# SPECIALIZATIONS OF INDECOMPOSABLE POLYNOMIALS

ARNAUD BODIN, GUILLAUME CHÈZE, AND PIERRE DÈBES

Abstract. We address some questions concerning indecomposable polynomials and their behaviour under specialization. For instance we give a bound on a prime $p$ for the reduction modulo $p$ of an indecomposable polynomial $P(x) \in \mathbb{Z}[x]$ to remain indecomposable. We also obtain a Hilbert like result for indecomposability: if $f(t_1, \ldots, t_r, x)$ is an indecomposable polynomial in several variables with coefficients in a field of characteristic $p = 0$ or $p > \deg(f)$, then the one variable specialized polynomial $f(t_1^* + \alpha_1^* x, \ldots, t_r^* + \alpha_r^* x, x)$ is indecomposable for all $(t_1^*, \ldots, t_r^*, \alpha_1^*, \ldots, \alpha_r^*) \in \overline{k}^{2r}$ outside a proper Zariski closed subset.

## 1. Introduction

Let $x$ be an indeterminate. A non-constant polynomial $f(x) \in k[x]$ with coefficients in a field $k$ is said to be *decomposable* in $k[x]$ if it is of the form $u(g(x))$ with $g$ <u>and</u> $u$ in $k[x]$ of degree $\geqslant 2$, and *indecomposable* otherwise. For polynomials in several variables, the definition is slightly different: for an integer $n \geqslant 2$ and a $n$-tuple $\underline{x} = (x_1, \ldots, x_n)$ of indeterminates, a non-constant polynomial $f(\underline{x}) \in k[\underline{x}]$ is *decomposable* in $k[\underline{x}]$ if it is of the form $u(g(\underline{x}))$ with $u \in k[t]$ of degree $\geqslant 2$ and $g(\underline{x}) \in k[\underline{x}]$; unlike for $n = 1$, the case $\deg(g) = 1$, $\deg(u) \geqslant 2$ is allowed.

The central theme of the paper is the following general problem. Let $A$ be an integral domain with quotient field $K$ and $f(x) \in A[x]$ be an indecomposable polynomial in $K[x]$. Given a ring morphism $\sigma : A \to k$ with $k$ a field, the question is whether the polynomial $f^\sigma(x)$ obtained by applying $\sigma$ to the coefficients of $f(x)$ is also indecomposable.

We first have the following general conclusion *à la Bertini-Noether*, under the assumption that $\deg(f)$ is prime to the characteristic of $K$[1]: the answer to the question is positive "generically", that is, for all $\sigma$ such that $I_f^\sigma \neq 0$ where $I_f$ is some non-zero element of $A$ depending only on $f$ (proposition 2.3). Based on a general decomposition result for polynomials, established

*Date*: August 31, 2011.
2000 *Mathematics Subject Classification.* 12E05, 11C08.
*Key words and phrases.* Irreducible and indecomposable polynomials.

[1] *i.e.* char$(K)$ equals 0 or does not divide $\deg(f)$.

in [2], our approach leads to quite explicit versions of the Bertini-Noether conclusion. For polynomials in several variables, similar conclusions had already been proved (see [3], [4], [5]); the single variable case is somewhat different.

We investigate further two typical situations. The first one is for $A = \mathbb{Z}$ and $\sigma : \mathbb{Z} \to \mathbb{F}_p$ a reduction morphism modulo $p$. The Bertini-Noether conclusion is here that $f^\sigma(x)$ is indecomposable if $p$ is suitably large. Our method leads to the following explicit version. To our knowledge no such bound as the one below was previously available.

**Theorem 1.1.** *Let $f(x) \in \mathbb{Z}[x]$ be indecomposable in $\mathbb{Q}[x]$. There exists a constant $\gamma_d$ depending only on $d = \deg(f)$ such that if $p > \gamma_d \, \|f\|_\infty^d$ is a prime, the reduced polynomial $\overline{f}(x)$ modulo $p$ is indecomposable in $\overline{\mathbb{F}}_p[x]$.*

We then focus on the situation where $A = k[\underline{t}]$ with $\underline{t} = (t_1, \dots, t_r)$ an $r$-tuple of indeterminates ($r \geqslant 1$), $k$ a field and $\sigma : k[\underline{t}] \to \overline{k}$ a specialization morphism sending each $t_i$ to a special value $t_i^* \in \overline{k}$, $i = 1, \dots, r$. In this situation, the Bertini-Noether conclusion is that if $f(\underline{t}, x) \in k[\underline{t}, x]$ is indecomposable in $k(\underline{t})[x]$ and of degree prime to the characteristic of $k$, then for all $\underline{t}^* = (t_1^*, \dots, t_r^*) \in k^r$ but in a proper Zariski closed subset, the specialized polynomial $f(t_1^*, \dots, t_r^*, x)$ is indecomposable in $k[x]$.

The indecomposability assumption excludes polynomials $f$ of the form $u(\underline{t}, g(\underline{t}, x))$ with $u, g \in k[\underline{t}, x]$. It is natural to ask whether the Bertini-Noether conclusion extends to such polynomials and more generally to all polynomials that are indecomposable in $k[\underline{t}, x]$ (as $(r+1)$-variable polynomials). Although this is not true in general (take for example $f(t, x) = tx^4$), we show nevertheless that the desired conclusion does hold up to some change of variables. Specifically we obtain the following result.

**Theorem 1.2.** *Let $f(\underline{t}, x)$ be indecomposable in $k[\underline{t}, x]$. Assume that $k$ is of characteristic $p = 0$ or $p > \deg(f)$. Then we have the following:*

(a) *if $\underline{\alpha} = (\alpha_1, \dots, \alpha_r)$ is an $r$-tuple of indeterminates, the polynomial $f(t_1 + \alpha_1 x, \dots, t_r + \alpha_r x, x)$ is indecomposable in $\overline{k(\underline{\alpha}, \underline{t})}[x]$;*

(b) *for all $(\alpha_1^*, \dots, \alpha_r^*) \in \overline{k}^r$ off a proper Zariski closed subset, the polynomial $f(t_1 + \alpha_1^* x, \dots, t_r + \alpha_r^* x, x)$ is indecomposable in $\overline{k(\underline{t})}[x]$;*

(c) *for all $(\alpha_1^*, \dots, \alpha_r^*, t_1^*, \dots, t_r^*) \in \overline{k}^{2r}$ off a proper Zariski closed subset, the polynomial $f(t_1^* + \alpha_1^* x, \dots, t_r^* + \alpha_r^* x, x)$ is indecomposable in $\overline{k}[x]$.*

Combined with the standard fact that $f(\underline{t}, x)$ is indecomposable in $\overline{k}[\underline{t}, x]$ if it is irreducible in $\overline{k}[\underline{t}, x]$, theorem 1.2 has the following consequence which makes it easy to produce indecomposable polynomials in one variable.

