Séminaire Delange-Pisot-Poitou.
Théorie des nombres

GÉRARD RAUZY

Approximations diophantiennes linéaires homogènes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 3 (1961-1962), exp. nº 1, p. 1-18

<http://www.numdam.org/item?id=SDPP_1961-1962__3__A1_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
3e année, 1961/62, n° 1

20 et 27 novembre 1961

APPROXIMATIONS DIOPHANTIENNES LINÉAIRES HOMOGÈNES

par Gérard RAUZY

1. Généralités.

1.1. Approximations diophantiennes. - Etant donné un élément $x = (x_1 , \dots , x_n)$ de Z^n (Z ensemble des entiers rationnels), on appellera hauteur de x la quantité : $\lceil x \rceil = \max\limits_{i=1,\dots,n} |x_i|$. La hauteur de x est un entier supérieur ou égal à zéro (l'égalité ayant lieu si et seulement si $x = 0$). On a

$$\lceil x + y \rceil \leqslant \lceil x \rceil + \lceil y \rceil \ , \qquad \lceil xy \rceil \leqslant \lceil x \rceil \lceil y \rceil \ , \qquad \lceil - x \rceil = \lceil x \rceil \quad .$$

La hauteur est donc liée de manière simple aux opérations sur les entiers ; en outre, il n'existe qu'un nombre fini d'entiers de hauteur donnée.

Soit $F(x)$ une fonction de la variable $x \in Z^n$, à valeurs dans un espace K muni d'une application que l'on notera $\|F(x)\|$ dans R^+ , ensemble des nombres réels positifs ou nuls ; soit d'autre part $\varphi(t)$ une fonction de R^+ dans R^+ , on dira que F admet l'approximation φ si :

$$\forall \ A \ , \ \exists \ x \ , \qquad \lceil x \rceil \geqslant A \ \text{ et } \ \|F(x)\| < \varphi(\lceil x \rceil) \quad .$$

On dira que l'approximation est propre, si en outre

$$\|F(x)\| > 0 \quad .$$

On appellera fonction d'approximation, une classe d'équivalence des fonctions de $t \in R^+$ dans R^+ , monotones, tendant vers 0 quand $t \to \infty$, l'équivalence étant associée à la relation de préordre :

$$\varphi_1 < \varphi_2 \iff \exists \ t_0 \ , \ \forall \ t > t_0 \ , \ \varphi_1(t) \leqslant \varphi_2(t) \quad .$$

φ_1 est dite alors plus fine que φ_2 .

De cette définition résulte que si F admet l'approximation φ , alors F admet l'approximation ψ pour tout ψ équivalente à φ (c'est-à-dire telle que $\varphi < \psi$, $\psi < \varphi$).

On peut alors introduire une relation d'ordre sur les fonctions d'approximation à partir de la relation de préordre introduite ; les problèmes qui se poseront en théorie de l'approximation seront alors, en adoptant la terminologie de KOKSMA [7] :

A_1 : Trouver pour une fonction F donnée, une fonction d'approximation φ la plus fine possible telle que F admette l'approximation φ ;

B : Trouver pour une fonction F donnée, une fonction d'approximation φ la moins fine possible telle que F n'admette pas l'approximation φ .

(Il faudrait, en fait, préciser que nous nous intéressons seulement aux fonctions d'un certain type, par exemple λt^{α} , $\lambda t^{\alpha}(\mathrm{Log}\ t)^{\beta}$, ... sinon les problèmes posés auraient des solutions triviales.)

On s'intéresse également à la densité des approximations obtenues : soit en donnant des encadrements comme dans le théorème de Borel ([2]), ou plus précisément dans le théorème de Szüsz ([13]) ; soit en fournissant des approximations "régulières" d'un nombre donné (PISOT [11]) ; soit en donnant des indications sur la croissance d'approximations d'un certain type ; par exemple, si

$$q_{k+1} > q_k \ ; \quad q_1 > 0 \quad \text{et si} \quad \|q_k \zeta\| \to 0$$

(ζ nombre irrationnel, x valeur absolue de la différence entre x et l'entier le plus voisin), alors, quel que soit n , $\overline{\lim}\, \Delta_n q_k = \infty$ quand $k \to \infty$ ($\Delta_n q_k$ différence n-ième) ; voir aussi les théorèmes de Siegel ([12]), préalables au théorème de Roth.

Dans cet esprit, on donnera le plus souvent les résultats d'approximation sous la forme (KOKSMA [7]) :

A_2 : $\forall\ t > t_0$, $\exists\ x$ tel que $\overline{|x|} \leqslant t$ et $\|F(x)\| < \varphi(t)$.

1.2. Approximations diophantiennes linéaires homogènes. - Par rapport au cas général d'une fonction $F(x)$ à valeurs dans un ensemble K , ce sera le cas où K est un groupe et où $F(x + y) = F(x) + F(y)$.

Plus précisément, nous supposerons que K est un ensemble tel que, Z^m , R^m , C^m , Q_P^m , ... (C ensemble des nombres complexes, Q_P ensemble des nombres P-adiques), prenant les valeurs 1 , 2 , ... , m et prenant les valeurs 1 , 2 , ... , n . Nous appellerons système de signature $(m\ ,\ n)$ le système de formes :

$$u_{\mu} = \sum_{\nu=1}^{n} \theta_{\mu\nu}\, x_{\nu} \ , \qquad x = (x_1\ , \ldots\ , x_n) \in Z^n \quad .$$

Nous prendrons comme norme sur la quantité $u = (u_{\mu})$, l'une des valeurs $\max |u_{\mu}|$, $\max \|u_{\mu}\|$, $\max |u_{\mu}|_P$, $|\alpha|$ désignant la valeur absolue ordinaire d'un nombre réel, $\|\alpha\|$ la valeur absolue modulo 1, $|\alpha|_P$ la valeur absolue P-adique.

