Volume V, No. 6, December 1983 décembre

COMPTES RENDUS MATHEMATIQUES

DE L'ACADEMIE DES SCIENCES

MATHEMATICAL REPORTS

OF THE ACADEMY OF SCIENCE

The Royal Society of Canada
La Société royale du Canada

SPECIALISATIONS DE POLYNOMES

Pierre DEBES

Presented by P. Ribenboim, F.R.S.C.

RESUME. Ce travail, inspiré par le théorème d'irréductibilité de Hilbert, étudie la structure arithmétique des polynômes spécialisés P(x,Y) où P est un polynôme irréductible à deux indéterminées X,Y.

INTRODUCTION. Soit P un polynôme irréductible dans $\mathbb{Q}[X,Y]$; d'après le théorème d'irréductibilité de Hilbert (1892) [4] l'ensemble des nombres rationnels x tels que P(x,Y) est irréductible dans $\mathbb{Q}[Y]$ est un ensemble infini.
En 1929, dans son mémoire sur les E-fonctions [6], C.L. Siegel donne également, sans démonstration, plusieurs résultats sur les valeurs de certaines G-fonctions. Bien qu'ils excluent le cas particulier des fonctions algébriques, qui est celui qui nous intéresse ici, ces résultats, en ouvrant une nouvelle voie d'approche du problème, ont eu une influence importante sur le développement du théorème de Hilbert. Cinquante ans plus tard, P. Bundschuh [3], généralisant des travaux de T. Schneider [5], et V.G. Sprindzuk [7],[8],[9] aborderont le cas exclu par Siegel en utilisant des méthodes analogues aux siennes. E. Bombieri, peu après [2], élargira le cadre de ces derniers résultats : il démontre en effet en 1980, un énoncé général sur les valeurs de G-fonctions, comme Siegel l'avait fait pour les E-fonctions.
Les théorèmes que nous montrons ici contiennent tous les résultats précédents relatifs aux valeurs de fonctions algébriques ; leur démonstration repose sur un développement de la méthode de Gel'fond ; ils généralisent le théorème d'irréductibilité de Hilbert en précisant à quelles conditions (effectives), P(x,Y) est divisible par un polynôme de degré donné.

NOTATIONS.
Les valeurs absolues v d'un corps de nombres F sont 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)

$$|x|_v = |x| \quad \text{pour tout nombre rationnel } x$$

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

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 :

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

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

$$h(x) = \frac{1}{[F : \mathbb{Q}]} \sum_v d_v^F \operatorname{Log} \max (1, |x|_v) \quad ,$$

la sommation étant étendue à toutes les places de F.

§ 1 - <u>UN PREMIER RESULTAT AVEC UNE SEULE PLACE</u>

Soient k un corps de nombres, ξ_o un élément de k, et P un polynôme irréductible dans k [X,Y]. On fait sur P l'hypothèse notée (H)

(H) - Il existe une série formelle $\mathbf{Y} = \sum_{m \geq o} \eta_m (X-\xi_o)^m$ à coefficients $\eta_m, m \geq o$ algébriques vérifiant :

$$P(X,\mathbf{Y}) = 0 \ -$$

On note K le corps $k((\eta_m)_{m \geq o})$; il est facile de voir que K est un corps de nombres. Sous ces hypothèses, on démontre le résultat suivant :

<u>THEOREME 1</u> - <u>Il existe deux constantes</u> a,b <u>(effectives), strictement positives et ne dépendant que de</u> P, ξ_o <u>telles que</u> :

<u>si</u> ξ <u>est un nombre algébrique différent de</u> ξ_o, d <u>un entier positif et</u> v <u>une place du corps</u> $K(\xi)$ <u>et si</u> :

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

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

A cause de l'inégalité de Liouville, l'hypothèse de l'énoncé ne peut être réalisée que si d<q. Le cas d=q-1 est intéressant puisque la conclusion du théorème est dans ce cas : $P(\xi,Y)$ est irréductible dans $k(\xi)[Y]$.

