EXTRACTA MATHEMATICAE Vol. **23**, Núm. 2, 173 – 180 (2008)

Autour d'un Théorème de Stein

Salah Najib

Université Lille 1, *Laboratoire Painlevé, U.F.R. Mathématiques,*
59655 *Villeneuve d'Ascq Cedex, France*
salah.najib@math.univ-lille1.fr, najibm@voila.fr

Presented by José A. de la Peña Received March 20, 2008

Abstract: Let K be a field of characteristic zero, $\overline{K}$ an algebraic closure of K and $P(X,Y)$ a non constant polynomial, with coefficients in K. For $\lambda \in \overline{K}$, denote the number of distinct irreducible factors $f_{\lambda,i}$ in a factorization of $P-\lambda$ over $\overline{K}$ by $n(\lambda)$. We rewrite without the *jacobian derivation* aspect of Stein's proof (1989) for showing the following statement: if P is non-composite then $\sum_\lambda (n(\lambda)-1)$ is at most equal to $\deg(P)-1$.

Key words: Irreducible polynomial, composite polynomial, spectrum of a polynomial, Stein's inequality.

AMS *Subject Class.* (2000): 12E05, 11C08.

1. Introduction

On se donne K un corps commutatif, $\overline{K}$ une clôture algébrique de K, n un entier ≥ 2, et $P(\underline{X}) := P(X_1,\ldots,X_n)$ un polynôme à n variables, à coefficients dans K.

Nous rappellons que le *spectre* du polynôme $P(\underline{X})$, qu'on note $\sigma(P)$, est le sous-ensemble de $\overline{K}$ donné par

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

Pour $\lambda \in \overline{K}$, on écrit

$$P(\underline{X}) - \lambda = \prod_{i=1}^{n(\lambda)} f_{\lambda,i}(\underline{X})^{k_{\lambda,i}}\,, \qquad k_{\lambda,i} \in \mathbb{N}^*\,,$$

une décomposition du polynôme $P(\underline{X}) - \lambda$ en facteurs irréductibles distincts $f_{\lambda,i} \in \overline{K}[\underline{X}]$. On définit aussi les nombres suivants :

$$\begin{cases} \rho_\lambda(P) \;=\; n(\lambda) - 1 \quad (\lambda \in \overline{K})\,, \\ \rho(P) \;=\; \displaystyle\sum_{\lambda \in \overline{K}} \rho_\lambda(P)\,, \end{cases}$$

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

Le polynôme $P(\underline{X})$ est dit *composé* sur K, s'il existe deux polynômes $u(T) \in K[T]$, $\deg(u) \geq 2$ et $Q(\underline{X}) \in K[\underline{X}]$ tels que $P(\underline{X}) = u(Q(\underline{X}))$.

Nous avons montré dans [8, Chapitre 1] le résultat suivant, dont découle la finitude de l'ensemble $\sigma(P)$ si le polynôme P est non-composé sur $\overline{K}$.

Théorème 1.1. *On a équivalence entre :*

(i) *$P(\underline{X}) - \lambda$ est réductible sur $\overline{K}$ pour une infinité de $\lambda \in \overline{K}$;*
(ii) *$P(\underline{X}) - \lambda$ est réductible sur $\overline{K}$ pour tout $\lambda \in \overline{K}$;*
(iii) *P est un polynôme composé sur $\overline{K}$;*[1]
(iv) *le polynôme $P(\underline{X}) - T$ est réductible dans $\overline{K(T)}[\underline{X}]$, où T est une variable.*

Dans [10], Y. Stein a montré (pour $K = \overline{K}$, $n = 2$ et K non-dénombrable de caractéristique 0) que si P est un polynôme non-composé alors le cardinal de $\sigma(P)$ est au plus égal à $\deg(P)-1$. Ce résultat sera appelé par la suite *inégalité de Stein*. Grâce à ce résultat, on peut ainsi préciser le Théorème 1.1 (pour $K = \overline{K}$, $n = 2$ et K non-dénombrable de caractéristique 0) : si $P(X,Y) \in K[X,Y]$ est non-composé, alors le polynôme $P(X,Y)+T$ est irréductible dans $\overline{K(T)}[X,Y]$ et pour toute spécialisation t de T dans K, le polynôme spécialisé reste irréductible sur K sauf peut-être pour au plus $\deg(P)-1$ valeurs $t \in K$. La méthode qu'a suivi Stein utilise la notion de "dérivation" d'une K-algèbre, notamment quelques propriétés des noyaux de "dérivations jacobiennes" de $K[X,Y]$ et de leur prolongement à $K(X,Y)$. Dans cet article, nous reprenons la preuve de Stein en éliminant l'aspect "dérivation jacobienne". De plus, nous en profitons pour apporter quelques autres simplifications.