On peut aussi prendre des normes de la forme $\max \lambda_\mu |u_\mu|$ $(\lambda_\mu \geq 0)$; on pourra prendre dans ce cas comme valeur absolue la quantité $|\alpha| = 1$ si $\alpha \neq 0$, $|0| = 0$. C'est ce que l'on fait, si l'on considère comme théorème d'approximation, la première partie du théorème de Roth (existence d'un polynôme à coefficients entiers de hauteur bornée, et d'indice élevé en un point à coordonnées algébriques).

Nous allons maintenant étudier les systèmes de signatures générales ou particulières, où les $\theta_{\mu\nu}$ seront des nombres réels ; nous prendrons comme valeurs absolues, la valeur absolue ordinaire ou la valeur absolue modulo 1.

2. Les systèmes de signature (m , n) .

2.1. Valeur absolue ordinaire : théorème de Dirichlet-Minkowski. - Soit

$$u_\mu = \sum_{\nu=1}^{m} \theta_{\mu\nu} x_\nu$$

un système de signature (m , n) avec $n > m$.

Il existe une constante C telle que :

$$\forall \ t \ \underline{\text{entier}} \geq 1 \ , \ \exists \ x = (x_1 , \dots , x_n) \neq 0 \ , \ \overline{|x|} \leq t \ , \ \max |u_\mu| \leq C \ t^{1-n/m} \ .$$

(Remarquons que l'exposant $1 - n/m$ est négatif, $C\, t^{1-n/m}$ tend vers 0 quand $t \to \infty$. Bien entendu, en changeant au besoin la constante C , l'énoncé est valable pour t réel ≥ 1 .)

Démonstration. - Si x est tel que $0 \leq x_\nu \leq t$ pour $\nu = 1 , \dots , n$, on a alors

$$g_\mu \leq u_\mu \leq d_\mu$$

avec

$$g_\mu = t \sum_\nu{}' \theta_{\mu\nu} \ , \qquad d_\mu = t \sum_\nu{}'' \theta_{\mu\nu}$$

(Σ' ou Σ'' désignant les sommes prises uniquement sur les quantités négatives ou positives). On a donc

$$d_\mu - g_\mu = t \sum_{\nu=1}^{n} |\theta_{\mu\nu}| \quad .$$

Posons alors

$$C = \max_\mu \sum_{\nu=1}^{n} |\theta_{\mu\nu}| \quad ,$$

et soit

$$N_\mu = \left[\frac{d_\mu - g_\mu}{Ct^{1-n/m}}\right] + 1 \quad .$$

Si x est tel que $0 \leqslant x_\nu \leqslant t$, chacun des $u_\mu(x)$ se trouve dans l'un des intervalles :

$$\left[g_\mu \, , \frac{d_\mu - g_\mu}{N_\mu} + g_\mu\right] , \left[\frac{d_\mu - g_\mu}{N_\mu} + g_\mu \, , 2\,\frac{d_\mu - g_\mu}{N_\mu} + g_\mu\right] , \ldots , \left[\frac{N_\mu - 1\,(d_\mu - g_\mu)}{N_\mu} + g_\mu \, , d_\mu\right] .$$

Les $u(x)$ peuvent donc occuper $N_1 \ldots N_m$ positions différentes, quand x prend l'une des $(t+1)^n$ positions telles que $0 \leqslant x_\nu \leqslant t$.

Mais

$$N_1 \ldots N_m \leqslant \prod_{\mu=1}^{m} \left(\frac{d_\mu - g_\mu}{Ct^{1-n/m}} + 1\right) \leqslant \prod_{\mu=1}^{m} \left(\frac{\sum_{\nu=1}^{n} |\theta_{\mu\nu}|}{C}\, t^{n/m} + 1\right) \quad ;$$

soit

$$N_1 \ldots N_m \leqslant \prod_{\mu=1}^{m} (t^{n/m} + 1) < \prod_{\mu=1}^{m} (t+1)^{n/m} \quad ;$$

d'où finalement

$$N_1 \ldots N_m < (t+1)^n \quad .$$

Il en résulte que deux x différents, soit y et z, vont donner des $u(y)$ et $u(z)$ tels que, pour chaque μ, $u_\mu(y)$ et $u_\mu(z)$ appartiennent au même intervalle. La longueur d'un tel intervalle est

$$\frac{d_\mu - g_\mu}{N_\mu} \leqslant \frac{d_\mu - g_\mu}{\left(\frac{d_\mu - g_\mu}{Ct^{1-n/m}}\right)} = Ct^{1-n/m} \quad .$$

En posant $x = y - z$ on voit que $\overline{|x|} \leqslant t$ et que $u_\mu(x) = u_\mu(y) - u_\mu(z)$ en vertu de la linéarité, donc que

$$|u_\mu(x)| \leqslant Ct^{1-n/m} \quad .$$

Comme y et z sont distincts, x n'est pas nul, ce qu'il fallait montrer

On voit que, pour t grand, on peut choisir C aussi voisin que l'on veut de $\left(\prod \sum_{\nu=1}^{m} |\theta_{\mu\nu}|\right)^{1/m}$.

2.2. Valeur modulo 1 : théorème de Kronecker. - Soit toujours

$$u_\mu = \sum_{\nu=1}^{m} \theta_{\mu\nu}\, x_\nu$$

un système de signature $(m\ ,\ n)$ sans restriction cette fois sur m et n.

