INITIATION AUX NOMBRES TRANSCENDANTS

par Michel WALDSCHMIDT

Alors qu'elles étaient, à leurs débuts, assez obscures et compliquées, certaines démonstrations de transcendance ont été énormément simplifiées au cours de la dernière décade. Cette clarification est essentiellement due à Lang, qui présentait au Séminaire Bourbaki en 1966 (exposé n° 305) un théorème sur la transcendance de nombres exp $(x_i y_j)$, et qui le démontrait *par la méthode classique de Gel'fond-Schneider, sauf que l'on s'en tire sans équation différentielle, et que la démonstration s'en trouve simplifiée au point d'être complètement triviale* (sic).

Il se trouve qu'en apportant une modification très minime dans le choix de certains paramètres, on peut démontrer de la même manière le théorème de Gel'fond et Schneider sur la transcendance de a^b. C'est ce que nous verrons dans la première partie, après avoir effectué un rapide survol de l'historique de ce problème.

Dans la deuxième partie, nous étudierons, dans le même esprit de simplification, un théorème de Baker sur l'indépendance linéaire de logarithmes de nombres algébriques.

I. Le Théorème de Gel'fond et Schneider sur la transcendance de a^b

§ 1. Aperçu historique [4,8]

En 1748, un siècle avant que Liouville ne construise le premier exemple de nombre transcendant, Euler conjecturait que le logarithme, pour une base rationnelle, d'un nombre rationnel (qui n'est pas une puissance rationnelle de la base) est transcendant.

En 1900, au Congrès de Paris, Hilbert constatait que cette conjecture n'était toujours pas résolue, les seules méthodes connues ne pouvant s'appliquer qu'aux valeurs, en des points algébriques, de fonctions satisfaisant une équation différentielle à coefficients algébriques. C'est ainsi que Hermite (1873) avait obtenu la transcendance de e, Lindemann (1882) celle de e^α, pour α algébrique non nul (et par conséquent la transcendance de π), et Weierstrass (1885) l'indépendance algébrique de $e^{\alpha_1}, \ldots, e^{\alpha_n}$, où $\alpha_1, \ldots, \alpha_n$ sont des nombres algébriques **Q**-linéairement indépendants.

En 1900, donc, dans son exposé « Mathematische Probleme » (voir: D. Hilbert, Gesammelte Abbhandlungen, New York, 1965; ou bien: *Bull. Amer. Math. Soc.*, *8*, (1902), 437-479), Hilbert énonçait une liste de 23 problèmes, dont le septième, « Irrationalität und Tranzendenz bestimmter Zahlen », reprenait la conjecture d'Euler:

Etudier la transcendance, ou même seulement l'irrationalité, des nombres a^b, *puissance d'un nombre algébrique* $a \neq 0, 1$ *par un nombre algébrique irrationnel* b, *par exemple* $2^{\sqrt{2}}$ *et* $e^\pi = i^{-2i}$.

Hilbert considérait ce problème comme très difficile, et il pensait que sa solution ne serait trouvée qu'après celles de l'hypothèse de Riemann et de la conjecture de Fermat.

Pourtant, dès 1929, une attaque sérieuse de ce problème est donnée par Gel'fond, à partir de travaux de Polya. Polya avait étudié, depuis 1914, les fonctions analytiques f qui vérifient $f(Z) \in \mathbf{Z}$ pour tout $Z \in \mathbf{Z}$, ce qui lui avait permis d'établir un premier *lien entre l'ordre d'une fonction analytique et la nature arithmétique de ses valeurs*. Gel'fond s'intéressa aux fonctions qui vérifient $f(Z) \in \mathbf{Z}$ pour tout $Z \in \mathbf{Z}[i]$, anneau des entiers de Gauss. Sa méthode, appliquée à des fonctions telles que $e^{\pi Z}$, lui permit d'apporter une première réponse au 7^e problème de Hilbert: si $a \neq 0, 1$ est algébrique, et si b est irrationnel quadratique, alors a^b est transcendant; en particulier e^π est transcendant.

Ce résultat fut amélioré par Kuzmin, puis Boehle. Et, en 1934, la solution définitive est trouvée, par Gel'fond et par Schneider, indépendamment l'un de l'autre.

THÉORÈME 1. (Gel'fond, Schneider). — *Soient* a, b *deux nombres algébriques,* $a \neq 0$, $a \neq 1$ *et* b *irrationnel. Alors le nombre :*

$$a^b = \exp(b . \operatorname{Log} a)$$

est transcendant.

Les méthodes de Gel'fond et de Schneider ont connu depuis des développements considérables. En 1934 et 1937, Schneider étudiait les valeurs de fonctions elliptiques; puis, en 1949, il généralisait tous ses résultats en un *critère de dépendance algébrique pour des fonctions analytiques* [10].

En 1949 également, Gel'fond obtenait des propriétés d'indépendance algébrique [5]; par exemple, si $a \neq 0, 1$ *est algébrique, et* b *irrationnel* *cubique, les deux nombres* a^b *et* a^{b^2} *sont algébriquement indépendants* (sur **Q**).

Ces résultats ont été étendus par Lang (depuis 1963) aux points de variétés de groupes [7, 8]; Lang déduit ses énoncés de *critères*, analogues à celui obtenu par Schneider en 1949, sur *la répartition des points où plusieurs fonctions méromorphes prennent simultanément des valeurs algébriques*. Grâce à une variante de ces critères, Ramachandra, en 1967, énonça de nouvelles propriétés des fonctions elliptiques [9]. Enfin Bombieri, en 1970, a permis l'extension de ces critères aux fonctions de plusieurs variables (voir [8]).

On ne peut pas terminer cet aperçu historique sans mentionner les travaux de Baker [1] (dont nous parlerons plus longuement dans la deuxième partie) et sans formuler quelques conjectures; les plus célèbres concernent:

— *l'indépendance algébrique de logarithmes de nombres algébriques*, par exemple la transcendance de:

$$\mathrm{Log}\, 2 \, . \, \mathrm{Log}\, 3 \, ,$$

et

— *l'ndépendance algébrique des nombres* e *et* π, par exemple la transcendance de:

$$e + \pi \, .$$

Nous verrons dans la deuxième partie pourquoi la méthode de Baker ne permet pas actuellement de résoudre la première de ces conjectures.

La deuxième conjecture (sur e et π) paraît vraiment hors d'atteinte des techniques actuelles, et il semble que, compte tenu des méthodes connues, le problème suivant soit plus accessible:

Les nombres π *et* e^π *sont-ils algébriquement indépendants* ?

Cette hiérarchie entre plusieurs problèmes non résolus doit être accompagnée de toute la prudence enseignée par l'expérience de Hilbert!

§ 2. Principes des démonstrations

Les résultats dont nous venons de parler ont tous à la fois un aspect arithmétique (la propriété pour un nombre d'être algébrique ou transcendant) et un aspect analytique (par exemple la définition de $a^b = \exp(b.\, \mathrm{Log}\, a)$). Le lien entre ces deux aspects est fourni par des résultats du type de ceux de Polya: on peut minorer l'ordre de croissance d'une fonction entière transcendante qui possède des valeurs algébriques en de nombreux points algébriques.

Regardons plus précisément comment exprimer cette propriété dans le cas du théorème 1. Supposons que a, b et a^b sont trois nombres algébriques, avec $a \neq 0$, $a \neq 1$, et $b \notin \mathbf{Q}$. Soit $\mathrm{K} = \mathbf{Q}(a,b,a^b)$.

Les deux fonctions

$$e^Z \text{ et } e^{bZ}$$

sont algébriquement indépendantes (sur $\mathbf{C}$), prennent leurs valeurs dans K aux points $Z = n.\ \mathrm{Log}\ a$, $n \in \mathbf{Z}$, et vérifient des équations différentielles à coefficients dans K. *Gel'fond* étudiait alors les propriétés d'une fonction

$$F(Z) = P(e^Z, e^{bZ}),$$

où $P \in K[X, Y]$ (voir par exemple [5] chap. III, § 2., ou [11] chap. III, § 2.).

