Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Jean-Pierre Serre

Dépendance d'exponentielles p-adiques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 7, n° 2 (1965-1966), exp. n° 15, p. 1-14

<http://www.numdam.org/item?id=SDPP_1965-1966__7_2_A4_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
7e année, 1965/66, n° 15

28 mars 1966

DÉPENDANCE D'EXPONENTIELLES p-ADIQUES

par Jean-Pierre SERRE

S. LANG ([2], [3]) a récemment démontré que deux exponentielles $e^{b_1 z}$, $e^{b_2 z}$, qui prennent des valeurs algébriques pour au moins trois valeurs indépendantes de z, sont multiplicativement dépendantes (i. e. le rapport b_1/b_2 est rationnel). Sa démonstration vaut aussi bien dans le cas réel ou complexe que dans le cas p-adique. Ce dernier cas est particulièrement intéressant : il a des applications à la théorie des "représentations p-adiques" des groupes de Galois des corps de nombres ; j'espère revenir ailleurs sur ce point.

Le contenu de cet exposé est le suivant : le paragraphe 1 reproduit la démonstration du théorème de Lang, dans le cas p-adique ; le paragraphe 2 en donne une généralisation à plusieurs variables, sous certaines hypothèses de répartition. Dans les deux cas, on a besoin de variantes p-adiques du lemme de Schwarz ; elles sont démontrées en Appendice.

§ 1. Le théorème de Lang

1.1. Enoncé du théorème.

Soit k un corps complet pour une valuation réelle v ; si c est tel que $0 < c < 1$, on pose

$$|x| = c^{v(x)} .$$

L'application $x \longmapsto |x|$ est une valeur absolue ultramétrique sur k.

On suppose également que k est de caractéristique zéro, et que sa caractéristique résiduelle est p ; on a $0 < v(p) < +\infty$.

On note E le "domaine de convergence" de la série exponentielle

$$\exp(z) = \sum_{n=0}^{\infty} z^n/n! ,$$

autrement dit l'ensemble des $z \in k$ tels que $v(z) > v(p)/(p-1)$.

On se donne :

(i) Un sous-groupe A de k, libre de rang fini $a \geqslant 2$ sur $\underset{\sim}{Z}$.

(ii) Des éléments b_i $(i = 1, \ldots, b)$ de k.

On pose :

$$e_i(z) = \exp(b_i z) \ .$$

On suppose que les e_i convergent sur A, i. e. que $b_i A \subset E$ pour tout i ; les e_i définissent alors des caractères de A, autrement dit des homomorphismes de A dans k^*.

THÉORÈME 1. - *Supposons que tous les* $e_i(x)$, $x \in A$, $1 \leqslant i \leqslant b$, *soient algébriques sur* $\underset{\sim}{Q}$. *Alors, si* $b > a/(a-1)$, *les* b_i *sont linéairement dépendants sur* $\underset{\sim}{Q}$.

Remarques.

1° Si $a = 2$, le théorème s'applique pour $b \geqslant 3$; si $a \geqslant 3$, il s'applique pour $b \geqslant 2$. On ignore ce qui se passe pour $a = b = 2$.

2° Dire que les b_i sont linéairement dépendants sur $\underset{\sim}{Q}$ équivaut à dire que les e_i sont multiplicativement dépendants, i. e. qu'il existe des entiers n_i non tous nuls tels que

$$\prod e_i^{n_i} = 1 \ .$$

1.2. Notations.

Soit K un corps de nombres. Si $x \in K$, nous appellerons dénominateur de x le plus petit entier $D \geqslant 1$ tel que Dx soit entier. Nous appellerons taille de x, et nous noterons $t(x)$, le nombre

$$t(x) = \sup(D, |\sigma(x)|) \ ,$$

où σ parcourt l'ensemble des plongements de x dans $\underset{\sim}{C}$. Lorsque x est entier, on a $D = 1$, et $t(x) = \sup(|\sigma(x)|)$.

Nous appliquerons ceci au corps K engendré par les $e_i(a_j)$, où (a_j) $(1 \leqslant j \leqslant a)$ est une base de A ; du fait que les e_i sont des homomorphismes, on a $e_i(x) \in K$ pour tout $x \in A$ et tout i.

