ACTA ARITHMETICA
139.1 (2009)

Indecomposable polynomials and their spectrum

by

Arnaud Bodin, Pierre Dèbes and Salah Najib (Lille)

1. Introduction. Fix an integer $n \geq 2$ and a n-tuple of indeterminates $\underline{x} = (x_1, \ldots, x_n)$. A non-constant polynomial $F(\underline{x}) \in k[\underline{x}]$ with coefficients in an algebraically closed field k is said to be *indecomposable* in $k[\underline{x}]$ if it is not of the form $u(H(\underline{x}))$ with $H(\underline{x}) \in k[\underline{x}]$ and $u \in k[t]$ with $\deg(u) \geq 2$. An element $\lambda^* \in k$ is called a *spectral value* of $F(\underline{x})$ if $F(\underline{x}) - \lambda^*$ is reducible in $k[\underline{x}]$. It is well-known that

(1) *$F(\underline{x}) \in k[\underline{x}]$ is indecomposable if and only if $F(\underline{x}) - \lambda$ is irreducible in $\overline{k(\lambda)}[\underline{x}]$ (where λ is an indeterminate)*,
(2) *if $F(\underline{x}) \in k[\underline{x}]$ is indecomposable, then the subset* $\mathrm{sp}(F) \subset k$ *of all spectral values of $F(\underline{x})$—the* spectrum *of $F(\underline{x})$—is finite; and in the opposite case*, $\mathrm{sp}(F) = k$,
(3) *more precisely, if $F(\underline{x}) \in k[\underline{x}]$ is indecomposable and for every $\lambda^* \in k$, $n(\lambda^*)$ is the number of irreducible factors of $F(\underline{x}) - \lambda^*$ in $k[\underline{x}]$, then $\rho(F) := \sum_{\lambda^* \in k}(n(\lambda^*) - 1) \leq \deg(F) - 1$. In particular*, $\mathrm{card}(\mathrm{sp}(F)) \leq \deg(F) - 1$.

Statement (3), which is known as Stein's inequality, is due to Stein [13] in characteristic 0 and Lorenzini [10] in arbitrary characteristic (but for two variables); see [11] for the general case.

This paper offers some new results in this context.

In §2, given an indecomposable polynomial $F(\underline{x})$ with coefficients in an integral domain A and a ring morphism $\sigma : A \to k$ with k an algebraically closed field, we investigate the connection between the spectrum of $F(\underline{x})$ and that of the polynomial $F^\sigma(\underline{x})$ obtained by applying σ to the coefficients of $F(\underline{x})$. Theorem 2.1 provides a conclusion *à la Bertini–Noether*, which, despite its basic nature, does not seem to be available in the literature: under minimal assumptions on A, the connection is the expected one gener-

2000 *Mathematics Subject Classification*: 12E05, 11C08, 12Y05.
Key words and phrases: irreducible and indecomposable polynomials, Stein's theorem, spectrum of a polynomial.

DOI: 10.4064/aa139-1-7

ically. For example if $A = \mathbb{Z}$, "spectrum" and "reduction modulo a prime p" commute if p is suitably large (depending on F). We give other typical applications, notably for a specialization morphism σ. Related results are given in [3].

For two variables, we give in §3 an indecomposability criterion for a reduced polynomial modulo some prime p (Theorem 3.1) that is more precise than Theorem 2.1: the condition "for suitably large p" is replaced by some explicit condition on $F(x, y)$ and p, possibly satisfied for small primes. This criterion uses some results on good reduction of curves and covers due to Grothendieck, Fulton et al.; we will follow here Zannier's version [14]. Another criterion based on the Newton polygon of a polynomial is given in [4].

§4 is devoted to the connection between the indecomposability properties over a field K and over its algebraic closure $\overline{K}$. While it has been known they are equivalent in many circumstances, for example in characteristic 0, it has remained to handle the inseparable case to obtain a definitive conclusion. That is the purpose of Proposition 4.1, which, conjoined with previous works, shows that the only polynomials $F(\underline{x})$ indecomposable in $K[\underline{x}]$ but decomposable in $\overline{K}[\underline{x}]$ are pth powers in $\overline{K}[\underline{x}]$, where $p > 0$ is the characteristic of K (Theorem 4.2).

§5 is aimed at counting the number of indecomposable polynomials of a given degree d with coefficients in the finite field $\mathbb{F}_q$. We show that most polynomials are indecomposable: the ratio I_d/N_d of indecomposables of degree d tends to 1 (as $d \to \infty$ or as $q \to \infty$), and we give some estimate for the error term $1 - I_d/N_d$. The constants involved in our estimates are explicit. For simplicity we mostly restrict to polynomials in two variables, as calculations become more intricate when $n > 2$. We also consider the one variable situation (for which the definition of indecomposability is slightly different, see §4.3) with the restriction that q and d are relatively prime. A unified treatment of the general case $n \geq 2$ is offered in a parallel work of von zur Gathen [8], who also considers the "wild case" ($n = 1$ with $(q, d) \neq 1$) in [9].

2. Spectrum and morphisms

Notation. If $\sigma : A \to B$ is a ring morphism, we denote the image of $a \in A$ by a^σ. For $P(\underline{x}) \in A[\underline{x}]$, we denote the polynomial obtained by applying σ to the coefficients of P by $P^\sigma(\underline{x})$. If $V \subset \mathbb{A}^n_A$ is the Zariski closed subset associated with a family of polynomials $P_i(\underline{x}) \in A[\underline{x}]$, we denote by V^σ the Zariski closed subset of $\mathbb{A}^n_B$ associated with the family of polynomials $P_i^\sigma(\underline{x}) \in B[\underline{x}]$.

If $S \subset A$ is a multiplicative subset such that all elements from S^σ are invertible in B, we still denote by σ the natural extension $S^{-1}A \to B$ of the original morphism σ.

Fix an integrally closed ring A, with a perfect fraction field K.

An effective divisor $D = \sum_{i=1}^{r} n_i a_i$ of $\overline{K}$ is said to be *K-rational* if the coefficients of the polynomial $P(T) = \prod_{i=1}^{r}(T - a_i)^{n_i}$ are in K ([1]). A morphism $\sigma : A \to k$ to an algebraically closed field k is then said to be *defined at D* if the coefficients of $P(T)$ have a common denominator $d \in A$ such that d^σ is non-zero in k ([2]). In this case we denote by $P^\sigma(T) \in k[T]$ the image polynomial of $P(T)$ by the morphism σ (extended to the fraction field of A with denominators a power of d) and by D^σ the effective divisor of k whose support is the set of roots of $P^\sigma(T)$ and coefficients are the corresponding multiplicities.

2.1. *Statement.* For more precision, we use the *spectral divisor* rather than the spectrum: it is the divisor $\mathrm{spdiv}(F) = \sum_{\lambda^* \in k}(n(\lambda^*) - 1)\lambda^*$ of the affine line $\mathbb{A}^1(k)$. Its support is the spectrum of F, and Stein's inequality rewrites $\deg(\mathrm{spdiv}(F)) \leq \deg(F) - 1$.

THEOREM 2.1. *Let $F(\underline{x}) \in A[\underline{x}]$ be indecomposable in $\overline{K}[\underline{x}]$. Then there exists a non-zero element $h_F \in A$ such that the following holds. For every morphism $\sigma : A \to k$ to an algebraically closed field k, if $h_F^\sigma \neq 0$, then $F^\sigma(\underline{x})$ is indecomposable in $k[\underline{x}]$, the morphism $\sigma : A \to k$ is defined at the divisor* $\mathrm{spdiv}(F)$, *and* $\mathrm{spdiv}(F^\sigma) = (\mathrm{spdiv}(F))^\sigma$; *in particular*, $\rho(F^\sigma) = \rho(F)$ *and* $\mathrm{sp}(F^\sigma) = (\mathrm{sp}(F))^\sigma$.

The first stage of the proof will produce the spectrum as a Zariski closed subset of the affine line $\mathbb{A}^1_A$ over the ring A. Specifically the following can be drawn from the proof: there is a proper ([3]) Zariski closed subset $V_F \subset \mathbb{A}^1_A$ such that for every morphism $\sigma : A \to k$ as above,

$(*)$ *the polynomial $F^\sigma(\underline{x})$, if it is of degree equal to* $\deg(F)$, *is indecomposable in $k[\underline{x}]$ if and only if the Zariski closed subset $V_F^\sigma \subset \mathbb{A}^1_k$ is proper, and in this case* $\mathrm{sp}(F^\sigma) = V_F^\sigma(k)$.

When applied to the inclusion morphism $A \to \overline{K}$, Theorem 2.1 shows that the spectrum of $F(\underline{x})$ is equal to the Zariski closed subset $V_F(\overline{K})$. In particular, it is K-rational. The same is true for the spectral divisor of $F(\underline{x})$ as $n(\lambda^\tau) = n(\lambda)$ for each $\lambda \in \overline{K}$ and each $\tau \in \mathrm{Gal}(\overline{K}/K)$.

Making the constant h_F from Theorem 2.1 explicit is an interesting next goal. This requires good bounds for the "Noether forms" associated with

([1]) Under our hypothesis "K perfect", this amounts to the invariance of $P(T)$, or of D, under $\mathrm{Gal}(\overline{K}/K)$.

([2]) Under our hypothesis "A integrally closed", this amounts to saying the elements a_i themselves have a common denominator $d \in A$ (that is, da_i is integral over A, $i = 1, \ldots, r$) such that $d^\sigma \neq 0$.

([3]) That is, distinct from the whole surrounding space (here the affine line $\mathbb{A}^1_A$ over the ring A); equivalently, there exists a non-zero polynomial in the associated ideal.

the polynomial $F(\underline{x})-\lambda \in \overline{K(\underline{\lambda})}[\underline{x}]$ in §2.3.1. Some work of Busé, Chèze and Najib in this direction is in progress [3].