Sous les mêmes hypothèses concernant a, b et a^b, les deux fonctions

$$Z \text{ et } a^Z$$

sont algébriquement indépendantes et prennent des valeurs dans K aux points $Z = n + m\,b$, $(n,m) \in \mathbf{Z} \times \mathbf{Z}$. *Schneider* utilise alors une fonction auxiliaire

$$F(Z) = P(Z, a^Z),$$

où $P \in K[X, Y]$ (voir par exemple [11] chap. III, § 1., ou [9] chap. III, § 1.). On n'a ici aucun renseignement sur les dérivées de F, mais on connaît « plus » de points Z où $F(Z) \in K$.

La méthode de Gel'fond est généralement mieux connue, grâce à... Schneider. En effet, en 1949, utilisant la méthode de Gel'fond (avec d'importantes améliorations), Schneider a obtenu un théorème général (voir § 1) suivant lequel deux fonctions algébriquement indépendantes f_1, f_2 d'ordre fini, satisfaisant un certain type d'équations différentielles à coefficients algébriques, ne peuvent prendre simultanément des valeurs algébriques qu'en un nombre fini de points. On obtient la transcendance de a^b en choisissant $f_1(Z) = e^Z$, $f_2(Z) = e^{bZ}$, et la transcendance de e^α, pour α algébrique non nul, en choisissant $f_1(Z) = Z$ et $f_2(Z) = e^{\alpha Z}$. Ce critère de Schneider [10] a été notablement simplifié par Lang [7] chap. III.

On peut également généraliser la méthode de Schneider pour l'appliquer à des fonctions f_1, f_2 algébriquement indépendantes; le résultat est par exemple une majoration du rang du $\mathbf{Z}$-module des points algébriques communs; lorsqu'on choisit $f_1(Z) = Z$ et $f_2(Z) = a^Z$, on retrouve le théorème 1. Un tel critère a été obtenu par Ramachandra [9] (le critère similaire qu'a obtenu Lang [7] chap. II, th. 2, ne contient pas la transcendance de a^b, parce que les deux fonctions f_1, f_2 sont supposées de même ordre; évidemment, on peut facilement corriger ce défaut). Mais les énoncés sont ici beaucoup plus compliqués.

Et pourtant, si on se contente de la transcendance de a^b, la méthode de Schneider et Ramachandra fournit une démonstration plus facile. C'est ce que nous allons voir.

§ 3. Schéma des démonstrations

Les démonstrations de transcendance que nous étudions, se font toutes suivant le même schéma général (à des permutations près des différents pas). On suppose que plusieurs fonctions méromorphes algébriquement indépendantes, $f_1, \ldots, f_d$, prennent des valeurs algébriques (ainsi, éventuellement, que leurs dérivées) en de « nombreux » points, et on désire obtenir une contradiction.

Premier pas. — Construction d'une fonction auxiliaire

Un lemme de Siegel (lemme 2), utilisant le « principe des tiroirs » de Dirichlet, permet de construire un polynôme non nul:

$$P \in \overline{\mathbf{Q}}\,[X_1, \ldots, X_d]$$

à coefficients algébriques, tel que la fonction entière $F = P(f_1, \ldots, f_d)$ s'annule (éventuellement avec un ordre de multiplicité élevé) en certains points.

Deuxième pas. — Construction d'un nombre algébrique $\gamma \neq 0$

On détermine un point $Z_0 \in \mathbf{C}$ où F (ou bien l'une de ses dérivées) prend une valeur algébrique $\gamma \neq 0$.

On peut effectuer ce pas en utilisant le fait que le nombre de zéros d'une fonction entière d'ordre $\leq \rho$ dans un disque $\{Z \in \mathbf{C}; |Z| \leq R\}$ est $0(R^\rho)$; on utilise aussi quelque fois un calcul de déterminant, ou encore la propriété pour une fonction entière non nulle de ne pas avoir toutes ses dérivées nulles en un point. Enfin, dans certains cas particuliers, on peut utiliser des formules d'interpolation pour obtenir une majoration très précise du nombre des zéros de F (voir par exemple le lemme 4 ou la majoration (20)).

Troisième pas. — Partie analytique : majoration de $|\gamma|$

Le lemme de Schwarz et le principe du maximum permettent de majorer une fonction possédant de nombreux zéros. On procède de la manière suivante.

LEMME 1. *Soit F une fonction entière, admettant des zéros $x_1, \dots, x_k$ (comptés avec leur ordre de multiplicité). Soit $x_0 \in \mathbf{C}$, $x_0 \neq x_i$ $(i=1, \dots, k)$; soit $s \geqq 0$ le plus petit entier tel que*

$$F^{(s)}(x_0) \neq 0 .$$

Soit $\lambda > 1$ un nombre réel, et soit :

$$R = \lambda^2 \, | \, x_0 \, | + (\lambda^2 + 1) \, . \sup_{1 \leqq h \leqq k} | \, x_h \, | \, . \tag{1}$$

Si la fonction F vérifie :

$$\sup_{|Z| = R} | \, F(Z) \, | = | \, F \, |_R \leqq \frac{(R - | \, x_0 \, |)^s}{s\,!} \lambda^k , \tag{2}$$

alors on a :

$$| \, F^{(s)}(x_0) \, | \leqq \lambda^{-k} . \tag{3}$$

En effet, soit

$$Q(X) = \prod_{h=1}^{k} (X - x_h) \in \mathbf{C}[X] ,$$

et

$$G(Z) = \frac{F(Z)}{(Z - x_0)^s} .$$

La fonction $\dfrac{G(Z)}{Q(Z)}$ est entière; le principe du maximum montre que, pour $R > | \, x_0 \, |$, on a:

$$| \, G(x_0) \, | \leqq | \, G \, |_R \, . \frac{| \, Q(x_0) \, |}{| \, Q \, |_R} .$$

Le choix (1) de R permet la majoration:

$$\sup_{|Z| = R} \left| \frac{x_0 - x_h}{Z - x_h} \right| \leqq \lambda^{-2} , \quad h = 1, \dots, k ,$$

donc:

$$\frac{| \, Q(x_0) \, |}{| \, Q \, |_R} \leqq \lambda^{-2k} .$$

D'autre part, grâce à la relation (2), on a:

$$| \, G \, |_R \leqq \frac{| \, F \, |_R}{(R - | \, x_0 \, |)^s} \leqq \frac{1}{s\,!} \lambda^k .$$

Comme

$$G(x_0) = \frac{1}{s\,!} F^{(s)}(x_0)\,,$$

on en déduit la conclusion (3).
On n'utilisera en fait le lemme 1 que dans le cas $s = 0$.

Quatrième pas. — Partie arithmétique : minoration de $|\gamma|$

Comme γ est un nombre algébrique non nul, il possède un dénominateur $d \in \mathbf{Z}$ (i.e. tel que $d.\,\gamma$ soit entier algébrique non nul). La norme de $d.\,\gamma$ sur $\mathbf{Q}$ est alors un entier rationnel non nul γ', d'où $|\gamma'| \geq 1$.

On en déduit une minoration de γ (voir (4)).

Conclusion. Si la minoration de $|\gamma|$ est incompatible avec la majoration (3), on obtient la contradiction désirée.

Remarque. Pour pouvoir effectuer les majorations et les minorations, on introduit au début de la démonstration un paramètre N (généralement choisi entier); les inégalités que l'on écrit sont alors vérifiées pour N suffisamment grand, c'est-à-dire minoré par un nombre fini d'inégalités (plus ou moins explicitées).

§ 4. Notations et résultats préliminaires

a) *La notation* $\ll$ [7]

Soient f, g deux fonctions réelles de variable réelle; on notera:

$$f(x) \ll g(x) \quad \textit{pour} \quad x \to +\infty$$

s'il existe deux réels positifs A et C tels que

$$x > A \Rightarrow f(x) \leq C\,.\,g(x)\,.$$

Avec cette notation, le résultat que nous avons cité au deuxième pas (§ 3.) sur le nombre de zéros, dans un disque $|Z| \leq R$, d'une fonction analytique d'ordre $\leq \rho$ s'énonce de la manière suivante.

