UNIVERSITÉ PARIS XI

U.E.R. MATHÉMATIQUE

91405 ORSAY FRANCE

N° 57

Michel WALDSCHMIDT

Séminaire sur les nombres transcendants

1972-1973

Publication mathématique d'Orsay

SEMINAIRE SUR LES NOMBRES TRANSCENDANTS

1972-1973

exposés :

Théorème de Lindemann-Weierstrass

Alain MACADRE
(Orsay 6 mars 1973)

I - Contexte historique

En 1748 Euler conjecture l'existence de nombres transcendants en considérant les logarithmes de nombres rationnels.

En 1844 Liouville donne une propriété des nombres transcendants et en montre l'existence.

En 1873 Hermite montre que e est transcendants par une nouvelle méthode indépendante des travaux de Liouville.

En 1882 Lindemann, en utilisant cette méthode, montre que si α est algébrique non nul, alors e^{α} est transcendant ; donc que π est transcendant.

En 1885 Weierstrass améliore le théorème de Lindemann et montre que si $b_1, b_2, \ldots, b_n$ sont des nombres algébriques distincts, alors $e^{b_1}, e^{b_2}, \ldots, e^{b_n}$ sont linéairement indépendants sur les nombres algébriques.

Ce théorème est équivalent au théorème suivant

Théorème : Soient $\alpha_1, \ldots, \alpha_s$ des nombres algébriques, $\mathbb{Q}$-linéairement indépendants. Alors $e^{\alpha_1}, \ldots, e^{\alpha_s}$ sont algébriquement indépendants.

La démonstration de Lindemann Weierstrass a été améliorée par Siegel et c'est cette démonstration que nous allons exposer.

II - Notations et rappels

1) Si K est un corps de nombres (i.e. une extension algébrique de $\mathbb{Q}$) on note par I_K l'anneau des entiers algébriques de K.

2) Soit $a \in K$. On appelle dénominateur de a un entier naturel d tel que $da \in I_K$. Soit $d(a)$ le plus petit dénominateur de a et soient $\sigma_1 \ldots \sigma_n$ (si $n = [K:\mathbb{Q}]$) les plongements de K dans C. On note

$$\|a\| = \max_{i=1,\ldots n} |\sigma_i(a)|$$

$$\text{taille } a = t(a) = \max[\operatorname{Log} \|a\| , \log d(a)] .$$

La taille vérifie l'inégalité suivante :

$$-[K:\mathbb{Q}] \operatorname{Log} d(a) - ([K:\mathbb{Q}]-1)t(a) \leqslant \operatorname{Log}|\sigma_i(a)| \qquad \text{(Ref (1)(2))} .$$

3) Si $P \in K[X]$ on note par $\|P\|$ le maximum des valeurs absolues des coefficients et de leurs conjugués de P.

4) Lemme de Siegel. Il existe une constante $c_k > 0$ ayant la propriété suivante :

Soient r et n deux entiers $n > r \geqslant 1$ et a_{ij} $(1 \leqslant i \leqslant r , 1 \leqslant j \leqslant n)$ des éléments de K. Soit d_i $(1 \leqslant i \leqslant r)$ un dénominateur commun positif de a_{ij} pour $1 \leqslant j \leqslant n$; soit $d = \max\limits_{1\leqslant i\leqslant r} d_i$ et $A = \max\limits_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant n}} \|a_{ij}\|$.

Alors il existe n éléments $x_1,\ldots,x_n$ de K entiers sur Z non tous nuls, tels que

$$\sum_{j=1}^{n} a_{ij}\, x_j = 0 \qquad \text{pour } 1 \leqslant i \leqslant r$$

et

$$\max_{j=1,\ldots n} \|x_j\| \leqslant c_K + c_K(c_K\, ndA)^{\frac{r}{n-r}} \qquad \text{(Ref (1) ou (4))} .$$

5) Domination. Soient P et Q deux polynômes à une variable

$$P = \Sigma\, a_{(\nu)} z^{\nu} \qquad \text{où} \quad a_{\nu} \in \mathbb{C}$$

$$Q = \Sigma\, b_{\mu}\, z^{\mu} \qquad \text{avec} \quad b_{\mu} \text{ réel} \geqslant 0 .$$

On dit que Q domine P et on note

$$P < Q$$

si pour tout (ν) on a $|a_{\nu}| < b_{(\nu)}$.

Une propriété est que $DP < DQ$ où D est la dérivation. (Ref (1))

III - Démonstration

Rappelons tout d'abord le théorème à démontrer

Théorème de L.W : Soient $\alpha_1,\ldots,\alpha_s$ des nombres algébriques, $\mathbb{Q}$-linéairement indépendants. Alors $e^{\alpha_1},\ldots,e^{\alpha_s}$ sont algébriquement indépendants.

Le point essentiel de la démonstration que nous allons donner est de montrer le lemme suivant :

Lemme fondamental : Si K est un corps de nombres, si $\beta_1,\ldots,\beta_m$ sont des éléments de K^* tous distincts et si $\alpha \in K^*$, alors le rang de

$$e^{\alpha\beta_1},\ldots,e^{\alpha\beta_m}$$

sur K est $\geqslant \frac{m}{2[K:\mathbb{Q}]}$.

Ce lemme est suffisant. En effet

A) Nous allons supposer démontré tout d'abord ce lemme fondamental et montrer comment le théorème de L.W. s'en déduit.

Soit $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_s)$.

Posons $f_1(\nu) = e^{\alpha_1\nu},\ldots,f_s(t) = e^{\alpha_s t}$.

Supposons que le théorème de L.W. ne soit pas vrai. Alors il existe un polynôme g, à coefficients dans K, non tous nuls, de degré d tel que l'on ait

$$g(f_1(\alpha),\ldots,f_s(\alpha)) = 0$$

pour $\alpha = 1$.

Le nombre de monômes

$$f_1^{\nu_1}\ldots f_s^{\nu_s} \quad \text{avec} \quad \nu_1+\ldots+\nu_s \in \nu$$

est $m_\nu = \Gamma_{s+1}^{\nu} = C_{\nu+s}^{\nu}$.

Or $f_1^{\nu_1}\dots f_s^{\nu_s} = e^{(\nu_1\alpha_1+\dots+\nu_s d_s)t}$

et on peut prendre pour $\beta_1,\dots,\beta_m$ les combinaisons linéaires $\nu_1\alpha_1+\dots+\nu_s\alpha_s$ avec $\nu_1+\dots+\nu_s \leqslant \nu$ où ν est un nombre que l'on prendra suffisamment grand. (On a donc $m = m_\nu$).

Mais si $g(f_1(\alpha),\dots,f_s(\alpha)) = 0$ on a aussi

$$f_1^{\mu_1}(\alpha)\dots f_s^{\mu_s}(\alpha) . g(f_1(\alpha),\dots,f_s(\alpha)) = 0 \quad \text{pour} \quad \mu_1+\dots+\mu_s \leqslant \nu-d .$$

On obtient ainsi $m_{\nu-d}$ relations pour les

$$m_\nu \text{ nombres } f_1^{\nu_1}(\alpha)\dots f_s^{\nu_s}(\alpha) \quad (\nu_1+\dots+\nu_s \leqslant \nu) .$$

Ces relations sont évidemment indépendantes puisque entre deux relations distinctes, les monômes ne sont pas tous les mêmes.

D'après le lemme fondamental, on doit avoir

$$m_\nu - m_{\nu-d} \geqslant \frac{m_\nu}{2[K:\mathbb{Q}]}$$

ce qui donne après division par m_ν

$$1 - \frac{1}{2[K:\mathbb{Q}]} \geqslant \frac{m_{\nu-d}}{m_\nu} .$$

Or $$\frac{m_{\nu-d}}{m_\nu} = \frac{\nu(\nu-1)\dots(\nu-d+1)}{(\nu+1)(\nu+s-1)\dots(\nu+s-d+1)}$$

que l'on peut rendre aussi proche que l'on veut de 1 en prenant ν assez grand . D'où une contradiction. Le polynôme g n'existe donc pas et le théorème de L.W. est démontré.

Il nous suffit donc de démontrer le lemme fondamental.

B) <u>Démonstration du lemme fondamental</u>.

La démonstration se fait en plusieurs pas.

Dans toute la suite, nous noterons

$$E_j(z) = e^{\beta_j z}$$

nous considérerons m comme donné évidemment et n comme un paramètre. Les constantes c, c_1, c_2 dépendent ainsi de β_j et m.

<u>1er pas</u> : On construit une nouvelle fonction

$$F_1(z) = P_1(z)F_1(z)+\ldots+P_m(z)F_m(z)$$

où $P_1,\ldots,P_m$ sont des polynômes à coefficients dans I_K et telle que F_1 ait un zéro d'ordre élevé au point $z=0$.

Plus précisément nous allons montrer le

<u>Lemme 1</u> : Etant donné l'entier $n > 0$, on peut trouver des polynômes $P_j \in I_K[z]$ non tous nuls tels que

(i) $d^o P_j < 2n$ et $\|P_j\| \leqslant c^n n^{2n}$

(ii) la fonction F_1 a un zéro d'ordre $\geqslant (2m-1)n$ en 0

(iii) si $$F_1(z) = \sum_{\nu=0}^{\infty} a_\nu \frac{z^\nu}{\nu!}$$

alors $|a_\nu| < c^\nu c^n n^{2n}$.

Posons $P_j(z) = p_{j,0} + p_{j,1}z + \ldots + p_{j,2n-1}z^{2n-1}$.

Nous avons $2n.m$ inconnues qui sont les $p_{j\mu}$.

D'autre part ou doit avoir

$$a_\nu = 0 \quad \text{pour} \quad \nu = 0, 1, \ldots, (2m-1)n-1$$

ce qui donne $(2m-1)n$ équations.

Ecrivons ces équations. Nous désignerons par Γ le cercle de centre 0 et de rayon 1 parcouru dans le sens positif. On a

$$\frac{a_\nu}{\nu!} = \frac{1}{2i\pi}\int_\Gamma \frac{F_1(z)}{z^{\nu+1}}\,dz = \sum_{\substack{j=0,1,\dots m\\ \mu=0,1,\dots m-1}} \left[p_{j\mu}\left(\frac{1}{2i\pi}\int_\Gamma z^{\mu-\nu-1}\,e^{\beta_j . z}dz\right)\right] .$$

D'où

$$\sum_{\substack{j=0,1\dots m\\ \mu=0,1\dots 2n-1}} p_{j\mu}\, c_{j,\mu,\nu} = 0 \qquad \text{pour } \nu = 0,1\dots,(2m-1)n-1$$

où $c_{j,\mu,\nu} = \begin{cases} 0 & \text{si } \nu-\mu < 0 \\ \dfrac{\beta_j^{\nu-\mu}}{(\nu-\mu)!} & \text{sinon} \end{cases}$

On a donc $c_{j,\mu,\nu} \in K$ et l'on voit que

$$\operatorname*{Max}_{j,\mu,\nu} |c_{j,\mu,\nu}| \leqslant c_1^n .$$

De même un dénominateur des $c_{j,\mu,\nu}$ sera majoré par $c_2^n . n^{2n}$.

Appliquons le lemme de Siegel. On peut trouver les $p_{j,\mu}$ non tous nuls, dans I_K tels que

$$\|p_{j\mu}\| \leqslant c_3^n\, n^{2n} \qquad \text{pour } j = 0,\dots m \text{ et } \mu = 0,1\dots,2n-1 .$$

On a donc

$$\|p_j\| < c_3^n\, n^{2n} .$$

Les coefficients de F_1 vérifient (ref (3))

$$a_\nu = \frac{\nu!}{2i\pi}\int_\Gamma \frac{F_1(z)}{z^{\nu+1}}\,dz$$

(où $a_\nu = 0$ pour $\nu = 0,1\dots,(2m-1)n-1$)

et on obtient encore

$$\sum_{\substack{j=0,\dots,m \\ \mu=0,1\dots(2n-1)}} (\nu!)p_{j\mu}\, c_{j\mu,\nu} = a_\nu$$

mais cette fois ci on n'a plus $\nu < (2m-1)n-1$.

On a $$|\nu!\, c_{j,\mu,\nu}| \leqslant \frac{\beta_j^{\nu-\mu}}{(\nu-\mu)!}.\nu! \leqslant c_1^n\, c_5^\nu .$$

On a donc

$$|a_\nu| < c_4^\nu\, c_5^n\, n^{2n}$$

et pour une certaine constante c on a

$$\|p_j\| \leqslant c^n\, n^{2n} \quad \text{et} \quad |a_j| \leqslant c^\nu\, c^n\, n^{2n}$$

<u>2è pas</u> : Au premier pas on a obtenu une forme linéaire $F_i(z)$ avec des polynômes en z qui approche zéro. Dans ce deuxième pas on va obtenir d'autres formes d'approximation en dérivant. Et ces formes vont être indépendantes.

Plus précisément démontrons le

<u>Lemme</u> 2 : Soient les E_j, P_j, F_1 définis au premier pas. Soit $F_{k+1} = D^k F_1$ (où D est la dérivation) (et $k = 1, 2,\dots$).

Posant $F_k = P_{k,1}\, E_1 + \dots + P_{k,m}\, E_m$ où les P_{kj} sont des polynômes. Alors le rang de la matrice $(P_{k,j})$ $(k,j = 1, 2,\dots m)$ est égal à m .

Posant $$E = \begin{bmatrix} E_1 \\ \vdots \\ E_m \end{bmatrix} \quad \text{et} \quad F = \begin{bmatrix} F_1 \\ \vdots \\ F_m \end{bmatrix}$$

On a

$$F = PE \quad \text{où} \quad P = (P_{k,j}) \; (k = j = 1,2\dots m) .$$

On a d'autre part

$$D^k F_1 = (D+\beta_1)^k P_1 . E_1 + \ldots + (D+\beta_m)^k P_m . E_m$$

Ainsi
$$P = \begin{bmatrix} P_1 & \ldots\ldots\ldots & P_m \\ (D+\beta_1)P_1 & \ldots\ldots\ldots & (D+\beta_m)P_m \\ (D+\beta_1)^{m-1}P_1 & \ldots\ldots & (D+\beta_m)^{m-1}P_m \end{bmatrix}$$

Soit $\Delta = \det P$.

Appelons $u_1 z^{d_1}, \ldots, u_m z^{d_m}$ les monômes de plus haut degré de respectivement $P_1, \ldots, P_m$.

Alors le terme de plus haut degré de $\Delta(z)$ est

$$\begin{vmatrix} u_1 & \ldots\ldots & u_m \\ \beta_1 u_1 & \ldots\ldots & \beta_m u_m \\ \beta_1^{m-1} u_1 & \ldots\ldots & \beta_m^{m-1} u_m \end{vmatrix} z^{d_1+\ldots+d_m}$$

le terme de plus haut degré peut s'écrire

$$\begin{vmatrix} 1 & \ldots\ldots & 1 \\ \beta_1 & \ldots\ldots & \beta_m \\ \beta_1^{m-1} & \ldots\ldots & \beta_m^{m-1} \end{vmatrix} u_1 u_2 \ldots u_m z^{d_1+\ldots+d_m}$$

Le déterminant qui apparaît dans le coefficient du monôme de plus haut degré est un déterminant de Van der Monde qui n'est pas nul à cause des hypothèses faites sur les β_i .

$\Delta_{(z)}$ a donc son monôme de plus haut degré qui n'est pas nul, donc $\Delta_{(z)} \not\equiv 0$ et le lemme 2 est montré.

<u>3è pas</u> : La matrice $(P_{kj}(z))$ $(k,j = 1,2,\ldots m)$ a pour rang m. Mais pour un nombre quelconque $\xi \neq 0$, la matrice $(P_{k,j}(\xi))$ $(k,j=1,2\ldots m)$ n'a pas obligatoirement pour rang m. Nous allons montrer dans ce troisième pas que si nous prenons suffisamment de dérivées on aura une matrice $(P_{kj}(\xi))$ $(j=1,2\ldots m,\ k=1,2\ldots\ ?)$ de rang m.

Pour cela montrons tout d'abord que

1) Si ξ est un nombre complexe non nul, il ne peut être un zéro de Δ d'ordre $> n$.

En effet on a $d^{o}\Delta \leqslant (2n-1)m$.

Soit $\tilde{P}$ la matrice transposée des mineurs de P.

On a $\tilde{P}\,P = \Delta I$.

Comme $F = PE$, on en déduit que $\Delta E = \tilde{P}F$.

Comme $\operatorname{ord}_o F_j \geqslant (2m-1)n-m$ et comme aucune des composantes de E ne s'annule pour $z = 0$, on en déduit que $\operatorname{ord}_o \Delta \geqslant (2m-1)n-m$.

$\Delta(z)$ est donc un polynôme de plus haut degré $\leqslant (2n-1)m$ et de plus bas degré $\geqslant (2m-1)n-m$.

On en déduit que

$$\operatorname{ord}_\xi \Delta \leqslant (2n-1)m-(2m-1)n+m\ .$$

D'où $\operatorname{ord}_\xi \Delta \leqslant n$ pour $\xi \neq 0$.

2) Le nombre n va nous donner le nombre de dérivées à prendre. Montrons le

<u>Lemme</u> 3 : Pour tout nombre complexe $\xi \neq 0$, la matrice $(P_{kj}(\xi))$ $(k=1,2,\ldots m+n$ et $j=1,2\ldots m)$ a pour rang m.

Soit $P_{(k)} = [P_{k,1} \ldots P_{k,m}]$.

On a donc

$$P_{(k)} = [(D+\beta_1)^{k-1} P_1 \ldots (D+\beta_1)^{k-1} P_m] .$$

Posant

$$D+Q = \begin{bmatrix} (D+\beta_1) & & & 0 \\ & \cdot & \cdot & \\ & & \cdot & \\ 0 & & & (D+\beta_m) \end{bmatrix}$$

on obtient l'égalité

$${}^tP_{(k+1)} = (D+Q)^k \, {}^tP_{(1)} .$$

D'autre part on a $\tilde{P}P = \Delta I = {}^tP . {}^t\tilde{P} = {}^t\tilde{P} . {}^tP$.

Puisque ${}^tP = [({}^tP_{(1)}) \ldots ({}^tP_{(m)})]$

on obtient

$$(D+Q)^{\mu} \, {}^tP = [({}^tP_{(1+\mu)}) \ldots ({}^tP_{m+\mu})] .$$

Soit $r = \mathrm{ord}_{\xi}\Delta$. (Alors $r \leqslant n$).

Appliquons $(D+Q)^r$ à ΔI

$$(D+Q)^r(\Delta I) = (D+Q)^r({}^t\tilde{P} . {}^tP) = \sum_{\mu=0}^{r} C_{\mu}[(D+Q)^{\mu} \, {}^tP]$$

où C_{μ} sont des matrices de polynômes.

Faisant $z = \xi$ on obtient

$$D^r\Delta(\xi)I = \sum_{\mu=0}^{r} C_{\mu}(\xi) . [{}^tP_{(1+\mu)}(\xi) \ldots {}^tP_{(m+\mu)}(\xi)]$$

A gauche on a une matrice scalaire non nulle.

A droite apparaissent les colonnes

$$\begin{bmatrix} P_{k,1}(\xi) \\ \vdots \\ P_{k,m}(\xi) \end{bmatrix}$$

avec $k \leqslant m+r \leqslant m+n$.

Le rang de ces colonnes est par conséquent égal au moins à m et le lemme 3 est montré.

Finalement, dans ce troisième pas nous avons trouvé une matrice $P_{kj}(\xi)$ qui est régulière.

4è pas : Nous allons montrer que les fonctions F_k ne sont pas "trop grandes".

Lemme 4 : Soit $k \leqslant m+n$. Si $n > c(\alpha)$ alors

$$|F_k(\alpha)| \leqslant c_5^n \, n^{3n} \, n^{-(2m-2)n}$$

$$\|P_{kj}(\alpha)\| \leqslant c_5^n \, n^{3n} \quad \text{et} \quad \operatorname{den} P_{kj}(\alpha) \leqslant c_5^n \; .$$

Montrons tout d'abord la première inégalité. Soit $N = (2m-1)n$ et posons

$$G_k(z) = \frac{F_k(z)}{z^{N-k+1}}$$

G_k est une fonction entière.

Choisissons α tel que $|\alpha| < N$. Appliquons le principe du maximum à la fonction G_k sur le cercle de centre 0 et de rayon N . On obtient

$$|G_k(\alpha)| \leqslant |G_k|_N$$

$$|G_k|_N = \left| \frac{(D+\beta_1)^{k-1} P_1(z)}{z^{N-k+1}} \, e^{\beta_1 z} + \dots + \frac{(D+\beta_m)^{k-1} P_m(z)}{z^{N-k+1}} \, e^{\beta_m z} \right| \leqslant$$

$$\leqslant m \, C_{51}^N \, \operatorname*{Max}_j \left| \frac{(D+\beta_j)^{k-1} P_j(z)}{z^{N-k+1}} \right|_N \; .$$

Or

$$\operatorname*{Max}_j \left|\frac{(D+\beta_j)^{k-1}P_j(z)}{z^{N-k+1}}\right|_N \leqslant \frac{2n\ c_{52}^n\ n^n\ \operatorname*{Max}_j \|P_j\|}{N^{N-2n+2-k}}$$

le n^n du numérateur provenant des entiers $(2n-1)(2n-2)\ldots.$ obtenus par dérivation) (ref (3)).

On a donc

$$\operatorname*{Max}_j \left|\frac{(D+\beta_j)^{k-1}P_j(z)}{z^{N-k+1}}\right|_N \leqslant \frac{c_{53}^n\ n_n^{2n}\ n^n}{[(2m-1)n]^{(2m-1)n-2n+2-m-n}}$$

$$\leqslant c_{54}^n\ n^{3n-(2m-2)n} \quad .$$

D'où

$$|F_k(\alpha)| \leqslant c_{55}^n\ n^{3n}\ n^{(2m-2)n}\ |\alpha|^{N-k} \ .$$

Soit

$$|F_k(\alpha)| \leqslant c_{56}^n\ n^{3n}\ n^{-(2m-2)n} \quad .$$

Pour la deuxième inégalité la démonstration se fait par récurrence. On a

$$P_j(z) < c^n\ n^{2n}(1+z)^{2n-1}$$

et par récurrence il est facile de voir que

$$(D+\beta_j)^k P_j < c_{57}^n\ n^{3n}(1+z)^{2n-1} \ .$$

Prenant $z = \alpha$, on obtient : $\|P_{kj}(\alpha)\| \leqslant c_{58}^n\ n^{3n}$.