2.2. *Typical applications*

2.2.1. Situation 1. If $A=\mathbb{Z}$, then $h_F \in \mathbb{Z}$, $h_F \neq 0$. Theorem 2.1, applied with $\sigma : \mathbb{Z} \to \overline{\mathbb{F}}_p$ the reduction morphism modulo a prime number p yields:

for all suitably large p, the reduced polynomial $\overline{F}(\underline{x})$ modulo p is indecomposable in $\overline{\mathbb{F}}_p[\underline{x}]$ and its spectral divisor is obtained by reducing that of $F(\underline{x})$, that is, $\mathrm{spdiv}(\overline{F}) = \overline{\mathrm{spdiv}(F)}$.

2.2.2. Situation 2. Take $A=k[\underline{t}]$ with k an algebraically closed field and $\underline{t}=(t_1,\dots,t_r)$ some indeterminates. Denote by $F(\underline{t},\underline{x})$ the polynomial $F(\underline{x})$ of the general statement. Theorem 2.1, applied with σ the specialisation morphism $k[\underline{t}] \to k$ that maps $\underline{t}=(t_1,\dots,t_r)$ to an r-tuple $\underline{t}^*=(t_1^*,\dots,t_r^*) \in k^r$ yields:

for all $\underline{t}^*$ off a proper Zariski closed subset of k^r, the specialized polynomial $F(\underline{t}^*,\underline{x})$ is indecomposable in $k[\underline{x}]$ and its spectral divisor is obtained by specializing that of $F(\underline{t},\underline{x})$.

2.2.3. Situation 3. $F(\underline{x})$ is the generic polynomial in n variables and of degree d. Take for A the ring $\mathbb{Z}[a_{\underline{i}}]$ generated by the indeterminates $a_{\underline{i}}$ corresponding to the coefficients of $F(\underline{x})$; the multi-index $\underline{i}=(i_1,\dots,i_n)$ ranges over the set $I_{n,d}$ of all n-tuples of integers ≥ 0 such that $i_1+\cdots+i_n \leq d$.

Classically the polynomial $F(\underline{x})$ is irreducible in $\overline{\mathbb{Q}(a_{\underline{i}})}[\underline{x}]$, hence it is indecomposable. Theorem 2.1, applied with $\sigma : A \to k$ a specialization morphism of the $a_{\underline{i}}$, shows that all polynomials $f(\underline{x}) \in k[\underline{x}]$ of degree d are indecomposable except possibly those from the proper Zariski closed subset corresponding to the equation $h_F=0$ (with h_F viewed in $k[a_{\underline{i}}]$).

For polynomials $f(\underline{x})$ outside the closed subset $h_F=0$, the spectrum of f is obtained by specializing the generic spectrum. However, we have:

Proposition 2.2. *For $d>2$ or $n>2$, the generic spectrum is empty. For $d=n=2$, it contains a single element, given by*

$$a_{00} - \frac{a_{02}a_{10}^2 + a_{20}a_{01}^2 - a_{01}a_{10}a_{11}}{4a_{02}a_{20}-a_{11}^2}.$$

For $d>2$ or $n>2$, polynomials with a non-empty spectrum lie in the Zariski closed subset $h_F=0$.

Proof. Assume that the generic spectrum is not empty. If k is an algebraically closed field and $\mathcal{R}_{n,d}$ (resp. $\mathcal{P}_{n,d}|_{a_{\underline{0}}=0}$) denotes the set of polynomials $P(\underline{x}) \in k[\underline{x}]$ of degree $\leq d$ that are reducible in $k[\underline{x}]$ (resp. whose constant term is zero), the correspondence $P(\underline{x}) \mapsto P(\underline{x})-P(\underline{0})$ induces an algebraic morphism $\mathcal{R}_{n,d} \to \mathcal{P}_{n,d}|_{a_{\underline{0}}=0}$ which is generically surjective (that

is, surjective above a non-empty Zariski open subset of $\mathcal{P}_{n,d}|_{a_{\underline{0}}=0}$). It follows that $\mathcal{R}_{n,d}$ is of codimension ≤ 1 in the space $\mathcal{P}_{n,d}$ of all polynomials in $k[\underline{x}]$ of degree $\leq d$. This observation provides the desired conclusion in the case $n = 2$ and $d > 2$: indeed $\operatorname{codim}_{\mathcal{P}_{2,d}}(\mathcal{R}_{2,d}) = d - 1$ [7, Theorem 2].

For $d = n = 2$, the equation "$(ux+ay+b)(vx+cy+d) = F(x, y)$ modulo the constant term" with unknowns u, a, b, v, c, d is readily solved: reduce to the case $a_{20} = u = v = 1$, find the unique solution for the 4-tuple (a, b, c, d) and compute bd; the generic spectral value is then $a_{00} - bd$.

Finally assume that for $d \geq 2$ and $n > 2$, there exists a generic spectral value $\lambda \in \overline{K}$ (with $K = \mathbb{Q}(a_{\underline{i}})$). Let $F(\underline{x}) - \lambda = Q(\underline{x})R(\underline{x})$ be a non-trivial factorization in $\overline{K}[\underline{x}]$. Specializing $x_3, \ldots, x_n$ to 0 gives a non-trivial factorization in $\overline{K}[x_1, x_2]$ of the generic polynomial of degree d in two variables. From the first part of the proof, we have $d = 2$. Furthermore, the above case provides the necessary value of λ. Now specializing x_2 and $x_4, \ldots, x_n$ to 0 leads to a different value. This is a contradiction. ∎

2.3. *Proof of Theorem 2.1*

2.3.1. *1st stage: elimination theory.* This stage is aimed at showing Proposition 2.3 below, which generalizes the Bertini–Noether theorem [6, Prop. 9.4.3]. It is proved in the general situation

(Hyp) *a polynomial* $\mathcal{F}(\underline{\lambda}, \underline{x}) \in A[\underline{\lambda}, \underline{x}]$ *is irreducible in* $\overline{K(\underline{\lambda})}[\underline{x}]$, *where* $\underline{\lambda} = (\lambda_1, \ldots, \lambda_s)$ *is an* s*-tuple of indeterminates* ($s \geq 0$).

We will use it in the special case $\mathcal{F}(\underline{\lambda}, \underline{x}) = F(\underline{x}) - \lambda$. The hypotheses "$A$ integrally closed" and "K perfect" are not necessary for this stage.

As in Situation 3, consider some indeterminates $(a_{\underline{i}})_{\underline{i} \in I_{n,d}}$ corresponding to the coefficients of a polynomial of degree d in n variables. A polynomial with coefficients in a ring R corresponds to a morphism $\phi : \mathbb{Z}[a_{\underline{i}}] \to R$; denote by $F(a_{\underline{i}}^{\phi})(\underline{x}) \in A[\underline{x}]$ the corresponding polynomial. Let $\varphi_{\underline{\lambda}} : \mathbb{Z}[a_{\underline{i}}] \to A[\underline{\lambda}]$ be the morphism corresponding to the polynomial from statement (Hyp): $\mathcal{F}(\underline{\lambda}, \underline{x}) = F(a_{\underline{i}}^{\varphi_{\underline{\lambda}}})(\underline{x})$.

From Noether's theorem [12, §3.1, Theorem 32], there exist finitely many universal homogeneous forms $\mathcal{N}_h(a_{\underline{i}})$ ($1 \leq h \leq D = D(n, d)$) in the $a_{\underline{i}}$ and with coefficients in $\mathbb{Z}$ such that:

(4) for every morphism $\phi : \mathbb{Z}[a_{\underline{i}}] \to k$ to an algebraically closed field k, the polynomial $F(a_{\underline{i}}^{\phi})(\underline{x})$, if it is of degree d, is reducible in $k[\underline{x}]$ if and only if $\mathcal{N}_h(a_{\underline{i}}^{\phi}) = 0$ for $h = 1, \ldots, D$.

For ϕ taken to be the morphism $\varphi_{\underline{\lambda}} : \mathbb{Z}[a_{\underline{i}}] \to A[\underline{\lambda}] \subset \overline{K(\underline{\lambda})}$, the elements $\mathcal{N}_h(a_{\underline{i}}^{\varphi_{\underline{\lambda}}}) \in A[\underline{\lambda}]$ are polynomials $N_h(\underline{\lambda})$. Let $V_{\mathcal{F}} \subset \mathbb{A}_A^s$ be the Zariski closed subset corresponding to the ideal they generate; it is a proper closed subset. Indeed, as $\mathcal{F}(\underline{\lambda}, \underline{x})$ is irreducible in $\overline{K(\underline{\lambda})}[\underline{x}]$, from (4), at least one

of the polynomials $N_h(\underline{\lambda})$, say $N_{h_0}(\underline{\lambda})$, is non-zero. Denote by $a_{\mathcal{F}} \in A$ the product of a non-zero coefficient of $N_{h_0}(\underline{\lambda})$ and the non-zero coefficient of some monomial of $\mathcal{F}(\underline{\lambda}, \underline{x})$ of degree d in $\underline{x}$.

If R is an integral domain and $\Sigma : A[\underline{\lambda}] \to R$ a morphism, then (4), with ϕ taken to be $\Sigma \circ \varphi_{\underline{\lambda}} : \mathbb{Z}[a_{\underline{i}}] \to R \hookrightarrow \kappa$ and $\kappa = \overline{\mathrm{Frac}(R)}$, shows that the polynomial $\mathcal{F}^{\Sigma} \in R[\underline{x}]$, if of degree d, is irreducible in $\kappa[\underline{x}]$ if and only if at least one of the elements $N_h^{\Sigma} \in R$ is non-zero (note that $\mathcal{F}^{\Sigma} = F(a_{\underline{i}}^{\Sigma\varphi_{\underline{\lambda}}})(\underline{x})$ and $\mathcal{N}_h(a_{\underline{i}}^{\Sigma\varphi_{\underline{\lambda}}}) = \mathcal{N}_h(a_{\underline{i}}^{\varphi_{\underline{\lambda}}})^{\Sigma}$), or, equivalently, if the corresponding Zariski closed subset of $\mathrm{Spec}(R)$ is proper.