Tout au long du reste de ce travail, K désigne un corps algébriquement clos (i.e., $K = \overline{K}$), non-dénombrable de caractéristique 0; X et Y sont deux variables algébriquement indépendantes sur K et enfin $P(X,Y) \in K[X,Y]$ un polynôme non-constant.

2. Inégalité de Stein

L'inégalité de Stein est celle donnée par le théorème suivant :

[1]Il est bien connu qu'en caractéristique 0 : "composé sur K" est équivalent à "composé sur $\overline{K}$" (voir par exemple [2, Théorème 7]). Cependant, cette équivalence n'est plus vraie en toute généralité (lorsque la caractéristique est > 0); voir par exemple [2, §8]. Nous renvoyons à [3] pour un énoncé général sur cette question.

Théorème fondamental. *Si $P(X,Y)$ est un polynôme non-composé alors*

$$\rho(P) < \deg(P)\,.$$

La preuve de ce théorème sera donnée dans la section 4.

Remarques. (1) Cette inégalité a été améliorée dans de nombreuses directions; en particulier elle est désormais connue sur un corps de caractéristique arbitraire et un nombre quelconque de variables. Pour plus de détails, nous renvoyons par exemple à [7] ou [8, Chapitre 3].

(2) Nous démontrerons ici le Théorème fondamental dans le cas où le corps K est non-dénombrable. Cette hypothèse intervient dans le Lemme 3.2. Des arguments généraux permettent de passer du cas non-dénombrable au cas général : nous renvoyons à [8, Chapitre 1, §1.4] pour cette réduction.

(3) Dans [5], A. Bodin a donné récemment un analogue du Théorème fondamental pour une fraction rationnelle en $n \geq 2$ variables; mais avec la borne $\deg(P)^2$ au lieu de $\deg(P)$.

(4) Une dernière généralisation fait l'objet de [4]. L'étude de la réductibilité des polynômes $P(\underline{X})-\lambda$, revient à étudier la réductibilité des polynômes $P(\underline{X})$ dont on a perturbé le coefficient constant. Dans [4], nous avons abordé avec A. Bodin et P. Dèbes la question suivante : étant donné un corps K algébriquement clos (de caractéristique quelconque) et un polynôme $P \in K[\underline{X}]$, décrire les ensembles des monômes $\{Q_1,\dots,Q_\ell\}$ dans $K[\underline{X}]$ pour lesquels $P(\underline{X})-\sum_{i=1}^{\ell} T_iQ_i(\underline{X})$ est réductible dans $\overline{K(\underline{T})}[\underline{X}]$, où $\underline{T}=(T_1,\dots,T_\ell)$ est un ℓ-uplet de variables algébriquement indépendantes.

3. Résultats préliminaires

Dans cette section, nous présentons les ingrédients principaux pour démontrer le théorème fondamental.

La proposition suivante donne une caractérisation de la relation de dépendance algébrique.

Proposition 3.1. *Pour $f \in K(X,Y)$ une fonction rationnelle donnée, les deux assertions suivantes sont équivalentes :*

(i) *f et P sont algébriquement dépendants sur K;*

(ii) *f est constante sur une infinité de composantes irréductibles des courbes de niveau $\{P=\lambda\}$.*

Démonstration. Dans cette preuve, on note $Z(F)$ l'ensemble algébrique (l'hypersurface) de K^2 défini par le polynôme F de $K[X,Y]$. L'ensemble $Z(F)$ est un fermé de l'espace affine K^2 pour la topologie de Zariski.