Soient F une fonction entière (i.e. holomorphe dans tout le plan complexe) et $\rho \geqslant 0$ un nombre réel, tels que:

$$\operatorname{Log} |F|_R = \operatorname{Log} \sup_{|Z| = R} |F(Z)| \ll R^\rho \quad \text{pour} \quad R \to \infty$$

(on dit que la fonction F est d'ordre $\leq \rho$); pour $r > 0$, soit $N(r,F)$ le nombre de zéros (comptés avec leur multiplicité) de F dans le disque $\{ Z \in \mathbf{C} ; | Z | \leq r \}$; on a:

$$N(r, F) \ll r^{\rho} \quad \text{pour} \quad r \to +\infty .$$

b) *Taille d'un nombre algébrique*

Précisions un peu comment s'effectue le quatrième pas de la démonstration (§ 3),

Soit K un corps de nombres (c'est-à-dire une extension algébrique finie de $\mathbf{Q}$), et soit $a \in K$. Un entier rationnel $d \in \mathbf{Z}$ est un *dénominateur* de a si $d\,a$ est entier sur $\mathbf{Z}$ (rappelons que l'anneau des entiers de K sur $\mathbf{Z}$ forme un $\mathbf{Z}$-module libre de dimension $[K : \mathbf{Q}]$). Soit $d(a)$ le plus petit dénominateur positif de a; soient $\sigma_1, \ldots, \sigma_n$ (avec $n = [K:\mathbf{Q}]$) les différents plongements de K dans $\mathbf{C}$. On définit:

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

et

$$t(a) = \max \{ \operatorname{Log} \| a \| ; \operatorname{Log} d(a) \} .$$

Ces valeurs ne dépendent pas du choix du corps de nombres K contenant a.

La *taille* $t(a)$ possède la propriété fondamentale suivante [7] chap. II: *Pour tout* $a \in K$, $a \neq 0$, on a:

$$-2[K : \mathbf{Q}]\, t(a) \leq \operatorname{Log} | a | . \tag{4}$$

En effet, le nombre

$$N_{K/\mathbf{Q}}(d(a).a) = \prod_{i=1}^{n} d(a) . \sigma_i(a) ,$$

($N_{k/\mathbf{Q}}$ est l'application « norme » de K sur $\mathbf{Q}$), est un entier rationnel non nul, donc supérieur ou égal à 1 en valeur absolue; donc pour tout plongement σ_i de K dans $\mathbf{C}$; on a:

$$\operatorname{Log} | \sigma_i(a) | \geq -n . \quad d(a) - (n-1) \operatorname{Log} \| a \| ,$$

avec $n = [K : \mathbf{Q}]$.

Ainsi, pour minorer un nombre algébrique $\gamma \neq 0$, il suffit de majorer $[\mathbf{Q}(\gamma) : \mathbf{Q}]$ et $t(\gamma)$.

Nous aurons à utiliser les propriétés suivantes de la taille:

— si $a_1, \ldots, a_k$ sont des nombres algébriques, on a:

$$t(a_1 \ldots a_k) \leq t(a_1) + \ldots + t(a_k) ;$$
$$t(a_1 + \ldots + a_k) \leq \operatorname{Log} k + t(a_1) + \ldots + t(a_k) ;$$

— si, de plus, $a_1, \ldots, a_k$ sont entiers sur $\mathbf{Z}$, alors:

$$t(a_1 + \ldots + a_k) \leq \operatorname{Log} k + \max_{1 \leq i \leq k} t(a_i).$$

c) *Un lemme de Siegel*

La construction de la fonction auxiliaire (§ 3., premier pas) repose sur un lemme, dû à Siegel (1929), qui permet de résoudre, dans un corps K, un système d'équations linéaires homogènes à coefficients dans K, pourvu que le nombre d'inconnues soit supérieur au nombre d'équations. Nous n'utiliserons ce résultat que dans un corps de nombres, mais on peut formuler un énoncé analogue au lemme 2 concernant une extension de $\mathbf{Q}$ de type fini (pouvant avoir un degré de transcendance $\geqslant 1$), après avoir défini une fonction « taille » sur un tel corps.

LEMME 2. (Siegel). *Soit K un corps de nombres. Il existe une constante $C_K > 0$ ayant la propriété suivante.*

Soient r et n deux entiers, $n > r \geq 1$, et $a_{i,j}$ $(1 \leq i \leq r,\ 1 \leq j \leq n)$ des éléments de K. Soit d_i, $(1 \leq i \leq r)$ un dénominateur commun positif de

$$a_{i,1}, \ldots, a_{i,n}.$$

Enfin soit

$$d = \max_{1 \leq i \leq r} d_i, \quad et \quad A = \max_{\substack{1 \leq i \leq r \\ 1 \leq j \leq n}} \| a_{i,j} \|.$$

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

$$\text{(5)} \qquad \sum_{j=1}^{n} a_{i,j} x_j = 0 \quad \text{pour} \quad 1 \leq i \leq r$$

et

$$\text{(6)} \qquad \max_{1 \leq j \leq n} \| x_j \| \leq C_K (C_K . n . d . A)^{r/(n-r)} + C_K .$$

On trouvera des variantes du lemme 2 dans [5] chap. II, lemme II; [7] chap. I, lemme 3; [9] chap. III, lemme 1; [10] appendice, lemme 31; [11] chap. II, § 2., lemme 2.

L'existence d'une solution non triviale $(x_1, \ldots, x_n)$ du système (5) résulte de la non injectivité de l'application:

$$L : K^n \to K^r,$$

définie par

$$L(x_1, \ldots, x_n) = (\sum_{j=1}^{n} a_{i,j}x_j)_{i=1,\ldots,r},$$

grâce à la condition $n > r$.

Pour obtenir la majoration (6), il faut se fatiguer un peu plus. *Etudions d'abord le cas $K = \mathbf{Q}$ et $d = 1$*

Supposons donc $a_{i,j} \in \mathbf{Z}$ avec $A = \max |a_{i,j}| \geqq 1$. Etant donnés deux entiers positifs m et B, on définit l'ensemble

$$\mathbf{Z}(m,B) = \{(x_1, \ldots, x_m) \in \mathbf{Z}^m ; \quad |x_l| \leqq B \quad \text{pour} \quad l = 1, \ldots, m\}.$$

On a

$$\text{Card}\, \mathbf{Z}(m,B) = (1+2B)^m.$$

D'autre part L applique $\mathbf{Z}(n,B)$ dans $\mathbf{Z}(r,nAB)$. Choisissons:

$$B = [\frac{1}{2} + \frac{1}{2}(nA)^{\frac{r}{n-r}}] \qquad \text{(partie entière)},$$

de telle manière que l'on ait:

$$(1+2B)^{n-r} > (nA)^r,$$

donc

$$\text{Card}\, \mathbf{Z}(n,B) = (1+2B)^n > (1+2nAB)^r = \text{Card}\, \mathbf{Z}(r,nAB).$$

Ainsi l'application $L : \mathbf{Z}(n,B) \to \mathbf{Z}(r,nAB)$ n'est pas injective (c'est ce qu'on appelle le « principe de Dirichlet »), donc il existe $(y_j) \neq (Z_j)$ appartenant à $\mathbf{Z}(n,B)$ tels que

$$L(y_1, \ldots, y_n) = L(Z_1, \ldots, Z_n).$$

Alors $(x_j) = (y_j - Z_j)$ vérifie

$$L(x_1, \ldots, x_n) = 0$$

et

$$|x_j| \leqq 2B \leqq 1 + (nA)^{\frac{r}{n-r}},$$

ce qui montre que l'on peut choisir $C_{\mathbf{Q}} = 1$.

Dans le cas général, soit $\delta = [K : \mathbf{Q}]$, et soit $(\omega_1, \ldots, \omega_\delta)$ une base d'entiers de K sur $\mathbf{Z}$.

Comme $\omega_h \,.\, \omega_{h'}$ est entier sur $\mathbf{Z}$ ($1 \leq h \leq \delta$, $1 \leq h' \leq \delta$), il existe des entiers rationnels $\Omega_{h,h',k}$ vérifiant

$$\omega_h \,.\, \omega_{h'} = \sum_{k=1}^{\delta} \Omega_{h,h',k} \,.\, \omega_k \,, \quad 1 \leq h \leq \delta \,, \quad 1 \leq h' \leq \delta \,.$$

Soit

$$\Omega = \max_{1 \leq h,\, h',\, k \leq \delta} | \, \Omega_{h,h',k} \, | \,.$$

On décompose les éléments $d_i \,.\, a_{i,j}$ dans la base $(\omega_1, \ldots, \omega_\delta)$: il existe des entiers $\alpha_{i,j,h} \in \mathbf{Z}$, ($1 \leq i \leq r$, $1 \leq j \leq n$, $1 \leq h \leq \delta$), tels que

$$d_i \,.\, a_{i,j} = \sum_{h=1}^{\delta} \alpha_{i,j,h} \,.\, \omega_h \,;$$

on a de plus

$$\max_{1 \leq h \leq \delta} | \, \alpha_{i,j,h} \, | \leq C_1 \,.\, \| \, d_i \,.\, a_{i,j} \, \| \,, \quad 1 \leq i \leq r \,, \quad 1 \leq j \leq n \,,$$

où C_1 est égal à $\delta \,.\, e^{C'_1}$, C'_1 étant le maximum des tailles des coefficients de l'inverse de la matrice $[\sigma_{h'}(\omega_h)]_{h,h'=1,\ldots,\delta}$ (C_1 est une constante ne dépendant que de K).

