ACTA ARITHMETICA
XLVII (1986)

G-fonctions et théorème d'irréductibilité de Hilbert

par

PIERRE DEBES (Paris)

Jusqu'à l'article de Bombieri sur les *G*-fonctions [1], on ne disposait pas de résultats généraux sur la nature arithmétique des valeurs en des points algébriques de *G*-fonctions satisfaisant des équations différentielles linéaires, de tels résultats ayant pourtant été énoncés dans le célèbre article de C. L. Siegel de 1929 [20]. La méthode de Siegel, fructueuse dans le cadre des *E*-fonctions, présente en effet de nombreuses difficultés quand on cherche à l'appliquer aux *G*-fonctions. Bombieri est parvenu à y faire face, au moyen d'arguments sophistiqués comme le théorème de Dwork–Robba. Nous proposons ici une approche différente du problème, basée sur la méthode de Gel'fond, qui évite les complications de la méthode de Siegel, et conduit à un nouvel énoncé sur l'irrationalité et l'indépendance linéaire des valeurs de *G*-fonctions (théorème principal).

Les fonctions algébriques constituent un exemple typique de *G*-fonctions vérifiant des équations différentielles linéaires; on obtient dans ce cas particulier un énoncé (théorème 2) qui généralise simultanément des résultats de P. Bundschuh [3], T. Schneider [17], [18] et de V. G. Sprindžuk [21]–[24] sur le théorème d'irréductibilité de Hilbert.

Présenté ici comme le fruit d'une méthode analytique, le théorème 2 possède en fait une origine purement algébrique: le paragraphe 2.4, qui s'appuie sur un article de Bombieri sur le théorème de décomposition de Weil ([2], voir aussi [7]), explique qu'il provient essentiellement de la quadraticité de la hauteur sur les variétés abéliennes. Le théorème 3, version géométrique du théorème 2, permet d'autre part de donner corps au lien mis en évidence par M. Fried [12] entre les travaux de V. G. Sprindžuk et ceux de R. Weissauer.

La dernière partie est consacrée au théorème d'irréductibilité de Hilbert; le théorème 2 conduit à une nouvelle version qui montre en gros que toute partie hilbertienne d'un corps de nombres contient "beaucoup" de progressions géométriques.

Notations.

Valeurs absolues. Nous adopterons les normalisations suivantes des valeurs absolues $|\ |_v$ associées aux places v d'un corps de nombres F:

si $v|p$ (c'est-à-dire si v est au dessus du nombre premier p)

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

si $v|\infty$ (c'est-à-dire si v est archimédienne)

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

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

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

$$d_v^F = [F_v : \boldsymbol{Q}_v],$$

M_F (resp. M_F^0) désignera l'ensemble des places (resp. des places finies) de F. Compte tenu de nos normalisations, la formule du produit s'écrit

$$\prod_{v \in M_F} |x|_v^{d_v^F} = 1$$

pour tout x dans F non nul.

Hauteurs. Soient (F, v) un corps valué et Ω une famille finie non vide d'éléments de F; nous appellerons v-hauteur et v-hauteur logarithmique de la famille Ω, les quantités $H_v(\Omega)$ et $h_v(\Omega)$ suivantes

$$H_v(\Omega) = \max_{\omega \in \Omega} |\omega|_v, \qquad h_v(\Omega) = \log H_v(\Omega).$$

Si F est un corps de nombres, on définit alors la hauteur absolue H et la hauteur logarithmique absolue h de la façon suivante: si $\operatorname{card} \Omega \geqslant 2$, on pose

$$H(\Omega) = \prod_{v \in M_F} H_v(\Omega)^{d_v^F/[F:\boldsymbol{Q}]}, \qquad h(\Omega) = \log H(\Omega);$$

si $\Omega = \{\omega\}$, on parle alors de hauteur du nombre algébrique ω qu'on définit par

$$H(\omega) = H(\{1, \omega\}), \qquad h(\omega) = h(\{1, \omega\}).$$

Il est classique que les définitions de H et de h ne dépendent pas du corps de nombres F contenant les éléments de la famille Ω.

Enfin, par v-hauteur $H_v(\Phi)$, hauteur absolue $H(\Phi)$ etc... d'un N-uple $\Phi = (\phi_1, \ldots, \phi_N)$ de polynômes ϕ_i à coefficients dans F, nous entendrons la v-hauteur, la hauteur absolue etc... de la famille des coefficients des polynômes $\phi_1, \phi_2, \ldots, \phi_N$.

1. *G*-fonctions.

1.1. *G*-fonctions et *G*-opérateurs différentiels. Soit $\mathscr{Y} = \sum_{m \geqslant 0} \eta_m X^m$ une série formelle à coefficients dans un corps de nombres K. On définit la taille $\sigma(\mathscr{Y})$ de la série $\mathscr{Y}$ par

$$\sigma(\mathscr{Y}) = \overline{\lim_{m \to +\infty}} \frac{1}{m}\left[\frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K} d_v^K h_v\left((\eta_h)_{h<m}\right)\right].$$

DEFINITION 1. On dit que $\mathscr{Y}$ est une *G-fonction* si

$$\sigma(\mathscr{Y}) < +\infty.$$

On définit également la taille $\sigma(Y)$ d'un vecteur Y à coordonnées

$$\mathscr{Y}_i = \sum_{m \geq 0} \eta_{im} X^m, \qquad i = 1, 2, \ldots, n$$

dans $K[[X]]$ par la quantité

$$\sigma(Y) = \overline{\lim_{m \to +\infty}} \frac{1}{m}\left[\frac{1}{[K:\mathbf{Q}]} \sum_{v \in M_K} d_v^K h_v\left((\eta_{ih})_{\substack{1 \leq i \leq n \\ h<m}}\right)\right].$$

Il est clair que, si $\mathscr{Y}_i \neq 0$ pour $i = 1, 2, \ldots, n$,

$$\max_{1 \leq i \leq n} \sigma(\mathscr{Y}_i) \leqslant \sigma(Y) \leqslant \sum_{i=1}^{n} \sigma(\mathscr{Y}_i).$$

Remarque 1. Il résulte de la définition qu'une G-fonction a un rayon de convergence strictement positif en toute place v d'un corps de nombres contenant ses coefficients.

Supposons maintenant donnés un opérateur différentiel linéaire L, défini sur un corps de nombres k et

$$Y = \begin{bmatrix} \mathscr{Y}_1 \\ \vdots \\ \mathscr{Y}_n \end{bmatrix}$$

un vecteur de taille $\sigma(Y)$ finie, solution de $LY = 0$. Nous nous proposons d'étudier les relations de dépendance linéaire sur k liant les valeurs en un point ξ de k des G-fonctions $\mathscr{Y}_1, \ldots, \mathscr{Y}_n$ et de montrer que, sous des hypothèses convenables sur ξ, elles ne peuvent pas être trop nombreuses si $\mathscr{Y}_1, \ldots, \mathscr{Y}_n$ sont $k(X)$-linéairement indépendantes. La méthode que nous allons développer — comme celle de Bombieri d'ailleurs — oblige cependant à certaines restrictions sur l'opérateur L: nous devrons supposer que L est un G-opérateur différentiel. Nous allons maintenant définir cette nouvelle notion.

Soient k un corps de nombres, n un entier non nul et $A \in M_{n \times n}(k(X))$ une matrice $n \times n$ à coefficients dans $k(X)$. On s'intéresse à l'opérateur différentiel linéaire

$$L = D - A.$$

D désignant la dérivation par rapport à l'indéterminée X du corps $\overline{\mathbf{Q}}((X))$. On notera R le p.p.c.m. dans $k[X]$ des dénominateurs de la matrice A; $B = (B_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ la matrice $B = RA$ qui est donc à coefficients dans $k[X]$ et δ le nombre entier défini par

$$\delta = \max(\deg R, \max_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}} \deg B_{ij}).$$

PROPOSITION 1. *Soient Ω une extension de k et z un élément de Ω, ordinaire pour l'opérateur L (i.e. $R(z) \neq 0$). Il existe une famille*

$$(P_{M,m,j})_{\substack{M \geqslant 0 \\ 0 \leqslant m \leqslant M \\ 0 \leqslant j \leqslant \delta}}$$

de matrices $n \times n$ à coefficients dans le corps k, ayant la propriété suivante. Un vecteur $y = \sum_{m \geqslant 0} y_{z,m}(X-z)^m$ à composantes dans $\Omega[[X-z]]$ est solution de $Ly = 0$ si et seulement si

$$(1) \qquad R(z)\, y_{z,M+1} = \sum_{j=0}^{\delta} \Big(\sum_{m=0}^{M} P_{M,m,j} \cdot y_{z,m} \Big) z^j \quad \text{pour} \quad M = 0, 1, 2, \ldots$$

Démonstration. Introduisons tout d'abord une nouvelle notation. Si $\psi \in \Omega[X, Y]^N$ est un N-uple de polynômes et x, y deux éléments de Ω, nous noterons $\psi_{x,y}$, et ψ_x si $y = 0$, le N-uple de polynômes défini par

$$\psi_{x,y}(X-x, Y-y) = \psi.$$

Dire que y est une solution de $Ly = 0$ signifie alors que

$$(2) \qquad R_z\, Dy_z = B_z\, y_z$$

où $y_z \in \Omega[[X]]$ désigne la série formelle $y_z = \sum_{m \geqslant 0} y_{z,m} X^m$. Cette relation s'écrit

$$\Big(\sum_{h=0}^{\delta} \frac{1}{h!} R^{(h)}(z)\, X^h \Big) \Big(\sum_{h \geqslant 0} (h+1)\, y_{z,h+1}\, X^h \Big) = \Big(\sum_{h=0}^{\delta} \frac{1}{h!} B^{(h)}(z)\, X^h \Big) \Big(\sum_{h \geqslant 0} y_{z,h} X^h \Big).$$

On égale alors les termes en X^M, puis on applique la formule de Taylor en 0 aux expressions polynômiales $R^{(h)}(z)$ pour $h = 1, 2, \ldots, \delta$ et $B^{(h)}(z)$ pour $h = 0, 1, 2, \ldots, \delta$. Après avoir réordonné les termes, on obtient:

$$(M+1)\, R(z)\, y_{z,M+1}$$
$$= \sum_{j=0}^{\delta} \left[\sum_{m=0}^{M} \left(\frac{1}{(M-m)!} B^{(M-m+j)}(0) - \frac{m}{(M-m+1)!} R^{(M-m+j+1)}(0) \right) \cdot y_{z,m} \right] z^j / j!$$

ce qui est bien de la forme indiquée en (1). ∎

On déduit aussitôt de la proposition 1 que si z est un point ordinaire pour L et η un élément quelconque de Ω^n alors il existe une unique solution de (2) qu'on notera

$$y_z(\eta) = \sum_{m \geqslant 0} y_{z,m}(\eta)\, X^m$$

qui vérifie

$$y_{z,0}(\eta) = \eta.$$

Dans la suite, b désigne une base quelconque de k^n; il est facile de vérifier que les définitions que nous allons donner et où b intervient, sont indépendantes du choix de cette base.

Soit $z \in k$ un point ordinaire pour L; on définit alors le coefficient $s(L, z)$ qui ne dépend que de L et de z par

$$s(L, z) = \overline{\lim_{m \to +\infty}} \frac{1}{m}\left[\frac{1}{[k: Q]} \sum_{v \in M_k} d_v^k \max_{\eta \in b} h_v\left((y_{z,h}(\eta))_{h<m}\right)\right].$$

Au cours de la démonstration du théorème principal, nous aurons besoin de majorations du type

$$s(L, \xi) \leqslant a_1 h(\xi) + a_2 \quad \text{avec} \quad a_1 = a_1(L) \text{ et } a_2 = a_2(L) \tag{3}$$

en tout point ξ de k, ordinaire pour L. Nous allons voir que pour disposer de telles majorations, il suffit d'imposer une condition du même type au point générique.