Alors

$$\forall\ t \geqslant 1\ ,\ \exists\ x = (x_1\ ,\ \dots\ ,\ x_n) \neq 0\ \ \underline{\text{tel que}}\ \ \overline{|x|} \leqslant t\ ,\ \max \|u_\mu\| < t^{-n/m}$$

($\|\alpha\|$ désignant la quantité $\min\limits_{p \in Z} |\alpha - p|$).

Démonstration. - Elle est identique à la précédente, à cela près qu'il faut remplacer g_μ et d_μ par 0 et 1 (en outre, la valeur 1 est exclue ce qui permet d'avoir une inégalité stricte). L'intérêt de cette formule est qu'il n'y figure plus de constante numérique dépendant du système. Il est aisé de voir que l'on peut en déduire le théorème précédent : si nous avons donné la démonstration de celui-ci, c'est qu'elle permet d'avoir une meilleure valeur pour la constante quand t est grand.

2.3. Le théorème précédent admet une "réciproque" ; il n'est pas possible, pour un système quelconque, d'admettre une fonction d'approximation en $o(t^{-n/m})$. De manière plus précise

$$\forall\ (m\ ,\ n)\ ,\ \exists\ \gamma > 0\ \ \underline{\text{et des}}\ \ \theta_{\mu\nu}\ \ \underline{\text{tels que}}\ \ \max \|u_\mu(x)\| \geqslant \gamma\, \overline{|x|}^{-n/m} \quad .$$

<u>Démonstration</u>. - Nous posons $\ell = m + n$ et considérons un système de ℓ entiers algébriques conjugués de degré ℓ distincts soient : $\Phi_1 , \dots , \Phi_\ell$. (Racines par exemple du polynôme $\prod_{i=1}^{\ell} (z - iq) - 1$ avec q entier positif assez grand).

Posons alors

$$Q_k(x , y) = \sum_{\nu=1}^{n} \Phi_k^{m+\nu-1} x_\nu + \sum_{\mu=1}^{m} \Phi_k^{\mu-1} y_\mu \qquad \text{pour} \quad k = 1 , \dots , \ell$$

soit

$$Q_k(x , y) = y_1 + \Phi_k y_2 + \dots + \Phi_k^{m-1} y_m + \Phi_k^m x_1 + \dots + \Phi_k^{m+n-1} x_k \quad .$$

Si tous les x_ν ne sont pas nuls, cette quantité est un entier algébrique non nul. La quantité $\prod_{k=1}^{\ell} Q_k(x , y)$ est donc un entier rationnel non nul, on a donc :

$$\prod_{k=1}^{\ell} |Q_k(x , y)| \geqslant 1 \quad .$$

Le système de m équations à m inconnues $\ell_1 , \dots , \ell_m$

$$\ell_1 + \Phi_k \ell_2 + \dots + \Phi_k^{m-1} \ell_m = - (\Phi_k^m x_1 + \dots + \Phi_k^{\ell-1} x_m) \qquad k = 1 , \dots , m ,$$

a pour déterminant le déterminant de Vandermonde de $\Phi_1 , \dots , \Phi_n$ qui sont distinctes. C'est donc un système de Cramer que nous résolvons

$$\ell_\mu = \sum_{\nu=1}^{n} \theta_{\mu\nu} x_\nu \quad .$$

Nous avons alors

pour $k = 1 , \dots , m$,

$$Q_k(x , y) = \sum_{\mu=1}^{m} \Phi_k^{\mu-1} (y_\mu - \sum_{\nu=1}^{n} \theta_{\mu\nu} x_\nu) \quad ,$$

et pour $m + 1 \leqslant k \leqslant \ell$,

$$Q_k(x , y) = \sum_{\mu=1}^{m} \Phi_k^{\mu-1} (y_\mu - \sum_{\nu=1}^{n} \theta_{\mu\nu} x_\nu) + \sum_{\nu=1}^{n} \omega_{k\nu} x_\nu \quad .$$

Pour un système de x_ν donnés non tous nuls, choisissons alors les y_μ de manière que

$$|\sum_\nu \theta_{\mu\nu} x_\nu - y_\mu| = \|\sum \theta_{\mu\nu} x_\nu\| \quad .$$

Nous aurons alors avec des constantes C_1 et C_2 indépendantes des x_ν et des y_μ,

$$\text{pour} \quad k = 1 \, , \, \dots \, , \, m$$

$$|Q_k(x \, , \, y)| \leqslant C_1 \max_\mu \|\sum_\nu \theta_{\mu\nu} x_\nu\| \quad ;$$

$$\text{pour} \quad m + 1 \leqslant k \leqslant \ell$$

$$|Q_k(x \, , \, y)| \leqslant C_1 \max_\mu \|\sum_\nu \theta_{\mu\nu} x_\nu\| + C_2 \, \overline{|x|} \quad .$$

Mais

$$\max_\mu \|\sum_\nu \theta_{\mu\nu}\| < 1 \quad \text{et} \quad C_1 + C_2 \, \overline{|x|} \leqslant (C_1 + C_2) \, \overline{|x|} = C_3 \overline{|x|} \quad ,$$

puisque $\overline{|x|} \geqslant 1$.