D'autre part, si m est un entier $\geqslant 1$, nous noterons $A(m)$ l'ensemble des éléments de A de la forme $\sum m_j a_j$, avec $0 \leqslant m_j < m$. On a $\mathrm{Card}(A(m)) = m^a$.

1.3. Démonstration du théorème 1.

Quitte à multiplier les b_i par une puissance de p, on peut supposer que les séries $e_i(z)$ convergent sur le disque $|z| \leqslant R$, avec $R > 1$ [par abus de langage, nous dirons qu'une série $\sum a_n z^n$ converge sur le disque $|z| \leqslant R$ si $R^n |a_n|$ tend vers 0 - convention analogue pour plusieurs variables]. Quitte à remplacer A par $p^n A$, avec n assez grand, on peut aussi supposer que A est contenu dans le disque unité $|z| \leqslant 1$.

On aura à considérer des polynômes en les e_i :

$$P(e)(z) = \sum c_{n_1 \ldots n_b} e_1(z)^{n_1} \ldots e_b(z)^{n_b} \quad ;$$

on écrira un tel polynôme $\sum c_n e^n(z)$.

Soit maintenant N un entier $\geqslant 1$ (que l'on fera tendre vers $+\infty$), et considérons un polynôme du type précédent, avec $n_i < 2N^a$ pour tout i. Cherchons à déterminer les coefficients c_n de telle sorte que $P(e)$ s'annule en tous les éléments de $A(N^b)$. Les c_n répondant à la question sont les solutions d'un système linéaire homogène à $2^b N^{ab}$ inconnues et N^{ab} équations. Les coefficients de ce système sont les

$$e^n(x) = \prod e_i(a_j)^{n_i m_j} \text{ , avec } n_i < 2N^a \text{ , } m_j < N^b \text{ .}$$

Ces coefficients appartiennent à K. De plus, si d est un entier $\geqslant 1$, tel que $d.e_i(a_j)$ soit entier pour tout i, j, les produits

$$d^{2N^{a+b}}.e^n(x)$$

sont des entiers de K, et leur taille est majorée par $C_1^{N^{a+b}}$, où C_1 est une constante (i. e. ne dépend pas de N). D'après un lemme classique de SIEGEL (cf. [5], p. 37), on peut trouver une solution (c_n) non triviale du système en question, les c_n étant en outre des entiers de K de taille $\leqslant C_2^{N^{a+b}}$, où C_2 est une autre constante. Nous désignerons par P_N le polynôme en les e_i correspondant. C'est une série entière ; elle converge sur le disque $|z| \leqslant R$.

Supposons maintenant que les b_i soient linéairement indépendants sur $\mathbb{Q}$; les e_i sont alors multiplicativement indépendants, et les produits $e_1^{n_1} \ldots e_b^{n_b}$ sont

deux à deux distincts. Comme ce sont des homomorphismes, un argument classique montre qu'ils sont linéairement indépendants. Il s'ensuit que le polynôme P_N considéré ci-dessus n'est pas nul ; il ne possède donc qu'un nombre fini de racines dans le disque $|x| \leqslant R$. Il existe alors un plus grand entier M tel que P_N s'annule en tous les éléments de $A(M^b)$. On a $N \leqslant M$. Soit x un élément de $A((M+1)^b)$ en lequel P_N ne s'annule pas. Posons $y = P_N(x)$. Nous allons majorer la valeur absolue p-adique $|y|$ de y , ainsi que sa taille $t(y)$; la comparaison des résultats montrera que $b \leqslant a/(a-1)$.

Majoration de $t(y)$. - On a

$$y = \sum c_n e^n(x) \quad ;$$

les c_n sont entiers, et leur taille est majorée par $C_2^{N^{a+b}}$. D'autre part, on a :

$$e^n(x) = \prod e_i(a_j)^{n_i m_j} \text{ , avec } n_i < 2N^a \text{ , } m_j < (M+1)^b \text{ .}$$

On en conclut que les $e^n(x)$ sont de taille $\leqslant C_3^{M^{a+b}}$, et ont un dénominateur commun $\leqslant C_4^{M^{a+b}}$. Comme le nombre de termes de la sommation est négligeable devant de tels facteurs, on en déduit

$$t(y) \leqslant C_5^{M^{a+b}} \text{ .}$$

Majoration de $|y|$. - Soit $\sum p_n z^n$ le développement en série entière de la fonction P_N . Posons :

$$|P_N|_R = \sup R^n |p_n| \quad \text{et} \quad |P_N|_1 = \sup |p_n| \text{ .}$$