Le théorème 1 contient simultanément deux résultats de P.Bundschuh ([3] THEOREME 1) et de V.G. Sprindzuk ([7] THEOREME 1). Dans l'énoncé de P. Bundschuh v est archimédienne et $k=\mathbb{Q}$; l'énoncé de V.G. Sprindzuk 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 $d=q-1$. En outre, dans ces deux énoncés, on fait sur P l'hypothèse notée (H'):

(H') - Le polynôme $P(\xi_o,Y)$ admet une racine simple η_o -

Et d'après un lemme classique, si P vérifie (H'), alors P vérifie (H) avec $K=k(\eta_o)$. Le théorème 1 est un corollaire du théorème 2, qui est l'objet du paragraphe 2. Son énoncé fait intervenir simultanément plusieurs places, tenant compte ainsi à la fois des points de vue archimédiens et p-adiques.

§ 2 - LE THEOREME PRINCIPAL

Soient k, ξ_o, P, $\mathbf{Y}$, K comme dans le paragraphe 1. Pour toute place v de K, soit R_v le rayon de convergence de $\mathbf{Y}$ pour la métrique v ; d'après des théorèmes classiques d'analyse, R_v est strictement positif. La série formelle $\mathbf{Y}$ induit donc sur la boule ouverte $B(\xi_o,R_v)=\{x\in K_v / |x-\xi_o|_v<R_v\}$ une fonction Y_v, strictement analytique [1] sur toute boule fermée de $B(\xi_o,R_v)$ vérifiant :

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

Le théorème suivant est le principal résultat de cette note.

<u>THEOREME 2</u> - <u>Il existe deux constantes (effectives)</u> A,B <u>strictement positives, ne dépendant que de</u> P <u>et de</u> ξ_o <u>ayant la propriété suivante</u> :
<u>si</u> ξ <u>est un élément de</u> k, <u>différent de</u> ξ_o, Q <u>un polynôme dans</u> k [Y] <u>divisant</u> $P(\xi,Y)$ <u>dans</u> k [Y] <u>et</u> $S(\xi_o,\xi,Q)$ <u>l'ensemble des places de</u> K <u>vérifiant</u> :

$$|\xi - \xi_o|_v < R_v \quad \text{et} \quad Q(Y_v(\xi)) = 0 \ ,$$

<u>alors</u>

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

V.G. Sprindzuk a démontré ce résultat en 1982 [9] dans le cas où P est absolument irréductible et vérifie l'hypothèse (H') avec $\eta_o\in k$ (et donc K=k)(En fait, l'hypothèse d'irréductibilité absolue est ici superflue puisqu'elle résulte de (H) si K=k). D'autre part, les constantes A et B dépendent dans son énoncé également du degré de k sur $\mathbb{Q}$. Dans son article sur les G-fonctions [2], E. Bombieri montre que les relations k-linéairement indépendantes liant les valeurs en un point

ξ de k, de G-fonctions à coefficients dans k, linéairement indépendantes sur k(X) ne sont pas trop nombreuses. Or si P vérifie l'hypothèse (H) avec de plus k=K, les séries $1, \mathbf{Y}, \ldots, \mathbf{Y}^{(\deg_Y P-1)}$ sont des G-fonctions à coefficients dans k linéairement indépendantes sur k(X). L'application du théorème de Bombieri à ce cas particulier permet d'obtenir le théorème 1 dans le cas k=K.

§ 3 - APPLICATIONS

Dans ce paragraphe, nous supposons, outre les hypothèses du théorème 2, que $\xi_0 = 0$. Le corollaire suivant, montre, sous certaines conditions, l'irréductibilité des polynômes spécialisés $P(\xi^m, Y)$ où m est un entier suffisamment grand.

