Groupe d'étude d'Analyse ultramétrique
(Y. AMICE, G. CHRISTOL, P. ROBBA)
10e année, 1982/83, n° 10, 10 p.

31 janvier 1983

UNE VERSION EFFECTIVE DU THÉORÈME D'IRRÉDUCTIBILITÉ DE HILBERT

par Pierre DÈBES (*)

Introduction. - Nous nous intéressons dans cet exposé à la structure arithmétique des polynômes spécialisés $P(x, Y)$, où P est un polynôme irréductible dans $k[X, Y]$, k est un corps de nombres, et x un élément de k.

Il n'existe aucune raison a priori pour que $P(x, Y)$ soit irréductible dans $k[Y]$; cependant tous les travaux réalisés sur la question montrent que l'ensemble des éléments x de k tels que $P(x, Y)$ soit irréductible dans $k[Y]$ est "gros", en des sens divers ; par exemple, d'après le théorème d'irréductibilité de Hilbert [5], qui est le point de départ des investigations ultérieures, cet ensemble est infini.

Mais jusqu'à ces dernières années, on ne disposait pas de résultats effectifs, c'est-à-dire des résultats disant où sont, et où ne sont pas, les éléments x de k "exceptionnels" (ceux pour lesquels $P(x, Y)$ se décompose dans $k[Y]$), disant si un élément donné x de k est, ou n'est pas, "exceptionnel", enfin s'il l'est, comment se décompose $P(x, Y)$. Les théorèmes 1 et 2 de cet exposé, qui généralisent des résultats de P. BUNDSCHUH [2] et de V. G. SPRINDZUK ([8], [9]) apportent quelques éléments de réponse à ces questions.

Notations. - Les valeurs absolues v d'un corps de nombres F seront normalisées de telle façon que :

- si v/p (c'est-à-dire si v prolonge la métrique p-adique sur $\mathbb{Q}$, p étant un nombre premier)

$$|p|_v = p^{-1} ;$$

- si v/∞ (c'est-à-dire si v est archimédienne),

$$|x|_v = |x| \text{ pour tout entier rationnel } x .$$

($|\ |$ désignant la valeur absolue usuelle sur $\mathbb{Z}$).

Si v est une place de F, nous noterons F_v le complété de F pour la métrique v, et d_v^F le degré local de la place v par rapport à $\mathbb{Q}$ défini par :

$$d_v^F = [F_v : \mathbb{Q}_v] .$$

(*) Pierre DEBES, Institut Henri Poincaré, ERA 979, 11 rue Pierre et Marie Curie, 75231 PARIS CEDEX 05.

M_F désignera l'ensemble des valeurs absolues normalisées de F.

Si x est un nombre algébrique, $h(x)$ désignera la hauteur logarithmique absolue de x définie de la manière suivante : si F est un corps de nombres auquel x appartient

$$h(x) = \frac{1}{[F : \mathbb{Q}]} \sum_{v \in M_F} d_v^F \log \max (1 , |x|_v) .$$

Il est classique que cette définition ne dépend pas du corps de nombres F contenant x.

1. Un résultat d'irréductibilité.

Soient k un corps de nombres, et P un polynôme irréductible dans $k[X , Y]$. On suppose en outre que P vérifie l'hypothèse suivante, notée (H) :

(H) Il existe une série formelle $\underset{\sim}{Y} = \sum_{n \geq 0} \eta_n X^n$ à coefficients η_n, $n \geq 0$, algébriques vérifiant

$$P(X , \underset{\sim}{Y}) = 0 .$$

Soit K le corps $k((\eta_n)_{n \geq 0})$; il est facile de voir que K est un corps de nombres.

THÉORÈME 1. - Il existe deux constantes a, b, strictement positives, ne dépendant que de P, telles que :

Si ξ est un nombre algébrique non nul, d un entier positif, v une place du corps $K(\xi)$, et si

$$(1) \qquad |\xi|_v^{d_v^{K(\xi)}/[K(\xi):\mathbb{Q}]} < a \exp\{- \frac{d[k(\xi) : k]}{\deg_Y P} h(\xi) - b \sqrt{h(\xi)}\} ,$$

alors $P(\xi , Y)$ est divisible dans $k(\xi)[Y]$ par un polynôme irréductible dans $k(\xi)[Y]$ de degré strictement supérieur à d.