Nous obtenons finalement

$$1 \leqslant \prod_{k=1}^{\ell} |Q_k(x \, , \, y)| \leqslant C_1^m \, C_3^n (\max_\mu \|\sum_\nu \theta_{\mu\nu} x_\nu\|)^m \, \overline{|x|}^n \quad ,$$

ce qui est le résultat cherché en posant

$$\gamma = (C_1^m \, C_3^n)^{-1/m} \quad .$$

3. Les signatures $(1 \, , \, n)$ et $(n \, , \, 1)$.

3.1. Transfert. - Soit

$$L_\mu = \sum_{\nu=1}^{n} \theta_{\mu\nu} x_\nu \qquad \mu = 1 \, , \, \dots \, , \, m \quad ,$$

et considérons le système transposé

$$M_\nu = \sum_{\mu=1}^{m} \theta_{\mu\nu} y_\mu \qquad \nu = 1 \, , \, \dots \, , \, n \quad .$$

On démontre alors que, si le système L_μ admet (modulo 1) l'approximation $\frac{1}{C} t^{-n/m}$, le système M_μ admet l'approximation $\frac{1}{\gamma} t^{-m/n}$, où γ est une fonction de C , m , n (Voir par exemple CASSELS [3]).

Un cas particulier important est le théorème de transfert de Khinčin, pour les signatures $(1, n)$ et $(n, 1)$; nous en donnons la démonstration, car la constante γ à laquelle il conduit est beaucoup plus précise que celle à laquelle conduit le théorème général.

THÉORÈME. - <u>Si</u> $L = \theta_1 x_1 + \dots + \theta_n x_n - y$ <u>n'admet pas l'approximation</u> $\frac{1}{C} t^{-n}$, <u>alors, pour</u> $\nu = 1, \dots, n$, <u>le système des formes</u> $M_\nu = \theta_\nu u - v_\nu$ <u>n'admet pas l'approximation</u> $\frac{1}{Cn} t^{-1/n}$.

<u>Démonstration.</u> - Nous supposons donc que, $\forall$ x tel que $\boxed{x} > A$, on ait $|L| \geqslant \frac{1}{C} \boxed{x}^{-n}$. Soit alors un système $(u, v_1, \dots, v_n)$ tel que $u > \{A(A+1)\}^n$.

Le système aux variables $x_1, \dots, x_n, y$

$$|x_1 \frac{v_1}{u} + x_2 \frac{v_2}{u} + \dots + x_n \frac{v_n}{u} - y| < t^{-n}$$

admet, d'après le théorème de Kronecker, une solution, quel que soit $t \geqslant 1$, telle que $1 \leqslant \boxed{x} \leqslant t$.

Nous prendrons $t^{-n} = u^{-1}$, soit $t = u^{1/n}$.

On a alors

$$|x_1 \frac{v_1}{u} + \dots + x_n \frac{v_n}{u} - y| < \frac{1}{u} \quad ,$$

soit

$$x_1 v_1 + \dots + x_n v_n - uy = 0 \quad ,$$

avec $1 \leqslant \boxed{x} \leqslant u^{1/n}$.

Mais si $\boxed{x} \leqslant A$, alors si

$$x'_\nu = (A+1)\, x_\nu \ , \quad y' = (A+1)\, y$$

on a encore

$$x'_1 v_1 + \dots + x'_n v_n - uy' = 0 \quad ,$$

avec

$$A < \boxed{x'} \leqslant A(A+1) \leqslant u^{1/n} \quad .$$

Le système $x_1 v_1 + \dots + x_n v_n - uy = 0$ admet donc toujours une solution avec

$$A < \lceil x \rceil \leqslant u^{1/n} \quad .$$

Mais on a alors

$$x_1 M_1 + \dots + x_n M_n = uL \quad ;$$

soit

$$|u|\,|L| \leqslant n \lceil x \rceil \max_\nu |M_\nu| \quad .$$

Comme $\lceil x \rceil > A$,

$$|L| \geqslant \frac{1}{C} \lceil x \rceil^{-n} \quad ,$$

d'où

$$\max_\nu |M_\nu| \geqslant \frac{u|L|}{n\lceil x \rceil} \geqslant \frac{u}{nC} \frac{1}{\lceil x \rceil^{n+1}} \geqslant \frac{u}{nC} \frac{1}{u^{1+1/n}} \geqslant \frac{1}{nC} u^{-1/n} \quad .$$

Ce théorème nous permet ainsi de passer des résultats sur la signature $(1 , n)$ aux résultats sur la signature $(n , 1)$; il est obtenu en appliquant le principe des tiroirs.

3.2. Théorème de Minkowski. - On pose $C_n = \sup C$, la borne supérieure étant prise sur les constantes C telles que le système des n formes $M_\nu = \theta_\nu u - v_\nu$ admette l'approximation $\frac{1}{C} t^{-1/n}$ quels que soient les nombres θ_ν . Un résultat d'Hurwitz donne $C_1 = \sqrt{5}$; on a d'autre part $C_2 \geqslant \sqrt{19/8}$ (MINKOWSKI). Le théorème de Kronecker montre que l'on a toujours $C_n \geqslant 1$. La théorie des fractions continues permet alors d'en déduire simplement que $C_1 \geqslant 2$. En généralisant cette méthode, on peut alors donner pour C_n une borne inférieure meilleure que 1.

Nous allons montrer le résultat de Minkowski : $C_n \geqslant 1 + 1/n$.

Démonstration. - Nous allons montrer que, quels que soient $\theta_1 , \dots , \theta_n$ le système :

$$\max_\nu |M_\nu| \leqslant \frac{n}{n+1} u^{-1/n} \quad \text{avec} \quad M_\nu = u\theta_\nu - v_\nu \quad ,$$

admet une infinité de solutions en entiers u et v_ν .

Nous supposons irrationnel l'un au moins des θ_ν , sinon le théorème est évident.