Let $\sigma : A \to k$ be a morphism with k algebraically closed. Apply the above first with Σ taken to be the morphism $\sigma : A[\underline{\lambda}] \to k[\underline{\lambda}]$ and then, for $\underline{\lambda}^* \in k^s$, with Σ taken to be the morphism $s_{\underline{\lambda}^*} \circ \sigma : A[\underline{\lambda}] \to k$ obtained by composing $\sigma : A[\underline{\lambda}] \to k[\underline{\lambda}]$ with the specialization morphism $s_{\underline{\lambda}^*} : k[\underline{\lambda}] \to k$ to $\underline{\lambda}^*$. We conclude:

Proposition 2.3 (Bertini–Noether generalized).

(a) *The polynomial $\mathcal{F}^{\sigma}(\underline{\lambda}, \underline{x})$, if it is of degree d in $\underline{x}$, is irreducible in $\overline{k(\underline{\lambda})}[\underline{x}]$ if and only if the Zariski closed subset $V_{\mathcal{F}}^{\sigma} \subset \mathbb{A}_k^s$ is proper. All these conditions are satisfied if $a_{\mathcal{F}}^{\sigma}$ is non-zero in k.*

(b) *If the polynomial $\mathcal{F}^{\sigma}(\underline{\lambda}^*, \underline{x})$ is of degree d, then it is reducible in $k[\underline{x}]$ if and only if $\underline{\lambda}^*$ is in the set $V_{\mathcal{F}}^{\sigma}(k)$.*

2.3.2. *2nd stage: implications for the spectrum of $F(\underline{x})$.* We return to the situation where $\mathcal{F}(\lambda, \underline{x}) = F(\underline{x}) - \lambda$. Denote the Zariski closed subset $V_{\mathcal{F}}$ from §2.3.1 by V_F; it is a Zariski closed subset of the affine line $\mathbb{A}_A^1$. The preceding conclusions, conjoined with the connection, recalled in §1, between indecomposability of $F(\underline{x})$ and irreducibility of $F(\underline{x}) - \lambda$, yield statement $(*)$ from §2.1.

Denote by $s_F(\lambda)$ the g.c.d. of the polynomials $N_h(\lambda)$ in the ring $K[\lambda]$. Write it as $s_F(\lambda) = S_F(\lambda)/c_1$ with $S_F(\lambda) \in A[\lambda]$ and $c_1 \in A$ non-zero. The polynomial $S_F(\lambda)$ is non-zero and its distinct roots in $\overline{K}$, say $\lambda_1, \ldots, \lambda_s$, which are the common roots in $\overline{K}$ of the polynomials $N_h(\lambda)$, are the spectral values of $F(\underline{x})$ (note that $F(\underline{x}) - \lambda^*$ is of degree d for all $\lambda^* \in \overline{K}$). Thus we have $S_F(\lambda) = c_2 \prod_{i=1}^{s} (\lambda - \lambda_i)^{n_i} \in A[\lambda]$ for some exponents $n_i > 0$ and $c_2 \in A$, $c_2 \neq 0$. It follows that the set $\mathrm{sp}(F) = \{\lambda_1, \ldots, \lambda_s\}$ is K-rational. As already noted, the same is then true for the spectral divisor $\mathrm{spdiv}(F)$.

2.3.3. *3rd stage: invariance of the spectrum of F via morphisms .* Fix a morphism $\sigma : A \to k$ with k algebraically closed. Denote by a_F the element $a_{\mathcal{F}}$ from §2.3.1 for $\mathcal{F} = F(\underline{x}) - \lambda$. If $a_F^{\sigma} \neq 0$, then $F^{\sigma}(\underline{x})$ is of degree d and indecomposable in $k[\underline{x}]$. Furthermore, its spectral values are the roots in k of the g.c.d. of the polynomials $N_h^{\sigma}(\lambda)$.

Note that the element c_2 above is a common denominator of $\lambda_1, \dots, \lambda_s$; if $c_2^\sigma \neq 0$, the morphism $\sigma : A \to k$ is defined at spdiv(F).

LEMMA 2.4. *There exists* $c_3 \in A$, $c_3 \neq 0$, *such that, if* $a_F^\sigma c_1^\sigma c_2^\sigma c_3^\sigma \neq 0$, *the polynomial* $S_F^\sigma(\lambda) \in k[\lambda]$ *equals* (*up to some non-zero multiplicative constant in* k) *the g.c.d. in* $k[\lambda]$ *of the polynomials* $N_h^\sigma(\lambda)$ $(1 \leq h \leq D)$. *In particular*, $\mathrm{sp}(F^\sigma) = (\mathrm{sp}(F))^\sigma$.

Proof. The problem is whether the g.c.d. commutes with σ. The Euclidean algorithm provides the g.c.d. as the last non-zero remainder. To reach our goal, it suffices to guarantee that for each division $a = bq + r$ in $K[\lambda]$ involved in the algorithm, the identity $a^\sigma = b^\sigma q^\sigma + r^\sigma$, with σ suitably extended, be the division of a^σ by b^σ in $k[\lambda]$. For this, write a, b, q and r in the form $n(\lambda)/m$ with $n(\lambda) \in A[\lambda]$ and $m \in A$, consider the product β of denominators m of a, b, q and r with the coefficients of highest degree monomials in the numerators $n(\lambda)$ of b and r and require that $\beta^\sigma \neq 0$. Multiplying all elements β for all divisions leading to the g.c.d. of two, then of all polynomials in question, leads to a non-zero element $c_3 \in A$ which satisfies the desired statement. ∎

REMARK 2.5. Morphisms and g.c.d. do not commute in general: for example $\gcd(\lambda, \lambda + a)$ is 1 generically, but equals λ if $a = 0$.

2.3.4. *4th stage: invariance of* spdiv(F) *via morphisms.* It remains to extend the conclusion "$\mathrm{sp}(F^\sigma) = (\mathrm{sp}(F))^\sigma$" to the spectral divisor spdiv(F). We will show how to guarantee that, *via* the morphism σ, the spectral values remain distinct and the associated decompositions of $F(\underline{x}) - \lambda$ have the same numbers of distinct irreducible factors ([4]).

Consider the discriminant of the polynomial $\prod_{i=1}^{s}(\lambda - \lambda_i)$; it is a non-zero element of K. Write it as c_4/c_5 with $c_4, c_5 \in A$, non-zero. If $c_4^\sigma c_5^\sigma \neq 0$, the polynomials $S_F(\lambda)$ and $S_F^\sigma(\lambda)$ have the same number of distinct roots, whence $\mathrm{card}(\mathrm{sp}(F^\sigma)) = \mathrm{card}((\mathrm{sp}(F))^\sigma) = \mathrm{card}(\mathrm{sp}(F))$.

For $i = 1, \dots, s$, let $F(\underline{x}) - \lambda_i = \prod_{j=1}^{n(\lambda_i)} Q_{ij}(\underline{x})^{k_{ij}}$ be a factorization (into distinct irreducible polynomials) in $\overline{K}[\underline{x}]$. Let E/K be a finite Galois extension that contains the finite set $\mathcal{C}$ of all coefficients involved in all above factorizations, c_6 be a non-zero element of A such that $c_6 c$ is integral over A for all $c \in \mathcal{C}$, and c_7 be the discriminant of a basis of E over K the elements of which are integral over A. Denote by B the fraction ring of A with denominator a power of $c_6 c_7$, and by B'_E the integral closure of B in E. The ring B'_E is a free B-module of rank $[E : K]$. Assume that $c_6^\sigma c_7^\sigma \neq 0$. The morphism $\sigma : A \to k$ extends to a morphism $B \to k$, and, as k is

([4]) The argument will also show the degrees of these irreducible factors, say $Q_{\lambda,j}$, remain the same and thus so does the quantity $\min_{\lambda \in \mathrm{sp}(F)}(\sum_j \deg(Q_{\lambda,j}) - 1)$, which replaces $\deg(F) - 1$ in Lorenzini's refined version [10] of Stein's inequality.

algebraically closed, this morphism $\sigma : B \to k$ can in turn be extended to a morphism $\widetilde{\sigma} : B'_E \to k$.

The polynomials $Q_{ij}(\underline{x})$ are in the ring $B'_E[\underline{x}]$ and are absolutely irreducible. The (classical) Bertini–Noether theorem provides a non-zero element $\beta \in B'_E$ such that, if $\beta^{\widetilde{\sigma}} \neq 0$, then each of the polynomials $Q_{ij}^{\widetilde{\sigma}}(\underline{x})$ is absolutely irreducible. Therefore the decomposition $F^\sigma(\underline{x}) - \lambda_i^{\widetilde{\sigma}} = \prod_{j=1}^{n(\lambda_i)} Q_{ij}^{\widetilde{\sigma}}(\underline{x})$ obtained from the preceding one by applying $\widetilde{\sigma}$, is the factorization of $F^\sigma(\underline{x}) - \lambda_i^{\widetilde{\sigma}}$ into irreducible polynomials in $k[\underline{x}]$.

