(t, \underline{x}) = P(\underline{x}) - tQ(\underline{x})$ *with* $P \in k[\underline{x}]$ *of degree* $d \geqslant 1$. *Assume that*

(a) Q *is a monomial of degree* $\leqslant d$ *and is relatively prime to* P,

(b) $\Gamma(P) \cup \Gamma(Q)$ *is not contained in a line,*

(c) Q *is not a pure power (if* $Q(\underline{x}) = a x_1^{k_1} \cdots x_\ell^{k_\ell}$ *then* $\gcd(k_1, \dots, k_\ell) = 1$).

Then $F(t, \underline{x})$ *is generically irreducible.*

For example if $P \notin k[x_1]$ and is not divisible by x_1, then $P(\underline{x}) - tx_1$ is generically irreducible.

Theorem 3.2. *Let $P \in k[\underline{x}]$ be a polynomial of degree $d \geqslant 1$ and $Q_1, \ldots, Q_s$ be monomials of degree $\leqslant d$. Assume further that*

(a) *$s \geqslant 2$ and $P, Q_1, \ldots, Q_s$ are relatively prime,*

(b) *$\Gamma(P) \cup \Gamma(Q_1) \cup \ldots \cup \Gamma(Q_s)$ is not contained in a line,*

(c) *if $\mathrm{char}(k) = p > 0$, at least one of $P, Q_1, \ldots, Q_s$ is not a p-th power.*

Then $P(\underline{x}) - t_1 Q_1(\underline{x}) - \cdots - t_s Q_s(\underline{x})$ is generically irreducible.

For example, in characteristic 0, for each $k \in \{1, \ldots, d\}$, the polynomial $P(x_1, \ldots, x_\ell) + t_1 x_1^k + \cdots + t_\ell x_\ell^k$ is generically irreducible.

3.2. Applications of Gao's criteria

The situation is that of polynomials

$$F(t, \underline{x}) = P(\underline{x}) - tQ(\underline{x}) \text{ with } P, Q \in k[\underline{x}].$$

3.2.1. Gao's first criterion

Gao gives this *iff* condition for a polyhedron to be non-summable [Gao01] (which he explains to be a generalization of the Eisenstein criterion).

Theorem 3.3 *(Gao). Let $P \in k[\underline{x}]$ such that*

(*) *$\Gamma(P)$ is contained in a hyperplane $H \subset \mathbb{R}^\ell$ not passing through the origin.*

Denote the vertices of $\Gamma(P)$ by $v_1, \ldots, v_k$. Then $\Gamma_0(P)$ is not summable if and only if the coordinates of $v_1, \ldots, v_k$ are relatively prime.

This result leads to this generic irreducibility criterion.

Corollary 3.4. *Let $P \in k[\underline{x}]$ satisfying (*) above and $Q \in k[\underline{x}]$ such that*

(a) *the coordinates of all the vertices of $\Gamma(P)$ are relatively prime,*

(b) *$Q(0, \ldots, 0) \neq 0$, $\Gamma(Q) \subset \Gamma_0(P)$ and no monomial of Q is a vertex of $\Gamma(P)$.*

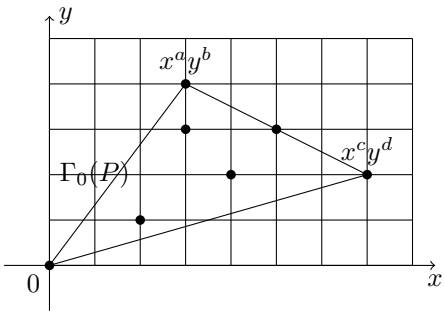
Then the polynomial $F = P - tQ$ is generically irreducible and even has this stronger property: $P - t^*Q$ is irreducible in $k[\underline{x}]$ for every $t^* \in k \setminus \{0\}$.

Proof. Assumptions (a) and (*) and Gao's Theorem 3.3 show that $\Gamma_0(P)$ is not summable. As $\Gamma(P - tQ) = \Gamma_0(P)$, Minkowski's theorem concludes that $P - tQ$ is generically irreducible and has the stronger property. □

To completely determine $\mathrm{sp}(P - tQ)$, it remains to decide whether P is irreducible or not. Both may happen: for $P(x, y) = x^p - y^q$ with $\gcd(p, q) = 1$, we have $\mathrm{sp}(P - t) = \emptyset$ while for $P(x, y) = x^p - xy^q$, $\mathrm{sp}(P - t) = \{0\}$.

