ACTA ARITHMETICA
114.2 (2004)

Sur le spectre d'un polynôme à plusieurs variables

par

Salah Najib (Lille)

Dans toute la suite K désigne un corps commutatif de caractéristique nulle, $\overline{K}$ une clôture algébrique de K et $\underline{X} = (X_1, \ldots, X_n)$ $(n \geq 2)$ des indéterminées algébriquement indépendantes sur K, que nous noterons X et Y pour $n = 2$.

Cet article, dans la suite de travaux de Bertini, Krull et Stein, a pour objet de montrer que pour tout ensemble $\{a_1, \ldots, a_s\}$ d'éléments distincts de K et pour tous entiers $\varrho_1, \ldots, \varrho_s$ positifs non nuls, il existe un polynôme $P(\underline{X})$ dans $K[\underline{X}]$ non composé tel que $P(\underline{X}) - a_i$ ait exactement $\varrho_i + 1$ facteurs irréductibles dans $\overline{K}[\underline{X}]$, $i = 1, \ldots, s$, et $P(\underline{X}) - \lambda$ soit irréductible pour tout $\lambda \notin \{a_1, \ldots, a_s\}$.

1. Présentation des résultats. Étant donné un polynôme non constant $P(\underline{X}) \in K[\underline{X}]$, le *spectre* de P est le sous-ensemble de $\overline{K}$ défini par

$$\sigma(P) = \{\lambda \in \overline{K} : P(\underline{X}) - \lambda \text{ est réductible sur } \overline{K}\}.$$

Il est clair que si P est un polynôme *composé* sur K, c'est-à-dire, s'il existe deux polynômes $R(T) \in K[T]$ avec $\deg(R) \geq 2$ et $Q(\underline{X}) \in K[\underline{X}]$ tels que $P(\underline{X}) = R(Q(\underline{X}))$, alors le spectre $\sigma(P)$ est un sous-ensemble infini de $\overline{K}$ (en fait $\sigma(P) = \overline{K}$). D'après un théorème de Bertini [12, chap. 3, §3, cor. 1], la réciproque est aussi vraie. De plus on voit facilement que si P est irréductible sur $\overline{K}$, alors il est non composé ([1]).

Cet article est une étude de l'ensemble $\sigma(P)$ et des factorisations associées $P - \lambda = \prod_{i=1}^{n(\lambda)} f_{\lambda,i}^{k_{\lambda,i}}$ en irréductibles $f_{\lambda,i} \in \overline{K}[\underline{X}]$ pour $\lambda \in \sigma(P)$.

2000 *Mathematics Subject Classification*: Primary 12D05, 12E25; Secondary 12E05, 11xxx.

([1]) Mais irréductible sur K ne suffit pas (penser à $P(X, Y) = (XY)^2 - 2$). Rappelons de plus que P est non composé sur $\overline{K}$ si et seulement si P est non composé sur K (voir [1]). Récemment Ayad et Ryckelynck [3] ont donné une méthode pour détecter si un polynôme $P \in K[X, Y]$ est composé et sinon déterminer les valeurs $\lambda \in \sigma(P)$.

Comme dans [13], on définit les nombres suivants :

$$\varrho_\lambda(P) = n(\lambda) - 1 \quad (\lambda \in \overline{K}), \qquad \varrho(P) = \sum_{\lambda \in \overline{K}} \varrho_\lambda(P)$$

qui sont respectivement le *degré partiel* relatif à λ et le *degré total de réductibilité* du polynôme P.

On a le résultat suivant, que nous appellerons *inégalité de Stein* :

$$\varrho(P) < \deg(P).$$

Ce résultat a été démontré par Stein [13] en 1989 pour le cas $n = 2$, et a été étendu pour $n \geq 2$ par Cygan [4] en 1992 (tous deux font des hypothèses sur le corps (non dénombrable, etc.) mais nous expliquons en §2.1 comment en déduire le résultat pour un corps de caractéristique 0 arbitraire). Pour $n = 2$, l'inégalité a été améliorée par Lorenzini [11] en 1993, qui a montré qu'en caractéristique quelconque,

$$\varrho(P) \leq \min_{\lambda \in \sigma(P)} \Big\{ \sum_i \deg(f_{\lambda,i}) \Big\} - 1 \leq \deg(P) - 1.$$

Cygan et Lorenzini donnent aussi l'exemple du polynôme non composé

$$P(X, Y) = X + Y \prod_{i=0}^{d-2} (X - i)$$

(pour lequel $\sigma(P) = \{0, \ldots, d-2\}$ et $\varrho_i(P) = 1$ pour tout $i \in \sigma(P)$) qui montre que l'inégalité de Stein est optimale.

Le résultat suivant, que nous allons déduire de notre théorème principal, montre plus précisément que l'ensemble fini $\sigma(P)$ et les paramètres correspondants $\varrho_\lambda(P) > 0$ sont *a priori* quelconques.

Théorème 1. *Étant donnés un entier $s \geq 1$, un ensemble $\{a_1, \ldots, a_s\}$ d'éléments distincts de K et des entiers $\varrho_1, \ldots, \varrho_s$ positifs non nuls, il existe un polynôme $P(\underline{X})$ dans $K[\underline{X}]$ non composé (et même irréductible sur $\overline{K}$ si $a_1, \ldots, a_s$ sont non nuls) tel que $\sigma(P) = \{a_1, \ldots, a_s\}$ et $\varrho_{a_i}(P) = \varrho_i$ pour tout $i = 1, \ldots, s$.*

Si on voit les éléments λ du spectre $\sigma(P)$ comme des pôles vis-à-vis de l'irréductibilité et les paramètres $\varrho_\lambda(P)$ comme l'ordre de ces pôles, le théorème 1 affirme qu'on peut trouver des polynômes P de pôles et d'ordres fixés à l'avance (ce qui dans l'esprit est analogue au théorème de Riemann–Roch).