Pour conclure à l'irréductibilité du polynôme $P(\xi , Y)$ sur $k(\xi)$, il suffit de vérifier que la condition (1) du théorème 1 est réalisée pour $d = \deg_Y P - 1$. D'ailleurs à cause de l'inégalité triviale :

$$\frac{d_v^{K(\xi)}}{[K(\xi) : \mathbb{Q}]} \log |\xi|_v \geq - h(\xi) ,$$

le nombre $d = \deg_Y P - 1$ est la valeur maximale de d pour laquelle la condition (1) peut être réalisée.

Le théorème 1 généralise simultanément deux résultats, l'un de P. BUNDSCHUH ([2], Théorème 1), l'autre de V. G. SPRINDZUK ([8], Théorème 1) ; dans l'énoncé de P.

BUNDSCHUH, v est archimédienne, $k = \mathbb{Q}$ et les constantes a , b dépendent aussi du degré de ξ ; quant à l'énoncé de V. G. SPRINDZUK, il correspond au cas particulier du théorème 1 où $k = K = \mathbb{Q}$, P est absolument irréductible (c'est-à-dire irréductible sur la clôture algébrique de $\mathbb{Q}$), ξ est un nombre rationnel, v une place finie de $\mathbb{Q}$ et $d = \deg_Y P - 1$; en outre, dans ces deux énoncés, on fait sur P l'hypothèse suivante que nous noterons (H') :

(H') Il existe un nombre algébrique η_0 vérifiant

$$P(0\ ,\ \eta_0) = 0 \quad \text{et} \quad P'_Y(0\ ,\ \eta_0) \neq 0\ .$$

Il est classique que si P vérifie (H') , alors P vérifie (H) avec $K = k(\eta_0)$.

Dans le cas d'un élément ξ de k , non nul, tel qu'il existe une unique place v de K telle que $|\xi|_v < 1$ (par exemple, si $\xi = p^n$, où p est un nombre premier non décomposé dans K , c'est-à-dire tel que l'idéal engendré par p dans l'anneau des entiers de K soit une puissance d'un idéal premier, et n est un entier supérieur à 1) la condition (1), avec $d = \deg_Y P - 1$, s'écrit

$$-\frac{h(\xi)}{\deg_Y P} + b\sqrt{h(\xi)} - \log a < 0\ .$$

On déduit donc du théorème 1, le résultat suivant :

COROLLAIRE. - <u>Soit</u> ξ <u>un élément de</u> k^* <u>tel que</u> $M_K(\xi) = \{v \in M_K\ ;\ |\xi|_v < 1\}$ <u>ait exactement un élément</u>.

<u>Si</u> $h(\xi) > h_0$ (<u>où</u> h_0 <u>est une constante positive ne dépendant que de</u> P <u>et de</u> $\underset{\sim}{Y}$), <u>alors</u> $P(\xi\ ,\ Y)$ <u>est irréductible dans</u> $k[Y]$.

<u>Remarque</u>. - Si $K = \mathbb{Q}$ (cas traité par SPRINDZUK dans [8]), le corollaire s'applique aux ξ de la forme p^n , où n est un entier supérieur à 1 et p un nombre premier quelconque.

Intuitivement, le résultat du corollaire signifie que si un nombre ξ est "aritmétiquement simple", alors $P(\xi\ ,\ Y)$ est lui aussi arithmétiquement simple dans $k[Y]$ Le théorème 2, plus général que le théorème 1, va mettre en évidence un lien entre la structure arithmétique de ξ (la décomposition de l'idéal fractionnaire engendré par ξ dans l'anneau des entiers de K , qui interviendra dans l'énoncé par l'intermédiaire de l'ensemble des places v de K telles que $|\xi|_v < 1$) et celle de $P(\xi\ ,\ Y)$ (décomposition en irréductibles de l'anneau principal $k[Y]$).

2. <u>Le résultat global</u>.

Soient k , P , $\underset{\sim}{Y}$, K comme dans le paragraphe 1. Pour toute place v de K , nous noterons R_v le rayon de convergence de la série formelle $\underset{\sim}{Y}$ pour la métrique v .