Déterminer des éléments $x_1, \ldots, x_n$ de K, entiers sur $\mathbf{Z}$ et non tous nuls, vérifiant (5), revient à rechercher des entiers rationnels $\xi_{j,h}$, ($1 \leq j \leq n$, $1 \leq h \leq \delta$), non tous nuls, tels que

$$x_j = \sum_{h=1}^{\delta} \xi_{j,h} \, \omega_h \,, \quad 1 \leq j \leq n \,,$$

et

$$\sum_{j=1}^{n} \sum_{h=1}^{\delta} \Big(\sum_{h'=1}^{\delta} \alpha_{i,j,h'} \,.\, \Omega_{h',h,k} \Big) \,.\, \xi_{j,h} = 0 \qquad 1 \leq i \leq r \,, \quad 1 \leq k \leq \delta .$$

On a ainsi à résoudre un système de $r\,\delta$ équations à $n\,\delta$ inconnues, à coefficients dans $\mathbf{Z}$ majorés par

$$\Big| \sum_{h'=1}^{\delta} \alpha_{i,j,h'} \,.\, \Omega_{h',h,k} \Big| \leq C_2 \, d \, A \,,$$

où $C_2 = \delta \,.\, C_1 \,.\, \Omega$.

On sait donc résoudre ce système avec

$$\max_{j,h} | \, \xi_{j,h} \, | \leq 1 + (C_2 n d A)^{\frac{r}{n-r}} \,,$$

donc

$$\max_{1 \leq j \leq n} \| x_j \| \leq C_3 + C_3 (C_2 n d A)^{\frac{r}{n-r}},$$

où

$$C_3 = \delta \,.\, \max_{1 \leq h \leq \delta} \| \omega_h \| \,.$$

Finalement, on choisit

$$C_K = \max (C_2, C_3) \,.$$

Remarque. Quand on utilisera le lemme de Siegel, on choisira $n = 2r$, et la majoration (6) se réduira toujours à

$$\max_{1 \leq j \leq n} t(x_j) \leq 3 \,.\, \max_{\substack{1 \leq j \leq r \\ 1 \leq j \leq n}} t(a_{i,j}) \,.$$

d) *Dépendance algébrique de fonctions exponentielles*

Nous avons affirmé plus haut (§ 2.) que, si $b \notin \mathbf{Q}$, les deux fonctions e^Z et e^{bZ} sont algébriquement indépendantes sur $\mathbf{C}$, et que, si $a \neq 0, 1$, les deux fonctions Z et a^Z sont algébriquement indépendantes sur $\mathbf{C}$ (on dit que la fonction a^Z est transcendante — sous-entendu sur $\mathbf{C}(Z)$).

Plus généralement, on a le résultat suivant:

LEMME 3. *Soient* $b_1, \ldots, b_l$ *des nombres complexes. Les fonctions:*

$$Z, e^{b_1 Z}, \ldots, e^{b_l Z}$$

sont algébriquement indépendantes sur $\mathbf{C}$ *si et seulement si les nombres*

$$b_1, \ldots, b_l$$

sont $\mathbf{Q}$*-linéairement indépendants.*

Il revient au même de dire que si $W_1, \ldots, W_q$ sont des nombres complexes deux à deux distincts, et si $a_{i,j}$, $(1 \leq i \leq p,\ 1 \leq j \leq q)$ sont des nombres complexes non tous nuls, alors la fonction

$$F(Z) = \sum_{i=1}^{p} \sum_{j=1}^{q} a_{i,j} \,.\, Z^{i-1} \,.\, e^{W_j Z} \tag{7}$$

n'est pas identiquement nulle.

Ce résultat est immédiat par récurrence sur q, grâce à la relation [6] chap. 12:

$$\frac{d^p}{d\,Z^p}\, e^{-W_q Z} \,.\, F(Z) \;=\; \sum_{i=1}^{p} \sum_{j=1}^{q-1} b_{i,j} \,.\, Z^{i-1} \,.\, e^{(W_j - W_q)Z} \,,$$

avec

$$b_{i,j} \;=\; \sum_{l=i}^{p} \frac{p\,!}{(l-i)\,!\,(p-l+i)\,!} \cdot \frac{(l-1)\,!}{(i-1)\,!} \,.\, (W_j - W_q)^{p-l+i} \,.\, a_{l,j} \,,$$

et à la remarque que, pour tout $j = 1\,,\,\ldots\,,\,q-1$, on a:

$$(b_{i,j} = 0 \quad \text{pour} \quad 1 \leqq i \leqq p) \Rightarrow (a_{l,j} = 0 \quad \text{pour} \quad 1 \leqq l \leqq p)\,.$$

Le lemme 3 sera amplement suffisant pour ce que nous voulons faire dans la première partie. Mais, pour démontrer le théorème de Baker (part II), nous aurons besoin de renseignements beaucoup plus précis sur les zéros des fonctions (7) (cf. les lemmes 4 et 5 et la relation (20)).

§ 5. Démonstration du théorème 1

Soient a et b deux nombres algébriques, $a \neq 0$, $a \neq 1$, $b \notin \mathbf{Q}$, et supposons que

$$a^b = \exp\,(b\,.\,\mathrm{Log}\, a)$$

soit algébrique (Log désignant une détermination quelconque du logarithme complexe).

Soit N un nombre entier « arbitrairement grand » (voir la remarque à la fin du § 3); si f et g sont deux applications de $\mathbf{N}$ dans $\mathbf{R}$, on écrira:

$$f \ll g$$

au lieu de

$$f\,(N) \ll g\,(N) \quad \text{pour} \quad N \to +\,\infty\,.$$

On définit deux fonctions $p\,(N)$ et $q\,(N)$ de N par les relations

(8) $$p\,(N) \;=\; 2\,N^3 \quad \text{et} \quad q\,(N) \;=\; N\,.$$

Nous justifierons ce choix à la fin de la démonstration.

Premier pas. — Il existe des éléments de K

$$a_{i,j}(N)\,, \quad \big(1 \leqq i \leqq p\,(N)\,,\; 1 \leqq j \leqq q\,(N)\big)\,,$$

non tous nuls, entiers sur $\mathbf{Z}$, *majorés par*

(9) $$\max_{i,\,j}\, \mathrm{Log}\, \|\, a_{i,j}(N) \,\| \ll p\,(N)\; \mathrm{Log}\; q\,(N) + N^2 \,.\, q\,(N) \ll N^3 \,.\, \mathrm{Log}\; N\,,$$

tels que la fonction :

$$(10) \qquad F_N(Z) = \sum_{i=1}^{p(N)} \sum_{j=1}^{q(N)} a_{i,j}(N)\, Z^{i-1}\, a^{jZ}$$

vérifie :

$$F_N(\lambda+\mu b) = 0 \quad \text{pour} \quad 1 \leqq \lambda \leqq N^2, \quad 1 \leqq \mu \leqq N^2, \quad (\lambda,\mu) \in \mathbf{Z}^2 .$$

Pour obtenir ce résultat, on applique le lemme de Siegel (lemme 2) au système de N^4 équations

$$\sum_{i=1}^{p(N)} \sum_{j=1}^{q(N)} a_{i,j}(N) \,.\, (\lambda+\mu b)^{i-l} \,.\, a^{j.\lambda} \,.\, (a^{bj})^{\mu} = 0$$
$$1 \leqq \lambda \leqq N^2, \quad 1 \leqq \mu \leqq N^2,$$