Comme P_N converge sur le disque $|z| \leqslant R$, le produit $R^n |p_n|$ tend vers 0 , et les nombres ci-dessus sont finis. Comme $|x| \leqslant 1$, on a $|y| = |P_N(x)| \leqslant |P_N|_1$. D'autre part, puisque P_N s'annule sur $A(M^b)$, il a au moins M^{ab} racines distinctes dans le disque unité, et le lemme de Schwarz (cf. Appendice, proposition 1) montre que

$$|P_N|_1 \leqslant R^{-M^{ab}} |P_N|_R \text{ .}$$

Enfin, $|P_N|_R$ est majoré par $\sup |e^n|_R$, et ceux-ci eux-mêmes sont majorés par $C_6^{M^{a+b}}$, comme on le voit par un calcul analogue à celui fait pour $t(y)$. On en déduit :

$$|y| \leqslant |P_N|_1 \leqslant R^{-M^{ab}} C_6^{M^{a+b}} .$$

Supposons que $ab > a + b$, i. e. $b > a/(a-1)$. Le terme en M^{ab} l'emporte alors sur celui en M^{a+b}, et l'on obtient une majoration :

$$|y| \leqslant C_7^{-M^{ab}} , \text{ avec } C_7 > 1 .$$

Mais il y a une relation entre $|y|$ et $t(y)$:

LEMME. - Soit $d = [K:\mathbb{Q}]$, et supposons la valeur absolue de k normalisée de telle sorte que $|p| = 1/p$. On a alors

$$|y| \geqslant t(y)^{-2d} \text{ pour tout } y \in K^{\times} .$$

Soit D le dénominateur de y, et soit $z = Dy$; l'élément z est entier. On a $|D| \leqslant 1$, d'où $|y| \geqslant |z|$. Soit Nz la norme de z dans $\mathbb{Q}$; c'est un entier, évidemment divisible par z ; d'où $|z| \geqslant |Nz|$. Si p^a est la plus grande puissance de p qui divise Nz, on a $|Nz| = p^{-a}$, d'où $|Nz| \geqslant 1/|Nz|_\infty$, où $|Nz|_\infty$ désigne la valeur absolue usuelle de l'entier Nz. Comme Nz est le produit des conjugués de z, et que la norme usuelle de ceux-ci est $\leqslant D.t(y)$, on a

$$|Nz| \geqslant D^{-d}\, t(y)^{-d} \geqslant t(y)^{-2d} ,$$

d'où le lemme.

Appliquons ce lemme à l'élément y considéré plus haut ; on a vu que $t(y) \leqslant C_5^{M^{a+b}}$; on en tire $|y| \geqslant C_5^{-2dM^{a+b}}$, ce qui est en contradiction avec $|y| \leqslant C_7^{-M^{ab}}$ puisque $ab > a + b$. On ne peut donc pas avoir à la fois l'indépendance des b_i et l'inégalité $b > a/(a-1)$, ce qui démontre le théorème.

§ 2. Le cas de plusieurs variables

2.1. La notion de parfaite densité.

Soit G un groupe topologique, isomorphe à $(\mathbb{Z}_p)^r$, où $\mathbb{Z}_p$ désigne le groupe des entiers p-adiques. Soit A un sous-groupe libre de type fini de G, et soit (a_j), $1 \leqslant j \leqslant a$, une base de A. Comme précédemment, si m est un nombre réel > 0, nous désignerons par $A(m)$ le sous-ensemble de A formé des $\sum m_j a_j$, avec $0 \leqslant m_j < m$.

Supposons que A soit dense dans G ; cela équivaut à dire que, pour tout entier

$n \geqslant 0$, l'application canonique $A \longrightarrow G/p^nG$ est surjective.

DÉFINITION. - Soit λ un nombre réel positif $\leqslant 1$. On dit que A est λ-dense dans G s'il existe une constante C telle que, pour tout entier $n \geqslant 0$, l'application

$$A(Cp^{\lambda n}) \longrightarrow G/p^nG$$

soit surjective.