Pour toute place finie v de k, on se fixe une extension Ω_v complète et algébriquement close de k_v et qui contient une unité t_v dont l'image dans le corps résiduel de Ω_v soit transcendante sur le corps résiduel de k_v. On définit alors le coefficient $s(L)$ qui ne dépend plus que de L (cf. remarque 4) par:

$$s(L) = \overline{\lim_{m \to +\infty}} \frac{1}{m}\left[\frac{1}{[k: Q]} \sum_{v \in M_k^0} d_v^k \max_{\eta \in b} h_v\left((y_{t_v,h}(\eta))_{h<m}\right)\right]. \tag{4}$$

Definition 2. Nous dirons que L est un *G-opérateur différentiel* si

$$s(L) < +\infty.$$

Remarque 2. Le coefficient $s(L)$ doit être comparé au coefficient introduit par Bombieri pour définir les opérateurs différentiels fuchsiens de type arithmétique ([1], p. 46). Celui-ci vaut

$$\frac{1}{[k: Q]} \sum_{v \in M_k^0} d_v^k \max_{\eta \in b}\left(\overline{\lim_{m \to +\infty}} \frac{1}{m} h_v\left((y_{t_v,h}(\eta))_{h<m}\right)\right)$$

et s'obtient donc en intervertissant "$\overline{\lim}$" et "$\sum$" puis "$\overline{\lim}$" et "max" dans le membre de droite de (4). Sauf peut-être dans des situations très pathologiques, il sera donc supérieur à $s(L)$ si bien qu'un opérateur différentiel fuchsien de type arithmétique sera "presque toujours" un G-opérateur différentiel. Dans toutes les applications, en particulier quand L sera un opérateur différentiel associé à une fonction algébrique (cf. § 2), les deux notions coïncideront.

Proposition 2. *Soit L un G-opérateur différentiel. Alors il existe deux*

constantes a_1 et a_2 ne dépendant que de L telles que, pour tout point ξ dans k, ordinaire pour L, on ait

$$s(L, \xi) \leqslant a_1 h(\xi) + a_2.$$

Remarque 3. Il résulte de la proposition 2 que si Lest un G-opérateur différentiel, alors pour tout point ordinaire ξ dans k, les solutions y dans $k[[X]]^n$ du système différentiel translaté $(R_\xi D - B_\xi)\, y = 0$ sont nécessairement toutes des G-fonctions.

La proposition suivante, qui nous servira dans la démonstration de la proposition 2 à majorer les termes correspondant aux places finies dans $s(L, \xi)$ montre tout l'intérêt de la notion de point générique.

Proposition 3. *Soient v une place finie de k, z un point ordinaire pour L dans Ω_v et η un vecteur dans k^n. Alors pour tout entier M et toute famille de matrices $Q_0, \ldots, Q_M$ dans $M_{1\times n}(k)$, on a:*

$$(5) \qquad \Big|\sum_{m=0}^{M} Q_m \cdot y_{z,m}(\eta)\Big|_v \leqslant \Big|\sum_{m=0}^{M} Q_m \cdot y_{t_v,m}(\eta)\Big|_v \left[\frac{H_v(R)\max(1, |z|_v)^\delta}{|R(z)|_v}\right]^M.$$

Remarque 4. On déduit facilement de la proposition 3 que le coefficient $s(L)$ ne dépend pas du choix du point générique t_v. (Prendre $z = t'_v$ un second point générique et remarquer que $|R(t'_v)|_v = H_v(R)$.)

Démonstration. On démontre la proposition 3 par récurrence sur M. Pour $M = 0$, l'inégalité (5) est triviale puisque par définition

$$y_{z,0}(\eta) = y_{t_v,0}(\eta) = \eta.$$

Supposons donc le résultat vrai pour l'entier M et soit $Q_0, Q_1, \ldots, Q_{M+1}$ une famille de matrices $1 \times n$ à coefficients dans k. En utilisant la proposition 1, on obtient

$$\sum_{m=0}^{M+1} Q_m \cdot y_{z,m}(\eta) = \sum_{m=0}^{M} Q_m \cdot y_{z,m}(\eta) + \frac{1}{R(z)} Q_{M+1}\Big[\sum_{j=0}^{\delta}\Big(\sum_{m=0}^{M} P_{M,m,j} \cdot y_{z,m}(\eta)\Big) z^j\Big]$$

soit

$$(6) \qquad \sum_{m=0}^{M+1} Q_m \cdot y_{z,m}(\eta) = \frac{1}{R(z)}\left[\sum_{j=0}^{\delta}\left(\sum_{m=0}^{M}\left(\frac{1}{j!} R^{(j)}(0)\, Q_m + Q_{M+1} \cdot P_{M,m,j}\right) \cdot y_{z,m}(\eta)\right) z^j\right].$$

On obtient donc, en utilisant l'hypothèse de récurrence et l'égalité $H_v(R) = |R(t_v)|_v$

$$\Big|\sum_{m=0}^{M+1} Q_m \cdot y_{z,m}(\eta)\Big|_v \leqslant W\left[\frac{H_v(R)\max(1, |z|_v)^\delta}{|R(z)|_v}\right]^{M+1}$$

où

$$W = \max_{0 \leqslant j \leqslant \delta} \left| \frac{1}{R(t_v)} \sum_{m=0}^{M} \left(\frac{1}{j!} R^{(j)}(0) Q_m + Q_{M+1} \cdot P_{M,m,j} \right) \cdot y_{t_v,m}(\eta) \right|_v .$$

Or, comme t_v est générique, W vaut

$$W = \left| \sum_{j=0}^{\delta} \frac{1}{R(t_v)} \left[\sum_{m=0}^{M} \left(\frac{1}{j!} R^{(j)}(0) Q_m + Q_{M+1} \cdot P_{M,m,j} \right) \cdot y_{t_v,m}(\eta) \right] t_v^j \right|_v$$

soit, d'après la relation (6)

$$W = \left| \sum_{m=0}^{M+1} Q_m \cdot y_{t_v,m}(\eta) \right|_v . \quad \blacksquare$$

Nous sommes maintenant en mesure de démontrer la proposition 2. Notons pour tout point ξ dans k, ordinaire pour L

$$s^0(L, \xi) = \overline{\lim_{m \to +\infty}} \frac{1}{m} \left[\frac{1}{[k:Q]} \sum_{v \in M_k^0} d_v^k \max_{\eta \in b} h_v\left((y_{\xi,h}(\eta))_{h<m} \right) \right]$$

et

$$s^\infty(L, \xi) = \overline{\lim_{m \to +\infty}} \frac{1}{m} \left[\frac{1}{[k:Q]} \sum_{\substack{v \in M_k \\ v \mid \infty}} d_v^k \max_{\eta \in b} h_v\left((y_{\xi,h}(\eta))_{h<m} \right) \right].$$

De la proposition 3, on déduit que

$$s^0(L, \xi) \leqslant \delta h(\xi) + s(L) + h(R) + \log(1+\delta). \tag{7}$$

Voyons maintenant la contribution des places archimédiennes. En utilisant le fait que si $(u_m)_{m \geqslant 0}$ est une suite à termes positifs non tous nuls, on a:

$$\overline{\lim_{m \to +\infty}} \max_{0 \leqslant h \leqslant m} u_h^{1/m} = \max\left(1, \overline{\lim_{m \to +\infty}} u_m^{1/m}\right)$$

on obtient que

$$s^\infty(L, \xi) \leqslant \frac{1}{[k:Q]} \sum_{\substack{v \in M_k \\ v \mid \infty}} d_v^k \log^+ \frac{1}{r_v(\xi)} \tag{8}$$

où $r_v(\xi)$ désigne le plus petit des rayons de convergence v-adiques des solutions dans $k[[X]]^n$ de $Dy = A_\xi y$. Or, pour v archimédienne, $r_v(\xi)$ est supérieur ou égal à la plus petite des distances v-adiques de ξ à l'une des singularités de L, soit

$$r_v(\xi) \geqslant \inf_{x, R(x)=0} |x - \xi|_w$$

où w est une place au-dessus de v du corps engendré par k et par les racines de R. Grâce à l'inégalité de Liouville, on obtient la majoration

$$\max\left(1, \frac{1}{r_v(\xi)}\right) \leqslant \frac{2H_v(R_\xi)}{|R(\xi)|_v}$$

et donc

$$\frac{1}{[k:Q]} \sum_{\substack{v \in M_k \\ v|\infty}} d_v^k \log^+ \frac{1}{r_v(\xi)} \leqslant h(R_\xi) + \log 2 \tag{9}$$

$$\leqslant \delta h(\xi) + h(R) + (1+\delta)\log 2 + \log(1+\delta).$$

Finalement, comme

$$s(L, \xi) \leqslant s^0(L, \xi) + s^\infty(L, \xi)$$

on obtient le résultat désiré en regroupant (7), (8) et (9). ∎

1.2. Enoncé du théorème principal. Soient k un corps de nombres, $n \geqslant 1$ un entier et A une matrice $n \times n$ à coefficients dans $k(X)$. On suppose que l'opérateur $L = D - A$ est un G-opérateur différentiel.

On se donne également Y un vecteur solution de $LY = 0$ de composantes n G-fonctions $\mathscr{y}_1, \ldots, \mathscr{y}_n$ à coefficients dans un corps de nombres K contenant k. Pour toute place v de K, on note R_v le rayon de convergence v-adique du vecteur Y et $Y_{1,v}, \ldots, Y_{n,v}$ les fonctions naturellement induites par $\mathscr{y}_1, \ldots, \mathscr{y}_n$ sur la boule ouverte $B(0, R_v)$ de K_v.

On suppose de plus que les séries formelles $\mathscr{y}_1, \ldots, \mathscr{y}_n$ sont $k(X)$-linéairement indépendantes et que

$$\frac{1}{[K:Q]} \sum_{v \in M_K} d_v^K \log^+ \frac{1}{R_v} < +\infty.$$

Sous ces conditions, on a le résultat suivant.

THÉORÈME PRINCIPAL. *Soient ξ un élément non nul de k, ϱ un entier et $\Lambda = (\lambda_{ij})_{\substack{1 \leqslant i \leqslant \varrho \\ 1 \leqslant j \leqslant n}}$ une matrice à coefficients dans k de rang ϱ. Soit enfin $S(\xi, \Lambda)$ l'ensemble des places v de K vérifiant:*

$$|\xi|_v < \min(1, R_v) \quad \text{et} \quad \sum_{j=1}^{n} \lambda_{ij} Y_{j,v}(\xi) = 0 \quad \text{pour} \quad i = 1, 2, \ldots, \varrho.$$

Alors

$$\frac{1}{[K:Q]} \sum_{v \in S(\xi, \Lambda)} d_v^K \log|\xi|_v + \frac{n-\varrho}{n} h(\xi) \geqslant -C_1 - C_2\sqrt{h(\xi)} \tag{10}$$

où C_1 et C_2 sont deux constantes ne dépendant que de L et de Y.

Remarques. 1. De façon précise, on peut prendre C_1 et C_2 égaux à

$$C_1 = 2h(R)+s(L)+\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v^K \log^+ \frac{1}{R_v}$$
$$+\tfrac{9}{2}(1+2\delta)+(3+\delta)\log 2+2\log(1+\delta),$$

$$C_2 = n\left(\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v^K \log^+ \frac{1}{R_v}+\sigma(\boldsymbol{Y})\right)+\tfrac{9}{4}(1+2\delta)+\log 2.$$

2. L'inégalité du théorème principal est essentiellement la même que celle que démontre Bombieri ([1], Main Theorem, p. 49). Cependant, l'hypothèse sur l'opérateur L est ici différente puisque Bombieri suppose que L est un opérateur différentiel fuchsien de type arithmétique (cf. § 1.1, Rem. 2). Signalons enfin qu'à la différence de Bombieri nous ne supposons pas les séries formelles $\mathscr{Y}_1, \ldots, \mathscr{Y}_n$ à coefficients dans le corps de base k.

L'intérêt majeur de cet article réside dans la façon dont nous allons aborder le problème. Notre approche reste analytique, mais s'appuie, non pas sur la méthode de Siegel comme chez Bombieri, mais sur un développement de la méthode mise en oeuvre par Gel'fond pour résoudre le 7ème problème de Hilbert (cf. [25], Chap. 3). Celle-ci va s'avérer plus simple dans le cas présent.

La méthode de Siegel prévoit tout d'abord la construction d'une fonction auxiliaire qui s'annule à un ordre élevé au point 0. On montre ensuite, à l'aide du théorème de Shidlovski, qu'un certain déterminant lié aux nombres λ_{ij} et aux dérivées au point ξ de la fonction auxiliaire, est non nul. On obtient le résultat voulu en minorant puis en majorant cette quantité.

Cette dernière étape, dans le cas de G-fonctions, présente de nombreuses difficultés, dues essentiellement aux factoriels qui apparaissent lors des différentiations successives de la fonction auxiliaire, et qui obligent à recourir à des résultats délicats comme le théorème de Dwork–Robba ([1], § 5 et § 6).

Nous allons voir que l'emploi de la méthode de Gel'fond permet d'éviter ces complications. Nous procéderons de la façon suivante. On va également construire une fonction auxiliaire, mais qui s'annulera à un ordre élevé au point ξ et pour les places v dans l'ensemble $S(\xi, \Lambda)$. Cette construction n'est qu'un peu plus difficile: elle repose sur le travail préparatoire du paragraphe § 1.1, notamment la proposition 2. Nous minorerons et majorerons ensuite, tout simplement le premier terme non nul du développement de Taylor au point 0 de la fonction auxiliaire.