à $p(N) \,.\, q(N) = 2\,N^4$ inconnues $a_{i,j}(N), \big(1 \leqq i \leqq p(N), 1 \leqq j \leqq q(N)\big)$ les coefficients ayant une taille majorée par

$$t\big((\lambda+\mu b)^{i-l} \,.\, a^{j\lambda} \,.\, (a^b)^{j\mu}\big) \ll p(N) \,.\, \operatorname{Log} q(N) + N^2 q(N) .$$

Notons que si $\Delta \in \mathbf{Z}$ est un dénominateur de a, b et a^b, alors $\Delta^{\,p(N)+2N^2q(N)}$ est un dénominateur de

$$(\lambda+\mu b)^{i-l} \,.\, a^{j\lambda} \,.\, (a^b)^{j\mu} .$$

Deuxième pas. — Il existe un entier $M(N) \geqq N^2$ *tel que :*

1) $F_N(\lambda+\mu b) = 0$ *pour* $1 \leqq \lambda \leqq M(N), \quad 1 \leqq \mu \leqq M(N)$

2) *Il existe* $(\lambda_1, \mu_1) \in \mathbf{Z} \times \mathbf{Z}, \quad 1 \leqq \lambda_1 \leqq M(N) + 1,$
$1 \leqq \mu_1 \leqq M(N) + 1,$

avec

$$\gamma = F_N(\lambda_1 + \mu_1 b) \neq 0 .$$

La fonction F, qui n'est pas identiquement nulle (grâce au lemme 3), vérifie

$$\operatorname{Log} \| F_N \|_R \ll R \quad \text{pour} \quad R \to +\infty$$

(i.e. elle est d'ordre $\leqq 1$), donc le nombre de ses zéros dans un disque $|Z| \leqq R$ est majoré par $\ll R$ pour $R \to +\infty$ (Les constantes impliquées pour $R \to +\infty$ peuvent dépendre de N). Or le nombre de points $\{\lambda + \mu b\,;\ (\lambda,\mu) \in \mathbf{N} \times \mathbf{N}\}$ dans ce disque ne vérifie pas cette majoration. Donc l'un des nombres $F(\lambda+\mu b)$, $(\lambda,\mu) \in \mathbf{N} \times \mathbf{N}$, est non nul.

Troisième pas. — Le nombre $\gamma = F_N(\lambda_1+\mu_1 b)$ *vérifie la majoration :*

$$(11) \qquad \operatorname{Log} |\gamma| \ll -M(N)^2 . \quad \operatorname{Log} M(N) .$$

On utilise le lemme 1 avec

$$\{x_1, \dots, x_k\} = \{\nu + \mu b\,, \quad 1 \leqq \nu \leqq M(N)\,, \quad 1 \leqq \mu \leqq M(N)\}\,,$$

(donc $k = M(N)^2$), et $x_0 = \lambda_1 + \mu_1 b$, $s = 0$, $\lambda = M(N)^{1/8}$.

Il faut vérifier (2) sous l'hypothèse (1), c'est-à-dire:

$$\operatorname{Log} |F|_R \leqq k \operatorname{Log} \lambda = \frac{1}{8} M(N)^2 . \quad \operatorname{Log} M(N)$$

pour

$$R = \lambda^2 |x_0| + (\lambda^2+1) \sup_{1 \leqq h \leqq k} |x_h| \ll M(N)^{5/4} .$$

Or pour cette valeur de R on a:

$$\operatorname{Log} |F|_R \ll q(N) . M(N)^{5/4} + p(N) . \operatorname{Log} M(N) \ll M(N)^{7/4} ,$$

grâce à (8), (9), (10) et à la relation $M(N) \geqq N^2$. Donc pour N assez grand la condition (2) est vérifiée, d'où (3):

$$\operatorname{Log} |F_N(\lambda_1+\mu_1 b)| \leqq -k \operatorname{Log} \lambda = -\frac{1}{8} M(N)^2 \operatorname{Log} M(N) .$$

Quatrième pas. — La taille de γ *vérifie*

$$(12) \quad t(\gamma) \ll p(N) \operatorname{Log} M(N) + q(N) M(N) \ll M(N)^{3/2} . \operatorname{Log} \big(M(N)\big),$$

donc, grâce à (4), *le nombre* $|\gamma|$ *est minoré par :*

$$(13) \qquad \operatorname{Log} |\gamma| \gg -M(N)^{3/2} . \operatorname{Log} \big(M(N)\big) .$$

Notons, comme dans le premier pas, Δ un dénominateur de a, b et a^b. Le nombre

$$\Delta^{p(N) + 2(M(N)+1) . q(N)} . \gamma$$

est entier sur $\mathbf{Z}$, donc

$$\operatorname{Log} d(\gamma) \ll p(N) + M(N) q(N) .$$

D'autre part la majoration

$$\operatorname{Log} \|\gamma\| \ll p(N) . \operatorname{Log} M(N) + M(N) q(N)$$

est une conséquence immédiate de (9) et (10); on obtient ainsi (12); (13) est alors une conséquence de (4).

Conclusion. Les conditions (11) et (13) étant incompatibles pour N (donc $M(N)$) assez grand, on obtient la contradiction attendue.

Ceci démontre le théorème 1.

Remarque sur le choix de $p(N)$ et $q(N)$

On remarque que les seules propriétés que l'on ait utilisées pour les fonctions $p(N)$ et $q(N)$ définies par (8) sont les suivantes.

Ces deux fonctions sont monotones croissantes, tendent vers $+\infty$ avec N, et vérifient

$$\frac{1}{N^2} q(N) \to 0 \quad \text{et} \quad \frac{1}{N^4} p(N) \operatorname{Log} N \to 0 \quad \text{quand} \quad N \to \infty\,;$$

$$p(N) \,.\, q(N) \geqq 2N^4\,.$$

Il y avait évidemment d'autres choix possibles que (8).

II. Le théorème de Baker sur l'indépendance linéaire de logarithmes de nombres algébriques

§ 1. Enoncé du théorème

Dans la première partie, nous avons étudié le théorème de Gel'fond et Schneider sur la transcendance de a^b. Ce théorème peut s'énoncer de la manière suivante.

Si les logarithmes de deux nombres algébriques sont $\mathbf{Q}$-linéairement indépendants, alors ces logarithmes sont $\overline{\mathbf{Q}}$-linéairement indépendants ($\overline{\mathbf{Q}}$ désignant le corps des nombres algébriques, clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$).

Gel'fond [5] avait suggéré que la propriété devait être vraie pour n logarithmes, et il avait mis en évidence l'importance de cette conjecture qu'il considérait comme le problème fondamental dans la théorie analytique des nombres transcendants. Baker résolvait en 1966 le cas où les nombres algébriques sont multiplicativement indépendants [1], I, puis en 1967 le cas général [1], II; il démontrait même plus [1], III.

Théorème 2 (Baker). *Soient $\alpha_1, \ldots, \alpha_m$ des nombres algébriques dont les logarithmes sont $\mathbf{Q}$-linéairement indépendants.*

Alors :

$$1\,,\ \mathrm{Log}\ \alpha_1\,,\ \ldots\,,\ \mathrm{Log}\ \alpha_m$$

sont $\overline{\mathbf{Q}}$*-linéairement indépendants.*

Par des arguments très simples d'algèbre linéaire, on peut déduire du théorème 2 le corollaire suivant.

COROLLAIRE 1. *Soient* $\alpha_1, \ldots, \alpha_m, \beta_o, \ldots, \beta_m$ *des nombres algébriques* ($\alpha_i \neq 0$). *On suppose que l'une des propriétés suivantes est vérifiée.*

1. $\beta_0 \neq 0$
2. $\mathrm{Log}\ \alpha_1, \ldots, \mathrm{Log}\,\alpha_m$ *sont* **Q***-linéairement indépendants, et l'un des nombres* $\beta_1, \ldots, \beta_m$ *est irrationnel.*
3. $\mathrm{Log}\,\alpha_1, \ldots, \mathrm{Log}\,\alpha_m$ *sont non nuls, et* $1, \beta_1, \ldots, \beta_m$ *sont* **Q***-linéairement indépendants.*

Alors le nombre

$$e^{\beta_o}\,\alpha_1^{\ \beta_1} \ldots \alpha_m^{\ \beta_m}$$

est transcendant.

