Numéro d'ordre : 3611

Université de Lille I
U.F.R. de Mathématiques. Laboratoire P. Painlevé U.M.R. 8524

Factorisation des polynômes $P(X_1, \ldots, X_n) - \lambda$ et théorème de Stein.

Thèse

de

Salah NAJIB

pour obtenir le titre de

Docteur en mathématiques pures

Spécialité : **Théorie des nombres**

Soutenue le 18 mars 2005 devant la Commission d'Examen :

Président		
Michel	**Langevin**	Université de Bordeaux I
Rapporteurs		
Peter	**Fleischmann**	University of Kent (GB)
Dino	**Lorenzini**	University of Georgia (USA)
Examinateurs		
Bruno	**Deschamps**	Université du Maine (Le Mans)
Eric	**Reyssat**	Université de Caen
R. James	**Shank**	University of Kent (GB)
Directeurs		
Mohamed	**Ayad**	Université du Littoral
Pierre	**Dèbes**	Université Lille I

Remerciements

En premier lieu, les mots sont faibles pour exprimer ma reconnaissance à mes directeurs de thèse Mohamed Ayad et Pierre Dèbes pour tout ce qu'ils m'ont apporté durant l'élaboration de ce travail. Leur passion et leur soif de découvrir, peut-être plus encore que leur disponibilité de tous les instants et leur impressionnante culture mathématique, ont transformé toutes nos discussions en véritables moments de bonheur. A leurs côtés, l'étude des polynômes et leur irréductibilité m'est apparue comme un agréable voyage.

Je suis très reconnaissant à Peter Fleischmann d'avoir accepté d'être rapporteur ; je le remercie aussi pour les encouragements qu'il m'a prodigués à la fin de son agréable exposé à Lille. Thank you Peter.

J'ai bien sûr été très honoré que Dino Lorenzini ait accepté d'être rapporteur de ma thèse, et je tiens également à le remercier d'avoir été aussi précis et consciencieux dans ses observations. Le présent texte porte la trace de son magnifique article "Reducibility of polynomials in two variables", et de ses commentaires sur mon travail.

Les corps hilbertiens apparaissent souvent dans ce travail. Je suis content que Bruno Deschamps soit membre de mon jury ; je le remercie par ailleurs pour ses conseils lors de notre discussion à la fin de l'un de ses exposés ici à Lille.

Je tiens à remercier chaleureusement Michel Langevin de m'avoir fait l'honneur d'accepter de faire partie de mon jury ; j'ai été sensible aux remarques qu'il m'a faites et aux conseils qu'il m'a donnés à la fin de mon premier exposé à la Chevaleret (Paris).

Mon premier exposé à Caen m'a donné l'occasion de rencontrer Eric Reyssat et d'avoir avec lui une discussion intéressante. Je voudrais le remercier de me faire le plaisir d'être membre de mon jury.

Je tiens à remercier R. James Shank, de me faire le grand honneur de venir de Kent à Lille pour être membre de mon jury. Thank you James.

Durant ma thèse j'ai eu des échanges fructueux avec Michael Fried, particulièrement sur la composition des polynômes en une variable, qui a un lien fort avec ses travaux, notamment le problème de "Hilbert-Siegel". Donc, je le remercie de l'intérêt évident qu'il a porté à mon travail. Thank you Mike.

Driss Essouabri, Pierre Liardet et Jean-Pierre Tignol ont manifesté un vif intérêt pour cette thèse qui se situe à la frontière de leur domaines de préoccupations ; je les en remercie très chaleureusement.

Je remercie mes enseignants de l'université d'El-Jadida (Maroc) pour leur encouragements tout au long de toute ma vie universitaire.

J'ai assuré les TD du cours de statistique et de probabilité de Nadia Bensaid et Olivier Torres à l'université de Lille 3. J'ai beaucoup apprécié leurs qualités d'enseignant : ils sont à la fois exigeants et respectueux des étudiants. Par ailleurs ce sont eux qui m'ont donné l'occasion de fréquenter le monde des mathématiques appliquées. Je remercie aussi tout le personnel de l'université de Lille 3.

Je tiens à remercier également, Mohammed Ably, Eva Bayer-Fluckiger, Jean-Luc Chabert, Pietro Corvaja, Jean D'Almeida, Jean-Claude Douai, Michel Emsalem, Youssef Hantout, Sadok Kallel, Mostapha Mbekhta, Mohamed M'zari, Niels Borne, Patrice Philippon, Ould Saïd Elias, Philippe Ryckelynck, Alain Salinier, Bouchaïb Sodaigui, Daniel Tanré, Michel Waldschmidt, Umberto Zannier pour leur soutien durant ces trois années.

Je remercie nos secrétaires Raymonde Berat, Soledad Cuenca et Valérie Hemeidan. Je remercie mes collègues Jean-Jacques et Michel de l'imprimerie du batiment M2. Je remercie également tout le personnel de l'université de Lille 1.

Je tiens à remercier ma famille, notamment ma mère, de son soutien inconditionnel durant toute ma vie étudiante. Merci pour tout.

Enfin et surtout, je pense à mon épouse, pour avoir supporté et accepté que je me plonge de longues journées dans mon travail.

Je salue les copains thésards de mathématique et d'informatique. Je salue tous mes amis de la résidence universitaire Galois, quelle ambiance au sein de cette chouette bande !

Je veux dire à tous mes amis combien ils comptent pour moi et comme leur soutien m'a tenu chaud. J'ai été particulièrement ému de l'intérêt porté à mon travail par Stéphane, Jean-Paul, Yann, Elguendafi, Mouloudi, Mohamed, Nidal, Anna, Abdessamad, Abdellah, Séverine, Stylian.

Villeneuve d'Ascq, le 15 mars 2005.

Table des matières

Notations

$A[X_1, \ldots, X_n]$ anneau des polynômes à n indéterminées à coefficients dans un anneau A
$K(X_1, \ldots, X_n)$ corps des fractions rationnelles à n indéterminées à coefficients dans le corps K
$K(X, Y)^*$ groupe multiplicatif du corps $K(X, Y)$
$\chi(K)$ caractéristique du corps K
$\overline{K}$ une clôture algébrique de K
ker$D$ noyau de la dérivation D
rg(M) rang de la matrice M
$Z(P)$ fermé de Zariski associé au polynôme P
$H(P_1, \ldots, P_r)$ partie Hilbertienne associée aux polynômes $P_1, \ldots, P_r$
deg(P) degré du polynôme P
deg$_X(P)$ degré du polynôme P ordonné suivant les puissances décroissantes de X
deg$_{\underline{X}}(P)$ degré total de P, vu comme polynôme en $\underline{X} = (X_1, \ldots, X_n)$
(A,B) pgcd des polynômes A et B
$M_{n\times n}(K)$ anneau des matrices carrées $n \times n$ à coefficients dans K
$GL_n(K)$ groupe linéaire de K^n
$\sigma(P)$ spectre du polynôme P
$A \setminus B$ complémentaire de B dans l'ensemble A
card(F) cardinal de l'ensemble F
$\rho_\lambda(P)$ ordre partiel de réductibilité du polynôme P associé à un $\lambda \in \overline{K}$
$\rho(P)$ ordre total de réductibilité du polynôme P.

Introduction

Les questions que nous allons étudier portent sur la réductibilité des polynômes en plusieurs variables sur un corps arbitraire. Plus précisément, soient K un corps quelconque et $P(X_1, \ldots, X_n)$ un polynôme non constant, en les indéterminées $X_1, \ldots, X_n$ $(n \geq 2)$, à coefficients dans le corps K. L'ensemble des valeurs λ qui sont dans une clôture algébrique $\overline{K}$ de K pour lesquelles le polynôme $P - \lambda$ est réductible sur $\overline{K}$, qui est appelé le *spectre* de P et noté $\sigma(P)$, joue un rôle central dans ce travail.

Une première information, qu'on obtient à partir du théorème de Bertini-Krull est que si P est non composé sur $\overline{K}$, alors l'ensemble $\sigma(P)$ est fini. En 1989, Stein a donné une première majoration du cardinal de $\sigma(P)$, dans la situation où le corps de base K est algébriquement clos, non dénombrable de caractéristique nulle. De façon précise, il a montré que si $P(X, Y)$ est non composé sur K alors $\mathrm{card}(\sigma(P)) \leq \deg(P) - 1$; géométriquement, si $P(X, Y)$ est non composé sur K alors le nombre de fibres réductibles du polynôme P est $\leq \deg(P) - 1$. Ce résultat constitue le point de départ de cette thèse.

En 1992, Cygan a étendu l'inégalité de Stein au cas d'un nombre $n \geq 2$ quelconque de variables (par réduction au cas $n = 2$), sur $K = \mathbb{C}$. Dans la même année, Kaliman a développé l'interprétation géométrique ci-dessus du résultat de Stein sur $K = \mathbb{C}$ et pour le cas de deux variables $(n = 2)$. Le résultat de Kaliman donne une première amélioration de la borne démontrée par Stein.

Un peu plus tard, en 1993, Vistoli a prouvé le résultat dans le cas d'un corps algébriquement clos, de caractéristique nulle et un nombre $n \geq 2$ quelconque de variables. En 1993 également, Lorenzini a considéré pour la première fois le cas de caractéristique quelconque, pour $n = 2$; il a donné d'autre

part une deuxième amélioration de la borne qui figure dans l'inégalité originale.

Au chapitre 3, nous donnerons une nouvelle démonstration qui prouve la meilleure inégalité, celle de Lorenzini, sur un corps de caractéristique quelconque et pour un nombre $n \geq 2$ quelconque de variables ; nous procédons par réduction au cas $n = 2$ (voir chapitre 3, théorème fondamental).

Nous nous sommes également intéressés à la question suivante : étant donné un ensemble fini $S \subset K$, peut-on construire un polynôme P dont le spectre soit l'ensemble S? Nous répondons par l'affirmative au chapitre 4.

Plus précisément, notre résultat est qu'on peut fixer à l'avance les éléments λ du spectre ainsi que le nombre de facteurs irréductibles des $P(\underline{X})-\lambda$, et même, dans une certaine mesure tous les facteurs irréductibles des $P - \lambda$ sauf un (voir théorèmes 4.1.1 et 4.1.2 pour plus de précision). Ce résultat est établi sur un corps K infini, de caractéristique quelconque et pour un nombre $n \geq 2$ quelconque de variables.

Nous avons divisé le texte en quatre chapitres.

Chapitre 1 : Généralités. Nous y introduisons les outils et le langage utilisés dans toute la suite de ce travail. On rappele les définitions de *composition* de polynômes, de *spectre* $\sigma(P)$, *d'ordre partiel* $\rho_\lambda(P)$ relatif à λ, *d'ordre total* $\rho(P)$ de réductibilité d'un polynôme non constant P. Puis on montre à partir du théorème de Bertini-Krull que le spectre $\sigma(P)$ d'un polynôme non composé P est fini. C'est le résultat fondamental de ce chapitre. Nous montrerons également que ce spectre est indépendant du corps algébriquement clos contenant les coefficients de P.

Chapitre 2 : Inégalité de Stein et méthode de Stein. On considère un corps K algébriquement clos, non dénombrable de caractéristique nulle et $P(X, Y) \in K[X, Y]$ un polynôme non constant. L'inégalité de Stein est celle donnée par le théorème suivant :

Théorème — *Si* $P(X, Y)$ *est non composé alors* $\mathrm{card}(\sigma(P)) \leq \rho(P) \leq \deg(P) - 1$.

Dans ce chapitre, nous reprenons la méthode utilisée par Stein. Elle passe par une étude préalable des "*noyaux des dérivations jacobiennes*".

Chapitre 3 : Améliorations de l'inégalité de Stein. Ce chapitre reprend pour l'essentiel le contenu de notre article "Une généralisation de l'inégalité de Stein-Lorenzini". Son objet est de montrer par une nouvelle méthode purement algébrique la meilleure inégalité de Lorenzini dans le cas d'un corps de caractéristique quelconque et pour un nombre $n \geq 2$ quelconque de variables. Nous utilisons une induction sur le nombre de variables n.

Chapitre 4 : Sur le spectre d'un polynôme à plusieurs variables. Ce chapitre reprend notre article "Sur le spectre d'un polynôme à plusieurs variables" (paru à Acta Arithmetica). Le résultat principal est qu'on peut construire des polynômes $P(\underline{X})$ pour lesquels les éléments λ du spectre donnés avec le nombre de facteurs irréductibles de $P(\underline{X}) - \lambda$, c'est-à-dire $\rho_\lambda(P) + 1$, ont été fixés à l'avance. Dans l'article correspondant, on supposait K de caractéristique 0. Ici, K est infini de caractéristique quelconque. Ce résultat plus général apparaît dans l'article ultérieur (qui correspond au chapitre 3) comme conséquence de l'extension de l'inégalité de Stein au cas de caractéristique ≥ 0 et de $n \geq 2$ variables.