Pour la troisième égalité, la démonstration se fait aussi par récurrence : on montre que

$$\operatorname{den}(D+\beta_j)^k P_j(z) \leqslant (\operatorname{den}\ \beta_j)^k \operatorname{den}\ P_j \ .$$

Prenant $z = \alpha$ on obtient

$$\operatorname{den}\ P_{kj}(\alpha) \leqslant c_{59}^n \ .$$

Prenant alors c_5 supérieur à c_{56} , c_{58} et c_{59} on a le résultat cherché. Nous sommes maintenant en mesure de démontrer le lemme final.

<u>5è pas</u> : (pas final). De l'indépendance linéaire des fonctions $E_1, \ldots E_m$ sur les polynômes nous allons déduire une borne inférieure du rang des nombres $E_1(\alpha) \ldots, E_m(\alpha)$ sur K.

<u>Lemme fondamental</u> : Le rang de $E_1(\alpha), \ldots, E_m(\alpha)$ sur K est $\geqslant \frac{m}{2[K:Q]}$.

On a, si on appelle r ce rang

$$\mathcal{E} = E_1(\alpha).K + E_2(\alpha)K + \ldots + E_m(\alpha).K = E_{e_1}(\alpha).K \oplus \ldots \oplus E_{e_r}(\alpha).K .$$

D'après le lemme 3 on sait qu'il existe une matrice $\mathcal{P}(\alpha)$ régulière, donc une matrice bijective de K^m dans K^m. L'image par $\mathcal{P}(\alpha)$ d'un sous espace vectoriel de dimension r est un sous espace vectoriel de dimension r.

Or $\mathcal{P}(\alpha)$ transforme

$$(E_1(\alpha), \ldots, E_m(\alpha) \quad \text{en} \quad (F_{k_1}(\alpha), \ldots, F_{k_m}(\alpha))$$

où $k_1, \ldots, k_m$ sont inférieurs à $m+n$.

Donc $(F_{k_1}(\alpha), \ldots, F_{k_m}(\alpha))$ a un rang égal à r. Il existe donc $m-r$ relations entre ces nombres. Il y a donc $m-r$ combinaisons linéaires égales à 0 de ces nombres, donc $m-r$ combinaisons linéaires égales à 0 des $E_i(\alpha)$.

On peut écrire, en prenant même $\lambda_{ij} \in I_K$ (en multipliant les égalités par les dénominateurs adequats)

$$\begin{cases} 0 = \lambda_{11} \quad E_1(\alpha) + \ldots + \lambda_{1m} E_m(\alpha) \\ \\ 0 = \lambda_{m-r,1} E_1(\alpha) + \ldots + \lambda_{m-r,m} E_m(\alpha) \\ F_{k_1} = P_{k_{1},1} \quad E_1(\alpha) + \ldots + P_{k_m,1} \quad E_m(\alpha) \\ F_{k_r} = P_{k_r,1} \quad E_1(\alpha) + \ldots + P_{k_r,1} \quad E_m(\alpha) \end{cases}$$

et la matrice des coefficients des $E_i(\alpha)$ est régulière.

Soit δ son déterminant. On a, en résolvant le système par rapport à $E_1(\alpha)$

$$\delta E_1(\alpha) = B_1 F_{k_1}(\alpha) + \ldots + B_r F_{kr}(\alpha)$$

où $B_1, \ldots B_r$ sont les mineurs de δ relatifs à la première colonne.

D'après le lemme 4 on a

$$\begin{cases} \text{taille}(\delta) \leqslant 3nr \log n + O(n) \\ \text{den } \delta \leqslant O(n) \end{cases}$$

et on obtient aussi

$$|B_j|, \ldots, |B_r| \leqslant c_{12}^n \, n^{3n(r-1)}$$

$$\text{et} \qquad |F_k(\alpha)| < c_{14}^n \, n^{3n} \, n^{-(2m-2)n}$$

D'où

$$\begin{aligned} \text{Log } \delta &\leqslant 3n(r-1)\text{Log } n + 3n \text{ Log } n - (2m-2)n \text{ Log } n + O(n) \\ &\leqslant 3nr \text{ Log } n - (2m-2)n \text{ Log } n + O(n) \; . \end{aligned}$$

Appliquant l'inégalité sur la taille, divisant par $n \text{ Log } n$ et prenant n assez grand, on obtient

$$(2m-2) \leqslant 3r[K : \mathbb{Q}] \; .$$

D'où le lemme fondamental.

IV - Extension du théorème de L.W.

En regardant quelles sont les propriétés de la fonction exponentielle utilisée, Shidlovsky a réussi à généraliser le théorème de L.W. aux E-fonctions.

Une E fonction est une fonction qui admet un développement en série de la forme

$$f(z) = \sum_{n=0}^{\infty} \alpha_n \frac{z^n}{n!}$$

où $\alpha_n \in K$ (K corps de nombres) et satisfait

E1 $\|\alpha_n\| \leqslant c^n$ pour une certaine constante c (ou mieux $\leqslant O(n^{\varepsilon n})$ pour tout $\varepsilon > 0$).

E2 Il existe une suite de nombres $d_n \in \mathbb{Z}$, $d_n > 0$ tq d_n est un dénominateur pour α_k $(k = 0,\ldots n)$ et $d_n \leqslant c^n$ (ou mieux $O(n^{\varepsilon n})$).

Exemple de E-fonction : La fonction de Bessel

$$J_0(z) = \Sigma \frac{z^{2n}}{(n!)2} .$$

La difficulté dans l'extension du théorème de L.W. est de démontrer le lemme 2 pour les E-fonctions.

Le théorème de L.W. Shidlovsky est

Soient $f_1,\ldots,f_s$ des E-fonctions, algébriquement indépendantes sur $K(z)$ et qui satisfont des équations différentielles linéaires du type

$$X' = QX$$

où x est un vecteur colonne et Q une matrice carrée de fonctions rationnelles de $K(z)$. Soit $\alpha \in K^*$ et α distinct des pôles des fonctions de Q. Alors les valeurs

$$f_1(\alpha),\ldots,f_s(\alpha) \quad \text{sont algébriquement indépendantes.}$$

Application de ce théorème

- fonctions exponentielles bien sûr

- fonctions de Bessel solution de l'équation

$$y'' + \frac{1}{z}y' + \left(1-\frac{\lambda^2}{z^2}\right)y = 0$$

où λ appartient à un corps de nombres.

<u>Bibliographie</u>

[1] LANG. Introduction to transcendental numbers (Addison and Wesley).

[2] LANG. Algebra (Addison and Wesley).

[3] Laurent SCHWARTZ. Cours d'analyse (Herrmann).

[4] Th. SCHNEIDER. Introduction aux nombres transcendants (Gauthier-Villars.

A. MACADRE
I.U.T. de Reims
rue des Crayènes
51100 REIMS

Rappels historiques sur la théorie des nombres irrationnels et transcendants

Françoise CHANET
(Orsay 13 mars 1973)

Un nombre algébrique est une solution d'équation algébrique à coefficients entiers générale alors qu'un nombre rationnel est solution d'une équation algébrique à coefficients entiers du premier degré. La seconde notion est donc apparue beaucoup plus tôt que la première ; et les résultats sur les nombres irrationnels (= non rationnels) sont plus anciens et plus simples souvent, mais pas toujours, que les résultats analogues sur les nombres transcendants (= non algébriques).

I. Avant 1840.

Pour les Grecs il n'y a de nombres que les entiers (ceux bien sûr que nous disons maintenant strictement positifs). Néanmoins ils utilisent les "rapports d'entiers" (autrement dit les rationnels strictement positifs) toujours d'ailleurs du point de vue géométrique des "rapports de longueurs équivalents"), décrivant leurs opérations et démontrant certaines propriétés algébriques de ces opérations. La grande découverte de l'école de Pythagore (vers -500) est que la diagonale du carré n'est pas dans un "rapport d'entiers" avec son côté, en termes modernes que $\sqrt{2}$ est irrationnel. D'autre part le rapport de la circonférence au diamètre (ce que nous appelons le nombre π) n'est pas considéré comme un "rapport d'entiers" et Archimède (vers -200) en donne des approximations successives par la méthode des polygones. Ces deux résultats fondent la théorie des irrationnels. Quant aux problèmes de transcendance, du fait du caractère géométrique des mathématiques grecques, ils ne sont abordés que par le biais du fameux problème de la quadrature du cercle et de problèmes analogues de construction par la règle et le compas, dont l'impossibilité résulte en fait de l'insolubilité de certaines équations (en rationnels).

La théorie des nombres irrationnels et transcendants prend ensuite un vrai départ au 18ème siècle : elle bénéficie de la mise au point de l'algèbre formelle à partir du 15ème et de l'essor de l'analyse (fonctions exponentielles et logarithmes) à partir du 17ème. De plus sans en avoir fait de construction formelle les mathématiciens de cette époque se placent dans le corps des complexes (nombres imaginaires) au besoin. Une des première mentions des nombres transcendants est faite par Euler en 1748 dans son "Introductio in analysin infinitorum" (Oeuvres complètes-tome VIII-page 108) : "il apparaît clairement que les logarithmes rationnels proviennent des puissances de la base a. Si b n'est pas une telle puissance $\log_a(b)$ n'est même pas irrationnel car sinon (par exemple ?) on aurait avec b rationnel : $a^{\sqrt{n}} = b$ ce qui est impossible. Ces logarithmes ni rationnels ni irrationnels ont droit à l'appellation de transcendants." Quoi qu'on puisse penser des arguments d'Euler, on peut remarquer qu'il pose le problème (irrationnel dans ce contexte = algébrique réel) au sujet des logarithmes qui effectivement sont explorés jusqu'au moment présent (Baker). Vers ce milieu du 18ème siècle également se perfectionne la théorie des développements en fractions continue, très liée à l'irrationnalité puisqu'un réel est rationnel si et seulement si son développement est fini, et un peu à la transcendance puisque vers époque Lagrange montre qu'un réel est algébrique de degré 2 si et seulement si son développement est périodique. De cette manière Lambert en 1761 (C. R. Ac. Sc. Prusse) donne une démonstration à vrai dire incomplète de l'irrationnalité de π ; on peut trouver cette démonstration complétée par Legendre dans les Comptes rendus de l'Académie des Sciences de l'année 1855. On peut remarquer aussi que le développement de e en fractions continue : $[2, 1, \underbrace{2, 1, 1}, \dots, \underbrace{2n, 1, 1}, \dots]$ trouvé "intuitivement" par Euler entraîne que e n'est ni rationnel ni même un nombre quadratique. En 1815 Fourier prouvera l'irrationnalité de e d'une manière très simple en utilisant son développement en série : $e = 1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{n!} + \dots$.

II. De 1840 à 1920 : théorie classique.

La théorie des nombres transcendants est véritablement fondée par Liouville qui à propos de problèmes d'approximation diophantienne établit pour la première fois l'existence de nombres transcendants ; son théorème (C. R. Ac. Sc. Paris 1844) s'énonce en effet : si α est une racine réelle du polynôme P irréductible dans $\mathbb{Z}[X]$ de degré s , il existe une constante $c \in \mathbb{R}_+^*$ telle que quels que soient q dans $\mathbb{N}^*$ et p dans $\mathbb{N}$ on a l'inégalité : $\left|\frac{p}{q} - \alpha\right| \geqslant \frac{c}{q^s}$.

Si on considère donc la somme d'une série $\sum_n \frac{1}{q^{N_n}}$ où q est un entier positif et N_n une suite d'entiers telle que $\frac{N_{n+1}}{N_n}$ tende vers $+\infty$ avec n , on voit qu'elle ne vérifie la propriété de Liouville pour aucun s donc qu'elle est transcendante. (ex. $N_n = n!$). Les nombres ainsi construits -nombres de Liouville- ont été très étudiés par Maillet cf. C. R. Ac. Sc. Paris de 1901 à 1907.

Ces problèmes d'approximation continueront jusqu'à nos jours à représenter un aspect de la théorie des nombres irrationnels et transcendants, en particulier à permettre de créer des nombres transcendants autres que ceux rencontrés dans l'analyse. Rappelons le plus célèbre d'entre eux : il s'agit d'estimer $\theta(n)$ borne inférieure des $c \in \mathbb{R}_+^*$ tels que pour tout ε appartenant à $\mathbb{R}_+^*$ et tout α nombre réel algébrique de degré n l'inégalité $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{c+\varepsilon}}$ n'est vraie que pour un nombre fini de rationnels $\frac{p}{q}$. Les théorème de Liouville et de Dirichlet donnent déjà : $2 \leqslant \theta(n) \leqslant n$. Thue en 1908 trouva la majoration $\theta(n) \leqslant \frac{n}{2}+1$ améliorée au cours du 20ème siècle par Siegel, Mahler, Schneider avant que Roth en 1955 (Mathematika) ne donne le résultat définitif : $\theta(n) = 2$. Plus centrale dans la théorie est la définition de la mesure de transcendance de x nombre complexe : c'est une fonction $\Phi(x,m,H) = \min\ (|P(x)|$ où P est un polynôme à coefficients entiers de hauteur $\leqslant H$ et de degré $\leqslant m$). Bien sûr x est algébrique si et seulement si pour m et H suffisamment grands cette fonction s'annule. Majorer cette fonction est simple (principe des tiroirs) : si x est réel on a $\Phi(x,m,H) < e^{\lambda m}\ H^{-m}$ et sinon $\Phi(x,m,H) < e^{\lambda m}\ H^{-\frac{m-1}{2}}$. C'est sur le problème plus intéressant de sa minoration qu'on a commencé à travailler dès la fin du 19ème siècle. Par exemple Borel en 1899 montre que : $\Phi(e,m,H) > H^{-c(m)\log\log H}$; mais là aussi le gros des résultats fut obtenu au cours du 20ème siècle en particulier par Mahler.

Le résultat de Borel est bien sûr un raffinement du résultat fondamental d'Hermite, qui en 1873 prouve la transcendance de e. Sa démonstration et celles plus simples que Hurwitz ... donneront un peu plus tard s'appuient sur les propriétés simples de la fonction exponentielle, d'intégrabilité par exemple, et sur des combinaisons "astucieuses" donnant, e étant supposé algébrique, une quantité entière non nulle et tendant vers 0.

En 1882 Lindemann adapte cette méthode pour prouver la transcendance de π et trois ans plus tard Weierstrass (cf Mathematische Werke II p. 341 ssq) donne la généralisation connue sous le nom de théorème de Lindemann-Weierstrass : soient $a_1,\ldots,a_n$ des nombres algébriques non tous nuls et $b_1,\ldots,b_n$ des nombres algébriques deux à deux distincts ; alors $a_1e^{b_1}+\ldots+a_ne^{b_n} \neq 0$.

On en déduit un premier résultat d'indépendance algébrique : celle des puissances de e dont les exposants sont $\mathbb{Q}$-linéairement indépendants.

Ce théorème de Lindemann-Weierstrass semble un point final dans cette direction de recherche utilisant les valeurs aux points algébriques des fonctions vérifiant des équations différentielles à coefficients algébriques. C'est pourquoi Hilbert dans sa fameuse liste de problèmes du Congrès international de Paris 1900 considère le 7ème : étudier la transcendance de a^b , a et b algébriques et b irrationnel comme très difficile, de l'ordre de difficulté de l'hypothèse de Riemann p.e. En fait à peine plus de trente ans après ce problème est résolu grâce à de nouvelles méthodes impliquant une connaissance plus profonde des fonctions analytiques. Mentionnons enfin qu'à la fin du 19ème siècle Cantor a donné la plus élégante méthode de démonstration de l'existence de nombres transcendants : l'ensemble des nombres algébriques est dénombrable alors que $\mathbb{R}$ ou $\mathbb{C}$ a la puissance du continu.

II. Depuis 1920 : résolution du 7ème problème de Hilbert etc...

Vers 1920 des mathématiciens (Polya, Gel'fond,...) étudient les fonctions analytiques prenant des valeurs entières aux points entiers (de $\mathbb{Z}$, $Z[i]$), en particulier du point de vue de leur croissance. Ainsi Gel'fond en utilisant une méthode d'interpolation prouve-t-il dès 1929 que si a et b sont algébriques $\neq 0,1$ b étant irrationnel quadratique, a^b est transcendant. Ce résultat est amélioré par Kuzmin, puis Böhle ; et en 1934 Gel'fond et Schneider indépendamment démontrent leur célèbre théorème : si a est algébrique et différent de $0,1$, si b est algébrique irrationnel, alors a^b est transcendant.

La conjecture d'Euler est ainsi justifiée presque deux siècles plus tard. C'est le point de départ de nombreux travaux, spécialement des écoles russe et allemande. Ainsi dès 1933 Mahler étend aux exponentielles p-adiques (sa démonstration ainsi que celle du théorème principal sera améliorée par Lang). Gel'fond en 1934 trouve un premier résultat sur les mesures de transcendance des a^b (qui sera amélioré par son école) : analogue à celui de Borel. Schneider se consacre de 1934 à 1937 aux fonctions elliptiques sur lesquelles il obtient de beaux résultats dont on peut donner quelques exemples : -la longueur d'une ellipse à axes algébriques est transcendante- -la fonction $\wp$ de Weierstrass prend des valeurs transcendantes aux points algébriques- etc... et en 1941 $B(p,q) = \int_0^1 x^{p-1}(1-x)^{q-1}dx$ est transcendant pour tous p et q rationnels.

Siegel entreprend une étude arithmétique des valeurs aux points algébriques d'une assez grande classe de fonctions entières, les E-fonctions : [si α appartient à K corps de nombres de degré h sur $\mathbb{Q}$, on note $|\bar{\alpha}| = \max(|\alpha_i|\ \alpha_p \ldots \alpha_j$ conjugués de $\alpha)]$. Une fonction entière $\sum_{n=0}^{+\infty} c_n \frac{z^n}{n!}$ est une E-fonction si :

(1) tous les c_n appartiennent à un certain corps de nombres de d° fini

(2) pour tout ε de $\mathbb{R}_+^*$ $\quad |\bar{c}_n| = \mathcal{O}_{n \to +\infty}(n^{\varepsilon})$

(3) il existe une suite de q_n entiers positifs tels que pour tous n et k le nombre $q_n c_k$ est un entier algébrique et que pour tout ε de $\mathbb{R}_+^*$ on ait : $q_n = \mathcal{O}_{n \to +\infty}(n^{\varepsilon})$.

Ces E-donctions forment un anneau fermé pour la dérivation, l'intégration et la multiplication par un nombre algébrique. Elles comprennent les polynômes à coefficients algébriques, e^z, $\cos z$, $J_\lambda(z)$ fonction de Bessel. C'est d'ailleurs sur des fonctions très proches des J_λ que Siegel établit son premier théorème en 1929, dont une conséquence est la transcendance de la fraction continue : $[1, 2, 3, \ldots, n, \ldots]$. Voici le théorème général de Siegel (1949) :

Si $f_1, \ldots, f_n$ sont des E-fonctions solutions du système linéaire à coefficients dans $\mathbb{Q}(Z)$ d'équations différentielles : $y_k' = \sum_{i=1}^{m} Q_{k,i}\, y_i \quad k = 1, \ldots, m$ telles que les $\frac{(m+N)!}{N!m!}$ produits de puissances de ces fonctions : $f_1^{k_1} \cdot \ldots \cdot f_m^{k_m}$ $k_1 + \ldots + k_m \leqslant N$ forment un système normal de E-fonctions, alors les valeurs de $f_1, \ldots, f_m$ en un α point algébrique non nul et non pôle sont algébriquement indépendantes.

Si les équations sont affines sur $\mathbb{Q}(Z)$ on a une équivalence entre la $\mathbb{Q}$-indépendance algébrique des valeurs en α et la $\mathbb{Q}(Z)$-indépendance algébrique des F_j. Citons encore un résultat de Shidlovskii (1953) dans cet ordre d'idées :

on considère pour λ rationnel non entier négatif la fonction :

$\varphi_\lambda(z) = \sum_{n=0}^{+\infty} \frac{z^n}{(\lambda+1)\ldots(\lambda+n)}$ et $\alpha_1,\ldots,\alpha_n$ des nombres $\mathbb{Q}$-linéairement indépendants ; alors les nombres $\varphi_\lambda(\alpha_1),\ldots,\varphi_\lambda(\alpha_n)$ sont algébriquement indépendants. C'est une généralisation de Lindemann-Weierstrass.

Avant de passer aux résultats les plus récents il faut évoquer au moins une partie de l'oeuvre considérable accomplie dans la théorie des nombres transcendants par Kurt Mahler -déjà cité- depuis 1930. Un des plus connus est sa classification des nombres transcendants datant de 1932 : pour un nombre ξ on définit avec a et n entiers positifs $w_n(a,\xi) = \min_{\substack{|a_i|\leqslant a \\ \sum_{i=0}^{n} a_i \xi_i \neq 0}} \left(\left|\sum_{i=0}^{n} a_i \xi^i\right|\right)$ puis à n fixé $w_n(\xi) = \limsup_a \frac{\operatorname{Log}\frac{1}{w_n(a)}}{\operatorname{Log} a}$ et enfin $w(\xi) = \limsup \frac{w_n}{n}$. On appelle alors $\mu(\xi)$ le premier n éventuellement infini pour lequel w_n devient infini. On remarque que $w(\xi)$ et $\mu(\xi)$ ne peuvent pas être simultanément finis et on pose

ξ est un A-nombre	si	$w = 0$	$\mu = +\infty$
ξ est un S-nombre	si	$0 < w < +\infty$	$\mu = +\infty$
ξ est un T-nombre	si	$w = +\infty$	$\mu = +\infty$
ξ est un U-nombre	si	$w = +\infty$ et	$\mu < +\infty$.