La méthode de Gel'fond s'était déjà révélée fructueuse dans le cadre des fonctions algébriques ([3], [4], [5]). Nous généralisons ici ces travaux.

1.3. Démonstration du théorème principal. Les constantes c_i, $i = 1, 2, \ldots, 10$ qui interviennent dans la suite sont des quantités positives ne

dépendant que de L et de Y. D'autre part, nous dirons qu'une suite $(u_M)_{M\geqslant 0}$ à termes réels est un $\bar{o}(1)$ si

$$\overline{\lim_{M\to+\infty}}\, u_M \leqslant 0.$$

Enfin, nous noterons $[x]$ la partie entière de tout nombre réel x.

Soit donc ξ un élément non nul de k. Le terme de gauche dans l'inégalité du théorème principal étant supérieur à $-h(\xi)$, on peut, quitte à prendre finalement C_2 assez grand, supposer que ξ est un point ordinaire pour L, de hauteur $h(\xi)\geqslant 4$.

On se donne également $\Lambda=(\lambda_{ij})_{\substack{1\leqslant i\leqslant \varrho\\ 1\leqslant j\leqslant n}}$ une matrice à coefficients dans k de rang ϱ. Nous noterons $(e_\lambda)_{1\leqslant\lambda\leqslant n-\varrho}$ une base du sous-espace vectoriel V de k^n défini par les équations

$$\sum_{j=1}^{n}\lambda_{ij}x_j=0 \quad \text{pour} \quad i=1,2,\ldots,\varrho.$$

LEMME 1. *Soient $M>0$ un entier et p l'entier défini par $p=M[\sqrt{h(\xi)}]$. Alors il existe un n-uple $\Phi=(\phi_1,\ldots,\phi_n)$ de polynômes non tous nuls $\phi_i=\sum_j \phi_{ij}X^j$ à coefficients ϕ_{ij} dans k, vérifiant*

(a) $\deg\phi_i<p$ *pour* $i=1,2,\ldots,n$,

(b) *pour* $\lambda=1,2,\ldots,n-\varrho$, *la série formelle* $\Phi_\xi\cdot y_\xi(e_\lambda)$ *a un zéro d'ordre* $\geqslant M$ *en* 0,

(c) $\dfrac{h(\Phi)}{M}\leqslant\dfrac{n-\varrho}{n}h(\xi)+c_1+c_2\sqrt{h(\xi)}+\bar{o}(1)$.

Démonstration. On a *a priori*

$$\Phi_\xi\cdot y_\xi(e_\lambda)=\sum_{m\geqslant 0}\left(\sum_{h=0}^{m}\frac{1}{h!}\Phi^{(h)}(\xi)\cdot y_{\xi,m-h}(e_\lambda)\right)X^m.$$

La condition (b) du lemme 1 est donc équivalente au système d'équations

$$L_{\lambda,m}\big((\phi_{ij})_{\substack{1\leqslant i\leqslant n\\ 0\leqslant j<p}}\big)=0, \qquad \lambda=1,2,\ldots,n-\varrho,\ m=1,2,\ldots,M$$

où

$$L_{\lambda,m}=\sum_{i,j}A_{\lambda,m-1,i,j}X_{ij}$$

et

$$A_{\lambda,m,i,j}=\sum_{h=0}^{\min(m,j)}\binom{j}{h}\xi^{j-h}y_{i,\xi,m-h}(e_\lambda)$$

$y_{i,\xi,m-h}(e_\lambda)$ désignant le $(m-h)$-ième coefficient de la i-ième composante de $y_\xi(e_\lambda)$.

C'est un système linéaire de $(n-\varrho)M$ équations à np inconnues. L'hypothèse $h(\xi) \geqslant 4$ impose $np-(n-\varrho)M \geqslant nM > 0$. D'après le lemme de Siegel démontré dans [1] (p.7), il existe un n-uple $\Phi = (\phi_1, \ldots, \phi_n)$ de polynômes $\phi_i \in k[X]$ non tous nuls, vérifiant les conditions (a) et (b) du lemme 1 et

$$H(\Phi) \leqslant \prod_{\substack{1 \leqslant \lambda \leqslant n-\varrho \\ 1 \leqslant m \leqslant M}} H(L_{\lambda,m})^{1/(np-(n-\varrho)M)} \exp(o(1)). \tag{11}$$

Reste donc, pour obtenir (c) à majorer la hauteur des formes linéaires $L_{\lambda,m}$. Soit v une place de k. Pour $1 \leqslant \lambda \leqslant n-\varrho$, $1 \leqslant i \leqslant n$, $0 \leqslant j < p$ et $0 \leqslant m < M$, on a

$$|A_{\lambda,m,i,j}|_v \leqslant \max(1, |\xi|_v)^p H_v\big((y_{\xi,h}(e_\lambda))_{h<M}\big) \quad \text{si } v \text{ est finie,}$$

$$|A_{\lambda,m,i,j}|_v \leqslant 2^p \max(1, |\xi|_v)^p H_v\big((y_{\xi,h}(e_\lambda))_{h<M}\big) \quad \text{si } v \text{ est archimédienne.}$$

On en déduit que pour $\lambda = 1, 2, \ldots, n-\varrho$ et $m = 1, 2, \ldots, M$ on a

$$h(L_{\lambda,m}) \leqslant ph(\xi) + p\log 2 + \frac{1}{[k:Q]} \sum_{v \in M_k} d_v^k \max_{1 \leqslant \lambda \leqslant n-\varrho} h_v\big((y_{\xi,h}(e_\lambda))_{h<M}\big).$$

En reportant dans (11), on obtient

$$\frac{h(\Phi)}{M} \leqslant \frac{(n-\varrho)h(\xi)}{n-(n-\varrho)/[\sqrt{h(\xi)}]} + \log 2 \sqrt{h(\xi)} + \frac{(n-\varrho)s(L,\xi)}{n[\sqrt{h(\xi)}]-(n-\varrho)} + \bar{o}(1).$$

On conclut grâce à l'hypothèse "L est un G-opérateur différentiel" et la proposition 2 qui permet de majorer le terme $s(L, \xi)$. ∎

Considérons maintenant la solution Y du système différentiel $LY = 0$, donnée dans l'énoncé du théorème principal; ses composantes $y_1, \ldots, y_n$ étant supposées $k(X)$-linéairement indépendantes, la série formelle

$$\Phi \cdot Y = \phi_1 y_1 + \ldots + \phi_n y_n$$

est non nulle. Le théorème de Shidlovski ([19], Ch.5) permet alors de majorer $\bar{I}$, l'ordre en 0 de cette série par

$$\bar{I} \leqslant np + c_3. \tag{12}$$

On note ensuite γ le coefficient de $X^{\bar{I}}$ dans $\Phi \cdot Y$; c'est un élément non nul du corps K; on peut donc écrire la formule du produit

$$\prod_{v \in M_K} |\gamma|_v^{d_v^K} = 1. \tag{13}$$

Nous allons maintenant majorer les $|\gamma|_v$. De l'inégalité ainsi obtenue, nous déduirons le résultat voulu. On définit tout d'abord deux ensembles S_1 et S_2 de la manière suivante:

$$S_1 = \{v \in M_K : v \in S(\xi, \Lambda), v \mid \infty \text{ et } |\xi|_v \geqslant \min(1, R_v)/2\}, \quad S_2 = S(\xi, \Lambda) \setminus S_1.$$

Nous allons distinguer deux types de majoration suivant que v appartient à S_2 ou pas.

LEMME 2. *On a*

$$\frac{1}{M}\left|\frac{1}{[K:Q]}\sum_{v\notin S_2} d_v^K \log|\gamma|_v\right| \leqslant \frac{1}{M}\left[\frac{1}{[K:Q]}\sum_{v\notin S_2} d_v^K h_v(\Phi)\right] + c_4\sqrt{h(\xi)} + \bar{o}(1).$$

Démonstration. Notons pour $i = 1, 2, \ldots, n$, $\mathscr{Y}_i = \sum_{m\geqslant 0} \eta_{i,m} X^m$. De la formule

$$\gamma = \sum_{i=1}^{n}\sum_{h=0}^{\bar{l}} \phi_{i,h}\,\eta_{i,\bar{l}-h}$$

on déduit que

$$|\gamma|_v \leqslant H_v(\Phi)\, H_v\big((\eta_{ih})_{\substack{1\leqslant i\leqslant n\\ h\leqslant \bar{l}}}\big) \qquad \text{si } v \text{ est finie,}$$

$$|\gamma|_v \leqslant n(\bar{l}+1)\, H_v(\Phi)\, H_v\big((\eta_{ih})_{\substack{1\leqslant i\leqslant n\\ h\leqslant \bar{l}}}\big) \qquad \text{si } v \text{ est archimédienne.}$$

On obtient donc, en utilisant (12)

$$\frac{1}{[K:Q]}\sum_{v\notin S_2} d_v^K \log|\gamma|_v \leqslant \frac{1}{[K:Q]}\sum_{v\notin S_2} d_v^K h_v(\Phi) + \frac{1}{[K:Q]}\sum_{v\in M_K} d_v^K h_v\big((\eta_{ih})_{\substack{1\leqslant i\leqslant n\\ h\leqslant np+c_3}}\big) + o(M)$$

soit

$$\frac{1}{[K:Q]}\sum_{v\notin S_2} d_v^K \log|\gamma|_v \leqslant \frac{1}{[K:Q]}\sum_{v\notin S_2} d_v^K h_v(\Phi) + (np+c_3)\,\sigma(Y) + M\cdot\bar{o}(1)$$

ce qui fournit la conclusion désirée, puisque les séries $\mathscr{Y}_1, \ldots, \mathscr{Y}_n$ sont des G-fonctions. ∎

LEMME 3. *Pour tout ε tel que $0 < \varepsilon < \min_{v\in S_2}\big(\min(R_v/2,\, R_v - |\xi|_v)\big)$ on a*

$$\frac{1}{M}\left[\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K \log|\gamma|_v\right] \leqslant \frac{1}{[K:Q]}\sum_{v\in S(\xi,\Lambda)} d_v^K \log|\xi|_v + \frac{1}{M}\left[\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K h_v(\Phi)\right] + \frac{(1+n\sqrt{h(\xi)})}{[K:Q]}\left[\sum_{v\in S_2} d_v^K \log^+\frac{1}{R_v - 2\varepsilon}\right] + c_5 + o(1).$$

Démonstration. Soit v une place de $S(\xi, \Lambda)$. Le vecteur

$$\boldsymbol{Y}_v = \begin{bmatrix} Y_{1,v} \\ \vdots \\ Y_{n,v} \end{bmatrix}$$

est une solution de $L\boldsymbol{Y}_v = 0$ définie au voisinage de ξ; d'autre part, par définition de l'ensemble $S(\xi, \Lambda)$, le vecteur $\boldsymbol{Y}_v(\xi)$ appartient à l'espace vectoriel $V \otimes_k K_v$ dont $(e_\lambda)_{1 \leqslant \lambda \leqslant n-\varrho}$ est une base sur K_v. Le point ξ étant ordinaire pour L, il existe une famille unique $(\mu_{v,\lambda})_{1 \leqslant \lambda \leqslant n-\varrho}$ d'éléments de K_v, vérifiant

$$\boldsymbol{Y}_v(x) = \sum_{\lambda=1}^{n-\varrho} \mu_{v,\lambda}\, \boldsymbol{y}_{\xi,v}(e_\lambda)(x-\xi) \tag{14}$$

pour tout x dans un voisinage v-adique de ξ. Dans (14), nous avons noté $\boldsymbol{y}_{\xi,v}(e_\lambda)$ la fonction naturellement induite par $\boldsymbol{y}_\xi(e_\lambda)$ au voisinage de ξ pour la place v.

On en déduit qu'au voisinage de ξ, on a

$$(\Phi \cdot \boldsymbol{Y}_v)(x) = \sum_{\lambda=1}^{n-\varrho} \mu_{v,\lambda} \big(\Phi_\xi \cdot \boldsymbol{y}_{\xi,v}(e_\lambda)\big)(x-\xi).$$

Par construction de Φ, la fonction $\Phi \cdot \boldsymbol{Y}_v$ admet donc en ξ un zéro d'ordre $\geqslant M$.