Chapitre 1

Généralités

Dans ce chapitre, nous rappelons les notions de *spectre* et de *degrés partiel et total de réductibilité* d'un polynôme. Nous allons donner aussi les premiers résultats généraux qui montrent notamment que le spectre d'un polynôme non composé est fini et ne dépend pas du corps algébriquement clos contenant les coefficients.

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

1.1 Problème

Le problème qui motive ce travail est la réductibilité des polynômes $P(\underline{X}) - \lambda$ pour $\lambda \in \overline{K}$. Plus précisément, on va étudier l'ensemble des valeurs $\lambda \in \overline{K}$ pour lesquelles le polynôme $P(\underline{X}) - \lambda$ est réductible sur $\overline{K}$.

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

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

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

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

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

1.2 Finitude de $\sigma(P)$

Dans cette section, on va donner une caractérisation de la finitude du spectre $\sigma(P)$. Plus précisément, nous allons donner une preuve du théorème fondamental ci-dessous.

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 $P(\underline{X}) = u(Q(\underline{X}))$. [1]

Théorème fondamental — *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* $\overline{K}$,
(iv) *le polynôme* $P(\underline{X}) - T$ *est réductible dans* $\overline{K(T)}[\underline{X}]$, *où* T *est une variable.*

Ainsi, si le polynôme $P(\underline{X})$ est non composé, son spectre est un ensemble fini.

Dégageons également l'implication suivante que nous utiliserons plusieurs fois : si $P(\underline{X})$ est irréductible dans $\overline{K}[\underline{X}]$ alors $P(\underline{X})$ est non composé sur $\overline{K}$. Noter que "irréductible dans $K[\underline{X}]$" ne suffit pas : penser à $P(\underline{X}) = (XY)^2 - 2$.

Nous allons établir le théorème fondamental à partir de la proposition suivante qui est due à Bertini pour $K = \mathbb{C}$ (1882) et à Krull pour le cas général (1937).

1. On peut noter que pour tout polynôme non constant $P(\underline{X}) \in K[\underline{X}]$, il existe $p_0 \in K[\underline{X}]$ non composé et $\phi \in K[T]$ tels que $P(\underline{X}) = \phi(p_0(\underline{X}))$.

Proposition 1.2.1 — *Soient* $\underline{T} = (T_1, \ldots, T_m)$ *des variables algébriquement indépendantes sur* $\overline{K}(\underline{X})$ *et* $F(\underline{X}, \underline{T}) \in K[\underline{X}, \underline{T}]$ *un polynôme irréductible avec* $\deg_{\underline{T}}(F) = 1$.
Alors $F(\underline{X}, \underline{\lambda})$ *est réductible sur* $\overline{K}$ *pour tout* $\underline{\lambda} = (\lambda_1, \ldots, \lambda_m) \in \overline{K}^m$, *tel que* $\deg_{\underline{X}} F(\underline{X}, \underline{\lambda}) = \deg_{\underline{X}} F(\underline{X}, \underline{T})$ *si et seulement si*

- *ou bien* $\chi(K) = 0$ *et*

$$F(\underline{X}, \underline{T}) = \sum_{i=0}^{d} a_i(\underline{T}) \Phi(\underline{X})^{d-i} \Psi(\underline{X})^i,$$

avec $d \geq 1$ *un entier,* $a_i(\underline{T}) \in \overline{K}[\underline{T}]$, $(i = 0, \ldots, d)$ *et* $\Phi(\underline{X}), \Psi(\underline{X}) \in \overline{K}[\underline{X}]$ *tels que* $\deg_{\underline{X}} F > \max(\deg \Phi(\underline{X}),\ \deg \Psi(\underline{X}))$,

- *ou bien* $F(\underline{X}, \underline{T}) \in \overline{K}[\underline{X}^p, \underline{T}]$, *avec* $p = \chi(K) > 0$ *et* $\underline{X}^p = (X_1^p, \ldots, X_n^p)$.

Preuve. Une preuve de cette proposition est donnée dans [33 ; théorème 37, §3.3]. ■

1.3 Preuve du théorème fondamental

L'équivalence **(i)** $\Leftrightarrow$ **(iv)** est le classique théorème de Bertini-Noether (voir par exemple [14 ; prop. 9.29, p. 120]).

Les deux implications **(iv)** $\Rightarrow$ **(ii)** et **(ii)** $\Rightarrow$ **(i)** sont évidentes.

Pour l'implication **(iii)** $\Rightarrow$ **(ii)**, on suppose que $P(\underline{X})$ est composé sur $\overline{K}$, c'est-à-dire il existe deux polynômes $u(Z) \in \overline{K}[Z]$, avec $\deg(u) \geq 2$ et $Q(\underline{X}) \in \overline{K}[\underline{X}]$ tels que $P(\underline{X}) = u(Q(\underline{X}))$. Alors pour tout $\lambda \in \overline{K}$, le polynôme $P(\underline{X}) - \lambda$ est réductible sur $\overline{K}$. En effet, $u(Z) - \lambda$ considéré comme polynôme en Z, se factorise sur $\overline{K}$ en produit de facteurs du premier degré

$$u(Z) - \lambda = a \prod_{j=1}^{s} (Z - \alpha_j),$$

où $a \in K^*$ et les α_j sont des éléments de $\overline{K}$. Alors

$$P(\underline{X}) - \lambda = u(Q(\underline{X})) - \lambda = a\prod_{j=1}^{s}(Q(\underline{X}) - \alpha_j).$$

Enfin, pour l'implication **(ii)** $\Rightarrow$ **(iii)**, on va distinguer les deux cas suivants :

1$^{\text{er}}$cas : $\chi(K) = 0$.

Supposons que **(ii)** est satisfaite. Alors comme $\deg_{\underline{X}}(P(\underline{X})-T) = \deg_{\underline{X}}(P(\underline{X})-\lambda)$ pour tout $\lambda \in \overline{K}$, d'après la proposition 1.2.1, pour $m = 1$, on peut écrire

$$\textbf{(*)} \qquad P(\underline{X}) - T = \sum_{i=0}^{d} a_i(T)\Phi(\underline{X})^{d-i}\Psi(\underline{X})^i,$$

avec $d \geq 1$ un entier, $a_i(T) \in \overline{K}[T]$, $(i = 0, \ldots, d)$ et $\Psi(\underline{X}), \Phi(\underline{X}) \in \overline{K}[\underline{X}]$ tels que $\deg_{\underline{X}}(P) > \max(\deg(\Phi), \deg(\Psi))$.

En dérivant les deux membres de l'égalité **(*)** par rapport à T, on obtient

$$\textbf{(**)} \qquad -1 = \sum_{i=0}^{d} a_i'(T)\Phi(\underline{X})^{d-i}\Psi(\underline{X})^i,$$

ou encore

$$-1 = a_{i_0}'(T)\Psi(\underline{X})^{i_0}\prod_{i=1}^{d-i_0}(\Phi(\underline{X}) - \beta_i\Psi(\underline{X})),$$

où $\beta_1, \ldots, \beta_{d-i_0}$ sont les racines de $\sum_{i=0}^{d} a_i'(T)z^{d-i} = 0$ et i_0 est le premier indice tel que $a_{i_0}'(T) \neq 0$. Alors puisque $\Phi(\underline{X})$ et $\Psi(\underline{X})$ ne doivent pas être à la fois dans $\overline{K}$, on a nécessairement $i_0 = d$, $\Psi(\underline{X}) = c \in \overline{K}$, $a_i(T) = a_i$ pour $i < d$ et $a_d(T) = -T + \alpha$, $\alpha \in K$. D'où

$$P(\underline{X}) - T = b_0\Phi(\underline{X})^d + b_1\Phi(\underline{X})^{d-1} + \ldots + b_{d-1}\Phi(\underline{X}) + c^d(-T + \alpha),$$

avec $b_i = c^i a_i$ pour $i = 0, \ldots, d-1$. Donc pour $T = 0$, on a

$$P(\underline{X}) = u(\Phi(\underline{X}))$$

avec

$$u(Z) = b_0 Z^d + b_1 Z^{d-1} + \ldots + b_{d-1} Z + c^d \alpha.$$

De plus, on a $\deg(P) = \deg(u)\deg(\Phi)$, et comme $\deg(P) > \max(\deg(\Phi), \deg(\Psi))$ par hypothèse, on a alors $\deg(u) > 1$. Ceci montre bien que le polynôme P est composé sur $\overline{K}$.

2$^{\text{eme}}$cas : $\chi(K) = p > 0$.

Supposons que $P(\underline{X}) - \lambda$ est réductible sur $\overline{K}$ pour tout $\lambda \in \overline{K}$. Alors, d'après la proposition 1.2.1 pour $m = 1$, on a $P(\underline{X}) - T = F(\underline{X}^p, T) \in \overline{K}[\underline{X}^p, T]$. En particulier, pour $T = 0$, on obtient $P(\underline{X}) = F(\underline{X}^p, 0) \in \overline{K}[\underline{X}^p]$. D'où $P(\underline{X})$ s'écrit sous la forme $[G(\underline{X})]^p$ avec $G(\underline{X}) \in \overline{K}[\underline{X}]$ et donc le polynôme P est composé sur $\overline{K}$. ■

1.4 Indépendance du spectre par rapport au corps

Dans cette section, nous allons montrer que la propriété "$P(\underline{X}) \in C[\underline{X}]$ est composé sur C" ne dépend pas du corps algébriquement clos C, et que, dans le cas où P est non composé, son spectre n'en dépend non plus. Ce résultat nous permettra, par exemple dans la première section du chapitre 3, de déduire certains résultats pour tout corps de caractéristique 0 à partir du cas $K = \mathbb{C}$.

Soient C un corps algébriquement clos de caractéristique quelconque, $K \subset C$ un sous-corps et $P(\underline{X}) \in K[\underline{X}]$. On pose

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

et

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

les spectres du polynôme P relatifs respectivement aux corps C et $\overline{K}$. Le second correspond à notre définition de départ du spectre. Nous allons démontrer la proposition suivante :

Proposition — *Si P est non composé sur $\overline{K}$ alors P est non composé sur C et $\sigma_C(P) = \sigma_{\overline{K}}(P)$; la définition du spectre ne dépend pas du corps algébriquement clos contenant les coefficients de P. De même pour les nombres $\rho_\lambda(P)$ et $\rho(P)$.*

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

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

Soit F le corps engendré sur $\overline{K}$ par λ et les coefficients de Q et R; c'est une extension de type fini, on peut donc l'écrire $F = \overline{K}(t_1, \ldots, t_d)$. Le corps F est isomorphe au corps des fractions $\mathrm{frac}(\overline{K}[X_1, \ldots, X_d]/I)$ de l'anneau quotient de $\overline{K}[X_1, \ldots, X_d]$ par un idéal premier I. La factorisation **(*)** se réécrit sous la forme

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

Notons $Z(I)$ le fermé de Zariski associé à l'idéal I. Pour tout d-uplet $({t_1}^0, \ldots, {t_d}^0)$ d'éléments de $\overline{K}$ dans un ouvert de Zariski de $Z(I)$, la spécialisation correspondante fournit une décomposition non triviale dans $\overline{K}[\underline{X}]$

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

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

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 facteurs irréductibles $f_{\lambda,i} \in \overline{K}[\underline{X}]$ 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 $\overline{K}$ et donc les nombres $\rho_\lambda(P)$ et $\rho(P)$ non plus. ■

1.5 Commentaires

1.5.1 Sur la composition des polynômes

On a le résultat qui est dû à Furushima [16] pour le cas de deux variables, qui est aussi redémontré par Lin et Zaidenberg dans [23]. Ensuite, il est étendu par Cygan [7] et également par Ploski [31] pour un nombre $n \geq 2$ de variables pour prendre la forme suivante : *soit* $P \in \mathbb{C}[\underline{X}]$, *alors il existe* $p_0 \in \mathbb{C}[\underline{X}]$ *primitif (au sens de ces auteurs c'est-à-dire, les polynômes* $p_0 - c$ *sont irréductibles pour tout* $c \in \mathbb{C}$ *sauf un nombre fini) et* $\phi \in \mathbb{C}[T]$ *tels que* $P(\underline{X}) = \phi(p_0(\underline{X}))$, *(en remplacant* p_0 *par* $p_0 - c$ *et* $\phi(T)$ *par* $\phi(T + c)$, *on peut prendre* p_0 *irréductible).* De plus, cette décomposition est unique à un automorphisme linéaire près (voir par exemple [7]). De plus, noter que modulo le théorème fondamental de ce chapitre, les deux notions "primitif" et "non composé" sont équivalentes.