**Corollary 1.3.** *Let $f(\underline{t}, x)$ be irreducible in $\overline{k}[\underline{t}, x]$. Assume that $k$ is of characteristic $p = 0$ or $p > \deg(f)$. Then for all $(\alpha_1^*, \ldots, \alpha_r^*, t_1^*, \ldots, t_r^*) \in \overline{k}^{2r}$ off a proper Zariski closed subset, the polynomial $f(t_1^* + \alpha_1^* x, \ldots, t_r^* + \alpha_r^* x, x)$ is indecomposable in $\overline{k}[x]$.*

The assumption on the characteristic of $k$ in theorem 1.2 guarantees that $f(\underline{t}, x)$ is indecomposable in $\overline{k}[\underline{t}, x]$ under the condition that it is indecomposable in $k[\underline{t}, x]$. This follows from [3, theorem 4.2]. A similar result holds for polynomials in one variable [7, lemma 21.8.11]. We will use these results in several occasions. We will further show that this assumption on the characteristic of $k$ cannot be removed in theorem 1.2 (see remark 4.3).

Theorem 1.2 and corollary 1.3 can be made more explicit: for two variables polynomials ($r = 1$), the exceptional Zariski closed subset has a degree bounded by $\deg(f)^3 + 2\deg(f)^2$, see corollary 4.8.

A main step in theorem 1.2 is to go from two to one variable (that is, the case $r = 1$). A key ingredient is a partial differential equation satisfied by the roots of a polynomial equation (Burger's equation lemma 4.4) due to Wood [14] and investigated further by Lecerf and Galligo [8].

**Acknowledgments.** The second author thanks G. Lecerf and A. Galligo for interesting discussions about Burger's equation.

## 2. Preliminaries and first results

2.1. **Decomposition of polynomials.** A useful tool is the following decomposition result for polynomials in one variable, established in [2].

Let $A$ be an integral domain, $f \in A[x]$ be a monic polynomial of degree $d$ and $m \geqslant 2$ be a divisor of $d$ that is invertible in $A$. Then there exists a unique triple $(u, g, h)$ of polynomials in $A[x]$ such that

$$f(x) = u(g(x)) + h(x) \qquad (m\text{–dec})$$

with the conditions that

(i) $u$ and $g$ are monic,

(ii) $\deg(u) = m$, the coefficient of $x^{m-1}$ in $u$ is 0 and $\deg(h) < d - \dfrac{d}{m}$,

(iii) $h(x) = \sum_i h_i x^i$ with $(\deg(g) \mid i \Rightarrow h_i = 0)$.

In particular, if $A$ is a field and $1 < m < d$, $f(x)$ is $m$-decomposable in $A[x]$ (*i.e.* decomposable with the polynomial $u$ from the definition of degree $m$) if and only if $h(x) = 0$ in the above $m$-decomposition.

*Remark* 2.1. Using this decomposition, one easily deduces the following statement which can be compared to theorem 2 of [1]:

*Let $f(t_1, \dots, t_r, x) \in k[t_1, \dots, t_r][x]$ be a monic polynomial with $\deg(f) = d$ prime to the characteristic of $k$ and $m$ be a divisor of $d$ with $1 < m < d$. If $f$ is $m$-decomposable in $k[t_1, \dots, t_r][x]$ then for all $f'(t_1, \dots, t_r) \in k[t_1, \dots, t_r] \setminus k$, $f + f'$ is $m$-indecomposable in $k[t_1, \dots, t_r][x]$.*

Indeed assume $f = u(g)$ with $u \in k[x]$ of degree $m$ and $g \in k[t_1, \dots, t_r][x]$. Deduce that the $m$-decomposition (with $A = k[t_1, \dots, t_r]$) of $f+f'$ is $f+f' = u'(g)$ with $u'(x) = u(x)+f'$ (and no remainder). As $u' \notin k[x]$, conclude with proposition 7 from [2] that $f + f'$ is not $m$-decomposable in $k[t_1, \dots, t_r][x]$.

Next we recall from [2] this more technical information on the decomposition ($m$-dec) that we will use later: the polynomial $g(x)$ is the *approximate $m$-root* of $f(x)$. More specifically if $f(x) = x^d + a_1 x^{d-1} + \cdots + a_d$ and $g(x) = x^{\frac{d}{m}} + b_1 x^{\frac{d}{m}-1} + \cdots + b_{\frac{d}{m}}$, we have

$$(\mathcal{S}) \qquad \begin{cases} a_1 = mb_1 \\ a_2 = mb_2 + \binom{m}{2} b_1^2 \\ \vdots \\ a_i = mb_i + \displaystyle\sum_{\substack{j_1+2j_2+\cdots+(i-1)j_{i-1}=i \\ j_1+j_2+\cdots+j_{i-1} \leqslant m}} c_{j_1\cdots j_{i-1}} b_1^{j_1} \cdots b_{i-1}^{j_{i-1}}, \qquad 1 \leqslant i \leqslant \frac{d}{m} \end{cases}$$

where the coefficients $c_{j_1\cdots j_{i-1}}$ are the multinomial coefficients defined by the following formula:

$$c_{j_1\cdots j_{i-1}} = \binom{m}{j_1, \dots, j_{i-1}} = \frac{m!}{j_1! \cdots j_{i-1}!(m - j_1 - \cdots - j_{i-1})!}.$$

Once $g$ has been obtained we get the full decomposition as follows: first compute $f^{(1)} = f - g^m$ and set $u^{(1)} = x^d$, $h^{(1)} = 0$. If for the highest monomial $\alpha x^i$ of $f^{(1)}$, $i$ is divisible by $\frac{d}{m}$ then set $f^{(2)} = f^{(1)} - \alpha g^{i\frac{m}{d}}$, $u^{(2)} = u^{(1)} + \alpha x^{i\frac{m}{d}}$ and $h^{(2)} = h^{(1)}$ ; if $i$ is not divisible by $\frac{d}{m}$ then set $f^{(2)} = f^{(1)} - \alpha x^i$, $u^{(2)} = u^{(1)}$ and $h^{(2)} = h^{(1)} + \alpha x^i$. Then iterate the process with $f^{(1)}$ replaced by $f^{(2)}$.

2.2. **Further degree estimates for polynomials in two variables.** Let $A$ be an integral domain and $f(t, x) \in A[t, x]$ of degree $d$, monic in $x$:

$$f(t, x) = x^d + a_1(t)x^{d-1} + \cdots + a_d(t)$$

with $\deg a_i(t) \leqslant i$, $1 \leqslant i \leqslant d$.