It remains to ensure that for i fixed, the polynomials $Q_{ij}^{\widetilde{\sigma}}(\underline{x})$ are different, even up to non-zero multiplicative constants. For any two (distinct) polynomials $Q_{ij}(\underline{x})$, $Q_{ij'}(\underline{x})$, the matrix with rows the tuples of coefficients of the two polynomials has a 2×2-block with a non-zero determinant. Denote the product of all such determinants for all possible couples $(Q_{ij}(\underline{x}), Q_{ij'}(\underline{x}))$ by δ; it is a non-zero element of B'_E. Denote then by ν the norm of $\beta\delta$ relative to the extension E/K. As A is integrally closed, so is B and $\nu \in B$. Write it as $\nu = c_8/(c_6c_7)^\gamma$ with $c_8 \in A$ and $\gamma \in \mathbb{N}$. Condition $c_6^\sigma c_7^\sigma c_8^\sigma \neq 0$ implies $\beta_F^{\widetilde{\sigma}} \delta_F^{\widetilde{\sigma}} \neq 0$. Theorem 2.1 is finally established for $h_F = a_F \prod_{i=1}^8 c_i$.

Remark 2.6. The same proof, with the polynomial $\mathcal{F}(\underline{\lambda}, \underline{x})$ from §2.3.1 of the form $F(\underline{x}) - \lambda G(\underline{x})$ with $F(\underline{x}), G(\underline{x}) \in A[\underline{x}]$ and $\deg G \leq \deg F$, leads to the more general form of Theorem 2.1 for which indecomposable polynomials are replaced by indecomposable rational functions (in this case, "indecomposable" means not of the form $u(H(\underline{x}))$ with $H(\underline{x})$ and $u(t)$ rational functions and $\deg(u) \geq 2$ ([5])). A spectral value of a rational function $F(\underline{x})/G(\underline{x})$ is an element λ such that the polynomial $F(\underline{x}) - \lambda G(\underline{x})$ is reducible. Statements (1)–(3) from §1 remain true, except that the bound in Stein's inequality should be replaced by $(\deg(F))^2 - 1$ [2], [10]. More generally, one can take $\mathcal{F}(\underline{\lambda}, \underline{x})$ of the form $F(\underline{x}) - \lambda_1 G_1(\underline{x}) - \cdots - \lambda_s G_s(\underline{x})$ with $F(\underline{x}), G_1(\underline{x}), \ldots, G_s(\underline{x}) \in A[\underline{x}]$ and handle other situations studied in the literature.

3. An indecomposability criterion modulo p. In this section $n = 2$, A is a Dedekind domain and its fraction field K is assumed to be of characteristic 0. Fix also a non-zero prime ideal $\mathfrak{p}$ of A and assume its residue field $k = A/\mathfrak{p}$ is of characteristic $p > 0$. Denote by $\widetilde{x}$ the image of an element x under the reduction morphism $A \to k$. The situation "$A = \mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$" is typical.

Let $F(x, y) \in A[x, y]$ be an indecomposable polynomial in $\overline{K}[x, y]$ of degree $d \geq 1$, monic in y.

([5]) The degree of a rational function is the maximum of the degrees of its numerator and denominator.

Here is our strategy to guarantee indecomposability of $F(x,y)$ modulo $\mathfrak{p}$. Pick $\lambda^* \in A \setminus \mathrm{sp}(F)$ (using Stein's theorem, this can be done for λ^* not too large). Thus $F(x,y)-\lambda^*$ is irreducible in $\overline{K}[x,y]$. It follows from the classical Bertini–Noether theorem that if "$\mathfrak{p}$ is large enough", then the reduced polynomial $F(x,y)-\lambda^*$ modulo $\mathfrak{p}$ is absolutely irreducible. Therefore $F(x,y)$ is indecomposable modulo $\mathfrak{p}$ (as there is at least one non spectral value). However, the constants involved in the condition "$\mathfrak{p}$ large enough" are too large for a practical algorithmic use. We will follow an alternative approach, based on good reduction criteria for covers, and more precisely Zannier's criterion [14].

Consider the discriminant with respect to y of $F(x,y)-\lambda$:

$$\Delta_F(x,\lambda) = \mathrm{disc}_y(F(x,y)-\lambda).$$

Denote then the product of all distinct irreducible factors of $\Delta_F(x,\lambda)$ in $K(\lambda)[x]$ by $\Delta_F^{\mathrm{red}}(x,\lambda)$; more precisely, $\Delta_F^{\mathrm{red}}(x,\lambda)$ is defined by the following formula, which is also algorithmically more practical:

$$\Delta_F^{\mathrm{red}}(x,\lambda) = c(\lambda)\,\frac{\Delta_F(x,\lambda)}{\gcd(\Delta_F(x,\lambda),(\Delta_F)'_x(x,\lambda))}$$

where the g.c.d. is calculated in the ring $K(\lambda)[x]$ (using the Euclidean algorithm for example) and $c(\lambda) \in K(\lambda)$ is the rational function, defined up to some invertible element in A, that makes $\Delta_F^{\mathrm{red}}(x,\lambda)$ a primitive polynomial in $A[\lambda][x]$. Consider next the polynomial

$$\Delta_F(\lambda) = \mathrm{disc}_x(\Delta_F^{\mathrm{red}}(x,\lambda)).$$

We have $\Delta_F(\lambda) \in A[\lambda]$ and $\Delta_F(\lambda) \neq 0$. Finally, let $\Delta_0(\lambda) \in A[\lambda]$ be the coefficient of the highest monomial in $\Delta_F(x,\lambda)$ (viewed in $A[\lambda][x]$).

THEOREM 3.1. *Assume, in addition to $F(x,y)$ being indecomposable in $\overline{K}[x,y]$, that the reduced polynomial $\widetilde{\Delta}_0(\lambda)\widetilde{\Delta}_F(\lambda)$ is non-zero in $k[\lambda]$ and that $p > \deg_y(F)$. Then $\widetilde{F}(x,y)$ is indecomposable in $\overline{k}[x,y]$.*

The assumption $p > \deg_y(F)$ can be replaced by the weaker condition that p does not divide the order of the Galois group of $F(x,y)-\lambda$, viewed as a polynomial in $\overline{K(\lambda)}(x)$ (see footnote 8).

The assumptions of Theorem 3.1 may not be sufficient to guarantee the extra conclusions $\mathrm{sp}(\widetilde{F}) = \widetilde{\mathrm{sp}(F)}$ and $\mathrm{spdiv}(\widetilde{F}) = \widetilde{\mathrm{spdiv}(F)}$ from Theorem 2.1 (which may not even be well-defined). They, however, still imply that if $V_F \subset \mathbb{A}^1_A$ is the Zariski closed subset from §2.1, then the reduced Zariski closed subset $\widetilde{V}_F \subset \mathbb{A}^1_{\overline{k}}$ is proper and its points are the spectral values of $\widetilde{F}$: $\mathrm{sp}(\widetilde{F}) = \widetilde{V}_F(\overline{k})$.

REMARK 3.2 (an indecomposability test). Theorem 3.1 provides the following procedure to decide whether a non-constant polynomial $F(x,y) \in \mathbb{Q}[x,y]$ is indecomposable.

One may assume that $F(x,y) \in \mathbb{Z}[x,y]$ and $\deg_y(F) > 0$. Up to changing y to ay for some $a \in \mathbb{Z}$, one may also reduce to the case of $F(x,y)$ monic with respect to the reverse lexicographic order (for which $y > x$). Observe that the polynomial $\Delta_F(x,\lambda) = \mathrm{disc}_y(F(x,y) - \lambda)$ is non-zero in general (whether F is indecomposable or not): indeed, none of the roots y of $(\partial F/\partial y)(x,y)$, which are in $\overline{\mathbb{Q}(x)}$, can also be a root of $F(x,y) - \lambda$. Consequently, the polynomial $\Delta_0(\lambda)\Delta_F(\lambda)$ is non-zero in general. Pick a prime p satisfying the assumptions of Theorem 3.1: $p > \deg_y(F)$ and $\widetilde{\Delta}_0(\lambda)\widetilde{\Delta}_F(\lambda)$ is non-zero in $\mathbb{F}_p[\lambda]$. Test for decomposability of $\widetilde{F}(x,y)$ (from §4, it is sufficient to only consider decompositions over $\mathbb{F}_p$ instead of $\overline{\mathbb{F}}_p$). If $\widetilde{F}(x,y)$ is decomposable, then $F(x,y)$ is decomposable by Theorem 3.1. As we explain below, the converse also holds: if $\widetilde{F}(x,y)$ is indecomposable, then $F(x,y)$ is indecomposable.

Namely, if $F(x,y)$ is decomposable then $F(x,y)$ has a non-trivial decomposition $F(x,y) = u(H(x,y))$ with u and H with coefficients in $\overline{\mathbb{Q}}$ and even in $\mathbb{Q}$ (see §4). Furthermore, $F(x,y) \in \mathbb{Z}[x,y]$ being monic forces these coefficients to be in $\mathbb{Z}$. For one variable, this is explained in [5], and in general one can reduce to this case thanks to a Kronecker substitution. Specifically, one may assume that $H(x,y)$ is monic (with respect to the same order), and then so is u, and that $H(0,0) = 0$. Write $F(x,x^m) = u(H(x,x^m))$ with m large enough to have $F(x,x^m)$ and $H(x,x^m)$ monic. From [5, Theorem 2], $u(t)$ and $H(x,x^m)$ must have integral coefficients, and consequently so does $H(x,y)$ (for $m \gg 1$). Finally, reduction modulo p of $F(x,y) = u(H(x,y))$ provides a non-trivial decomposition of $\widetilde{F}(x,y)$.