Notre théorème principal montre de plus que, quitte à ne demander que l'inclusion $\{a_1, \ldots, a_s\} \subset \sigma(P)$, on peut également imposer à l'avance tous les facteurs irréductibles de $P(\underline{X}) - a_i$ $(i = 1, \ldots, s)$ sauf un. De façon précise :

THÉORÈME 2. *Soient $s \geq 1$ un entier, $a_1, \ldots, a_s$ des éléments distincts de K et $f_1, \ldots, f_s$ des polynômes de $K[\underline{X}]$ tels que $(f_i) + (f_j) = K[\underline{X}]$ si $i \neq j$. Alors il existe une infinité de polynômes $P \in K[\underline{X}]$ non composés (et même irréductibles sur $\overline{K}$ si $a_1, \ldots, a_s$ sont non nuls) tels que $P - a_i = f_i H_i$, avec $H_i \in K[\underline{X}]$ irréductible dans $\overline{K}[\underline{X}]$ et ne divisant pas f_i, $i = 1, \ldots, s$.*

De plus, si les polynômes $f_1, \ldots, f_s$ soit sont constants soit se décomposent dans $K[\underline{X}]$ en produit de facteurs irréductibles distincts de degré 1, alors on peut ajouter à la conclusion que $\deg(P) = (\sum_{i=1}^{s} \deg(f_i)) + 1$.

REMARQUES 1. (a) Dans cet énoncé, certains des polynômes f_i peuvent être choisis constants non nuls. Pour ces indices, la conclusion du théorème 2 est que $P(\underline{X}) - a_i$ est irréductible sur $\overline{K}$, i.e., $\varrho_{a_i}(P) = 0$. Cela entraîne qu'il suffit de montrer l'énoncé sans la condition "P non composé". En effet, en appliquant cet énoncé plus faible à la famille $a_0, a_1, \ldots, a_s$ avec $a_0 \notin \{a_1, \ldots, a_s\}$ et en prenant $f_0 \in K \setminus \{0\}$, on obtient alors, en plus des conclusions relatives à $a_1, \ldots, a_s$, que $P(\underline{X}) - a_0$ est irréductible sur $\overline{K}$, donc est non composé, ce qui entraîne que $P(\underline{X})$ lui-même est non composé. Si $a_1, \ldots, a_s$ sont non nuls, le même argument, avec $a_0 = 0$, fournit l'énoncé plus fort encore, où la conclusion "$P \in K[\underline{X}]$ irréductible sur $\overline{K}$" remplace "$P \in K[\underline{X}]$ non composé".

(b) La condition $(f_i) + (f_j) = K[\underline{X}]$ qui apparaît dans les hypothèses de l'énoncé est nécessaire puisque, pour $i \neq j$, $(P - a_i)$ et $(P - a_j)$ sont étrangers et donc tout diviseur du polynôme $P - a_i$ engendre un idéal étranger à celui qui est engendré par tout diviseur du polynôme $P - a_j$.

Preuve du théorème 1 (à partir du théorème 2). Prenons des polynômes f_i $(i = 1, \ldots, s)$ qui s'écrivent comme produit de ϱ_i polynômes dans $K[\underline{X}]$ irréductibles dans $\overline{K}[\underline{X}]$ et qui vérifient $(f_i) + (f_j) = K[\underline{X}]$ si $i \neq j$. D'après le théorème 2, il existe une infinité de polynômes $P(\underline{X}) \in K[\underline{X}]$ non composés (et même irréductibles sur $\overline{K}$ si $a_1, \ldots, a_s$ sont non nuls) tels que $P - a_i = f_i H_i$, avec $H_i \in K[\underline{X}]$ irréductible dans $\overline{K}[\underline{X}]$ et ne divisant pas f_i, $i = 1, \ldots, s$. En particulier, $P - a_i$ est réductible dans $K[\underline{X}]$ (puisque $f_i \notin K$), $i = 1, \ldots, s$. L'ensemble $\sigma(P)$ contient donc tous les éléments $a_1, \ldots, a_s$. De plus, $\varrho_{a_i}(P)$ est égal au nombre de facteurs irréductibles de f_i, c'est-à-dire ϱ_i, $i = 1, \ldots, s$.

Maintenant, on va montrer qu'on peut en plus garantir l'égalité $\sigma(P) = \{a_1, \ldots, a_s\}$. Pour cela, prenons

$$f_i(\underline{X}) = \prod_{k=1}^{\varrho_i} (\alpha_1 X_1 + \cdots + \alpha_n X_n + \alpha_{i,k}),$$

pour $i = 1, \ldots, s$, où $\alpha_1, \ldots, \alpha_n$ sont des éléments de K non tous nuls et où les $\alpha_{i,k}$ sont des éléments deux à deux distincts de K. Ces polynômes

satisfont les conditions du théorème 2, et d'après la seconde partie de ce dernier, on peut demander en plus que $\deg(P) = (\sum_{i=1}^{s} \deg(f_i)) + 1$. Supposons maintenant que $\sigma(P)$ contient au moins un λ différent de tous les a_i. Alors, puisque $\deg(f_i) = \varrho_i = \varrho_{a_i}(P)$, $i = 1, \ldots, s$, on a

$$\varrho(P) \geq \Big(\sum_{i=1}^{s} \varrho_{a_i}(P) \Big) + \varrho_\lambda(P) = \Big(\sum_{i=1}^{s} \deg(f_i) \Big) + \varrho_\lambda(P) > \deg(P) - 1,$$

ce qui contredit l'inégalité de Stein. ∎

Le théorème 2, notre résultat principal, est démontré dans la section 3. Dans la section 2 nous établissons quelques résultats préliminaires à la preuve du théorème 2. Enfin dans la section 4, nous énonçons et démontrons un résultat analogue au théorème 2 dans le cas d'une variable (sur un corps hilbertien).