Let $m|d$ and write the decomposition $f = u(g) + h$ associated to $m$, where $f$ is viewed as a one variable polynomial in $x$ over $A[t]$. We have

$$g(t,x) = x^{\frac{d}{m}} + b_1(t)x^{\frac{d}{m}-1} + \cdots + b_{\frac{d}{m}}(t) \in A[t,x],$$
$$h(t,x) = \sum h_i(t)x^i,$$

and

$$u(t,x) = x^m + u_2(t)x^{m-2} + \cdots + u_m(t) \in A[t,x].$$

**Lemma 2.2.** *Under the assumptions and notation above, we have*

(1) $\deg_x g = \frac{d}{m}, \deg_x u = m, \deg_x h < d - \frac{d}{m}$;
(2) $\deg_t g \leqslant \frac{d}{m}, \deg_t u \leqslant d, \deg_t h \leqslant d$;
(3) $\deg g = \frac{d}{m}, \deg u \leqslant d, \deg h \leqslant d$.

*Proof.* The first item follows from the definition of the approximate $m$-root and the existence of such a decomposition. We prove below a refinement of the second point.

Fix some index $i$ with $1 \leqslant i \leqslant d/m$. First we have $\deg b_i(t) \leqslant i$: indeed from system $(\mathcal{S})$ we have $\deg b_1(t) = \deg a_1(t) \leqslant 1$. Furthermore, $mb_i(t)$ is a $\mathbb{Z}$-linear combination of $a_i(t)$ (which satisfies $\deg a_i(t) \leqslant i$) and of terms $b_1^{j_1} \cdots b_{i-1}^{j_{i-1}}$ with $j_1 + 2j_2 + \cdots + (i-1)j_{i-1} = i$. By induction we obtain $\deg b_i(t) \leqslant i$. This yields $\deg_t g \leqslant \frac{d}{m}$ and $\deg_t g^j \leqslant j\frac{d}{m}$.

If $\frac{d}{m}$ does not divide $i$, the coefficient $h_i(t)$ of $h(t,x) = \sum_{i=1}^{d} h_i(t)x^{d-i}$ is the coefficient of the highest monomial $\alpha_i(t)x^{d-i}$ in the difference between $f$ and powers of $g$.

If $\frac{d}{m}$ divides $i$, let $j$ such that $i = j\frac{d}{m}$ and denote the former coefficient by $u_j(t)$ (it is the coefficient of $x^{m-j}$ in $u$). Then $\deg u_j(t) = \deg \alpha_i(t) \leqslant j\frac{d}{m} \leqslant d$ $(j = 2, \dots, m)$. This implies that $\deg_t u_j(t)g^{m-j} \leqslant d$.

Conjoining the two cases, conclude that $\deg_t h \leqslant d$.

This gives the second item and $\deg g = \frac{d}{m}$, $\deg h \leqslant d$. As $u$ is the sum of terms $u_j(t)x^{m-j}$ with $\deg u_j(t) \leqslant j\frac{d}{m}$, we have $\deg u \leqslant \max_{j=2,\dots,m}\big(j\frac{d}{m} + (m-j)\big) \leqslant d$. □

2.3. **The Bertini-Noether conclusion.** If $\sigma : A \to B$ is a ring morphism, we denote the image of elements $a \in A$ by $a^\sigma$. For $p(\underline{x}) \in A[\underline{x}]$, we denote the polynomial obtained by applying $\sigma$ to the coefficients of $p$ by $p^\sigma(\underline{x})$.

Proposition 2.3 below is the analog for indecomposable polynomials of the classical Bertini-Noether theorem for absolutely irreducible polynomials [7, proposition 9.4.3].

2.3.1. *General statement.* Fix an integral domain $A$ with quotient field $K$.

**Proposition 2.3.** *Let $f(x) \in A[x]$ be indecomposable in $K[x]$ of degree $d$ prime to the characteristic $p \geqslant 0$ of $K$. Then there exists a non-zero element $I_f \in A$ such that the following holds. For every morphism $\sigma : A \to k$ in a field $k$, if $I_f^\sigma \neq 0$, then $f^\sigma(x)$ is indecomposable in $\overline{k}[x]$.*

*Proof.* Let $a_0$ be the coefficient of $x^d$ in $f(x)$, $\gamma = da_0$ and $A_{\gamma^\infty}$ be the localized ring of $A$ by the powers of $\gamma$. The polynomial $f(x)/a_0$ is in $A_{a_0^\infty}[x]$, is monic and is indecomposable in $K[x]$. For each non-trivial divisor $m$ of $d$, let

$$f(x)/a_0 = u_m(g_m(x)) + h_m(x)$$

be the $m$-decomposition of $f(x)/a_0$ in $A_{\gamma^\infty}[x]$ ($m$ is invertible in $A_{\gamma^\infty}$). Each polynomial $h_m(x)$ writes $h_m(x) = h_m^A(x)/\gamma^{\nu_m}$ for some $h_m^A(x) \in A[x]$ and $\nu_m \in \mathbb{N}$, and is non-zero (as $f$ is indecomposable in $K[x]$). Let $h_{m0}$ be the (non-zero) coefficient of $h_m^A(x)$ of highest degree and set $I_f = \gamma \prod_m h_{m0}$. Consider next a morphism $\sigma : A \to k$ in a field $k$ such that $I_f^\sigma \neq 0$. This morphism uniquely extends to some morphism $A_{\gamma^\infty} \to k$, still denoted by $\sigma$. It is easily checked that the $m$-decomposition of $(f/a_0)^\sigma(x)$ in $k[x]$ is

$$(f/a_0)^\sigma(x) = u_m^\sigma(g_m^\sigma(x)) + h_m^\sigma(x)$$

As $h_m^\sigma \neq 0$ for all $m$, $(f/a_0)^\sigma$, and so also $f^\sigma$, is indecomposable in $k[x]$. $\square$

2.3.2. *Examples.* (a) For $A = \mathbb{Z}$, then $I_f \in \mathbb{Z}$, $I_f \neq 0$. Proposition 2.3, applied with $\sigma : \mathbb{Z} \to \mathbb{F}_p$ the reduction morphism modulo a prime number $p$, yields the following:

*for all suitably large $p$, the reduced polynomial $\overline{f}(x)$ modulo $p$ is indecomposable in $\overline{\mathbb{F}_p}[x]$.*

This example will be refined in section 3.