On déduit également du théorème de Baker la transcendance du nombre

$$\int_0^1 \frac{d\,x}{1 + x^3} = \frac{1}{3}\,(\mathrm{Log}\ 2 + \frac{\pi}{\sqrt{3}})\,.$$

Plus généralement, Van der Poorten (On the arithmetic nature of definite integrals of rational functions. *Proc. Amer. Math. Soc.* 29, (1971), 451-456) a montré que le théorème 2 permettait de déterminer la nature arithmétique d'intégrales définies de fonctions rationnelles; par exemple:

COROLLAIRE 2. *Soient P et Q deux polynômes non nuls à coefficients algébriques, avec* $\deg P < \deg Q$, *les zéros de Q dans* **C** *étant deux à deux distincts. Soit* Γ *un contour dans le plan complexe, qui est fermé ou bien qui a des extrémités algébriques ou infinies.*
Si l'intégrale

$$\int_\Gamma \frac{P\,(Z)}{Q\,(Z)}\,d\,Z$$

existe, alors elle est nulle ou transcendante.

Dans l'énoncé du résultat de Baker, nous avons négligé l'aspect effectif du théorème: non seulement Baker démontrait qu'une forme linéaire non triviale en 1, $\operatorname{Log} \alpha_1, \ldots, \operatorname{Log} \alpha_m$, à coefficients algébriques, est non nulle, mais en plus il minorait une telle forme, en fonction des tailles des nombres $\alpha_1, \ldots, \alpha_m$ et des coefficients.

Cette négligence nous permet de simplifier notablement la démonstration, mais nous interdit aussi l'étude des conséquences les plus importantes (mais également moins élémentaires que les précédentes) de cette méthode, telles que

— les applications aux équations diophantiennes, par exemple la recherche de points rationnels sur des courbes de genre 1 (Baker, Coates);
— l'étude des approximations de nombres algébriques par des nombres rationnels, et la recherche d'analogues effectifs du théorème de Thue, Siegel, Roth (Baker, Coates);
— les problèmes de nombres de classes, en particulier dans les corps quadratiques imaginaires (Baker, Stark, Bundschuh et Hock);
— l'étude des nombres ayant de grands facteurs premiers (Ramachandra, Tijdeman, Shorey).

La résolution de nombreux autres problèmes de théorie des nombres fait intervenir des minorations de formes linéaires de logarithmes.

Enfin l'analogue p-adique du théorème 2 permit à Brumer de résoudre, dans le cas abélien, une conjecture de Leopoldt sur le rang p-adique du groupe des unités d'un corps de nombres. Pour résoudre cette conjecture dans le cas non abélien, il suffirait que l'on puisse démontrer l'analogue p-adique de la

Conjecture. *Soient* $\alpha_1, \ldots, \alpha_m$ *des nombres algébriques dont les logarithmes sont* $\mathbf{Q}$*-linéairement indépendants. Alors* $\operatorname{Log} \alpha_1, \ldots, \operatorname{Log} \alpha_m$ *sont algébriquement indépendants.*

Une approche très intéressante — et entièrement différente de celle de Baker — a été faite par Galotschkin et Nurmagomedov, utilisant une méthode de Siegel et Shidlovskii; ils démontrent que, $P \in \mathbf{Q}[X_1, \ldots, X_m]$ étant un polynôme non nul, si les nombres $\alpha_1, \ldots, \alpha_m$ sont suffisamment proches de 1 (d'autant plus proches que le degré total du polynôme est plus grand), alors $P(\operatorname{Log} \alpha_1, \ldots, \operatorname{Log} \alpha_m) \neq 0$ (on peut même minorer effectivement ce nombre). Par exemple, si q est un nombre entier, $q > e^{694}$, alors le nombre

$$\operatorname{Log}\left(1+\frac{1}{q}\right). \quad \operatorname{Log}\left(1-\frac{1}{q}\right)$$

est irrationnel.

Un tel résultat en p-adique serait suffisant pour résoudre complètement la conjecture de Leopoldt; malheureusement, la méthode de Siegel et Shidlovskii n'a pas encore été traduite en p-adique (on ignore encore, par exemple, si l'analogue p-adique du théorème de Lindemann Weierstrass est vrai).

§ 2. Idées de la démonstration du théorème 2

La méthode de Baker est une extension de celles de Gel'fond et Schneider — d'ailleurs le théorème 2 contient la transcendance de a^b pour a et b algébrique, $a \neq 0$, 1 et b irrationnel.

De plus le théorème 2 contient la transcendance de e^{α}, pour $\alpha \neq 0$ algébrique; or on peut effectuer la démonstration de la transcendance de e^{α} par la méthode de Gel'fond (ceci a été fait par Schneider en 1949; cf. I, § 2) en considérant les deux fonctions

$$f_1(Z) = Z\,; \quad f_2(Z) = e^Z\,,$$

et les points $Z = n\,\alpha$, $n \in \mathbf{Z}$ (voir par exemple [7] chap. III ou [10] chap. II, § 4).

La première chose à faire est donc d'exprimer analytiquement les hypothèses du théorème 2. *Supposons que $\alpha_1, \ldots, \alpha_m$ soient des nombres algébriques dont les logarithmes sont* **Q**-*linéairement indépendants.*

Alors les fonctions

$$Z\,, \alpha_1^Z\,, \ldots\,, \alpha_m^Z$$

sont algébriquement indépendantes (lemme 3), prennent des valeurs algébriques pour $Z \in \mathbf{Z}$ (et même pour $Z \in \mathbf{Q}$), et vérifient des équations différentielles à coefficients dans le corps

$$\mathbf{Q}\,(\operatorname{Log}\alpha_1, \ldots, \operatorname{Log}\alpha_m)$$

(qui a un degré de transcendance sur $\mathbf{Q}$ supérieur ou égal à 1).

Nous allons étudier les conséquences de ces équations différentielles sur les dérivées d'une fonction

$$F(Z) = P(Z, \alpha_1^Z, \ldots, \alpha_m^Z)\,,$$

où $P \in \overline{\mathbf{Q}}\,[X_o\,, \ldots\,, X_m]$ est un polynôme à coefficients algébriques.

Soit

$$(14) \quad P = \sum_{\lambda_o=0}^{q_o-1} \cdots \sum_{\lambda_m=0}^{q_m-1} p(\lambda_o, \dots, \lambda_m) X_o^{\lambda_o} \dots X_m^{\lambda_m},$$

que l'on notera

$$(15) \quad P = \sum_{(\lambda)} p(\lambda) X_o^{\lambda_o} \dots X_m^{\lambda_m};$$

ainsi

$$(16) \quad F(Z) = \sum_{(\lambda)} p(\lambda) Z^{\lambda_o} \exp\,(\lambda_1 \operatorname{Log} \alpha_1 + \dots + \lambda_m \operatorname{Log} \alpha_m) Z .$$

La dérivée d'ordre $s \geqq 0$ de F est un polynôme en $\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_m$, les coefficients étant des fonctions entières qui prennent des valeurs algébriques pour $Z \in \mathbf{Z}$.

Supposons d'abord que les nombres $\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_m$ *sont algébriquement dépendants sur* $\mathbf{Q}$,disons par exemple

$$\operatorname{Log} \alpha_m \in \overline{\mathbf{Q}}\,[\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_{m-1}];$$

ainsi $\operatorname{Log} \alpha_m$ est un polynôme en $\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_{m-1}$; soit $(c-1)$ le degré total de ce polynôme.

On peut exprimer la dérivée d'ordre s de F comme un polynôme en $\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_{m-1}$, soit:

$$(17) \quad \frac{d^s}{dZ^s} F = \sum_{\sigma_1=0}^{cs} \cdots \sum_{\sigma_{m-1}=0}^{cs} (\operatorname{Log} \alpha_1)^{\sigma_1} \dots (\operatorname{Log} \alpha_{m-1})^{\sigma_{m-1}} \cdot f_{s, \sigma_1, \dots, \sigma_{m-1}},$$

et les fonctions $f_{s, \sigma_1, \dots, \sigma_{m-1}}(Z)$ prennent des valeurs algébriques pour $Z \in \mathbf{Z}$.

Essayons alors d'effectuer la démonstration en utilisant la méthode exposée dans la première partie (§ 3).

Dans un premier temps, on construit un polynôme (14), (15), tel que la fonction (16) possède de nombreux zéros, soient

$$(18) \quad \frac{d^s}{dZ^s} F(x) = 0 \quad \text{pour} \quad x = 0, \dots, x_0 - 1,$$

et $\qquad s = 0, \dots, s_0 - 1 .$

(Les valeurs de x_0, s_0, q_0, $q_1, \dots, q_m$ seront précisées plus tard, en fonction d'un paramètre N « suffisamment grand », comme d'habitude).