Dans le cas de deux variables X et Y, Ayad et Ryckelynck dans [4] ont donné une méthode pour détecter qu'un polynôme $P(X, Y)$ est composé et sinon déterminer les valeurs $\lambda \in \sigma(P)$ qui sont en nombre fini. Ayad dans [2], a donné aussi notamment en caractéristique nulle et dans le cas de deux variables, d'autres conditions qui sont équivalentes au fait qu'un polynôme P est non composé, par exemple, que *"l'anneau* $K[P]$ *est intégralement fermé dans* $K[X, Y]$*"*. On a aussi le fait suivant qui est une conséquence du théorème 7 démontré dans [2] pour $n = 2$ et pour le cas où $\chi(K) = 0$: *"P est non composé sur K" si et seulement si "P est non composé sur* $\overline{K}$*"*. Cependant, cette équivalence ne reste plus vraie dans le cas où $\chi(K) = p > 0$, par exemple, si on suppose le corps K non parfait et on considère le polynôme $P(X, Y) = X^p + aY^p$, avec $a \in K \setminus K^p$. On vérifie aisément que P est composé sur $\overline{K}$ mais non sur K. Pour plus de détails, nous renvoyons par exemple à [2], [4], [29] et [30].

1.5.2 Sur le cas d'une seule variable

Dans le cas d'une seule variable, si on adopte la première définition de composition d'un polynôme, alors tout polynôme de degré ≥ 2 sera composé, d'où l'introduction d'une nouvelle définition. 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 $p(X) = r(q(X))$. Par exemple, on a le fait suivant : *supposons que* $p(X) \in K[X]$ *et que* $\chi(K) = 0$ *ou* $(\deg(p), \chi(K)) = 1$. *Alors* $p(X)$ *est strictement non composé sur* K *si et seulement si* $p(X)$ *est strictement non composé sur* $\overline{K}$, (voir par exemple [15] ou [33]).

Pour $p(X) \in \mathbb{Q}[X]$ donné de degré ≥ 2, si $t \in p(\mathbb{Q})$ alors $p(X) - t$ est réductible. Dans ce contexte, Fried dans [12], [13] a montré le résultat suivant : *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.* Cette approche a été développée par Müller dans [27], à savoir : *soit* $f(T, X) \in \mathbb{Q}[T, X]$ *absolument irréductible. Supposons que, pour une infinité de* $t \in \mathbb{Z}$, $f(t, X)$ *est réductible mais n'a pas de facteur linéaire. Peut-on conclure nécessairement* $\deg_X(f) = 5$? Müller a montré que oui si le groupe de Galois de $f(T, X)$ sur $\mathbb{Q}(T)$ est le groupe symétrique ou si $\deg_X(f)$ est premier.

De plus Dèbes et Fried ont montré dans [9], [10] 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* $t \in \mathbb{Z} \setminus p(\mathbb{Q})$. 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 $\deg(p) = 5$.

Chapitre 2

Inégalité de Stein et méthode de Stein

Étant donnés deux polynômes $f(X,Y),\ g(X,Y) \in K[X,Y]$, considérons un faisceau de courbes planes $\alpha f(X,Y) + \beta g(X,Y)$, où $\alpha,\ \beta \in K$. Si on suppose que la courbe générique dans ce faisceau est irréductible, alors combien le faisceau contient-il de courbes réductibles ? Ce problème a été étudié par Ruppert [32] qui a montré qu'on a au plus $d^2 - 1$ courbes réductibles, où $d = \max(\deg(f),\ \deg(g))$. L'étude de la réductibilité des polynômes $P(X,Y) - \lambda$ est un cas particulier de ce problème général. Dans ce cas, on a une borne meilleure, obtenue initialement par Stein dans [35] en caractéristique 0 suite aux travaux de Bertini, Krull et Ruppert : si $P(X,Y)$ est non composé sur K, alors $\mathrm{card}(\sigma(\mathrm{P})) \leq \rho(P) \leq d - 1$.

Dans ce chapitre, on va expliquer la méthode qu'a suivi Stein pour démontrer son résultat que l'on appellera par la suite *inégalité de Stein*.

Tout au long des deux premières sections de ce chapitre, K désigne un corps algébriquement clos, de caractéristique nulle et non dénombrable et X et Y sont deux variables algébriquement indépendantes sur K et enfin $P(X,Y) \in K[X,Y]$ un polynôme non constant.

2.1 Inégalité de Stein

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

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

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

où le nombre $\rho(P)$ a été défini dans le chapitre 1, section 1.1.

Géométriquement, si le polynôme P est non composé alors le nombre de ses fibres réductibles $\Gamma_\lambda := \{(x,y) \in K^2 : P(x,y) = \lambda\}, \ \ (\lambda \in K)$ (qui sont des courbes algébriques affines) est au plus égal à $\deg(P) - 1$.

On peut ainsi préciser le théorème fondamental du chapitre 1 (pour $n = 2$) : 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 $t \in K$.

L'exemple classique suivant montre que la borne $\deg(P)-1$ est optimale : soit $P(X,Y) = Y + X\prod_{i=0}^{d-2}(Y+i)$, avec $d = \deg(P) \geq 2$. On a $\deg_X(P) = 1$, donc P est non composé. De plus on a $P(X,Y)+j = (Y+j)+X\prod_{i=0}^{d-2}(Y+i)$. On déduit facilement que $\sigma(P) = \{0,\ldots,d-2\}$ et que $\rho(P) = d-1 = \deg(P)-1$.

Il y a des améliorations de l'inégalité de Stein ; elles feront l'objet du chapitre 3.

2.2 Méthode de Stein

La méthode de Stein utilise la notion de dérivation d'une $K-$algèbre, notamment quelques propriétés des noyaux des dérivations jacobiennes de $K[X,Y]$ et de leur prolongement à $K(X,Y)$.

2.2.1 Noyaux des dérivations jacobiennes

Soit E une algèbre commutative sur un anneau A commutatif unitaire. On appelle *dérivation* de E une application $D : E \to E$, A-linéaire, telle que : $D(xy) = D(x)y + xD(y)$ pour tous $x,\ y \in E$.

Dans cette section, on considérera un type spécifique de dérivations. On définit l'application :

$$D_P : K[X,Y] \to K[X,Y]$$

$$f \mapsto D_P(f) = \frac{\partial P}{\partial X}\frac{\partial f}{\partial Y} - \frac{\partial P}{\partial Y}\frac{\partial f}{\partial X}$$

D_P est une dérivation de $K[X,Y]$ appelée *dérivation jacobienne*. De plus, D_P se prolonge d'une façon unique en une dérivation $\widetilde{D_P}$ de $K(X,Y)$ définie par

$$\widetilde{D_P}(\frac{u}{v}) = \frac{D_P(u)v - D_P(v)u}{v^2}$$

pour u et v des éléments de $K[X,Y]$ premiers entre eux.

Stein a exploité les noyaux des dérivations D_P et $\tilde{D_P}$ que l'on notera respectivement $C(P)$ et $\tilde{C}(P)$. On vérifie aisément que $C(P)$ est une sous $K-$algèbre de $K[X,Y]$, que $\tilde{C}(P)$ est un sous-corps de $K(X,Y)$ et que la propriété suivante est satisfaite : pour tout $r \in \mathbb{Z}$, $f^r \in C(P) \Rightarrow f \in C(P)$ et également $f^r \in \tilde{C}(P) \Rightarrow f \in \tilde{C}(P)$. La proposition suivante donne une caractérisation de ces noyaux.

Proposition 2.2.1.1 — *Pour $f \in K(X,Y)$ une fonction rationnelle donnée, les assertions suivantes sont équivalentes :*
(i) *$f \in \tilde{C}(P)$,*
(ii) *f et P sont algébriquement dépendants sur K,*
(iii) *f est constante sur toute composante irréductible des courbes de niveau $\{P = \lambda\}$ sauf pour un nombre fini de λ,*
(iv) *f est constante sur une infinité de composantes irréductibles des courbes de niveau $\{P = \lambda\}$.*

Preuve. Le fait que $f \in \tilde{C}(P)$ est équivalent à dire que le déterminant de la matrice jacobienne de P et f est nul. Or, il est classique que le rang de cette matrice est égal au degré de transcendance de l'extension algébrique $K(P,f)/K$ qui vaut 1 si et seulement si f et P sont algébriquement dépendants sur K (voir par exemple [22 ; p. 12]). D'où l'équivalence **(i)** $\Leftrightarrow$ **(ii)**.

Dans le reste de 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.

(ii) ⇒ (iii) : supposons que P et f sont algébriquement dépendants sur K, c'est-à-dire, on a une relation de type :

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

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. Ecrivons aussi $f(X,Y) = u(X,Y)/w(X,Y)$, avec $(u,w) = 1$. 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 :

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

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 $V_\lambda \subset f^{-1}(\{c_j\})$. D'où f est constante sur V_λ.

(iii) ⇒ (iv) : évident.

(iv) ⇒ (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 $\widetilde{D_P}(f) = 0$ 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 $\widetilde{D_P}(f) = \frac{N(X,Y)}{D(X,Y)}$, avec $N(X, Y),\ D(X, Y) \in K[X, Y]$ 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 $\widetilde{D_P}(f) \equiv 0$, c'est-à-dire $f \in \tilde{C}(P)$. ■

La remarque suivante est une conséquence de l'équivalence **(i) ⇔ (ii)**.

Remarque 2.2.1.2. *Soit $A \in C(P)$ avec $\deg(A) \geq 1$. Alors on a $C(A) = C(P)$ et $\tilde{C}(A) = \tilde{C}(P)$.*

En effet, si $f \in \tilde{C}(A)$, alors f et A sont algébriquement dépendants sur K, d'où f est algébrique sur $K(A)$. Or, $A \in C(P)$, donc A est algébrique sur $K(P)$, par conséquent f est algébrique sur $K(P)$. D'où $f \in \tilde{C}(P)$ d'après la proposition 2.2.1.1, et de la même manière, on montre que $\tilde{C}(P) \subset \tilde{C}(A)$. On a donc $\tilde{C}(A) = \tilde{C}(P)$, dont découle $C(A) = C(P)$. ■

Le théorème suivant qui relie les noyaux $C(P)$ et $\tilde{C}(P)$ au spectre de P est le résultat central de ce chapitre. Il est démontré au §2.2.3.

Théorème 2.2.1.3 — *On a équivalence entre :*
(1) $\deg(P) = \min\{\deg(Q)/Q \in C(P) \setminus K\}$,
(2) $\sigma(P) \neq K$,
(3) $C(P) = K[P]$,
(4) $\tilde{C}(P) = K(P)$,
(5) $P(X, Y)$ *est non composé.*

2.2.2 Lemme préliminaire

Dans la suite, on note $G(P)$ le groupe multiplicatif engendré par tous les diviseurs des polynômes $P-\lambda$, pour tout $\lambda \in K$. On a

$$G(P) = \bigcup_{\underline{\lambda} \in K^m} G(P, \underline{\lambda}),$$

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

Lemme 2.2.1.4 — *Soient $F_1, \ldots, F_r \in G(P)$. Si $r \geq \deg(P)$ alors il existe $m_1, \ldots, m_r$ des entiers non tous nuls tels que la fonction rationnelle $\prod_{i=1}^{r} F_i^{m_i}$ appartienne à $\tilde{C}(P)$.*

Preuve. Soient $F_1, \ldots, F_r \in G(P, \underline{\lambda})$ pour un certain $\underline{\lambda} = (\lambda_1, \ldots, \lambda_m) \in K^m$. 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 M la matrice :

$$\mathrm{M} = \begin{pmatrix} \nu_{11} & \nu_{12} & \cdots & \nu_{1d} \\ \nu_{21} & \nu_{22} & \cdots & \nu_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ \nu_{r1} & \nu_{r2} & \cdots & \nu_{rd} \end{pmatrix}$$

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 $\mathrm{rg}(M) < d \leq \deg(P)$ 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 $\sum_{i=1}^{r} m_i(\lambda, S)\nu_{ij} = 0, \quad (j = 1, \ldots, d)$.

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 $q_1, \ldots, q_d$. 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 $(m_1(\lambda,S),\ldots,m_r(\lambda,S)) \in \mathbb{Z}^r \setminus \{(0,\ldots,0)\}$ 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 couple (λ,S) pour lesquels les $r-$uplets $(m_1(\lambda,S),\ldots,m_r(\lambda,S))$ prennent la même valeur, qu'on note $(m_1,\ldots,m_r)$. En conséquence, la fonction rationnelle $f = \prod_{i=1}^r F_i^{m_i}$ est constante sur les composantes S correspondantes. D'où $f \in \tilde{C}(P)$ en vertu de la proposition 2.2.1.1. ■

2.2.3 Preuve du théorème 2.2.1.3.

Nous utiliserons les définitions suivantes.