(b) Take $A = k[\underline{t}]$ with $k$ a field and $\underline{t} = (t_1, \dots, t_r)$ some indeterminates. Denote by $f(\underline{t}, x)$ the polynomial $f(x)$ of proposition 2.3. Assume that $\deg(f)$ is prime to the characteristic of $k$ and that $f(\underline{t}, x)$ is indecomposable in $k(\underline{t})[x]$. In this situation $I_f \in k[\underline{t}]$ and proposition 2.3, applied with $\sigma$ the specialization morphism $k[\underline{t}] \to \overline{k}$ that maps $\underline{t} = (t_1, \dots, t_r)$ to an $r$-tuple $\underline{t}^* = (t_1^*, \dots, t_r^*) \in \overline{k}^r$ yields the following:

*for all $\underline{t}^*$ off a proper Zariski closed subset of $\overline{k}^r$ (viz.* the subset $\{I_f(\underline{t}) = 0\}$*), the specialized polynomial $f(\underline{t}^*, x)$ is indecomposable in $\overline{k}[x]$.*

This example will be refined in section 4.

(c) Let $f(x) = x^d + a_1x^{d-1} + \cdots + a_d$ be the generic polynomial of degree $d \geqslant 1$ in one variable. Take for $A$ the ring $\mathbb{Z}[\underline{a}]$ generated by the $d$-tuple of indeterminates $\underline{a} = (a_1, \ldots, a_d)$ corresponding to the coefficients of $f(x)$. The argument below shows that $f(x)$ is indecomposable in $\mathbb{Q}(\underline{a})[x]$. Proposition 2.3, applied next with $\sigma : A \to k$ a specialization morphism of $\underline{a}$ and $k$ any field of characteristic 0, yields that all degree $d$ polynomials in $k[x]$ are indecomposable but possibly those from the proper Zariski closed subset corresponding to the equation $I_f = 0$ (with $I_f$ viewed in $k[\underline{a}]$).

To show that $f(x)$ is indecomposable in $\mathbb{Q}(\underline{a})[x]$, assume $f(x) = u(g(x))$ with $u, g \in \mathbb{Q}(\underline{a})[x]$ of degree $\geqslant 2$. As $f$ is monic, such a decomposition would exist with $u$ and $g$ monic in $\mathbb{Q}[\underline{a}][x]$; this follows from lemma 4.6 below. But then by specializing $\underline{a}$, it could be concluded that all degree $d$ polynomials in $\mathbb{Q}[x]$ are decomposable. This is not the case, as for example corollary 1.3 shows.

## 3. Proof of theorem 1.1

The proof is somewhat similar to the proof of lemma 2.2.

Let $f \in \mathbb{Z}[x]$ of degree $d$, $m$ be a divisor of $d$ and $p > d$ be a prime number. As in the proof of proposition 2.3, we reduce to the case that $f$ is monic by dividing $f(x)$ by the leading coefficient $a_0$ and viewing the resulting polynomial in $\mathbb{Z}_{a_0^\infty}[x]$. Then the reduction modulo $p$ of the $m$-decomposition $f = u(g) + h$ and the $m$-decomposition of the reduced polynomial modulo $p$ both exist and they coincide.

We say that a polynomial $p(x) = p_0x^d + p_1x^{d-1} + \cdots + p_d$ of degree $\leqslant d$ is *$f$-tame of order $d$* if there exist constants $\gamma_{i,d}$ such that $|p_i| \leqslant \gamma_{i,d} \| f \|_\infty^i$ for all $i = 0, \ldots, d$. This definition depends on $\|f\|_\infty$ and not on $\|p\|_\infty$. Of course $f$ is itself $f$-tame of order $d$.

Using the system $(\mathcal{S})$, it follows by induction on $i$ that $|b_i| \leqslant \gamma_{i,d} \|f\|_\infty^i$, $i = 1, \ldots, \frac{d}{m}$; thus $g$ is $f$-tame of order $\frac{d}{m}$. Recall now how the decomposition is continued. If $\frac{d}{m}$ does not divide $i$, the coefficient $h_i$ of $h = \sum_{i=1}^d h_i x^{d-i}$ is the coefficient of the highest monomial $\alpha_i x^{d-i}$ in the difference between $f$ and powers of $g$.

If $\frac{d}{m}$ divides $i$, say $i = j\frac{d}{m}$, then pick the coefficient $\alpha_i$ of the highest monomial above and set $u_j = \alpha_i$: this is the coefficient of $x^{m-j}$ in $u(x)$. Deduce that $|u_j| = |\alpha_i| \leqslant \gamma_j \|f\|_\infty^{j\frac{d}{m}} \leqslant \gamma \|f\|_\infty^d$ ($j = 2, \ldots, m$) for some constants $\gamma_j, \gamma$.

This implies that $u_j g^{m-j}$ is $f$-tame of order $d$ (even if it is a polynomial of degree $< d$). Whence $h$ is $f$-tame of order $d$ and so $\|h\|_\infty \leqslant \gamma_d \|f\|_\infty^d$.

Conclusion: as $f$ is not $m$-decomposable in $\mathbb{Q}[x]$, $h(x) \neq 0$. If $p > \gamma_d \|f\|_\infty^d$ then $h(x) \pmod p \neq 0$ and so $f(x) \pmod p$ is not $m$-decomposable in $\overline{\mathbb{F}_p}[x]$.

## 4. Proof of theorem 1.2

First note that assertions (b) and (c) immediately follow from assertion (a) and proposition 2.3. We are left with proving assertion (a). With no loss of generality we may assume that $\deg_{t_i} f \geqslant 0$. And this, due to the assumption on the characteristic of $k$, amounts to $\partial f / \partial t_i \neq 0$, $i = 1, \dots, r$. Also recall that due to the assumption on the characteristic of $k$, the polynomial $f(\underline{t}, x)$ is indecomposable in $\overline{k}[\underline{t}, x]$ [3, theorem 4.2].

We divide the proof into two stages.

4.1. **Stage 1: from $r$ to 2 variables.** Here we show that for $r \geqslant 2$, the polynomial $f(t_1 + \alpha_1 x, \dots, t_{r-1} + \alpha_{r-1} x, t_r, x)$ is indecomposable in the polynomial ring $\overline{k(\alpha_1, \dots, \alpha_{r-1}, t_1, \dots, t_{r-1})}[t_r, x]$.

For this stage we use the following classical characterization: if $\underline{y}$ is a tuple of at least two indeterminates and $L$ an algebraically closed field, a polynomial $f(\underline{y}) \in L[\underline{y}]$ is indecomposable in $L[\underline{y}]$ if and only if $f(\underline{y}) - T$ is irreducible in $\overline{L(T)}[\underline{y}]$ (where $T$ is a new indeterminate). The desired conclusion readily follows by induction from the following result, which as explained in [11, §2], is a reformulation of the Matsusaka-Zariski theorem [7, proposition 10.5.2].