A cause du choix des normalisations des valeurs absolues que nous avons fait, R_v

ne dépend pas du corps k ; si k_0 est le corps engendré par $\mathbb{Q}$ et les coefficient de P, et K_0 le corps $k_0((\eta_m)_{m\geq 0})$, alors R_v est égal au rayon de convergence de $\underset{\sim}{Y}$ dans le complété de K_0 pour la restriction de v à K_0.

D'autre part, pour toute place v de K, R_v est strictement positif. Si P vérifie l'hypothèse (H'), c'est simplement une conséquence du théorème des fonctions implicites. Dans le cas où P vérifie seulement l'hypothèse (H), il faut recourir à des résultats plus sophistiqués : le théorème d'Eisenstein [4] pour les places finies, et le théorème de Frobenius-Malgrange [6] pour les places archimédiennes (il est classique que la série formelle $\underset{\sim}{Y}$ étant algébrique sur $k(X)$ est solution formelle, d'une équation différentielle linéaire à coefficients dans $k(X)$ à points singuliers réguliers ; d'après le théorème de Frobenius-Malgrange, c'est une solution convergente).

La série formelle $\underset{\sim}{Y}$ induit donc sur la boule ouverte

$$B(0\ ,\ R_v) = \{x \in K_v\ ;\ \ |x|_v < R_v\}$$

une fonction Y_v, strictement analytique sur toute boule fermée de $B(0\ ,\ R_v)$ et vérifiant :

$$\text{Pour tout } x \text{ dans } B(0\ ,\ R_v)\ ,\quad P(x\ ,\ Y_v(x)) = 0\ .$$

Le théorème suivant est le résultat principal de cet exposé.

THÉORÈME 2. - <u>Il existe deux constantes</u> A, B <u>positives ne dépendant que de</u> P <u>et</u> $\underset{\sim}{Y}$, <u>ayant la propriété suivante</u> :

<u>Si</u> ξ <u>est un élément de</u> k, <u>non nul</u>, Q <u>un polynôme dans</u> $k[Y]$ <u>divisant</u> $P(\xi\ ,\ Y)$ <u>dans</u> $k[Y]$, <u>et</u> $S(\xi\ ,\ Q)$ <u>l'ensemble des places</u> v <u>de</u> K <u>vérifiant</u> :

$$|\xi|_v < R_v \quad \underline{\text{et}} \quad Q(Y_v(\xi)) = 0\ .$$

<u>Alors</u>

$$(2)\qquad \left|\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S(\xi,Q)} d_v^K \log \min(1\ ,\ |\xi|_v) + \frac{\deg Q}{\deg_Y P}\, h(\xi)\right| \leq A + B\sqrt{h(\xi)}\ .$$

Le résultat du théorème 2 est complètement effectif : les constantes A et B sont toutes deux calculables à partir des données ; je donnerai dans [3] une valeur explicite pour ces constantes. Notons aussi que, quitte à les grossir un peu, on peut demander à ces constantes de ne dépendre que de P : il n'y a en effet qu'un nombre fini de séries formelles (au plus $\deg_Y P$) vérifiant l'hypothèse (H). V. G. SPRINDZUK a démontré le théorème 2 en 1982 [9] dans le cas où P est absolument irréductible et vérifie l'hypothèse (H') avec $\eta_0 \in k$ (et donc $K = k$). (En fait l'hypothèse d'irréductibilité absolue est dans ce cas superflue puisqu'elle résulte de (H) si $K = k$.). D'autre part, dans son énoncé, A et B dépendent également du corps k.

On peut interpréter le théorème 2 comme un résultat sur la distribution des $Y_v(\xi)$ qui sont définis, à l'intérieur de l'ensemble des racines de $P(\xi, Y)$. En effet, d'après la formule du produit,

$$h(\xi) = -\frac{1}{[K : Q]} \sum_{v\in M_K} d_v^K \log \min (1, |\xi|_v) ;$$

l'inégalité (2) du théorème 2 signifie donc, qu'à un $O(h(\xi)^{-1/2})$ près, la probabilité (selon la loi image par l'application $v \mapsto d_v^K \log |\xi|_v$) qu'a une place v, dans $M_K(\xi) = \{v \in M_K ; |\xi|_v < 1\}$, d'appartenir à un ensemble du type $S(\xi, Q)$ (Q étant un diviseur de $P(\xi, Y)$ dans $k[Y]$), c'est-à-dire la probabilité qu'a un $Y_v(\xi)$ d'être une racine de Q, est égale à $\deg Q/\deg_Y P$, ce qui est relativement naturel.