ξ est algébrique si et seulement si c'est un A-nombre. Les nombres transcendants se répartissent donc en S-, T-, et U-nombres. Le théorème de Mahler dit que deux nombres de classe différente sont algébriquement indépendants. Il établit aussi que les nombres de Liouville sont des U-nombres $(w = 1)$, que e est un S-nombre, que π est un S-nombre ou un T-nombre. Depuis bien d'autres résultats ont été acquis. En 1937 Mahler à partir d'un résultat de Schneider paru l'année précédente prouve que si P est un polynôme prenant des valeurs entières aux points entiers un nombre écrit en base q : $x = \overline{0, P(1) \quad P(n)\ldots}$ est transcendant non de Liouville. Il s'occupe aussi d'approximation, en particulier précise les mesures de transcendance de $\mathrm{Log}\,\alpha$, e, π (voir aussi les travaux de Popken et Feld'man).

Le plus important des résultats récents est sans doute le théorème de Baker (1966) : soient $\alpha_1,\ldots,\alpha_m$ des nombres algébriques dont les logarithmes sont $\mathbb{Q}$-linéairement indépendants ; alors les nombres $1, \mathrm{Log}\,\alpha_1,\ldots,\mathrm{Log}\,\alpha_m$ sont $\mathbb{Q}$-linéairement indépendants. Baker, puis Stark et Feld'man ont donné des minorations précises des formes linéaires de logarithmes.

De nombreuses conjectures ont été faites récemment dont la plus globale est celle de Schanuel : si $x_1,\ldots,x_n$ sont des nombres $\mathbb{Q}$-linéairement indépendants le degré de transcendance sur $\mathbb{Q}$ du corps $\mathbb{Q}(x_1,\ldots,x_n,e^{x_1},\ldots,e^{x_n})$ est supérieur ou égal à n. Pour finir nous rappelons que nombre de problèmes d'énoncé élémentaire ne sont pas résolus : la constante d'Euler est-elle irrationnelle ?

Quelle est la nature arithmétique de $e\pi$, $e+\pi,\ldots,\pi^{\pi}$, $e^{e},\ldots,2^{e}$ même et plus généralement e et π sont-ils algébriquement indépendants ?

Bibliographie

Fel'dman, N.I., and Shidlovskii, A.B.- The development and present state of the theory of transcendental numbers. Russian Mathematical Surveys, vol. 22 n° 3 (1967) p. 1-79.

Construction de nombres transcendants, grâce aux théorèmes de Liouville, Thue, Siegel et Roth

Maurice MIGNOTTE
(Orsay 20 mars 1973)

Introduction

Cet exposé consistera d'abord en un énoncé assez bref de résultats sur l'approximation diophantienne des nombres algébriques qui, vu leur difficulté, ne seront généralement pas démontrés. Ces résultats seront utilisés pour construire certaines familles de nombres transcendants.

Il apparaîtra à l'évidence que la théorie est encore à un stade peu satisfaisant. En particulier, les nombres transcendants que l'on construit par cette méthode sont souvent très spéciaux et je ne connais aucune démonstration de transcendance d'un nombre "usuel" par cette méthode.

Notations : Soit x un réel :

$[x]$ désigne la partie entière de x ,

$\{x\} = x - [x]$ est la partie fractionnaire de x ,

on notera $\|x\|$ la distance de x à l'entier le plus proche.

I - Approximation des nombres réels par des rationnels

1. Approximation des nombres rationnels par des rationnels

Commençons par un résultat évident.

Théorème 1 : Soit $\alpha = \frac{a}{b}$ un rationnel, avec $b \geqslant 1$, et soit $\frac{p}{q}$ un nombre rationnel distinct de α, $q > 0$, alors on a

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{bq} .$$

Démonstration :

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq-pb|}{bq} \geqslant \frac{1}{bq} .$$

C.Q.F.D.

Donnons une conséquence triviale de ce résultat, mais qui indique le principe de la construction future de nombres transcendants à partir d'un théorème sur l'approximation des nombres algébriques.

Corollaire 1 : Soit α un nombre réel tel que pour tout $A > 0$, l'équation

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq}$$

admette une solution alors α est irrationnel.

Exemple : On obtient ainsi l'irrationnalité de $e, x\,\mathrm{ch}\,\frac{1}{x}, x \sin\frac{1}{x}, \cos\frac{1}{x}, \mathrm{ch}\,\frac{1}{x}$, avec $x^2 \in \mathbb{N}^*$. On peut même obtenir un résultat plus fort, à savoir :

Corollaire 2 : Soit x, avec $x^2 \in \mathbb{N}^*$. Soient $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ non tous nuls. Alors le nombre

$$\alpha = a_1\,\mathrm{ch}\,x + a_2\frac{1}{x}\,\mathrm{sh}\,x + a_3\cos x + a_n\frac{1}{x}\sin\frac{1}{x}$$

est irrationnel.

2. Approximation des nombres irrationnels par des rationnels

Théorème 2 (Dirichlet 1842) : Soit α un nombre irrationnel. Il existe une infinité de nombres rationnels $\frac{p}{q}$ tels que

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q^2} . \tag{1}$$

Démonstration :

Soit Q un entier $\geqslant 1$. Considérons les nombres $\alpha_k = \{k\alpha\}$, $k = 0,\ldots,Q$, de l'intervalle $[0,1]$. Partageons cet intervalle en Q segments égaux de longueur $\frac{1}{Q}$. Les $Q+1$ points α_k sont répartis dans Q intervalles, l'un deux contiendra donc deux points (principe des tiroirs). D'où l'existence de deux entiers m et n distincts tels que

$$|(n-m)\alpha - ([m\alpha] - [n\alpha])| < \frac{1}{Q} .$$

Si on pose $q = n-m$ et $p = [m\alpha] - [n\alpha]$, on a alors

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{qQ} \leqslant \frac{1}{q^2} .$$

Le fait que Q soit arbitraire permet de montrer que (1) admet une infinité de solutions.

Ce résultat peut être amélioré.

Théorème 3 (Hurwitz, 1891) :

(i) Pour tout irrationnel α , il existe une infinité de rationnels $\frac{p}{q}$, avec $(p,q) = 1$, qui vérifient

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}\, q^2} . \tag{2}$$

(ii) Ce résultat n'est plus vrai si on remplace la constante $\sqrt{5}$ par un nombre plus grand.

Démonstration : Voir par exemple Hardy et Wright Chap. XI.

Pour une généralisation aux nombres quadratiques imaginaires, voir Poitou (1953).

Le travail de Markov a beaucoup précisé ce théorème, nous nous contentons de donner une toute petite partie de ses résultats (voir Cassels, Chap. II).

Théorème 4 (Markov, 1879) :

Il y a une infinité non dénombrable de nombres irrationnels (non équivalents, au sens des fractions continues) tels que

$$\underline{\lim}\ q\,\|q\alpha\| = \frac{1}{3}\ .$$

Corollaire : Il existe une infinité non dénombrable de nombres transcendants α pour lesquels il existe une constante $c = c(\alpha) > 0$ avec

$$(3) \qquad \left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$$

pour tout q.

Remarque 1 : Un nombre α vérifie (3), pour une certaine constante c, si, et seulement si, les quotients partiels du développement en fraction continue de α sont bornés. Je ne connais pas d'exemple de nombre usuel dont on ait démontré qu'il vérifie (3) en dehors des nombres irrationnels quadratiques. Par contre, on sait que beaucoup de nombres usuels n'appartiennent pas à cette classe, par exemple c'est le cas de $e^{1/p}$ pour t entier (on connait le développement en fraction continue de ce nombre, voir par exemple les ouvrages de Penon (1913) ou Lang (1966)). Il semble bien que tout nombre algébrique de degré $\geqslant 3$ a des quotients partiels non bornés ; en tout cas le calcul d'un grand nombre de réduit de nombreux nombres algébriques semble confirmer cette conjecture, voir par exemple Neumann et Tuckerman (1955), Richtunyer, Devany et Metropolis (1962), Bryuno (1964).

La plupart des irrationnels ne vérifient pas (3) :

<u>Théorème</u> 5 (Khintchine 1926) :

Soit $\psi(q)$ une fonction positive. Considérons les inégalités

$$(4) \qquad \left|\alpha - \frac{p}{q}\right| < \frac{\psi(q)}{q} .$$

Alors

(i) Si la série $\sum_{q=1}^{\infty} \psi(q)$ converge alors (4) n'a qu'un nombre fini de solutions $\frac{p}{q}$, $q > 0$, pour presque tout α (au sens de la mesure de Lebesgue).

(ii) Si ψ est décroissante (au sens large) et la série ci-dessus diverge, cette inégalité a une infinité de solutions pour presque tout α.

<u>Démonstration</u> :

(i) Considérons d'abord le cas où $\alpha \in I = [0,1[$. Soit q fixé. L'ensemble des $\alpha \in I$ qui vérifient (4) est contenu dans l'union de $q+1$ intervalles (centrés aux points $0, \frac{1}{q}, \frac{2}{q}, \dots, 1$) de longueur $\frac{2\psi(q)}{q}$, sa mesure est donc au plus égale à $4\psi(q)$. Ainsi, l'ensemble des $\alpha \in I$ pour lesquels (4) admet une solution avec $q \geqslant Q$ a une mesure au plus égale à

$$4 \sum_{q \geqslant Q} \psi(q) ,$$

quantité qui tend vers 0 avec Q^{-1}. La conclusion est alors évidente.

(ii) Voir par exemple Khintchine (1964) ou Cassels ch.VII. Pour des résultats semblables voir aussi Borel (1909) et Bernstein (1912) où Hardy et Wright Th.196, Th.197 chap.XI.

Exemples :

1. L'ensemble des nombres α irrationnels qui pour un $\varepsilon = \varepsilon(\alpha) > 0$ sont tels que l'inégalité

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

admette une infinité de solutions est de mesure nulle.

2. La conclusion précédente a encore lieu si on remplace l'inégalité ci-dessus par

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2 (\log q)^{1+\varepsilon}} .$$

II - Approximation des nombres algébriques

1. Le théorème de Liouville

Théorème 6 (Liouville 1844) :

Soit α un nombre algébrique de degré $n \geqslant 2$. Il existe une constante $c = c(\alpha) > 0$ telle que, pour tout rationnel $\frac{p}{q}$, $q \geqslant 1$, on ait l'inégalité

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n} .$$

Démonstration :

Soit P le polynôme minimal de α, i.e. le polynôme de degré n, à coefficients entiers, primitif et de terme principal positif tel que $P(\alpha) = 0$.

Soit d'abord $\frac{p}{q}$ tel que

$$\left|\alpha-\frac{p}{q}\right| \leqslant 1 .$$

On a alors

$$\frac{1}{q^n} \leqslant \left|P\left(\frac{p}{q}\right)\right| = \left|P\left(\frac{p}{q}\right)-P(\alpha)\right| = \left|\alpha-\frac{p}{q}\right| P'(\zeta) , \quad \text{avec} \quad \zeta \in \left]\alpha, \frac{p}{q}\right[,$$

d'où

$$\frac{1}{Mq^n} \leqslant \left|\alpha-\frac{p}{q}\right| \quad \text{avec} \quad M = \max\left(\sup_{\alpha-1\leqslant x\leqslant\alpha+1} |P'(x)|, 1\right) .$$

Cette dernière inégalité a encore lieu si $\left|\alpha-\frac{p}{q}\right| > 1$. D'où le résultat.

Remarque 2 : Le théorème de Dirichlet montre que ce résultat est essentiellement le meilleur possible dans le cas des irrationnels quadratiques.

2. Les nombres de Liouville

On dira qu'un nombre α est de Liouville si, pour tout $A > 0$, il existe un nombre rationnel $\frac{p}{q}$, $q \geqslant 1$, tel que

$$0 < \left|\alpha-\frac{p}{q}\right| < \frac{1}{q^A} .$$

Le théorème 6 montre qu'un tel nombre est transcendant. Il est bon de rappeler qu'avant Liouville l'existence de nombres transcendants n'était pas démontrée.

Exemple : L'application

$$\sum_{n\geqslant 1} \varepsilon_n 2^{-n} \mapsto \sum_{n\geqslant 1} \varepsilon_n 2^{-n!} , \quad \varepsilon_n \in \{0,1\}$$

définit une injection de l'ensemble des nombres irrationnels de l'intervalle $]0,1[$ dans l'ensemble des nombres de Liouville.

L'ensemble $\mathcal{L}$ des nombres de Liouville a donc la puissance du continu (il est étonnant de lire dans l'article de Fel'dman et Shidlovski (1967) qu'on ne sait pas si $\mathcal{L}$ est dénombrable). Il est aussi facile de voir que $\mathcal{L}$ est partout dense dans $\mathbb{R}$. Par contre le théorème 5, exemple 1, montre que $\mathcal{L}$ est de mesure nulle. Ce n'est pas un fait isolé, tous les ensembles de nombres transcendants qu'on définira plus loin seront aussi de mesure nulle, ce qui montre le faiblesse des méthodes d'approximation diophantienne pour la construction de nombres transcendants.

On peut aussi facilement caractériser les nombres de Liouville par les propriétés de leur développement en fraction continue. Soit $\alpha = [a_0;a_1,a_2,\ldots,a_n,\ldots]$ un nombre irrationnel. On sait que

$$\frac{1}{(a_{n+1}+2)q_n^2} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{a_{n+1}q_n^2} \quad \text{avec} \quad \frac{p_n}{q_n} = [a_0;a_1,\ldots,a_n] .$$

On voit donc que α est un nombre de Liouville si, et seulement si,

$$\lim \frac{\log a_{n+1}}{\log a_n} = +\infty ,$$

il suffit de se souvenir en plus que si $\frac{p}{q}$ vérifie

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

alors il existe n tel que $\frac{p}{q} = [a_0;a_1,\ldots,a_n]$.

Pour des exemples de nombres transcendants, mis sous forme de fractions continues, obtenu grâce au théorème de Liouville ou à sa généralisation à l'approximation par les irrationnels quadratiques voir Maillet (1904, 1906a., 1907 a.b.c), Perron(1913), Perna (1913,1914), Gigli (1923).

3. Une généralisation du théorème de Liouville

Théorème 7 : Soit α un nombre algébrique de degré $n \geqslant 1$ et soit $P(x)$ un polynôme à coefficients entiers de degré d et de hauteur H donc α n'est pas racine. Alors on a

$$|P(\alpha)| \geqslant \frac{c^d}{H^{n-1}}, \quad \text{avec} \quad c = c(\alpha) > 0 .$$

Pour $n = 1$, on retrouve le théorème de Liouville.

Démonstration :

Soit q un dénominateur de α, alors q^d est un dénominateur de $P(\alpha)$ et

$$1 \leqslant |\mathrm{Norm}(q^d P(\alpha))| \leqslant |q^d P(\alpha)| \; (q^d (1+a)^d H)^{n-1}$$

où a désigne la hauteur de α. D'où la conclusion.

On en déduit facilement l'énoncé suivant (voir Schneider (1957) chp. I, §3).

Corollaire : Si α est algébrique de degré n et ξ algébrique de degré d et de hauteur H, alors, pour $\xi \neq \alpha$, on a

$$|\alpha - \xi| > \frac{c_1^d}{H^n}, \quad \text{où} \quad c_1 = c_1(\alpha) > 0 .$$

Bibliographie : Brauer (1929a, 1929b), Bombieri (1958) et Güting (1961).

De ce corollaire on peut déduire le résultat suivant.

Proposition 1 : Toute racine réelle positive de la fonction

$$F(x) = \sum_{\nu=0}^{\infty} \frac{(-1)^\nu a_\nu x^\nu}{(\nu!)^{\nu!}}$$

a une valeur transcendante si les a_ν sont des entiers naturels tels que $0 < a_\nu < B^\nu$, où B est une constante > 0.

Démonstration : Voir Schneider (1957) Th.5, Ch.I, §4.

Bibliographie : Cohn (1946).

4. Le théorème de Roth

Théorème 7 (Roth 1955) :

Soit α algébrique de degré $n > 1$. Pour tout $\varepsilon > 0$ donné, l'inégalité

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$$

n'a qu'un nombre fini de solutions.

Pour des résultats antérieurs plus faibles voir Thue (1908, 1909), Siegel (1921), Dyson (1947), Gefond (1952) chap.1.

Démonstration :

Voir par exemple Cassels ch.VI.

Remarque 3 (W. Schmidt 1971, page 12) : In view of Dirichlet's theorem, the exponent 2 is best possible here. But it is conceivable that the factor q^{ε} could be replaced by a smaller factor. But nothing is known in this direction. The metrical result (exemple 2, Th.5 suggests that

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2(\log q)^{1+\varepsilon}}$$

has only finitely many solutions for every positive δ. The first written account of this conjecture appears to be in Lang (1965).

Conséquence : Soit α un nombre et soit $\varepsilon > 0$ tels que l'inégalité

$$(5) \qquad |\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$$

admette une infinité de solutions $\frac{p}{q}$ distinctes. Alors α est transcendant.

Exemple : $\alpha = \sum_{n=1}^{\infty} 2^{-3^n}$ est transcendant.

Remarque 4 : D'après l'exemple 1 du th.5, l'ensemble $\mathfrak{R}$ des nombres transcendants construits par cette méthode est de mesure nulle. Là encore, je ne connais pas d'exemple de nombre transcendant usuel dont on sache qu'il appartient à $\mathfrak{R}$. Par contre, par exemple, le nombre e^{α}, α algébrique non nul, n'appartient pas à cette classe : voir Mahler (1932), (1967), Baker (1965), Kappe (1966)...

Davenport et Roth (1955) ont montré que, si $\frac{p_n}{q_n}$ désigne la n-ième réduite d'un nombre algébrique irrationnel α, on a

$$\log \log q_n < \frac{c_1(\alpha) n}{\sqrt{\log n}} .$$

Baker (1962) a repris les travaux de Maillet (1906 chap.VII) et les a améliorés en utilisant les travaux de Davenport et Roth et démontre en particulier :

Proposition 2 : Soit $\alpha = [a_0; a_1, \dots, a_m, \dots]$. S'il existe une infinité de n tels que

$$* \qquad a_n = a_{n+1} = \dots = a_{n+\lambda(n)-1}$$

et si le développement n'est pas périodique et que $*$ a lieu pour $n = n_i$ avec

$$\lim_{i\to\infty} \frac{\log \lambda_i (\log n_i)^{\frac{1}{2}}}{n_i} = \infty, \text{ où } \lambda_i = \lambda(n_i), \text{ alors } \alpha \text{ est transcendant.}$$

De même que Maillet, il obtient des résultats plus généraux en considérant des blocs de a_i, consulter le papier cité à ce sujet.

Maillet construit aussi des nombres décimaux quasi-périodiques qui sont des nombres transcendants (de Liouville), grâce au théorème de Roth, ces résultats peuvent être améliorés.

Le théorème de Roth avait été précédé par un théorème de Schneider (1936) qui améliorait un résultat antérieur de Siegel (1921 b).

Théorème 8 (Schneider 1936) :

Soit α algébrique. Pour $\varepsilon > 0$ fixé, si $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$, $0 < q_1 < q_2 < \ldots$, $(p_1,q_1) = (p_2,q_2) = \ldots = 1$, sont des solutions de

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

alors

$$\lim \frac{\log q_{k+1}}{\log q_k} = +\infty .$$

Ce résultat était presque aussi utile que le théorème de Roth pour la construction de nombres transcendants. Par exemple, il suffit pour démontrer la transcendance de $\sum_{n\geqslant 1} 2^{-3^n}$.

Le théorème de Schneider a été amélioré par Cugiani, grâce au lemme de Roth.

Théorème 9 (Cugiani 1959) :

Soit α algébrique de degré d. Si

$$\left|\alpha - \frac{p}{q}\right| < q^{-2-20d(\log\log\log q)^{-\frac{1}{2}}}$$

admet une infinité de solutions $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$, $0 < q_1 < q_2 < \ldots$, $(p_1,q_1) = (p_2,q_2) = \ldots = 1$, alors

$$\lim \frac{\log q_{k+1}}{\log q_k} = +\infty .$$

Pour une généralisation voir Mahler (1961 appendice). Ce théorème a été quelque peu renforcé depuis.

<u>Théorème</u> 10 (Mignotte 1971) :

Soit α algébrique de degré d. Si l'inégalité

$$\left|\alpha - \frac{p}{q}\right| < q^{-(2+\theta(\log\log\log q)^{-\frac{1}{2}})} ,$$

avec $$\theta = \frac{4}{\sqrt{\alpha}}\sqrt{\log(f+2)\log 2} \quad , \quad 0 < \alpha < b ,$$

admet une infinité de solutions $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, 0 < q_1 < q_2 < \ldots; (p_1, q_1) = \ldots = 1$,

alors on a

$$\overline{\lim} \frac{\log q_{k+1}}{(\log q_k)^p} = \infty$$

pour tout $p \in [1, 2^{\frac{6-\alpha}{\alpha}}[$.

<u>Remarque</u> 5 : En utilisant des méthodes probabilistes, on peut améliorer un peu la valeur de θ.

5. <u>Généralisations du théorème de Roth</u>

Soit β un nombre algébrique, on pose $H(\beta) = H(P)$, où P désigne le polynôme minimal de β.

<u>Théorème</u> 11 (Levêque 1955, vol.2, chap.4) :

Soit α algébrique. Soit K un corps de nombres. On fixe $\varepsilon > 0$. Alors, il y a seulement un nombre fini d'éléments β de K tels que

$$|\alpha - \beta| < H(\beta)^{-2-\varepsilon} .$$

Si α et K sont réels l'exposant 2 est le meilleur possible.

Signalons seulement que ce résultat a été amélioré par Mahler (1963). Pour une discussion détaillée, voir W. Schmidt pages 22-23.

6. Conditions arithmétiques

Le premier à reconnaître l'importance d'approximations diophatiennes p-adiques fut K. Mahler.