Proof of Theorem 3.1. The prime ideal $\mathfrak{p} \subset A$ determines a discrete valuation v of K whose valuation ring is the localized ring $A_{\mathfrak{p}}$; the fraction field of $A_{\mathfrak{p}}$ and its residue field remain equal to K and k respectively. The hypotheses and conclusions from Theorem 3.1 are unchanged if A is replaced by $A_{\mathfrak{p}}$. The valued field (K,v) can then also be replaced by any finite extension of the completion K_v, and A by the new valuation ring; the discrete valuation v uniquely extends, the residue field is replaced by some (finite) extension of k, the indecomposability properties of $F(x,y)$ over K or over K_v are equivalent.

Thus we may and will assume that (K,v) is a complete discretely valued field, that A is its valuation ring (which is integrally closed) and that the field K and the residue field k contain as many (finitely many) algebraic elements over the original fields as necessary.

The polynomial $\Delta_F(x,\lambda)$ is in $A[x,\lambda]$ and its factorization into irreducible polynomials in $K(\lambda)[x]$ can be written

$$\Delta_F(x,\lambda) = \delta_0(\lambda)\prod_{i=1}^{s}\Delta_i(x,\lambda)^{\alpha_i}$$

where the polynomials $\Delta_i(x,\lambda)$ are in $A[x,\lambda]$, irreducible in $K(\lambda)[x]$, pairwise distinct (even up to some constant in K), and primitive in $A[\lambda][x]$, where $\delta_0(\lambda)\in A[\lambda]$ and where the α_i are positive integers. Then, up to some invertible element in A, we have

$$\Delta_F^{\mathrm{red}}(x,\lambda) = \prod_{i=1}^{s}\Delta_i(x,\lambda).$$

Also note that the polynomial $\Delta_0(\lambda)$ is a multiple in $A[\lambda]$ of the product of $\delta_0(\lambda)$ and the highest monomial coefficients $\delta_1(\lambda),\dots,\delta_s(\lambda)$ of the polynomials $\Delta_1(x,\lambda),\dots,\Delta_s(x,\lambda)$ (viewed in $A(\lambda)[x]$).

Pick next $\widetilde{\lambda}^*\in k$ such that $\widetilde{\Delta}_0(\widetilde{\lambda}^*)\widetilde{\Delta}_F(\widetilde{\lambda}^*)\neq 0$ in k, then lift it to some element $\lambda^*\in A$ such that $\lambda^*\notin \mathrm{sp}(F)$. This is possible in view of the preliminary remark.

The set of roots of $\Delta_F(x,\lambda^*)$ contains the set of finite ([6]) branch points of the cover of $\mathbb{P}^1_x$ ([7]) determined by the (absolutely irreducible) polynomial $F(x,y)-\lambda^*$. The preliminary remark makes it possible to assume that these roots are in K. Furthermore, as $\widetilde{\delta}_i(\widetilde{\lambda}^*)\neq 0$, we have $\delta_i(\lambda^*)\in A\setminus\mathfrak{p}$, $i=1,\dots,s$; therefore these roots are integral over A and so are in A.

As $\Delta_F(\lambda^*)\neq 0$, the roots of $\Delta_F^{\mathrm{red}}(x,\lambda^*)$ in $\overline{K}$ are distinct, and as $\delta_0(\lambda^*)\neq 0$, they are the roots of $\Delta_F(x,\lambda^*)$. As $\widetilde{\Delta}_0(\widetilde{\lambda}^*)\neq 0$, $\widetilde{\Delta}_F(x,\widetilde{\lambda}^*)$ is not the zero polynomial. As $\widetilde{\Delta}_F(\widetilde{\lambda}^*)\neq 0$, the roots of $\widetilde{\Delta}_F^{\mathrm{red}}(x,\widetilde{\lambda}^*)$, which are those of the polynomial $\widetilde{\Delta}_F(x,\widetilde{\lambda}^*)$, are distinct. Thus we conclude that the distinct roots of the polynomial $\Delta_F(x,\lambda^*)$, and *a fortiori* the branch points of the cover considered above, have distinct reductions modulo the ideal $\mathfrak{p}$.

It follows from standard results on good reduction of covers, and more precisely here, from the main theorem of [14] that, under the assumption $p>\deg_y(F)$ ([8]), $\widetilde{F}(x,y)-\widetilde{\lambda}^*$ is absolutely irreducible. Hence $\widetilde{F}(x,y)$ is indecomposable in $\overline{k}[x,y]$. ∎

([6]) That is, distinct from the point at infinity.

([7]) The subscript "x" indicates that the cover is induced by the correspondence $(x,y)\mapsto x$. In fact, the problem is symmetric in the variables x and y which can be switched in our statement.

([8]) It suffices to assume that p does not divide the order of the Galois group of $F(x,y)-\lambda^*$, which divides the order of the Galois group of $F(x,y)-\lambda$, which itself divides $(\deg_y(F))!$.

4. Indecomposability over K versus $\overline{K}$

4.1. *Statements* (for $n \geq 2$ variables). The indecomposability property over an algebraically closed field, which we recalled in §1, can in fact be defined over an arbitrary field: just require that the polynomials $u(t)$ and $H(\underline{x})$ involved have their coefficients in the field in question. The results below identify the only cases where the property is not the same over some field K and over some extension E. The following result handles the case where E/K is purely inseparable, which was missing in the literature.

PROPOSITION 4.1. *Let E/K be a purely inseparable algebraic field extension of characteristic $p > 0$ and $F(\underline{x}) \in K[\underline{x}]$. Assume $F(\underline{x})$ is not of the form $bG(\underline{x})^p + c$ with $G(\underline{x}) \in E[\underline{x}]$ and $b, c \in K$. Then $F(\underline{x})$ is indecomposable in $K[\underline{x}]$ if and only if it is indecomposable in $E[\underline{x}]$.*

If $E = \overline{K}$, the assumption on $F(\underline{x})$ merely says that $F(\underline{x})$ is not a pth power in $\overline{K}[\underline{x}]$, which in turn is equivalent to at least one exponent in $F(\underline{x})$ not being a multiple of p. Clearly this assumption cannot be removed: for example, if $\alpha \in \overline{K} \setminus K$ but $\alpha^p = a \in K$ then $x^p + ay^p$ is indecomposable in $K[\underline{x}]$ but decomposable in $\overline{K}[\underline{x}]$.

In [1, Proposition 1], Arzhantsev and Petravchuk show the equivalence from Proposition 4.1 without any assumption on $F(\underline{x})$, but in the case of a separable extension E/K (possibly of positive transcendence degree). As any extension is a purely inseparable algebraic extension of some separable extension, conjoining their result with ours shows that, under the assumption on $F(\underline{x})$ from Proposition 4.1, the equivalence holds for an arbitrary extension E/K. We can be more precise.

THEOREM 4.2. *Let E/K be a field extension and $F(\underline{x}) \in K[\underline{x}]$ be a non-constant polynomial. Then the following are equivalent*:

(i) *$F(\underline{x})$ is indecomposable in $K[\underline{x}]$ but decomposable in $E[\underline{x}]$.*
(ii) (a) *K is of characteristic $p > 0$ and E/K is inseparable*,
(b) *$F(\underline{x}) = bG(\underline{x})^p + c$ for some $G(\underline{x}) \in E[\underline{x}]$ and $b, c \in K$*,
(c) *$G(\underline{x})^p$ is indecomposable in $K[\underline{x}]$.*

Condition (ii)(c) implies that $G(\underline{x})$ is not of the form $u(H(\underline{x}))$ with $u \in E[t]$, $H(\underline{x}) \in E[\underline{x}]$, $\deg(u) \geq 2$ and both $u(t)^p \in K[t]$ and $H(\underline{x})^p \in K[\underline{x}]$. But there are other possible polynomials that should be excluded whose description is more intricate.

4.2. *Proofs*

Proof of Proposition 4.1. The converse part is obvious. For the direct part, assume $F(\underline{x})$ is decomposable in $E[\underline{x}]$. Then it is decomposable over some finite extension of K contained in E, which admits a finite system of generators $\alpha_1, \ldots, \alpha_s$ with irreducible polynomial over K of the form

$x^{p^n} - a$ with $a \in K$. The multiplicativity of the degree and of the separable degree imply that the extensions $K(\alpha_1, \ldots, \alpha_{j+1})/K(\alpha_1, \ldots, \alpha_j)$ are purely inseparable for $j = 1, \ldots, s-1$. By induction one reduces to the case $s = 1$, and then a new induction reduces to the case $E = K(\alpha)$ with $\alpha^p = a \in K \setminus K^p$.

Assume $F(\underline{x}) = h(G(\underline{x}))$ with $h(t) \in K(\alpha)[t]$ such that $\deg(h) \geq 2$ and $G(\underline{x}) \in K(\alpha)[\underline{x}]$. We deduce

$$F(\underline{x})^p = {}^p h(G(\underline{x})^p)$$

where, if $h(t) = \sum_{i=0}^{\deg(h)} h_i t^i$, we set ${}^p h(t) = \sum_{i=0}^{\deg(h)} h_i^p t^i$. As ${}^p h(t) \in K[t]$ and $G(\underline{x})^p \in K[\underline{x}]$ (since $y^p \in K$ for all $y \in K(\alpha)$), this shows that the field $K(F(\underline{x}), G(\underline{x})^p)$ is of transcendence degree 1 over K. From Gordan's Theorem [12, §1.2, Th. 3], there exists $\theta(\underline{x}) \in K(\underline{x})$ such that

$$K(F(\underline{x}), G(\underline{x})^p) = K(\theta(\underline{x})).$$

Furthermore from [12, §1.2, Th. 4], one may assume that $\theta(\underline{x}) \in K[\underline{x}]$. Thus

$$\begin{cases} F(\underline{x}) = u(\theta(\underline{x})) & \text{with } u(t) \in K(t), \\ G(\underline{x})^p = v(\theta(\underline{x})) & \text{with } v(t) \in K(t). \end{cases}$$

As $F(\underline{x})$ and $G(\underline{x})^p$ are polynomials, $u(t), v(t)$ are necessarily in $K[t]$. It follows from the indecomposability of $F(\underline{x})$ over K that $\deg(u) = 1$, which gives $G(\underline{x})^p = w(F(\underline{x}))$ for some $w \in K[t]$. But then $G(\underline{x})^p = w \circ h(G(\underline{x}))$, which, since $G(\underline{x})$ is non-constant, amounts to $T^p = w \circ h(T)$ where T is an indeterminate. As $\deg(h) \geq 2$ and p is a prime, we have $\deg(w) = 1$ and $\deg(h) = p$, which gives $F(\underline{x}) = bG(\underline{x})^p + c$ for some $b, c \in K$.