Regardons la relation (17): On ne connaît rien sur les nombres $\operatorname{Log} \alpha_1$, ..., $\operatorname{Log} \alpha_{m-1}$ (sinon qu'ils sont transcendants), mais ils peuvent fort bien être algébriquement indépendants, auquel cas les conditions (18) sont équivalentes à

$$(19) \quad f_{s, \sigma_1, \dots, \sigma_{m-1}}(x) = 0 \quad \text{pour} \quad \begin{cases} x = 0, \dots, x_0 - 1, \\ s = 0, \dots, s_0 - 1, \\ \sigma_i = 0, \dots, c\, s_0, \ (1 \leqq i \leqq m-1). \end{cases}$$

Quoi qu'il en soit, les relations (19) entraînent toujours (18), et c'est donc le système (19) que nous allons résoudre.

Il s'agit d'un système linéaire homogène en $p(\lambda)$, à coefficients dans un corps de nombres; le nombre d'inconnues est $q_0 \dots q_m$ (où $q_i - 1$ est le degré de P par rapport à X_i), le nombre d'équations est $x_0\, s_0\, (cs_0 + 1)^{m-1} \ll x_0\, s_o^m$.

Donc, à condition que

$$q_0 \dots q_m \geqq 2\, x_0\, s_0\, (cs_0 + 1)^{m-1},$$

le lemme de Siegel permet d'effectuer le premier pas.

Remarquons ici que l'hypothèse

$$\operatorname{Log} \alpha_m \in \overline{\mathbf{Q}}\, [\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_{m-1}]$$

nous a permis de majorer le nombre d'équations par $\ll x_0\, s_o^m$, et donc de choisir $q_0 \dots q_m \gg \ll x_0\, s_o^m$; sans cette hypothèse, on aurait seulement $\ll x_0\, s_o^{m+1}$ pour le nombre d'équations, et on aurait été contraint de choisir $q_0, \dots, q_m$ plus grands: $(q_0 \dots q_m \gg \ll x_0 s_o^{m+1})$.

Le deuxième pas consiste à construire un point $Z_0 \in \mathbf{C}$ où la fonction F (ou bien l'une de ses dérivées) ne s'annule pas.

Or on connait un résultat très précis sur les zéros des fonctions (7) (cf. le lemme 4 ou la relation (20)), mais un peu long à démontrer. Nous nous contenterons, pour simplifier, de *supposer* $\alpha_1, \dots, \alpha_m$ *multiplicativement indépendants* (c'est-à-dire $2\, i\, \pi$, $\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_m$ **Q**-linéairement indépendants), et nous montrerons alors (lemme 5) *qu'il existe un entier* y, $0 \leqq y \leqq q_0\, q_1 \dots q_m - 1$, *tel que*

$$F(y) \neq 0.$$

Le principe de la suite de la démonstration réside en la recherche d'une majoration de $|F(y)|$, puis d'une majoration de la taille $t(F(y))$, pour contredire la relation

(4) $\quad -2[\mathbf{Q}(\alpha):\mathbf{Q}]\,.\,t(\alpha) \leqq \operatorname{Log}|\alpha| \quad si \quad \alpha \neq 0$ est algébrique.

La majoration de $t(F(y))$ *(quatrième pas)* se fait sans difficulté. Il n'en est pas de même de la majoration de $|F(y)|$, le cas général — où $\operatorname{Log}\alpha_1$, ..., $\operatorname{Log}\alpha_m$ sont algébriquement dépendants sur $\mathbf{Q}$-n'étant pas encore résolu.

Le troisième pas a donc pour but de fournir une majoration de $F(y)$; utilisons le lemme 1: les conditions (1) et (2) à vérifier pour obtenir (3) s'écrivent ici:

$$|F|_R \leqq \lambda^k \quad \text{pour} \quad R = \lambda^2 y + (\lambda^2+1)x_0\,,$$

avec $k = x_0 s_0$ et $\lambda > 1$. La conclusion serait alors

$$|F(y)| \leqq \lambda^{-k}\,.$$

Malheureusement la condition (1) sur R implique en particulier $R > y$, et on ne connaît que l'encadrement

$$x_0 \leqq y < x_0 s_0^m\,;$$

un calcul rapide montre alors que la majoration de $|F|_R$, pour $R > y$, est nettement plus mauvaise que λ^k (quel que soit le choix des fonctions x_0, s_0, q_0, ..., q_m, et quel que soit $\lambda > 1$ constant).

Néanmoins cette méthode permet de majorer $|F(x)|$ pour $x_0 \leqq x < x_1$ (où x_1 est par exemple $x_0\,.\,s_0^{1/4m}$; nous préciserons de toutes façons plus loin toutes ces valeurs).

On peut même majorer les dérivées $F^{(s)}(x)$, pour $0 \leqq s \leqq \dfrac{s_0}{2} - 1$; en effet, la fonction $F^{(s)}(Z)$, pour $0 \leqq s \leqq \dfrac{s_0}{2} - 1$, admet les zéros $0, \ldots, x_0 - 1$, d'ordre $\dfrac{s_0}{2}$, et la méthode précédente s'applique. Seulement ces valeurs $F^{(s)}(x)$, pour $s > 0$, ne sont pas des nombres algébriques, mais des éléments du corps $\mathbf{Q}(\operatorname{Log}\alpha_1, \ldots, \operatorname{Log}\alpha_{m-1})$; on ne peut donc pas utiliser l'argument algébrique (4) pour en déduire que ces valeurs sont nulles.

L'idée de Baker est alors de *majorer directement les nombres* $f_{s,\sigma_1,\ldots,\sigma_{m-1}}(x)$, *pour* $0 \leqq s \leqq \dfrac{s_0}{2} - 1$ (qui, eux, sont des nombres algébriques dont on peut aisément majorer la taille). Pour cela, il convient de montrer que *les fonctions* $f_{s,\sigma_1,\ldots,\sigma_{m-1}}(Z)$, pour $0 \leq s \leq \frac{s_0}{2} - 1$, *admettent les zéros* $0, 1, \ldots, x_0 - 1$, *d'ordre* $\frac{s_0}{2}$. On calcule donc les dérivées de ces fonctions: ce sont des polynômes en $\operatorname{Log}\alpha_1, \ldots, \operatorname{Log}\alpha_{m-1}$, dont on cherche à exprimer les coefficients en fonction des

$$f_{s+t,\, \sigma_1+\tau_1,\, \ldots,\, \sigma_{m-1}+\tau_{m-1}}(Z)\,, \quad \text{pour} \quad 0 \leq t \leq \frac{s_0}{2} - 1, \quad 0 \leq \tau_i \leq c\,\frac{s_0}{2}$$

(qui s'annulent par hypothèse pour $Z = 0, \ldots, x_0 - 1$). *Or ceci est possible lorsqu'on suppose non seulement*

$$\operatorname{Log} \alpha_m \in \overline{\mathbf{Q}}\,[\operatorname{Log}\alpha_1, \ldots, \operatorname{Log}\alpha_{m-1}]\,,$$

mais

$$\operatorname{Log} \alpha_m \in \overline{\mathbf{Q}} + \overline{\mathbf{Q}}\operatorname{Log}\alpha_1 + \ldots + \overline{\mathbf{Q}}\operatorname{Log}\alpha_{m-1}\,.$$

C'est là le point essentiel de la démonstration. Une fois que l'on a montré que les relations (19) entraînent

$$f_{s,\,\sigma_1,\,\ldots,\,\sigma_{m-1}}(x) = 0 \quad \text{pour} \quad \begin{cases} x = 0, \ldots, x_1 - 1\,; \\ s = 0, \ldots, \dfrac{s_0}{2} - 1\,; \\ \sigma_i = 0, \ldots, c\,\dfrac{s_0}{2}\,, \end{cases}$$

on obtient, par récurrence, pour tout entier l, $0 \leq l \leq l_0$,

$$f_{s,\,\sigma_1,\,\ldots,\,\sigma_{m-1}}(x) = 0 \quad \text{pour} \quad \begin{cases} x = 0, \ldots, x_l - 1\,; \\ s = 0, \ldots, \dfrac{s_0}{2^l} - 1\,; \\ \sigma_i = 0, \ldots, c\,\dfrac{s_0}{2^l}\,. \end{cases}$$

Or on peut choisir $x_1, \ldots, x_{l_o}$ tels que, en plus des propriétés précédentes, on ait

$$x_o\, s_o^m < x_{l_o}\,,$$

d'où la contradiction attendue: $F(y) = 0$.