Définitions 2.2.1.5 (a) *on dit qu'un système $\{F_1,\ldots,F_r\}$ d'éléments de $G(P)$ est P-libre si pour tout r-uplet $(m_1,\ldots,m_r) \in \mathbb{Z}^r$, on a $\prod_{i=1}^r F_i^{m_i} \in \tilde{C}(P)$ entraîne que $m_i = 0$ pour tout $i = 1,\ldots,r$.*
(b) *un système P-libre $\{F_1,\ldots,F_r\}$ d'éléments de $G(P)$ est dit maximal si pour tout $F \in G(P)$, la famille $(F_1,\ldots,F_r,F)$ n'est pas P-libre.*

(1) ⇒ (2) : supposons que $\sigma(P) = K$. Pour tout $\alpha \in K$, on choisit F_α un facteur irréductible de $P - \alpha$ tel que $\deg(F_\alpha) < \deg(P)$. Choisissons aussi un système P-libre maximal (qui existe d'après le lemme de Zorn). Cet ensemble est fini de cardinal $< \deg(P)$ d'après le lemme 2.2.1.4. Notons $F_1,\ldots,F_r$ ses éléments. On a $r \geq 1$ car $\{F_\alpha\}$ constitue un système P-libre : en effet, si on suppose que $F_\alpha^q \in \tilde{C}(P)$ pour un certain entier $q \neq 0$, on a alors $F_\alpha \in \tilde{C}(P) \cap K[X,Y] = C(P)$. Ceci est impossible puisque $\deg(F_\alpha) < \deg(P)$ et $\deg(P)$ est minimal.

Le système $\{F_1,\ldots,F_r,F_\alpha\}$ n'est pas P-libre. Par les définitions 2.2.1.5, il existe $m_{1\alpha},\ldots,m_{r\alpha}$ et m_α des entiers non tous nuls tels que $F_\alpha^{m_\alpha}\prod_{i=1}^r F_i^{m_{i\alpha}} \in \tilde{C}(P)$. De plus K étant non dénombrable, l'application $\alpha \mapsto (m_{1\alpha},\ldots,m_{r\alpha},m_\alpha)$ de K dans $\mathbb{Z}^{r+1}$ n'est pas injective. Donc il existe α, β deux éléments distincts de K tels que $m_\alpha = m_\beta = m$ et $m_{i\alpha} = m_{i\beta} = m_i$, pour tout $i = 1,\ldots,r$.

D'où

$$F_\alpha^m \prod_{i=1}^{r} F_i^{m_i} \in \tilde{C}(P) \quad \text{et} \quad F_\beta^m \prod_{i=1}^{r} F_i^{m_i} \in \tilde{C}(P).$$

Ainsi, $(F_\alpha/F_\beta)^m \in \tilde{C}(P)$, ce qui entraîne $F_\alpha/F_\beta \in \tilde{C}(P)$. De plus, en posant $P-\alpha = F_\alpha G_\alpha$ et $P-\beta = F_\beta\, G_\beta$, avec $G_\alpha,\ G_\beta \in K[X,Y]$, on a $F_\alpha G_\beta = (F_\alpha/F_\beta)(P-\beta) \in \tilde{C}(P) \cap K[X,Y] = C(P)$ et de façon analogue, on a $F_\beta G_\alpha \in C(P)$.

Considérons maintenant le produit

$$(P-\alpha)(P-\beta) = (F_\alpha G_\beta)(F_\beta G_\alpha).$$

Si $\deg(F_\alpha G_\beta) > \deg(P)$, alors $\deg(F_\beta G_\alpha) < \deg(P)$ ce qui contredit l'hypothèse **(1)**. Idem si on suppose que $\deg(F_\alpha G_\beta) < \deg(P)$. Il en résulte alors que $\deg(F_\alpha G_\beta) = \deg(F_\beta G_\alpha) = \deg(P)$.

On note $(F_\alpha G_\beta)^+$, $(F_\beta G_\alpha)^+$ et P^+ les formes homogènes dominantes de $F_\alpha G_\beta$, $F_\beta G_\alpha$ et P respectivement ; elles sont de même degré. De plus, on a $\mathrm{Jac}(F_\alpha G_\beta, P) = D_P(F_\alpha G_\beta) = 0$. Cela entraîne $\mathrm{Jac}((F_\alpha G_\beta)^+, P^+) = 0$. Par conséquent, $(F_\alpha G_\beta)^+$ et P^+ sont deux polynômes homogènes de même degré qui ont un jacobien nul. D'où necéssairement $(F_\alpha G_\beta)^+ = cP^+$, avec $c \in K^*$ (un simple exercice qui utilise l'identité d'Euler).

On pose $A = F_\alpha G_\beta - cP$. On a $A \in C(P)$ et $\deg(A) < \deg(P)$, donc $A = c_1 \in K$ d'après l'hypothèse **(1)**. D'où

$$F_\alpha G_\beta = cP + c_1 = c(P + \frac{c_1}{c})$$

et comme F_α divise $P-\alpha$, alors $\alpha = -c_1/c$. En appliquant le même argument au polynôme G_β (qui est non constant par construction), on obtient aussi $\beta = -c_1/c$, ce qui est impossible puisque $\beta \neq \alpha$. Finalement $\sigma(P) \neq K$.

(2) ⇒ (3) : l'inclusion $K[P] \subset C(P)$ est toujours vraie.

Pour l'inclusion inverse, supposons que $\sigma(P) \neq K$. Soit $Q \in C(P)$. D'après le théorème fondamental du chapitre 1, $\sigma(P)$ est fini. Combiné à la proposition 2.2.1.1, cela entraîne qu'il existe $\lambda \in K$ tel que $P-\lambda$ est irréductible et la restriction de Q à la courbe $\{P=\lambda\}$ est constante. On a donc

$$Q = Q_1(P-\lambda) + c_1,$$

avec $Q_1 \in K[X,Y]$ et $c_1 \in K^*$.

Si $\deg(Q_1) = 0$ alors $Q \in K[P]$. Dans le cas contraire, $Q_1 \in \tilde{C}(P) \cap K[X,Y] = C(P)$ et $\deg(Q_1) < \deg(Q)$. On répète alors l'opération avec Q_1 et ainsi de suite, on obtient finalement $Q \in K[P]$ d'où la seconde inclusion $C(P) \subset K[P]$.

(3) ⇒ (4) : l'inclusion $K(P) \subset \tilde{C}(P)$ est facile. Soit $f = A/B \in \tilde{C}(P)$, avec $A, B \in K[X,Y]$ tels que $(A,B) = 1$. D'après la proposition 2.2.1.1, P et f sont algébriquement dépendants sur K, c'est-à-dire, il existe alors un polynôme $\sum_{i=0}^{s} R_i(X)Y^i$ de $K[X,Y]$, avec $R_s(X) \neq 0$ tel que $\sum_{i=0}^{s} R_i(P)f^i = 0$. Alors

$$R_s(P)A^s = -B\left(R_0(P)B^{s-1} + R_1(P)AB^{s-2} + \ldots + R_{s-1}(P)A^{s-1}\right)$$

et puisque $(A,B) = 1$, il s'ensuit que $R_s(P) = BU$ avec $U \in K[X,Y]$. Par conséquent $f = A/B = AU/R_s(P)$ ce qui donne $AU \in \tilde{C}(P) \cap K[X,Y]$, c'est-à-dire $AU \in C(P) = K[P]$ et $f \in K(P)$. D'où $\tilde{C}(P) = K(P)$.

(4) ⇒ (5) : supposons que P est composé, c'est-à-dire, il existe deux polynômes $R(T) \in K[T]$, $\deg(R) \geq 2$ et $H \in K[X,Y]$ tels que

$$\textbf{(*)} \qquad P(X,Y) = R(H(X,Y)).$$

Alors H et P sont algébriquement dépendants sur K et on a $H \in C(P) \subset \tilde{C}(P)$. Par utilisation de notre hypothèse $\tilde{C}(P) = K(P)$, on peut écrire H sous la forme : $H = A(P)/B(P)$, avec $A(T), B(T) \in K[T]$ et $(A,B) = 1$. Il existe $C(T)$ et $D(T)$ deux polynômes de $K[T]$ tels que $C(T)A(T) + D(T)B(T) = 1$, ce qui donne $C(P)A(P) + D(P)B(P) = 1$. Or, H étant un polynôme, $B(P)$ divise $A(P)$ ce qui entraîne que $B(P) = c \in K^*$, par conséquent

$$\textbf{(**)} \qquad H = \alpha A(P) \in K[P],$$

où $\alpha = 1/c$. Donc en combinant **(*)** et **(**)**, on a nécessairement $\deg(R) = 1$, d'où la contradiction souhaitée.

(5) ⇒ (1) : supposons que P est non composé. Soit $P_1 \in C(P)$ de degré minimal non nul. D'après la remarque 2.2.1.2, on a $C(P_1) = C(P)$.

Cela entraîne que le polynôme P_1 vérifie l'assertion **(1)**. D'après l'implication **(1)** $\Rightarrow$ **(3)** qui est déjà prouvée, on a donc $C(P_1) = K[P_1]$. On déduit que $P = u(P_1)$ (puisque $P \in C(P) = K[P_1]$). Comme P est non composé, on a donc $\deg(u) = 1$ et $\deg(P) = \deg(P_1)$. ■

2.2.4 Preuve du théorème fondamental

On suppose que $P(X, Y)$ est non composé. D'après le théorème fondamental du chapitre 1, l'ensemble $\sigma(P)$ est fini. Notons $\lambda_1, \ldots, \lambda_r$ ses éléments. Supposons que $\sum_{j=1}^{r} \rho_{\lambda_j}(P) \geq \deg(P)$.

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

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

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

On considère la famille de polynômes

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

Tous les polynômes de cette famille sont dans le groupe $G(P, \lambda_1, \ldots, \lambda_r)$ 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 2.2.1.4, il existe une famille d'entiers non tous nuls $\{m_{1,1}, \ldots, m_{1,n_1-1}, \ldots, m_{r,1}, \ldots, m_{r,n_r-1}\}$ telle que la fonction rationnelle

$$\textbf{(1)} \qquad f = \prod_{j=1}^{r} \prod_{i=1}^{n_j-1} {F_{j,i}}^{m_{j,i}}$$

est dans $\tilde{C}(P)$. Mais d'après le théorème 2.2.1.3, on a $\tilde{C}(P) = K(P)$. On peut donc écrire $f = u(P)/v(P)$, avec $u(T), v(T) \in K[T]$ et $(u, v) = 1$. On note $\mu_1, \ldots, \mu_s$ les racines de u dans K et $\mu_{s+1}, \ldots, \mu_q$ celles de v. On a donc

$$(\mathbf{2}) \qquad f = a\frac{\prod_{i=1}^{s}(P-\mu_i)}{\prod_{i=s+1}^{q}(P-\mu_i)},$$

avec $a \in K^*$.

Soit $m_{k,\ell}$ un des entiers $m_{j,i}$ non nul. En comparant **(1)** et **(2)** on obtient que le facteur $F_{k,\ell}$ divise un des polynômes $P-\mu_i,\ \ i=1,\ldots,q$. Comme $F_{k,\ell}$ divise $P-\lambda_k$, il en résulte que $\lambda_k \in \{\mu_1,\ldots,\mu_q\}$, et donc par **(2)**, 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 **(1)** de f. D'où la contradiction qui permet de conclure que $\rho(P) < \deg(P)$. ■

2.3 Commentaires

2.3.1 Complément

Stein a montré aussi dans [35] que l'ensemble des polynômes $T(X,Y) \in K[X,Y]$ pour lesquels l'équation $D_P(F) = TF$ possède une solution $F \in K(X,Y)^*$ est un $\mathbb{Z}-$module libre de rang fini. De plus, si $P \in K[Q]$ avec $Q \in K[X,Y]$ non composé alors ce rang est égal à $\rho(Q)$. En particulier, si P est non composé alors $\rho(P)$ est le rang de cet $\mathbb{Z}-$module.

2.3.2 Caractéristique positive

L'analogue du théorème 2.2.1.3, en particulier l'équivalence (5) $\Leftrightarrow$ (3), c'est-à-dire le fait que $P(X,Y)$ est non composé sur K si et seulement si $C(P) = K[P]$ n'est pas vraie si $\chi(K) = p > 0$. Par exemple pour $P = X^p + Y$, on a $Y^p \in C(P)$, mais $Y^p \notin K[P]$. La méthode de Stein n'est plus valable dans le cas où $\chi(K) > 0$.

Dans les deux sous-sections suivantes, on suppose que $\chi(K) = 0$.

2.3.3 Dérivations plus générales

Beaucoup de travaux ont été faits sur la structure des noyaux $\ker D$ et $\ker\tilde{D}$ d'une dérivation non nulle D de $K[\underline{X}]$ et de son prolongement $\tilde{D}$ à $K(\underline{X})$ respectivement. On sait par exemple que le corps des fractions

frac(ker$D$) de ker$D$ est de manière générale, un sous-corps de $K(\underline{X})$, de degré de transcendance sur K au plus égal à $n-1$. Par contre l'inclusion des corps frac(ker$D$) $\subset$ ker$\tilde{D}$ est stricte en général. Par exemple, définissons la dérivation D de $K[X,Y]$ par

$$D(\phi) = X\frac{\partial \phi}{\partial X} + Y\frac{\partial \phi}{\partial Y},$$

pour tout $\phi \in K[X,Y]$. On a ker$D = K$ mais $X/Y \in$ ker$\tilde{D}$. On peut se demander à quelle condition sur la dérivation D l'égalité frac(ker$D$) = ker$\tilde{D}$ est satisfaite ?