En particulier, si P est absolument irréductible, les $Y_v(\xi)$, qui sont définis, sont (toujours à un terme d'erreur près) équidistribués à l'interieur des racines du polynôme $P(\xi, Y)$.

Disons enfin qu'à la lumière de cette interprétation du théorème 2, on comprend mieux pourquoi son résultat est banal dans les cas extrêmes $Q \in k^*$ et $Q - P(\xi, Y)$.

Le théorème 1 se déduit facilement du théorème 2 (nous le montrerons en détails dans [3]).

Le résultat que nous donnons maintenant généralise le corollaire du théorème 1 et corrobore l'idée que l'on en avait dégagée selon laquelle plus un nombre ξ est "arithmétiquement simple", moins la structure arithmétique de $P(\xi, Y)$ est complexe.

COROLLAIRE. - <u>Soient ξ un élément non nul de k, et $P(\xi, Y) : u\, Q_1^{\alpha_1}, \ldots, Q_2^{\alpha_2}$ la décomposition de $P(\xi, Y)$ en polynômes irréductibles distincts Q_i de l'anneau $k[Y]$. Si $h(\xi) > h_1$ (où h_1 est une constante positive ne dépendant que de P et de Y), et si $M_K(\xi)$ désigne l'ensemble des places v de K telles que $|\xi|_v < 1$, alors</u>

$$r \leq \operatorname{Card} M_K(\xi) .$$

<u>Démonstration</u>. - On déduit aisément du théorème 2, l'existence d'une constante $h_1 \geq 0$ vérifiant : Si $\xi \in k^*$ et $h(\xi) > h_1$, alors, pour tout polynôme Q divisant $P(\xi, Y)$ dans $k[Y]$ tel que $\deg Q \geq 1$, on a

$$S(\xi, Q) \cap M_K(\xi) \neq \emptyset .$$

L'application

$$\begin{cases} S_0 = \{v \in M_K(\xi) \ ; \ |\xi|_v < R_v\} \longrightarrow \{1 , 2 , \ldots , r\} \\ \qquad\qquad v \qquad\qquad\qquad \longmapsto i(v) \ , \text{ défini par } Q_{i(v)}(Y_v(\xi)) = 0 \ , \end{cases}$$

est donc surjective. L'inégalité demandée en résulte.

3. Une esquisse de démonstration du théorème 2

On remarque tout d'abord que ce que l'on veut obtenir, c'est une estimation de deg Q qui, si Q est un polynôme irréductible dans $k[Y]$, est égal au degré sur k des $Y_v(\xi)$ où v décrit l'ensemble $S(\xi , Q)$.

Le problème consiste donc en une étude arithmétique de valeurs de fonctions algébriques ; on va le traiter en utilisant des méthodes developpées pour l'étude de valeurs de fonctions transcendantes (Méthodes de SIEGEL, GEL'FOND, SCHNEIDER, ...).

C. L. SIEGEL, en 1929, fut le premier à envisager cette démarche : en effet, à la fin de son article sur les E-fonctions [7], il fait plusieurs remarques sur la possibilité d'utiliser sa méthode pour l'étude des G-fonctions ; or les fonctions algébriques constituent un exemple typique de G-fonctions.

Cinquante ans plus tard, en utilisant des méthodes analogues à celle de SIEGEL, P. BUNDSCHUH et V. G. SPRINDZUK aboutiront aux résultats mentionnés plus haut. La démonstration du théorème 2, dont nous allons maintenant exposer les grandes lignes, et qui généralise celle de P. BUNDSCHUH, s'appuie, elle, sur un développement de la méthode de GEL'FOND ([10], Chapitre 3).

Nous supposerons dans un premier temps que Q le diviseur de $P(\xi , Y)$ consideré dans l'énoncé du théorème 2, est un polynôme irréductible dans $k[Y]$.