Supposons maintenant v dans l'ensemble $S_2 \subset S(\xi, \Lambda)$. On note w un prolongement de v à $\overline{\boldsymbol{Q}}$, $\boldsymbol{C}_w$ le complété de $\overline{\boldsymbol{Q}}$ pour la place w et $\boldsymbol{Y}_w$ la fonction, qui prolonge $\boldsymbol{Y}_v$, induite par $\boldsymbol{Y}$ sur la boule ouverte $B_w = \{x \in \boldsymbol{C}_w : |x|_w < R_v\}$ de $\boldsymbol{C}_w$. D'après ce qui précède, la fonction

$$G_w : x \to \frac{(\Phi \cdot \boldsymbol{Y}_w)(x)}{x^I (x-\xi)^M}$$

est strictement analytique sur toute boule fermée de B_w et prend la valeur $G_w(0) = \gamma(-\xi)^{-M}$ en 0.

Soit ε un nombre réel vérifiant la condition de l'énoncé du lemme 3. En appliquant le principe du maximum à la fonction G_w sur la boule de C_w centrée en 0 et de rayon $\min(1, R_v - \varepsilon)$, on obtient

$$|\gamma|_v \leqslant |\xi|_v^M \min(1, R_v-\varepsilon)^{-(I+M)} H_v(\Phi)\, M_w\big(\boldsymbol{Y}, \min(1, R_v-\varepsilon)\big) \quad \text{si } v \text{ est finie,}$$

$$|\gamma|_v \leqslant |\xi|_v^M \min(1, R_v-2\varepsilon)^{-(I+M)} 2^M H_v(\Phi)\, npM_w\big(\boldsymbol{Y}, \min(1, R_v-\varepsilon)\big)$$

si v est archimédienne

où nous avons noté

$$M_w(\boldsymbol{Y}, r) = \max_{1 \leqslant i \leqslant n} \max_{|x|_v = r} |Y_{i,w}(x)|_w \quad \text{pour} \quad 0 < r < R_v.$$

En utilisant (12) on en déduit:

$$(15)\quad \frac{1}{M}\left[\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K \log|\gamma|_v\right] \leqslant \frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K \log|\xi|_v + \frac{1}{M}\left[\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K h_v(\Phi)\right] + \frac{(n\sqrt{h(\xi)}+1)}{[K:Q]}\left[\sum_{v\in S_2} d_v^K \log^+ \frac{1}{R_v-2\varepsilon}\right] + \log 2 + o(1).$$

D'autre part, il est évident que

$$(16)\quad -\frac{1}{[K:Q]}\sum_{v\in S_1} d_v^K \log|\xi|_v \leqslant \frac{1}{[K:Q]}\sum_{\substack{v\in M_K\\ v|\infty}} d_v^K \log^+ \frac{1}{R_v} + \log 2 = c_6.$$

En joignant (15) et (16), on obtient le résultat annoncé. ∎

Reportons maintenant dans (13) les résultats des lemmes 2 et 3. On obtient que, pour $\varepsilon > 0$ assez petit

$$0 \leqslant \frac{1}{[K:Q]}\sum_{v\in S(\xi,A)} d_v^K \log|\xi|_v + \frac{h(\Phi)}{M} + (1+n\sqrt{h(\xi)})\left[\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K \log^+ \frac{1}{R_v-2\varepsilon}\right] + c_5 + c_4\sqrt{h(\xi)} + \bar{o}(1)$$

et donc, en tenant compte de la majoration (c) du lemme 1

$$0 \leqslant \frac{1}{[K:Q]}\sum_{v\in S(\xi,A)} d_v^K \log|\xi|_v + \frac{n-\varrho}{n}h(\xi) + (1+n\sqrt{h(\xi)})\left[\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K \log^+ \frac{1}{R_v-2\varepsilon}\right] + c_7 + c_8\sqrt{h(\xi)} + \bar{o}(1).$$

On passe ensuite à la lim sup en M, puis on fait tendre ε vers 0; enfin on majore

$$\frac{1}{[K:Q]}\sum_{v\in S_2} d_v^K \log^+ \frac{1}{R_v} \quad \text{par} \quad \frac{1}{[K:Q]}\sum_{v\in M_K} d_v^K \log^+ \frac{1}{R_v}.$$

On obtient finalement

$$\frac{1}{[K:Q]}\sum_{v\in S(\xi,A)} d_v^K \log|\xi|_v + \frac{n-\varrho}{n}h(\xi) + c_9 + c_{10}\sqrt{h(\xi)} \geqslant 0. \ ∎$$

1.4. Première remarque sur l'utilisation du théorème principal. Soit S un ensemble de places v de k où $|\xi|_v < R_v$. Le théorème principal fournit une majoration du nombre ϱ des relations de k-dépendance linéaire, linéairement indépendantes sur k, existant entre les nombres $Y_{1,v}(\xi), \ldots, Y_{n,v}(\xi)$ pour v

dans S. Notons que cette majoration est d'autant meilleure que l'ensemble S est gros. Ainsi si S est l'ensemble de toutes les places v où $|\xi|_v < R_v$, l'inégalité (10) conduit nécessairement à

$$\varrho < 1$$

dès que ξ est de hauteur assez grande.

Cette remarque conduit aussitôt à de premiers résultats. On en déduit par exemple (cf. [1], Sect. 11) que l'ensemble des points ξ de k où il existe une relation de k-dépendance linéaire globale – c'est-à-dire une relation

$$\sum_{i=1}^{n} \lambda_i Y_{i,v}(\xi) = 0 \quad \text{avec } \lambda_1, \ldots, \lambda_n \text{ éléments de } k,$$

valide en toute place v où $|\xi|_v < R_v -$, est un ensemble fini.

En faisant des hypothèses supplémentaires sur ξ, on peut également donner des résultats d'indépendance linéaire: supposons que l'ensemble des places v de K telles que $|\xi|_v < 1$, que l'on notera désormais $M_K(\xi)$, ne possède qu'un élément v_0; La remarque précédente montre alors que les nombres $Y_{1,v_0}(\xi), \ldots, Y_{n,v_0}(\xi)$ sont définis et k-linéairement indépendants dès que $h(\xi)$ est assez grand. A titre d'illustration de ce dernier résultat, donnons le corollaire suivant.

COROLLAIRE 1. *Supposons en plus des hypothèses du théorème principal que $k = K = \mathbf{Q}$. Alors il existe une constante C ne dépendant que de L et de Y, vérifiant*

(a) *Pour tout nombre premier p et pour tout entier m tels que $p^m > C$ les nombres $Y_{1,p}(p^m), \ldots, Y_{n,p}(p^m)$ sont définis et $\mathbf{Q}$-linéairement indépendants.*

(b) *Pour tout entier non nul m tel que $|m| > C$, les nombres $Y_{1,\infty}(1/m), \ldots, Y_{n,\infty}(1/m)$ sont définis et $\mathbf{Q}$-linéairement indépendants.*

Nous reviendrons sur ces remarques dans le cas particulier des fonctions algébriques. Pour d'autres applications du théorème principal, non spécifiques aux fonctions algébriques, nous renvoyons à [1].

2. Fonctions algébriques.

2.1. Le théorème 2. Soit k un corps de nombres et P un polynôme irréductible dans $k[X, Y]$. On suppose qu'il existe une série formelle $\mathcal{Y} = \sum_{m \geq 0} \eta_m X^m$ à coefficients dans $\overline{\mathbf{Q}}$, solution de

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

Nous noterons K le corps $K = k((\eta_m)_{m \geq 0})$. Il est facile de voir que K est un corps de nombres et que $[K:k] \leq \deg_Y P$.

Le polynôme P étant irréductible dans $k(X)[Y]$, le corps $k(X, \mathcal{Y})$ est un

$k(X)$-espace vectoriel de dimension $n = \deg_Y P$ et la famille $\{1, \mathscr{y}, \ldots, \mathscr{y}^{n-1}\}$ en constitue une base. D'autre part, à cause de la formule

$$D\mathscr{y} = -\frac{P'_X(X, \mathscr{y})}{P'_Y(X, \mathscr{y})} \tag{1}$$

il est clair que la dérivation D laisse stable le corps $k(X, \mathscr{y})$. De ces deux dernières remarques, on déduit qu'il existe une matrice $n \times n$ à coefficients dans $k(X)$, A, vérifiant:

$$D\begin{bmatrix} 1 \\ \mathscr{y} \\ \vdots \\ \mathscr{y}^{n-1} \end{bmatrix} = A\begin{bmatrix} 1 \\ \mathscr{y} \\ \vdots \\ \mathscr{y}^{n-1} \end{bmatrix}. \tag{2}$$

Notons L l'opérateur $L = D - A$. On retrouve donc les données de la section précédente: un opérateur différentiel linéaire L et un vecteur

$$\boldsymbol{Y} = \begin{bmatrix} 1 \\ \mathscr{y} \\ \vdots \\ \mathscr{y}^{n-1} \end{bmatrix}$$

solution de $L\boldsymbol{Y} = 0$.

Le théorème d'Eisenstein [8] montre que $\mathscr{y}$ est une G-fonction et que

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v^K \log^+ \frac{1}{R_v} < +\infty.$$

L'indépendance linéaire sur $k(X)$ des composantes du vecteur $\boldsymbol{Y}$ elle, provient évidemment de l'irréductibilité de P dans $k(X)[Y]$. Reste donc, pour vérifier les hypothèses du théorème principal, à montrer que L est un G-opérateur différentiel. En gros, cela résulte également du théorème d'Eisenstein; ce dernier point mérite cependant quelques détails.

Il s'agit de montrer que, dans la situation présente, le coefficient $s(L)$ est fini. Pour toute place finie v de k, notons $\eta_{1,v}, \ldots, \eta_{n,v}$ les racines dans Ω_v du polynôme $P(t_v, Y)$. Ces racines étant distinctes, la famille

$$\boldsymbol{\eta}_{i,v} = \begin{bmatrix} 1 \\ \eta_{i,v} \\ \vdots \\ \eta_{i,v}^{n-1} \end{bmatrix}, \quad i = 1, 2, \ldots, n$$

constitue une base de Ω_v^n. Soient $R \in k[X]$ le résultant par rapport à Y des polynômes P et P'_Y et $P_n \in k[X]$ le coefficient de Y^n dans P. En utilisant les inégalités suivantes

$$\max_{1\leqslant i\leqslant n} H_v(\eta_{i,v})$$

$$\leqslant \Big[\prod_{i=1}^{n} \max(1, |\eta_{i,v}|_v)\Big]^{n-1} = \left[\frac{H_v(P(t_v, Y))}{|P_n(t_v)|_v}\right]^{n-1} = \left[\frac{H_v(P)}{H_v(P_n)}\right]^{n-1},$$

$$|\det(\eta_{1,v}, \ldots, \eta_{n,v})|_v^2 = |R(t_v)|_v/|P_n(t_v)|_v^{2n-1} = H_v(R)/H_v(P_n)^{2n-1}$$

on montre facilement que

$$s(L) = \overline{\lim_{m\to+\infty}} \frac{1}{m}\left[\frac{1}{[k:Q]} \sum_{v\in M_k^0} d_v^k \max_{1\leqslant i\leqslant n} h_v\big((y_{t_v,h}(\eta_{i,v}))_{h<m}\big)\right].$$

Or

$$y_{t_v}(\eta_{i,v}) = \begin{bmatrix} 1 \\ y_{t_v,i} \\ \vdots \\ y_{t_v,i}^{n-1} \end{bmatrix}$$

où $y_{t_v,i} \in \Omega_v[[X]]$ désigne la série formelle solution de $P_{t_v}(X, y_{t_v,i}) = 0$ et de premier terme $\eta_{i,v}$.

La proposition suivante, variante effective du théorème d'Eisenstein, permet de majorer la v-hauteur des coefficients de $y_{t_v,i}$.