**Proposition 4.1.** *Let $s \geqslant 3$ be an integer, $\underline{x} = (x_1, \dots, x_s)$ be an $s$-tuple of indeterminates and $Q(\underline{x}) \in k[\underline{x}]$ be an absolutely irreducible polynomial. Assume that $\partial Q / \partial x_1 \neq 0$. Then if $\alpha_1$ is a new indeterminate, the polynomial $Q(x_1 + \alpha_1 x_s, x_2, \dots, x_s)$ is irreducible in $\overline{k(\alpha_1, x_1)}[x_2, \dots, x_s]$.*

4.2. **Stage 2: from two to one variable.** Here we show that for $r \geqslant 1$, $f(t_1 + \alpha_1 x, \dots, t_r + \alpha_r x, x)$ is indecomposable in $\overline{k(\alpha_1, \dots, \alpha_r, t_1, \dots, t_r)}[x]$. From stage 1, we are reduced to proving the special case $r = 1$ of theorem 1.2 (a), which we restate below.

**Theorem 4.2.** *Let $f(t, x)$ be an indecomposable polynomial in $\overline{k}[t, x]$ with $k$ a field of characteristic $p = 0$ or $p > \deg(f)$. Then the polynomial $f(t + \alpha x, x)$ is indecomposable in $\overline{k(\alpha, t)}[x]$.*

Again because of the assumption on the characteristic of $k$, $f$ could equivalently be assumed to be indecomposable in $k[t,x]$.

*Remark* 4.3. The following example, inspired by [12, p. 21], shows the conclusion fails if the assumption on the characteristic $p$ is removed. Take $k = \mathbb{F}_p$ and $f(t,x) = x^{p^2} + x^p + t$. As $\deg_t(f) = 1$, $f(t,x)$ is indecomposable in $\overline{k}[t,x]$. But the polynomial $f(t+\alpha x, x) = x^{p^2} + x^p + t + \alpha x$ is decomposable in $\overline{k(\alpha,t)}[x]$ (and even in $\overline{k(\alpha)}[x]$): indeed, if $a,b \in \overline{k(\alpha)}$ satisfy $a + b^p = 1$ and $ab = \alpha$, then we have $x^{p^2} + x^p + t + \alpha x = (x^p + bx)^p + a(x^p + bx) + t$.

4.2.1. *Preliminary lemmas.* The following three lemmas will be used in the proof of theorem 4.2. The first one is due to Lecerf and Galligo [8]. It expresses in a simple and algebraic way a result already obtained by J.A. Wood [14]. We denote partial derivatives $\frac{\partial}{\partial\alpha}$ and $\frac{\partial}{\partial t}$ by $\partial_\alpha$ and $\partial_t$.

**Lemma 4.4** (Burger's equation lemma)**.** *Let $k$ be a field and $f \in k[t,x]$ be a polynomial of degree $d$. Let $q(\alpha,t,x) = f(t+\alpha x, x) \in k[\alpha,t,x]$. Suppose $\phi \in \overline{k(\alpha,t)}$ is a simple root in $x$ of the polynomial $q(\alpha,t,x)$, i.e., $q(\alpha,t,\phi) = 0$ and $\partial_x q(\alpha,t,\phi) \neq 0$. Then the derivations $\partial_\alpha$ and $\partial_t$ of $k(\alpha,t)$ uniquely extend to $k(\alpha,t,\phi)$ and we have $\partial_\alpha\phi = \phi \cdot \partial_t\phi$.*

*Proof.* Condition $\partial_x q(\alpha,t,\phi) \neq 0$ guarantees that $\partial_\alpha$ and $\partial_t$ uniquely extend to $k(\alpha,t,\phi)$. Differentiate then $q(\alpha,t,\phi) = 0$ with respect to $\alpha$ and with respect to $t$. Using next the special form $q(\alpha,t,x) = f(t+\alpha x, x)$ of $q$, this leads to the following formulas:

$$\begin{cases} \partial_x q(\alpha,t,\phi)\,\partial_\alpha\phi = -\partial_\alpha q(\alpha,t,\phi) = -\phi\,\partial_t f(\alpha+t\phi,\phi) \\ \partial_x q(\alpha,t,\phi)\,\partial_t\phi = -\partial_t q(\alpha,t,\phi) = -\partial_t f(\alpha+t\phi,\phi) \end{cases}$$

which yields what we want. □

**Lemma 4.5.** *Let $K$ be a field and $g \in K[v]$ be a polynomial such that $d = \deg(g)$ is prime to the characteristic of $K$. For all but at most $d-1$ values $c \in K$, the polynomial $g(v) + c$ has only simple roots in $\overline{K}$.*

*Proof.* Let $b_0 \in K$ be the coefficient of $v^d$ in $g$. The discriminant of $g+c$ is

$$\Delta = \mathrm{Res}(g+c, g') = d^d b_0^{2d-1} \prod_{\nu} (g(\nu) + c)$$

where in the product $\nu$ ranges over all roots $\nu \in \overline{K}$ of $g'$ (with repetition for multiple roots). If $c$ is distinct from the $d-1$ values $-g(\nu)$ then $\Delta \neq 0$ and $g(v) + c$ have only simple roots. □

**Lemma 4.6** (Turnwald)**.** *Let $A$ be an integrally closed domain of quotient field $K$ and $f \in A[x]$, monic in $x$. If $f$ is decomposable in $K[x]$ then $f$ admits a decomposition in $A[x]$, i.e. $f = u(g)$ with $u, g \in A[x]$ monic in $x$.*

See [13, proposition 2.2] or [6, theorem 2.1], [10, theorem 2.1].

4.2.2. *Proof of theorem 4.2.* We assume that $f(t + \alpha x, x) \in k[\alpha, t, x]$ is decomposable in $\overline{k(\alpha, t)}[x]$, and equivalently in $k(\alpha, t)[x]$, and we will prove that $f(t, x)$ is decomposable in $\overline{k}[t, x]$.

Adding a constant $c \in k$ to $f(x, y)$ changes $f(t+\alpha x, x)$ to $f(t+\alpha x, x)+c$ and does not affect the decomposability assumption nor the desired conclusion. Note next that $\deg_x(f(\alpha x, x)) = d$. As $p = 0$ or $p > d$, it follows from lemma 4.5 that some element $c \in k$ can be found such that the polynomial $f(\alpha x, x) + c$ has only simple roots in $\overline{k(\alpha)}$. Up to replacing $f$ by $f + c$ we may and will assume that this is the case for $f(\alpha x, x)$ itself.