Parmi les nombreux et importants travaux sur cette question, on peut citer : Mahler (1933 a.b.c), (1936) ; Parry (1940), (1950) ; Schneider (1950), (1957, Th.6 ch.I) ; Ridout (1957), (1958) ; Mahler (1961) ; Lang (1962) ; Mahler (1963) ; Stépanov (1967), Walliser (1969) ; Sprindzuck (1970), (1971);... .

Comme exemple nous ne citerons que le résultat suivant :

Théorème 12 (Ridout 1957) :

Soit α algébrique réel non nul et soient $p_1,\dots,p_r,q_1,\dots,q_s$ des nombres premiers distincts fixés. Supposons $\varepsilon > 0$. Alors il y a seulement un nombre fini de nombres rationnels $\frac{p}{4}$ avec

$$** \qquad p = p_1^{a_1}\dots p_r^{a_r}p' \ , \ q = q_1^{b_1}\dots q_s^{b_s}q'$$

où les a_i et b_j sont des entiers $\geqslant 0$ et où p' et q' sont des entiers non nuls et tels que

$$|\alpha - \frac{p}{q}| < \frac{1}{|p'q'|\,|pq|^{\varepsilon}} \ .$$

Conséquence : Le nombre $\alpha = \sum_1^{\infty} 2^{-2^n}$ est transcendant.

Remarque 6 : Soit $\mathfrak{R}_i$ l'ensemble des nombres non nuls tels que l'inégalité (6) admette une infinité de solutions de la forme **, le théorème de Ridout montre que ces nombres sont transcendants. Fraenkel (1962) a démontré que $\mathfrak{R}_i$ est de mesure nulle. Pour l'existence et la construction de certains nombres transcendants obtenus de cette manière voir Fraenkel (1964).

Pour des exemples de nombres transcendants obtenus par des théorèmes d'approximation, voir Kempner (1916 a.b.c) ; Blumberg (1916), (1926) ; Tschkaloff (1921 a.b) ; Izumi (1927), (1928) ; Itihara et Oishi (1933) ; Schneider (1950).

Voici quelques exemples dont on trouvera les démonstrations dans le livre de Schneider.

<u>Proposition</u> 3 : Pour x rationnel non nul, la série entière

$$\alpha = \sum_{\nu \geqslant 0} a^{-c^{\nu}} d_{\nu} x^{\nu}$$

prend des valeurs transcendantes quand a, c et les d sont entiers, $a \geqslant 2$, $c \geqslant 2$, $|d_{\nu}| < D^{\nu}$ où D est un nombre > 0, une infinité de d_{ν} étant de plus supposés non nuls.

<u>Proposition</u> 4 : La série de Fredholm $\alpha = \sum_{\nu=0}^{\infty} x^{2^{\nu}}$ prend des valeurs transcendantes pour $x = \frac{p}{q} \neq 0$ avec $|x| < q^{-(\frac{1}{2}+\varepsilon)}$, $\varepsilon > 0$.

<u>Proposition</u> 5 (Mahler 1937 a.b) :

Si $f(k)$ est un polynôme non constant, à valeurs entières, positif pour $k \geqslant 1$ et si on désigne par α le nombre dont le développement décimal est obtenu en plaçant, l'un après l'autre, à droite de la virgule, les entiers $f(1), f(2), \ldots$ écrits en base dix, alors α est transcendant sans être un nombre de Liouville.

<u>Exemple</u> : $\alpha = 0,\ 1\ 2\ 3.4\ 5\ 6\ 7\ 8\ 9\ 10\ 11 \ldots$.

Baker (1964) a montré que les nombres obtenus par la proposition 5 ne sont pas des U-nombres. Il a montré aussi qu'en général la connaissance de la mesure d'irrationnalité d'un nombre ne permet pas de dire si c'est un S-nombre un T-nombre ou un U-nombre.

Le théorème (10) admet des généralisations "arithmétiques" qui permettent d'améliorer certains des résultats précédents. Signalons une de ses conséquences :

<u>Proposition</u> 6 : Soit $g \geqslant 2$ un entier fixé. Soit (θ_n) une suite de réels de l'intervalle $]0,1[$. Soit w_n une suite de réels positifs qui tendent vers l'infini. Soit ν_n une suite d'entiers qui vérifient

$$\nu_1 \geqslant 3 , \ldots , \nu_{n+1} \geqslant \nu_n\left(1 + \frac{w_n}{\sqrt{\log \log \nu_n}}\right) .$$

Soit a_n une suite infinie d'entiers positifs, premiers avec g , qui vérifient

$$a_{n+1} \leqslant g^{\theta_n(\nu_{n+1}-\nu_n)} .$$

Si on suppose que la suite $(1-\theta_n)w_n$ tend vers l'infini et qu'il existe $p > 1$ tel que $(1-\theta_n)\nu_n^p$ tende vers l'infini alors le nombre

$$\alpha = \Sigma\, a_n\, g^{-\nu_n}$$

est transcendant.

Terminons ce paragraphe par un résultat concernant l'approximation des nombres algébriques par des nombres rationnels dont le dénominateur sont de la forme $u!$. Kasch (1953) a obtenu un résultat sur cette question. J'ai aussi obtenu, sans connaître l'exitence du travail de Kasch, un énoncé un peu différent à ce sujet. A l'intersection des deux, on trouve le résultat suivant

<u>Théorème</u> 13 (Kasch 1953) :

Soit α algébrique. Supposons $\varepsilon > 0$ fixé. Si les inégalités

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{1+\varepsilon}}$$

admettent une infinité de solutions de la forme $q_k = (u_k)!$, $(p_k, q_k) = 1$, alors on a

$$\overline{\lim} \frac{\log q_{k+1}}{\log q_k} = +\infty \, .$$

Kasch obtient par exemple la transcendance du nombre

$$\alpha = \sum_{\nu>0} \frac{1}{(2^n)!} \quad .$$

III - <u>Approximations simultanées des nombres irrationnels</u>

1. <u>Théorème</u> 14 (Dirichlet 1842) :

Soient $\alpha_1, \ldots, \alpha_\ell$ des nombres réels non tous rationnels. Alors, il y a une infinité de ℓ-uples $(\frac{p_1}{q}, \ldots, \frac{p_\ell}{q})$ avec $q > 0$ et $\text{p.g.c.d}(q, p_1, \ldots, p_\ell) = 1$ tels que

$$|\alpha_i - \frac{p_i}{q}| < \frac{1}{q^{1+\frac{1}{\ell}}} \, .$$

Pour une discussion très intéressante et de nombreux détails voir la monographie de W. Schmidt, §6.

2. Approximations simultanées des nombres algébriques par des rationnels

Théorème 15 (W. Schmidt 1970) :

Soient $\alpha_1,\dots,\alpha_\ell$ des nombres algébriques réels tels que $1,\alpha_1,\dots,\alpha_\ell$ soient linéairement indépendants sur $\mathbb{Q}$, et supposons $\varepsilon > 0$. Alors, il n'y a qu'un nombre fini d'entiers q tels que

$$q^{1+\varepsilon}\|\alpha_1 q\|\dots\|\alpha_\ell q\| < 1 .$$

Voir aussi Schmidt (1965), (1967), Wirsing (1971).

Corollaire : Les hypothèses étant celles du théorème ci-dessus, le système

$$\left|\alpha_i - \frac{p}{q}\right| < q^{-1-\frac{1}{\ell}-\varepsilon} , \quad i = 1,\dots,\ell ,$$

n'a qu'un nombre fini de solutions.

Exemple : Le théorème de Schmidt m'a permis de démontrer en particulier le résultat suivant : Si F_n désigne le n-ième nombre de Fibonacci alors

$$\alpha = \sum_{n\geq 1} \frac{1}{n!\,F_{2^n}}$$

est transcendant.

Conclusion :

Nous nous contenterons de recopier la conclusion du chapitre I du livre de Schneider. "Nous avons tenté dans ce chapitre, de tracer une voix méthodique pour reconnaître des nombres transcendants, qui sont définis par certains processus de passages à la limite convergeant bien. Il va de soi que, nous limitant aux théorèmes d'approximations généraux, nous ne pouvions d'aucune façon prétendre à un aperçu complet des résultats connus. Il semble pourtant raisonnable de pousser plus avant l'édification d'une telle méthode, d'abord en essayant d'améliorer encore les théorèmes d'approximation, puis en considérant des processus de convergence moins bons et en procédant à toute généralisation qui semble féconde pour les applications".

Références

Certaines des références ne sont pas citées dans le texte. Pour des bibliographies très complètes portant sur des sujets plus vastes voir la monographie de W. Schmidt, le long article de Fel'dman et Shidlovski (plus de 400 références!), les livres de Koksma, Perron, Cassels, Gel'fond et Schneider ainsi que la thèse de Cijsouw.

A. BAKER (1962) Continued fractions of transcendental numbers. Mathematika 9, 1-8.
(1964a) Rational approximations to certain algebraic numbers. Proc. London Math. Soc. (3) 14, 385-398.
(1964b) Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers. Quart. J. Math. Oxford Sci. (2) 15, 375-383.
(1964c) On mahler's classification of transcendental numbers. Acta Math. 111, 97-120.
(1965) On some diophantine inequalities involving the exponential function. Can. J. Math. 17, 616-626.
(1973) A sharpening of the bounds for linear forms in logarithms. Acta Arith.

G. BARON et E. BRAUNE (1970) Zür transzendenz von Lückenreihen mit ganzalgebraischen Koeffizienten und algebraischem Argument, Compositio Math., 22, 1-6.

F. BERNSTEIN (1912) Über eine Anwendung der Mengenlehre auf ein aus der Theorie der säkularen Störungen herrühendes Problem. Math. Ann. 71, 417-439.

H. BLUMBERG (1916) On a theorem of Kempner concerning transcendental numbers. Bull. Amer. Math. Soc., 22, 438-439.
(1926) Note on a theorem of Kempner concerning transcendental numbers. Bull. Amer. Math. Soc., 32, 351-356.

E. BOMBIERI (1958) Sull' approssimazione di numeri algebrici medianti numeri algebrici. Bull. Un. Mat. Ital. (3) 351-354.

E. BOREL (1909) Les probabilités dénombrables et leurs applications arithmétiques. Rend. Cir. Mat. Palermo 27, 247-271.

A. BRAUER (1929a) Uber diophantische Gleichungen mit endlich vielen Losungen. J. Reine Angew. Math., 160, 70-99.
(1929b) Uber die Approximation algebraischen Zahlen durch algebraischen Zahlen. Jber dtsch. Math. Ver. 38, 47.

A.D. BRYUNO (1964) The expansion of algebraic numbers in continued fractions (Russe) Sh. Vyschisl. Mat. i Mat. Fiz., 4, 211-221.

P. BUNDSCHUH (1971) Irrationalitätsmasse für e^a, $a \neq 0$ rational oder Liouville Zahl, Math. Ann. 192, 229-242.

H. CABANNES (1944) Application des fractions continues à la formation de nombres transcendants, Revue Sci., 82, 365-367.

J.W.S. CASSELS (1957) An introduction to diophantine approximation. Cambridge Tracts 45, Cambridge University Press.

P.L. CIJSOUW(1972) Transcendence measures. Acad. Service, Dodaarslann 95, Vinkeveen, The Netherlands.

H. COHN (1946) Note on almost algebraic numbers. Bull. Amer. Math. Soc. 52, 1042-1045.

M. CUGIANI (1947) Nuova osservazione sopra un vecchio theorema di Liouville. Bull. Uni. Mat. Ital., 2, 125-128.
(1959a) Sull'approssimabilità di un numero algebrico mediante numeri algebrici di un corpo assegnato, Bull. Un. Mat. Ital, 14, 151-162.
(1959b) Sulla approssimabilità dei numeri algebrici mediante numeri razionali, Ann. Mat. Pura Appl. 48, 135-145.

H. DAVENPORT (1937) Note on a result of Siegel. Acta Arith.2, 262-265.
(1968) A note on Thue's theorem. Mathematika 15, 76-87.

H. DAVENPORT et K.F. ROTH (1955) Rational approximations to algebraic numbers. Mathematika 2, 160-167.

L.G.P. DIRICHLET (1842) Verallzemcinerung eines satzes aus der Lehre oon den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen S.B. Preuss Akad. Wiss. 93-95.

F.J. DYSON (1947) The approximation to algebraic numbers by rationals. Acta Math. 79, 225-240.

N.J. FEL'DMAN (1962) On transcendental numbers having approximations of a given type. Uspekhi Mat. Nauk 17 (5), 145-151.
(1971) An effective sharpening of a theorem of Liouville. Izv. Akad. Nauk. SSSR Sci. Mak. 35, 973-990.

N.I. FEL'DMAN et A.B. SHIDLOVSKII (1967) The development and the present stage of the theory of transcendental numbers. Russian Math. Surveys 22, 1-79.

A.S. FRAENKEL (1962a) A class of transcendental numbers. Internal Congress Mathematicians, Stockholm, Abstracts of short communications, 26.
(1962b) On a theorem of Ridout in the theory of Diophantine approximations, Trans. Amer. Math. Soc., 105, 84-101.
(1964) Transcendental numbers and a conjecture of Erdös and Mahler. J. London Math. Soc., 39, 405-416.

A. O. GEL'FOND (1933) On necessary and sufficient criteria for the transcendence of numbers. Moskov. Gos. Univ. Ucl. Zap, 1, 6-8.

(1935) On the approximation of transcendental numbers by algebraic numbers. Dokl. Akad. Nauk SSSR, 2, 177-182.

(1949) The approximation of algebraic numbers by algebraic numbers and the theory of transcendental numbers. Uspekhi Mat. Nauk, 4 (4), 19-49 = Amer. Math. Soc. Transl. (1), 2 (1962), 81-124.

(1952) Transtsendentuye : algebraicheskie chisla, Gosudarsto. Izdat. Tekn. Teor. Lit. Moscow = Transcendental and algebraic numbers, Dover, New York 1960.

(1957) The problem of approximating algebraic numbers by rationals, Matem. prosv., 2, 35-50.

D. GIGLI (1923) Dei numeri trascendenti, 68p., Pavia

E.M. GRUBE (1965) Some p-adic and g-adic version of Roth's theorem, Dissert, Abstr. USA, 25, n°12, 7292.

R. GÜTING (1961) Approximation of algebraic numbers by algebraic numbers, Mich. Math. J., 8, 149-159.

(1963) On Mahler's function θ_n , Mich. Math. J., 10, 161-179.

(1965) Über der Zusammenhang zwischen rationalen Approximationen und Kettenbrüchen wicklungen Math.2, 90, 382-387.

G.H. HARDY et E.M. WRIGHT (1938) The theory of Numbers. Oxford, 4e édition, 1960.

H. HASSE (1939a) Simultane Approximation algebraischer Zahlen durch algebraische Zahlen, Nachr. Ges. Wiss. Göttingen, Fachgruppe I, N.F.I., 209-212.

(1939b) Simultane Approximation algebraischer Zahlen durch algebraischen Zahlen, Monatsh. Math. Phy., 48, 205-225.

A. HURWITZ (1891) Über die augenäherte Darstellung der Inationalzahlen durch rationale Brüche. Math. Ann. 39, 279-284.

S. HYYRÖ (1965a) Über Approximation algebraischen Zahlen durch rationale, Ann. Univ. Turker. Sci. A I, 84, 1-12.

(1965b) Über rationale Näherungswerte algebraischer Zahlen, Ann. Acad. Sci. Fenn. Sci. A I, Math n° 376, 1-16.

O.S. IÇEN (1956) Eine weitere Verallgemeinerung eines Schneiderschen Algebraizitätskriteriums, Rev. Fac. Sci. Univ. Istambul Sci. A, 21, 155-187.

(1957) Eine Verallgemeinerung und Ubertragung der Schneiderschen Algebraizitätskriterein ins p-adische urit Anwendung auf einen Transzendenzbeweis ins p-adischen, J. Reine Angew. Math., 198, 28-55.

T. ITIHARA et K. OISHI (1933) On transcendental numbers, Tôhoku Math. J., 37, 209-221.

S. IZUMI (1927) On transcendental numbers, Proc. Imp. Acad. Jap., 3, 300-391.

(1928) On transcendental numbers, Tôhoku Math. J., 29, 250-253.

L.C. KAPPE (1966) Zur Approximation von e^{α}, Ann. Univ. Sci. Budapest, Eötvös Sct. Math., 9, 3-14.

F. KASCH (1953) Zur Annäherung algebraischer Zahlen durch arithmetisch charakterisierte rational Zahlen, Math. Nachr., 10, 85-98.

A.J. KEMPNER (1916a) On transcendental numbers, Bull. Amer. Math. Soc., 22, 282-285.
(1916b) Generalization of a theorem on transcendental numbers, Bull. Amer. Math. Soc., 23, 59, 64-65.
(1916c) On transcendental numbers, Trans. Amer. Math. Soc. 17, 476-482.

A.Y. KHINTCHINE (1926) Zur metrischen Theorie der diophantischen Approximationen. Math. Z., 24, 706-714.
(1964) Continued fractions, Chicago Univ. Press.

J.F. KOKSMA (1936) Diophantische Approximationen. Ergebnisse d. Math. u. Grenzgeb. 4, Springer Verlag, Berlin
(1939) Über die Mahlersche Klasseneinteilung der tranzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen, Mh. Math. Phys, 48, 176-189.

O. KOLBERG (1963) A class of power series with transcendental sums for algebraic values of the variable, Arbok. Univ. Bergen Mat.-Naten. Ser. 1962, n° 18, 1-6.

R.O. KUZ'MIN (1930) On diophantine approximations to algebraic irrationals, Dokl. Akad. Nauk SSSR (A), n°8, 185-188.

S. LANG (1962) Diophantine Geometry. Interscience tracts in pure and applied math. 11, S. Wiley and Sons : New York-London.
(1965a) Report on diophantine approximations, Bull. Soc. Math. de France, 93, 117-192.
(1965b) Asymptotic approximation to quadratic irrationalities, Ann. 5 Math., 87, 481-487.
(1965c) Asymptotic approximation etc (II). Ibid., 488-496.
(1966a) Asymptotic diophantine approximation, Proc. of the Nat. Acad. of Sci., 55, 31-34.
(1966b) Introduction to diophantine approximations, Addison-Wesley Publ. Co. : Reading, Mass.
(1971) Transcendental numbers and diophantine approximations, Bull. Ann. Math. Soc., 77, 635-677.

W.J. LEVEQUE (1955) Topics in number theory, Addison-Wesley Publ. Co : Reading Mass.
(1951) Note on the transcendence of certain series, Proc. Amer. Math. Soc., 2, 401-403.

B. LEVI (1923) Seri numeri di Liouville e sur un corps non numerabile di numeri reali, AHi. Accad. naz. Lincei, Rend. (5) 32, 600-603.

J. LIOUVILLE (1844a) Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques, C. R. Acad. Sci. Paris, 18, 883-885.
(1844b) Nouvelle démonstration d'un théorème sur les irrationnelles algébriques inséré dans le compte rendu de la dernière séance, C. R. Acad. Sci. Paris, 18, 910-911.

(1851) Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnels algébriques, J. Math. Pures Appl. (1), 16, 133-142.

K. MAHLER (1931) Ein Beweis der Thue-Siegelschen Satzes über die Approximation algebraischen Zahlen für binomische Gleichungen, Math. Ann., 105, 267-276.

(1932a) Zur Approximation der Exponentialfunction und der logarithmus I et II, J. Reine Angew. Math., 166, 118-136 et 137-150.

(1932b) Über das Mass der Menge aller S. Zahlen, Math. Ann., 106, 131-139.

(1933a) Zur Approximation algebraischen Zahlen, I. Über den grossten Primteiler linärer Formen, Math. Ann., 107, 691-730..

(1933b) Zur Approximation algebraischen Zahlen, II. Uber die Anzahl der Darstellungen ganzer Zahlen durch binärer Formen, Math. Ann., 108, 37-55

(1933c) Zur Approximation algebraischen Zahlen, III. Über die mittlere Auzahl der Darstellungen grosser Zahlen durch binäre Formen, Acta Math., 62, 31-166.

(1936) Ein Analogon zu einem Schneiderscher Satz, Nederl. Akad. Wetersch. Proc. Ser. A, 39, 633-640 et 729-737.

(1937a) Arithmetische Eigenschaften einer Klasse von Dezimalbruchen, Nederl. Akad. Wetensch. Proc. Ser. A, 40, 421-428.

(1937b) Über die Dezimalbruchenwicklung gewisser Irrationalzahlen, Math. B. Zutphen 6, 22-36.

(1949a) On the theorem of Liouville in fields of positive characteristic, Canad. J. Math., 1, 397-400.

(1949b) On Dyson's improvement of the Thue-Siegel theorem, Niderl. Akad. Wetensch. Proc. Ser. A, 52, 1175-1184 = Indag. Math., 11, 449-458.

(1949c) On the continued fractions of quadratic and cubic irrationals, Ann. Math. Pura Appl., 30, 147-172.

(1951) On the generating functions of the integers with a missing digit, J. Indian Math. Soc., A 15, 33-40.

(1957) On the fractional parts of the powers of a rational number, II, Mathematika, 4, 122-124.

(1960) On a theorem by E. Bombieri, Nederl. Akad. Weteusch. Proc. Ser.A, 63 = Indag. Math., 22, 245-253 + 23 (1961) 161.

(1961) Lectures on diophantine approximations. Part.1 g-adic numbers and Roth's theorem. Univ. of Notre Dame Press. Notre Dame, Ind.

(1963) On the approximation of algebraic numbers by algebraic integers, J. Austral. Math. Soc., 1, 408-434.

(1965) Arithmetic properties of lacunary power series with integral coefficients, J. Austral. Math. Soc., 5, 56-64.

(1967) Applications of some formulae by Hermite to the approximation of exponentials and logarithms, Math. Ann., 161, 200-227.

E. MAILLET (1904) Sur les nombres quasi-rationnels et les fonctions arithmétiques ordinaires ou continues quasi-périodiques, C. R. Acad. Sci. Paris, 138, 410-411.

(1906a) Introduction à la théorie des nombres transcendants et des propriétés arithmétiques des fonctions, 274p., Paris, Gauthier-Villars.