PROPOSITION. *Soient (F, v) un corps valué ultramétrique, $\psi \in F[X, Y]$ un polynôme vérifiant*

$$\psi(0, 0) = 0 \quad \text{et} \quad \psi'_Y(0, 0) \neq 0$$

et $\tilde{y} = \sum_{m\geqslant 1} y_m X^m$ une série formelle à coefficients dans F, solution de $\psi(X, \tilde{y}) = 0$. Alors, pour tout entier $m \geqslant 1$, on a

$$|y_m|_v \leqslant \left[\frac{H_v(\psi)}{\psi'_Y(0, 0)|_v}\right]^{2m-1}.$$

La démonstration se fait par récurrence sur l'entier m, en utilisant l'expression donnant y_{m+1} en fonction des premiers termes $y_1, \ldots, y_m$, qu'on obtient à partir de l'équation fonctionnelle $\psi(X, \tilde{y}) = 0$. ∎

On déduit de cette proposition que pour tout entier $m > 0$

$$\Big[\max_{1\leqslant i\leqslant n} H_v\big((y_{t_v,h}(\eta_{i,v}))_{0<h<m}\big)\Big]^{1/m}$$

$$\leqslant \left[\max_{1\leqslant i\leqslant n} \frac{H_v(P_{t_v,\eta_{i,v}})}{|P'_Y(t_v, \eta_{i,v})|_v}\right]^{2(n-1)} \leqslant \left[\prod_{i=1}^{n} \frac{H_v(P_{t_v,\eta_{i,v}})}{|P'_Y(t_v, \eta_{i,v})|_v}\right]^{2(n-1)}$$

cette dernière majoration étant destinée à faire disparaître les $\eta_{i,v}$ au dénominateur. On obtient en effet:

$$\Big[\max_{1\leqslant i\leqslant n} H_v\big((y_{t_v,h}(\eta_{i,v}))_{0<h<m}\big)\Big]^{1/m} \leqslant \left[\frac{\big(\prod_{i=1}^{n} H_v(P_{t_v,\eta_{i,v}})\big)\,|P_n(t_v)|_v^{n-1}}{|R(t_v)|_v}\right]^{2(n-1)}.$$

Moyennant quelques dernières majorations faciles, on aboutit à

$$\Big[\max_{1\leqslant i\leqslant n} H_v\big((y_{t_v,h}(\eta_{i,v}))_{0<h<m}\big)\Big]^{1/m} \leqslant \left[\frac{H_v(P)^{2n}}{H_v(P_n)\,H_v(R)}\right]^{2(n-1)}$$

et donc à

$$s(L) \leqslant 2(n-1)\big[2nh(P)-h(P_n)-h(R)+\log\big((2n-1)!\,(1+\deg_x P)^{2n-2}\,n^n\big)\big].$$

Le théorème principal s'applique donc à la situation envisagée dans ce paragraphe. Nous allons en déduire le résultat suivant sur la décomposition dans $k[Y]$ des polynômes spécialisés $P(\xi, Y)$ où ξ est un élément de k.

THÉORÈME 2. *Soient k un corps de nombres et P un polynôme irréductible dans $k(X)[Y]$ possédant une racine $\mathscr{Y}$ dans $\overline{\boldsymbol{Q}}((X))$. On note K le corps engendré par k et les coefficients de $\mathscr{Y}$ et pour toute place v de K, R_v le rayon de convergence v-adique de $\mathscr{Y}$ et Y_v la fonction naturellement induite par $\mathscr{Y}$ sur la boule ouverte épointée $B^*(0, R_v) = \{x\in K_v:\ 0<|x|_v<R_v\}$ de K_v. Soient ξ un élément non nul de k, Q un polynôme divisant $P(\xi, Y)$ dans $k[Y]$ et $S(\xi, Q)$ l'ensemble des places v de K vérifiant:*

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

On a alors:

$$(3)\qquad \left|\frac{1}{[K:\boldsymbol{Q}]}\sum_{v\in S(\xi,Q)} d_v^K \log\min(1, |\xi|_v) + \frac{\deg Q}{\deg_Y P}\,h(\xi)\right| \leqslant C_3 + C_4\sqrt{h(\xi)}$$

où C_3 et C_4 sont deux constantes ne dépendant que de P et de $\mathscr{Y}$.

Remarques. 1. Les constantes C_3 et C_4 qui se déduisent des constantes C_1 et C_2 du théorème principal (cf. paragraphe suivant), sont effectives. Notons aussi que quitte à les grossir un peu, on peut leur demander de ne dépendre que de P.

2. Le théorème 2 généralise les travaux antérieurs sur les valeurs de fonctions algébriques [17], [18], [3], [21]–[24]. Dans l'énoncé principal de [24], le plus récent et le plus général d'entre eux, on suppose que P vérifie

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

ce qui impose $\mathscr{Y}\in\overline{\boldsymbol{Q}}[[X]]$, $K = k$ et P absolument irréductible. D'autre part —et c'est plus important (cf. § 2.4, Rem. 2)—, dans notre énoncé, contrairement à celui de Sprindžuk, les constantes C_3 et C_4 ne dépendent pas du corps k.

2.2. Démonstration du théorème 2. Tout d'abord, il est clair que l'on peut supposer que $\mathscr{Y} \in \overline{Q}[[X]]$. Considérons alors ξ un élément non nul de k et Q un diviseur dans $k[Y]$ du polynôme $P(\xi, Y)$. On suppose dans un premier temps que Q est irréductible dans $k[Y]$. Soit $v \in S(\xi, Q)$; le corps $k(Y_v(\xi))$ est alors un k-espace vectoriel de dimension $\deg Q$; il existe donc, entre les nombres $1, Y_v(\xi), \ldots, Y_v(\xi)^{n-1}$, $n - \deg Q$ relations k-linéaires, linéairement indépendantes sur k

$$\sum_{j=1}^{n} \lambda_{ij} Y_v(\xi)^{j-1} = 0, \quad i = 1, 2, \ldots, n - \deg Q.$$

En outre, on peut choisir ces relations indépendantes de $v \in S(\xi, Q)$ puisque les nombres $Y_v(\xi)$ où $v \in S(\xi, Q)$ sont conjugués sur k. On applique alors le théorème principal au point ξ et à la matrice $\Lambda = (\lambda_{ij})_{\substack{1 \leqslant i \leqslant n - \deg Q \\ 1 \leqslant j \leqslant n}}$, ce qui donne

$$\frac{1}{[K:Q]} \sum_{v \in S(\xi, Q)} d_v^K \log \min(1, |\xi|_v) + \frac{\deg Q}{n} h(\xi) \geqslant -C_1 - C_2 \sqrt{h(\xi)}.$$

Nous avons établi cette inégalité sous l'hypothèse Q irréductible dans $k[Y]$; pour le cas général, on remarque simplement que si Q_1 et Q_2 sont deux polynômes divisant $P(\xi, Y)$ dans $k[Y]$, premiers entre eux dans $k[Y]$, alors l'ensemble $S(\xi, Q_1 Q_2)$ est la réunion disjointe des deux ensembles $S(\xi, Q_1)$ et $S(\xi, Q_2)$.

Pour terminer la démonstration, il reste à majorer l'expression

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

on déduit cette majoration de la minoration établie plus haut en utilisant le fait suivant.

Si ξ est un point ordinaire et si $P(\xi, Y) = QT$ avec Q, $T \in k[Y]$ alors

$$|\varphi(\xi, Q) + \varphi(\xi, T)| = |\varphi(\xi, P(\xi, Y))| \leqslant \frac{1}{[K:Q]} \sum_{v \in M_K} d_v^K \log^+ \frac{1}{R_v}.$$

Ceci achève la démonstration du théorème 2. Les constantes C_3 et C_4 peuvent être choisies égales à

$$C_4 = nC_2 \quad \text{et} \quad C_3 = nC_1 + \frac{1}{[K:Q]} \sum_{v \in M_K} d_v^K \log^+ \frac{1}{R_v}.$$

2.3. Premiers corollaires. Rappelons que, pour tout ξ dans k, $M_K(\xi)$ désigne l'ensemble des places v de K telles que $|\xi|_v < 1$. Nous avons déjà remarqué (cf. § 1.4) que le théorème principal conduit à un résultat particulièrement simple quand l'ensemble $M_K(\xi)$ ne possède qu'un seul élément v_0, à savoir l'indépendance linéaire sur k des nombres $Y_{1,v_0}(\xi), \ldots, Y_{n,v_0}(\xi)$, dès que $h(\xi)$ est assez grand. Dans le cas présent,

c'est-à-dire $\mathscr{Y}_i = \mathscr{Y}^{i-1}$ pour $i = 1, 2, \ldots, n$ avec $\mathscr{Y}$ racine dans $\overline{Q}((X))$ du polynôme P, ce résultat signifie que, si card $M_K(\xi) = 1$, le polynôme $P(\xi, Y)$ est irréductible dans $k[Y]$ dès que ξ est de hauteur assez grande. Le corollaire suivant généralise ce résultat; il met en évidence un lien entre la structure arithmétique d'un élément ξ de k – sa décomposition dans l'anneau des entiers de K – et celle du polynôme $P(\xi, Y)$ – sa décomposition en irréductibles de l'anneau $k[Y]$. Les hypothèses sont celles du théorème 2.

COROLLAIRE 1. *Soient ξ un élément non nul de k et $P(\xi, Y) = uQ_1^{\alpha_1} \ldots Q_r^{\alpha_r}$ la décomposition du polynôme $P(\xi, Y)$ en polynômes irréductibles distincts Q_i $(1 \leqslant i \leqslant r)$, de l'anneau $k[Y]$. Si $h(\xi) > h_0$ où h_0 est une constante ne dépendant que de P et de $\mathscr{Y}$, alors*

$$r \leqslant \text{card } M_K(\xi).$$

En effet, on déduit facilement du théorème 2 que, dès que

$$\frac{1}{n} h(\xi) - C_4 \sqrt{h(\xi)} - C_3 > 0,$$

si Q est un polynôme divisant $P(\xi, Y)$ dans $k[Y]$ tel que $\deg Q \geqslant 1$, alors on a nécessairement

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

L'application

$$i\colon \begin{cases} \{v \in M_K\colon |\xi|_v < \min(1, R_v)\} \to \{1, 2, \ldots, r\}, \\ \qquad\qquad\qquad\qquad v \mapsto i(v) \end{cases}$$

où $i(v)$ est défini par $Q_{i(v)}(Y_v(\xi)) = 0$, est donc surjective. L'inégalité demandée en résulte.

Prenons maintenant $\xi = p^m$ avec p un nombre premier et $m \geqslant 1$ un entier. Si $K = Q$, on a $M_K(p^m) = \{p\}$ et le corollaire 1 montre alors que le polynôme $P(p^m, Y)$ est irréductible dans $Q[Y]$ dès que p^m est assez grand (cf. [21]). Par contre, si $K \supsetneq Q$, les choses ne sont pas si simples: si par exemple le nombre premier p se décompose dans le corps K, alors card $M_K(p^m) \geqslant 2$ et on ne peut plus conclure, au moyen du corollaire 1, à l'irréductibilité du polynôme $P(p^m, Y)$. Ceci étant, on peut tout de même préciser la décomposition du polynôme $P(p^m, Y)$, grâce au corollaire suivant.

COROLLAIRE 2. *Les hypothèses étant celles du théorème 2, soient p un nombre premier et m un entier. Si p^m (resp. $|m|$) est suffisamment grand (précisément, supérieur à une constante c ne dépendant que de P), alors pour tout polynôme Q divisant $P(p^m, Y)$ (resp. $P(1/m, Y)$) dans $k[Y]$, et tel que* $\deg Q \geqslant 1$, *on a*

(a) $\deg Q \geqslant \dfrac{\min\limits_{v|p} d_v^K}{[K:Q]} \deg_Y P$ (*resp.* $\deg Q \geqslant \dfrac{\min\limits_{v|\infty} d_v^K}{[K:Q]} \deg_Y P$),

(b) $\dfrac{\deg_Y P}{(\deg_Y P, [K:Q])}$ *divise* $\deg Q$,

où $(\deg_Y P, [K:Q])$ *désigne le plus grand des diviseurs communs à* $\deg_Y P$ *et à* $[K:Q]$.

Remarque 1. En particulier, le corollaire 2 donne l'irréductibilité du polynôme $P(p^m, Y)$ (resp. $P(1/m, Y)$) pour p^m assez grand (resp. $|m|$ assez grand) dans les cas suivants:

1. Le nombre premier p ne sc décompose pas dans le corps K (resp. le corps K est inclus dans un corps quadratique imaginaire).

2. Les nombres $\deg_Y P$ et $[K:Q]$ sont premiers entre eux.

D'autre part, si $[K:Q] < \deg_Y P$, on peut conclure que l'équation

$$P(p^m, y) = 0 \quad \text{(resp. } P(1/m, y) = 0\text{)}$$

n'a qu'un nombre fini de solutions en p premier, m entier et $y \in k$ (resp. en m entier et $y \in k$).