The special case of Corollary 3.4 for which $Q = 1$ yields this conclusion: if P satisfies conditions (*) and (a), then $P(\underline{x}) - t$ is generically irreducible and has the stronger irreducibility property. For all positive and relatively prime integers a, b, c, d, $P(x, y) = x^a y^b + x^c y^d$ is such a polynomial.

Example 3.5. Here is one further example where a polynomial P is deformed by a polynomial Q "below" P to obtain a polynomial $P - tQ$ satisfying the strong generic irreducibility property. Let $P(x, y) = x^a y^b + x^c y^d$ with $\gcd(a, b, c, d) = 1$ and $Q(x, y) \in k[x, y]$ be such that: (i) $Q(0, 0) \neq 0$ (ii) $\Gamma(Q) \subset \Gamma_0(P)$ and (iii) the monomials $x^a y^b$, $x^c y^d$ are not in $\Gamma(Q)$. Then we have $\mathrm{sp}(P - tQ) \subset \{0\}$.



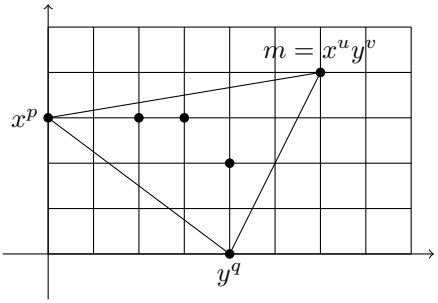
3.2.2. Gao's second criterion

The following result of [Gao01] makes it possible to construct non-summable polytopes, by induction on the dimension.

Theorem 3.6 *(Gao). Let $P \in k[\underline{x}]$ such that $\Gamma(P)$ is not summable, has at least two points, and is contained in a hyperplane H of $\mathbb{R}^\ell$. Suppose that $Q \in k[\underline{x}]$ is a polynomial such that $\Gamma(Q)$ is not included in H. Moreover suppose that there exists some monomial $m \in k[\underline{x}]$ such that $\Gamma(Q) \subset \Gamma(P + m)$. Then $\Gamma(P + Q)$ is not summable.*

With Theorem 3.6 one can deform a polynomial P not only by a polynomial Q "below" P, but also by some polynomial Q "above" P.

Example 3.7. Let $P(x, y) = x^p + y^q$ with p, q relatively prime. From Theorem 3.6 for $Q(x, y) = \sum_{\frac{i}{p} + \frac{j}{q} < 1} a_{ij} x^i y^j$ (whose monomials are below those of P) and $m = 1$, the polynomial $P(x, y) - tQ(x, y)$ has empty spectrum. Now take a polynomial Q such that for some $(u, v) \in \mathbb{N}^2$, the monomials of Q lie in the triangle $(p, 0), (0, q), (u, v)$ (and so are above those of P) and are distinct from $(p, 0)$ and $(0, q)$. From Theorem 3.6 with $m = x^u y^v$, the spectrum of $P(x, y) - tQ(x, y)$ is empty.



Similar examples can be given in higher dimension starting with $P(x_1, \dots, x_\ell) = x_1^{p_1} + \cdots + x_\ell^{p_\ell}$ with $p_1, \dots, p_\ell$ relatively prime.

Theorem 3.6 can also be used to explicitly produce a deformation of a (possibly reducible) polynomial $Q(\underline{x})$ into an irreducible one.

Example 3.8. Let $Q(x, y)$ be any polynomial and $P(x, y) = x^p + y^q$ with p, q relatively prime and $p, q > \deg Q$. Then the polynomial $(x^p + y^q) - tQ(x, y)$ has the strong generic irreducibility property, so $Q(x, y) + \mu(x^p + y^q)$ is irreducible in $k[x, y]$ for every $\mu \in k$, $\mu \neq 0$.

Acknowledgments

This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01) and by the ANR project "SUSI" (ANR-12-JS01-0002-01). The third author wishes to thank Laboratoire Painlevé of Université de Lille for its hospitality during several visits in 2014 and 2015.