COROLLAIRE - Soit ξ un élément de k non nul, de hauteur $h(\xi)$ non nulle (i.e ξ n'est pas une racine de l'unité) et vérifiant la propriété suivante :
pour tout ensemble S non vide et strictement inclus dans l'ensemble des places v de K telles que $|\xi|_v < 1$, la quantité $(\sum_{v \in S} d_v^K \operatorname{Log}|\xi|_v)/h(\xi)$ n'appartient pas à $\mathbb{Q}$.
Alors il existe un entier (effectif) m_0 ne dépendant que de P,k et de ξ tel que :
pour tout entier m, si $m \geq m_0$ alors $P(\xi^m, Y)$ est irréductible dans k [Y].

L'hypothèse faite sur ξ dans le corollaire est satisfaite s'il existe une place v_0 telle que le nombre réel $|\xi|_{v_0}$ soit strictement inférieur à 1 et n'appartienne pas au groupe multiplicatif engendré par les $|\xi|_v$ tels que $|\xi|_v < 1$ et $v \neq v_0$.

En particulier le corollaire s'applique dans les cas suivants :

a) La famille des $|\xi|_v$, où v décrit l'ensemble des places de K telles que $|\xi|_v < 1$ est non vide et multiplicativement libre ([9] pour le cas K = k)

b) L'ensemble des places v de K telles que $|\xi|_v < 1$ a exactement un élément (par exemple si $\xi = p^s$ où p est un nombre premier, s un entier plus grand que 1 et K = $\mathbb{Q}$ ou encore si $\xi = \frac{1}{s}$ où s est un entier non nul et K est inclus dans un corps quadratique imaginaire). Dans ce cas, on a un résultat plus précis : il existe une constante h_o ne dépendant que de P telle que : si $h(\xi) \geq h_o$ alors $P(\xi,Y)$ est irréductible sur k.

c) $k = \mathbb{Q}$ et il existe un nombre premier p tel que $|\xi|_p < 1$ et que l'idéal engendré par p dans l'anneau des entiers de K est une puissance d'un idéal premier.

d) $k = \mathbb{Q}$, K est inclus dans un corps quadratique imaginaire et $|\xi| < 1$.

e) $k = K = \mathbb{Q}$ (Conséquence de c) et d), voir aussi [8]).

L'exemple du polynôme $P = Y^2 - X$ montre que l'hypothèse (H) n'est pas superflue dans l'énoncé du corollaire et donc dans celui du théorème 2.

§ 4 COMPLEMENT AU THEOREME 2

Nous donnons ici un énoncé légèrement plus faible que celui du théorème 2, mais d'où ont disparu les fonctions algébriques.

Soient k un corps de nombres, ξ_o un élément de k, P un polynôme irréductible dans $k[X,Y]$. On suppose dans ce paragraphe qu'il existe un nombre algébrique η_o tel que

$$P(\xi_o,\eta_o) = 0 \qquad P'_Y(\xi_o,\eta_o) \neq 0 .$$

On note K le corps $k(\eta_o)$ et P_{ξ_o,η_o} le polynôme de $K[X,Y]$ défini par

$$P_{\xi_o,\eta_o}(X-\xi_o,\ Y-\eta_o) = P(X,Y) .$$

On a alors :

$$P_{\xi_o,\eta_o} = \sum_{\substack{o\leq i\leq \deg_X P\\ o\leq j\leq \deg_Y P}} C_{ij}\, X^i\, Y^j \qquad \text{avec} \quad C_{00} = 0 \quad \text{et} \quad C_{01} \neq 0 .$$

Soit ε un nombre réel strictement compris entre 0 et le minimum des $|C_{01}|_v$ où v décrit l'ensemble des places archimédiennes de K ; pour toute place v de K, on note $\beta_v(\varepsilon)$ la quantité définie par :

$$\begin{cases} \beta_v(\varepsilon) = \min\left(1, \dfrac{|C_{01}|_v}{\underset{2\leq j\leq \deg_Y}{\operatorname{Max}} |C_{oj}|_v}\right) & \text{si v est finie} \\[2ex] \beta_v(\varepsilon) = \min\left(1, \dfrac{|C_{01}|_v - \varepsilon}{\deg_Y P(\deg_Y P-1) \underset{2\leq j\leq \deg_Y P}{\operatorname{Max}} |C_{oj}|_v}\right) & \text{si v est infinie .} \end{cases}$$