Noter que, puisque A est dense, l'application $A/p^nA \longrightarrow G/p^nG$ est surjective ; comme $A(p^n)$ est un système de représentants de A/p^nA , on en conclut que $A(p^n) \longrightarrow G/p^nG$ est surjectif. Il s'ensuit que A est toujours 1-dense ; le seul cas intéressant est donc celui où $\lambda < 1$.

D'autre part, le nombre d'éléments de G/p^nG est p^{nr} , et celui de $A(Cp^{\lambda n})$ est équivalent à $C^a p^{\lambda an}$; le groupe A ne peut donc être λ-dense que si $\lambda a \geqslant r$, c'est-à-dire si $\lambda \geqslant r/a$.

DÉFINITION. - On dit que A est parfaitement dense dans G s'il est λ-dense pour $\lambda = r/a$.

Remarque. - On montre facilement que les définitions ci-dessus ne dépendent pas du choix de la base (a_j) .

Exemple. - Si $\alpha \in \underset{\sim}{Z}_p$ est quadratique sur $\underset{\sim}{Q}$, le sous-groupe $A = \underset{\sim}{Z} + \alpha\underset{\sim}{Z}$ de $\underset{\sim}{Z}_p$ est parfaitement dense.

Question. - Prenons pour G le groupe multiplicatif des unités p-adiques congrues à 1 mod p (resp. congrues à 1 mod 4 si $p = 2$), et soit A le sous-groupe engendré par des nombres rationnels a_j multiplicativement indépendants. Supposons A dense dans G . Est-il vrai que A est parfaitement dense ? J'ignore ce qu'il en est, même pour $p = 3$ et A engendré par 4 et 7 .

2.2. Enoncé du théorème.

Conservons les notations précédentes, et donnons-nous une famille finie d'homomorphismes continus $e_i : G \longrightarrow k^*$, le corps k vérifiant les conditions de 1.1. Soit b le nombre des e_i .

THÉORÈME 2. - Supposons que tous les $e_i(x)$, $x \in A$, $1 \leqslant i \leqslant b$, soient algébriques sur $\underset{\sim}{Q}$, et que A soit λ-dense dans G . Alors, si $b > r/(1 - \lambda)$, les e_i sont multiplicativement dépendants.

Dans le cas où A est parfaitement dense, on a $\lambda = r/a$, et l'inégalité devient $b > ar/(a - r)$; pour $r = 1$, c'est l'inégalité $b > a/(a - 1)$ du théorème 1 [mais ce dernier valait sans aucune hypothèse de λ-densité - le théorème 2 ne contient donc pas le théorème 1].

2.3. Démonstration du théorème 2. Préparatifs.

Soit C une constante telle que $A(Cp^{\lambda n}) \longrightarrow G/p^n G$ soit surjectif pour tout n. Nous choisirons dans $A(Cp^{\lambda n})$ un système de représentants $B(n)$ de $G/p^n G$; de plus, nous supposerons les $B(n)$ choisis de telle sorte que $B(n)$ soit contenu dans $B(n + 1)$; on voit tout de suite que c'est possible. On a

$$\mathrm{Card}(B(n)) = p^{nr} \text{ , avec } r = \dim G \ .$$

On note K le sous-corps de k engendré par les $e_i(x)$, $x \in A$; c'est un corps de nombres.

Enfin, on identifie G à $(\underset{\sim}{Z}_p)^r$ au moyen d'un isomorphisme. Les e_i sont alors transformées en des fonctions $e_i(z_1, \ldots, z_r)$ à r variables $z_i \in \underset{\sim}{Z}_p$. Mais tout homomorphisme continu de $\underset{\sim}{Z}_p$ dans k^* est donné localement par une exponentielle $z \longmapsto \exp(bz)$, avec $b \in k$. Les e_i sont donc des produits d'exponentielles, et en particulier sont analytiques en $z_1, \ldots, z_r$. Sur un voisinage convenable $p^n G$ de 0 dans G, on a

$$e_i(z) = \sum \alpha_{i,n} z^n \quad (\text{où } n \text{ désigne un multi-indice}),$$

la série étant convergente sur $p^n G$. Quitte à remplacer e_i par sa puissance p^{n+1}-ième, on peut donc supposer que e_i est donné, sur tout le polydisque unité $(\underset{\sim}{Z}_p)^r$, par une série $\sum \alpha_{i,n} z^n$ qui converge sur le polydisque $|z_i| \leqslant R$, avec $R > 1$. [Ici encore, ces précautions sont destinées à permettre l'application du lemme de Schwarz.]