If $f_d(t, x) \in k[t, x]$ denotes the homogeneous part of degree $d$ in $f(t, x)$, the leading coefficient of $f(\alpha x, x)$, relative to $x$, is $f_d(\alpha, 1)$. Consider now the polynomial $\tilde{q}(\alpha, t, x) = f(t + \alpha x, x)/f_d(\alpha, 1) = q(\alpha, t, x)/f_d(\alpha, 1)$. By construction $\tilde{q} \in k(\alpha)[t][x]$, is monic in $x$ and is decomposable in $k(\alpha, t)[x]$. By lemma 4.6 applied with $A = k(\alpha)[t]$, we get $\tilde{q} = u(g)$ with $u, g \in k(\alpha)[t][x]$, monic in $x$ and such that $\deg_x u = m \geqslant 2$ and $\deg_x g = d/m \geqslant 2$. Set

$$\tilde{q}(\alpha, t, x) = \prod_{i=1}^{d}(x - \phi_i) = \prod_{j=1}^{m}(g(\alpha, t, x) - \lambda_j),$$

so that $\phi_1, \dots, \phi_d \in \overline{k(\alpha, t)}$ are the roots of $\tilde{q}$, and $\lambda_1, \dots, \lambda_m \in \overline{k(\alpha, t)}$ are the roots of $u$. Furthermore, by uniqueness of factorization, there exists a partition of $\{1, \dots, d\}$ into subsets $I_1, \dots, I_m$ of $\{1, \dots, d\}$ such that:

$$\prod_{i \in I_j}(x - \phi_i) = g(\alpha, t, x) - \lambda_j \quad (j = 1, \dots, m)$$

We will use Newton's identities: for a polynomial $p(x) = x^n + p_1 x^{n-1} + \cdots + p_{n-1}x + p_n = \prod_{i=1}^{n}(x - \phi_i)$, setting $S_\ell = \sum_{i=1}^{n} \phi_i^\ell$, we have:

$$\text{(N)} \qquad S_\ell + p_1 S_{\ell-1} + \cdots + p_{\ell-1}S_1 + \ell p_\ell = 0 \quad (\ell = 1, \dots, n)$$

Applied to $g(\alpha, t, x) - \lambda_j$ (for which only the constant term depends on $j$), this provides the following: for every $\ell = 1, \dots, \frac{d}{m} - 1$ and $j = 1, \dots, m$,

$$\text{(*)} \qquad \sum_{i \in I_1} \phi_i^\ell = \sum_{i \in I_j} \phi_i^\ell \in k(\alpha)[t].$$

At this stage we use our initial reduction to the situation that $f(\alpha x, x)$ has only simple roots in $\overline{k(\alpha)}$. This implies first that $\tilde{q}(\alpha, t, x)$ has only simple roots in $\overline{k(\alpha, t)}$, and, second, that these roots, $\phi_1, \dots, \phi_d$, can be viewed in the ring $\overline{k(\alpha)}[[t]]$ of formal power series in $t$ with coefficients in $\overline{k(\alpha)}$, *via* some embedding $k(\alpha, t)(\phi_1, \dots, \phi_d) \subset \overline{k(\alpha)}((t))$; such an embedding indeed exists thanks to Hensel's lemma.

Differentiation of (*) for $\ell = \frac{d}{m} - 1$ with respect to $\alpha$ then provides

$$\sum_{i \in I_1} (\frac{d}{m} - 1) \cdot \partial_\alpha \phi_i \cdot \phi_i^{\frac{d}{m} - 2} = \sum_{i \in I_j} (\frac{d}{m} - 1) \cdot \partial_\alpha \phi_i \cdot \phi_i^{\frac{d}{m} - 2} \in k(\alpha)[t].$$

Use lemma 4.4 to deduce that

$$\sum_{i \in I_1} \phi_i \cdot \partial_t \phi_i \cdot \phi_i^{\frac{d}{m} - 2} = \sum_{i \in I_j} \phi_i \cdot \partial_t \phi_i \cdot \phi_i^{\frac{d}{m} - 2} \in k(a)[t]$$

and to conclude that

$$(**) \qquad \partial_t \left( \sum_{i \in I_1} \phi_i^{\frac{d}{m}} \right) = \partial_t \left( \sum_{i \in I_j} \phi_i^{\frac{d}{m}} \right) \in k(\alpha)[t] \qquad (j = 1, \dots, m)$$

Use this conclusion for $j = 1$ to write $\sum_{i \in I_1} \phi_i^{\frac{d}{m}} = P_1 + d_1$ for some $P_1 \in k(\alpha)[t]$ with $P_1(\alpha, 0) = 0$ and some $d_1 \in \overline{k(\alpha)}[[t^p]]$, and to deduce next that $\sum_{i \in I_j} \phi_i^{\frac{d}{m}} = P_1 + d_j$ for some $d_j \in \overline{k(\alpha)}[[t^p]]$, $j = 1, \dots, m$.

*Remark* 4.7. If the characteristic is $p = 0$, then the elements $d_1, \dots, d_m$ are constants in $\overline{k(\alpha)}$, and the end of the proof below is simpler.

The Newton identity (N) with $\ell = d/m$ and $p(x) = g(\alpha, t, x) - \lambda_j$ gives

$$\prod_{i \in I_j} (-\phi_i) = g_{d/m} = -\frac{m}{d} (S_{d/m} + g_1 S_{d/m-1} + \cdots + g_{d/m-1} S_1).$$

where $g_1, \dots, g_{d/m} \in k[\alpha, t]$ are the coefficients of $g$ with respect to $x$. From display (*), the sums $S_1, \dots, S_{\frac{d}{m}-1}$ lie in $k(\alpha)[t]$ and are independent of $j = 1, \dots, m$. And from above we have $S_{\frac{d}{m}} = P_1 + d_j$. Therefore there exists a polynomial $P_0 \in k(\alpha)[t]$ (independent of $j$) and elements $e_1, \dots, e_m \in \overline{k(\alpha)}[[t^p]]$ such that $\prod_{I_j} (-\phi_i) = P_0 + e_j$ ($j = 1, \dots, m$). This provides this formula for $\lambda_j$ ($j = 1, \dots, m$):

$$\lambda_j = g(\alpha, t, 0) - \prod_{i \in I_j} (-\phi_i) = g(\alpha, t, 0) - P_0 - e_j$$

Set $G(\alpha,t,x)=g(\alpha,t,x)-g(\alpha,t,0)+P_0\in k(\alpha)[t,x]$ so that

$$\tilde{q}(\alpha,t,x)=\prod_{j=1}^{m}(g(\alpha,t,x)-\lambda_j)=\prod_{j=1}^{m}(G(\alpha,t,x)+e_j).$$

This provides the decomposition $\tilde{q}=v(G)$ with $v(x)=\prod_{j=1}^m(x+e_j)$ in $\overline{k(\alpha)}[[t^p]][x]$ and $G\in k(\alpha)[t,x]$.