Note that because of the inductive process, the conclusion "$b, c \in K$" should really be that b, c are in the first subfield of the initial reduction. But $F(\underline{x})$ being in $K[\underline{x}]$ then implies that $b\gamma^p \in K$ for some non-zero $\gamma \in E$ and $bG(\underline{0})^p + c \in K$. Up to changing $G(\underline{x})$ to $\gamma^{-1}G(\underline{x}) - \gamma^{-1}G(\underline{0})$, one can indeed conclude that $b, c \in K$ in the general situation. ∎

Proof of Theorem 4.2. (i)⇒(ii): If K_s/K is the maximal separable extension contained in E, then, from the Arzhantsev–Petravchuk result, $F(\underline{x})$ is indecomposable in $K_s[\underline{x}]$. In particular $E \neq K_s$, which gives (ii)(a). Proposition 4.1 then provides condition (ii)(b) except that b and c are *a priori* in K_s, but using again the final note of the proof of Proposition 4.1, one can indeed choose $b, c \in K$. Condition (ii)(c) then readily follows from (ii)(b) and the indecomposability of $F(\underline{x})$ in $K[\underline{x}]$. The other implication (ii)⇒(i) is clear. ∎

4.3. *One variable.* In Proposition 4.1, $F(\underline{x})$ is a polynomial in two variables or more. In one variable, the indecomposability definition should be modified (for otherwise it is trivial): a polynomial $F(x) \in k[x]$ is said to be

indecomposable in $k[x]$ if it is not of the form $u(H(x))$ with $H(x) \in k[x]$ and $u \in k[t]$ with $\deg(u) \geq 2$ and $\deg(H) \geq 2$.

PROPOSITION 4.3. *The conclusion of Proposition* 4.1 *holds for one variable polynomials.*

Proof. The same proof can be used as for Proposition 4.1. It leads to

$$\begin{cases} F(x) = u(\theta(x)) & \text{with } u(t) \in K[t], \\ G(x)^p = v(\theta(x)) & \text{with } v(t) \in K[t]. \end{cases}$$

But from the indecomposability of $F(\underline{x})$ over K, we now deduce that $\deg(u) = 1$ or $\deg(\theta) = 1$.

The case $\deg(u) = 1$ is handled as before. In the other case, we deduce from $\deg(\theta) = 1$ that $K(F(x), G(x)^p) = K(x)$, which implies that $K(\alpha)(h(G(x)), G(x)^p) = K(\alpha)(x)$ and so that

$$K(\alpha)(x) \subset K(\alpha)(G(x)),$$

which forces $\deg(G) = 1$ and contradicts the decomposability assumption in one variable made at the beginning of the proof. ∎

5. Counting indecomposable polynomials over finite fields. For each integer $d \geq 1$, denote the number of polynomials in $\mathbb{F}_q[\underline{x}]$ ($\underline{x} = (x_1, \ldots, x_n)$) of degree d by N_d. We have

$$N_d = \begin{cases} (q^{\binom{n+d-1}{n-1}} - 1) \cdot q^{\binom{n+d-1}{n}} & \text{for general } n, \\ q^{(d+1)(d+2)/2}(1 - q^{-d-1}) & \text{for } n = 2, \\ (q-1)q^d & \text{for } n = 1. \end{cases}$$

Denote the number of those polynomials which are indecomposable (resp. decomposable) by I_d (resp. D_d). We have $N_d = I_d + D_d$.

We will study separately the case of $n \geq 2$ variables (§5.1–§5.4) and the case $n = 1$ (§5.5).

5.1. *Main result.* From §5.1 to §5.4, we assume $n \geq 2$.

THEOREM 5.1.

(a) *I_d/N_d tends to* 1 *when $d \to \infty$ with q fixed, and when $q \to \infty$ with d fixed.*

(b) *If d is a product of at most two prime numbers $p \leq p'$, then either*

- *$d = p$ and $D_d = q^d(q^n - 1)$, or*
- *$d = p^2$ and $D_d = q^{p-1}N_p + (q^d - q^{2p-1})(q^n - 1)$, or*
- *$d = pp'$ with $p < p'$ and*

$$D_d = q^{p-1}N_{p'} + q^{p'-1}N_p + (q^d - 2q^{p+p'-1})(q^n - 1).$$

(c) *Assume $n = 2$. If d is the product of at least three primes, then*

$$\left|\frac{D_d}{N_d} - \alpha_d\right| \le \alpha_d\beta_d \quad \textit{where} \quad \begin{cases} \alpha_d = \dfrac{q^{\ell-1+(d/\ell+1)(d/\ell+2)/2}}{q^{(d+1)(d+2)/2}}, \\ \beta_d = \dfrac{d}{q^{d/\ell}}, \end{cases}$$

and $\ell > 1$ is the first (hence prime) divisor of d.

A version of statement (c) in the general case of n variables is given in [8]. For $n = 2$, his first order estimate for D_d/N_d is the same as ours, that is, α_d; his error term is improved by a factor $O(q)$.

5.2. *An induction formula.* Let K be an arbitrary field. Let $F = u \circ H$ be a decomposition of $F \in K[\underline{x}]$ with $u \in K[t]$, $\deg u \ge 2$, and $H \in K[\underline{x}]$. We say that $F = u \circ H$ is a *normalized decomposition* if H is indecomposable, monic (i.e. the coefficient of the leading term of a chosen order is 1) and its constant term equals zero. Given a decomposition $F = u \circ H$, there exists an associated normalized decomposition $F = u' \circ H'$. The following lemma shows it is unique.

LEMMA 5.2. *Let $F = u \circ H = u' \circ H'$ be two normalized decompositions of $F \in K[\underline{x}]$. Then $u = u'$ and $H = H'$.*

Proof. It follows from $u(H) - u'(H') = 0$ that H and H' are algebraically dependent over K. By Gordan's theorem [12, §1.2, Theorems 3 and 4] (already used in §4.2), there exists a polynomial $\theta(\underline{x}) \in K[\underline{x}]$ such that $K[\theta] = K[H, H']$. That is, there exist $v, v' \in K[t]$ such that $H = v(\theta)$ and $H' = v'(\theta)$. As the two decompositions of F are normalized, H and H' are indecomposable, so $\deg v = \deg v' = 1$, and so using the other normalization conditions, we obtain $H = H'$. Finally, it follows from $u(H) = u'(H)$ that $u = u'$. ∎

COROLLARY 5.3 (induction formula). *With notation as in* §5.1, *we have*

$$I_d = N_d - \sum_{d' \mid d,\, d' < d} q^{d/d'-1} \times I_{d'}.$$

Proof. Let $d' \ge 1$ be a divisor or d. There are $(q-1)q^{d/d'}$ polynomials $u \in \mathbb{F}_q[t]$ of degree d/d' and $I_{d'}/q(q-1)$ normalized indecomposable polynomials $H \in \mathbb{F}_q[\underline{x}]$ of degree d'. The formula follows, as from Lemma 5.2, every polynomial F counted by D_d can be uniquely written as $F = u \circ H$ with u and H as above for some integer d' such that $d' \mid d$, $d' < d$. ∎

Combined with $I_1 = N_1 = q(q^n - 1)$ this formula provides an algorithm to compute I_d and D_d, which is convenient for small d.

5.3. *Proof of Theorem 5.1(a) and (b).* The formulas in (b) directly follow from Corollary 5.3. If $d = p$ is a prime number, we have $D_p = q^{p-1}I_1 = q^{p-1}N_1 = q^p(q^n - 1)$. If $d = p^2$ then

$$D_d = q^{p-1}I_p + q^{p^2-1}I_1 = q^{p-1}(N_p - q^p(q^n - 1)) + q^{p^2}(q^n - 1).$$

Computations are similar for $d = pp'$. To prove (a) we write

$$N_d - I_d = D_d = \sum_{d'|d,\, d'<d} q^{d/d'} I_{d'} \le \sum_{d'|d,\, d'<d} q^{d/d'} N_{d'}.$$

The sum has at most d terms and each is $\le q^d N_{d/2}$, whence

$$1 - \frac{I_d}{N_d} \le dq^d \frac{N_{d/2}}{N_d},$$

and the announced result follows, as the right-hand side term tends to 0 in the two situations considered in the statement of Theorem 5.1(a). ∎

5.4. *Proof of Theorem 5.1(c).* In this subsection we assume that $n = 2$ and that d has at least three prime divisors.

5.4.1. *A technical lemma*

LEMMA 5.4. *Let $b(d) = \frac{1}{2}(d+1)(d+2)$. Let $\ell > 1$ be the first divisor of d and $\ell' > \ell$ be the second divisor of d. Let $\lambda \ge \ell'$ be a divisor of d and $\ell'' > 1$ be the first divisor of d/ℓ. Then*

(1) $b(d/\ell') + \ell' \ge b(d/\lambda) + \lambda$,
(2) $b(d/\ell) + \ell - d/\ell \ge b(d/\ell') + \ell'$,
(3) $b(d/\ell) + 1 - d/\ell \ge b(d/\ell\ell'') + \ell''$.