(1906b) Sur la classification des irrationnelles, C. R. Acad. Sci. Paris, 143, 26-28.

(1907a) Sur les fractions continues arithmétiques et les nombres transcendants, J. Math. Pures Appl., (6) 3, 299-336.

(1907b) Sur les équations indéterminées en nombres transcendants de Liouville. Mem. Acad. Sci. Toulouse, (1) 7, 1-3.
(1907c) Sur les fractions continues arithmétiques et les nombres transcendants, C. R. Acad. Sci. Paris, 144, 1020-1022.

A. MARKOFF (1879) Sur les formes quadratiques binaires indéfinies. Math. Ann. 15, 381-409.

M. MIGNOTTE (1971) Approximations diophatiennes et nombres transcendants, Séminaire Delange-Pisot-Poitou 1970.71, n° 22, 18p.
(1972) Une généralisation d'un théorème de Cugiani-Mahler, Acta Arith., XXII, 57-67.

D. MORDOUCHAY-BOLTOWKOJ (1934) Sur les nombres transcendants dont les approximations successives sont définies par des équations algébriques, Rec. Math. Soc. Math. Moscou, 41, 221-232 (en russe, résumé en français).
(1935) Uber einige Eigenschaften der tranzendenten Zahlen, Tôhoku Math. 5, 40, 99-127.

J.VON NEUMANN et B. TUCKERMAN (1955) Continued expansion of $2^{1/3}$, Math. Tables Aids Comp., 9, 23-24.

I. NIVEN (1956) Irrational numbers, John Wiley, New-York (1963) Diophantine approximations, New-York, Interscience.

C.F. OSGOUD (1966a) A method in diophantine approximation, Acta Arith., 12, 111-130
(1966b) Some theorems on diophantine approximation, Trans. Amer. Math. Soc., 123, 64-87.

C.J. PARRY (1940) The p-adic generalisation of the Thue-Siegel theorem, J. London Math. Soc., 15, 293-305.
(1950) On the p-adic generalisation of the Thue-Siegel theorem, Acta Math., 83, 1-100.

L.G. PECK (1961) Simultaneous rational approximations to algebraic numbers, Bull. Amer. Math. Soc., 67, 197-201.

A. PERNA (1913) Intorno ai numeri transcendenti di Liouville, Ann. Inst. Tech. Napoli, 30, 1-11.
(1914) Sui numeri transcendenti in generale e sulla lococonstruzione in base al criterio di Liouville, Giorn. Matem. Battaglini, 52, 305-365.

O. PERRON (1913) Die Lehre von den Kettenbrüchen. Leipzig und Berlin ; 3e edition, 1954, Suttgart, B.G. Teubner.
(1921a) Irrationalzahlen. Berlin und Leipzig
(1921b) Über Diophantische Approximationen. Math. Ann., 83, 77-84.
(1932) Über mehrhrfach transzendente Erweiterungen der natürlichen Rationalitätsbereiches. Sitzunsber. Bayer. Akad. Wiss. H2, 79-86.

G. POITOU (1953) Sur l'approximation des nombres complexes par les nombres des corps quadratiques imaginaires, etc., Ann. Sci. Ec. Norm. Sup. Paris, (3), 70, 199-265.

A. PURI (1945) Transcendence of decimals, Math. Student, 12, 88-90.

K. RAMACHANDRA (1966) Approximation of algebraic numbers, Nachr. Akad. Wiss. Göttingen, Math. Phys. KI., 45-52.

R.M. REDHEFFER (1953) Power series and algebraic numbers, Amer. Math. Monthly, 60, 25-27.

R.D. RICHTMYER, M. DEVANY and N. METROPOLIS (1962) Continued expansions of algebraic numbers. Numerische Math., 4, 68-84.

D. RIDOUT (1957) Rational approximations to algebraic numbers. Mathematika. 4, 125-131.
(1958) The p-adic generalization of the Thue-Siegel-Roth theorem. Mathematika, 5, 40-48.

G. RODRIGUEZ (1964) Approssimabilità di irrazionali p-adici mediante numeri razionali, Rend. Ist. Lomb. Cl. Sci. (A), 98, 691-708.
(1965) Approssimabilità di irrazionali p-adici mediante numeri razionali, II. Bull. Uni. Mat. Ital. (3), 20, 232-244.

K.F. ROTH (1955) Rational approximations to algebraic numbers. Mathematika 2, 1-20 + Corrigendum, p. 168.

A. SCHINZEL (1967) Review of a paper by Hyyrö, ZentralblalttMath., 137, 257-258.
(1968) An improvement of Runge's Theorem on diophantine equations. Commentarii Pontif. Acad. Soc., 2, n°20.

W.M. SCHMIDT (1962) Simultaneous approximation and algebraic independence of numbers. Bull. Am. Math. Soc., 68, 475-478.
(1965) Über simultane Approximation algebraischer Zahlen durch rationale. Acta Math., 114, 159-206.
(1967) On simultaneous approximation of two algebraic numbers by rationals. Acta Math., 119, 27-50.
(1970) Simultaneous approximation to algebraic numbers by rationals. Acta Math., 125, 189-201.
(1971) Approximation to algebraic numbers. Enseign. Math., XVII, 187-253 = Monographie n° 19 de l'Enseign. Math., Imprimerie Kundig, Genève, 1972.

TH. SCHNEIDER (1935) Zur Approximation algebraischer Zahlen, Einladung 11, Deutschen Phys. Math. Tag., Stuttgart, 22.
(1936) Über die Approximation algebraischer Zahlen, J. Reine Angew. Math., 175, 182-192.
(1949) Über eine Dysonche Verschärfung des Satzes-thueschen Stazes. Arch. Math., 1, 288-295.
(1950) Zur Annäherung der algebraischen Zahlen durch rationale, J. Reine Angew. Math. 188, 115-128.
(1957) Einführung in die tranzendenten Zahlen, Springer, Berlin traduction française : Introduction aux nombres transcendants, Gauthier-Villars, Paris, 1959.

C.L. SIEGEL (1921a) Approximation algebraischer Zahlen. Math. Zeitscher., 10, 173-213.
(1921b) Über Nührungswerte algebraischer Zahlen. Math. Ann., 84, 80-99.
(1929) Über einige Anwendungen diophantischer Approximationen. Abh. d. Preuss Akad. Wiss, Math. Phys. Kl., n° 1.
(1970) Eine Erläuterungen zu Thues Untersuchen über Annäherungswerte algebraischer Zahlen und diophantische Gleichungen. Nachr. Akad. Wiss. Göttingen, Math. Phys. Kl., Nr. 8.

TH. SKOLEM (1960) A new version of some considerations of A. Thue, Math. Scand., 8, 71-80.

V.G. SPRINDZUCK (1970) An effective estimate of rational approximations to algebraic numbers (en Russe), Dokl. Akad. Nauk Belsmookoj SSR, 14, n° 8, 681-684.
(1971a) An improvement of the estimate of rational approximations to algebraic numbers (Russian). Dokl. Akad. Nauk Belsmookoj SSR, 15, n° 2, 101-104.
(1971b) On the greatest prime divisor of a binary form (Russian) Ibid., n° 5, 389-391.
(1971c) Rational approximations to algebraic numbers (Russian) Istvestia Akad. Nauk SSR, 5.

S.A. STEPANOW (1967) The approximation of an algebraic number by algebraic numbers of a special form (Russian). Vestnick Moskov. Univ., Ser. I, Math. Meh., 22, n° 6, 78-86.

E.G. STRAUS (1962) A remark on the p-adic Roth theorem, Internat. Congr. Mathem. Stockholm.

A. THUE (1908) Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen. Über rationale Annäherungswerte der reellen Wurzel der ganzen Funktion dritten Grades x^3-ax-b. On en general i store hele tal uløsbar ligning. Skrifter udgione of Videnskab s-Selskabet i Christiania.
(1909) Über Annäherungswerte algebraischer Zahlen. Journal of Math., 135 284-305.

L. TSCHAKALOFF (1921a) Arithmetische Eigenschaften der unendlichen Reihe $\sum_{\nu=0}^{\infty} x^{\nu} a^{-\frac{\nu(\nu-1)}{2}}$. Math. Amer., 80, 62-74.
(1921b) Arithmetische Eigenschaften der unendlichen Reihe, II Math. Ann., 84, 100-114.

S. UCHIYAMA (1959a) On the Thue-Siegel. Roth theorem, I, Proc. Japan Acad., 35, 413-416.
(1959b) On the Thue-Siegel. Roth theorem, II, Proc. Japan Acad., 35, 525-529.
(1960) On the Thue-Siegel. Roth theorem, III, Proc. Japan Acad., 36, 1-2.

R. WALLISER (1969) Zur Approximation algebraischer Zahlen durch arithmetisch charakterisierte algebraische Zahlen. Arch. Math (Basel), 20, 384-391.

G.C. WEBBER (1944) Transcendence of certain continued fractions, Bull. Amer. Math. Soc., 50, 736-740.

E. WIRSING (1961) Approximation mit algebraischen Zahlen beschränhten Grades. J. Reine Angew. Math., 206, 67-77.
(1971) On approximations of algebraic numbers by algebraic numbers of bounded degree. Proc. of Symp. in Pure Math., XX, (1969 Number Theory Institute) 213-247.

Les nombres colossalement abondants et le théorème de Lang

Jean-Louis NICOLAS
(Orsay 27 mars 1973)

Désignons par $\sigma(n) = \sum_{d|n} d$ la somme des diviseurs de n. On sait que σ est une fonction multiplicative et que $\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$ (cf, Hardy and Wright [2], chapitre XVI). Erdös et Alaoglu ont donné dans [1] la définition suivante

Définition : On dit que n est superabondant si :

$$(1) \qquad m < n \implies \frac{\sigma(m)}{m} < \frac{\sigma(n)}{n} .$$

On trouvera dans [1] et dans [5] quelques propriétés des nombres superabondants, en particulier :

Proposition 1 : Si la décomposition en facteurs premiers d'un nombre superabondant n est $n = 2^{\alpha_1} 3^{\alpha_2} \dots p_k^{\alpha_k}$, on a : $\alpha_1 \geqslant \alpha_2 \geqslant \dots \geqslant \alpha_k$ et $\alpha_k = 1$ sauf si $n = 4$ ou $n = 36$, en désignant par p_k le $k^{\text{ième}}$ nombre premier.

Proposition 2 : On a : $\overline{\lim} \frac{\sigma(n)}{n \log \log n} = e^\gamma$, où γ est la constante d'Euler.

Cette proposition se trouve dans Hardy and Wright [2], chapitre XVIII.

Soit $\varepsilon > 0$; il découle de la proposition 2 que $\lim_{n \to \infty} \frac{\sigma(n)}{n^{1+\varepsilon}} = 0$. La fonction $\frac{\sigma(n)}{n^{1+\varepsilon}}$ a donc un maximum absolu qu'elle atteint en un ou plusieurs points N_ε. On est ainsi conduit à la définition suivante :

Définition : On dit que N est colossalement abondant, s'il existe $\varepsilon > 0$, tel que la fonction $\frac{\sigma(n)}{n^{1+\varepsilon}}$ atteigne son maximum en N.

ε étant fixé, on a vu qu'il existe toujours au moins un nombre colossalement abondant N associé à ε et l'on a pour tout $n \geqslant 1$:

(2) $$\frac{\sigma(n)}{n^{1+\varepsilon}} \leqslant \frac{\sigma(N)}{N^{1+\varepsilon}}$$

d'autre part, tout nombre colossalement abondant est superabondant :

$$n < N \Longrightarrow \frac{\sigma(n)}{n} \leqslant \frac{\sigma(N)}{N}\left(\frac{n}{N}\right)^{\varepsilon} < \frac{\sigma(N)}{N}$$

Proposition 3 : Soit N un nombre colossalement abondant associé à ε. On définit, pour p premier et α entier $\geqslant 1$:

$$F(p,\alpha) = \frac{\log\left(1 + \frac{1}{p^{\alpha}+p^{\alpha-1}+\ldots+p}\right)}{\log p} = \frac{\log\left(\frac{p^{\alpha+1}-1}{p^{\alpha+1}-p}\right)}{\log p}$$

et pour $\alpha = 0$, $F(p,0) = +\infty$. Alors si p premier divise N avec l'exposant $\alpha \geqslant 0$, on a :

(3) $$F(p,\alpha) \geqslant \varepsilon \geqslant F(p,\alpha+1) .$$

Démonstration : Si $\alpha \geqslant 0$, on applique l'inégalité (2) avec $n = Np$. Il vient :

(4) $$\frac{\sigma(Np)}{\sigma(N)} \leqslant \left(\frac{Np}{N}\right)^{1+\varepsilon} = p^{1+\varepsilon}$$

et d'autre part :

(5) $$\frac{\sigma(Np)}{\sigma(N)} = \frac{\sigma(p^{\alpha+1})}{\sigma(p^{\alpha})} = \frac{p^{\alpha+2}-1}{p^{\alpha+1}-1} = p\left(1 + \frac{1}{p^{\alpha+1}+\ldots+p}\right)$$

En comparant (4) et (5), on obtient $\varepsilon \geqslant F(p,\alpha+1)$. L'inégalité $F(p,\alpha) \geqslant \varepsilon$ est évidente si $\alpha = 0$. Si $\alpha \geqslant 1$, on la démontre en appliquant (2) avec $n = \frac{N}{p}$.

Définition : On pose

$$E_p = \{F(p,\alpha)\ ,\ \alpha \geqslant 1\}$$

$$E = \bigcup_{p\ \text{premier}} E_p = \{\varepsilon_1\ ,\ \varepsilon_2,\ldots,\varepsilon_i,\ldots\}\ .$$

Pour tout $\eta > 0$, il n'y a qu'un nombre fini d'éléments de E supérieurs à η et l'on peut ranger les éléments de E en une suite décroissante : $\varepsilon_1 > \varepsilon_2,\ldots > \varepsilon_i$.

On pose $\varepsilon_0 = +\infty$.

Théorème : a) Si $\varepsilon \notin E$, la fonction $\frac{\sigma(n)}{n^{1+\varepsilon}}$ atteint son maximum en un seul point N_ε dont la décomposition en facteurs premiers est :

$$(6) \qquad N_\varepsilon = \prod_p p^{\alpha_p(\varepsilon)} \quad \text{avec} \quad \alpha_p(\varepsilon) = \left[\frac{\log(\frac{p^{1+\varepsilon}-1}{p^\varepsilon-1})}{\log p}\right] - 1\ .$$

Soit $i \geqslant 1$; pour tout $\varepsilon \in]\varepsilon_{i-1},\varepsilon_i[$, N_ε est constant et égal (par définition) à N_i . Les nombres N_i sont tous distincts.

b) Si les ensembles E_p sont tous disjoints, il n'y a pas d'autres nombres colossalement abondants que les N_i , et la fonction $\frac{\sigma(n)}{n^{1+\varepsilon_i}}$ atteint son maximum aux deux points N_i et N_{i+1}

c) Si les ensembles E_p ne sont pas tous disjoints, pour chaque $\varepsilon_i \in E_q \cap E_r$, la fonction $\frac{\sigma(n)}{n^{1+\varepsilon_i}}$ atteint son maximum en 4 points : N_i , qN_i , rN_i et $N_{i+1} = qr\,N_i$. Les nombres qN_i et rN_i sont colossalement abondants.

Démonstration : a) Soit p un nombre premier fixé. Comme $\varepsilon \notin E$, alors $\varepsilon \notin E_p$, et comme la suite $F(p,\alpha)$ est strictement décroissante en α , il existe α tel que :

$$(7) \qquad \frac{\log \frac{p^{\alpha+1}-1}{p^\alpha-1}}{\log p} = F(p,\alpha) > \varepsilon > F(p,\alpha+1)\ .$$

En résolvant en α , les inégalités (7) on trouve, en désignant par $[x]$ la partie entière de x

(8)
$$\alpha = \left[\frac{\log \frac{p^{1+\varepsilon}-1}{p^{\varepsilon}-1}}{\log p} \right] - 1$$

et la proposition 3 dit que l'exposant de p dans N_ε est α .

b) Choisissons $\varepsilon = \varepsilon_i = F(q,\beta)$. Pour $p \neq q$, $\varepsilon \notin E_p$ et l'exposant de p dans N_ε est déterminé par (7) ou (8). L'exposant de q peut être choisi égal à β ou $\beta-1$ d'après la proposition 3. Dans le premier cas on trouve N_{i+1} , dans le second N_i et la fonction $\frac{\sigma(n)}{n^{1+\varepsilon_i}}$ atteint son maximum en ces deux points.

c) Soit $\varepsilon = F(p,\alpha) \in E$. Alors ε est irrationnel. Si l'on avait $\varepsilon = \frac{a}{b}$, a et b entiers, on aurait $p^a = (1 + \frac{1}{p^\alpha + \dots + p})^b$ avec p^a entier et $(1 + \frac{1}{p^\alpha + \dots + p})^b$ non entier. D'après le théorème de Gelfond-Schneider ([3], chap. 3), ε est même transcendant.

Du théorème 1 de Lang ([3] chap. 2, et [4]), on déduit que si, p , q , r sont des nombres premiers distincts et si p^ε , q^ε , r^ε sont algébriques, alors ε doit être rationnel. Mais si $\varepsilon \in E_p$, p^ε est rationnel et on conclut que $E_p \cap E_q \cap E_r = \emptyset$.

S'il existe deux ensembles E_q et E_r non disjoints, et si l'on choisit $\varepsilon_i = F(q,\beta) = F(r,\gamma) \in E_q \cap E_r$, pour $p \neq q,r$ l'exposant de p est déterminé par (7) et (8), l'exposant de q peut être β ou $\beta-1$, et celui de r , γ ou $\gamma-1$ ce qui donne les 4 possibilités annoncées. Remarquons que le quotient des deux nombres colossalement abondants consécutifs qN_i et rN_i n'est pas un nombre premier.

<u>Tables numériques</u>. La table 1 donne les valeurs de $10^5\, F(p,\alpha)$. Les valeurs non indiquées sont inférieures à 1. Les colonnes "exposant = i" indiquent l'exposant de p dans N_ε. Ainsi pour $\varepsilon = 500\ 10^{-5}$, pour $p = 7$, on a $129 < 500 < 910$ et l'exposant de 7 dans N_ε est 2.

La table 2 donne les valeurs de $v^{-1}(F(p,\alpha))$ avec $v(x) = \dfrac{\log(1+\frac{1}{x})}{\log x}$. Comme v est une fonction décroissante de x, l'ordre des termes est inversé par rapport à la table 1. Elle permet de trouver les nombres colossalement abondants de plus grand facteur premier p donné. Pour avoir $p = 97$, on doit choisir $97 \leqslant x \leqslant 101$ = nombre premier suivant 97, et l'on trouve :

$$2^8\ 4^5\ 5^3\ 7^2\ 11^2\ 13\ \ 17 \ldots\ldots 97 \quad \text{pour} \quad x < 100{,}9$$

et

$$2^8\ 3^5\ 5^3\ 7^2\ 11^2\ 13^2\ 17 \ldots\ldots 97 \quad \text{pour} \quad x > 100{,}9 \ .$$

La table 3 donne la suite des nombres colossalement abondants.

Table 1

p\α	exposant = 0	α = 1	exposant = 1	α = 2	exposant = 2	α = 3	exposant = 3	α = 4	exposant = 4	α = 5
2		58 496		22 239		9 954		4 731		2 308
3		26 286		7 286		2 305		755		250
5		11 328		2 037		400		79		16
7		6 862		910		129		18		3
11		3 629		315		29		3		
13		2 889		214		16		1		
17		2 017		115		7				

Table 2

	$\alpha=1$		$\alpha=2$		$\alpha=3$		$\alpha=4$		$\alpha=5$
	2		3,29		5,44		9,08		15,36
	3		6,72		15,38		36,3		88,57
	5		16,8		60,50		230,4		920,5
	7	exposant = 1	31,4	exposant = 2	153,9	exposant = 3	812,8	exposant = 4	4 531,5
	11		73,4		554,9		4 580,6		40 080,3
	13		100,9		897,2		8 743,5		90 404,7
	17		168,8		1 951,4		24 842,7		335 898,5
	$\alpha=6$	exposant = 6	$\alpha=7$	exposant = 7	$\alpha=8$	exposant = 8	$\alpha=9$	exposant = 9	$\alpha=10$
$p=2$	26,3		45,7		80,2		142,4		255,4
$p=3$	221,7		567,6		1 480,4		3 919,7		10 507,9

Table 3

ε_1 =	58 496
ε_2 =	26 286
ε_3 =	22 239
ε_4 =	11 328
ε_5 =	9 954
ε_6 =	7 286
ε_7 =	6 862
ε_8 =	4 731
ε_9 =	3 629
ε_{10} =	2 889
ε_{11} =	2 308
ε_{12} =	2 305
ε_{13} =	2 037
ε_{14} =	2 017

n	$\sigma(n)$	$\sigma(n)/n$
1	1	1
2	3	1,5
2 3	12	2
4 3	28	2,333
4 3 5	168	2,8
8 3 5	360	3
8 9 5	1 170	3,25
8 9 5 7	9 360	3,7143
16 9 5 7	19 344	3,8381
16 9 5 7 11	232 128	4,1870
16 9 5 7 11 13	3 249 792	4,5091
32 9 5 7 11 13	6 604 416	4,5818
32 27 5 7 11 13	20 321 280	4,6993
32 27 25 7 11 13	104 993 280	4,8559
32 27 25 7 11 13 17	1 889 879 040	5,1416

Références

[1] Erdös (P) and Alaoglu (L).- On highly composite and similar numbers, Trans. Amer. math. Soc. t. 56, 1944, p. 448-469.

[2] Hardy (G.H.) and Wright (E.M.).- An introduction to the theory of numbers, 4th edition, Oxford at the Clarendon Press.

[3] Lang (S).- Introduction to transcendental numbers, Addison Wesley 1966.

[4] Lang (S.).- Nombres transcendants, Séminaire Bourbaki 18e année, 1965-66, n° 305.