Enfin nous supposons toute place v de K prolongée à la clôture algébrique de $\mathbb{Q}$. Alors sous ces hypothèses et notations on a le résultat suivant :

THEOREME 3 - Il existe deux constantes (effectives) A', B' strictement positives, ne dépendant respectivement que de ξ_o, P,ε et ξ_o,P ayant la propriété suivante. Soient ξ un élément de k différent de ξ_o, η un nombre algébrique tels que $P(\xi,\eta) = 0$; si $T(\xi_o,\xi,\eta)$ est l'ensemble des places v de K vérifiant :

il existe un conjugué η_v de η sur k tel que :

$$|\eta_v - \eta_o|_v < \beta_v(\varepsilon) ,$$

alors

$$\left|\frac{1}{[K:\mathbb{Q}]}\sum_{v\in T(\xi_o,\xi,\eta)} d_v^K \operatorname{Log} \min(1,|\xi-\xi_o|_v)+\frac{[k(\eta):k]}{\deg_Y P} h(\xi-\xi_o)\right| < A'+B'\sqrt{h(\xi-\xi_o)} \quad .$$

On a $\beta_v(\varepsilon) = 1$ sauf pour un nombre fini de places de K ; mais en général le résultat devient faux si l'on remplace tous les $\beta_v(\varepsilon)$ par 1 dans l'énoncé du théorème 3 (Considérer le polynôme $P=X^2+Y^2+2Y$ et la famille de points $P_h = (\xi_h,\eta_h)$ où $h>0$ et $\xi_h = \frac{2^{h+1}3^h}{2^{2h}+3^{2h}}$ $\eta_h = -\frac{2\ 3^{2h}}{3^{2h}+2^{2h}}$)

REFERENCES

[1] Y. AMICE : Les nombres p-adiques. Collection Sup. Le Mathématicien 14. Presses Universitaires de France. 1975.

[2] E. BOMBIERI : On G-Functions. Recent progress in analytic number theory. Vol. 2 p 1.67. Ed. Halberstam & Hooley. Proceed. Conf. Durham. 1979.

[3] P. BUNDSCHUH : Une nouvelle application de la méthode de Gel'fond. Séminaire Delange-Pisot-Poitou. Theorie des nombres. 19ème année 1977-78 N°42

[4] D. HILBERT : Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. J. Reine und Angew Math 110 (1892) p.104.129. Aussi Gesammelle Abhandlungen. Springer-Verlag, Berlin, Heidelberg, New York Vol. II N° 18 p. 267-287

[5] T. SCHNEIDER : Eine Bemerkung zu einem Satz von C.L. SIEGEL. Comm. Pure and applied Math. T 29 1976 p.775-782.

[6] C.L. SIEGEL : Über einige Anwendungen diophantischer Approximationen. Abhandlungen der Preussischen Akademie der Wissenschaften. Phys. Math. Klasse 1929 N°1 . Aussi Gesammelte Abhandlungen I P.209.266 Springer-Verlag, Berlin, Heidelberg, New York 1966

[7] V.G. SPRINDZUK : Hilbert'irreducibility theorem and rational points on algebraic curves. Doklady. Acad. Nauk SSSR 247 (1979) 285-289

[8] V.G. SPRINDZUK : Reducibility of polynomials and rational points of algebraic curves. Doklady. Acad. Nauk SSSR 250 (1980) 1327-1330

[9] V.G. SPRINDZUK : Arithmetic specialisations in polynomials. J. Reine und Angew. Math. Band 340 (1983) p. 26-52

Institut Henri Poincaré, PARIS, FRANCE

Received August 6, 1983