As $\tilde{q}$ and $G$ lie in $k(\alpha)[t,x]$ we deduce that $v\in k(\alpha,t)[x]$: indeed, once we know $\tilde{q}$ and $G$, the computation of $v$ is reduced to the resolution of a linear system. But then by lemma 4.6 one may take $v\in k(\alpha)[t,x]$. Up to a linear change of variables $x\mapsto x-a$, one may also assume that $v(x)$ is of the form $v(x)=x^m+v_2x^{m-2}+\cdots$ (*i.e.* $v_1=0$), so that we can apply lemma 2.2. Conclude that $\deg_t v\leqslant d$. As $v\in\overline{k(\alpha)}[[t^p]][x]$ and $p>d$ we deduce that $v\in k(\alpha)[x]$. This shows that $\tilde{q}$ is decomposable in $k(\alpha)[t,x]$.

Multiply the equality $\tilde{q}=v(G)$ by $f_d(\alpha,1)$ to get that $q$ is decomposable in $k(\alpha)[t,x]$, that is: $q(\alpha,t,x)=f(t+\alpha x,x)=v'(\alpha,(G'(\alpha,t,x))$ with $v'\in k(\alpha)[x]$ of degree $\geqslant 2$ and $G'(\alpha,t,x)\in k(\alpha)[t,x]$. For all but finitely many $\alpha^*\in\overline{k}$, specialization of $\alpha$ to $\alpha^*$ of this decomposition provides the non-trivial decomposition $f(t+\alpha^*x,x)=v'(\alpha^*,(G'(\alpha^*,t,x))$. But then the change of variables $(t,x)\mapsto(t-\alpha^*x,x)$ shows that $f(t,x)$ is decomposable in $\overline{k}[t,x]$.

4.3. **Explicit versions.** We explain here how our method can be used to get explicit results. For simplicity, we restrict to polynomials in two variables.

**Corollary 4.8.** *Let $f(t,x)$ be an indecomposable polynomial in $k[t,x]$ with degree $d$ where $k$ is a field of characteristic $p=0$ or $p>d$. Then there exist polynomials $h_{m,i}(\alpha,t)\in k[\alpha,t]$ where $m|d$, and $i=1,\dots,d-d/m$ of total degree $\leqslant md^2+2d$ with the following property: for all $(t^*,\alpha^*)\in k^2$, if for each divisor $m$ of $d$ there exists $i_0$ such that $h_{m,i_0}(\alpha^*,t^*)\neq 0$, then $f(t^*+\alpha^*x,x)$ is indecomposable of degree $d$ in $k[x]$.*

*Proof.* The proof is a variation of that of lemma 2.2 or of theorem 1.1. Set

$$q(\alpha,t,x)=f(t+\alpha x,x)=a'_0(\alpha,t)x^d+a'_1(\alpha,t)x^{d-1}+\cdots+a'_d(\alpha,t)$$

Due to the assumption $\deg f=d$ we get:

$$\deg_t a'_i(\alpha,t)\leqslant i,\quad \deg_\alpha a'_i(\alpha,t)\leqslant d-i,\quad \deg a'_i(\alpha,t)\leqslant d;\quad i=0,\dots,d.$$

In particular $a'_0(\alpha,t)=a'_0(\alpha)$ does not depend on $t$.

Consider then $\tilde{q}(\alpha,t,x)=q(\alpha,t,x)/a'_0(\alpha)$; this is a polynomial in $k(\alpha)[t,x]$, monic in $x$. Consider the $m$-decomposition of $\tilde{q}$ with respect to the variable $x$: $\tilde{q}=u_m(g_m)+h_m$.

*Variable $t$.* Apply lemma 2.2 to the polynomial $\tilde{q}$ seen as a polynomial in $A[t,x]$ with $A = k(\alpha)$, since $\deg_t a'_i(\alpha,t) \leqslant i$. This yields $\deg_t h \leqslant d$.

*Variable $\alpha$.* Consider now $\tilde{q}$ as a rational fraction in $\alpha$ and as a polynomial in $x$ to compute the degree in $\alpha$ of $h$ (we forget the variable $t$). Lemma 2.2 cannot be applied since the degree of the coefficients does not satisfy the correct hypothesis (moreover the coefficients are not polynomials in $\alpha$). The $m$-decomposition $\tilde{q} = u_m(g_m) + h_m$ lives in $A[\alpha]_{(a'_0(\alpha))^\infty}[x]$ with $A = k[t]$.

A polynomial $g(\alpha,x) = c_0 x^\delta + c_1(\alpha)x^{\delta-1} + \cdots + c_\delta(\alpha)$ in $A[\alpha]_{(a'_0(\alpha))^\infty}[x]$ is *$\alpha$-tame of order $\delta$* if each $c_i(\alpha)$ can be written ($i = 0,\ldots,\delta$):

$$c_i(\alpha) = \frac{c'_i(\alpha)}{a'_0(\alpha)^i} \text{ with } \deg c'_i(\alpha) \leqslant i\delta.$$

Note that $a'_0(\alpha)$ comes from $\tilde{q}$ and is fixed.

The following properties can easily be proved:

(1) $\tilde{q}(\alpha,t,x)$ is $\alpha$-tame of order $d$.
(2) The sum of two $\alpha$-tame polynomials of order $\delta$ is $\alpha$-tame of order $\delta$.
(3) The product of a $\alpha$-tame polynomial of order $\delta$ and a $\alpha$-tame polynomial of order $\delta'$ is $\alpha$-tame polynomial of order $\delta+\delta'$.
(4) The $k$-power a $\alpha$-tame polynomial of order $\delta$ is $\alpha$-tame of order $k\delta$.
(5) An $\alpha$-tame polynomial of order $jd$ is an $\alpha$-tame polynomial of order $md$ ($j = 1,\ldots,m$).

By inspection of system $(\mathcal{S})$, we have in the decomposition $\tilde{q} = u_m(g_m) + h_m$, that $g_m$ is $\alpha$-tame of order $d$. The proof is very similar to the one in lemma 2.2. Then by item (4), $g_m^j$ are $\alpha$-tame of order $jd$, and by item (5), $\tilde{q}$ and $g_m^j$ are $\alpha$-tame of order $md$, ($j = 1,\ldots,m$). As in lemma 2.2 we distinguish two cases:

If $\frac{d}{m}$ does not divide $i$, the coefficient $h_{m,i}(\alpha)$ of $h_m(x) = \sum_{i=1}^d h_{m,i}(\alpha)x^{d-i}$ is the coefficient of the highest monomial $\gamma_i(\alpha)x^{d-i}$ in the difference between $\tilde{q}$ and powers of $g_m$.