Démonstration du corollaire 2. Désignons par ξ soit le nombre p^m, soit le nombre $1/m$ et supposons que l'on ait:

$$\sqrt{h(\xi)} > \gamma \quad \text{(c'est-à-dire } p^m \geqslant \exp(\gamma^2) \text{ ou } |m| \geqslant \exp(\gamma^2) \text{ selon le cas)}$$

où γ désigne la racine positive du trinôme:

$$\frac{1}{\deg_Y P [K:Q]} X^2 - C_4 X - C_3.$$

Soit Q un polynôme de degré non nul divisant le polynôme $P(\xi, Y)$ dans $k[Y]$. L'ensemble $S(\xi, Q) \cap M_K(\xi)$ n'étant constitué que de places v de K au-dessus de p ou au dessus de ∞ (selon que $\xi = p^m$ ou $\xi = 1/m$), le théorème 2 donne

$$\left| \frac{1}{[K:Q]} \sum_{v \in S(\xi, Q)} d_v^K - \frac{\deg Q}{\deg_Y P} \right| h(\xi) \leqslant C_4 \sqrt{h(\xi)} + C_3$$

ce qui, joint à $\sqrt{h(\xi)} > \gamma$ impose

$$\deg_Y P \Big(\sum_{v \in S(\xi, Q)} d_v^K \Big) = \deg Q \cdot [K:Q].$$

On en déduit facilement les minorations annoncées de $\deg Q$. ∎

Corollaire 3. *Soient* $s \geqslant 0$ *un entier et* $P = P_s X^s + \ldots + P_0$, *où* $P_i \in Q[Y]$ *pour* $i = 0, 1, 2, \ldots, s$, *un polynôme irréductible dans* $Q[X, Y]$. *On*

suppose que P_s possède une racine simple η_0 dans $\overline{Q}$ et que $r = [Q(\eta_0): Q]$ le degré sur Q de cette racine vérifie

$$r < \deg_Y P.$$

Alors l'équation $P(x, y) = 0$ n'a qu'un nombre fini de solutions en nombres entiers x, y; si (x, y) est l'une d'elles alors $|x| \leqslant x_0$ où x_0 est une constante effective ne dépendant que de P.

Démonstration. Considérons le polynôme

$$\hat{P} = X^s P(X^{-1}, Y) = P_0 X^s + \ldots + P_s.$$

On vérifie facilement que $\hat{P}$ est un polynôme irréductible dans $Q[X, Y]$. D'autre part, le polynôme $\hat{P}(0, Y) = P_s$ admet une racine simple dans $\overline{Q}$, à savoir η_0. Il existe donc, d'après un lemme classique (voir par exemple [9], Ch. III, § 1.1), une série formelle $\mathscr{Y}$ de premier terme η_0, à coefficients dans $K = Q(\eta_0)$ vérifiant $\hat{P}(X, \mathscr{Y}) = 0$.

Le corollaire 2 s'applique donc. Soit $\hat{c}$ la constante du corollaire 2 associée au polynôme $\hat{P}$. L'inégalité (a) (cas archimédien) montre alors que si $|m| > \hat{c}$, et si Q est un polynôme de degré non nul divisant $\hat{P}(1/m, Y)$ dans $Q[Y]$, on a

$$\deg Q \geqslant \frac{\deg_Y P}{r} > 1.$$

Autrement dit, le polynôme $\hat{P}(1/m, Y)$ n'admet aucune racine dans Q si $|m| > \hat{c}$. Ceci fournit le résultat désiré puisque

$$\hat{P}(1/m, Y) = \frac{1}{m^s} P(m, Y).$$

Remarque 2. Le corollaire 3 reste valable si l'on suppose, au lieu de $r < \deg_Y P$, que η_0 est un nombre quadratique imaginaire. En effet, sous cette hypothèse, le corollaire 2 conduit à

$$\deg Q \geqslant \deg_Y P \geqslant 2.$$

2.4. Approche algébrique du théorème 2. Nous avons établi le théorème 2 comme conséquence du théorème principal. Depuis le travail de Bombieri sur le théorème de décomposition de Weil ([2], voir aussi [7]), on peut en donner une seconde démonstration, de nature algébrique, basée sur la théorie des hauteurs sur les courbes algébriques [14]. Le résultat apparaît alors comme une conséquence de la quadraticité de la hauteur sur les variétés abéliennes, ce qui explique en particulier l'estimation du reste en $O(\sqrt{h})$ dans le théorème 2. En termes de fonctions de Weil ([14], Ch. 10), on peut énoncer le résultat de Bombieri de la façon suivante.

Soit $C \subset \boldsymbol{P}^N$ une courbe projective irréductible lisse définie sur un corps de nombres k. Si $Q \in C(k)$ est un point k-rationnel sur C, nous noterons

$$\lambda_Q\colon\ C(k) \times M_k \to \boldsymbol{R}$$

la fonction de Weil associée au diviseur Q. (Précisément, λ_Q désigne un représentant fixé de la classe, modulo les fonctions M_k-bornées sur C [14], Ch. 10, § 1), des fonctions de Weil associées au diviseur Q.)

THÉORÈME 3. *Soient φ une fonction rationnelle sur C définie sur le corps de nombres k et $Q \in C(k)$ un pôle de φ. Alors il existe une M_k-constante $(\delta_v)_{v \in M_k}$, c'est-à-dire une famille de nombres réels δ_v, indexée par les places v de k, vérifiant $\delta_v = 0$ pour tout $v \in M_k$ sauf un nombre fini, telle que pour tout point $M \neq Q$ dans $C(k)$, on ait*

(4) *S'il existe $v \in M_k$ tel que $\lambda_Q(M, v) > \delta_v$, alors M n'est pas un pôle de φ.*

$$(5)\quad \frac{1}{[k:\boldsymbol{Q}]} \sum_{\substack{v \in M_k \\ \lambda_Q(M,v) > \delta_v}} d_v^k \log^+ |\varphi(M)|_v = -\frac{\operatorname{ord}_Q \varphi}{\deg \varphi} h(\varphi(M)) + O\left(\sqrt{h(\varphi(M))}\right)$$

où les constantes intervenant dans le $O(\ldots)$ ne dépendant que du plongement $C \subset \boldsymbol{P}^N$ et de la fonction φ.

Remarques. 1. En prenant pour C un modèle projectif lisse de la courbe algébrique plane définie par $P(x, y) = 0$ et φ égal à la fonction rationnelle $\varphi = 1/x$, on obtient le théorème 2. Inversement, on peut déduire le théorème 3 du théorème 2: il suffit pour cela d'appliquer le théorème 2 au polynôme $P \in \overline{\boldsymbol{Q}}(\varphi)[Y]$ ($\simeq \overline{\boldsymbol{Q}}(X)[Y]$), le polynôme minimal d'un élément primitif sur le corps $\overline{\boldsymbol{Q}}(\varphi)$ du corps $\overline{\boldsymbol{Q}}(C)$ des fonctions rationnelles sur C définies sur $\overline{\boldsymbol{Q}}$. Pour les détails, nous renvoyons à [6].

2. Dans le théorème 3, comme dans le théorème 2, les constantes ne dépendent pas du corps k. C'est une remarque importante: en effet, dans le cas contraire, à cause du résultat de Faltings [10], le théorème 3 n'aurait d'intérêt que pour les courbes de genre $g < 2$.

On peut rappeler brièvement le principe de la démonstration du théorème 3. En utilisant des propriétés standard des fonctions de Weil, notamment le théorème de décomposition de Weil ([14], Ch. 10, Th. 3.7), on montre que, pour un choix convenable de la M_k-constante $(\delta_v)_{v \in M_k}$, si Q est un pôle de φ et M un point dans $C(k)$ tels que $\lambda_Q(M, v) > \delta_v$

$$\log |\varphi(M)|_v = -\operatorname{ord}_Q \varphi \cdot \lambda_Q(M, v) + O_v(1)$$

où $O_v(1)$ est une fonction de M, bornée sur C et nulle pour tout $v \in M_k$ sauf un nombre fini. On en déduit que

$$(6)\quad \frac{1}{[k:\boldsymbol{Q}]} \sum_{\substack{v \in M_k \\ \lambda_Q(M,v) > \delta_v}} d_v^k \log^+ |\varphi(M)|_v = -\operatorname{ord}_Q \varphi \cdot h_Q(M) + O(1),$$

h_Q désignant la hauteur associée à la classe du diviseur Q dans le groupe de Picard de C.

On utilise ensuite le théorème de Néron sur la quadraticité de la hauteur sur les variétés abéliennes ([14], Ch. 5, § 3). Une conséquence de ce théorème est que, pour tous points Q, Q' dans $C(\overline{Q})$, on a ([14], Ch. 5, § 5):

$$h_{Q'} = h_Q + O(\sqrt{h_Q}).$$

Ce résultat, joint à

$$\sum_{Q \text{ pôle de } \varphi} \operatorname{ord}_Q \varphi = -\deg \varphi$$

permet de conclure.

Le corollaire suivant améliore légèrement le théorème p. 305 de [2]; il contient également les propositions 4.4 et 4.5 de [12].

COROLLAIRE. *Soit φ une fonction rationnelle sur C définie sur k. Soit μ le nombre de pôles de φ non conjugués sur k. Alors il n'y a qu'un nombre fini de points M dans $C(k)$ tels que*

$$\operatorname{card} M_k\big(1/\varphi(M)\big) < \mu.$$

Remarque 3. Le résultat du corollaire est effectif: la démonstration donne une majoration indépendante de k, de $h(\varphi(M))$ pour M dans $C(k)$ vérifiant $\operatorname{card} M_k\big(1/\varphi(M)\big) < \mu$.

Démonstration du corollaire. Soient $Q_1, \ldots, Q_\mu$ μ pôles de φ non conjugués sur k. Soient K la clôture normale sur k de $k(Q_1, \ldots, Q_\mu)$ le corps de définition de $Q_1, \ldots, Q_\mu$ et G son groupe de Galois. Notons alors, pour M dans $C(k)$, $i = 1, 2, \ldots, \mu$ et $\sigma \in G$, $S_{i,\sigma}(M)$ l'ensemble des places w de K telles que $\lambda_{Q_i^\sigma}(M, w) > \delta_w$, $(\delta_w)_{w \in M_K}$ désignant la M_K-constante du théorème 3. On a donc

$$(7) \quad \frac{1}{[K:Q]} \sum_{w \in S_{i,\sigma}(M)} d_w^K \log^+ |\varphi(M)|_w = -\frac{\operatorname{ord}_{Q_i} \varphi}{\deg \varphi} h\big(\varphi(M)\big) + O\Big(\sqrt{h\big(\varphi(M)\big)}\Big)$$

pour $i = 1, 2, \ldots, \mu$ et $\sigma \in G$.

Notons pour $i = 1, 2, \ldots, \mu$, $S_i(M)$ l'ensemble $S_i(M) = \bigcup_{\sigma \in G} S_{i,\sigma}(M)$. Comme $\lambda_{Q_i^\sigma}(M, w^\sigma) = \lambda_{Q_i}(M, w)$ pour tout $\sigma \in G$, le groupe G opère sur $S_i(M)$ pour $i = 1, 2, \ldots, \mu$; si l'on note $S_i^k(M)$ l'ensemble des places v de k se prolongeant dans $S_i(M)$, on a donc pour $i = 1, 2, \ldots, \mu$

$$(8) \quad \frac{1}{[K:Q]} \sum_{w \in S_i(M)} d_w^K \log^+ |\varphi(M)|_w = \frac{1}{[k:Q]} \sum_{v \in S_i^k(M)} d_v^k \log^+ |\varphi(M)|_v.$$

D'autre part, on peut supposer δ_w assez grand pour que les ensembles $S_{i,\sigma}(M)$ où $i = 1, 2, \ldots, \mu$ et σ décrit un ensemble de représentants des éléments de G modulo le groupe de Galois de l'extension $K/k(Q_i)$, soient

disjoints (cf. [14], Ch. 10, Cor. 3.3). (7), (8) et la définition de $S_i(M)$ donnent donc, pour $i = 1, 2, \ldots, \mu$

$$(9) \quad \frac{1}{[k:Q]} \sum_{v \in S_i^k(M)} d_v^k \log^+ |\varphi(M)|_v = -\frac{[k(Q_i):k] \operatorname{ord}_{Q_i} \varphi}{\deg \varphi} h(\varphi(M)) + Q\left(\sqrt{h(\varphi(M))}\right).$$

Considérons maintenant un point M dans $C(k)$ vérifiant $\operatorname{card} M_k(1/\varphi(M)) < \mu$. Les ensembles $S_i^k(M)$, $i = 1, 2, \ldots, \mu$ étant disjoints, il existe nécessairement un indice i tel que

$$\frac{1}{[k:Q]} \sum_{v \in S_i^k(M)} d_v^k \log^+ |\varphi(M)|_v = 0.$$

On déduit alors de (9)

$$h(\varphi(M)) = O\left(\sqrt{h(\varphi(M))}\right). \quad \blacksquare$$

Le théorème 3 reste valable si k est plus généralement une extension finie d'un corps muni d'un ensemble propre de valeurs absolues ([14], Ch. 2) satisfaisant la formule du produit (cf. [14], Ch. 5 et Ch. 10). Via le théorème 4.2 de [12] on peut alors déduire du corollaire que tout corps muni d'une formule du produit est un corps hilbertien, résultat dû à R. Weissauer (voir [12]).

Dans [12], M. Fried avait montré qu'on pouvait relier les travaux de R. Weissauer et ceux de V. G. Sprindžuk. Ce lien est donc concrétisé ici par le théorème 3 qui généralise simultanément leurs résultats.