Dans le cas de deux variables ($n = 2$), Zielinsky dans [37] a montré que *si D est une dérivation localement nilpotente de $K[X,Y]$ (i.e., pour tout $\phi \in K[X,Y]$ il existe un entier $m > 0$ tel que $D^m(\phi) = 0$) alors on a égalité.* Ce résultat a été développé par Ayad et Ryckelynck, qui ont montré dans [5], dans le cas $n \geq 2$, que si ker$D$ contient $n-1$ polynômes algébriquement indépendants alors on a égalité. Pour plus de détails, nous renvoyons par exemple à [5], [11], [29], [30] et [37].

2.3.4 Dérivations jacobiennes en n variables

Le théorème 2.2.1.3 suggère le problème suivant :

Problème. Si $\underline{X} = (X_1, \ldots, X_n)$, avec $n \geq 2$ et si on fixe $(n-1)$ polynômes $\underline{f} = (f_1, \ldots, f_{n-1})$ dans $K[\underline{X}]$ algébriquement indépendants sur K, on définit la dérivation jacobienne D de $K[\underline{X}]$ par

$$D(g) = \mathrm{Jac}(\underline{f}, g),$$

pour tout $g \in K[\underline{X}]$. Existe-il $\underline{h} = (h_1, \ldots, h_{n-1})$ un $(n-1)-$uplet de polynômes dans $K[\underline{X}]$, algébriquement indépendants sur K et non composés tel que ker$D = K[\underline{h}]$ et ker$\tilde{D} = K(\underline{h})$? Et quelle relation de dépendance existe-t-il entre les f_i et les h_j pour $i, j = 1, \ldots, n-1$?

En vertu du théorème 2.2.1.3, la réponse au problème est oui pour $n = 2$: on prend h_1 non composé tel que $f_1 \in K[h_1]$.

D'après les résultats de la section 2.3.3, on a frac(ker$D$) = ker$\tilde{D}$.

Il est connu d'après Makar-Limanov [25], que la dérivation D définie dans ce problème est localement nilpotente. Par conséquent, en vertu d'un résultat de Miyanishi [26], on a $\ker D = K[g_1, g_2]$, avec $g_1, g_2 \in K[X_1, X_2, X_3]$ algébriquement indépendants sur K. Mais, on ne sait pas la réponse aux autres questions du problème.

Autrement, pour $n \leq 3$, on sait d'après Nagata-Nowicki [29 ; théorème 2.6 et proposition 3.2] (résultats démontrés pour toute dérivation non nulle de $K[\underline{X}]$), que $\ker D = K[h_1, h_2]$, avec $h_1, h_2 \in K[X_1, X_2, X_3]$ algébriquement indépendants sur K et non composés. Mais, on ne sait pas exactement la relation de dépendance entre les f_i et les h_j pour $i, j = 1, 2$. Pour $n > 3$, le problème est ouvert. Nous donnons par exemple comme références [11], [25], [26], [29] et [30], pour avoir plus d'informations sur ce genre de problèmes.

Chapitre 3

Améliorations de l'inégalité de Stein

Dans ce chapitre, K désigne un corps commutatif de caractéristique $\chi(K)$ quelconque, $\overline{K}$ 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 $n = 2$ et enfin $P(\underline{X}) \in K[\underline{X}]$ un polynôme non constant.

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

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

une décomposition du polynôme $P - \lambda$ en facteurs irréductibles $f_{\lambda,i} \in \overline{K}[\underline{X}]$.

Dans tout ce qui suit, on conserve les définitions et notations du chapitre 1, notamment celle de spectre $(\sigma(P))$, d'ordres de réductibilité partiels et total $(\rho_\lambda(P),\ \rho(P))$ pour $\lambda \in \overline{K}$ et de polynôme composé.

Après un bref historique des diverses améliorations de l'inégalité de Stein depuis 1989, nous proposons une démonstration qui permet d'établir la meilleure inégalité, celle de Lorenzini, dans le contexte le plus général, c'est-à-dire, caractéristique et nombre de variables $n \geq 2$ quelconques et de généraliser ainsi tous les résultats antérieurs.

3.1 Améliorations déjà connues

Une première amélioration a été faite par Cygan [7] en 1992, qui a montré l'inégalité de Stein dans le cas d'un nombre $n \geq 2$ de variables et $K = \mathbb{C}$. La méthode employée par Cygan est plus analytique, et procède par réduction au cas $n = 2$ (i.e., en utilisant l'inégalité de Stein originale). La même année, Kaliman dans [19], a trouvé dans le cas où $K = \mathbb{C}$ et $n = 2$ une meilleure borne que celle de Stein, à savoir : *si le polynôme $P(X, Y)$ est non composé, alors le nombre de fibres réductibles $\{(x, y) \in \mathbb{C}^2 : P(x, y) = \lambda\}$ $(\lambda \in \mathbb{C})$ du polynôme P est inférieur strictement au nombre de composantes horizontales*[1] *de la courbe algébrique $\overline{X} \setminus \mathbb{C}^2$, pour $\overline{X}$ une compactification régulière de $\mathbb{C}^2$ (à savoir que cette compactification est dépend de P) ; ce nombre est inférieur strictement à* $\deg(P)$. Un peu plus tard, Vistoli [36] en 1993 donne une preuve pour le cas d'un corps de caractéristique nulle et un nombre $n \geq 2$ de variables.

On peut en fait déduire le résultat de Vistoli à partir du résultat de Cygan pour $K = \mathbb{C}$, en utilisant les résultats de la section 1.4 du chapitre 1. En effet, pour $P \in K[\underline{X}]$, non composé, 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 $\sigma_{\overline{K_0}}(P) = \sigma_{\overline{K}}(P)$. Le corps K_0 peut être plongé dans $\mathbb{C}$. D'après le §1.4 du chapitre 1, le spectre et les nombres $\rho_\lambda(P)$ du polynôme $P \in K[\underline{X}]$ ne dépendent pas du corps algébriquement clos contenant les coefficients de P et peuvent donc être évalués en voyant $P \in \mathbb{C}[\underline{X}]$ via le plongement de $\overline{K_0}$ dans $\mathbb{C}$. Le résultat de Cygan s'applique et fournit l'inégalité désirée (pour le polynôme $P \in K[\underline{X}]$ de départ).

Pour le cas $n = 2$ et K algébriquement clos de caractéristique quelconque, Lorenzini [24] en 1993 a amélioré l'inégalité de Stein pour obtenir la forme suivante :

si $P(\underline{X}) \in K[\underline{X}]$ est non composé sur K alors on a

$$\rho(P) \leq \min_{\lambda \in \sigma(P)} \{\sum_{i=1}^{n(\lambda)} \deg(f_{\lambda,i})\} - 1$$

1. d'après Kaliman, si $\overline{X}$ est une compactification régulière de $\mathbb{C}^2$ telle que l'application polynomiale $P : \mathbb{C}^2 \to \mathbb{C}$ s'étend à une application régulière $\overline{P} : \overline{X} \to \mathbb{C}P^1$, alors $\overline{X} \setminus \mathbb{C}^2$ est une courbe algébrique. Une composante de cette courbe est dite *horizontale* si la restriction de $\overline{P}$ à cette composante est une application non constante.

dont le terme de droite est toujours $\leq \deg(P) - 1$. [2]

3.2 Notre généralisation

Dans cette section, nous allons démontrer la meilleure inégalité de Lorenzini dans le cas général d'un corps de caractéristique quelconque et pour un nombre arbitraire $n \geq 2$ de variables. De façon plus précise, on va montrer le théorème suivant :

Théorème fondamental — *Si $P(\underline{X}) \in K[\underline{X}]$ est non composé sur $\overline{K}$ alors on a*

$$\rho(P) \leq \min_{\lambda \in \sigma(P)} \{\sum_{i=1}^{n(\lambda)} \deg(f_{\lambda,i})\} - 1.$$

Noter qu'on suppose ici que P est non composé sur $\overline{K}$, et pas seulement sur K. Comme nous l'avons rappelé dans le §1.5.1 du chapitre 1, les deux propriétés ne sont pas équivalentes en caractéristique > 0.

Nous démontrons ce résultat par réduction au cas $n = 2$. Dans le cas particulier de l'inégalité de Stein en caractéristique 0, nos arguments fournissent une nouvelle preuve des résultats de Cygan et Vistoli.

3.2.1 Résultats préliminaires

L'idée de départ de la preuve du théorème fondamental est de considérer un polynôme $P(\underline{X}) \in K[\underline{X}]$ comme un polynôme en $n-1$ variables en le voyant dans $K(X_1)[X_2, \ldots, X_n]$.

Un polynôme $P(\underline{X}) \in K[\underline{X}]$ absolument irréductible (i.e., irréductible sur $\overline{K}$) en général n'est pas irréductible dans $\overline{K(X_1)}[X_2, \ldots, X_n]$: par exemple, le polynôme $Z^2 - XY^2$ est irréductible dans $\overline{K}[X, Y, Z]$, mais il est réductible dans $\overline{K(X)}[Y, Z]$. Cependant, après changement de variable $X \mapsto T = X + Y$, on a $P(T - Y, Y, Z) = Z^2 + Y^3 - TY^2$ qui est irréductible dans $\overline{K(T)}[Y, Z]$. En

2. Noter que cette nouvelle inégalité est strictement meilleure si un des exposants $k_{\lambda,i}$ est > 1.

général, on a l'énoncé ci-dessous (proposition 3.3.1.1). On utilise la notation suivante : pour $P(\underline{X}) \in K[\underline{X}]$ et $A = (a_{ij}) \in M_{n\times n}(K)$ une matrice carrée d'ordre n, on note

$$P_A(\underline{X}) = P(A.\underline{X}) = P(\sum_{j=1}^{n} a_{1j}X_j, \ldots, \sum_{j=1}^{n} a_{nj}X_j).$$

Proposition 3.3.1.1 — *Soient K un corps infini, $h \geq 1$, $n \geq 3$ des entiers et $P_1, \ldots, P_h \in K[\underline{X}]$ des polynômes absolument irréductibles. Alors il existe une matrice $B \in GL_n(K)$ telle que pour tout $\ell = 1, \ldots, h$,*
(a) *le polynôme $P_\ell(B.\underline{X})$ est irréductible dans $\overline{K(X_1)}[X_2, \ldots, X_n]$,*
(b) *le degré du polynôme $P_\ell(B.\underline{X})$ en $(X_2, \ldots, X_n)$ est égal au degré de P_ℓ, i.e., $\deg_{(X_2,\ldots,X_n)}(P_\ell(B.\underline{X})) = \deg_{\underline{X}}(P_\ell)$.*

Ce résultat est démontré dans [34 ; chap. 5, théorème 3D] pour un seul polynôme. Mais en modifiant légèrement la preuve dans [34], on peut obtenir la version avec plusieurs polynômes. [3]

Pour le confort du lecteur, nous donnons ci-dessous une preuve directe de la proposition 3.3.1.1. L'outil principal est l'énoncé suivant :

Proposition 3.3.1.2 — *Soit $Q(\underline{X}) \in K[\underline{X}]$ un polynôme absolument irréductible. On suppose que $\frac{\partial Q}{\partial X_1} \neq 0$. Alors il existe un sous-ensemble fini C de K tel que pour tout $t \in K \setminus C$, le polynôme $Q(Z + tX_2, X_2, \ldots, X_n)$ est irréductible dans $\overline{K(Z)}[X_2, \ldots, X_n]$.*

Preuve. Cet énoncé est une traduction polynomiale de la proposition 9.31 de [14]. L'irréductibilité du polynôme $Q(\underline{X})$ dans $\overline{K}[\underline{X}]$ correspond à la ré-

3. Plus précisément, il suffit de montrer que le lemme 3F dans [34] est vrai pour tout $c \in K$ sauf un nombre fini (et pas seulement pour un certain $c \in K$). Pour cela, on garde les notations utilisées dans la preuve du lemme 3F de [34]. De plus, pour $c \in K$, on note $K_{(c)} = [K({X_1}^{(c)})]^0(X_2, \ldots, X_m)$ et P_c la propriété : *il existe $\tilde{c} \in K$ différent de c tel que $K_{(c)} = K_{(\tilde{c})}$*. La preuve donnée dans [34] montre en fait que la conclusion du lemme 3F de [34] est vraie pour tout c satisfaisant la propriété P_c. Soit H l'ensemble des éléments $c \in K$ qui ne vérifient pas la propriété P_c : si $c \in H$, alors $K_{(c)} \neq K_{(\tilde{c})}$ pour tout $\tilde{c} \neq c$, c'est-à-dire, le corps $K_{(c)}$ est représenté sous cette forme uniquement par c. Or, ce corps est l'un des corps intermédiaires entre $K(X_1, \ldots, X_m)$ et L, lesquels sont en nombre fini. Cela entraîne que H est fini et pour tout $c \in K \setminus H$, la propriété P_c est vérifiée.

gularité de l'extension $F := \text{frac}(\overline{K}[\underline{X}]/Q(\underline{X}))$ de K. En appliquant la proposition 9.31 de [14] à la dérivation $D = \frac{\partial}{\partial X_2}$ de $K[X_2, \ldots, X_n]$, qui grâce à l'hypothèse $\frac{\partial Q}{\partial X_1} \neq 0$ s'étend à F, on obtient l'existence d'un sous-ensemble fini $C \subset K$ tel que pour tout $t \in K \setminus C$, F est une extension régulière de $K(X_1 - tX_2)$, ce qui en posant $Z = X_1 - tX_2$ équivaut à dire que le polynôme $Q(Z + tX_2, X_2, \ldots, X_n)$ est irréductible dans $\overline{K(Z)}[X_2, \ldots, X_n]$. ■

Preuve de la proposition 3.3.1.1. Dans une première étape, on construit une matrice inversible A telle que chacun des polynômes $P_\ell(A.\underline{X})$ ait toutes ses dérivées partielles non nulles. Ensuite, on appliquera la proposition 3.3.1.2 aux polynômes $P_\ell(A.\underline{X})$.