2. Résultats préliminaires

2.1. *L'inégalité de Stein sur un corps de caractéristique* 0. Soient C un corps algébriquement clos de caractéristique 0, $K \subset C$ un sous-corps et $P(\underline{X}) \in K[\underline{X}]$. On note

$$\sigma_C(P) = \{\lambda \in C : P(\underline{X}) - \lambda \text{ est réductible sur } C\},$$
$$\sigma_{\overline{K}}(P) = \{\lambda \in \overline{K} : P(\underline{X}) - \lambda \text{ est réductible sur } \overline{K}\}$$

les spectres du polynôme P relatifs respectivement aux corps C et $\overline{K}$. On a :

Si P est non composé sur $\overline{K}$ alors $\sigma_C(P) = \sigma_{\overline{K}}(P)$. En particulier, la définition du spectre ne dépend pas du corps algébriquement clos contenant les coefficients de P.

En effet, il est clair que $\sigma_{\overline{K}}(P) \subset \sigma_C(P)$. Inversement, soit $\lambda \in \sigma_C(P)$, c'est-à-dire

$$(*) \qquad P(\underline{X}) - \lambda = Q(\underline{X})R(\underline{X}), \text{ avec } Q, R \in C[\underline{X}] \text{ non constants.}$$

Soit F le corps engendré sur $\overline{K}$ par λ et les coefficients de Q et R; $F/\overline{K}$ est une extension de type fini. On peut donc l'écrire $F = \overline{K}(t_1, \ldots, t_d, y)$, où $t_1, \ldots, t_d$ sont algébriquement indépendants sur $\overline{K}$ et y algébrique sur $\overline{K}(t_1, \ldots, t_d)$. Notons $h \in \overline{K}(t_1, \ldots, t_d)[Y]$ son polynôme minimal. La factorisation $(*)$ se réécrit sous la forme

$$P(\underline{X}) - \lambda(t_1, \ldots, t_d, y) = Q(t_1, \ldots, t_d, y)(\underline{X})R(t_1, \ldots, t_d, y)(\underline{X}).$$

Ainsi pour tout $(d+1)$-uplet $(t_1^0, \ldots, t_d^0, y^0)$ d'éléments de $\overline{K}$ tels que $h(t_1^0, \ldots, t_d^0, y^0) = 0$ sauf dans un fermé propre de Zariski, la spécialisation correspondante fournit une décomposition non triviale dans $\overline{K}[\underline{X}]$

$$(**) \qquad P(\underline{X}) - \lambda(t_1^0, \ldots, t_d^0, y^0) = Q(t_1^0, \ldots, t_d^0, y^0)(\underline{X}) R(t_1^0, \ldots, t_d^0, y^0)(\underline{X}).$$

On a donc $\lambda(t_1^0, \ldots, t_d^0, y^0) \in \sigma_{\overline{K}}(P)$.

Si $\lambda \in F \setminus \overline{K}$, cela donne une infinité d'éléments dans $\sigma_{\overline{K}}(P)$, ce qui contredit P non composé sur $\overline{K}$. D'où $\lambda \in \overline{K}$ et $P(\underline{X}) - \lambda$ réductible sur $\overline{K}$ par $(**)$; c'est-à-dire, $\lambda \in \sigma_{\overline{K}}(P)$. (Cela montre en particulier que P non composé sur $\overline{K}$ entraîne P non composé sur C.)

De plus si on écrit $P(\underline{X}) - \lambda = \prod_{i=1}^{n(\lambda)} f_{\lambda,i}(\underline{X})^{k_{\lambda,i}}$ une décomposition en irréductibles de $\overline{K}[\underline{X}]$ alors cette décomposition est aussi la décomposition dans $C[\underline{X}]$ (car irréductible dans $\overline{K}[\underline{X}]$ entraîne irréductible dans $C[\underline{X}]$). Les paramètres $n(\lambda)$ ne dépendent donc pas du corps algébriquement clos contenant $\overline{K}$.

Notons K_0 le corps engendré sur $\mathbb{Q}$ par les coefficients de P ; on a $P \in K_0[\underline{X}]$. De $K_0 \subset \overline{K}$ on déduit que $\sigma_{\overline{K}_0}(P) = \sigma_{\overline{K}}(P)$. D'autre part le corps K_0 peut être plongé dans $\mathbb{C}$. On a donc aussi $\sigma_{\overline{K}_0}(P) = \sigma_{\mathbb{C}}(P)$, d'où $\sigma_{\overline{K}}(P) = \sigma_{\mathbb{C}}(P)$. En appliquant le résultat de Cygan (i.e., l'inégalité de Stein sur $\mathbb{C}$), on obtient $\sum_{\lambda \in \overline{K}} \varrho_\lambda(P) \leq \deg(P) - 1$.

L'inégalité de Stein s'étend donc du cas $K = \mathbb{C}$ au cas de tout corps algébriquement clos de caractéristique 0.