2.4. Démonstration du théorème 2.

Elle est tout à fait analogue à celle du théorème 1. On commence par considérer des polynômes en les e_i de la forme

$$P(e)(z) = \sum c_{n_1 \ldots n_b} e_1(z)^{n_1} \ldots e_b(z)^{n_b} \ ,$$

où tous les n_i sont $< 2p^{nr}$ (n étant un entier $\geqslant 0$ que l'on fait tendre vers $+\infty$). On cherche à déterminer les coefficients c de telle sorte que $P(e)$ s'an-

nule en tout point de l'ensemble $B(bn)$ défini au n° 2.3. Cela donne un système linéaire homogène à $2^b p^{bnr}$ inconnues et p^{bnr} équations. Ses coefficients sont des produits

$$\prod e_i(a_j)^{n_i m_j} \text{ , avec } n_i < 2p^{nr} \text{ , } m_j < Cp^{\lambda bn} \text{ ;}$$

on en déduit, comme précédemment, que l'on peut prendre pour coefficients c des entiers de K, non tous nuls, de taille $\leqslant C_8^{p^{n(r+\lambda b)}}$. Soit P_n le polynôme correspondant.

Supposons que les e_i soient <u>multiplicativement indépendants</u>. Le même argument que dans le cas $r = 1$ montre que P_n est alors non nul. Comme la réunion des $B(m)$ est dense dans G, il s'ensuit qu'il existe un plus grand entier m tel que P_n s'annule sur $B(m)$; on a $m \geqslant bn$. Soit x un élément de $B(m+1)$ tel que $y = P_n(x)$ soit non nul. On va obtenir une contradiction en comparant des majorations de $|y|$ et de $t(y)$.

<u>Majoration de</u> $t(y)$. - On a

$$y = \sum c_{n_1 \ldots n_b} \prod e_i(a_j)^{n_i m_j} \text{ ,}$$

avec $n_i < 2p^{nr} \leqslant 2p^{mr/b}$, $m_j < Cp^{\lambda(m+1)}$, $t(c) \leqslant C_8^{p^{n(r+\lambda b)}}$. On en déduit :

$$t(y) \leqslant C_9^{p^{m(\lambda+r/b)}} \text{ .}$$

<u>Majoration de</u> $|y|$. - On définit comme dans le cas $r = 1$ les normes $|P_n|_R$ et $|P_n|_1$ de P_n relativement aux polydisques $|z_i| \leqslant R$ et $|z_i| \leqslant 1$. On a

$$|y| \leqslant |P_n|_1 \text{ .}$$

D'autre part, P_n s'annule en tous les points de $B(m)$, et l'application $B(m) \longrightarrow G/p^m G$ est surjective. D'après une variante à r variables du lemme de Schwarz (cf. Appendice, proposition 2), on a donc :

$$|P_n|_1 \leqslant R^{-p^m} |P_n|_R \text{ .}$$

Enfin, un calcul direct montre que $|P_n|_R \leqslant C_{10}^{p^{m(\lambda+r/b)}}$.

Supposons alors que $1 > \lambda + r/b$, i. e. que $b > r/(1-\lambda)$. L'exposant p^m l'emporte sur l'exposant $p^{m(\lambda+r/b)}$, et l'on obtient la majoration :

$$|y| \leqslant C_{11}^{-p^m} \text{ , avec } C_{11} > 1 \text{ .}$$

Mais les majorations obtenues pour $|y|$ et $t(y)$ sont incompatibles avec le lemme du n° 1.3. Le théorème 2 est donc démontré.

Appendice

Analogues p-adiques du lemme de Schwarz

A.1. Notations.