On se donne $n \geq 3$ un entier et $P_1, \ldots, P_h \in K[\underline{X}]$ des polynômes irréductibles sur $\overline{K}$. Pour $A = (a_{ij}) \in M_{n\times n}(K)$ une matrice carrée d'ordre n non nulle et pour $P = P_\ell$, on a pour $i = 1, \ldots, n$,

$$\frac{\partial P_A(\underline{X})}{\partial X_i} = a_{1i}\frac{\partial P}{\partial X_1}(A.\underline{X}) + \ldots + a_{ni}\frac{\partial P}{\partial X_n}(A.\underline{X}).$$

On considère le sous-espace vectoriel de $M_{n\times n}(K)$:

$$M_{i,P} := \{A \in M_{n\times n}(K) : a_{1i}\frac{\partial P}{\partial X_1}(\underline{X}) + \ldots + a_{ni}\frac{\partial P}{\partial X_n}(\underline{X}) = 0\}.$$

L'ensemble $M_{i,P}$ est différent de $M_{n\times n}(K)$. En effet, il existe $j = j(P) \in \{1, \ldots, n\}$ tel que $\frac{\partial P(\underline{X})}{\partial X_j} \neq 0$: sinon, en caractéristique nulle, le polynôme P serait constant, et, en caractéristique $p > 0$, on aurait $P = P(X_1^p, \ldots, X_n^p) \in (\overline{K}[\underline{X}])^p$. Si $i = j$, la matrice identité I_n n'est pas dans $M_{i,P}$. Si $i \neq j$, en prenant la matrice A de $M_{n\times n}(K)$ telle que

$$P_A(\underline{X}) = P(X_1, \ldots, X_{j-1}, X_j + aX_i, X_{j+1}, \ldots, X_n)$$

on a

$$\frac{\partial P_A(\underline{X})}{\partial X_i} = \frac{\partial P}{\partial X_i}(A.\underline{X}) + a\ \frac{\partial P}{\partial X_j}(A.\underline{X}) \neq 0$$

pour tout $a \in K$ sauf peut-être pour une valeur au plus.

Les sous-espaces $M_{i,P}$ ($i = 1, \ldots, n$ et $P = P_1, \ldots, P_h$), sont des fermés de Zariski de $M_{n\times n}(K)$ ainsi que $M_{n\times n}(K) \setminus GL_n(K)$. Comme le corps K est

infini, $M_{n\times n}(K)$ n'en est pas la réunion [4]. En conclusion il existe $A \in GL_n(K)$ telle que pour $P = P_1, \ldots, P_h$ et $i = 1, \ldots, n$, on a
$a_{1i}\ \frac{\partial P}{\partial X_1}(\underline{X}) + \ldots + a_{ni}\ \frac{\partial P}{\partial X_n}(\underline{X}) \neq 0$ et par conséquent
$a_{1i}\ \frac{\partial P}{\partial X_1}(A.\underline{X}) + \ldots + a_{ni}\ \frac{\partial P}{\partial X_n}(A.\underline{X}) \neq 0$, c'est-à-dire $\frac{\partial P_A(\underline{X})}{\partial X_i} \neq 0$.

Pour la deuxième étape, on fixe une matrice $A \in GL_n(K)$ qui vérifie la conclusion de la première étape. D'après la proposition 3.3.1.2, il existe un sous-ensemble fini C de K tel que si $t \in K \setminus C$, chacun des polynômes

$$P_\ell(A.(X_1 + tX_2, X_2, \ldots, X_n))$$

est irréductible dans $\overline{K(X_1)}[X_2, \ldots, X_n]$.

De plus, quitte à grossir un peu l'ensemble fini C, on peut supposer que ce polynôme est aussi de degré en $(X_2, \ldots, X_n)$ égal à $\deg_{\underline{X}}(P_\ell)$. En effet, on a $\deg_{\underline{X}} P_\ell(A.\underline{X}) = \deg_{\underline{X}}(P_\ell)$. Ecrivons

$$P_\ell(A.\underline{X}) = P_{\ell,d}(\underline{X}) + P_{\ell,d-1}(\underline{X}) + \ldots,$$

où les $P_{\ell,k}$ sont des polynômes homogènes, avec $\deg_{\underline{X}}(P_{\ell,k}) = k$ pour $k = 0, \ldots, d = \deg_{\underline{X}}(P_\ell)$. Les polynômes $P_{\ell,k}(X_1 + tX_2, X_2, \ldots, X_n)$ pour $t \in K$ et $k < d$ sont de degré en $(X_2, \ldots, X_n)$ strictement inférieur à d; et pour tout t sauf un nombre fini, on a

$$\deg_{(X_2,\ldots,X_n)} P_{\ell,d}(X_1 + tX_2, X_2, \ldots, X_n) = d$$

(voir que si $Q(\underline{X})$ est homogène de degré d, alors $Q(tX_2, X_2, \ldots, X_n)$ (comme polynôme en $(X_2, \ldots, X_n)$) l'est aussi pour tout $t \in K$ sauf un nombre fini).

La conclusion annoncée est satisfaite pour la matrice

$$B = A.\begin{pmatrix} 1 & t & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}, \qquad (t \notin C). \qquad \blacksquare$$

4. sinon, $M_{n\times n}(K)$ serait réunion finie d'hypersurfaces et il existerait un polynôme à n^2 variables et à coefficients dans K, non nul et dont la valeur en tout point de K^{n^2} serait nulle.

3.2.2 Preuve du théorème fondamental

Ici, le corps K est arbitraire et $\underline{X} = (X_1, \ldots, X_n)$, avec $n \geq 2$.

Le cas $n = 2$ a été démontré par Lorenzini [24 ; corollaire 1].

Supposons $n \geq 3$. Soit $P(\underline{X})$ un polynôme non composé sur $\overline{K}$. Soit $\lambda_0 \in \overline{K} \setminus \sigma(P)$, c'est-à-dire, le polynôme $P(\underline{X}) - \lambda_0$ est irréductible dans $\overline{K}[\underline{X}]$. De plus pour tout λ dans $\sigma(P)$, on écrit

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

une décomposition de $P(\underline{X})-\lambda$ en facteurs irréductibles $f_{\lambda,j} \in \overline{K}[\underline{X}]$. D'après la proposition 3.3.1.1 (appliquée au corps infini $\overline{K}$), il existe une matrice $B \in GL_n(\overline{K})$ telle que les polynômes $P(B.\underline{X}) - \lambda_0$ et $f_{\lambda,j}(B.\underline{X})$ sont irréductibles dans $\overline{K(X_1)}[X_2, \ldots, X_n]$ et de degré en $(X_2, \ldots, X_n)$ égal à $\deg_{\underline{X}}(P(\underline{X}) - \lambda_0)$ et $\deg_{\underline{X}}(f_{\lambda,j}(\underline{X}))$ respectivement pour tout $\lambda \in \sigma(P)$ et pour tout $j = 1, \ldots, n(\lambda)$. En particulier $P(B.\underline{X}) - \lambda_0$ est non composé sur $\overline{K(X_1)}$, ce qui entraîne que $P(B.\underline{X})$ lui-même est non composé sur $\overline{K(X_1)}$. Ici et dans la suite, le polynôme $P(B.\underline{X})$ ainsi que les polynômes $f_{\lambda,j}(B.\underline{X})$ sont considérés comme polynômes en $(X_2, \ldots, X_n)$ (tandis que P et les $f_{\lambda,j}$ le sont comme polynômes en $\underline{X}$).

En substituant $B.\underline{X}$ à $\underline{X}$ dans **(*)**, on obtient

$$P(B.\underline{X}) - \lambda = \prod_{j=1}^{n(\lambda)} f_{\lambda,j}(B.\underline{X})^{k_{\lambda,j}},$$

ce qui entraîne que $\sigma(P)$ (sous-ensemble de $\overline{K}$) est contenu dans $\sigma(P(B.\underline{X}))$ (sous-ensemble de $\overline{K(X_1)}$). De plus du fait que la matrice B est inversible, les facteurs $f_{\lambda,j}(B.\underline{X})$ sont distincts si les $f_{\lambda,j}(\underline{X})$ le sont. Par conséquent, pour $\lambda \in \sigma(P)$, les deux polynômes $P - \lambda$ et $P(B.\underline{X}) - \lambda$ ont le même nombre $n(\lambda)$ de facteurs irréductibles dans $\overline{K}[\underline{X}]$ et dans $\overline{K(X_1)}[X_2, \ldots, X_n]$ respectivement. Cela montre en particulier que $\rho(P) \leq \rho(P(B.\underline{X}))$.

Cette réduction va nous permettre de montrer le théorème fondamental par récurrence sur n. En effet, si on suppose que la conclusion de ce théorème est satisfaite pour un polynôme de $(n-1)$ variables, alors on a

$$\rho(P(B.\underline{X})) \leq \min_{\lambda \in \sigma(P(B.\underline{X}))} \{\sum_{j=1}^{\tilde{n}(\lambda)} \deg_{(X_2,\ldots,X_n)}(\Phi_{\lambda,j})\} - 1,$$

où les $\Phi_{\lambda,j}$ sont les facteurs irréductibles de $P(B.\underline{X}) - \lambda$ dans $\overline{K(X_1)}[X_2, \ldots, X_n]$ et $\tilde{n}(\lambda)$ leur nombre. Pour $\lambda \in \sigma(P)$, les $\Phi_{\lambda,j}$ correspondent aux $f_{\lambda,j}(B.\underline{X})$ et $\tilde{n}(\lambda) = n(\lambda)$. On déduit les inégalités

$$\rho(P) \leq \rho(P(B.\underline{X})) \leq \min_{\lambda \in \sigma(P)} \{\sum_{j=1}^{n(\lambda)} \deg_{(X_2,\ldots,X_n)}(f_{\lambda,j}(B.\underline{X}))\} - 1$$

dont le terme de droite est égal à $\min_{\lambda \in \sigma(P)} \{\sum_{j=1}^{n(\lambda)} \deg_{\underline{X}}(f_{\lambda,j})\} - 1$. ■

3.3 Commentaires

Pour démontrer notre théorème fondamental, on pouvait aussi penser à une réduction directe de n à 2 variables. Les résultats suivants vont dans ce sens.

Soient K un corps quelconque et $P(\underline{X}) \in K[\underline{X}]$ de degré total $\deg_{\underline{X}}(P) = d$.

Par la substitution suivante

$$X_i = a_i X + b_i Y + c_i, \;\; 1 \leq i \leq n,$$

avec a_i, b_i et c_i des éléments de K, on obtient dans $K[X, Y]$ le polynôme suivant :

$$\tilde{P} = P(a_1 X + b_1 Y + c_1, \ldots, a_n X + b_n Y + c_n).$$

Pour un choix "générique" de $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$, les deux polynômes P et $\tilde{P}$ ont la même factorisation dans $\overline{K}[\underline{X}]$ et dans $\overline{K}[X, Y]$ respectivement. Précisons.

Supposons qu'on prenne arbitrairement les $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ dans un sous-ensemble fini S de K. Pour quelle probabilité, les deux polynômes P et $\tilde{P}$ ont la même factorisation dans $\overline{K}[\underline{X}]$ et dans $\overline{K}[X, Y]$ respectivement ? Pour $K = \mathbb{C}$, Bajaj, Canny, Garrity et Warren ont montré dans [6 ; théorème 4.2] en modifiant la preuve de Mumford de la proposition 4.17 dans [28], que cette probabilité est au moins égal à $1 - (d^4 - 2d^3 + d^2 + d + 1)/\mathrm{card}(S)$. Pour un corps quelconque, Von Zur Gathen, a montré dans [18 ; théorème 4.5] en utilisant la théorie de l'élimination, qu'une telle probabilité est au moins

égal à $1 - 9^{d^2}/\mathrm{card}(S)$. Ensuite, en utilisant son algorithme de factorisation, Kaltofen, dans [20 ; corrolaire 2] l'a amélioré en $1 - 2d^4/\mathrm{card}(S)$. Et récemment, Gao, a montré dans [17 ; théorème 5.1] le résultat suivant : *si* $\chi(K) = 0$ *ou* $> 2d^2$. *Pour tout choix de* a_i, b_i *et* c_i *dans* S, *avec une probabilité au moins égal à* $1-2d^3/\mathrm{card}(S)$ *tous les facteurs absolument irréductibles de* P *restent des facteurs absolument irréductibles de* $\tilde{P}$ *après substitution.*

Gao a donné aussi la version ci-dessous, qui n'utilise pas le langage des probabilité, en introduisant la notion suivante qui est liée au théorème d'irréductibilité de Hilbert.