(i) $\Rightarrow$ (ii) : Supposons que P et f sont algébriquement dépendants sur K, c'est-à-dire, on a une relation de type :

$$\sum_{i=0}^{m} R_i(P) f^i = 0\,, \tag{1}$$

avec $R_i(T) \in K[T]$, $(R_0, \ldots, R_m) = 1$ et $R_m(P) \neq 0$.

Puisque K est un corps algébriquement clos, on peut écrire

$$R_m(T) = a \prod_{i=1}^{s} (T - \lambda_i)\,,$$

où $a \in K^*$ et $\lambda_1, \ldots, \lambda_s$ sont les racines de $R_m(T)$ dans K. Écrivons aussi $f(X,Y) = u(X,Y)/w(X,Y)$, avec $u, w \in K[X,Y]$ et $(u,w) = 1$. Alors la relation (1) donne

$$\sum_{i=0}^{m} R_i(P) u^i w^{m-i} = 0\,.$$

Ceci entraîne que w divise $R_m(P)$ dans $K[X,Y]$. Il s'ensuit que tout facteur irréductible de $w(X,Y)$ divise l'un des facteurs $P(X,Y) - \lambda_i$, $(i = 1, \ldots, s)$.

Soit maintenant $\lambda \neq \lambda_1, \ldots, \lambda_s$. Alors $Z(P-\lambda) \cap Z(w) = \emptyset$, car si $(x,y) \in K^2$ vérifie $w(x,y) = 0$, on a alors $P(x,y) = \lambda_i$ pour un certain indice $i \in \{1, \ldots, s\}$, et $P(x,y) = \lambda$ n'est alors pas possible pour notre choix de λ. Considérons une composante irréductible V_λ de la courbe de niveau $\{P = \lambda\}$. On a $V_\lambda \cap Z(w) = \emptyset$ et donc $w(x,y) \neq 0$ pour tout $(x,y) \in V_\lambda$. La relation (1) donne alors :

$$\sum_{i=0}^{m} R_i(\lambda) f(x,y)^i = 0\,, \qquad (x,y) \in V_\lambda\,.$$

Comme les nombres $R_0(\lambda), \ldots R_m(\lambda)$ ne peuvent être simultanément nuls, les nombres $f(x,y)$ avec $(x,y) \in V_\lambda$ ne peuvent prendre qu'un nombre fini de valeurs $c_1, \ldots, c_d$ dans K, c'est-à-dire $V_\lambda \subset \bigcup_{j=1}^{d} f^{-1}(\{c_j\})$. Or, chaque $f^{-1}(\{c_j\})$ $(j = 1, \ldots, d)$ est un fermé pour la topologie de Zariski de K^2 et comme V_λ est irréductible, il existe un indice $j \in \{1, \ldots, d\}$ tel que $V_\lambda \subset f^{-1}(\{c_j\})$. Par conséquent f est constante sur toute composante irréductible V_λ des courbes de niveau $\{P = \lambda\}$ sauf pour un nombre fini de λ. D'où (ii).

(ii) $\Rightarrow$ (i) : On désigne par $(V_n)_{n>0}$ une suite infinie de composantes irréductibles des courbes de niveau de P où la fonction f est constante; on note $\{P = \lambda_n\}$ la courbe de niveau dont V_n est une composante $(n > 0)$. Il est classique que "f est constante sur V_n" entraîne que le déterminant $\mathrm{Jac}(P, f)$ de la matrice jacobienne de P et f est nul sur V_n $(n > 0)$: cela se voit par exemple en écrivant que $K(V_n) = K(X, y)$ avec y solution de $P(X, y) = \lambda_n$ et que la dérivation $\frac{\partial}{\partial X}$ se prolonge au corps de fonctions $K(V_n)$ par $\frac{\partial y}{\partial X} = -\frac{\partial P}{\partial X}/\frac{\partial P}{\partial Y}$ et en développant $\frac{\partial}{\partial X}(f(X, y)) = 0$. Posons

$$\mathrm{Jac}(P, f) = \frac{N(X, Y)}{D(X, Y)}, \qquad \text{avec } N, D \in K[X, Y] \text{ et } (N, D) = 1\,.$$

Le fermé $Z(N)$ contient donc une infinité de composantes irréductibles V_n qui sont deux à deux disjointes. Il en résulte que $N \equiv 0$ et donc $\mathrm{Jac}(P, f) \equiv 0$. Il est classique (voir par exemple [6, p. 12]) que cela entraîne que f et P sont algébriquement dépendants sur K. ∎

Dans la suite, pour $\underline{\lambda} = (\lambda_1, \ldots, \lambda_m) \in K^m$, on note $G(P, \underline{\lambda})$ le groupe multiplicatif engendré par tous les diviseurs des polynômes $P - \lambda_i$, pour $i = 1, \ldots, m$.