2.2. *Quelques résultats sur les corps hilbertiens.* Soient m, r et d des entiers ≥ 1. Soient $\underline{T} = (T_1, \ldots, T_m)$, $\underline{Z} = (Z_1, \ldots, Z_d)$ des indéterminées algébriquement indépendantes sur K et $P_1(\underline{T}, \underline{Z}), \ldots, P_r(\underline{T}, \underline{Z})$ des polynômes irréductibles dans $K(\underline{T})[\underline{Z}]$. Rappelons qu'on appelle *partie hilbertienne* de K^m associée aux polynômes $P_1, \ldots, P_r$ le sous-ensemble de K^m défini par

$$H_{P_1,\ldots,P_r} = \{\underline{t} = (t_1, \ldots, t_m) \in K^m : P_i(\underline{t}, \underline{Z}) \text{ est irréductible dans } K[\underline{Z}]\},$$

et qu'un corps K est dit *hilbertien* si les parties hilbertiennes sont Zariski-denses dans K^m pour tous entiers $m, r, d \geq 1$.

Dans la suite de ce texte, on va utiliser la proposition ci-dessous qui montre en particulier que pour K un corps infini, le corps $K(X)$ est hilbertien, et qui donne une forme spéciale d'éléments de ce corps dans une partie hilbertienne donnée.

PROPOSITION. *Soient K un corps infini, H une partie hilbertienne de $K(X)$ et $m \geq 1$ un entier. Alors il existe un polynôme $\phi \in K[X, t]$ non nul tel que pour tout $(x_0, t_0) \in K^2$ avec $\phi(x_0, t_0) \neq 0$ et pour tout $\lambda_0 \in K$ sauf un nombre fini, l'élément $t^* = t_0 + \lambda_0(X - x_0)^m$ de $K(X)$ est dans la partie hilbertienne H.*

Pour la preuve de ce résultat et pour plus de détails, nous renvoyons par exemple à [9] ou [10, prop. 4.1, p. 236].

Nous utilisons aussi le résultat suivant qui raffine le caractère hilbertien du corps $K(X)$ dans une forme que nous n'avons pas trouvée dans la littérature, à savoir :

THÉORÈME 3. *Soient $P_1(X,T,\underline{Z}),\dots,P_r(X,T,\underline{Z})$ des polynômes irréductibles dans $\overline{K}[X,T,\underline{Z}]$ de degré >0 en $\underline{Z}$. Alors il existe une infinité de polynômes $t(X)\in K[X]$ de degré 1 tels que les polynômes $P_j(X,t(X),\underline{Z})$ sont irréductibles dans $\overline{K}[X][\underline{Z}]$ pour $j=1,\dots,r$.*

Cela veut dire que les polynômes spécialisés $P_j(X,t(X),\underline{Z})\in K[X][\underline{Z}]$ sont non seulement irréductibles dans $\overline{K}(X)[\underline{Z}]$ mais aussi primitifs.

On va déduire le théorème 3 de la proposition précédente et du lemme suivant.

LEMME 1. *Soient $A_0(X,T),\dots,A_d(X,T)\in K[X,T]$ des polynômes premiers entre eux. Alors il existe deux ensembles finis F et G de $\overline{K}$ tels que pour tout $t(X)\in K[X]$ vérifiant "$t(x)\notin F$ pour tout $x\in G$", les polynômes $A_i(X,t(X))$ sont premiers entre eux dans $\overline{K}[X]$ pour $i=0,\dots,d$.*

Preuve. Les polynômes $A_0(X,T),\dots,A_d(X,T)$ sont *a priori* premiers entre eux dans $K[X,T]$, et il est facile de vérifier qu'ils le sont dans $K(X)[T]$. Par conséquent, il existe $u_0(X,T),\dots,u_d(X,T)\in K[X,T]$ et il existe $\delta(X)\in K[X]$ non nul tels que

$$u_0(X,T)A_0(X,T)+\cdots+u_d(X,T)A_d(X,T)=\delta(X).$$

Pour toute spécialisation $t(X)$ de T dans $K[X]$, on a

$$u_0(X,t(X))A_0(X,t(X))+\cdots+u_d(X,t(X))A_d(X,t(X))=\delta(X).$$

Pour tout $x\in\overline{K}$, alors il existe un indice $i(x)$ tel que $A_{i(x)}(x,T)\neq 0$: sinon $(X-x)$ serait un diviseur de chaque $A_i(X,T)$ dans $\overline{K}[X,T]$, ce qui contredirait que les polynômes $A_0,\dots,A_d$ sont premiers entre eux.

Soient $x_1,\dots,x_l$ les racines de $\delta(X)$ dans $\overline{K}$. On pose

$$F=\{y\in\overline{K} : y \text{ racine d'un des polynômes } A_{i(x_j)}(x_j,T),\ j=1,\dots,l\},$$

$$G=\{x_1,\dots,x_l\}.$$

Soit $t(X)\in K[X]$ vérifiant "$t(x)\notin F$ si $x\in G$". Montrons qu'alors les polynômes $A_i(X,t(X))$ sont premiers entre eux dans $\overline{K}[X]$ pour $i=0,\dots,d$. Sinon ces polynômes auraient un diviseur irréductible commun $H(X)$. On aurait que $H(X)$ divise $\delta(X)$ et donc un des éléments de G, disons x_j, serait racine de $H(X)$. Mais alors on aurait $A_i(x_j,t(x_j))=0$ pour tout $i=0,\dots,d$, ce qui pour $i=i(x_j)$ contredit le fait que $t(x_j)\notin F$. ∎

Preuve du théorème 3. Soient $P_1,\dots,P_r$ des polynômes irréductibles dans $\overline{K}[X,T,\underline{Z}]$ de degré >0 en $\underline{Z}$. Alors ils sont primitifs comme polynômes en $\underline{Z}$ à coefficients dans $\overline{K}[X,T]$ et ils sont irréductibles dans $\overline{K}(X)(T)[\underline{Z}]$.