Proof. (1) We have

$$b(d/\ell') + \ell' - b(d/\lambda) - \lambda = \frac{1}{2}\left(\frac{d}{\ell'} - \frac{d}{\lambda}\right)\left(\frac{d}{\ell'} + \frac{d}{\lambda} + 3 - 2\,\frac{\ell'\lambda}{d}\right) \ge 0,$$

because $d/\ell' - d/\lambda \ge 0$ and

$$\frac{d}{\ell'} + \frac{d}{\lambda} + 3 - 2\frac{\ell'\lambda}{d} \ge \frac{d}{\ell'} + 4 - 2\ell' \ge 0,$$

as d has at least three prime divisors.

(2) We have $\ell\ell' \le d$ so $\ell' - \ell \le d/\ell$. Moreover, $d/\ell' \le d/\ell - 2$ and for all $d \ge 6$ we have $b(d/\ell') \le b(d/\ell - 2)$. Hence

$$b(d/\ell) - b(d/\ell') + \ell - \ell' - d/\ell \ge b(d/\ell) - b(d/\ell - 2) - 2d/\ell = 1.$$

(3) If we set $\delta = d/\ell$ then

$$b(\delta) + 1 - \delta - b(\delta/\ell'') - \ell'' = \frac{1}{2}\left(\delta - \frac{\delta}{\ell''}\right)\left(\delta + \frac{\delta}{\ell''} - 2\right) + \frac{1}{2}\left(3\delta - 5\,\frac{\delta}{\ell''} - 2\ell'' + 2\right).$$

Now $\delta - \delta/\ell'' \geq 0$, $\delta + \delta/\ell'' - 2 \geq 0$ and as δ has at least two prime divisors, it follows that $u(\ell'') = 3\delta - 5\delta/\ell'' - 2\ell'' + 2 \geq u(2) = \delta/2 - 2 \geq 0$. ∎

5.4.2. *An upper bound for D_d.* Using the notation of Lemma 5.4, we have

$$\begin{aligned}
D_d &= q^{\ell-1} I_{d/\ell} + \sum_{\lambda \mid d,\, \lambda > \ell} q^{\lambda-1} I_{d/\lambda} \quad \text{(Corollary 5.3)} \\
&\leq q^{\ell-1} N_{d/\ell} + \sum_{\lambda \mid d,\, \lambda > \ell} q^{\lambda-1} N_{d/\lambda} \\
&\leq q^{b(d/\ell)+\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right) + \sum_{\lambda \mid d,\, \lambda > \ell} q^{\lambda-1} q^{b(d/\lambda)} \\
&\qquad\qquad \text{(explicit formula for } N_{d/\lambda}) \\
&\leq q^{b(d/\ell)+\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right) + (d-1) q^{b(d/\ell')+\ell'-1} \quad \text{(Lemma 5.4(1))} \\
&\leq q^{b(d/\ell)+\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right)\left(1 + \frac{d}{q^{b(d/\ell)-b(d/\ell')+\ell-\ell'}}\right) \\
&\qquad\qquad \left(\text{because } \frac{d-1}{1-q^{-d/\ell-1}} \leq d\right) \\
&\leq q^{b(d/\ell)+\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right)\left(1 + \frac{d}{q^{d/\ell}}\right) \quad \text{(Lemma 5.4(2))}.
\end{aligned}$$

5.4.3. *A lower bound for D_d.* Start from $D_d \geq q^{\ell-1} I_{d/\ell}$. Then use §5.4.2 (or the formulas already proved from Theorem 5.1(b)) to bound $I_{d/\ell} = N_{d/\ell} - D_{d/\ell}$ from below. We obtain

$$\begin{aligned}
D_d &\geq q^{\ell-1} \times \left(q^{b(d/\ell)}\left(1 - \frac{1}{q^{d/\ell+1}}\right)\right. \\
&\qquad \left. - q^{b(d/\ell\ell'')+\ell''-1}\left(1 - \frac{1}{q^{d/\ell\ell''+1}}\right)\left(1 + \frac{d/\ell}{q^{d/\ell\ell''}}\right)\right) \\
&\geq q^{\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right)(q^{b(d/\ell)} - 2q^{b(d/\ell\ell'')+\ell''-1}) \quad \left(\text{because } \frac{d/\ell}{q^{d/\ell\ell''}} \leq 1\right) \\
&= q^{\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right) q^{b(d/\ell)}\left(1 - \frac{2}{q^{b(d/\ell)-b(d/\ell\ell'')+1-\ell''}}\right) \\
&\geq q^{b(d/\ell)+\ell-1}\left(1 - \frac{1}{q^{d/\ell+1}}\right)\left(1 - \frac{2}{q^{d/\ell}}\right) \quad \text{(Lemma 5.4(3))}.
\end{aligned}$$

5.4.4. *Final estimate for D_d/N_d.* The upper and lower bounds for D_d yield the inequalities

$$\frac{q^{b(d/\ell)+\ell-1}}{q^{b(d)}} \times \frac{1-q^{-d/\ell-1}}{1-q^{-d-1}} \times \left(1-\frac{2}{q^{d/\ell}}\right) \le \frac{D_d}{N_d} \le \frac{q^{b(d/\ell)+\ell-1}}{q^{b(d)}} \times \frac{1-q^{-d/\ell-1}}{1-q^{-d-1}} \times \left(1+\frac{d}{q^{d/\ell}}\right),$$

a little more precise than the announced statement. ∎

5.5. *One variable.* Here we assume $n = 1$. For polynomials in one variable, we use the definition of indecomposability given in §4.3.

5.5.1. *Main result*

THEOREM 5.5. *Assume q and d are relatively prime.*

(a) *If d is a product of at most two prime numbers $p \le p'$, then either*

- *$d = p$ and $D_d = 0$, or*
- *$d = p^2$ and $D_d = \frac{q-1}{q} q^{2p}$, or*
- *$d = pp'$ with $p < p'$ and*

$$2\,\frac{q-1}{q}\,q^{p+p'} - q^5 \le D_d \le 2\,\frac{q-1}{q}\,q^{p+p'}.$$

(b) *Assume d is the product of at least three prime numbers. Let $\ell > 1$ be the first divisor of d and $\ell' > \ell$ be its second divisor. Then*

$$\frac{d}{2\ell}\,\frac{1}{q^{d/\ell-d/\ell^2-\ell+1}} \le \frac{D_d}{N_d} - \alpha_d \le \frac{d-2}{2q^{\ell+d/\ell-\ell'-d/\ell'}} \quad \text{where} \quad \alpha_d = \frac{2}{q^{d-\ell-d/\ell+1}}.$$

As a consequence, I_d/N_d tends to 1 when $d \to \infty$ with q fixed, and $q \to \infty$ with d fixed.

Theorem 5.5 fails if the assumption $(q, d) = 1$ is removed. For example for $q = 2$ and d even one can compute that $D_d/N_d \sim 3 \cdot 2^{-d/2}$ while $\alpha_d = 4 \cdot 2^{-d/2}$ in this case.

From now on we assume q and d are relatively prime. The rest of the paper is devoted to the proof of Theorem 5.5. Our strategy is similar to the one used for $n \ge 2$. We view the set $\mathcal{D}_d$ of all decomposable polynomials $f(x) \in \mathbb{F}_q[x]$ of degree d as the union of smaller sets which we will estimate. More specifically, we write

$$\mathcal{D}_d = \bigcup_{\lambda \mid d,\ \ell \le \lambda \le d/\ell} \mathcal{D}_{\lambda, d/\lambda}$$

where $\mathcal{D}_{\lambda,d/\lambda} \subset \mathcal{D}_d$ is the subset of all $f(x)$ which admit a decomposition $f = u \circ v$ with $u, v \in \mathbb{F}_q[x]$, $\deg u = \lambda \ge 2$, $\deg v = d/\lambda \ge 2$, v monic and

of constant term equal to 0. A difference with the case $n \geq 2$ is that we do *not* have a partition.

5.5.2. *1st stage: upper bounds.* (Assumption $(q,d)=1$ is not used in this subsection.) For every divisor $\lambda \geq 1$ of d, denote the cardinality of $\mathcal{D}_{\lambda,d/\lambda}$ by $D_{\lambda,d/\lambda}$. We have

$$D_{\lambda,d/\lambda} \leq N_\lambda \frac{N_{d/\lambda}}{q(q-1)} = \frac{q-1}{q}\, q^{\lambda+d/\lambda}.$$

If $\ell > 1$ is the first divisor of d and $\ell' > \ell$ the second divisor, we have

$$D_d \leq \sum_{\lambda|d,\, \ell\leq\lambda\leq d/\ell} D_{\lambda,d/\ell} \leq \frac{q-1}{q} \sum_{\lambda|d,\, \ell\leq\lambda\leq d/\ell} q^{\lambda+d/\lambda}.$$

The idea is that the main contribution comes from $D_{\ell,d/\ell}$ and $D_{d/\ell,\ell}$.

If d is the product of exactly two prime numbers ℓ and d/ℓ, then these are the only contributions and we have the desired upper bound. Otherwise we write $\lambda + d/\lambda \leq \ell' + d/\ell'$ to bound the extra terms and obtain

$$D_d \leq \frac{q-1}{q}\, q^{\ell+d/\ell}\left(2 + \frac{d-2}{q^{\ell+d/\ell-\ell'-d/\ell'}}\right),$$

which yields all announced upper bounds in Theorem 5.5. We also deduce this practical bound:

$$D_d \leq d\,\frac{q-1}{q}\, q^{\ell+d/\ell}$$

(as $\ell + d/\ell - \ell' - d/\ell' \geq 1$).

5.5.3. *2nd stage: uniqueness results.* We will use Ritt's theorems to control the number of possible decompositions of a given polynomial.