[5] Nicolas (J.L.).- Ordre maximal d'un élément du groupe S_n des permutations et "higlhy composite numbers", Bull. Soc. Math. France, 97, 1969, p. 129-191.

Nombres irrationnels

Samir KARAM
(Orsay 3 avril 1973)

L'existence des nombres irrationnels fut connue depuis les grecs. Pythagore prouva que $\sqrt{2}$ est irrationnel par l'impossibilité de solutions entières de $a^2 = 2b^2$. A nos jours, il est connu que cette catégorie de nombres est très vaste puisqu'elle englobe les nombres normaux et les nombres transcendants. Cependant, l'irrationalité de nombres tels que 2^e, π^e, $\pi^{\sqrt{2}}$ et celle de la fameuse constante d'Euler $\gamma = \lim\limits_{n\to\infty} (1 + \frac{1}{2} +\ldots+ \frac{1}{n} - \log n)$ n'est pas encore établie.

I - e et π sont irrationnels

. Si $e = \frac{a}{b}$, $b \in \mathbb{N}^*$, on sait que e s'écrit

$$e = 1 + \frac{1}{1!} +\ldots+ \frac{1}{n!} +\ldots$$

Pour $K \geqslant b$ alors $b|K!$ et

$$\alpha = K!(e - 1 - \frac{1}{1!} -\ldots- \frac{1}{K!}) \quad \text{est un entier naturel}$$

tel que $0 < \alpha = \frac{1}{(K+1)} + \frac{1}{(K+1)(K+2)} +\ldots< \frac{1}{(K+1)} + \frac{1}{(K+1)^2} +\ldots= \frac{1}{K}$

ce qui est absurde.

Par contre l'irrationalité de π est moins évidente et plusieurs preuves en ont été données. On va en donner deux : la 1ère courte et élémentaire donnée par Niven ([1]), et la seconde plus générale donnée par Schneider ([2], p. 39).

. <u>1ère preuve</u> :

<u>Théorème</u> : π^2 et π sont irrationnels.

<u>Démonstration</u> : soit $f(x) = \frac{x^n(1-x)^n}{n!} = \frac{1}{n!} \sum_{m=n}^{2n} c_m x^m$ avec $c_m = (-1)^{m-n}\binom{n}{m-n} \in \mathbb{Z}$

pour $n \leqslant m \leqslant 2n$.

Si $0 < x < 1 \implies 0 < f(x) < \frac{1}{n!}$ (1).

Aussi $f(0) = 0$, $f^{(m)}(0) = 0$ si $m < n$ ou $m > 2n$, et

$$n \leqslant m \leqslant 2n \implies f^{(m)}(0) = \frac{m!}{n!} c_m \in \mathbb{Z} .$$

Ainsi $f(x)$ et toutes ses dérivées ont des valeurs entières en $x = 0$, et aussi en $x = 1$ car $f(1-x) = f(x)$.

Si π^2 était rationnel alors $\pi^2 = \frac{a}{b}$ où a et b sont entiers positifs.

Soit alors

$$G(x) = b^n\{\pi^{2n}f(x) - \pi^{2n-2}f''(x) + \pi^{2n-4}f^{(4)}(x)+\ldots+(-1)^n f^{(2n)}(x)\}$$

alors $G(0)$ et $G(1)$ sont entiers rationnels.

Aussi

$$\frac{d}{dx}\{G'(x)\sin \pi x - \pi G(x)\cos \pi x\} = \{G''(x) + \pi^2 G(x)\}.\sin \pi x$$

$$= b^n.\pi^{2n+2}.f(x).\sin \pi x = \pi^2.a^n.f(x).\sin \pi x .$$

On en tire

$$\pi\int_0^1 a^n.\sin \pi x.f(x)dx = \left[\frac{G'(x).\sin \pi x}{\pi} - G(x).\cos \pi x\right]_0^1 = G(0) + G(1) \in \mathbb{Z} .$$

Mais d'après (1)

$$0 < \pi\int_0^1 a^n.\sin \pi x.f(x)dx < \frac{\pi a^n}{n!}$$

et $\frac{\pi a^n}{n!}$ devient < 1 pour n assez grand. D'où le résultat.

. <u>2ème preuve</u> :

<u>Théorème</u> : si $\alpha \neq 0$, alors α et e^{α} n'appartiennent pas tous deux au corps des nombres de Gauss $[\mathbb{Q}(i)]$.

<u>Démonstration</u> :

On part de l'identité

$$\frac{1}{\zeta-z} = \frac{1}{\zeta-\zeta_0} + \frac{z-\zeta_0}{(\zeta-\zeta_0)(\zeta-\zeta_1)} +\ldots+ \frac{\prod_{\nu=0}^{n-1}(z-\zeta_\nu)}{\prod_{\nu=0}^{n}(\zeta-\zeta_\nu)} + \frac{\prod_{\nu=0}^{n}(z-\zeta_\nu)}{(\zeta-z)\prod_{\nu=0}^{n}(\zeta-\zeta_\nu)}$$

établie par récurrence sur n , où $\zeta_0 , \zeta_1,\ldots,\zeta_n$ et z sont des nombres complexes n'annulant pas les dénominateurs.

Soit $f(\zeta)$ une fonction de la variable complexe ζ , régulière dans $\mathcal{G}$ borné, simplement connexe, alors en multipliant l'identité par $\frac{1}{2i\pi} f(\zeta)$ et en intégrant les deux membres sur la frontière Γ de $\mathcal{G}$, on obtient, lorsque $\zeta_0,\ldots,\zeta_n$, z sont intérieurs à Γ , par l'application de l'intégrale de CAUCHY :

$$f(z) = f(\zeta_0) + a_1(z-\zeta_0) +\ldots+ a_n \prod_{\nu=0}^{n-1} (z-\zeta_\nu) + R_n(z) \qquad (2)$$

où
$$a_\ell = \frac{1}{2i\pi}\int_\Gamma \frac{f(\zeta)d\zeta}{\prod_{\nu=0}^{\ell}(\zeta-\zeta_\nu)} \quad \text{pour } \ell = 1,\ldots,n \qquad (3)$$

et
$$R_n(z) = \prod_{\nu=0}^{n}(z-\zeta_\nu) \times \frac{1}{2i\pi}\int_\Gamma \frac{f(\zeta)\,d\zeta}{(\zeta-z)\prod_{\nu=0}^{n}(\zeta-\zeta_\nu)} \qquad (4) .$$

On dira $\zeta_0,\ldots,\zeta_n,\ldots$ sont des valeurs d'interpolation pour (2). En particulier, on choisit

$$f(z) = e^{\alpha z} , \ \alpha \neq 0$$

et pour valeurs d'interpolation

$$\zeta_\nu = \begin{cases} 0 & \text{si} \quad \nu \quad \text{pair} \\ 1 & \text{si} \quad \nu \quad \text{impair} \end{cases}$$

On choisit pour Γ la circonférence de centre 0, contenant le point $\zeta = 1$ en son intérieur. On déduit alors de (3) les valeurs de a_ℓ pour $\ell = 2t+\delta$ ($t \in \mathbb{N}$ et $\delta = 0$ ou 1) :

$$a_\ell = \frac{1}{2i\pi} \int_\Gamma \frac{e^{\alpha\zeta}\, d\zeta}{\zeta^{t+1}(\zeta-1)^{t+\delta}} \quad \text{pour} \quad \ell = 1,\ldots,n \tag{5}$$

En appliquant le théorème des résidus à la fonction $z \mapsto \dfrac{e^{\alpha z}}{z^{t+1}(z-1)^{t+\delta}}$ et au contour Γ, on trouve

$$a_\ell = \frac{1}{t!} \left(\frac{e^{\alpha z}}{(z-1)^{t+\delta}}\right)^{(t)} \Bigg/_{z=0} + \frac{1}{(t-\delta+1)!} \left(\frac{e^{\alpha z}}{z^{t+1}}\right)^{(t+\delta-1)} \Bigg/_{z=1} \tag{6}$$

La dérivée $\left(\dfrac{e^{\alpha z}}{(z-1)^{t+\delta}}\right)^{(t)}$ peut s'écrire :

$$\sum_{i=0}^{t} \binom{t}{i} \alpha^i e^{\alpha z} (-1)^{t-i} (t+\delta)(t+\delta+1)\ldots(2t+\delta-i-1)(z-1)^{-(2t+\delta-i)} .$$

Le numérateur de cette quantité se présente comme un polynôme en z et une forme linéaire à coefficients entiers de $e^{\alpha z}$, $\alpha e^{\alpha z},\ldots,\alpha^t e^{\alpha z}$, et son dénominateur divise $(z-1)^{2t+\delta}$.

Si $\alpha = a_{(1)} + b_{(1)} i$ où $a_{(1)}$ et $b_{(1)} \in \mathbb{Q}$ et où q_1 est le plus petit dénominateur commun de $a_{(1)}$ et $b_{(1)}$, on obtient pour $z = 0$ un nombre de Gauss dont le dénominateur divise q_1^t. De façon analogue

$$\left(\frac{e^{\alpha z}}{z^{t+1}}\right)^{(t+\delta-1)} = \sum_{i=0}^{t+\delta-1} \binom{t+\delta-1}{i} \alpha^i e^{\alpha z} . (-1)^{(t+\delta+i-1)} (t+1)\ldots(2t+\delta-1-i) z^{-(2t+\delta-i)} .$$

Le numérateur est un polynôme en z et une forme linéaire à coefficients entiers en $e^{\alpha z}$, $\alpha e^{\alpha z},\ldots,\alpha^{t+\delta-1}e^{\alpha z}$ et dont le dénominateur divise $z^{2t+\delta}$.

Si e^{α} est un nombre de Gauss de dénominateur q_2 , on obtient pour $z = 1$ un nombre de Gauss dont le dénominateur divise $q_1^{t+\delta-1}q_2$.

Par (6) on déduit que a_ℓ est de la forme $a+bi$, a et $b \in \mathbb{Q}$ et dont le dénominateur divise $t!q_1^tq_2$. Lorsque $a_\ell \neq 0$, on aura

$$|t!.q_1^t.q_2.a_\ell| \geqslant 1 \tag{7}$$

Soit $\ell > 5$, donc $t > 2$, et choisissons pour Γ dans (5) une circonférence de rayon $|\zeta| = t$. Alors

$$|\zeta-1| > \frac{t}{2} \quad \text{car} \quad |\zeta-1| > t-1 > \frac{t}{2} .$$

De (5) et de $\displaystyle\max_{|\zeta|=t} |e^{\alpha\zeta}| \leqslant e^{|\alpha|.t}$ on tire

$$|a_\ell| < \frac{1}{2\pi}.\frac{e^{|\alpha|.t}}{t^{t+1}(\frac{t}{2})^{t+\delta}}.2\pi t = e^{|\alpha|.t}.2^{t+\delta}.t^{-(2t+\delta)} .$$

Combinée avec (7), cette majoration donne

$$t!\ q_1^t.q_2\times e^{|\alpha|.t}.2^{t+\delta} > t^{2t+\delta} \text{ , et comme } t^t > t!$$

on obtient
$$q_1^t\ q_2\ e^{|\alpha|.t}\ 2^{t+\delta} > t^{t+\delta}$$

ce qui est absurde pour t assez grand. Donc $\exists n_0 \ / \ \ell > n_0 \implies a_\ell = 0$ dans (2).

De (4) on tire la limite du reste quand $n \to \infty$. On choisit $f(z) = e^{\alpha z}$ et pour Γ le cercle de centre 0 et de rayon $|\zeta| = n$. Alors pour z fixé et n suffisamment grand, on déduit de (4) :

$$|R_n(z)| < \prod_{\nu=0}^{n} |z-\zeta_\nu| \times \frac{1}{2\pi} \times \frac{e^{|\alpha|n}}{(\frac{n}{2})^{n+2}} \times 2\pi n$$

et on voit que $\lim\limits_{n\to\infty} |R_n(z)| = 0$.

Dans (2) avec $f(z) = e^{\alpha z}$, on passe à la limite en n . Alors $e^{\alpha z}$ aura une série d'interpolation ayant un nombre fini de termes $\neq 0$, donc un polynôme, ce qui est absurde lorsque $\alpha \neq 0$.

II – Autres propriétés des irrationnels

Théorème : x réel est rationnel $\Longleftrightarrow$ le développement décimal de x est périodique.

Théorème : x entier algébrique et $x \notin \mathbb{Z} \Longrightarrow x$ est irrationnel.

Théorème : Les entiers algébriques réels de degré quelconque fixé $n \geqslant 2$ sont denses dans $\mathbb{R}$.

Démonstration :

Soient α et β réels, $\alpha < \beta$. Prouvons alors que $\exists \gamma \in \bar{\mathbb{Q}} \cap \mathbb{R}$, $\deg.\gamma = n$ et $\alpha < \gamma < \beta$. $\mathbb{Q}$ étant la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.

Notons d'abord que

$$x + \alpha > 0 \Longrightarrow$$

$$(x+\beta)^n - (x+\alpha)^n = \{(x+\alpha) + (\beta-\alpha)\}^n - (x+\alpha)^n > n(x+\alpha)^{n-1}(\beta-\alpha) .$$

Mais $n(x+\alpha)^{n-1}(\beta-\alpha)$ tend vers l'infini pour x tendant vers l'infini. On en déduit $\exists j \in \mathbb{N}^*$ tel que

$$j+\alpha > 0 \quad \text{et} \quad j+\beta > 0 \quad \text{et} \quad (j+\beta)^n - (j+\alpha)^n > 5 .$$

Ainsi l'intervalle ouvert de $\mathbb{R}$ d'extrémités $(j+\alpha)^n$ et $(j+\beta)^n$ contient au moins 4 entiers positifs consécutifs et en particulier un de la forme $4K+2$.

Mais l'application $]\alpha,\beta[\to](j+\alpha)^n , (j+\beta)^n[$

$$x \mapsto (j+x)^n$$

étant continue alors on tire

$$\exists \gamma \in \mathbb{R} , \alpha < \gamma < \beta \text{ et } (j+\gamma)^n = 4K+2 .$$

Il s'ensuit que γ est entier algébrique racine du polynôme unitaire

$$f(x) = (x+j)^n - 2(1+2K) = 0 .$$

Pour finir la démonstration, il faut établir que $\deg.\gamma = n$, ou que $f(x)$ est irréductible sur $\mathbb{Q}$. Mais cela équivaut à montrer que

$f(x-j) = x^n - 2(1+2K)$ est irréductible sur $\mathbb{Q}$, ce qui résulte du critère d'Eisenstein :

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \qquad a_i \in \mathbb{Z}$$

si $\exists p$ premier $p | a_i$ pour $i = 1,2,\dots,n$

$$p \nmid a_0 \text{ et } p^2 \nmid a_n$$

alors $f(x)$ est irréductible sur $\mathbb{Q}$. Ici $p = 2$.

BIBLIOGRAPHIE

[1] NIVEN.- Bull. Amer. Math. Soc. 53 (1947) p. 509.

[2] SCHNEIDER.- Initiation aux nombres transcendants. G.V. Paris (1959).

[3] NIVEN.- Irrational numbers 1963. John Wiley and Sons.

Classification des nombres d'après Mahler

Christian LAVAULT
(Orsay 8 mai 1973)

I. Introduction :

On sait construire certains nombres transcendants par différentes méthodes, on en connait qui sont valeurs de certaines fonctions transcendantes quand l'argument est algébrique. Il est naturel de songer à ranger en classes distinctes les nombres transcendants et même tous les nombres complexes ; on sait en effet que l'ensemble des nombres transcendants a la puissance du continu puisque l'ensemble des nombres algébriques est dénombrable.

Le plus naturel, pour répartir les nombres complexes en classes est d'entreprendre une classification du point de vue de la dépendance algébrique ; on souhaiterait que des nombres de classes différentes soient toujours algébriquement indépendants et, si possible, que les nombres d'une classe donnée soient algébriquement dépendants ; i.e. qu'ils vérifient une relation du type $\sum_{\sigma=0}^{s} \sum_{\tau=0}^{t} A_{\sigma,\tau}\, \xi^{\sigma}\, \eta^{\tau} = 0$ pour $A_{\sigma,\tau}$ entiers ξ et η complexes donnés.

En particulier, les nombres algébriques devraient former une classe.

Il n'existe pas actuellement de partition vérifiant toutes ces propriétés. La classification de Mahler est cependant un premier pas dans cette voie :

1 - Les nombres de classes distinctes sont algébriquement indépendants.

2 - Mais la dépendance des nombres d'une classe donnée n'est vérifiée que pour

les A-nombres (nombres algébriques).

De plus, une des classes (T) a longtemps été considérée comme pouvant être vide et, surtout, la classe S contient "presque tous" les nombres transcendants. Nous verrons en abordant la classification de Koksma ce que le "presque tous" signifie.

II. Principe utilisé par Mahler :

Soit $\xi \in \mathbb{C}$, on cherche à déterminer le degré d'exactitude avec lequel des polynômes en ξ non identiquement nuls et à coefficients entiers approchent zéro non trivialement. Exactement, soit $\xi \in C$ et n et H entiers fixés ; on forme :

$$w_n(H,\xi) = \underset{\substack{0 \leqslant |a_\nu| \leqslant H \\ \text{entiers} \\ \Sigma a_\nu \xi^\nu \neq 0}}{\mathrm{Min}} \left(\left| \sum_{\nu=0}^{n} a_\nu \xi^\nu \right| \right)$$

On voit que si $n \geqslant 1$ et $H \geqslant 1$, $w_n(H,\xi) \leqslant 1$. En effet, l'expression entre parenthèse vaut 1 pour $a_0 = 1$, $a_i = 0$ $i = 1,2\ldots n$ et ne croît pas quand n et H croissent.

Formons maintenant $w_n(\xi) = w_n = \overline{\lim\limits_{H \to \infty}} \dfrac{-\mathrm{Log}\, w_n(H,\xi)}{\mathrm{Log}\, H}$

$$\text{et} \quad w(\xi) = w = \overline{\lim_{n \to \infty}} \frac{w_n(\xi)}{n}$$

$$\text{moyennant quoi,} \quad w = \overline{\lim_{n\to\infty}}\ \overline{\lim_{H\to\infty}} \frac{-\mathrm{Log}\, w_n(H,\xi)}{n\ \mathrm{Log}\, H} .$$

Pour $n \geqslant 1$, il est clair que $0 \leqslant w_n \leqslant \infty$ et $0 \leqslant w \leqslant \infty$; de plus, on a $w_{n+1}(H,\xi) \leqslant w_n(H,\xi)$ donc $w_{n+1}(\xi) \geqslant w_n(\xi)$.

w est donc une quantité qui est soit finie non négative, soit infinie positive

On définit alors μ comme, s'il existe, le plus petit indice tel que $w_\mu = \infty$

et, dans le cas contraire, (i.e : si w_n admet pourtant n une borne supérieure finie) comme $\mu = \infty$.

Il suit que, pour μ fini, $w = \infty$.

Pour ξ donné, μ et w ne peuvent donc être tous deux finis. Il existe donc pour les valeurs de μ et w les 4 possibilités suivantes qui définissent une partition de l'ensemble des $\xi \in \mathbb{C}$:

ξ est un A-nombre si $w = 0$, $\mu = \infty$

S-nombre si $0 < w < \infty$, $\mu = \infty$

T-nombre si $w = \infty$, $\mu = \infty$

U-nombre si $w = \infty$, $\mu < \infty$.

La classe T est celle dont on a ignoré longtemps si elle est vide ; la classe S contient "presque tous" les nombres transcendants ; les classes T et U se laissent à nouveau subdiviser en conservant la propriété d'indépendance algébrique de 2 nombres de classes distinctes.

Ces sous-partitions s'obtiennent en remplaçant pour les T-nombres

$$\overline{\lim_{n\to\infty}} \frac{w_n(\xi)}{n} \quad \text{par} \quad \overline{\lim_{n\to\infty}} \frac{w_n(\xi)}{n^\sigma} \qquad \sigma > 1$$

et pour les U-nombres, $\overline{\lim\limits_{H\to\infty}} \dfrac{-\mathrm{Log}\, w_n(H,\xi)}{\mathrm{Log}\, H}$ par

$$\overline{\lim_{H\to\infty}} \frac{-\mathrm{Log}(H,\xi)}{(\mathrm{Log}\, H)^\tau} \qquad \tau > 1$$

$(\mathrm{Log}\, H)^\tau$ et n^σ deviennent alors des fonctions à croissance plus rapide que $\mathrm{Log}\, H$ et n.

III. Conséquences directes :

1. Si ξ est un S-nombre, on a $\overline{\lim\limits_{H\to\infty}} \frac{w_n(\xi)}{n} = w(\xi) < \infty$ par conséquent,

$\exists\, \theta_o > 0$ tel que $w_n(\xi) = \overline{\lim\limits_{H\to\infty}} \frac{-\mathrm{Log}\, w_n(H,\xi)}{\mathrm{Log}\, H} < \theta_o n \qquad n = 1,2,\ldots$

Donc, $\forall\, \varepsilon > 0$, $\exists\, H_o(n,\theta_o,\varepsilon)$ tel que $\forall\, H > H_o(n,\theta_o,\varepsilon)$,

$$\frac{-\mathrm{Log}\, w_n(H,\xi)}{\mathrm{Log}\, H} < (\theta_o+\varepsilon)n$$

donc $w_n(H,\xi) > H^{-(\theta_o+\varepsilon)n}$.

Si on pose

$$c_n = c(\xi,n,\theta_o,\varepsilon) = \min_{H=1}^{H_o(n,\theta_o,\varepsilon)} \left(\tfrac{1}{2}\, w_n(H,\xi).H^{(\theta_o+\varepsilon)n}, 1\right)$$

on a : $\qquad w_n(H,\xi) > c_n\, H^{-(\theta_o+\varepsilon)n}$ avec $c_n > 0$ indépendant de H.

et on en tire une

Définition : on appelle type du S-nombre ξ le nombre θ borne inférieure de tous les θ_i pour lesquels il existe un c_n tel que $w_n(H,\xi) > c_n\, H^{-\theta n}$ $\forall\, H = 1,2,\ldots$

On a : $\theta = \sup\limits_{n=1}^{\infty} \left(\frac{w_n(\xi)}{n}\right)$.