Ainsi, en vertu de la proposition pour $m = 1$, il existe un polynôme $\phi \in K[X,t]$ non nul tel que pour tout $(x_0,t_0) \in K^2$ avec $\phi(x_0,t_0) \neq 0$, et pour tout $\lambda_0 \in K$ sauf dans un ensemble fini E, l'élément $t(X) = t_0 + \lambda_0(X - x_0)$ de $\overline{K}(X)$ est dans la partie hilbertienne $H_{P_1,\dots,P_r}$.

Considérons chaque polynôme $P_j(X,T,\underline{Z})$ comme polynôme en $\underline{Z}$ à coefficients dans $K[X,T]$:

$$P_j(X,T,\underline{Z}) = \sum_{\underline{i}=(i_1,\dots,i_d)} A_{j,\underline{i}}(X,T) Z_1^{i_1} \cdots Z_d^{i_d},$$

avec $i_1 + \cdots + i_d \leq \deg_{\underline{Z}}(P_j)$ pour $j = 1,\dots,r$.

D'après l'hypothèse du théorème 3, pour chaque $j = 1,\dots,r$, les polynômes $A_{j,\underline{i}}(X,T)$ sont premiers entre eux dans $\overline{K}[X,T]$. En vertu du lemme 1, il existe deux ensembles finis F_j et G_j tels que pour tout $t(X) \in K[X]$ vérifiant "$t(x) \notin F_j$ pour tout $x \in G_j$", les polynômes $A_{j,\underline{i}}(X,t(X))$ sont premiers entre eux dans $\overline{K}[X]$ pour $j = 1,\dots,r$.

On pose ensuite $F = \bigcup_{j=1}^r F_j$ et $G = \bigcup_{j=1}^r G_j$; ce sont deux ensembles finis. D'autre part, l'ensemble

$$U = \{(x,t) \in K^2 : x \neq g \text{ pour tout } g \in G\}$$

est un ouvert de Zariski, donc est dense dans K^2. On peut alors choisir $(x_0,t_0) \in U$ qui n'appartienne pas au fermé propre de Zariski, $Z(\phi) = \{(x,t) \in K^2 : \phi(x,t) = 0\}$. Soit finalement $\lambda_0 \neq (f - t_0)/(g - x_0)$ pour tout $f \in F$ et pour tout $g \in G$ et $\lambda_0 \notin E$ (c'est-à-dire un nombre fini d'exceptions). La condition sur λ_0 entraîne que "$t(x) = t_0 + \lambda_0(x - x_0) \notin F$ pour tout $x \in G$". En particulier "$t(x) \notin F_j$ pour tout $x \in G_j$ $(j = 1,\dots,r)$". Pour $t(X)$ ainsi construit, on voit que les polynômes $P_j(X,t(X),\underline{Z})$ sont irréductibles dans $\overline{K}(X)[\underline{Z}]$ (proposition) et sont primitifs (lemme 1), $j = 1,\dots,r$. ∎

Remarque 2. Le théorème 3 n'est plus vrai si on remplace $K[X]$ par $\mathbb{Z}$. En effet : si on prend le polynôme $P(T,Z) = (T^2 - T)Z + (T^2 - T + 2)$, qui est primitif dans $\mathbb{Z}[T][Z]$, alors pour tout $t \in \mathbb{Z}$, $t^2 - t$ et $t^2 - t + 2$ sont des entiers pairs et donc $P(t,Z)$ est réductible dans $\mathbb{Z}[Z]$.

On termine ces préliminaires par le lemme suivant qui résulte de façon immédiate du lemme de Gauss.

Lemme 2. *Soient $A(\underline{X})$ et $B(\underline{X})$ deux polynômes de $K[\underline{X}]$ qui n'ont pas de facteur commun dans $K[\underline{X}]$. Alors le polynôme $P(\underline{X},T) = A(\underline{X}) + TB(\underline{X})$ est irréductible dans $\overline{K}[\underline{X},T]$.*

Remarque 3. Une application du théorème 3 au polynôme $P(\underline{X},T)$ du lemme 2 (vu comme polynôme dans $K[X_1][T][X_2,\dots,X_n]$) fournit l'énoncé suivant : si $A(\underline{X})$ et $B(\underline{X})$ sont premiers entre eux dans $K[\underline{X}]$ et de degré > 0 en $(X_2,\dots,X_n)$, alors il existe une infinité de $m(X_1) \in K[X_1]$ tels

que $A(\underline{X}) + m(X_1)B(\underline{X})$ est irréductible dans $\overline{K}[\underline{X}]$, ce qui constitue un analogue du fameux théorème de la progression arithmétique.

3. Preuve du théorème 2. Dans une première étape, on montre l'existence d'un polynôme $P_0 \in K[\underline{X}]$ tel que $P_0(\underline{X}) - a_i = f_i(\underline{X})p_i(\underline{X})$, avec $p_i \in K[\underline{X}]$ pour tout $i = 1, \ldots, s$. Cela résulte du lemme chinois : l'hypothèse $(f_i) + (f_j) = K[\underline{X}]$ si $i \neq j$ entraîne que l'homomorphisme $\phi : K[\underline{X}] \to \prod_{i=1}^{s} K[\underline{X}]/(f_i)$ est surjectif.