Soit $t > 1$. Considérons le domaine de R^{n+1} défini par les inégalités

$$\text{pour} \quad \nu = 1 , \dots , n \qquad t^{-n}|x_0| + t|\theta_\nu x_0 - x_\nu| \leqslant (n+1)^{1/n+1} = \delta \quad .$$

C'est un domaine convexe, fermé, symétrique par rapport à l'origine.

Calculons son volume V . Pour cela, nous effectuons la transformation linéaire

$$\begin{cases} z_0 = t^{-n} x_0 \\ z_\nu = t(\theta_\nu x_0 - x_\nu) \qquad \nu \geqslant 1 \end{cases} ,$$

de déterminant $(-1)^n$ qui n'affecte pas les volumes.

Le domaine devient alors le domaine défini par $|z_0| + |z_\nu| \leqslant \delta$ pour $\nu = 1 , \dots , n$, dont le volume est alors

$$V = 2 \int_0^\delta 2^n (\delta - x)^n \, dx$$

(en coupant par les plans $z_0 = \pm x$, on a des régions $|z_\nu| \leqslant \delta - x$ de volume $2^n(\delta - x)^n$).

En intégrant on obtient donc $V = 2^{n+1}$.

Le domaine contient donc un point à coordonnées entières distinct de l'origine quel que soit $t > 1$, soit $x_0 = u$, $x_\nu = v_\nu$ pour $\nu \geqslant 1$.

Supposons $t > \delta$; alors u n'est pas nul, sinon on aurait $t|v_\nu| \leqslant \delta$. Soit $v_\nu = 0$ pour $\nu \geqslant 1$ le point ne serait pas distinct de l'origine.

D'autre part, en prenant des valeurs de t suffisamment grandes on va pouvoir obtenir des valeurs pour u arbitrairement grandes. En effet, si θ_1 par exemple est irrationnel, et si l'on suppose que $1 \leqslant |u| \leqslant A$, alors $|\theta_1 u - v_1|$ admet un minimum ρ strictement positif. Il suffit alors de prendre $t > \delta/\rho$ pour que $|u| > A$.

Mais, si

$$t^{-n}|u| + t|\theta_\nu u - v_\nu| \leqslant \delta \quad ,$$

en écrivant

$$t|\theta_\nu u - v_\nu| = \underbrace{n^{-1} t|\theta_\nu u - v_\nu| + n^{-1} t|\theta_\nu u - v_\nu| + \dots + n^{-1} t|\theta_\nu u - v_\nu|}_{n \text{ termes égaux}} \quad ,$$

et en appliquant aux $n + 1$ termes du premier membre l'inégalité de la somme et de la moyenne géométrique soit

$$(\alpha_0\ \alpha_1 \dots \alpha_n)^{1/(n+1)} \leqslant \frac{\alpha_0 + \dots + \alpha_n}{n + 1} \quad ,$$

on obtient, pour $\nu = 1 , \dots , n$

$$(n + 1)\ |u|^{1/(n+1)}\ (n^{-1}|\theta_\nu\ u - v_\nu|)^{n/(n+1)} \leqslant (n + 1)^{1/(n+1)} \quad ,$$

soit

$$(n + 1)^{n+1}\ |u|\ (n^{-1}|\theta_\nu\ u - v_\nu|)^n \leqslant (n + 1)$$

$$\frac{n + 1}{n}\ |u|^{1/n}\ |\theta_\nu\ u - v_\nu| \leqslant 1 \quad .$$

Donc, il existe des u arbitrairement grands tels que

$$\max_\nu |M_\nu| \leqslant \frac{n}{n + 1}\ |u|^{1/n} \quad .$$

C. Q. F. D.

Des améliorations dans le cas général du théorème de Minkowski ont été fourni par BLICHFELDT [1] qui a montré que

$$C_n \geqslant \frac{n + 1}{n}\ \{1 + (\frac{n - 1}{n + 1})^{n+3}\}^{1/n} \quad .$$

Toutes ces constantes tendent vers 1 quand $n \to \infty$.

En outre il est possible de donner une idée sur la densité de u permettant l'approximation (voir toujours BLICHFELDT) et de donner des théorèmes analogues dans l'approximation de nombres complexes par des entiers d'un corps complexe (voir MINKOWSKI [8]).

3.3. Nous allons maintenant nous intéresser aux bornes supérieures des quantités C_n . - Il s'agit cette fois de fournir des systèmes particuliers de nombres θ_ν $(\nu = 1 , 2 , \dots , n)$ qui n'admettent pas d'approximation en $\frac{1}{C}\ t^{-1/n}$.

En utilisant le principe de transfert, un résultat dû à PERRON donne $C_n \leqslant \sigma n$ (PERRON [9]) avec

$$\sigma = \prod_{\mu=1}^{n}\ \sum_{\nu=1}^{n}\ |\theta_\nu^{(\mu)} - \theta_\nu| \quad ,$$

$\theta_1 , \ldots , \theta_n$ étant des entiers algébriques réels d'un corps K de degré $n+1$, tels que le système $1 , \theta_1 , \ldots , \theta_n$ soit libre sur le corps des rationnels, $\theta_\nu^{(\mu)}$ les conjugués de θ_ν dans les corps $K^{(\mu)}$ conjugués de K.

La démonstration est très voisine de celle que nous avons donnée en 2.3.

FURTWÄNGLER [4] a généralisé ce résultat dans le théorème suivant :

Si D_n est le discriminant d'un corps de nombres réels de degré $n+1$, on a alors $C_n \leqslant \sqrt[2n]{|D_n|}$. On en déduit alors

$$C_2 \leqslant \sqrt[4]{23} , \quad C_n \leqslant \sqrt[2n]{n+1}\,\sqrt{2(n+1)} .$$

De meilleures valeurs peuvent être obtenues pour n fixé à l'aide de machines ; cependant $\sqrt[4]{23}$ est la meilleure valeur possible avec ce procédé. Remarquons que les bornes supérieures de C_n tendent toutes vers l'infini avec n.