Soit k un corps complet pour une valeur absolue ultramétrique non triviale. Soit

$$f = \sum a_{n_1 \ldots n_r} z_1^{n_1} \ldots z_r^{n_r} = \sum a_n z^n \text{ ,}$$

une série formelle à coefficients dans k . Si R est un nombre réel > 0 , on pose :

$$|f|_R = \sup R^{|n|} |a_n| \text{ , où } |n| = \sum n_i \text{ .}$$

On a $|f + g|_R \leqslant \sup(|f|_R , |g|_R)$, $|\lambda f|_R = |\lambda| . |f|_R$, et

$$|fg|_R = |f|_R . |g|_R \text{ si } |f|_R \text{ et } |g|_R \text{ sont finis.}$$

Lorsque $|f|_R$ est fini, la série $f(z)$ converge dans le polydisque $|z_i| < R$; elle converge même dans le polydisque $|z_i| \leqslant R$ si $R^{|n|} |a_n|$ tend vers 0 . On a :

$$|f(z)| \leqslant |f|_R \text{ .}$$

Lorsque en outre le corps résiduel de k est infini, et que le groupe des valeurs de $k^\times$ est dense, on a :

$$|f|_R = \sup |f(z)| \text{ pour } |z_i| < R \text{ .}$$

Si $R' \leqslant R$, on a $|f|_{R'} \leqslant |f|_R$; le but du lemme de Schwarz est d'améliorer cette inégalité, sous l'hypothèse que f a "beaucoup" de racines dans le polydisque $|z_i| \leqslant R'$.

A.2. Le cas des fonctions d'une variable.

Supposons que $r = 1$. Soient $R' < R$ deux nombres réels > 0 , et soit $f(z) = \sum a_n z^n$ une série telle que $|f|_R$ soit fini. Il en résulte que f con-

verge sur le disque $|z| \leqslant R'$; on peut donc parler de ses racines sur ce disque.

PROPOSITION 1 (cf. MAHLER [4]). - Si f a h racines dans le disque $|z| \leqslant R'$, on a :

$$|f|_{R'} \leqslant (\frac{R'}{R})^h \, |f|_R \ .$$

Remarquons d'abord que, si f a une racine a telle que $|a| \leqslant R'$, on peut écrire f sous la forme $f = (z - a)f_1$, avec $|f_1|_R < +\infty$; en effet, c'est clair si $a = 0$, et le cas général se ramène à celui-là par translation. En appliquant ce résultat aux racines a_i $(1 \leqslant i \leqslant h)$ de f dans le disque $|z| \leqslant R'$, on voit que l'on peut écrire f sous la forme

$$f = P.g \ , \text{ avec } P(z) = \prod (z - a_i) \text{ et } |g|_R < +\infty \ .$$

On a $|P|_R = R^h$ et $|P|_{R'} = R'^h$. On en déduit :

$$|f|_{R'} = R'^h.|g|_{R'} \leqslant R'^h.|g|_R = (\frac{R'}{R})^h.R^h.|g|_R = (\frac{R'}{R})^h.|f|_R \ .$$

C. Q. F. D.

Remarque. - On aurait pu aussi appliquer la théorie du polygone de Newton à f.

A.3. Le cas général. Énoncé du résultat.

Lorsque $r > 1$, les racines de f dans le polydisque $|z_i| \leqslant R'$ peuvent former des sous-espaces analytiques de dimension $r - 1$, et sont en général en nombre infini. Le fait que f ait beaucoup de racines n'entraîne alors rien de plus que l'inégalité triviale :

$$|f|_{R'} \leqslant \frac{R'}{R}.|f|_R \ .$$

Il est donc nécessaire de faire des hypothèses restrictives sur la position de ces racines. Je vais me borner à un cas très particulier, où l'on suppose que ces racines sont très bien réparties ; il serait intéressant d'avoir des énoncés plus généraux.

Plus précisément, nous supposerons que k vérifie les hypothèses du n° 1.1, donc contient le corps p-adique $\mathbb{Q}_p$. On se donne un nombre entier $n \geqslant 0$, et un sous-ensemble B de $(\mathbb{Z}_p)^r$ tel que l'application $B \longrightarrow (\mathbb{Z}_p/p^n \mathbb{Z}_p)^r$ soit bijective. On se donne d'autre part une série $f(z_1 , \ldots , z_r)$ telle que $|f|_R < +\infty$, R étant un nombre réel > 1. Cette série converge sur le polydisque unité, lequel contient B.

PROPOSITION 2. - Si f s'annule sur B, on a :

$$|f|_1 \leqslant R^{-p^n} |f|_R \ .$$

Noter que l'exposant de R^{-1} est bien p^n et non $\mathrm{Card}(B) = p^{nr}$. L'exemple de la fonction $f = z_1(z_1 - 1) \ldots (z_1 - p^n + 1)$ montre d'ailleurs que cet exposant ne peut pas être amélioré.