2. Soit ξ un U-nombre :

$$\exists\, \mu = \mu(\xi) < \infty \text{ tel que } \forall n \geqslant \mu,\ w_n(\xi) = \infty$$

c'est-à-dire $\qquad \overline{\lim\limits_{H\to\infty}} \frac{-\mathrm{Log}\, w_n(H,\xi)}{\mathrm{Log}\, H} = \infty$.

Dans ce cas, pour tout $\theta > 0$ et tout $n \geqslant \mu$, on peut trouver une suite partielle H_λ telle que

$$\frac{-\mathrm{Log}\, w_n(H_\lambda,\xi)}{\mathrm{Log}\, H_\lambda} > \theta n$$

soit : $\qquad w_n(H_\lambda,\xi) < H_\lambda^{-\theta n}$.

Il existe donc des polynômes à coefficients entiers, de hauteur $H \leqslant H_\lambda$ pour lesquels on ait, quel que soit H_λ et θ donnés, $0 \neq |\sum_{\nu=0}^{n} a_\nu \xi^\nu| < H_\lambda^{-\theta n}$ avec $|a_\nu| \leqslant H_\lambda$ $\lim_{\lambda\to\infty} H_\lambda = \infty$.

[On rappelle à ce sujet que H est hauteur d'un polynôme $P(x) = \sum_{\sigma=0}^{s} a\sigma\, x^{s-\sigma}$ si $H = \operatorname{Max}_{\sigma=0}^{s} |a\sigma|$].

Il existe une infinité de tels polynômes. Il en résulte que tout nombre de Liouville est un U-nombre tel que $\mu = 1$. [Un nombre de Liouville ξ est tel que il existe une suite p_n/q_n avec $(p_n, q_n) = 1$ et s_n telle que $\overline{\lim}\, s_n = \infty$ telles que

$$|\xi - \frac{p_n}{q_n}| \leqslant \frac{1}{q_n^{s_n}} \text{].}$$

3. Si ξ est un T-nombre, il ne peut être un U-nombre donc

$$w_n(H,\xi) > c_n . H^{-\theta_n n} \quad (n = 1, 2 \ldots)$$

$$\begin{cases} \theta_n = \theta(\xi, n) > 0 \\ c_n = c(\xi, n, \theta_n) . \end{cases}$$

Mais, si $\overline{\lim}_{n\to\infty} \theta_n < \infty$, alors ξ vérifie la propriété des S-nombres vue au 1. Ceci n'est pas possible et donc $\overline{\lim}_{n\to\infty} \theta_n = \infty$ pour tout T-nombre.

IV. <u>Deux théorèmes</u> :

<u>Théorème</u> 1 : tout nombre algébrique est un **A**-nombre et tout **A**-nombre est algébrique.

<u>Démonstration</u> : α) Soit ξ algébrique de degré s et $P(x) = \sum_{\nu=0}^{n} a_\nu x^\nu$ un polynôme à coefficients entiers de hauteur H tel que $P(\xi) \neq 0$.

On a : $0 \neq |\sum_{\nu=0}^{n} a_\nu \xi^\nu| > \frac{c}{H^{s-1}}$ où $c = c(\xi,n)$

ceci entraîne : $w_n(\xi) \leqslant \overline{\lim_{H\to\infty}} (\frac{-\mathrm{Log}\ c}{\mathrm{Log}\ H} + s-1) = s-1$ et donc, $w(\xi) \leqslant \overline{\lim_{n\to\infty}} \frac{s-1}{n} = 0$

donc ξ est un $\mathbb{A}$-nombre $(w = 0)$.

β) Soit $\xi \in \mathbb{C}$ <u>transcendant</u>, on sait que $w_n(H,\xi) < c\, H^{-\frac{n-1}{2}}$ donc

$w_n(\xi) \geqslant \frac{n-1}{2}$ et $w(\xi) \geqslant \frac{1}{2}$ donc $w \neq 0$ et ξ n'est pas un $\mathbb{A}$-nombre. cqfd.

<u>Théorème</u> 2 : si deux nombres ξ et η sont algébriquement dépendants, ils appartiennent à la même classe.

La démonstration est assez longue et technique (voir Schneider Introduction aux nombres transcendants p. 70).

V. <u>Un résultat sur les S-nombres et le lien avec la classification de Koksma</u> :

<u>Proposition</u> : a) tous les nombres réels sont des S-nombres de type $1 \leqslant \theta \leqslant 2$ sauf ceux d'un ensemble négligeable pour la mesure de Lebesgue sur la droite.

b) tous les nombres complexes sont des S-nombres de type $\frac{1}{2} \leqslant \theta \leqslant 3/2$ sauf ceux d'un ensemble Lebesgue-négligeable dans le plan.

Cette proposition exprime le fait que "presque tous" les nombres transcendants sont des S-nombres. Sa démonstration est simplifiée si on considère la classification de Koksma pour les nombres transcendants, classification en S^*-nombres
T^*-nombres
U^*-nombres

qui a la propriété que $\xi \in S^* \Longrightarrow \xi \in S$.

. On fait donc la démonstration pour les S^*-nombres et on en déduit la propriété pour les S-nombres.

Actuellement, on arrive à un résultat encore plus précis qui avait été conjecturé par Mahler :

<u>Théorème</u> : "presque tous" les nombres réels sont des S-nombres de type 1 et "presque tous" les complexes sont des S-nombres de type $\frac{1}{2}$.

<u>Bibliographie</u> : Schneider, Th.- Introduction aux nombres transcendants. Paris, Gauthier Villars, 1959.

Nombres transcendants p-adiques

Alin RALAIVOLA
(Orsay 15 mai 1973)

Transcendance de α^{β} dans le cas p-adique

Soit p un nombre premier. On note $\mathbb{C}_p$ le complété de la clôture algébrique du corps p-adique $\mathbb{Q}_p$ et $|\ |_p$ la valeur absolue ultramétrique associée : je la prends normalisée c'est-à-dire $|p|_p = \frac{1}{p}$.

Dans le corps $\mathbb{C}_p$, α^{β} n'est autre que l'expression $\exp(\beta \log \alpha)$. D'où le besoin de restreindre β et α à des domaines particuliers qui sont ici les domaines de définition de la fonction logarithme et de la fonction exponentielle p-adiques.

Voici le théorème à démontrer :

Soient α et β deux éléments du corps $\mathbb{C}_p$ tels que $|\alpha-1|_p < 1$ et $|\beta \log \alpha|_p < p^{-\frac{1}{p-1}}$. On suppose que α et β sont algébriques sur Q et que β est irrationnel.

Alors : α^{β} est transcendant.

Pour la démonstration on aura besoin des deux lemmes suivants. On utilisera la notation suivante :

Notation : soit $f(z) = \sum a_n z^n$ une série entière dans $\mathbb{C}_p$. On note pour R réel positif $(R > 0)$ la quantité :

$$|f|_R = \sup |a_n|_p R^n .$$

Il est facile de voir que : 1) $|f+g|_R \leqslant \sup(|f|_R, |g|_R)$

2) $|\lambda f|_R \leqslant |\lambda|_p \, |f|_R$

3) $|f.g|_R = |f|_R . |g|_R$.

Supposons que pour $R > 0$, $|f|_R$ soit fini : pour R' tel que $0 < R' \leqslant R$ $|f|_{R'}$ est également fini et :

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

Le premier lemme nous donne une amélioration de cette inégalité.

Premier lemme dû à Schwarz (cf [1]). Soit $f(z) = \sum a_n z^n$ une série convergente dans le disque $|z|_p \leqslant R$. Soit $R' < R$, donc f converge aussi dans le disque $|z|_p \leqslant R'$. Supposons que f a h racines dans $|z|_p \leqslant R'$.

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

Démonstration : supposons que a soit racine de f dans $|z|_p \leqslant R'$. On peut écrire $f(z) = (z-a).f_1$ où $|f_1|_R < +\infty$. Ceci est évident pour $a = 0$ sinon on fait une translation pour se ramener à ce cas.

Par récurrence on peut écrire :

$$f(z) = P(z).g(z) \quad \text{où} \quad P(z) = \prod_{i=1}^{h} (z-a_i) \quad \text{et} \quad |g|_R < +\infty .$$

On a d'une manière évidente :

$$|P|_R = R^h \quad \text{et} \quad |P|_{R'} = R'^h .$$

Enfin :

$$|f|_{R'} = R'^h . |g|_{R'} \leqslant R'^h |g|_R = (\frac{R'}{R})^h R^h |g|_R = (\frac{R'}{R})^h . |f|_R \qquad \text{c.q.f.d.}$$

Le deuxième lemme concerne la taille d'un nombre algébrique : on verra que les expressions sont identiques dans le cas p-adique et le cas complexe.

<u>Définition</u> : soient K un corps de nombres, et $x \in K$. On appelle <u>dénominateur</u> de x le plus petit entier $D \geqslant 1$ tel que Dx soit entier sur z.

Posons :

$$\theta(x) = \sup(D, |\sigma(x)|_p)$$

où σ parcourt l'ensemble des plongements de x dans $\mathbb{C}$. On appelle <u>taille de</u> x, noté $t(x)$, le nombre $\operatorname{Log} \theta(x)$ c'est-à-dire :

$$t(x) = \sup(\operatorname{Log} D, \operatorname{Log}|\sigma(x)|_p).$$

<u>Deuxième lemme</u> (cf [1])

Soit $d = [K : \mathbb{Q}]$. Alors $\log |y|_p \geqslant -2d\ t(y)$ pour tout $y \in K^*$.

<u>Démonstration</u> : soit D le dénominateur de y. Notons $z = Dy$: z est entier sur $\mathbb{Q}$ et $|D|_p \leqslant 1$, donc $|y|_p \geqslant |z|_p$. Soit $N(z)$ la norme de z : c'est un entier, divisible par z, donc $|z|_p \geqslant |N(z)|_p$. La formule du produit donne $|N(z)|_p \geqslant \frac{1}{|N(z)|_\infty}$ en notant $|\ |_\infty$ la valeur absolue usuelle. Or $N(z)$ est le produit des conjugués de z et la norme usuelle de ceux-ci est majorée par $D.\theta(y)$, donc :

$$|N(z)|_p \geqslant D^{-d}\theta(y)^{-d} \geqslant \theta(y).^{-2d} \qquad \text{c.q.f.d.}$$

<u>Démonstration du théorème</u> : faisons une remarque préliminaire

<u>Remarque 1</u> : soit β tel que $|\beta|_p = p^{-k}$ où $k \in Z$. Multiplions β par p^k : il est clair alors que $|\beta p^k|_p = 1$ donc appartient au disque $|z|_p \leqslant 1$. Donc quitte à multiplier β et $\log \alpha$ par des puissances de p, on peut supposer que $i + j\beta$ appartient au disque $|z|_p \leqslant 1$ (i et j sont des entiers positifs) et que la fonction $\alpha^z = \exp(z \log \alpha)$ est convergente dans $|z|_p \leqslant R$ où $R > 1$.

Raisonnons donc par l'absurde. Supposons que α^{β} est algébrique et considérons le corps $K = \mathbb{Q}(\alpha, \beta, \alpha^{\beta})$.

Déterminons les coefficients $p(\lambda,\mu)$ du polynôme à deux variables de $K[X,Y]$ noté $P(X,Y)$ tel que si :

$$P(X,Y) = \sum_{\lambda=0}^{p(N)-1} \sum_{\mu=0}^{q(N)-1} p(\lambda,\mu)\, X^{\lambda}\, \varphi^{\mu}$$

la fonction

$$F(z) = P(z, \alpha^{z}) \quad \text{où} \quad z \in \mathbb{C}_p$$

ait des racines aux points $i + j\beta$ où $0 \leqslant i,j \leqslant S(N) - 1$.

(Les quantités $p(N)$, $q(N)$, $S(N)$ dépendent proportionnellement du nombre N qu'on suppose très grand et qu'on fera tendre à l'infini à la fin de la démonstration).

On a donc un système d'équations définies par :

$$F(i+j\beta) = \sum_{\nu} \sum_{\mu} p(\lambda,\mu)\ (i+j\beta)^{\lambda} . \alpha^{i\mu} . (\alpha^{\beta})^{j\mu} = 0 \qquad (1)$$

pour $0 \leqslant i,j \leqslant S(N)-1$ $\quad 0 \leqslant \lambda \leqslant p(N)-1$ $\quad 0 \leqslant \mu \leqslant q(N)-1$.

Les inconnues sont les $p(\lambda,\mu)$ et les coefficients sont donnés par :

$(i+j\beta)^{\lambda} \alpha^{i\mu}\ \beta^{j\mu}$.

<u>MAJORATION de la taille des coefficients</u>

Soit d un dénominateur commun de α, β, α^{β} : alors $d^{p(N)+2q(N).\delta(N)}$ est un dénominateur du coefficient $(i+j\beta)^{\lambda}.\alpha^{i\mu}.(\alpha^{\beta})^{j\mu}$, puisque :

$$d^{p(N)+2q(N).S(N)} . (i+j\beta)^{\lambda}\ \alpha^{i\mu}\ (\alpha^{\beta})^{j\mu} = (di+jd\beta)^{\lambda} . (d\alpha)^{i\mu} (d.\alpha^{\beta})^{j\mu} . d^{p(N)-\lambda+2q(N)\delta(N)-i\mu-j\mu}$$

est un produit d'entiers de K, donc lui-même entier de K.

Pour tout plongement σ de ce coefficient dans $\mathbb{C}$ on a :

$$|\sigma(\text{coefficient})|_p \leqslant |i+j\sigma(\beta)|_p^{\lambda} . |\sigma(\alpha)|_p^{i\mu} |\sigma(\alpha^\beta)|_p^{j\mu} \leqslant |S(N)|_p^{p(N)} . (j+|\sigma(\beta)|_p)^{p(N)} .$$
$$. |\sigma(\alpha)|_p^{p(N).S(N)} . |\sigma(\alpha^\beta)|^{q(N).S(N)} .$$

Comme $|S(N)|_p \leqslant 1$, la taille des coefficients est majorée par :

$$t(\text{coefficient}) << p(N) + 2q(N).S(N).$$

D'après le lemme de Siegel, pour que le système d'équations (1) ait des relations il suffit que le nombre d'inconnues soit supérieur au nombre d'équations c'est-à-dire $p(N)q(N) > S(N)^2$.

Par exemple : $p(N) = 2N^3$, $q(N) = N$ et $S(N) = N^2$.

Puisque $p(N)$ et $q(N).S(N)$ sont du même ordre de grandeur on a donc :

$$t(\text{coefficient}) << N^3 .$$

Il existe donc un ensemble $\{p(\lambda,\mu)\}$ de solutions non triviales du système d'équations et, de plus,

$$t(p(\lambda,\mu)) << N^3 \qquad \forall\lambda . \forall\mu$$

Les fonctions z et α^z sont algébriquement indépendantes puisque z et e^z le sont. La fonction $F(z)$ n'est donc pas identiquement nulle. D'après la remarque 1 les points $i+j\beta$ sont dans le disque $|z|_p \leqslant 1$ $(0 \leqslant i,j \leqslant N^2-1)$.

C'est encore vrai pour tout $\underbrace{\text{indice}}_{i,j}$ plus grand que N^2 . Soit donc $M(N)$ le plus petit entier tel que :

$$F(i+j\beta) = 0 \qquad \text{pour} \quad 0 \leqslant i,j \leqslant M(N)-1$$

et
$$F(i_o+j_o\beta) \neq 0 \quad \text{pour} \quad 0 \leqslant i_o,j_o \leqslant M(N) .$$

Evidemment $M(N)$ est un entier supérieur ou égal à N^2 .

<u>Existence de</u> $M(N)$. La fonction $F(z)$ est une série entière et on sait que le zéro d'une série entière est isolé. Dans le compact $|z|_p \leqslant 1$, les zéros de $F(z)$ ne sauraient être infinité puisque 0 deviendrait un point d'accumulation (limite de p^n lorsque $n \to \infty$) et ceci contredirait le fait d'être isolé.

On pourra utiliser aussi le théorème suivant pour l'existence de $M(N)$ (cf [2]).

<u>Théorème</u> : soit f une fonction méromorphe dans un disque $\mathfrak{D}$ et (z_n) une suite de points différents convergeant vers $z_0 \in \mathfrak{D}$. Supposons que pour tout i , $i = 0,1\ldots z_i$ pas pôle de f et $f(z_i) = 0$ pour $i = \ ,\ldots,n$. Alors f est identiquement nulle.

Notons γ l'élément $F(i_0+j_0\beta)$.

<u>Majoration de la taille de</u> γ .

γ s'écrit :

$$\gamma = F(i_0+j_0\beta) = \sum_{\nu}\sum_{\mu} p(\lambda,\mu)(i_0+j_0\beta)^{\lambda}\ \alpha^{i_0\mu}(\alpha^{\beta})^{j_0\mu} .$$

Donc γ est un élément algébrique sur $\mathbb{Q}$ comme étant une somme de produits d'éléments algébriques.

Pour tout plongement σ de γ dans le corps de complexes $\mathbb{C}$ on a :

$$|\sigma(\gamma)|_p \leqslant \sup_{(\lambda,\mu)} |\sigma(p(\lambda,\mu))|_p . |i_0+j_0\ \sigma(\beta)|_p^{\lambda} . |\sigma(\alpha)|_p^{i_0\mu} . |\sigma(\alpha^{\beta})|_p^{j_0\mu}$$

de $t(p(\lambda,\mu)) << N^3$ je déduis que $|\sigma(p(\lambda,\mu))|_p << e^{N^3}$

donc :

$$|\sigma(\gamma)|_p << e^{N^3} . (1, |\sigma(\beta)|_p)^{2N^3} . |\sigma(\alpha)|_p^{M(N).N} . |\sigma(\alpha^{\beta})|_p^{M(N)N} . |M(N)|_p^{2N^3} .$$

Puisque $|M(N)|_p \leqslant 1$:

$$\operatorname{Max}_{\sigma} |\sigma(\gamma)|_p << N^3 + 2N^3 . \operatorname{Max}_{\sigma} . \operatorname{Log}(1+|\sigma(\beta)|_p) + M(N).N \operatorname{Max}_{\sigma}(\operatorname{Log}|\sigma(\alpha)|_p + \operatorname{Log}|\sigma(\alpha^{\beta})|_p) - 2N^3.$$

Remarque 2 : puisque $|\alpha-1|_p < 1$ on a $|\alpha|_p = |\alpha-1+1|_p \leqslant \sup(|\alpha-1|_p,1) = 1$ donc $|\alpha|_p = 1$.

– D'autre part, $|\alpha^\beta|_p = |\alpha^\beta-1+1|_p \leqslant \sup(|\alpha^\beta-1|_p,1)$; il suffit donc de démontrer que $|\alpha^\beta-1|_p$ est supérieur strictement à 1 pour déduire que $|\alpha^\beta|_p > 1$.

D'après [3] (p. 49-50) on a $|\exp(x)-1|_p = |x|_p$

donc :

$$|\alpha^\beta-1|_p = |\beta \text{ Log } \alpha|_p .$$

D'après la remarque 1 on suppose $|\beta|_p = 1$ donc $|\beta \text{ Log } \alpha|_p = |\text{Log } \alpha|$. Toujours d'après cette même remarque, α^z converge dans $|z|_p \leqslant R$ où $R > 1$, on peut supposer que $|\text{Log } \alpha|_p > 1$ et par conséquent $|\alpha^\beta|_p > 1$.

On déduit donc de cette remarque 2 et du fait que $M(N) \gg N^2$:

$$\text{Log } |\bar{\gamma}|_p \ll N^3 .$$

Si d est un dénominateur commun de α, β et α^β, d^{3N^3} est un dénominateur de γ car :

$$d^{3N^3}\gamma = \sum_\lambda \sum_\mu p(\lambda,\mu)\ (di_o+j_o d\beta)^\lambda (d\alpha)^{i_o\mu} . (d\alpha^\beta)^{j_o\mu} d^{3N^3-\lambda-i_o\mu-j_o\mu}$$

est une somme de produits d'éléments entiers sur $\mathbb{Q}$, donc est entier lui-même. On déduit donc une majoration de la taille de γ soit : taille de $\gamma \ll N^3$.

Majoration de $|\gamma|_p$.

D'après la remarque 1, F est convergente dans $|z|_p \leqslant R$ où $R > 1$ et s'annulle aux $M(N)^2$ points $i+j\beta$ de $|z|_p \leqslant 1$.

Il est clair que :

$$|\gamma|_p = |F(i_o+j_o\beta)|_p \leqslant |F|_1 .$$

Le premier lemme donne :

$$|F|_1 \leqslant \left(\frac{1}{R}\right)^{M(N)^2} |F|_R .$$

Et comme $M(N) \geqslant N^2$ et $R > 1$

$$|F|_1 \leqslant \left(\frac{1}{R}\right)^{N^4} . |F|_R \qquad (2)$$

Réécrivons la quantité $F(z)$:

$$F(z) = \sum_{\nu=0}^{p(N)-1} \sum_{\mu=0}^{q(N)-1} p(\lambda,\mu)\, z^{\lambda} (\alpha^z)^{\mu} .$$

Les fonctions z et α^z sont continues dans le compact $|z|_p \leqslant R$, donc bornées par conséquent :

$$|F|_R \leqslant p(N).q(N)|p(\lambda,\mu)|_p . C_1^{p(N)}\ C_2^{q(N)} \leqslant C_3^{N^3}$$

où C_1, C_2, C_3 sont des constantes positives indépendantes de N .

De l'expression (2) on obtient :

$$|F|_1 \leqslant \left(\frac{1}{R}\right)^{N^4}\ C_3^{N^3} \leqslant C_4^{-N^4}$$

où C_4 est une autre constante positive supérieure à 1 strictement. Cette dernière majoration se déduit du fait que $N^4 > N^3$ dès que $N \geqslant 2$.