If $\frac{d}{m}$ divides $i$, let $j$ such that $i = j\frac{d}{m}$ and denote the former coefficient by $u_{m,j}(\alpha)$ (it is the coefficient of $x^{m-j}$ in $u_m$). Then $u_{m,j}(\alpha) = \gamma_i(\alpha) = \frac{\gamma'_i(\alpha)}{a'_0(\alpha)^i}$. This implies that $u_{m,j}(\alpha)g_m^{m-j}$ is $\alpha$-tame of order $md$.

Both cases imply that $u_m(g_m)$ and $h_m$ are $\alpha$-tame of order $md$.

*Conclusion.* The $m$-decomposition $\tilde{q} = u_m(g_m) + h_m$ provides a decomposition $q(\alpha,t,x) = a'_0(\alpha) \times \frac{1}{a'_0(\alpha)^d}(u'_m(g'_m) + h'_m)$ with $h'_m = \sum h'_{m,i}(\alpha,t)x^{d-\frac{d}{m}-i}$ a *polynomial* in $k[\alpha,t,x]$ whose coefficients satisfy: $\deg_\alpha h'_{m,i} \leqslant md^2$ and $\deg_t h'_{m,i} \leqslant d$. Hence $\deg h'_{m,i} \leqslant md^2 + d$. Finally, if $a'_0(\alpha) \neq 0$ then as usual

$q$ is $m$-decomposable if and only if $h'_{m,i} = 0$ for all $i$.
We set $h_{m,i}(\alpha, t) = a'_0(\alpha)\, h'_{m,i}(\alpha, t)$ and we have the desired result. □

**Corollary 4.9.** *Let $f(t, x)$ be an indecomposable polynomial in $k[t, x]$ with degree $d$ where $k$ is a field of characteristic $p = 0$ or $p > d$. Let $S$ be a finite subset of $k$. For a uniform random choice of $\alpha$, $t$ in $S$, the probability*

$$\mathcal{P}\big(\{f(t^* + \alpha^* x, x) \text{ is indecomposable in } k[x] \mid \alpha, t \in S\}\big)$$

*is at least equal to $1 - \mathcal{D}/|S|$, with $\mathcal{D} = \sigma_1(d).d^2 + 2\sigma_0(d).d$ where $\sigma_1(d) = \sum_{m|d} m$, $\sigma_0(d)$ is the number of divisors of $d$ and $|S|$ is the cardinality of $S$.*

*Proof.* By corollary 4.8, $f(t^* + \alpha^* x, x)$ is indecomposable in $k[x]$, if for all $m|d$ there exists $i_0$ such that $h_{m,i_0}(\alpha^*, t^*) = 0$. Thus if $(\alpha^*, t^*)$ belongs to $\mathcal{A} = \bigcap_{m|d} \bigcup_{1\leqslant i\leqslant d-d/m} \{(\alpha^*, t^*) \mid h_{m,i}(\alpha^*, t^*) \neq 0\}$ then $f(t^* + \alpha^* x, x)$ is indecomposable in $k[x]$. Now, we consider the complement, $\mathcal{A}^c$, of this event, and we remark that:

$$\begin{aligned}
\mathcal{A}^c &= \bigcup_{m|d} \bigcap_{1\leqslant i\leqslant d-d/m} \{(\alpha^*, t^*) \mid h_{m,i}(\alpha^*, t^*) = 0\} \\
&\subset \bigcup_{m|d} \{(\alpha^*, t^*) \mid h_{m,1}(\alpha^*, t^*) = 0\} \\
&\subset \{(\alpha^*, t^*) \mid \prod_{m|d} h_{m,1}(\alpha^*, t^*) = 0\} = \mathcal{B}.
\end{aligned}$$

Thus $\mathcal{P}(\mathcal{A}^c) \leqslant \mathcal{P}(\mathcal{B})$ and then $1 - \mathcal{P}(\mathcal{B}) \leqslant \mathcal{P}(\mathcal{A})$.
As $\deg(h_{m,1}) \leqslant md^2 + 2d$, by Zippel-Schwartz's lemma, see e.g. [9, lemma 6.44], applied to the event $\mathcal{B}$, we have

$$1 - \frac{\sum_{m|d}(md^2 + 2d)}{|S|} \leqslant 1 - \mathcal{P}(\mathcal{B}).$$

This gives the desired result. □

## References


[1] M. Ayad, A. Nidal, *On composite polynomials.* Int. J. Algebra 2 (2008), no. 5-8, 315–326.

[2] A. Bodin, *Decomposition of polynomials and approximate roots.* Proc. Amer. Math. Soc. 138 (2010), 1989-1994.

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

[4] L. Busé, G. Chèze, S. Najib, *Noether forms for the study of non-composite rational functions and their spectrum.* Acta Arith. 147, (2011), 217–231.

[5] G. Chèze, S. Najib, *Indecomposability of polynomials via Jacobian matrix.* Journal of Algebra 324, 1, 1–11,(2010).

[6] A. Dujella, I. Gusić, *Indecomposability of polynomials and related diophantine equations.* Quart. J. Math. 57, (2006), 193-201.

[7] M. Fried, M. Jarden, *Field Arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete 11, Springer-Verlag, 2004.

[8] A. Galligo, G. Lecerf, *Faster algorithms for factoring bivariate polynomials over large fields.* work in progress.

[9] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, second edition, Cambridge University Press, 2003.

[10] I. Gusić, *On decomposition of polynomials over rings.* Glas. Mat. Ser. III, Vol. 43 (63), (2008), 7-12.

[11] S. Najib, *Une généralisation de l'inégalité de Stein-Lorenzini.* J. Algebra 292 (2005), 566–573.

[12] A. Schinzel, *Polynomials with special regard to reducibility.* Encyclopedia of Mathematics and its Applications 77. Cambridge University, 2000.

[13] G. Turnwald, *On Schur's conjecture.* J. Austral. Math. Soc. 58 (1995), 312–357.

[14] J.A. Wood, *A simple criterion for local hypersurfaces to be algebraic.* Duke Math. J. 51 (1984), no. 1, 235–237.

*E-mail address*: `Arnaud.Bodin@math.univ-lille1.fr`

*E-mail address*: `guillaume.cheze@math.univ-toulouse.fr`

*E-mail address*: `Pierre.Debes@math.univ-lille1.fr`

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France

Institut de Mathématiques de Toulouse, Université Paul Sabatier Toulouse 3, 31062 Toulouse Cedex 9, France

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France