De plus les polynômes $P \in K[\underline{X}]$ pour lesquels $P - a_i$ est divisible par f_i pour $i = 1, \ldots, s$ sont de la forme

$$P(\underline{X}) = P_0(\underline{X}) + d(\underline{X}) \prod_{i=1}^{s} f_i(\underline{X})$$

avec $d(\underline{X}) \in K[\underline{X}]$. Quitte à changer $P_0(\underline{X})$, on peut supposer que $\deg_{X_2}(p_i) > 0$, $i = 1, \ldots, s$.

On se demande maintenant si parmi ces polynômes $P(\underline{X})$, il en existe pour lesquels $P(\underline{X}) - a_i = f_i(\underline{X})H_i(\underline{X})$ avec H_i irréductible dans $\overline{K}[\underline{X}]$ et ne divisant pas f_i, $i = 1, \ldots, s$.

Pour répondre à cette question, nous allons utiliser le théorème 3. Nous allons l'appliquer aux polynômes

$$p_i(\underline{X}) + T \prod_{\substack{1 \leq j \leq s \\ j \neq i}} f_j(\underline{X}), \qquad i = 1, \ldots, s,$$

avec les variables X, T et $\underline{Z}$ du théorème 3 prises respectivement égales à X_1, T et $(X_2, \ldots, X_n)$. Vérifions d'abord que ces polynômes satisfont les conditions du théorème 3. Pour vérifier l'irréductibilité de ces polynômes dans $\overline{K}[X, T, \underline{Z}] = \overline{K}[\underline{X}, T]$, on utilise le lemme 2.

Les polynômes p_i et $\prod_{1 \leq j \leq s,\, j \neq i} f_j$ sont premiers entre eux dans $K[\underline{X}]$. En effet : si p est un diviseur irréductible dans $K[\underline{X}]$ de ces deux polynômes, alors p divise l'un des f_j $(j \neq i)$ et p divise p_i, donc p est un diviseur commun des polynômes $P_0 - a_i$ et $P_0 - a_j$, ce qui est impossible pour $j \neq i$.

Nous pouvons donc appliquer le théorème 3 : il existe une infinité de $m(X_1) \in K[X_1]$ de degré 1 tels que les polynômes

$$p_i(\underline{X}) + m(X_1) \prod_{\substack{1 \leq j \leq s \\ j \neq i}} f_j(\underline{X}), \qquad i = 1, \ldots, s,$$

sont irréductibles dans $\overline{K}[\underline{X}]$. En posant, pour tout $i = 1, \ldots, s$,

$$P(\underline{X}) = P_0(\underline{X}) + m(X_1) \prod_{i=1}^{s} f_i(\underline{X}),$$

$$H_i(\underline{X}) = p_i(\underline{X}) + m(X_1) \prod_{\substack{1 \le j \le s \\ j \ne i}} f_j(\underline{X})$$

on obtient

$$P(\underline{X}) - a_i = f_i(\underline{X}) H_i(\underline{X})$$

et les polynômes H_i $(i = 1, \dots, s)$ sont irréductibles dans $\overline{K}[\underline{X}]$. De plus, on peut choisir $m(X_1)$ de telle sorte que H_i ne divise pas $f_i,\ i = 1, \dots, s$: pour une infinité de choix du polynôme $m(X_1)$ (de degré 1), les polynômes H_i correspondants ne sont pas proportionnels et ne peuvent donc pas être tous des diviseurs irréductibles de $f_i,\ i = 1, \dots, s$. Compte tenu de la remarque 1(a), cela achève la preuve de la première partie du théorème 2.

Pour la deuxième partie, on note $I \subset \{1, \dots, s\}$ l'ensemble des indices i tels que f_i est non constant. On suppose que les polynômes f_i avec $i \in I$ se décomposent dans $K[\underline{X}]$ en produit de facteurs irréductibles distincts de degré 1. On pose, pour chaque $i \in I$, $f_i(\underline{X}) = \prod_{k=1}^{m_i} g_{i,k}(\underline{X})$ où $m_i \ge 1$ est le nombre de facteurs de f_i. La condition $(f_i) + (f_j) = K[\underline{X}]$ pour $i \ne j$ dans I entraîne que les facteurs $g_{i,k}$ et $g_{j,h}$ sont étrangers, c'est-à-dire n'ont pas de zéros communs dans $(\overline{K})^n$ pour tous $k = 1, \dots, m_i$ et $h = 1, \dots, m_j$; les $g_{i,k}$ sont donc de la forme $\alpha_1 X_1 + \cdots + \alpha_n X_n + \alpha_{i,k}$ (à un coefficient multiplicatif près), avec $i \in I,\ k = 1, \dots, m_i$ et où les $\alpha_{i,k}$ sont deux à deux distincts. Pour tous indices $i, j \in I$, $k = 1, \dots, m_i$ et $h = 1, \dots, m_j$ tels que $(i,k) \ne (j,h)$, on pose

$$u_{i,k,j,h} = \frac{1}{\alpha_{i,k} - \alpha_{j,h}}, \qquad v_{i,k,j,h} = -u_{i,k,j,h}\,;$$

on a alors

$$u_{i,k,j,h} g_{i,k}(\underline{X}) + v_{i,k,j,h} g_{j,h}(\underline{X}) = 1.$$

Pour tout couple (i,k) fixé, avec $i \in I$ et $k = 1, \dots, m_i$, en développant l'identité

$$\prod_{(j,h) \ne (i,k)} (u_{i,k,j,h} g_{i,k}(\underline{X}) + v_{i,k,j,h} g_{j,h}(\underline{X})) = 1,$$

on voit que le polynôme défini par

$$b_{i,k}(\underline{X}) = \prod_{(j,h) \ne (i,k)} v_{i,k,j,h} g_{j,h}(\underline{X})$$

vérifie $1 - b_{i,k} \in (g_{i,k})$ et $b_{i,k} \in \bigcap_{(j,h) \ne (i,k)} (g_{j,h})$. On pose alors

$$P_0(\underline{X}) = \sum_{i \in I} \sum_{k=1}^{m_i} a_i b_{i,k}(\underline{X}).$$