References

[ASGL04] Fatima Abu Salem, Shuhong Gao, Alan G.B. Lauder, Factoring polynomials via polytopes, in: ISSAC 2004, ACM, New York, 2004, pp. 4–11.

[Bod08] Arnaud Bodin, Reducibility of rational functions in several variables, Israel J. Math. 164 (2008) 333–347.

[BCD12] Arnaud Bodin, Guillaume Chèze, Pierre Dèbes, Specializations of indecomposable polynomials, Manuscripta Math. 139 (3–4) (2012) 391–403.

[BDN09a] Arnaud Bodin, Pierre Dèbes, Salah Najib, Indecomposable polynomials and their spectrum, Acta Arith. 139 (1) (2009) 79–100.

[BDN09b] Arnaud Bodin, Pierre Dèbes, Salah Najib, Irreducibility of hypersurfaces, Comm. Algebra 37 (6) (2009) 1884–1900.

[BC11] L. Busé, G. Chèze, On the total order of reducibility of a pencil of algebraic plane curves, J. Algebra 341 (2011) 256–278.

[BCN11] Laurent Busé, Guillaume Chèze, Salah Najib, Noether forms for the study of non-composite rational functions and their spectrum, Acta Arith. 147 (3) (2011) 217–231.

[Dèb16] Pierre Dèbes, Reduction and specialization of polynomials, Acta Arith. 172 (2) (2016) 175–197.

[FJ04] Michael D. Fried, Moshe Jarden, Field Arithmetic, second edition, Ergeb. Math. Grenzgeb., vol. 11, Springer-Verlag, Berlin, 2004.

[Gao01] Shuhong Gao, Absolute irreducibility of polynomials via Newton polytopes, J. Algebra 237 (2) (2001) 501–520.
[Gao03] Shuhong Gao, Factoring multivariate polynomials via partial differential equations, Math. Comp. 72 (242) (2003) 801–822.
[GL01] S. Gao, A.G.B. Lauder, Decomposition of polytopes and polynomials, Discrete Comput. Geom. 26 (1) (2001) 89–104.
[GR03] Shuhong Gao, Virgínia M. Rodrigues, Irreducibility of polynomials modulo p via Newton polytopes, J. Number Theory 101 (1) (2003) 32–47.
[Gro71] Alexandre Grothendieck, Revêtements étales et groupe fondamental, Lecture Notes in Math., vol. 224, Springer, 1971.
[GM71] Alexandre Grothendieck, Jacob P. Murre, The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme, Lecture Notes in Math., vol. 208, Springer, 1971.
[Kal95] Erich Kaltofen, Effective Noether irreducibility forms and applications, in: 23rd Symposium on the Theory of Computing, New Orleans, LA, 1991, J. Comput. System Sci. 50 (2) (1995) 274–295.
[Lor93] Dino Lorenzini, Reducibility of polynomials in two variables, J. Algebra 156 (1) (1993) 65–75.
[Naj04] Salah Najib, Sur le spectre d'un polynôme à plusieurs variables, Acta Arith. 114 (2) (2004) 169–181.
[Naj05] Salah Najib, Une généralisation de l'inégalité de Stein–Lorenzini, J. Algebra 292 (2) (2005) 566–573.
[Ngu11] Viet Kh. Nguyen, On certain extremal pencils of curves with respect to the total reducibility order, Proc. Japan Acad. Ser. A Math. Sci. 87 (2011) 194–198.
[Rup86] Wolfgang Ruppert, Reduzibilität ebener Kurven, J. Reine Angew. Math. 369 (1986) 167–191.
[Rup99] Wolfgang M. Ruppert, Reducibility of polynomials $f(x, y)$ modulo p, J. Number Theory 77 (1) (1999) 62–70.
[Sch00] A. Schinzel, Polynomials with Special Regard to Reducibility, Encyclopedia Math. Appl., vol. 77, Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.
[Sch76] Wolfgang M. Schmidt, Equations over Finite Fields. An Elementary Approach, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin–New York, 1976.
[Ste89] Yosef Stein, The total reducibility order of a polynomial in two variables, Israel J. Math. 68 (1) (1989) 109–122.
[Zan97] U. Zannier, On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$, Arch. Math. 68 (1997) 129–138.