LEMME 3.2. *Soient $F_1, \ldots, F_r \in G(P, \underline{\lambda})$. Si $r \geq \deg(P)$ alors il existe $m_1, \ldots, m_r$ des entiers non tous nuls tels que la fonction rationnelle $\prod_{i=1}^{r} F_i^{m_i}$ est algébriquement dépendante avec P.*

Démonstration. Soient $F_1, \ldots, F_r \in G(P, \underline{\lambda})$. Il est classique (voir par exemple [1]) que l'ensemble E des $\lambda \in K$ tel que $\{P = \lambda\}$ est une courbe singulière est fini. On choisit un $\lambda \in K \setminus (E \cup \{\lambda_1, \ldots, \lambda_m\})$ et une composante irréductible S de la courbe de niveau $\{P = \lambda\}$. Soient $q_1, \ldots, q_d$ les points à l'infini de S dans un modèle projectif lisse $\overline{S}$ de S. Notons ν_{ij} l'ordre de F_i au point q_j, et $\mathcal{M}$ la matrice $(\nu_{ij})_{1 \leq i \leq r,\ 1 \leq j \leq d}$.

Les fonctions F_i sont régulières et n'ont pas de zéros sur S d'après notre choix de λ. Les zéros et pôles de chaque fonction F_i $(i = 1, \ldots, r)$, vues sur $\overline{S}$, se trouvent donc dans la partie à l'infini. La nullité du degré du diviseur (F_i), se traduit donc par $\sum_{j=1}^{d} \nu_{ij} = 0$ pour tout $i = 1, \ldots, r$. Par conséquent $\mathrm{rg}(\mathcal{M}) < d \leq \deg(P)$ et grâce à notre hypothèse $r \geq \deg(P)$, il existe alors $m_1(\lambda, S), \ldots, m_r(\lambda, S)$ des entiers non tous nuls tels que

$$\sum_{i=1}^{r} m_i(\lambda, S)\nu_{ij} = 0\,, \qquad j = 1, \ldots, d\,.$$

Considérons maintenant la fonction rationnelle

$$f_{\lambda,S} = \prod_{i=1}^{r} F_i^{m_i(\lambda,S)}\,.$$

Cette fonction est régulière et n'a pas de zéros sur S. De plus, par construction, elle n'a ni zéros ni pôles aux points à l'infini $q_1,\dots,q_d$. Par conséquent $f_{\lambda,S}$ est constante sur S.

Conclusion : pour tous choix de λ et S comme ci-dessus, il existe un r-uplet $(m_1(\lambda,S),\dots,m_r(\lambda,S)) \in \mathbb{Z}^r \setminus \{(0,\dots,0)\}$ tel que la fonction rationnelle $f_{\lambda,S} = \prod_{i=1}^{r} F_i^{m_i(\lambda,S)}$ est constante sur la composante irréductible S. Comme le corps K est supposé non-dénombrable, il existe une infinité de couples (λ,S) pour lesquels les r-uplets $(m_1(\lambda,S),\dots,m_r(\lambda,S))$ prennent la même valeur, qu'on note $(m_1,\dots,m_r)$. En conséquence, la fonction rationnelle $f = \prod_{i=1}^{r} F_i^{m_i}$ est constante sur les composantes S correspondantes. D'où f et P sont algébriquement dépendants sur K en vertu de la Proposition 3.1. ∎

Remarque. Le Lemme 3.2 a été démontré dans [10, Proposition 1.3], à l'aide du noyau de la dérivation jacobienne de $K(X,Y)$ associée au polynôme P.