3. Théorème d'irreductibilité de Hilbert. Soient k un corps de nombres et P un polynôme irréductible dans $k(X)[Y]$; le théorème d'irréductibilité de Hilbert (1892) [13] montre que l'ensemble $H_{P,k}$ constitué des éléments x de k tels que le polynôme $P(x, Y)$ soit irréductible dans $k[Y]$, est un ensemble infini.

A. Schinzel en 1965 [15] et un peu plus tard M. Fried [11], ont montré que l'ensemble $H_{P,k}$ contenait une progression arithmétique $(am+b)_{m \geq 0}$; il contient donc également une progression géométrique $((b(a+1)^m)_{m \geq 0})$. Dans cette section, on démontre une nouvelle version du théorème d'irréductibilité de Hilbert, qui précise ce dernier résultat.

3.1. Le résultat-clé. Dans ce paragraphe, les notations et les hypothèses sont celles du théorème 2. La proposition suivante, que nous allons déduire du théorème 2, est le résultat-clé de cette section.

PROPOSITION 1. *Soient ξ un élément non nul de k, $m \geq 0$ un entier et Q un polynôme divisant le polynôme $P(\xi^m, Y)$ dans $k[Y]$. Alors si m est*

suffisamment grand (supérieur à un entier m_0 ne dépendant que de P, k et ξ), il existe une partie $S(Q)$ de l'ensemble $M_K(\xi)$ telle que:

$$(1) \qquad \frac{1}{[K:Q]} \sum_{v \in S(Q)} d_v^K \log|\xi|_v + \frac{\deg Q}{\deg_Y P} h(\xi) = 0.$$

Démonstration. Considérons la suite $(u_m)_{m \geqslant 0}$ définie par

$$u_m = \max_{Q \in D_m} \left| \frac{1}{[K:Q]} \sum_{v \in S(Q)} d_v^K \log|\xi|_v + \frac{\deg Q}{\deg_Y P} h(\xi) \right|$$

où $S(Q) = S(\xi^m, Q) \cap M_K(\xi)$ et D_m désigne l'ensemble des diviseurs Q dans $k[Y]$ du polynôme $P(\xi^m, Y)$. En utilisant le fait que $h(\xi^m) = mh(\xi)$, on déduit du théorème 2 que pour tout entier $m > 0$

$$(2) \qquad 0 \leqslant u_m \leqslant \frac{C_3}{m} + \frac{C_4 \sqrt{h(\xi)}}{\sqrt{m}}.$$

D'autre part, pour tout $m \geqslant 0$ et pour tout polynôme dans D_m, on a

$$S(Q) \subset M_K(\xi) \quad \text{et} \quad 0 \leqslant \deg Q \leqslant \deg_Y P,$$

ξ, P, et k étant fixés, la suite $(u_m)_{m \geqslant 0}$ prend donc un nombre fini de valeurs. Comme, d'après (2), elle tend vers 0, elle est nulle à partir d'un certain rang m_0. ∎

Corollaire. *Supposons de plus que le nombre ξ vérifie la propriété suivante: il existe une place v_0 dans $M_K(\xi)$ telle qu'aucune puissance non nulle de $|\xi|_{v_0}$ n'appartienne au groupe multiplicatif engendré par les $|\xi|_v$ où $v \in M_K(\xi) \backslash \{v_0\}$ (c'est-à-dire $|\xi|_{v_0}^{\mathbf{Z}} \cap \prod_{\substack{v \in M_K(\xi) \\ v \neq v_0}} |\xi|_v^{\mathbf{Z}} = \{1\}$).*

Alors, pour $m \geqslant m_0$, le polynôme $P(\xi^m, Y)$ est irréductible dans $k[Y]$.

En effet, soient m un entier supérieur à m_0 et Q un diviseur dans $k[Y]$ du polynôme $P(\xi^m, Y)$. Comme

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

on peut écrire la relation (1)

$$(3) \qquad (\deg_Y P - \deg Q) \sum_{v \in S(Q)} d_v^K \log|\xi|_v - (\deg Q) \sum_{v \in M_K(\xi) \backslash S(Q)} d_v^K \log|\xi|_v = 0.$$

Or l'hypothèse faite sur ξ signifie que $\log|\xi|_{v_0}$ n'appartient pas au $\mathbf{Q}$-espace vectoriel engendré par les $\log|\xi|_v$ où v décrit $M_K(\xi)\backslash\{v_0\}$. De (3), on déduit donc que, soit $\deg Q = \deg_Y P$ (si $v_0 \in S(Q)$), soit $\deg Q = 0$ (si $v_0 \in M_K(\xi) \backslash S(Q)$). ∎

Remarque. Le corollaire s'applique en particulier dans les cas suivants

(a) La famille des nombres $|\xi|_v$ où v décrit $M_K(\xi)$ est non vide et multiplicativement libre (cas traité dans [24]).

(b) $k = \boldsymbol{Q}$ et il existe un nombre premier p qui ne se décompose pas dans le corps K et tel que $|\xi|_p < 1$ (v_0 est dans ce cas l'unique place de K au-dessus de p).

(c) $k = \boldsymbol{Q}$, K est inclus dans un corps quadratique imaginaire et $|\xi| < 1$ (v_0 est ici l'unique place archimédienne du corps K).

(d) $k = K = \boldsymbol{Q}$ et $\xi \neq 0, 1, -1$ (cas traité dans [22]); c'est une conséquence des cas (b) et (c).

Ceci étant, on peut donner des exemples où aucun élément ξ du corps k ne vérifie l'hypothèse du corollaire, et même où la relation (1) possède une autre solution que $\deg Q = 0$ et $\deg Q = \deg_Y P$. (Prendre $P = M(Y) - X$ où M est le polynôme minimal sur $\boldsymbol{Q}$ d'un élément primitif du corps $K = \boldsymbol{Q}(\sqrt{13}, \sqrt{17})$ (cf. [6], Ch. VI, § 1).)

Nous allons voir maintenant comment contourner cette difficulté et démontrer le résultat escompté, à savoir l'existence, si P possède une racine dans $\overline{\boldsymbol{Q}}((X))$, d'un nombre ξ dans k tel que le polynôme $P(\xi^m, Y)$ soit irréductible dans $k[Y]$ pour m assez grand.

3.2. Enoncé du théorème 4. Notre objectif est d'établir le résultat suivant.

THÉORÈME 4. *Soient k un corps de nombres et $P_1, P_2, \ldots, P_N$ N polynômes irréductibles dans $k(X)[Y]$. Pour $i = 1, 2, \ldots, N$, on note $H_{P_i,k}$ l'ensemble des éléments x de k tels que $P_i(x, Y)$ soit irréductible dans $k[Y]$. Alors, pour toute partie finie S de M_k, l'ensemble $\bigcap_{i=1}^{N} H_{P_i,k}$ contient une progression géométrique $(ab^m)_{m\geq 1}$ dont la raison b vérifie*

$$|b|_v < 1 \quad \textit{pour tout } v \textit{ dans } S.$$

De plus, si les polynômes $P_1, P_2, \ldots, P_N$ possèdent une racine dans $\overline{\boldsymbol{Q}}((X))$, on peut prendre $a = 1$.

Remarque. Pour ce dernier point, il est clair que l'hypothèse "$P_1, \ldots, P_N$ possèdent une racine dans $\overline{\boldsymbol{Q}}((X))$" n'est pas superflue. (Prendre par exemple $P_1 = Y^2 - X$.)

3.3. Démonstration du théorème 4. On suppose dans un premier temps que les polynômes $P_1, \ldots, P_N$ sont totalement décomposés dans $\overline{\boldsymbol{Q}}((X))$, c'est-à-dire que toutes les racines des polynômes $P_1, \ldots, P_N$ sont dans $\overline{\boldsymbol{Q}}((X))$. Il est classique (cf. [14], Ch. 9, Prop. 1.1) qu'on peut associer à chaque polynôme P_i, une famille finie de polynômes $A_{i,j}$, $j = 1, 2, \ldots, l_i$ irréductibles dans $k(X)[Y]$, de degré ≥ 2 et possédant la propriété suivante: sauf pour un nombre fini de $x \in k$, si aucun des polynômes $A_{i,1}(x, Y), \ldots, A_{i,l_i}(x, Y)$ n'a de racines dans k, alors le polynôme $P_i(x, Y)$ est irréductible dans $k[Y]$. De plus, sous l'hypothèse faite sur les polynômes P_i, on peut demander à ces

polynômes $A_{i,j}$ d'avoir une racine dans $\overline{Q}((X))$: les $A_{i,j}$ apparaissent en effet (cf. dem. de la prop. 1.1 du Ch. 9 de [14]) comme les polynômes minimaux de fonctions polynomiales des racines des P_i.

D'autre part, un autre argument classique (cf. [14], Ch. 9, prop. 3.3) permet de se ramener à la situation $k = Q$. Compte tenu de ces remarques, il suffit, pour démontrer le théorème 4 dans le cas considéré, de prouver le théorème 4 bis ci-dessous.

THÉORÈME 4 bis. *Soient $A_1, A_2, \ldots, A_l$ l polynômes irréductibles dans $Q(X)[Y]$, de degré $\geqslant 2$, et possédant une racine dans $\overline{Q}((X))$. Alors pour toute partie finie S de M_Q, il existe un nombre rationnel b tel que*

(a) $|b|_v < 1$ *pour tout v dans S,*

(b) *Pour m suffisamment grand (supérieur à un entier m_1 ne dépendant que de $A_1, \ldots, A_l$ et de S), aucun des polynômes $A_1(b^m, Y), \ldots, A_l(b^m, Y)$ n'a de racines dans Q.*

On va déduire le théorème 4 bis de la proposition suivante.

PROPOSITION 2. *Soit A un polynôme irréductible dans $Q(X)[Y]$, de degré $\geqslant 2$ et possédant une racine $\tilde{y}$ dans $\overline{Q}((X))$. On note K le corps engendré par Q et les coefficients de la série de Laurent $\tilde{y}$. Soit ξ un nombre rationnel non nul. Si l'une des deux hypothèses suivantes est vérifiée*

(a) $[K:Q] < \deg_Y A$ *et* $|\xi| \neq 1$,

(b) $[K:Q] \geqslant 2$ *et il existe un nombre premier p vérifiant* $\min\limits_{\substack{v \in M_K \\ v|p}} d_v^K \geqslant 2$ *et tel que* $|\xi|_p < 1$,

alors, pour m suffisamment grand (supérieur à un entier m_2 ne dépendant que de A et de ξ), le polynôme $A(\xi^m, Y)$ n'a pas de racines dans Q.

Démonstration de la proposition 2. Soient $m \geqslant 0$ un entier et Q un diviseur dans $Q[Y]$ de degré non nul du polynôme $A(\xi^m, Y)$; il s'agit de montrer que pour m assez grand, on a $\deg Q > 1$. D'après la proposition 1 si m est supérieur à un entier m_2, qui ne dépend que de A et de ξ, alors il existe une partie $S(Q)$ de l'ensemble $M_K(\xi)$ telle que

$$\frac{1}{[K:Q]} \sum_{v \in S(Q)} d_v^K \log|\xi|_v + \frac{\deg Q}{\deg_Y A} h(\xi) = 0.$$

Dans le cas présent, ξ est un nombre rationnel; la relation précédente s'écrit donc

$$\sum_{w \in M_Q(\xi)} \left(\frac{1}{[K:Q]} \sum_{\substack{v \in S(Q) \\ v|w}} d_v^K - \frac{\deg Q}{\deg_Y A} \right) \log|\xi|_w = 0.$$

Comme les nombres $\log|\xi|_w$, où w décrit $M_Q(\xi)$, sont Q-linéairement indépendants, on obtient que pour toute place w dans $M_Q(\xi)$ et pour $m \geqslant m_2$

$$\frac{1}{[K:Q]} \sum_{\substack{v \in S(Q) \\ v|w}} d_v^K = \frac{\deg Q}{\deg_Y A}$$

et donc, puisque $\deg Q \neq 0$

$$\deg Q \geqslant \frac{\deg_Y A}{[K:\mathbf{Q}]} \min_{\substack{v \in M_K \\ v|w}} d_v^K.$$

On en déduit facilement le résultat annoncé. (Pour (b), il suffit d'utiliser l'inégalité $[K:\mathbf{Q}] \leqslant \deg_Y A$.)

Pour pouvoir conclure que l'on est toujours dans l'une des deux hypothèses de la proposition 2, on utilise un lemme de Hasse ([16], II. 23, Lemme, p. 192) disant qu'un polynôme dans $\mathbf{Z}[X]$ de degré $\geqslant 2$, admettant une racine modulo p pour tous les nombres premiers p, sauf un nombre fini, est nécessairement réductible dans $\mathbf{Q}[X]$. En termes de corps, cela signifie que dans tout corps de nombres K distinct de $\mathbf{Q}$, il existe une infinité de nombres premiers p tels que $\min_{\substack{v \in M_K \\ v|p}} d_v^K \geqslant 2$.