On vérifie facilement que $P_0(\underline{X}) - a_i$ est divisible par $g_{i,k}$ pour tous $i \in I$ et

$k = 1, \ldots, m_i$, et donc est divisible par f_i pour tout $i = 1, \ldots, s$. De plus

$$\deg(P_0) \leq \max_{i,k}\{\deg(b_{i,k})\} = \Big(\sum_{i=1}^{s} \deg(f_i)\Big) - 1.$$

Finalement, pour le polynôme P correspondant, on a

$$\deg(P) = \Big(\sum_{i=1}^{s} \deg(f_i)\Big) + 1. \ \blacksquare$$

REMARQUE 4. Si on prend des polynômes $f_1, \ldots, f_s$ dans $K[\underline{X}]$ de la forme $f_i(\underline{X}) = \prod_{k=1}^{m_i} (g(\underline{X}) + \alpha_{i,k})$, avec $g \in K[\underline{X}] \setminus K$ et les éléments $\alpha_{i,k} \in K$ deux à deux distincts, alors en utilisant le même procédé que ci-dessus, on peut trouver une solution particulière P_0 telle que

$$\deg(P_0) \leq \Big(\sum_{i=1}^{s} \deg(f_i)\Big) - \deg(g).$$

Par conséquent le polynôme correspondant

$$P(\underline{X}) = P_0(\underline{X}) + m(X_1) \prod_{i=1}^{s} f_i(\underline{X})$$

est encore de degré $(\sum_{i=1}^{s} \deg(f_i)) + 1$.

4. Le cas d'une seule variable. On finit cet article par un analogue de notre résultat dans le cas d'une seule variable, en supposant le corps K hilbertien (par exemple $K = \mathbb{Q}$). Dans ce cas nous dirons qu'un polynôme $p(X) \in K[X]$ est *strictement composé sur* K s'il existe deux polynômes $r(X), q(X) \in K[X]$ avec $\deg(r) \geq 2$ et $\deg(q) \geq 2$ tels que $p(X) = r(q(X))$.

Rappelons le résultat suivant, dû à Fried [7], [8] : Les seuls polynômes non strictement composés $p(X) \in \mathbb{Q}[X]$ pour lesquels $p(X) - t$ est réductible pour une infinité de $t \in \mathbb{Z} \setminus p(\mathbb{Q})$ sont de degré 5. Ainsi pour un polynôme non strictement composé $p(X) \in \mathbb{Q}[X]$, si on définit le spectre $\sigma(p)$ comme l'ensemble des $t \in \mathbb{Z}$ tels que $p(X) - t$ est réductible sur $\mathbb{Q}$, alors $\sigma(p) \setminus p(\mathbb{Q})$ est fini, sauf dans le cas exceptionnel où $\deg(p) = 5$. De plus Dèbes et Fried ont montré [5], [6] que le cas $\deg(p) = 5$ est réellement exceptionnel : il existe des polynômes non strictement composés $p(X) \in \mathbb{Q}[X]$ (de degré 5) pour lesquels $p(X) - t$ est réductible pour une infinité de $t \in \mathbb{Z} \setminus p(\mathbb{Q})$.

Dans ce contexte, on a l'analogue de notre résultat principal (théorème 2), pour K un corps hilbertien, à savoir :

THÉORÈME 4. *Soient $s \geq 1$ un entier, $a_1, \ldots, a_s$ des éléments distincts de K et $f_1, \ldots, f_s$ des polynômes de $K[X]$ tels que $(f_i) + (f_j) = K[X]$ si $i \neq j$. Alors il existe une infinité de polynômes $p(X) \in K[X]$ non strictement composés sur K (et même irréductibles si $a_1, \ldots, a_s$ sont non nuls) tels*

que $p(X) - a_i = f_i(X)h_i(X)$, *avec* $h_i(X) \in K[X]$ *irréductible pour tout* $i = 1, \ldots, s$.

Preuve. Quitte à ajouter à $a_1, \ldots, a_s$ un élément supplémentaire a_{s+1} de K et à $f_1, \ldots, f_s$ un polynôme f_{s+1} premier à $f_1, \ldots, f_s$, on peut supposer que $\sum_{i=1}^{s} \deg(f_i)$ est un nombre premier. Cette réduction nous sera utile en fin de preuve.

L'existence d'un polynôme $p_0(X) \in K[X]$ tel que $p_0(X) - a_i = f_i(X)p_i(X)$, avec $p_i(X) \in K[X]$ pour $i = 1, \ldots, s$, se démontre comme dans le théorème 2 (par le lemme chinois). Et les polynômes $p(X) \in K[X]$ pour lesquels $p(X) - a_i$ est divisible par $f_i(X)$, $i = 1, \ldots, s$, sont de la forme

$$p(X) = p_0(X) + t(X) \prod_{i=1}^{s} f_i(X)$$

avec $t(X) \in K[X]$. De plus, on peut choisir $p_0(X)$ tel que $\deg(p_0) < \sum_{i=1}^{s} \deg(f_i)$.