Les constantes f_i , $1 \leq i \leq 8$, intervenant dans la démonstration du théorème sont des quantités positives ne dépendant que de P et de $\underset{\sim}{Y}$, excepté les $f_{3,v}$, v décrivant M_K , qui dépendent aussi de v , mais dont le produit est convergent et ne dépend lui, que de P et de $\underset{\sim}{Y}$. D'autre part, il est clair que l'expression à majorer dans l'énoncé du théorème 2 est inférieure à $h(\xi)$. Nous pouvons donc au cours de la démonstration (ce que je ferai plusieurs fois sans le dire) supposer que $h(\xi)$ est assez grand (supérieur à une constante (ne dépendant que de P et de $\underset{\sim}{Y}$)).

1re étape : Construction de fonctions auxiliaires possédant de nombreux zéros.

Soient $L > 0$ un entier, et p l'entier défini par $p = L[\sqrt{h(\xi)}]$ ([ ] désignant la partie entière) ; on construit un polynôme non nul $\varphi = \sum_{i,j} \varphi_{i,j} X^i Y^j$ à coefficients dans k , vérifiant :

(a) $\deg_X \varphi < p$, $\deg_Y \varphi < \deg_Y P$.

(b) Si $v \in S(\xi , Q)$, alors

1° $\Phi_v = \Phi(X , Y_v)$ a un zéro d'ordre supérieur à L en 0 ,

2° Φ_v a un zéro d'ordre supérieur à L en ξ ,

(c) $h(\Phi) \leq L(\frac{\deg Q}{\deg_Y P} h(\xi) + f_1 \sqrt{h(\xi)} + f_2 + o(1))$,

où

$$h(\Phi) = \frac{1}{[k : Q]} \sum_{v \in M_k} d_v^k \log H_v(\Phi)$$

$$\text{et} \quad H_v(\Phi) = \max\{|\Phi_{ij}|_v \ ; \ 0 \leq i \leq \deg_X \Phi \ ; \ 0 \leq j \leq \deg_Y \Phi\} .$$

Il s'agit de trouver une solution non triviale et "pas trop grande" à un système d'équations linéaires, on utilise pour ceci un lemme de Siegel bien adapté à la situation (du type de celui qu'utilise E. BOMBIERI dans [1]).

On dispose de $p \deg_Y P$ inconnues ; voyons quel est le nombre d'équations du système.

La condition (b-1°) est indépendante de $v \in S(\xi , Q)$. En effet, les développements de Taylor à l'origine des Φ_v sont tous égaux à $\Phi(X , \underline{Y})$. Ensuite, les coefficients des équations qui traduisent cette condition, étant des sommes de produits de η_m , appartiennent à K . La condition (b-1°) est donc finalement équivalente à $L[K : k]$ équations.

Montrons que la condition (b-2°) ne dépend également pas de $v \in S(\xi , Q)$. On peut supposer que $P_Y'(\xi , Y_v(\xi)) \neq 0$. Les coefficients $(y_{m,v})_{m \geq 0}$ du développement de Taylor des Y_v en ξ sont alors tous déterminés à partir du premier par une relation de récurrence sur k (précisément $y_{m+1,v} = A_m(y_{0,v} , \ldots , y_{m,v})$ où $A_m \in k(X_0 , \ldots , X_m)$).

D'autre part, si v_1 et v_2 sont dans $S(\xi , Q)$, $Y_{v_1}(\xi)$ et $Y_{v_2}(\xi)$ sont conjugués sur k car on a supposé Q irréductible sur k . On déduit des deux remarques précédentes que les développements de Taylor en ξ des Y_v, **où** $v \in S(\xi, Q)$ sont conjugués sur K . Φ étant à coefficients dans k , ceux des Φ_v , où $v \in S(\xi, Q)$, **le** sont **aussi,** la condition (b-2°) ne dépend donc effectivement pas de $v \in S(\xi , Q)$.

Les coefficients des équations traduisant la condition (b-2°) sont ici dans un corps de degré sur k égal à $\deg Q$ ($\deg Q = [k(Y_v(\xi)) : k]$) . La condition (b-2°) est donc équivalente à $L \deg Q$ équations.

La condition de résolubilité du système s'écrit donc :

$$p \deg_Y P > L([K : k] + \deg Q) .$$

Elle est réalisée dès que $h(\xi)$ est suffisamment grand.