La démonstration du théorème 4 bis est maintenant claire. D'après ce qui précède, on peut associer à chacun des polynômes A_i, $i = 1, 2, \ldots, l$ un nombre premier p_i vérifiant pour tout nombre rationnel ξ non nul, $|\xi|_{p_i} < 1 \Rightarrow$ Le polynôme $A_i(\xi^m, Y)$ n'a pas de racines dans $\mathbf{Q}$ pour m assez grand.

(Noter que, sous l'hypothèse (a), n'importe quel nombre premier p_i convient.)

Il suffit alors de prendre pour b une puissance assez grande du nombre b_0 défini par

$$b_0 = \left(\prod_{i=1}^{l} p_i\right)\left(\prod_{p \in S} p\right) \qquad \text{si} \quad \infty \notin S,$$

$$b_0 = \frac{1}{p_\infty}\left(\prod_{i=1}^{l} p_i\right)\left(\prod_{\substack{p \in S \\ p \neq \infty}} p\right) \qquad \text{si} \quad \infty \in S$$

où p_∞ est un nombre premier distinct des p_i, $i = 1, \ldots, l$ et des p dans S, et choisi suffisamment grand pour que $b_0 < 1$. Ceci termine la démonstration du théorème 4 dans le cas où les polynômes $P_1, \ldots, P_N$ sont tous totalement décomposés dans $\overline{\mathbf{Q}}((X))$.

Revenons maintenant au cas général. Notons pour $i = 1, 2, \ldots, N$, $f(P_i)$ le plus petit entier f tel que le polynôme $P_i(X^f, Y)$ soit totalement décomposé dans $\overline{\mathbf{Q}}((X))$; l'existence de $f(P_i)$ est assurée par le théorème de Puiseux (cf. [9], Ch. III, § 1.6). On est tenté de se ramener au cas précédent en considérant les polynômes $P_i(X^{f(P_i)}, Y)$, mais il peut arriver que l'un de ces polynômes soit réductible dans $k(X)[Y]$ (Penser à $P_1 = Y^2 - X$.) Pour lever cette difficulté, on utilise la proposition suivante.

PROPOSITION 3. *Soient P un polynôme irréductible dans $k(X)[Y]$ et $f \geqslant 1$ un entier. Soit $P(X^f, Y) = \Pi_1 \ldots \Pi_r$ une décomposition du polynôme $P(X^f, Y)$*

en polynômes irréductibles dans $\overline{Q}(X)[Y]$. *On note* L *le corps engendré par* k *et les coefficients des polynômes* Π_i, $i = 1, 2, \ldots, r$. *Soit enfin* α *un élément non nul de* k *tel que le polynôme* $T^f - \alpha$ *soit irréductible dans* $L[T]$. *Alors, le polynôme* $P(\alpha X^f, Y)$ *est irréductible dans* $k(X)[Y]$.

Démonstration. Soit β un nombre algébrique tel que $\beta^f = \alpha$. Les polynômes $\Pi_1, \ldots, \Pi_r$ étant irréductibles dans $\overline{Q}(X)[Y]$, une décomposition du polynôme $P(\alpha X^f, Y)$ en irréductibles de $\overline{Q}(X)[Y]$ est donnée par

$$P(\alpha X^f, Y) = \Pi_1(\beta X, Y) \times \ldots \times \Pi_r(\beta X, Y).$$

Si $P(\alpha X^f, Y) = QR$ avec Q, R dans $k(X)[Y]$, on a donc nécessairement à un facteur près dans $k(X)$

$$Q = Q_1(\beta X, Y) \quad \text{et} \quad R = R_1(\beta X, Y) \quad \text{avec} \quad Q_1, R_1 \text{ dans } L(X)[Y].$$

Par hypothèse, le polynôme $T^f - \alpha$ est irréductible dans $L[T]$; en particulier, pour j entier, β^j n'appartient à L que si j est dans l'idéal $f\mathbf{Z}$; Q et R étant à coefficients dans $k \subset L$, Q_1 et R_1 sont nécessairement de la forme

$$Q_1 = Q_2(X^f, Y) \quad \text{et} \quad R_1 = R_2(X^f, Y) \quad \text{avec } Q_2, R_2 \text{ dans } L(X)[Y].$$

On a donc

$$Q = Q_2(\alpha X^f, Y), \quad R = R_2(\alpha X^f, Y). \tag{4}$$

De $P(\alpha X^f, Y) = QR$, on déduit maintenant que $P = Q_2 R_2$; or d'après (4), les polynômes Q_2 et R_2 appartiennent à $k(X)[Y]$. L'irréductibilité de P dans $k(X)[Y]$ impose que, ou bien Q_2 ou bien R_2, et donc, ou bien Q ou bien R soit de degré nul. ∎

Ce résultat étant acquis, terminons la démonstration du théorème 4. On écrit pour $i = 1, 2, \ldots, N$, $P_i(X^{f(P_i)}, Y) = \Pi_{i,1} \times \ldots \times \Pi_{i,r_i}$ une décomposition du polynôme $P(X^{f(P_i)}, Y)$ en polynômes irréductibles dans $\overline{Q}(X)[Y]$. Notons L_i le corps engendré par k et les coefficients des polynômes $\Pi_{i,j}$, $j = 1, 2, \ldots, r_i$ et $L = L_1 \ldots L_N$ le corps engendré par les L_i, $i = 1, 2, \ldots, N$.

On choisit ensuite α un élément non nul du corps k tel que pour $i = 1, 2, \ldots, N$, le polynôme $T^{f(P_i)} - \alpha$ soit irréductible dans $L[T]$: on peut prendre par exemple pour α un nombre premier impair qui ne divise pas le discriminant du corps de nombres L; l'irréductibilité dans $L[T]$ des polynômes $T^{f(P_i)} - \alpha$ résulte alors du théorème de Capelli ([16], I. 13, Th. 21).

On considère alors les polynômes $P_{i,\alpha}$, définis par

$$P_{i,\alpha} = P_i(\alpha X^{f(P_i)}, Y) \quad \text{pour} \quad i = 1, 2, \ldots, N.$$

Ces polynômes sont, comme les polynômes $P(X^{f(P_i)}, Y)$, totalement décomposés dans $\overline{Q}((X))$; mais d'après la proposition 3, eux sont irréductibles dans $k(X)[Y]$.

D'après le premier cas, l'ensemble $\bigcap_{i=1}^{N} H_{P_i,\alpha,k}$ contient une progression géométrique $(\beta^m)_{m\geqslant 1}$ avec β dans k vérifiant $|\beta|_v < 1$ pour tout v dans S. Posons $a = \alpha$ et $b = \beta^f$ où f est le p.p.c.m. des nombres $f(P_1), \ldots, f(P_N)$; alors il est clair que la progression géométrique $(ab^m)_{m\geqslant 1}$ satisfait la conclusion du théorème 4.

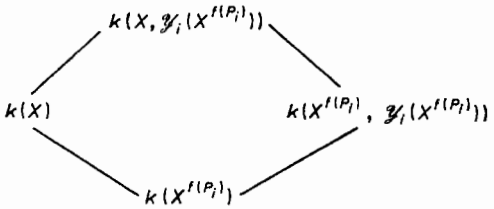
Enfin, il reste à voir que l'on peut prendre $a = 1$ si chacun des polynômes P_i possède une racine $\mathscr{Y}_i$ dans $\overline{Q}((X))$. Pour cela, on se ramène également au cas totalement décomposé, mais en raisonnant cette fois sur les polynômes $P_i(X^{f(P_i)}, Y)$ qui, sous l'hypothèse considérée, et contrairement au cas général, sont nécessairement irréductibles dans $k(X)[Y]$. En effet, on voit facilement que, pour $i = 1, 2, \ldots, N$, on a

$$[k(X^{f(P_i)}, \mathscr{Y}_i(X^{f(P_i)})) : k(X^{f(P_i)})] = \deg_Y P_i,$$

$$[k(X) : k(X^{f(P_i)})] = f(P_i),$$

$$[k(X, \mathscr{Y}_i(X^{f(P_i)})) : k(X^{f(P_i)}, \mathscr{Y}_i(X^{f(P_i)}))] = f(P_i).$$

On déduit alors du diagramme suivant



que

$$[k(X, \mathscr{Y}_i(X^{f(P_i)})) : k(X)] = \deg_Y P_i$$

ce qui signifie que $P_i(X^{f(P_i)}, Y)$ est irréductible dans $k(X)[Y]$. ∎

References

[1] E. Bombieri, *On G-functions*, in: *Recent progress in analytic number theory*, H. Halberstam and C. Hooley ed., Academic Press, 1981, Vol. 2, p. 1–67.

[2] – *On Weil's "Théorème de Décomposition"*, Amer. J. Math. 105 (1983), p. 295–308.

[3] P. Bundschuh, *Une nouvelle application de la méthode de Gel'fond*, Sem. Delange–Pisot–Poitou, Théorie des Nombres, 19ème année (1977/78), n° 42.

[4] P. Dèbes, *Une version effective du théorème d'irréductibilité de Hilbert*, Sem. Anal. Ultramétrique Amice–Christol–Robba, 10ème année (1982/83), n° 10. Ou les Journées de St Etienne, Algorithmique, Calcul formel, Arithmétique, Publ. Univ. St Etienne, n° XXIX.

[5] – *Spécialisations de polynômes*, Math. Rep. Acad. Sci., Royal Soc. Canada, vol. V, n° 6, Déc. 1983.

[6] – *Valeurs algébriques de fonctions algébriques et théorème d'irréductibilité de Hilbert*, Thèse de 3ème cycle, Univ. P. et M. Curie (Paris VI), 1984.

[7] – *Quelques remarques sur un article de Bombieri concernant le Théorème de Décomposition de Weil*, Amer. J. Math. 107 (1985), p. 39–44.
[8] B. Dwork et P. Robba, *On natural radii of p-adic convergence*, Trans. Amer. Math. Soc. 256 (1979), p. 199–213.
[9] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Pure and Applied Math. A series of monographs and textbooks, 23, Academic Press, 1966.
[10] G. Faltings, *Endlichkeitssätzes für abelsche Varietüten über Zahlkörpern*, Invent. Math. 73 (1983), p. 349–366.
[11] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory 6 (1974), p. 211-231.
[12] – *On the Sprindzuk–Weissauer approach to universal Hilbert subsets*, Israel Journal 51 (1985), 347-363
[13] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzahligen Koeffizienten*, Gesammelte Abhandlungen, Springer-Verlag, 1983 [reimpression Chelsea, 1965], Vol. 2, n° 18, p. 264–286. Ou J. Reine Angew. Math. 110 (1982), p. 104–129.
[14] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.
[15] A. Schinzel, *On Hilbert's Irreducibility Theorem*, Ann. Polon. Math. 16 (1965), p. 334–340.
[16] – *Selected topics on polynomials*, The University of Michigan Press, Ann Arbor 1982.
[17] T. Schneider, *Rationale Punkte über einer algebraischen Kurve*, Sem. Delange–Pisot–Poitou, Théorie des Nombres, 15ème année (1973/74), n° 20.
[18] – *Eine Bemerkung zu einem Satz von C. L. Siegel*, Comm. Pure Appl. Math. 29 (1976), p. 775–782.
[19] A. B. Shidlovski, *Approximations diophantiennes et nombres transcendants*, Publ. Univ. Moscou, 1982.
[20] C. L. Siegel, *Über Einige Anwandungen diophantischer Approximationen*, Abhandlungen der Preussischen Akademie der Wissenschaften. Phys. Math. Klasse 1929, n° 1. Ou *Gesammelte Abhandlungen*, Springer-Verlag, 1966, vol. 1, n° 16, p. 209–266.
[21] V. G. Sprindžuk, *Hilbert's Irreducibility Theorem and rational points on algebraic curves*, Doklady Acad. Nauk. SSSR 247 (1979), p. 285–289.
[22] – *Reducibility of polynomials and rational points on algebraic curves*, ibid. 250 (1980), p. 1327–1330.
[23] – *Diophantine equations involving unknown primes*, Trudy M.I.A.N. SSSR 158 (1981), p. 180–186.
[24] – *Arithmetic specializations in polynomials*, J. Reine Angew. Math. 340 (1983), p. 26–52.
[25] M. Waldschmidt, *Nombres transcendants*, Lecture Notes in Math., 402, Springer-Verlag, 1976.

INSTITUT HENRI POINCARÉ
11, RUE P. ET M. CURIE
75231 PARIS CEDEX 05
FRANCE

Reçu le 3.6.1985 (1516)