De façon similaire à la preuve du théorème 2, on considère les polynômes

$$P(T, X) = p_0(X) + T \prod_{i=1}^{s} f_i(X),$$

$$Q_i(T, X) = p_i(X) + T \prod_{\substack{1 \le j \le s \\ j \ne i}} f_j(X) \qquad (i = 1, \ldots, s).$$

On montre comme dans la section 3 que les polynômes $Q_i(T, X)$ $(i = 1, \ldots, s)$, et $P(T, X)$ si $a_1, \ldots, a_s$ sont non nuls, sont irréductibles dans $\overline{K}[T, X]$.

Il découle de l'hypothèse "K hilbertien" appliquée aux polynômes $Q_i(T, X)$, $i = 1, \ldots, s$, et en plus à $P(T, X)$ dans le cas où $a_1, \ldots, a_s$ sont non nuls, qu'il existe une infinité de $t \in K$ tels que les polynômes correspondants, spécialisés en $T = t$, sont irréductibles sur K.

Pour de tels $t \in K$, on obtient bien, en posant $p(X) = P(t, X)$ et $h_i(X) = Q_i(t, X)$, que $p(X) - a_i = f_i(X)h_i(X)$, avec $h_i(X)$ irréductible sur K, $i = 1, \ldots, s$.

Enfin, pour tous ces t sauf un nombre fini, $\deg P(t, X) = \deg_X(P) = \sum_{i=1}^{s} \deg(f_i)$ est premier (grâce à la réduction préliminaire) et donc $p(X)$ est non strictement composé sur K.

De plus, dans le cas où $a_1, \ldots, a_s$ sont non nuls, pour les $t \in K$ choisis comme ci-dessus, on a aussi le polynôme $p(X) = P(t, X)$ irréductible sur K. ∎

Remarques 5. (a) Dans la preuve ci-dessus, nous assurons la non-composition des polynômes $p(X)$ en les construisant comme spécialisations de polynômes $P(T, X)$ de degré premier en X. Plus généralement il est vrai

que si $P(T,X)$ est non strictement composé sur $K(T)$ alors $P(t,X)$ est non strictement composé sur K pour une infinité de $t \in K$.

En effet, $P(T,X)$ non strictement composé sur $K(T)$ équivaut à dire que le groupe de Galois G du polynôme $P(T,X)-Z$ sur $K(T)(Z)$ agit de façon primitive sur les racines $x_1,\dots,x_d$ (où $d=\deg_X(P)$) dans $\overline{K(T,Z)}$ de ce polynôme ([12] ou [2, énoncé 4-9]). Cette action est (équivalente à) l'action de G sur les classes à gauche de G modulo le sous-groupe H qui fixe x_1. Grâce à l'hypothèse "K hilbertien" on peut trouver une infinité de $t \in K$ tels que G reste le groupe de Galois du polynôme spécialisé $P(t,X)-Z$ sur $K(Z)$ et H reste le fixateur de $x_1(t)$. Pour ces t, l'action précédente correspond alors aussi à celle de G sur les racines $x_1(t),\dots,x_d(t)$. Cette dernière action est donc primitive. On en conclut donc que pour les t considérés, $P(t,X)$ est non strictement composé sur K.

(b) Étant donné $\{a_1,\dots,a_s\} \subset K$, le théorème 4 permet de construire $p(X) \in K[X]$ non strictement composé tel que $\{a_1,\dots,a_s\} \subset \sigma(p)$. Il parait plus difficile de prescrire exactement $\sigma(p)$ comme dans le cas de $n \geq 2$ variables. En effet, les résultats de finitude de l'ensemble $\sigma(p) \setminus p(\mathbb{Q})$ démontrés par Fried utilisent le théorème de Siegel sur les points entiers des courbes algébriques, lequel n'est pas effectif. On ne peut donc pas les utiliser pour borner efficacement $\sigma(p)$, comme l'inégalité de Stein avait permis de le faire pour $n \geq 2$ variables.

Remerciements. Ce travail est une partie de ma thèse. Je voudrais remercier mes directeurs de thèse M. Ayad et P. Dèbes pour m'avoir fait découvrir ce sujet. Je remercie également les professeurs M. Fried et D. Lorenzini pour les discussions à propos de ce travail.

Références

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

[2] —, *Théorie de Galois, 115 exercices corrigés. Niveau II*, Ellipses, Paris, 1997.

[3] M. Ayad and P. Ryckelynck, *On the spectrum of bivariate polynomials*, preprint, LMPA, 2002.

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

[5] P. Dèbes and M. Fried, *Arithmetic variation of fibers in families of curves. I: Hurwitz monodromy criteria for rational points on all members of the family*, J. Reine Angew. Math. 409 (1990), 106–137.

[6] —, —, *Integral specialization of families of rational functions*, Pacific J. Math. 190 (1999), 45–85.

[7] M. Fried, *Applications of the classification of simple groups to monodromy. Part II: Davenport and Hilbert–Siegel problem*, preprint, 1986, 1–55.

[8] M. Fried, *Variables separated polynomials, the genus* 0 *problem and moduli spaces*, in: Number Theory in Progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 169–228.
[9] M. Fried and M. Jarden, *Field Arithmetic*, Springer, Berlin, 1986.
[10] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, New York, 1983.
[11] D. Lorenzini, *Reducibility of polynomials in two variables*, J. Algebra 156 (1993), 65–75.
[12] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge Univ. Press, Cambridge, 2000.
[13] Y. Stein, *The total reducibility order of a polynomial in two variables*, Israel J. Math. 68 (1989), 175–186.

UFR Mathématiques
Université Lille 1
59655 Villeneuve d'Ascq Cedex, France
E-mail: salah.najib@math.univ-lille1.fr

Reçu le 5.12.2003
et révisé le 18.2.2004 (4675)