Le lemme de Siegel garantit alors l'existence d'une solution non triviale dans

$k^{p\deg_Y P}$ dont la hauteur est majorée en fonction de la hauteur des coefficients du système. Il s'agit donc maintenant pour obtenir (c) de majorer la hauteur des coefficients des développements de Taylor en 0 et en ξ des Y_v. C'est sûrement la partie la plus technique et la plus longue de la démonstration, nous n'en donnerons que les arguments essentiels. Disons seulement que le problème consiste à obtenir des majorations des valeurs absolues des coefficients y_n, $n \geq 0$, d'une série formelle $y = \sum_{n\geq 0} y_n X^n$ vérifiant $F(X , y) = 0$ où $F \in \overline{\mathbb{Q}}[X , Y]$ ($\overline{\mathbb{Q}}$ désigne la clôture algébrique de $\mathbb{Q}$).

Pour les places finies, on utilise le théorème d'Eisenstein [4], on a, pour tout $n \geqslant 1$,

$$|y_n|_v \leqslant |T|_v^{-n} ,$$

T étant la constante d'Eisenstein de la série y.

Pour les places archimediennes, on utilise les inégalités de Cauchy, ce qui donne, pour tout $n \geqslant 0$,

$$|y_n|_v \leqslant \frac{M(r)}{r^n}$$

où $0 < r < R_v$ et $M(r) = \sup_{|x|_v = r} |y(x)|_v$.

La difficulté réside dans la nécessité d'obtenir des résultats précis et complètement explicites de façon à pouvoir les appliquer au développement de Taylor des Y_v en 0, et surtout en ξ.

2e étape :

$$\deg_Y \Phi < \deg_Y P \text{ , donc } \Phi(X , \underset{\sim}{Y}) \neq 0 ;$$

alors $\overline{\lambda} = V_X(\Phi(X , \underset{\sim}{Y})) < + \infty$. ($V_X$ désigne la valuation X-adique dans $\overline{\mathbb{Q}}[[X]]$.)

On note $\overline{\delta}$ le coefficient de $X^{\overline{\lambda}}$ dans $\Phi(X , \underset{\sim}{Y})$; $\overline{\delta}$ est un élément de K non nul. A ce niveau de la méthode, on utilise un argument arithmétique, ici la formule du produit :

$$\prod_{v\in M_K} |\xi|_v^{d_v^K} = 1 . \tag{3}$$

3e étape : Majoration des $|\overline{\delta}|_v$.

On distingue 2 types de majorations suivant que v appartient à $S(\xi , Q) \cap M_K(\xi)$ ou non. (Rappelons que $M_K(\xi)$ est l'ensemble des places v de K telles que $|\xi|_v < 1$).

Si $v \notin S(\xi , Q) \cap M_K(\xi)$: On a $\bar{\delta} = \sum_{i,j} \Phi_{i,j}\, n_{ij}$ où les n_{ij} sont des sommes de produits de η_h ; on en déduit, en utilisant les majorations faites à la fin de la 1re étape, que

$$|\bar{\delta}|_v \lesssim p_v\, H_v(\Phi)\, f_{3,v}^{\bar{\ell}} \quad \text{où} \quad \begin{cases} p_v = p & \text{si } v \text{ est archimédienne} \\ p_v = 1 & \text{sinon.} \end{cases}$$

Si $v \in S(\xi , Q) \cap M_K(\xi)$: On utilise ici un argument analytique. On applique le principe du maximum à la fonction

$$G_v : x \longmapsto \frac{\varphi_v(x)}{x^{\bar{\ell}}(x - \xi)^L}$$

définie sur $B(0 , R_v)$, qui, par construction du polynôme Φ , est strictement analytique sur toute boule fermée de $B(0 , R_v)$, et qui prend la valeur $G_v(0) = \bar{\delta}(-\xi)^{-L}$ en 0 . On obtient :

$$|\bar{\delta}|_v \lesssim p_v\, |\xi|_v^L\, H_v(\Phi)\, f_{3,v}^{\bar{\ell}+L} \quad \text{où } p_v \text{ est défini comme précedemment .}$$

En reportant dans (3), on obtient :

$$(4) \qquad 1 \lesssim p[\textstyle\prod_{v\in S(\xi,Q)} \min\,(1\ ,\ |\xi|_v)^{d_v^K}]^{L/[K:Q]} \exp(h(\Phi))\, f_4^{\bar{\ell}+L} .$$

4e étape : Lemme de zéros.