Signalons enfin que le résultat de FURTWÄNGLER peut également s'étendre au cas d'approximations dans des corps complexes (voir HOFREITER [5]).

3.4. Signature (1.2). - Des résultats très précis ont été obtenus qui feront l'objet d'un autre exposé.

4. Systèmes réguliers et systèmes singuliers.

4.1. Définition. - Nous dirons que le système

$$u_\mu = \sum_{\nu=1}^{n} \theta_{\mu\nu}\, x_\nu \qquad \mu = 1 , \ldots , m$$

est un système singulier si, pour tout $\varepsilon > 0$, il existe t_0 tel que

$$\forall \quad t > t_0 , \ \exists \quad x \neq 0 , \qquad \lceil x \rceil \leqslant t , \qquad \max \|u_\mu(x)\| < \varepsilon t^{-n/m} .$$

Ce qui entraîne que toute fonction $\varphi(t) = o(t^{-n/m})$ est fonction d'approximation pour le système. Mais réciproquement s'il en est ainsi le système n'est pas nécessairement singulier. Par exemple, nous verrons que quelle que soit la fonction d'approximation $\varphi(t)$, il existe un nombre irrationnel θ tel que $\|x\theta\|$ admette $\varphi(t)$ comme approximation. Or, si θ est irrationnel, $\|x\theta\|$ est toujours un

<u>système régulier</u> c'est-à-dire n'est pas un système singulier : en effet, soit q_n la n-ième "meilleure approximation" de θ.

Soit $t = q_{n+1} - 1$; alors, si $1 \leqslant x \leqslant t$, on a

$$\|x\theta\| \geqslant \|q_n \theta\| \quad ,$$

et

$$q_{n+1} \|q_n \theta\| > \frac{1}{2} \quad ,$$

donc

$$\|x\theta\| \geqslant \frac{1}{2(t+1)} \quad .$$

Il n'est donc pas possible de prendre $\varepsilon < 1/2$, $\|x\theta\|$ est toujours régulier.

4.2. <u>Justification de la définition</u>. - Nous allons voir que <u>l'ensemble des systèmes singuliers de signature</u> (m, n) <u>est de mesure nulle</u> (mesure de l'ensemble des $\theta_{\mu\nu}$ considérés comme les coordonnées d'un point de R^{mn}).

<u>Démonstration</u>. - Nous pouvons nous borner à considérer les systèmes tels que $0 \leqslant \theta_{\mu\nu} < 1$ (l'ensemble des pavés ainsi constitués dans R^{mn}, étant dénombrable).

Considérons alors les systèmes tels que $\exists\ x \neq 0$ $\boxed{x} \leqslant t$, $\max \|u_\mu(x)\| < \varepsilon t^{-n/m}$, ε et t étant donnés. Soit $\mathcal{E}(\varepsilon, t)$ un tel ensemble de système.

x étant donné non nul, soit $x_{\nu_0} \neq 0$, et les $\theta_{\mu\nu}$ étant donnés pour $\nu \neq \nu_0$, la condition précédente impose que chacun des $\theta_{\mu\nu_0}$ se déplace dans un intervalle de longueur au plus $2\varepsilon t^{-n/m}$.

D'autre part, chacun des $\theta_{\mu\nu}$, pour $\nu \neq \nu_0$, se déplace dans un intervalle de longueur au plus 1 par hypothèse. Donc x étant donné le système $\theta_{\mu\nu}$ est contenu dans un ensemble de mesure au plus $(2\varepsilon t^{-n/m})^m$.

Mais, t étant donné, il y a au plus si $t \geqslant 1$, $(2t+1)^n \leqslant (3t)^n$ valeurs possibles pour x telles que $\boxed{x} \leqslant t$. Finalement les $\theta_{\mu\nu}$ tels que $\exists\ x \neq 0$, $\boxed{x} \leqslant t$, $\max \|u_\mu(x)\| < \varepsilon t^{-n/m}$ se trouvent dans un ensemble de mesures au plus $3^n 2^m \varepsilon^m$; c'est-à-dire que : $\operatorname{mes} \mathcal{E}(\varepsilon, t) \leqslant 3^n 2^m \varepsilon^m$.
Soit alors $\mathcal{E}(\varepsilon)$ l'ensemble des systèmes $\theta_{\mu\nu}$ tels que $\exists\ t_0 \geqslant 1$ avec

$$\forall\ t \geqslant t_0\ ,\ \exists\ x \neq 0\ ,\ \boxed{x} \leqslant t\ ,\ \max \|u_\mu(x)\| < \varepsilon t^{-n/m} \quad .$$

On a

$$\mathcal{E}(\varepsilon) = \bigcup_{t_0 \geq 1} \left(\bigcap_{t \geq t_0} \mathcal{E}(\varepsilon , t) \right) .$$

Or si $t_0 \geq t_0'$,

$$\bigcap_{t \geq t_0'} \mathcal{E}(\varepsilon , t) \subset \bigcap_{t \geq t_0} \mathcal{E}(\varepsilon , t) .$$

Donc

$$\text{mes } \mathcal{E}(\varepsilon) = \lim_{t_0 \to \infty} \text{mes } \bigcap_{t \geq t_0} \mathcal{E}(\varepsilon , t) .$$

Mais

$$\text{mes } \bigcap_{t \geq t_0} \mathcal{E}(\varepsilon , t) \leqslant \text{mes } \mathcal{E}(\varepsilon , t_0) \leqslant 2^m 3^n \varepsilon^m .$$

Donc

$$\text{mes } \mathcal{E}(\varepsilon) \leqslant 2^m 3^n \varepsilon^m .$$

L'ensemble des systèmes singuliers intersection de tous les ensembles $\mathcal{E}(\varepsilon)$ est donc bien de mesure nulle puisque $2^m 3^n \varepsilon^m \to 0$ quand $\varepsilon \to 0$.