On dit qu'un point $(a_1, b_1, c_1, \ldots, a_n, b_n, c_n) \in K^{3n}$ est de *bonne Hilbertienneté* pour le polynôme P si tous les facteurs de P irréductibles dans $\overline{K}[\underline{X}]$ restent des facteurs de $\tilde{P}$ irréductibles dans $\overline{K}[X, Y]$. On définit $H_P(S)$ la densité des points dans S^{3n} de bonne Hilbertienneté pour le polynôme P, i.e.,

$$H_P(S) = \frac{(\text{le nombre de points de bonne Hilbertienneté pour } P \text{ dans } S^{3n})}{(\mathrm{card}(S))^{3n}}.$$

Alors sous les mêmes hypothèses de sa première version (théorème 5.1), on a d'après Gao [17 ; théorème 5.1'] :

$$H_P(S) \geq 1 - 2d^3/\mathrm{card}(S).$$

Si on regarde $a_1, b_1, c_1, \ldots, a_n, b_n, c_n$ comme des variables algébriquement indépendantes sur K et on pose $L = K(a_1, b_1, c_1, \ldots, a_n, b_n, c_n)$, alors $\tilde{P} \in L[X, Y]$.

Pour démontrer son théorème 5.1, Gao a utilisé un autre résultat qui est dû à Kaltofen [20], à savoir : *le polynôme* $\tilde{P}$ *est absolument irréductible sur* L *si et seulement si le polynôme* P *est absolument irréductible sur* K.

Chapitre 4

Sur le spectre d'un polynôme à plusieurs variables

Dans ce dernier chapitre, K désigne un corps commutatif infini de caractéristique $\chi(K)$ quelconque, $\overline{K}$ 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 $n = 2$ et enfin $P(\underline{X}) \in K[\underline{X}]$ un polynôme non constant.

Ce présent chapitre 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 facteurs irréductibles $f_{\lambda,i} \in \overline{K}[\underline{X}]$ pour $\lambda \in \sigma(P)$. Plus précisément, nous allons montrer, qu'on peut construire des polynômes $P(\underline{X}) \in K[\underline{X}]$ non composés sur $\overline{K}$ pour lesquels les éléments λ du spectre, avec le nombre de facteurs irréductibles de $P(\underline{X}) - \lambda$, c'est-à-dire $\rho_\lambda(P)+1$, sont donnés à l'avance. Nous montrerons qu'on peut même imposer à l'avance tous les facteurs irréductibles de $P(\underline{X}) - \lambda$ sauf un. Ce résultat est établi sur un corps infini K de caractéristique quelconque et pour un nombre $n \geq 2$ quelconque de variables.

4.1 Présentation des résultats

Nous allons montrer le résultat suivant.

Théorème 4.1.1 — *Soient K un corps infini et $\underline{X} = (X_1, \ldots, X_n)$ avec $n \geq 2$. Etant donnés*

- un entier $s \geq 1$ et un ensemble $\{a_1, \ldots, a_s\}$ d'éléments distincts de K,

- des entiers $\rho_1, \ldots, \rho_s$ positifs non nuls,

alors il existe un polynôme $P(\underline{X})$ dans $K[\underline{X}]$ non composé sur $\overline{K}$ (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 $\rho_{a_i}(P) = \rho_i,\ i = 1, \ldots, s$.

Si on voit les éléments λ du spectre $\sigma(P)$ comme des pôles vis-à-vis de l'irréductibilité et les paramètres $\rho_\lambda(P)$ comme l'ordre de ces pôles, le théorème 4.1.1 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 ci-dessous montre en 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 4.1.2 — *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 $K[\underline{X}]$ étrangers deux à deux, i.e., 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 sur $\overline{K}$ (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 4.1.3. (a) Dans cet énoncé, certains des polynômes f_i peuvent être choisis constants non nuls. Pour ces indices, la conclusion du théorème 4.1.2 est que $P(\underline{X}) - a_i$ est irréductible sur $\overline{K}$, i.e., $\rho_{a_i}(P) = 0$. Cela entraîne qu'il suffit de montrer l'énoncé sans la condition "P non composé sur $\overline{K}$". 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 sur $\overline{K}$, ce qui entraîne, que $P(\underline{X})$ lui-même est non composé sur $\overline{K}$. 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 sur $\overline{K}$".

(b) La condition $(f_i) + (f_j) = K[\underline{X}]$ qui apparait 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 4.1.1 (à partir du théorème 4.1.2). 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 4.1.2, il existe une infinité de polynômes $P(\underline{X}) \in K[\underline{X}]$ non composés sur $\overline{K}$ (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, $\rho_{a_i}(P)$ 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 pour $i = 1, \ldots, s$

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

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 aux conditions du théorème 4.1.2, 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 $\deg(f_i) = \rho_i = \rho_{a_i}(P)$, $i = 1, \ldots, s$;
on a

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

ce qui contredit la version générale de l'inégalité de Stein (i.e., le théorème fondamental du chapitre 3). ■

Remarques 4.1.4. (a) La preuve montre la forme plus précise suivante du théorème 4.1.1 : si en plus de $s \geq 1$, $\{a_1, \ldots, a_s\} \subset K$ et $\rho_1, \ldots, \rho_s \in \mathbb{N}^*$, on fixe aussi une forme linéaire $\ell(\underline{X}) = \alpha_1 X_1 + \cdots + \alpha_n X_n$ non nulle et une famille $\{\alpha_{i,k} |\ i = 1, \ldots, s, k = 1, \ldots, \rho_i\}$ d'éléments deux à deux distincts de K, alors il existe un polynôme $P(\underline{X})$ dans $K[\underline{X}]$ non composé sur $\overline{K}$ tel que $\prod_{k=1}^{\rho_i}(\ell(\underline{X}) + \alpha_{i,k})$ divise $P(\underline{X}) - a_i$, $i = 1, \ldots, s$, et $\deg(P) = \sum_{i=1}^{s} \rho_i + 1$.

(b) L'énoncé du théorème 4.1.1 est plausible pour un corps K fini (auquel cas $s \leq \mathrm{card}(K)$) : nous n'avons pas de contre-exemple. Si K est fini, on peut, par application du résultat au corps infini $\overline{K}$ obtenir un polynôme $P \in \overline{K}[\underline{X}]$ satisfaisant aux conclusions voulues. Mais il n'est pas clair qu'on puisse choisir $P \in K[\underline{X}]$. C'est de l'application du théorème 4.1.2 que provient la restriction à "K infini". Elle est principalement utilisée dans la proposition 4.1.1.1 ci-dessous qui donne explicitement des éléments d'une partie hilbertienne de $K(X)$. Il est vrai que le corps $K(X)$ est hilbertien pour K fini mais on ne dispose pas dans ce cas d'une forme aussi précise de ce résultat que pour un corps infini.

Le théorème 4.1.2, notre résultat principal, est démontré dans la section 4.1.2. Dans le paragraphe 4.1.1 nous établissons quelques résultats préliminaires à la preuve du théorème 4.1.2. Ensuite dans la section 4.2, nous énonçons et démontrons un résultat analogue au théorème 4.1.2, dans le cas d'une variable (sur un corps hilbertien). Enfin dans la section 4.3 nous donnons une deuxième preuve du théorème 4.1.1 dans le cas où le corps K est algébriquement clos.

4.1.1 Résultats préliminaires.

Quelques résultats sur les corps hilbertiens. Soient m, r et d des entiers ≥ 1. Pour $\underline{T} = (T_1, \ldots, T_m)$, $\underline{Z} = (Z_1, \ldots, Z_d)$ des indéterminées algébriquement indépendantes sur K et $P_1(\underline{T}, \underline{Z}), \ldots, P_r(\underline{T}, \underline{Z})$ r 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 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 4.1.1.1 — *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 [14] ou [21 ; prop. 4.1, p. 236].

Nous allons montrer 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 4.1.1.2 — *Soient $P_1(X,T,\underline{Z}),\ldots,P_r(X,T,\underline{Z})$ 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 $j=1,\ldots,r$.*

Cela veut dire que les polynômes spécialisés $P_1(X,t(X),\underline{Z}),\ldots,$ $P_r(X,t(X),\underline{Z}) \in K[X][\underline{Z}]$ sont non seulement irréductibles dans $\overline{K}(X)[\underline{Z}]$ mais sont également primitifs (i.e., les $P_r(X,t(X),\underline{Z})$ considérés comme polynômes en $\underline{Z}$, leurs coefficients sont premiers entre eux dans $K[X]$).

On va déduire le théorème 4.1.1.2 de la proposition 4.1.1.1 et du lemme suivant.

Lemme 4.1.1.3 — *Soient $A_0(X,T),\ldots,A_d(X,T) \in K[X,T]$ 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 $i=0,\ldots,d$.*

Preuve. Les polynômes $A_0(X,T),\ldots,A_d(X,T)$ 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 $u_0(X,T),\ldots,\ u_d(X,T) \in K[X,T]$ et il existe $\delta(X) \in K[X]$ non nul
tels que

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

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

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

Pour tout $x \in \overline{K}$, 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 $A_0,\ldots,A_d$ sont premiers entre eux.

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

$$\begin{cases} F = \{y \in \overline{K} : y \text{ racine d'un des polynômes } A_{i(x_j)}(x_j,T),\ j = 1,\ldots,l\} \\ G = \{x_1,\ldots,x_l\} \end{cases}$$

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 $i = 0,\ldots,d$. Sinon ces polynômes auraient une racine commune dans $\overline{K}$, qui serait alors un des éléments de G, disons x_j. Mais alors on aurait $A_i(x_j,t(x_j)) = 0$ pour tout $i = 0,\ldots,d$, ce qui, pour $i = i(x_j)$ contredit le fait que $t(x_j) \notin F$. ■

Preuve du théorème 4.1.1.2. Soient $P_1,\ldots,P_r$ 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 4.1.1.1 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 $H_{P_1,\ldots,P_r}$.

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

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

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

D'après l'hypothèse du théorème 4.1.1.2, pour chaque $j = 1, \ldots, r$, les polynômes $A_{j,\underline{i}}(X, T)$ sont premiers entre eux dans $\overline{K}[X, T]$. En vertu du lemme 4.1.1.3, 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 $j = 1, \ldots, r$.

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 $\lambda_0 \neq \frac{f - t_0}{g - x_0}$, 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 $x \in G_j$, $(j = 1, \ldots, r)$". Pour $t(X)$ ainsi construit, on obtient que les polynômes $P_j(X, t(X), \underline{Z})$ sont irréductibles dans $\overline{K}(X)[\underline{Z}]$ (proposition 4.1.1.1) et sont primitifs (lemme 4.1.1.3), $j = 1, \ldots, r$. ■

Remarque 4.1.1.4. Le théorème 4.1.1.2 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 4.1.1.5 — *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 4.1.1.6. Une application du théorème 4.1.1.2 au polynôme $P(\underline{X}, T)$ du lemme 4.1.1.5 (vu comme polynôme dans $K[X_1][T][X_2, \ldots, X_n]$) 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 $(X_2, \ldots, X_n)$, alors il existe une infinité de $m(X_1) \in K[X_1]$

tel 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.

4.1.2 Preuve du théorème 4.1.2.

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'homorphisme $\phi : K[\underline{X}] \to \prod_{i=1}^{s} K[\underline{X}]/(f_i)$ 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 4.1.1.2. Nous allons l'appliquer aux polynômes

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

avec les variables X, T et $\underline{Z}$ du théorème 4.1.1.2 prises respectivement égales à X_1, T et $(X_2, \ldots, X_n)$. Vérifions d'abord que ces polynômes satisfont aux conditions du théorème 4.1.1.2. Pour vérifier l'irréductibilité de ces polynômes dans $\overline{K}[X, T, \underline{Z}] = \overline{K}[\underline{X}, T]$, on utilise le lemme 4.1.1.5.

Les polynômes p_i et $\prod_{\substack{1 \leq j \leq s \\ j \neq i}} f_j$ 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 4.1.1.2 : il existe une infinité de $m(X_1) \in K[X_1]$ de degré 1 tels que les polynômes

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

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

$$\begin{cases} P(\underline{X}) &= P_0(\underline{X}) + m(X_1) \prod_{i=1}^{s} f_i(\underline{X}), \\ H_i(\underline{X}) &= p_i(\underline{X}) + m(X_1) \prod_{\substack{1 \leq j \leq s \\ j \neq i}} f_j(\underline{X}) \end{cases}$$

on obtient

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

et les polynômes $H_i,\ (i = 1, \ldots, s)$ sont irréductibles dans $\overline{K}[\underline{X}]$. De plus, on peut choisir $m(X_1)$ de telle sorte que H_i ne divise pas $f_i,\ i = 1, \ldots, s$: 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 être tous des diviseurs irréductibles de $f_i,\ i = 1, \ldots, s$. Compte tenu de la remarque 4.1.3 (a), cela achève la preuve de la première partie du théorème 4.1.2.