PROPOSITION 5.6. *Let K be a field and $f \in K[x]$ be a polynomial of degree $d > 0$. Assume the characteristic p of K does not divide d. Suppose we have two decompositions $f = u \circ v = u' \circ v'$ of f with*

- *u, v, u', v' indecomposable,*
- *$\deg u = \deg u' \geq 2$, $\deg v = \deg v' \geq 2$,*
- *v, v' monic with a zero constant term.*

Then $u = u'$ and $v = v'$.

Proof. This follows from the first Ritt theorem [12, §1.3, Theorem 7], which more generally describes in which cases an equality $G_1 \circ \cdots \circ G_r = H_1 \circ \cdots \circ H_s$ with G_i, H_j indecomposable of degree > 1 may hold. ∎

As an immediate consequence, we obtain the case $d = p^2$ of Theorem 5.5(a): namely, we have $D_{p^2} = D_{p,p} = \frac{q-1}{q} q^{2p}$.

5.5.4. *3rd stage: lower bounds for $D_{d/\ell,\ell}$ and $D_{\ell,d/\ell}$.*

LEMMA 5.7. *Assume d is not a prime number. Then*

$$D_{\ell,d/\ell} \geq \frac{q-1}{q}\, q^{\ell+d/\ell}\left(1 - \frac{d/\ell}{q^{d/\ell-d/\ell^2-\ell+1}}\right),$$

and the same inequality holds with $D_{\ell,d/\ell}$ replaced by $D_{d/\ell,\ell}$.

Proof. We only give the proof for $D_{\ell,d/\ell}$ as computations for $D_{d/\ell,\ell}$ are the same. In $\mathcal{D}_{\ell,d/\ell}$ we will only count those polynomials f which decompose as $f = u \circ v$ with u and v as in Proposition 5.6. Then we obtain

$$\begin{aligned} D_{\ell,d/\ell} &\geq \frac{1}{q(q-1)}\, I_\ell \cdot I_{d/\ell} \\ &\geq \frac{1}{q(q-1)}\, N_\ell\,(N_{d/\ell} - D_{d/\ell}) \quad (D_\ell = 0 \text{ as } \ell \text{ is prime}) \\ &= \frac{1}{q(q-1)}\,(q-1)q^\ell((q-1)q^{d/\ell} - D_{d/\ell}) \\ &= \frac{q-1}{q}\, q^{\ell+d/\ell}\left(1 - \frac{D_{d/\ell}}{(q-1)q^{d/\ell}}\right). \end{aligned}$$

If d is the product of exactly two primes then $D_{d/\ell} = 0$ and

$$(*) \qquad D_{\ell,d/\ell} \geq \frac{q-1}{q}\, q^{\ell+d/\ell},$$

which in this case is better than the announced result.

If d is the product of at least three primes, use the practical upper bound for D_d obtained in Stage 1 to write $D_{d/\ell} \leq \frac{d}{\ell}\,\frac{q-1}{q}\, q^{\ell+d/\ell^2}$ and deduce

$$\begin{aligned} D_{\ell,d/\ell} &\geq \frac{q-1}{q}\, q^{\ell+d/\ell}\left(1 - \frac{(d/\ell)\frac{q-1}{q}\, q^{\ell+d/\ell^2}}{(q-1)q^{d/\ell}}\right) \\ &= \frac{q-1}{q}\, q^{\ell+d/\ell}\left(1 - \frac{d/\ell}{q^{d/\ell-d/\ell^2-\ell+1}}\right). \ \blacksquare \end{aligned}$$

5.5.5. *Estimating the multiple decompositions.* Next we write

$$D_d \geq \operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cup \mathcal{D}_{d/\ell,\ell}) = D_{\ell,d/\ell} + D_{d/\ell,\ell} - \operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}).$$

In order to estimate D_d we need to estimate the intersection.

LEMMA 5.8. *We have*

$$\begin{cases} \operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}) \leq \dfrac{d}{\ell}\, q^{d/\ell^2+2\ell-1}, \\ D_d \geq 2\,\dfrac{q-1}{q}\, q^{\ell+d/\ell}\left(1 - \dfrac{2d}{\ell}\,\dfrac{1}{q^{d/\ell-d/\ell^2-\ell+1}}\right). \end{cases}$$

The lower bound for D_d is the remaining inequality to be proved in Theorem 5.5(b). The more precise inequality $(**)$ in the proof below will complete the proof of Theorem 5.5(a) in the special case $d = pp'$.

Proof of Lemma 5.8. (a) If $\gcd(\ell, d/\ell) = 1$ then $\operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}) \le q^5$.

Indeed, let $f \in \mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}$ and let $f = u \circ v$ be a decomposition with $\deg u = \ell$ and $\deg v = d/\ell$. We follow Ritt's second theorem (see [12, §1.4, Theorem 8] and the notation there). The hypotheses of that result are satisfied because the derivative u' of u is non-zero; otherwise $f' = 0$, and so $f \in \mathbb{F}_q[x^p]$ and the characteristic p of $\mathbb{F}_q$ divides $d = \deg f$. In the first case of Ritt's second theorem we have $L_1 \circ u = x^r P(x)^n$ and $v \circ L_2 = x^n$ (where $r \ge 0$, $P \in \mathbb{F}_q[x]$ and L_1, L_2 are linear functions). In our situation we get $n = d/\ell$ and $\ell = r + (d/\ell)\deg P$. Then $\deg P = (\ell^2 - \ell r)/d \le \ell^2/d < 1$, so $\deg P = 0$, $L_1 \circ u = x^\ell$ and $v \circ L_2 = x^{d/\ell}$. Considering all possible linear functions yields at most $(q-1)^2 q^2$ such decompositions. In the second case of Ritt's second theorem we have $L_1 \circ u = D_m(x, a^n)$ and $v \circ L_2 = D_n(x, a)$, $a \in \mathbb{F}_q$ (where $D_n(x, a)$ denote Dickson's polynomials). We here obtain $m = \ell$ and $n = d/\ell$. Considering all possible linear functions and all $a \in \mathbb{F}_q$ yields at most $(q-1)^2 q^3$ such decompositions. Finally, we obtain

$$(**) \qquad \operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}) \le (q-1)^2 q^2 + (q-1)^2 q^3 \le q^5.$$

(b) If $\gcd(\ell, d/\ell) \ne 1$ then $\operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}) \le \frac{d}{\ell}\, q^{d/\ell^2 + 2\ell - 1}$.

Indeed, let $f \in \mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}$ and let $f = u \circ v$ be a decomposition with $\deg u = \ell$ and $\deg v = d/\ell$. By Ritt's first theorem and because $\gcd(\ell, d/\ell) \ne 1$, either u or v is decomposable. But as ℓ is a prime, $\mathcal{D}_\ell$ is empty and so $v \in \mathcal{D}_{d/\ell}$. Thus we obtain

$$\begin{aligned}
\operatorname{card}(\mathcal{D}_{\ell,d/\ell} \cap \mathcal{D}_{d/\ell,\ell}) &\le N_\ell \, \frac{1}{q(q-1)} \, D_{d/\ell} \\
&\le \frac{1}{q(q-1)} \, (q-1) q^\ell \, \frac{d}{\ell} \, q^{\ell + d/\ell^2} \qquad \text{(end of §5.5.2)} \\
&\le \frac{d}{\ell} \, q^{d/\ell^2 + 2\ell - 1}.
\end{aligned}$$

The conclusion follows, as for all $d > 6$ we have $d/\ell^2 + 2\ell - 1 \ge 5$. ∎

Acknowledgments. We wish to thank Joachim von zur Gathen for interesting discussions in Lille and in Bonn.

References

[1] I. V. Arzhantsev and A. P. Petravchuk, *Closed polynomials and saturated subalgebras of polynomial algebras*, Ukraïn. Mat. Zh. 59 (2007), 1783–1790.

[2] A. Bodin, *Reducibility of rational fractions in several variables*, Israel J. Math. 164 (2008), 333–348.

[3] L. Busé, G. Chèze and S. Najib, *Noether's forms for the study of non-composite rational functions and their spectrum*, preprint.
[4] G. Chèze and S. Najib, *Indecomposable polynomials via jacobian matrix*, preprint.
[5] A. Dujella and I. Gusić, *Indecomposability of polynomials and related diophantine equations*, Quart. J. Math. Oxford Ser. 498 (2005), 173–199.
[6] M. Fried and M. Jarden, *Field Arithmetic*, Ergeb. Math. Grenzgeb. 11, Springer, 2004.
[7] J. von zur Gathen, *Counting reducible and singular bivariate polynomials*, Finite Fields Appl. 14 (2008), 944–978.
[8] —, *Counting decomposable multivariate polynomials*, preprint.
[9] —, *Counting decomposable univariate polynomials*, preprint.
[10] D. Lorenzini, *Reducibility of polynomials in two variables*, J. Algebra 156 (1993), 65–75.
[11] S. Najib, *Une généralisation de l'inégalité de Stein–Lorenzini*, ibid. 292 (2005), 566–573.
[12] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia Math. Appl. 77, Cambridge Univ. Press, 2000.
[13] Y. Stein, *The total reducibility order of a polynomial in two variables*, Israel J. Math. 68 (1989), 109–122.
[14] U. Zannier, *On the reduction modulo p of an absolutely irreducible polynomial $f(x, y)$*, Arch. Math. (Basel) 68 (1997), 129–138.

Laboratoire Paul Painlevé, Mathématiques
Université Lille 1
59655 Villeneuve d'Ascq Cedex, France
E-mail: Arnaud.Bodin@math.univ-lille1.fr
Pierre.Debes@math.univ-lille1.fr
Salah.Najib@math.univ-lille1.fr

Received on 22.11.2008 (5867)