4.3. Transfert. - Le théorème que nous avons déjà cité en 3.1 montre que si L est un système singulier, alors son transposé est également un système singulier, et réciproquement.

Un autre théorème de transfert au cas non homogène prouve alors que la condition nécessaire et suffisante pour que le système $\sum_{\nu=1}^{n} \theta_{\mu\nu} x_\nu$ $(\mu = 1 , \ldots , m)$ soit régulier est qu'il existe un nombre $\delta > 0$ tel que

$$\max_{\mu} \left\| \sum_{\nu} \theta_{\mu\nu} x_\nu - \alpha_\mu \right\| < \delta \overline{|x|}^{-n}$$

ait une infinité de solutions quel que soit α réel. (Voir CASSELS [3]).

4.4. Rang de linéarité. - Nous dirons qu'un système de nombres θ_ν , $\nu = 1 , \ldots , n$, est de rang m s'il existe m nombres $\theta_{\nu_1} , \ldots , \theta_{\nu_m}$ tels que

$$x_1\,\theta_{\nu_1} + x_2\,\theta_{\nu_2} + \cdots + x_m\,\theta_{\nu_m} + y = 0$$

avec $x_1 , \cdots , x_m , y$ entiers rationnels, n'est possible qu'avec $x_1 = x_2 = \cdots = x_m = y = 0$, et s'il n'en n'existe pas $m + 1$.

Si alors, $\theta_1 , \cdots , \theta_n$ est de rang $m < n$, le système est singulier. Plus précisément le système $\theta_\nu u - v_\nu$ admet l'approximation $1/t^{1/m}$. (Voir, par exemple, PERRON [10]).

Le problème intéressant est donc de trouver des systèmes, de rang n exactement, qui soient singuliers; nous avons vu que cela n'est pas possible pour $n = 1$. Cela le devient pour $n > 1$ comme le prouve le théorème suivant dû à KHINČIN (généralisable à des signatures quelconques autres que $(1 , 1)$.

4.5. Quelle que soit la fonction $\omega(t) > 0$, il existe θ_1 et θ_2 tels que

(A) : $\forall\ t \geqslant 1 ,\ \exists\ x \neq 0 ,\ \lceil x \rceil \leqslant t ,\quad \| x_1\,\theta_1 + x_2\,\theta_2 \| < \omega(t)$;

(B) : $\forall\ x \neq 0 ,\quad \| x_1\,\theta_1 + x_2\,\theta_2 \| > 0$. (Voir démonstration dans CASSELS [3].)

4.6. Existence de systèmes admettant des fonctions d'approximations données. - Un théorème dû à PERRON [9], montre que quelle que soit la fonction $\varphi(t) > 0$, il existe des systèmes $M_\nu = u\theta_\nu - v_\nu$ $(\nu = 1 , \cdots , n)$ non triviaux, c'est-à-dire, de rang de linéarité n admettant l'approximation $\varphi(t)$.

Pour cela, posons

$$\theta_\nu = \sum_{\lambda=1}^{\infty} \frac{\nu^\lambda}{g_1 \cdots g_\lambda} \quad \text{avec } g_1 > n ,\ g_\lambda \text{ entier strictement croissant ,}$$

$$\text{et} \quad g_{\lambda+1} > n + \frac{n^{\lambda+1}}{\varphi(g_1 \cdots g_\lambda)} \quad .$$

Le reste $R_\lambda^{(\nu)}$ de cette série est

$$R_\lambda^{(\nu)} = \sum_{\mu=\lambda+1}^{\infty} \frac{\nu^\mu}{g_1 \cdots g_\mu}$$

d'où

$$\frac{\nu^{\lambda+1}}{g_1 \cdots g_{\lambda+1}} < R_\lambda^{(\nu)} < \frac{\nu^{\lambda+1}}{g_1 \cdots g_{\lambda+1}} \left(1 + \frac{\nu}{g_{\lambda+2}} + \frac{\nu^2}{g_{\lambda+2}\, g_{\lambda+3}} + \cdots\right) .$$

En majorant chacun des termes de la série par $\dfrac{\nu^k}{g_{\lambda+1}^k}$, et en sommant la progression géométrique ainsi obtenue, on obtient :

$$\frac{\nu^{\lambda+1}}{g_1 \cdots g_\lambda} \frac{1}{g_{\lambda+1}} < R_\lambda^{(\nu)} < \frac{\nu^{\lambda+1}}{g_1 \cdots g_\lambda} \frac{1}{g_{\lambda+1} - \nu} .$$

Posons alors

$$u = g_1 \cdots g_\lambda , \qquad v_\nu = \sum_{\mu=1}^{\lambda} \frac{\nu^\mu}{g_1 \cdots g_\mu} \times (g_1 \cdots g_\lambda) .$$

On a

$$M_\nu = R_\lambda^{(\nu)} \times g_1 \cdots g_\lambda ,$$

donc

$$|M_\nu| < \frac{\nu^{\lambda+1}}{g_{\lambda+1} - \nu} .$$

Or

$$g_{\lambda+1} - n > \frac{n^{\lambda+1}}{\varphi(z_1 \cdots z_\lambda)}$$

donc, on a bien

$$|M_\nu| < \varphi(u) .$$

Il reste à montrer maintenant que le rang de linéarité est n .