Pour la deuxième partie, on note $I \subset \{1, \ldots, s\}$ 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 $m_i \geq 1$ est le nombre de facteurs de f_i. La condition $(f_i) + (f_j) = K[\underline{X}]$ pour $i \neq j$ 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 $k = 1, \ldots, m_i$ et $h = 1, \ldots, m_j$; les $g_{i,k}$ sont donc de la forme $\alpha_1 X_1 + \ldots + \alpha_n X_n + \alpha_{i,k}$ (à un coefficient multiplicatif près), avec $i \in I,\ k = 1, \ldots, m_i$ et où les $\alpha_{i,k}$ sont deux à deux distincts. Pour tous indices $i, j \in I,\ k = 1, \ldots, m_i$ et $h = 1, \ldots, m_j$ tels que $(i,k) \neq (j,h)$, on pose $u_{i,k,j,h} = \frac{1}{\alpha_{i,k} - \alpha_{j,h}}$ et $v_{i,k,j,h} = -u_{i,k,j,h}$; 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 $k = 1, \ldots, m_i$, en développant l'identité

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

on obtient que le polynôme défini par

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

vérifie $1 - b_{i,k} \in (g_{i,k})$ et $b_{i,k} \in \bigcap_{(j,h)\neq(i,k)} (g_{j,h})$. 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 $\deg(P_0) \leq \max_{i,k}\{\deg(b_{i,k})\} = (\sum_{i=1}^{s} \deg(f_i)) - 1$.

La première partie de la preuve, appliquée pour ce polynôme $P_0(\underline{X})$ conduit à un polynôme $P(\underline{X})$ satisfaisant aux conditions souhaitées avec $\deg(P) = (\sum_{i=1}^{s} \deg(f_i)) + 1$. ■

Remarque. On peut donner des conditions plus générales sur le choix des polynômes f_i. En effet : 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 $\deg(P_0) \leq (\sum_{i=1}^{s} \deg(f_i)) - \deg(g)$. 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 $(\sum_{i=1}^{s} \deg(f_i)) + 1$.

4.2 Le cas d'une seule variable

Dans cette avant dernière section, nous allons donner 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 disons 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 [12], [13] qui figure aussi avec son développement dans le §1.5.2 du chapitre 1 : *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 $\deg(p) = 5$.

Dans ce contexte, on a l'analogue de notre résultat principal (théorème 4.1.2), pour K un corps hilbertien, à savoir :

Théorème 4.2.1 — *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 4.1.2 (par le lemme chinois). Et les polynômes $p(X) \in K[X]$ pour lesquels $p(X) - a_i$ est divisible par $f_i(X)$ pour $i = 1, \ldots, s$, 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 4.1.2, on considère les polynômes

$$\begin{cases} P(T,X) &= p_0(X) + T\prod_{i=1}^{s} f_i(X), \\ Q_i(T,X) &= p_i(X) + T\prod_{\substack{1\le j\le s \\ j\neq i}} f_j(X) \end{cases}$$

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, le polynôme $p(X)=P(t,X)$ est irréductible sur K. ■

Remarques 4.2.2. (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 qu'en caractéristique nulle, 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 $x_1,\ldots,x_d$ dans $\overline{K(T,Z)}$ (où $d=\deg_X(P)$) de ce polynôme ([3 ; énoncé 4-9] ou [33]). 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 $t\in K$ tel 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 $x_1(t),\ldots,x_d(t)$. 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) Etant donné $\{a_1, \ldots, a_s\} \subset K$, le théorème 4.2.1 permet de construire $p(X) \in K[X]$ non strictement composé tel que $\{a_1, \ldots, a_s\} \subset \sigma(p)$. 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 la version générale de l'inégalité de Stein (voir chapitre 3, théorème fondamental) avait permis de le faire pour $n \geq 2$ variables.

4.3 Une deuxième preuve du théorème 4.1.1 (K algébriquement clos)

Dans cette partie, on suppose que le corps K est algébriquement clos.

En développant la remarque 4 dans [24], nous allons donner sous cette hypothèse supplémentaire une nouvelle preuve du théorème 4.1.1. Cette preuve est plus directe, mais ne fournit pas la forme générale plus précise donnée dans la remarque située à la fin de §4.1.2, ni donc le théorème 4.1.2.

Soient $s \geq 1$ un entier, $a_1, \ldots, a_s \in K$ distincts et $\rho_1, \ldots, \rho_s$ des entiers positifs non nuls. On peut supposer que $\rho_1 \geq \rho_i, \ \ i = 1, \ldots, s$. Posons $m = \rho_1$ et $b_2 = a_2 - a_1, \ldots, \ b_s = a_s - a_1$.

Soit $\ell(X_1) \in K[X_1]$ un polynôme quelconque de degré m tels que les deux polynômes $\ell(X_1) - b_i$ et $\ell'(X_1)$ n'ont pas de zéro commun, pour $i = 2, \ldots, s$. Sous l'hypothèse K infini, l'existence de tels polynômes est facile à établir.

On pose pour tout $i = 2, \ldots, s$,

$$\ell(X_1) - b_i = \prod_{j=1}^{m} L_{ji}(X_1)$$

où les $L_{ji}, \ (j = 1, \ldots, m)$ sont des polynômes de degré 1, qui sont distincts. On considère le polynôme suivant :

$$t(\underline{X}) = 1 + X_2 \left(\prod_{j \in I_2} L_{j2}(X_1) \right) \ldots \left(\prod_{j \in I_s} L_{js}(X_1) \right)$$

où $I_2, \ldots, I_s$ sont des sous-ensembles de $\{1, \ldots, m\}$ de cardinal $\rho_2, \ldots, \rho_s$ respectivement. (On peut remplacer X_2 par tout polynôme $r(\underline{X})$ de degré 1 en l'une au moins des variables $X_2, \ldots, X_n$).

Le polynôme $P(\underline{X}) = \ell(X_1)\ t(\underline{X})$ est non composé sur $\overline{K}$ car $\deg_{X_2}(P) = 1$.

De plus, on a pour $i = 2, \ldots, s$,

$$P(\underline{X}) - b_i = \prod_{j \in I_i} L_{ji}(X_1) \left[\prod_{j \notin I_i} L_{ji}(X_1) + X_2\ \ell(X_1)\ g_i(X_1) \right],$$

avec

$$g_i(X_1) = \prod_{k \neq i} \left(\prod_{j \in I_k} L_{jk}(X_1) \right).$$

L'ensemble $\sigma(P)$ contient les éléments $b_2, \ldots, b_s$ et contient aussi 0 (car P est réductible). De plus $\rho_0(P) \geq m$ et $\rho_{b_i}(P) \geq \mathrm{card}(I_i) = \rho_i$ pour tout $i = 2, \ldots, s$. Donc $\rho(P) \geq m + \sum_{i=2}^{s} \rho_i$.

D'autre part, on a $\deg(P) = m+1+\sum_{i=2}^{s} \rho_i$. Par suite $\rho(P) \geq \deg(P)-1$.

Le théorème fondamental du chapitre 3 donne $\sigma(P) = \{0,\ b_2, \ldots, b_s\}$, $\rho_0(P) = m$ et $\rho_{b_i}(P) = \rho_i,\ \ i = 2, \ldots, s$.

Compte tenu des définitions des b_i et de m, le polynôme $P(\underline{X}) + a_1$ est non composé et vérifie : $\sigma(P + a_1) = \{a_1, \ldots, a_s\}$ et $\rho_{a_i}(P + a_1) = \rho_i$ pour tout $i = 1, \ldots, s$. ■

Bibliographie

[1] Abhyankar, S.S., Heinzer, W.J., Sathaye, A., *Translates of polynomials,* Reprinted from A Tribute to Seshadri. Perspectives in Geometry and Representation Theory, preprint.

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

[3] Ayad, M., *Théorie de Galois, 115 exercices corrigés. Niveau II*, Ellipses, Paris, (1997).

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

[5] Ayad, M., Ryckelynck. P., *On the kernel of some derivations of $k(x_1,\ldots,x_n)$*, Comm. Algebra **30** (2002), no. 5, 2505-2510.

[6] Bajaj, C., Canny, J., Garrity, T., Warren, J., *Factoring rational polynomials over the complex numbers,* SIAM J. Comput. **22** (1993), 318-331.

[7] Cygan, E., *Factorization of polynomials,* Bull. Polish Acad. Sci. Math.(1) **40** (1992), 45-52.

[8] Derksen, H.G.J., *The kernel of a derivation,* Journal of Pure and Applied Algebra **84** (1993), 13-16.

[9] Dèbes, P., Fried, M., *Arithmetic variation of fibers algebraic families of curves. Part I : criteria for existence of rational points,* J. Reine Angew. Math. **409** (1990), 106-137.

[10] Dèbes, P., Fried, M., *Integral specialisation of families of rational functions,* Pacific J. Math. (1) **190** (1999), 45-52.

[11] Van Den Essen, A., *Polynomial automorphisms and the Jacobian Conjecture,* Progress in Mathematics Vol. **190,** Birkhäuser, Verlag, Basel, Boston, Berlin, (2000).

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

[13] Fried, M., *Variables separated polynomials, the genus* 0 *problem and moduli spaces,* in Number Theory in Progress, Procedings of the Number Theory Conference in Zakopane (1999), 75-102.

[14] Fried, M., Jarden, M., *Field Arithmetic*, Springer-Verlag, (1986).

[15] Fried, M., MacRae, R., *On the invariance of chains of fields,* Illinois J. Math. **13** (1969), 165-171.

[16] Furushima, M., *Finite groups of polynomial automorphisms in the complex affine plane*, I, Mem. Fac. Sci., Kyushu Univ., Ser. A, **36** (1982), 85-105.

[17] Gao, S., *Factoring multivariate polynomials via rational differential equation,* Math. Comput. **72**, (2002), no. 242, 801-822.

[18] Von Zur Gathen, J., *Irreducibility of multivariate polynomials,* J. Comput. System Sci. **31**, (1985), no. 2, 225-264

[19] Kaliman, S., *Two remarks on polynomials in two variables,* Pacific J. Math. **154** (1992), 285-295.

[20] Kaltofen, E., *Effective Noether irreducibility forms and applications,* Symposuim on the theory of Computing (New Orleans, LA, 1991). J. Comput. System Sci. **50,** (1995), no. 2, 274-295.

[21] Lang, S., *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York (1983).

[22] Lefshetz, S., *Algebraic Geometry,* Princeton University Press (1953).

[23] Lin, V., Zaidenberg, M., *An irreducible simply connected curve in* $\mathbb{C}^2$ *is equivalent to a quasihomogeneous curve,* Soviet Math. Dokl., **28** (1983), 200-204.

[24] Lorenzini, D., *Reducibility of polynomials in two variables*, J. Algebra **156** (1993), 65-75.

[25] Makar-Limanov, L., *Locally nilpotent derivations, a new ring invariant and applications,* Lecture Notes, (1998), preprint.

[26] Miyanishi, M., *Normal affine subalgebras of a polynomial ring,* algebraic and topological theories to the memory of Dr. Takehiko Miyata, Kinokuniya, Tokyo, (1985), pp. 37-51.

[27] Müller, P., *Hilbert's irreducibility theorem for polynomials of prime degree and for generic polynomials,* Israel J. Math. **109** (1999), 319-337.

[28] Mumford, D., *Algebraic Geometry I : Complex Projective Varieties,* Spriger-Verlag, Berlin, New York, (1976).

[29] Nagata, M., Nowicki, A., *Rings of constants for $k-$derivations in $k[x_1, \ldots, x_n]$,* J. Math. Kyoto Univ. **28** (1988), 111-118.

[30] Nowicki, A., *Polynomial derivations and their rings of constants,* Toruń, 1994.

[31] Ploski, A., *On the irreducibility of polynomials in several complexe variables,* Bull. Pol. Ac. : Math. **39** (1991), 241-247.

[32] Ruppert, W., *Reduzibilitãt Ebener Kurven,* J. Reine Angew. Math. **369** (1986), 167-191.

[33] Schinzel, A., *Slected topics on polynomials,* Ann Arbor Publications, University of Michigan Press, (1982).

[34] Schmidt, W. M., *Equations over finite fields, an elementary approach*, Springer-Verlag (1976).

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

[36] Vistoli, A., *The number of reducible hypersurfaces in a pencil,* Invent. math. **112** (1993), 247-262.

[37] Zielinsky, J., *On the algebra of constants of polynomial in two variables,* Colloquium Mathematicum, **83** (2000), 267-269.