L'objet de cette étape est d'obtenir une majoration de $\bar{\ell}$, l'ordre en 0 des Φ_v . On utilise pour ceci un lemme de zéros classique (voir par exemple [2] lemme 1). P étant irréductible dans $k[X , Y]$, R le résultant par rapport à la variable Y des polynômes P et Φ , est un polynôme en X , non nul ; il est facile de voir que l'ordre en 0 de $\Phi(X , \underline{Y})$, $\bar{\ell}$, est majoré par l'ordre en 0 de R , lui-même majoré par $\deg R$. Ce qui donne :

$$\bar{\ell} \lesssim p \deg_Y P + f_5 .$$

En reportant ceci dans (4), et en utilisant la majoration de $h(\Phi)$ donnée dans la première étape, on obtient :

$$0 \lesssim L[\frac{1}{[K : Q]} \textstyle\sum_{v\in S(\xi,Q)} d_v^K \log \min(1\ ,\ |\xi|_v) + \frac{\deg Q}{\deg_Y P}\, h(\xi) + f_6 \sqrt{h(\xi)} + f_7 + o(1)] .$$

Il suffit alors de diviser par L , puis de le faire tendre vers $+\infty$, pour obtenir l'une des deux inégalités annoncées dans le théorème, la minoration de l'expression

$$\varphi(\xi , Q) = \frac{1}{[K : Q]} \textstyle\sum_{v\in S(\xi,Q)} d_v^K \log \min(1\ ,\ |\xi|_v) + \frac{\deg Q}{\deg_Y P}\, h(\xi) .$$

Nous avons établi cette inégalité dans le cas où Q est irréductible dans $k[Y]$; pour étendre ce résultat au cas général d'un polynôme Q divisant $P(\xi , Y)$ dans $k[Y]$, on utilise la remarque suivante :

Si Q_1 et Q_2 sont 2 polynômes divisant $P(\xi , Y)$ dans $k[Y]$, premiers entre eux dans $k[Y]$, alors $S(\xi , Q_1 Q_2)$ est la réunion disjointe des ensembles $S(\xi , Q_1)$ et $S(\xi , Q_2)$.

Quant à la majoration de $\varphi(\xi , Q)$ (la seconde inégalité annoncée dans le théorème on la déduit en fait de la minoration en utilisant le fait suivant :

Si $P(\xi , Y) = QT$, où $T \in k[Y]$, alors

$$|\varphi(\xi , Q) + \varphi(\xi , T)| \leq f_8 .$$

RÉFÉRENCES

[1] BOMBIERI (E.). - On the Thue-Siegel-Dyson theorem, Acta Math., Uppsala, t. 148, 1982, p. 255-296.

[2] BUNDSCHUH (P.). - Une nouvelle application de la méthode de Gel'fond, Séminaire Delange-Pisot-Poitou : Théorie des Nombres, 19e année, 1977/78, n° 42, 8 p.

[3] DÈBES (P.). - Thèse de 3e cycle. En cours de rédaction.

[4] DWORK (B.) and ROBBA (P.). - On natural radii of p-adic convergence, Trans. Amer. math. Soc., t. 256, 1979, p. 199-213.

[5] HILBERT (D.). - Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, Gesammelte Abhandlungen, vol. 2, n° 18, p. 264-286. - Berlin, Springer-Verlag, 1933 [réimpression Chelsea, 1965] ; ou J. für die reine und angew. math., t. 110, 1892, p. 104-129.

[6] MALGRANGE (B.). - Sur les points singuliers des équations différentielles linéaires, Enseignement math., Genève, t. 20, 1970, p. 147-176.

[7] SIEGEL (C. L.). - Über einige Anwendungen diophantischer Approximationen, Gesammelte Abhandlungen, vol. 1, n° 16, p. 209-266. - Berlin, Heidelberg, New York, Springer-Verlag, 1966.

[8] SPRINDZUK (V. G.). - Hilbert's irreducibility theorem and national points on algebraic curves, Doklady Akad. Nauk SSSR, t. 247, 1979, p. 285-289.

[9] SPRINDZUK (V. G.). - Arithmetic specialisations in polynomials, J. für die reine und angew. Math., t. 340, 1983, p. 26-52.

[10] WALDSCHMIDT (M.). - Nombres transcendants. - Berlin, Heidelberg, New York, Springer-Verlag, 1976 (Lecture Notes in Mathematics, 402).