4. Preuve du théorème fondamental

On suppose que $P(X,Y)$ est non-composé. D'après le Théorème 1.1, l'ensemble $\sigma(P)$ est fini. Notons $\lambda_1,\dots,\lambda_r$ ses éléments. Supposons que

$$\sum_{j=1}^{r} \rho_{\lambda_j}(P) \geq \deg(P)\,.$$

On note, pour tout $j = 1,\dots,r$,

$$P - \lambda_j = \prod_{i=1}^{n_j} F_{j,i}^{k_{j,i}}\,, \qquad k_{j,i} \in \mathbb{N}^*,$$

une décomposition de $P - \lambda_j$ en produit de facteurs irréductibles $F_{j,i} \in K[X,Y]$. On considère la famille de polynômes

$$\{F_{1,1},\dots,F_{1,n_1-1},\dots,F_{r,1},\dots,F_{r,n_r-1}\}\,.$$

Tous les polynômes de cette famille sont dans le groupe $G(P, \lambda_1, \dots, \lambda_r)$ et leur nombre est

$$\sum_{j=1}^{r}(n_j - 1) = \sum_{j=1}^{r} \rho_{\lambda_j}(P) \geq \deg(P)\,.$$

Par conséquent, d'après le Lemme 3.2, il existe une famille d'entiers non tous nuls $\{m_{1,1}, \dots, m_{1,n_1-1}, \dots, m_{r,1}, \dots, m_{r,n_r-1}\}$ telle que la fonction rationnelle

$$f = \prod_{j=1}^{r} \prod_{i=1}^{n_j-1} {F_{j,i}}^{m_{j,i}} \tag{2}$$

soit algébriquement dépendante avec P. Mais d'après le lemme de Gordan (voir [9, §1.2, Theorem 3 and Theorem 4]) appliqué pour $n = 2$ à $\mathbf{K}= K(P, f)$, on a $P,\ f \in K(h)$, avec $h \in K[X, Y]$. De plus P est un polynôme non-composé, alors $P = a \cdot h + b$, avec $(a, b) \in K^* \times K$. Par conséquent $f \in K(P)$. On peut donc écrire $f = q(P)/t(P)$, avec $q(T), t(T) \in K[T]$ et $(q, t) = 1$. On note $\mu_1, \dots, \mu_s$ les racines de q dans K et $\mu_{s+1}, \dots, \mu_N$ celles de t. On a donc

$$f = \eta \cdot \frac{\prod_{i=1}^{s}(P - \mu_i)}{\prod_{i=s+1}^{N}(P - \mu_i)}\ , \tag{3}$$

avec $\eta \in K^*$.

Soit $m_{k,\ell}$ un des entiers $m_{j,i}$ non nul. En comparant (2) et (3), on obtient que le facteur $F_{k,\ell}$ divise un des polynômes $P - \mu_i$, $i = 1, \dots, N$. Comme $F_{k,\ell}$ divise $P - \lambda_k$, il en résulte que $\lambda_k \in \{\mu_1, \dots, \mu_N\}$, et donc par (3), que $P - \lambda_k$ est un facteur du numérateur ou du dénominateur de f. Mais alors F_{k,n_k} devrait apparaître dans la décomposition (2) de f. D'où la contradiction qui permet de conclure que $\rho(P) < \deg(P)$. ∎

Acknowledgements

L'auteur veut remercier le Prof. P. Dèbes et l'anonyme referee dont les commentaires lui ont permis de beaucoup améliorer le texte. Il veut aussi remercier le staff du centre Abdus Salam "ICTP", Trieste (Italy) où une grande partie de cet article a été écrite.

Références

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

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

[3] A. Bodin, P. Dèbes, S. Najib, On indecomposable polynomials and their spectrum (preprint).

[4] A. Bodin, P. Dèbes, S. Najib, Irreducibility of hypersurfaces, *Comm. Algebra* (to appear).

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

[6] S. Lefshetz, "Algebraic Geometry", Princeton University Press, Princeton, N.J., 1953.

[7] S. Najib, Une généralisation de l'inégalité de Stein-Lorenzini, *J. Algebra* **292** (2) (2005), 566–573.

[8] S. Najib, "Factorisation des Polynômes $P(X_1,\dots,X_n)-\lambda$ et Théorème de Stein", Thèse de Doctorat, Université Lille 1, 2005.

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

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