<u>Conclusion</u>. Utilisons le deuxième lemme $\mathrm{Log}|\gamma|_p \geqslant -2d\ t(\gamma)$ où $d = [K : \mathbb{Q}]$.

On obtient alors la contradiction suivante : $N^4 << N^3$ et le théorème est démontré.

Bibliographie

[1] Les dépendances d'exponentielles p-adiques par Jean-Pierre Serre, séminaire Delange Pisot Poitou 7e année 1965-66 n° 15.

[2] Un théorème plus général de transcendance p-adique fut démontré par W. Adams dans American Journal of Mathematics, 1966 (88) pages 279-308.

[3] Georges BACHMAN. Introduction to p-adic numbers and valuation theory. Academic Press.

La conjecture de Schanuel

Michel WALDSCHMIDT
(Orsay 22 mai 1973)

La conjecture la plus générale concernant les propriétés de transcendance de la fonction exponentielle a été énoncée par S. Schanuel (cf. [5] p. 30).

(S) Si $x_1,\ldots,x_n$ sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, alors le degré de transcendance sur $\mathbb{Q}$ du corps

$$\mathbb{Q}(x_1,\ldots,x_n, e^{x_1},\ldots,e^{x_n})$$

est supérieur ou égal à n .

Cette conjecture (S) contient toutes les propriétés connues sur la nature arithmétique des valeurs de la fonction exponentielle (mises à part, évidemment, les propriétés liées aux approximations diophantiennes) ; elle est également réputée contenir toutes les conjectures raisonnables que l'on peut énoncer sur ces valeurs. Nous étudions ici plusieurs conséquences de (S) .

Préliminaires

Nous noterons $\mathbb{Q}$ le corps des nombres rationnels, $\overline{\mathbb{Q}}$ le corps des nombres algébriques, c'est-à-dire la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.

Si E est une extension d'un corps k et si $x_1,\dots,x_n$ sont des éléments de E , on dit que $x_1,\dots,x_n$ sont algébriquement indépendants sur k (ou bien qu'ils forment une partie algébriquement libre de E sur k) si l'homomorphisme canonique

$$\beta : k[X_1,\dots,X_n] \to k[x_1,\dots,x_n] ,$$

(de l'anneau des polynômes sur k à n indéterminées, sur le sous-anneau de E engendré par $x_1,\dots,x_n$), défini par

$$\beta(X_i) = x_i \quad \text{pour} \quad 1 \leqslant i \leqslant n ,$$

est un isomorphisme.

Dans ces conditions, tout sous-ensemble de l'ensemble $\{x_1,\dots,x_n\}$ forme une partie algébriquement libre de E sur k ; en particulier chacun des x_i est transcendant sur k .

On dira donc qu'une partie F de E est algébriquement libre sur k si toute partie finie de F est algébriquement libre sur k .

Une partie B de E est une base de transcendance de E sur k si B vérifie l'une des trois propriétés équivalentes suivantes :

(i) B est une partie maximale algébriquement libre de E sur k.

(ii) B est une partie algébriquement libre de E sur k , et E est une extension algébrique de $k[B]$.

(iii) B est une partie minimale de E telle que E soit une extension algébrique de $k[B]$.

Toute extension E de k admet une base de transcendance, et deux telles bases sont équipotentes. Si E admet une base de transcendance finie, le nombre $n \geqslant 0$ d'éléments de cette base est appelé <u>degré de transcendance</u> (ou <u>dimension algébrique</u>) de E sur k, et noté

$$n = \dim_k E \ .$$

Si E_1 (resp. k_1) est une extension algébrique de E (resp. k), on a

$$\dim_k E = \dim_{k_1} E_1 = \dim_{k_1} E = \dim_k E_1 \ .$$

Notons qu'une extension de k est algébrique si et seulement si elle a un degré de transcendance nul sur k.

Par convention, nous dirons que des nombres complexes $x_1,\ldots,x_q$ sont <u>algébriquement indépendants</u> s'ils sont algébriquement indépendants sur $\mathbb{Q}$ (ou sur $\overline{\mathbb{Q}}$, cela revient au même), c'est-à-dire si

$$\dim_{\mathbb{Q}} \mathbb{Q}(x_1,\ldots,x_q) = q \ .$$

Un nombre complexe est dit <u>transcendant</u> (resp. <u>algébrique</u>) s'il est transcendant sur $\mathbb{Q}$ (resp. algébrique sur $\mathbb{Q}$, c'est-à-dire dans $\overline{\mathbb{Q}}$).

Enfin nous dirons qu'un nombre complexe ℓ est un <u>logarithme</u> d'un nombre a si $e^{\ell} = a$; en particulier, un nombre ℓ est un logarithme d'un nombre algébrique si $e^{\ell} \in \overline{\mathbb{Q}}$. Par exemple $i\pi$ est un logarithme d'un nombre algébrique.

La notation Log sera utilisée exclusivement pour désigner le logarithme népérien d'un nombre réel positif.

§1. Le théorème de Lindemann-Weierstrass

Le plus ancien résultat d'indépendance algébrique, dû à Lindemann et Weierstrass [4, 5, 8], résoud la conjecture (S) dans le cas particulier où $x_1,\dots,x_n$ sont algébriques.

Théorème 1.1. *Si $x_1,\dots,x_n$ sont des nombres algébriques, $\mathbb{Q}$-linéairement indépendants, alors les nombres*

$$e^{x_1},\dots,e^{x_n}$$

sont algébriquement indépendants sur $\mathbb{Q}$.

On peut énoncer ce résultat sous la forme équivalente suivante :

Théorème 1.2. *Si $\alpha_1,\dots,\alpha_m$ sont des nombres algébriques deux à deux distincts, alors les nombres*

$$e^{\alpha_1},\dots,e^{\alpha_m}$$

sont $\overline{\mathbb{Q}}$-linéairement indépendants.

On déduit de cet énoncé le théorème de Hermite Lindemann :

Théorème 1.3. *Si $\alpha \neq 0$ est algébrique, alors e^{α} est transcendant.*

Donc, si $\ell \neq 0$ est un logarithme d'un nombre algébrique, alors ℓ est transcendant. En particulier

Théorème 1.4. *Le nombre π est transcendant.*

En choisissant $x_1 = 1$ et $x_2 = i\pi$, on constate que (S) implique également la

Conjecture 1.5. *Les deux nombres* e *et* π *sont algébriquement indépendants.*

En fait (S) contient des propriétés encore plus fortes sur e et π (voir (4.1) et (4.2)).

§2. Indépendance algébrique de logarithmes

Après avoir examiné le cas où $x_1,\ldots,x_n$ sont algébriques, il est naturel d'examiner le cas où $e^{x_1},\ldots,e^{x_n}$ sont algébriques ; la conclusion de (S) est alors l'indépendance algébrique de $x_1,\ldots,x_n$.

Conjecture 2.1. *Soient* $\ell_1,\ldots,\ell_n$ *des logarithmes de nombres algébriques. Si* $\ell_1,\ldots,\ell_n$ *sont* $\mathbb{Q}$-*linéairement indépendants, alors* $\ell_1,\ldots,\ell_n$ *sont algébriquement indépendants.*

Un premier pas vers cette conjecture, consistant à étudier les polynômes de degré 1 en $\ell_1,\ldots,\ell_n$ à coefficients algébriques a été effectué par Baker [1] qui démontre le

Théorème 2.2. *Si* $\ell_1,\ldots,\ell_n$ *sont des logarithmes* $\mathbb{Q}$-*linéairement indépendants de nombres algébriques, alors les nombres*

$$1,\ell_1,\ldots,\ell_n$$

sont $\overline{\mathbb{Q}}$-*linéairement indépendants.*

On déduit du théorème 2.2 le théorème 1.3 de Hermite Lindemann, ainsi que le théorème de Gel'fond Schneider [4, 5, 8].

Théorème 2.3. Si $\ell \neq 0$ et $b \notin \mathbb{Q}$ sont deux nombres complexes, l'un des trois nombres

$$b \ , \ a = e^{\ell} \ , \ a^{b} = e^{b\ell}$$

est transcendant.

§3. Indépendance algébrique de puissances algébriques de nombres algébriques

Le théorème 2.3 de Gel'fond Schneider suggère le problème suivant (Schneider [8] problème 7).

Conjecture 3.1. Si $\ell \neq 0$ est un logarithme d'un nombre algébrique α, et si $1,\beta_1,\ldots,\beta_n$ sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, alors les nombres

$$\alpha^{\beta_1} = e^{\ell\beta_1},\ldots,\alpha^{\beta_n} = e^{\ell\beta_n}$$

sont algébriquement indépendants.

La conjecture 3.1 est une conséquence immédiate de (S) ; d'ailleurs, si on on considère les nombres

$$x_1 = \ell \ , \ x_2 = \beta_1\ell,\ldots,x_{n+1} = \beta_n\ell \ ,$$

on remarque que (S) contient même l'indépendance algébrique des nombres

$$\ell \ , \ e^{\ell\beta_1},\ldots,e^{\ell\beta_n} \ .$$

D'autre part l'exemple des nombres

$$\ell = \operatorname{Log} 2 \ ; \ \beta_1 = 2+\sqrt{2} \ ; \ \beta_2 = 2-\sqrt{2}$$

montre qu'il est insuffisant de supposer $\beta_1,\ldots,\beta_n$ irrationnels et $\mathbb{Q}$-linéairement indépendants pour que la conclusion de la conjecture 3.1 puisse être vraie.

Un cas particulier de 3.1 est une conjecture de Gel'fond :

Conjecture 3.2. *Si $\ell \neq 0$ est un logarithme d'un nombre algébrique α, et si β est un nombre algébrique de degré $d = [\mathbb{Q}(\beta) : \mathbb{Q}] \geqslant 2$, alors le degré de transcendance sur Q du corps*

$$\mathbb{Q}(\alpha^{\beta},\ldots,\alpha^{\beta^{d-1}})$$

est égal à $d-1$.

Le théorème 2.3 de Gel'fond Schneider résoud le cas $d=2$, et Gel'fond [4] a résolu le cas $d=3$.

Ramachandra a cherché à généraliser 3.2. Il avait démontré [7] le

Théorème 3.3. *Si x_1,x_2,x_3 (resp. y_1,y_2) sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, alors l'un des six nombres*

$$e^{x_i y_j} \ , \ i = 1,2,3 \ , \ j = 1,2$$

est transcendant.

Il avait remarqué ensuite que, si x_1,x_2,x_3 (resp. $y_1,\ldots,y_d$) sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, alors $d-1$ des nombres

$$e^{x_i y_j} \ , \ i = 1,2,3 \ , \ j = 1,\ldots,d$$

sont transcendants. Aussi avait-il conjecturé que

(3.4) d−1 de ces nombres sont algébriquement indépendants.

D'autre part, S. Lang [5] avait également démontré 3.3, puis il avait conjecturé :

Conjecture 3.5. Si x_1, x_2 (resp. y_1, y_2) sont deux nombres complexes $\mathbb{Q}$-linéairement indépendants, alors un des quatre nombres

$$e^{x_1 y_1}, \ e^{x_1 y_2}, \ e^{x_2 y_1}, \ e^{x_2 y_2}$$

est transcendant.

Cette conjecture (3.5) est équivalente au problème 1 de Schneider [8] :

Conjecture 3.6. Si ℓ_1, ℓ_2, ℓ_3 sont des logarithmes de nombres algébriques, tels que

$$\ell_1 \neq 0 \ ; \ \frac{\ell_2}{\ell_1} \notin \mathbb{Q} \ ; \ \frac{\ell_3}{\ell_1} \notin \mathbb{Q} \ ,$$

alors le nombre

$$\exp\left[\frac{\ell_2 . \ell_3}{\ell_1}\right]$$

est transcendant.

En suivant le même raisonnement que Ramachandra, on observe que, si la conjecture 3.5 est vraie, et si x_1, x_2 (resp. $y_1, \ldots, y_n$) sont des nombres complexes $\mathbb{Q}$-linéairement indépendants, alors $n-1$ des nombres

$$e^{x_i y_j} \ , \ i = 1, 2 \ ; \ j = 1, \ldots, n$$

sont Aussi était-il naturel de conjecturer que $n-1$ de ces nombres sont algébriquement indépendants (cf [9]).

Or il n'en est rien, comme le montre l'exemple des nombres

$x_1 = 1$; $x_2 = \sqrt{2}$; $y_1 = \operatorname{Log} 2$; $y_2 = \sqrt{2} \operatorname{Log} 2$; $y_3 = \operatorname{Log} 3$; $y_4 = \sqrt{2} \operatorname{Log} 3$;

(l'indépendance linéaire de y_1, y_2, y_3, y_4 est une conséquence de 2.3 par exemple).

De même les nombres

$$x_1 = 1 \qquad x_2 = \sqrt[3]{2} \qquad ; x_3 = \sqrt[3]{4} \qquad ;$$

$$y_1 = \operatorname{Log} 2 \; ; \; y_2 = \sqrt[3]{2} \operatorname{Log} 2 \; ; \; y_3 = \sqrt[3]{4} \operatorname{Log} 2 \; ;$$

$$y_4 = \operatorname{Log} 3 \; ; \; y_5 = \sqrt[3]{2} \operatorname{Log} 3 \; ; \; y_6 = \sqrt[3]{4} \operatorname{Log} 3 \; ,$$

fournissent <u>un contre-exemple à</u> (3.4).

On peut néanmoins énoncer une conjecture, conséquence de (S), et contenant (3.5).

<u>Conjecture</u> 3.7. <u>Soient</u> $u_1, \ldots, u_m$ <u>des nombres complexes</u>, $\mathbb{Q}$-<u>linéairement indépendants</u> ; <u>soit</u> v <u>un nombre complexe, transcendant sur</u> $\mathbb{Q}$. <u>Alors le degré de transcendance sur</u> $\mathbb{Q}$ <u>du corps</u>

$$\mathbb{Q}(e^{u_1}, \ldots, e^{u_m}, e^{vu_1}, \ldots, e^{vu_m})$$

<u>est supérieur ou égal à</u> $m-1$.

Pour montrer que 3.7 (et donc aussi 3.5, qui correspond à $m=2$) est une conséquence de (S), on ordonne $u_1, \ldots, u_m$ de telle manière que, pour un entier ℓ, $0 \leqslant \ell \leqslant m$,

$$(u_1, \ldots, u_m \, , \, vu_1, \ldots, vu_\ell)$$

soit une base du $\mathbb{Q}$-espace vectoriel engendré par $u_1, \ldots, u_m$, $vu_1, \ldots, vu_m$.

Comme v est transcendant (le résultat serait vrai aussi pour v algébrique de degré supérieur ou égal à $\ell-1$), le degré de transcendance sur $\mathbb{Q}$ du corps

$$\mathbb{Q}(v, u_1, \ldots, u_m)$$

est inférieur ou égal à $\ell+1$. D'autre part, si (S) est vraie, le degré de transcendance du corps

$$\mathbb{Q}(u_1, \ldots, u_m \, , \, vu_1, \ldots, vu_\ell \, , \, e^{u_1}, \ldots, e^{u_m} \, , \, e^{vu_1}, \ldots, e^{vu_\ell})$$

est supérieur ou égal à $m+\ell$; a fortiori le degré de transcendance sur $\mathbb{Q}$ du corps

$$\mathbb{Q}(u_1, \ldots, u_m \, , \, vu_1, \ldots, vu_m \, , \, e^{u_1}, \ldots, e^{u_m} \, , \, e^{vu_1}, \ldots, e^{vu_m})$$

est supérieur ou égal à $m+\ell$. Donc $m-1$ des nombres

$$e^{u_i} \, , \, e^{vu_i} \qquad (1 \leqslant i \leqslant m)$$

sont algébriquement indépendants.

§4. Autres conséquences de (S)

La conjecture de Schanuel permet de déterminer le degré de transcendance de corps obtenus en adjoignant à $\mathbb{Q}$ des nombres complexes définis à partir de la fonction exponentielle (ou de fonctions logarithmes). On constate dans chaque exemple que le degré de transcendance est le plus grand que l'on puisse espérer. Ainsi, pour illustrer ce fait, nous allons montrer que (S) contient la

Conjecture 4.1. *Les* 16 *nombres suivants sont algébriquement indépendants* :

$$e, \pi, e^{\pi}, \mathrm{Log}\ \pi, e^{e}, \pi^{e}, \pi^{\pi}, \mathrm{Log}\ 2, 2^{\pi}, 2^{e}, 2^{i}, e^{i}, \pi^{i}, \mathrm{Log}\ 3, (\mathrm{Log}\ 2)^{\mathrm{Log}\ 3}, 2^{\sqrt{2}} \, .$$

(En particulier, chacun de ces nombres doit être transcendant).

Considérons les 17 nombres $x_1,\ldots,x_{17}$ suivants :

$1, i\pi, \pi, \mathrm{Log}\,\pi, e, e\,\mathrm{Log}\,\pi, \pi\,\mathrm{Log}\,\pi, \mathrm{Log}\,2, \pi\,\mathrm{Log}\,2, e\,\mathrm{Log}\,2, i\,\mathrm{Log}\,2, i, i\,\mathrm{Log}\,\pi, \mathrm{Log}\,3,$
$\mathrm{Log}\,\mathrm{Log}\,2, \mathrm{Log}\,3.\mathrm{Log}\,\mathrm{Log}\,2, \sqrt{2}\,\mathrm{Log}\,2$.

Pour que 4.1 soit une conséquence de (S), il suffit que (S) entraîne l'indépendance linéaire de $x_1,\ldots,x_{17}$ sur $\mathbb{Q}$; il suffit donc, a fortiori, que (S) contienne l'indépendance algébrique des 6 nombres

$$\pi, \mathrm{Log}\,\pi, e, \mathrm{Log}\,2, \mathrm{Log}\,3, \mathrm{Log}\,\mathrm{Log}\,2 .$$

Le même raisonnement, à partir des nombres $x'_1,\ldots,x'_6$:

$$1, i\pi, \mathrm{Log}\,\pi, \mathrm{Log}\,2, \mathrm{Log}\,3, \mathrm{Log}\,\mathrm{Log}\,2$$

ramène le problème à l'indépendance algébrique des 5 nombres

$$\pi, \mathrm{Log}\,\pi, \mathrm{Log}\,2, \mathrm{Log}\,3, \mathrm{Log}\,\mathrm{Log}\,2 ,$$

donc à l'indépendance linéaire des nombres

$$i\pi, \mathrm{Log}\,\pi, \mathrm{Log}\,2, \mathrm{Log}\,3, \mathrm{Log}\,\mathrm{Log}\,2 .$$

En considérant les exponentielles des parties réelles, on doit montrer que π, 2, 3, $\mathrm{Log}\,2$ sont multiplicativement indépendants (sur $\mathbb{Z}$) ; or on sait déjà que (S) contient l'indépendance algébrique de π et $\mathrm{Log}\,2$, d'après (2.1) (c'est-à-dire en choisissant $x_1 = i\pi$ et $x_2 = \mathrm{Log}\,2$ dans (S)). D'où le résultat.

Une conséquence un peu moins évidente de (S) est une conjecture de Lang [6]. On définit par récurrence une suite croissante (K_n) de sous-corps de $\mathbb{C}$ de la manière suivante :

$$K_o = \bar{\mathbb{Q}} \; ; \; K_n = \overline{K_{n-1}(\exp(K_{n-1}))} \; ;$$

autrement dit K_n est la clôture algébrique du corps obtenu en adjoignant à K_{n-1} les nombres

$$\exp t \; , \; t \in K_{n-1} \; .$$

<u>Conjecture</u> 4.2

$$\pi \notin \bigcup_{n \geq 0} K_n \; .$$

La démonstration de l'implication (S) $\Longrightarrow$ (4.2) est esquissée dans [6].

Terminons en indiquant une dernière conjecture [3], conséquence de (S), et contenant les résultats et les conjectures des paragraphes 1 et 2

<u>Conjecture</u> 4.3. <u>Soient</u> $\alpha_1, \ldots, \alpha_n$ <u>des nombres algébriques,</u> $\mathbb{Q}$-<u>linéairement indépendants ; soient</u> $\ell_1, \ldots, \ell_m$ <u>des logarithmes</u> $\mathbb{Q}$-<u>linéairement indépendants de nombres algébriques. Alors les nombres</u>

$$e^{\alpha_1}, \ldots, e^{\alpha_m} \; , \; \ell_1, \ldots, \ell_m$$

<u>sont algébriquement indépendants.</u>

Références

[1] Alan BAKER. Linear forms in the logarithms of algebraic numbers. I, II, III, Mathematika, 13 (1966), 204-216 ; ibid., 14 (1967), 102-107, 220-228.

[2] I. KAPLANSKY. Hilbert's problems (en préparation ; voir : The Mathematical Intelligencer, n° 5 (1973) p. 3-5).

[3] Alexandre Ossipowitch GELFOND. Sur quelques résultats nouveaux dans la théorie des nombres transcendants. C. R. Acad. Sci. Paris, Ser. **A**, 119 (1934) p. 259.

[4] Alexandre Ossipovitch GELFOND. Transcendental and algebraic numbers, G.I.T.T.L., Moscou,(1952)Trad. anglaise, Dover, New-York, (1960).

[5] Serge LANG. Introduction to transcendental numbers. Addison-Wesley, Reading, Mass., (1966).

[6] Serge LANG. Transcendental numbers and diophantine approximations. Bull. Amer. Math. Soc., 77, n° 5 (1971), 635-677.

[7] K. RAMACHANDRA. Contributions to the theory of transcendental numbers. Acta Arith., 14 (1968), 65-88.

[8] Theodor SCHNEIDER. Introduction aux nombres transcendants. Springer Verlag, Berlin, (1957) ; trad. française Paris, Gauthier-Villars, (1959).

[9] Michel WALDSCHMIDT. Indépendance algébrique des valeurs de la fonction exponentielle, Bull. Soc. Math. France, t. 99 (1971) 285-304, et Séminaire Delange Pisot Poitou, 1970/71, n° 6, 8p.

Université de Paris-Sud
Mathématique Bâtiment 425
91405 ORSAY