Soit une relation $x_1 \theta_1 + \cdots + x_n \theta_n + y = 0$. En multipliant les deux membres par $g_1 \cdots g_\lambda$, on obtient alors

$$x_1\, g_1 \cdots g_\lambda R_\lambda^{(1)} + \cdots + x_n\, g_1 \cdots g_\lambda R_\lambda^{(n)} = \text{entier} .$$

Mais la quantité du premier membre est inférieure à

$$\lceil x \rceil \frac{n^{\lambda+2}}{g_{\lambda+1} - n} < n \lceil x \rceil \varphi(g_1 \ldots g_\lambda) \quad .$$

A condition que $\varphi(t)$ tende vers 0 quand $t \to \infty$, ce que l'on peut évidemment toujours supposer, cette quantité est inférieure à 1 en module à partir d'un certain λ, donc nulle.

On a donc

$$x_1 R_\lambda^{(1)} + \ldots + x_n R_\lambda^{(n)} = 0 \qquad \text{dès que} \quad \lambda > \lambda_0 \quad .$$

Soit x_p le x de plus grand indice non nul.

$$x_1 R_\lambda^{(1)} + \ldots + x_p R_\lambda^{(p)} = 0 \, , \qquad x_p \neq 0 \quad .$$

On a

$$|x_p R_\lambda^{(p)}| > \frac{p^{\lambda+1}}{g_1 \ldots g_\lambda} \frac{1}{g_{\lambda+1}}$$

et

$$|x_1 R_\lambda^{(1)} + \ldots + x_{p-1} R_\lambda^{(p-1)}| < \lceil x \rceil \frac{(p-1)^{\lambda+2}}{g_1 \ldots g_\lambda(g_{\lambda+1} - (p-1))} \quad ,$$

dès que λ est assez grand

$$g_{\lambda+1} - (p-1) > (1/2) \; g_{\lambda+1} \quad .$$

Donc

$$|x_1 R_\lambda^{(1)} + \ldots + x_{p-1} R_\lambda^{(p-1)}| < 2\lceil x \rceil \frac{(p-1)^{\lambda+2}}{g_1 \ldots g_{\lambda+1}} < 2\lceil x \rceil \frac{(p-1)^{\lambda+2}}{p^{\lambda+1}} |x_p R_\lambda^{(p)}| \quad .$$

Comme $\dfrac{(p-1)^{\lambda+2}}{p^{\lambda+1}} \to 0$ quand $\lambda \to \infty$, à partir d'un certain rang $\lambda > \lambda_1$, on aurait :

$$|x_1 R_\lambda^{(1)} + \ldots + x_{p-1} R_\lambda^{(p-1)}| < |x_p R_\lambda^{(p)}| \quad ,$$

ce qui est en contradiction avec l'égalité écrite.

JARNIK [6] a donné des résultats beaucoup plus précis par exemple :

Si $\Omega \geqslant \frac{1}{n}$, il existe des systèmes $M_\nu = u\theta_\nu - v_\lambda$ qui admettent l'approximation $\frac{2}{t^\Omega}$, mais qui n'admettent pas l'approximation $\frac{1}{t^\Omega \operatorname{Log}^2 t}$.

BIBLIOGRAPHIE

[1] BLICHFELDT (H. F.). - A new principle in the geometry of numbers with some applications, Trans. Amer. math. Soc., t. 15, 1914, p. 227-235.

[2] BOREL (Emile). - Contribution à l'analyse arithmétique du continu, J. Math. pures et appl., Série 5, t. 9, 1903, p. 329-375.

[3] CASSELS (J. W. S.). - An introduction to diophantine approximation. - Cambridge, at the University Press, 1957 (Cambridge Tracts in Math. and math. Physics, 45).

[4] FÜRTWANGLER (P.). - Über die simultane Approximation von Irrationalzahlen, I., Math. Annalen, t. 96, 1927, p. 169-175 ; II., Math. Annalen, t. 99, 1928, p. 71-83.

[5] HOFREITER (Nicolas). - Über die Approximation von komplexen Zahlen, Monatsh. für Math. und Phys., t. 42, 1935, p. 401-416.

[6] JARNIK (V.). - Ein Existenzsatz aus der Theorie der diophantischen Approximationen, Prace mat.-fiz., t. 39, 1932, p. 135-144.

[7] KOKSMA (J. F.). - Diophantische Approximationen. - Berlin, J. Springer, 1936 (Ergebnisse der Mathematik, 4).

[8] MINKOWSKI (Hermann). - Geometrie der Zahlen, 1. Lieferung. - New-York, Chelsea publisching Company, 1953.

[9] PERRON (Oskar). - Über diophantische Approximationen, Math. Annalen, t. 83, 1921, p. 77-84.

[10] PERRON (Oskar). - Irrationalzahlen, 2te Auflage. - New-York, Chelsea publishing Company, 1948.

[11] PISOT (Charles). - Quelques résultats d'approximation diophantienne, Colloques internationaux du C. N. R. S. : Algèbre et théorie des nombres [24. 1949. Paris] ; p. 57-58. - Paris, Centre national de la Recherche scientifique, 1950.

[12] SIEGEL (C.). - Über den Thueschen Satz, Krist. Vid. Selsk. Skr., t. 1, 1921, n° 16, 12 p.

[13] SZÜSZ (P.). - Über die Approximation einer reellen Zahl durch Brüche, Acta Math. Acad. Scient. Hungar, t. 10, 1959, p. 69-75.