Question. - Existe-t-il un résultat analogue dans le cas archimédien, autrement dit pour les fonctions de plusieurs variables complexes ? Même question pour le théorème 2.

A.4. Démonstration de la proposition 2.

La méthode consiste à écrire f comme série de polynômes d'interpolation relatifs à la suite des entiers positifs (cf. Y. AMICE [1]). De façon précise, pour tout entier positif α, posons :

$$P_\alpha(X) = X(X - 1) \ldots (X - \alpha + 1) \ ,$$

et si $\alpha = (\alpha_1 , \ldots , \alpha_r)$ est un multi-indice, posons :

$$P_\alpha(z) = P_{\alpha_1}(z_1) \ldots P_{\alpha_r}(z_r) \ , \text{ où } z = (z_1 , \ldots , z_r) \ .$$

On a

$$P_\alpha(z) = z^\alpha + \sum_{|\beta|<|\alpha|} b_\beta^\alpha \, z^\beta \ , \text{ où les } b_\beta^\alpha \text{ sont des entiers.}$$

D'où :

$$z^\alpha = P_\alpha + \sum_{|\beta|<|\alpha|} c_\alpha^\beta \, P_\beta \ , \text{ où les } c_\alpha^\beta \text{ sont des entiers.}$$

Si $f = \sum a_\alpha z^\alpha$ est la série donnée, on a $a_\alpha \to 0$ (puisque $|f|_R$ est fini). Remplaçant les z^α par leur expression en fonction des P_α, on obtient un développement en série pour f :

$$f = \sum b_\alpha P_\alpha \ .$$

[En fait, les z^α et les P_α constituent deux bases normales de l'espace de Banach des séries convergentes sur le polydisque unité, la norme étant $f \longmapsto |f|_1$. Cf. [1], Chap. III.]

On vérifie tout de suite que l'on a :

$$|f|_1 = \sup |b_\alpha| \qquad \text{et} \qquad |f|_R = \sup R^{|\alpha|} . |b_\alpha| \ .$$

Tout revient donc à majorer les b_α .

Supposons que la valuation v soit normée de telle sorte que $v(p) = 1$, et posons :

$$b(\alpha) = v(b_\alpha)$$

$$q(\alpha) = v(\alpha!) \text{ , où } \alpha! = \alpha_1! \dots \alpha_r! \text{ .}$$

LEMME. - Soit X l'ensemble des $\alpha = (\alpha_1 , \dots , \alpha_r)$ tels que $\alpha_i \leqslant p^n - 1$ pour tout i . Soit m le minimum de $q(\alpha) + b(\alpha)$ pour $\alpha \in X$. Il existe un $\gamma \notin X$ tel que $q(\gamma) + b(\gamma) \leqslant m$.

Soit X_m l'ensemble des $\alpha \in X$ tels que $q(\alpha) + b(\alpha) = m$, et soit α un élément de X_m tel que $|\alpha|$ soit minimum. Soit x l'élément de B tel que $x \equiv \alpha \mod p^n$. Par hypothèse, on a $f(x) = 0$. Cela s'écrit :

$$\sum b_\gamma P_\gamma(x) = 0$$

La valuation de $b_\gamma P_\gamma(x)$ est égale à $b(\gamma) + v(P_\gamma(x))$. Or, on sait (cf. par exemple [1]) que le polynôme $Q_\gamma = P_\gamma/\gamma!$ applique $(\underset{\sim}{Z}_p)^r$ dans $\underset{\sim}{Z}_p$; on a donc $v(P_\gamma(x)) \geqslant q(\gamma)$, d'où

$$v(b_\gamma P_\gamma(x)) \geqslant q(\gamma) + b(\gamma) \text{ ,}$$

l'égalité étant réalisée si et seulement si $Q_\gamma(x) \not\equiv 0 \mod p$.

Supposons d'abord que l'on ait $\gamma \in X$. La classe de $Q_\gamma(x) \mod p$ ne dépend alors que de la classe de $x \mod p^n$ (c'est là une propriété générale des polynômes d'interpolation d'une suite très bien répartie, cf. [1], p. 135, lemme 4). On a donc

$$Q_\gamma(x) \equiv Q_\gamma(\alpha) \mod p \text{ .}$$

Si $\gamma_i > \alpha_i$ pour un indice i , on a $Q_\gamma(\alpha) = 0$, d'où

$$Q_\gamma(x) \equiv 0 \mod p \text{ .}$$

Pour $\gamma = \alpha$, on a $Q_\alpha(\alpha) = 1$, d'où $Q_\alpha(x) \equiv 1 \mod p$, et

$$v(b_\alpha P_\alpha(x)) = q(\alpha) + b(\alpha) = m \text{ .}$$

Si $\gamma \in X$ est distinct de α , on a :

$$v(b_\gamma P_\gamma(x)) \geqslant m + 1 \text{ .}$$

En effet, c'est clair si $\gamma \notin X_m$, car alors $q(\gamma) + b(\gamma) \geqslant m + 1$. Et si $\gamma \in X_m$,

on a $|\gamma| > |\alpha|$, et l'une des composantes γ_i de γ est $> \alpha_i$, d'où

$$v(P_\gamma(x)) \geqslant q(\gamma) + 1 \quad .$$

D'autre part, puisque la somme des $b_\gamma P_\gamma(x)$ est nulle, il existe un $\gamma \neq \alpha$ tel que

$$v(b_\gamma P_\gamma(x)) \leqslant v(b_\alpha P_\alpha(x)) = m \quad .$$

Vu ce qui précède, on a $\gamma \notin X$. D'autre part,

$$q(\gamma) + b(\gamma) \leqslant v(b_\gamma P_\gamma(x)) \leqslant m \quad ,$$

ce qui achève la démonstration du lemme.

Fin de la démonstration de la proposition 2. - Soit c le nombre réel < 1 tel que $x = c^{v(x)}$ pour tout $x \in k$. Ecrivons R et $|f|_R$ comme puissances de c :

$$R = c^{-k} \quad (\text{avec } k > 0) \qquad \text{et} \qquad |f|_R = c^h \quad .$$

On a alors

$$b(\alpha) \geqslant k|\alpha| + h \quad ,$$

et il nous faut prouver que $|f|_1 \leqslant c^{h+kp^n}$, i. e. que

$$b(\alpha) \geqslant k.p^n + h \quad .$$

C'est clair si $|\alpha| \geqslant p^n$. Dans le cas contraire, on a $\alpha \in X$, et le lemme ci-dessus montre qu'il existe $\gamma \notin X$ tel que

$$q(\gamma) + b(\gamma) \leqslant q(\alpha) + b(\alpha) \quad .$$

On a alors :

$$b(\alpha) \geqslant b(\gamma) + q(\gamma) - q(\alpha) \quad .$$

Puisque $\gamma \notin X$, on a $|\gamma| \geqslant p^n$, d'où $b(\gamma) \geqslant k.p^n + h$.

D'autre part, $q(\gamma) = \sum v(\gamma_i!)$; par hypothèse, l'un des γ_i est $\geqslant p^n$, d'où

$$q(\gamma) \geqslant v(\gamma_i!) \geqslant v(p^n!) = (p^n - 1)/(p - 1) \quad .$$

Enfin, on a

$$q(\alpha) = \sum v(\alpha_i!) \leqslant \sum \alpha_i/(p - 1) = |\alpha|/(p - 1) \leqslant (p^n - 1)/(p - 1)$$

puisqu'on a supposé $|\alpha| < p^n$.

En combinant ces inégalités, on trouve

$$b(\alpha) \geqslant k.p^n + h \quad ,$$

ce qui achève la démonstration.

BIBLIOGRAPHIE

[1] AMICE (Yvette). - Interpolation p-adique, Bull. Soc. math. France, t. 92, 1964, p. 117-180.

[2] LANG (Serge). - Nombres transcendants, Séminaire Bourbaki, 18e année, 1965/66, n° 305.

[3] LANG (Serge). - Algebraic values of meromorphic functions II, Topology (à paraître).

[4] MAHLER (Kurt). - Über transzendente p-adischen Zahlen, Compositio Mathematica, t. 2, 1935, p. 259-275.

[5] SIEGEL (Carl Ludwig). - Transcendental numbers. - Princeton, Princeton University Press, 1949 (Annals of Mathematics Studies, 16).