§ 3. Etude des zéros de polynômes exponentiels

Nous avons vu pourquoi la démonstration du théorème 2 nécessite des renseignements précis sur les zéros de polynômes exponentiels (7). Baker [1] et Fel'dman [2], [3], ont résolu différemment cette difficulté; depuis, Tijdeman (On the number of zeros of general exponential polynomials. *Proc. Nederl. Akad. Wetensch., (Indag. Math.), Ser. A, 74* (1971), 1-7) a obtenu un énoncé très général, dont nous utiliserons le corollaire suivant:

Lemme 4 (Tijdeman). *Soient* $p_1, \ldots, p_q$ *des nombres entiers positifs,* $a_{i,j}$ $(1 \leq i \leq p_j;\ 1 \leq j \leq q)$ *des nombres complexes non tous nuls, et* $w_1, \ldots, w_q$ *des nombres complexes deux à deux distincts. Le nombre* $N(R,F)$ *de zéros (comptés avec leur ordre de multiplicité) de la fonction*

$$F(Z) = \sum_{j=1}^{q} \sum_{i=1}^{p_j} a_{i,j} \, . \, Z^{i-1} \, . \, e^{w_j Z} \, ,$$

dans le disque $\{ Z \in \mathbf{C} \; ; \; |Z| \leq R \}$, *est majoré par :*

$$N(R,F) \leq 3(n-1) + 4R\Delta \, ,$$

où

$$n = \sum_{j=1}^{q} p_j \quad et \quad \Delta = \max_{1 \leq j \leq q} |w_j| \, .$$

Une autre majoration de $N(R,F)$, qui donnerait les mêmes résultats ici, a été obtenue par l'auteur (Indépendance algébrique des valeurs de la fonction exponentielle. *Bull. Soc. Math. France*, 99 (1971), 285-304):

$$N(R,F) \leq \min_{\lambda > 0} \left[\frac{n}{\lambda} + 2 \, . \, \frac{1 + n^{\lambda}}{\lambda \operatorname{Log} n} (1 + R\Delta) \right] . \tag{20}$$

Plutôt que de donner ici une nouvelle démonstration de l'une ou l'autre de ces majorations de $N(R,F)$, il semble préférable de se limiter au cas où les nombres $2i\pi$, $\operatorname{Log} \alpha_1, \ldots, \operatorname{Log} \alpha_m$ sont $\mathbf{Q}$-linéairement indépendants (nous montrerons à la fin de l'exposé comment le lemme 4 ou la majoration (20) permet de résoudre le cas général).

Nous supposons donc que les $q_1 \ldots q_m = p$ nombres

$$\exp\{\lambda_1 \operatorname{Log} \alpha_1 + \ldots + \lambda_m \operatorname{Log} \alpha_m\} \, , \quad 0 \leq \lambda_i \leq q_i - 1 \, ,$$

sont deux à deux distincts; notons les $u_1, \ldots, u_p$; pour

$$u_h = \exp(\lambda_1 \operatorname{Log} \alpha_1 + \ldots + \lambda_m \operatorname{Log} \alpha_m) \, ,$$

notons

$$p_h(\lambda_0) = p(\lambda_0, \lambda_1, \ldots, \lambda_m).$$

Ainsi la fonction (16) s'écrit

$$F(Z) = \sum_{\lambda_o=0}^{q_o-1} \sum_{h=1}^{p} p_h(\lambda_o) Z^{\lambda_o} u_h^Z,$$

et le lemme 5, dû à Fel'dman ([2], lemme 5 et [3], lemme 7) montrera que, si $F \neq 0$ (c'est-à-dire si l'un des nombres $p_h(\lambda_0)$, $1 \leq h \leq p, 0 \leq \lambda_0 \leq q_0 - 1$, est non nul), alors l'un des nombres

$$F(y), \quad y = 0, \ldots, q_0 p - 1$$

est non nul.

Lemme 5. (Fel'dman). *Soient $u_1, \ldots, u_p$ des nombres complexes. Le déterminant*

$$\Delta(q_0, u_1, \ldots, u_p) = | x^k u_l^x |,$$

(où x, $(x=0, \ldots, q_0 p-1)$ est l'indice de ligne par exemple, et (k,l), $(k = 0, \ldots, q_0-1; l=1, \ldots, p)$ celui de colonne), est égal à

$$(21) \qquad \Delta(q_0, u_1, \ldots, u_p) = \left(\prod_{i=0}^{q_o-1} i!\right)^p . \left(\prod_{h=1}^{p} u_h^{\frac{1}{2}q_0(q_0-1)}\right) . \left(\prod_{l=2}^{p} \prod_{\lambda=1}^{l-1} (u_l - u_\lambda)^{q_o^2}\right).$$

Démonstration (d'après [2]*)*

Le polynôme $\Delta(Z) = \Delta(q_0, u_1, \ldots, u_{p-1}, Z) \in \mathbf{C}[Z]$ est divisible par $Z^{\frac{1}{2}q_0(q_0-1)}$, et ses dérivées s'annulent aux points u_h, $h = 1, \ldots, p-1$, jusqu'à l'ordre $q_o^2 - 1$. Or le degré de $\Delta(Z)$ est:

$$(q_0 p - 1) + (q_0 p - 2) + \ldots + (q_0 p - q_0) = p q^2 - \tfrac{1}{2} q_0 (q_0 + 1),$$

d'où:

$$\Delta(Z) = A_p . Z^{\frac{1}{2}q_0(q_0-1)} . \prod_{h=1}^{p-1} (Z - u_h)^{q_o^2},$$

où A_p est le coefficient de plus haut degré de $\Delta(Z)$. On obtient ainsi:

$$\Delta(q_0, u_1, \ldots, u_p) = \Delta(q_o, u_1, \ldots, u_{p-1}) . \delta . u_p^{\frac{1}{2}q_0(q_0-1)} . \prod_{h=1}^{p-1} (u_p - u_h)^{q_o^2},$$

avec

$$\delta = | x^k |_{\substack{k=0,\ldots,q_o-1 \\ x=q_o p-q_o,\ldots,q_o p-1}} = \prod_{i=0}^{q_o-1} i!,$$

d'où la relation (21) par récurrence sur p.

§ 4. Démonstration du théorème de Baker

Soient $\alpha_1, \ldots, \alpha_m, \beta_0, \ldots, \beta_{m-1}$ des nombres algébriques tels que

$$(22) \qquad \operatorname{Log} \alpha_m = \beta_0 + \beta_1 \operatorname{Log} \alpha_1 + \ldots + \beta_{m-1} \operatorname{Log} \alpha_{m-1}.$$

Soit

$$K = \mathbf{Q}(\alpha_1, \ldots, \alpha_m, \beta_0, \ldots, \beta_{m-1}).$$

Considérons un polynôme

$$(14) \qquad P = \sum_{\lambda_o=0}^{q_o-1} \ldots \sum_{\lambda_m=0}^{q_m-1} p(\lambda_o, \ldots, \lambda_m) X_o^{\lambda_o} \ldots X_m^{\lambda_m}$$

$$(15) \qquad = \sum_{(\lambda)} p(\lambda) X_o^{\lambda_o} \ldots X_m^{\lambda_m} \in K[X_o, \ldots, X_m].$$

La fonction $F(Z) = P(Z, \alpha_1^Z, \ldots, \alpha_m^Z)$ s'écrit

$$(16) \qquad F(Z) = \sum_{(\lambda)} p(\lambda) Z^{\lambda_0} \alpha_1^{\lambda_1 Z} \ldots \alpha_m^{\lambda_m Z}.$$

La relation (22) permet de remplacer

$$\alpha_1^{\lambda_1} \ldots \alpha_m^{\lambda_m}$$

par:

$$e^{\lambda_m \beta_o} \alpha_1^{\lambda_1 + \lambda_m \beta_1} \ldots \alpha_{m-1}^{\lambda_{m-1} + \lambda_m \beta_{m-1}},$$

c'est-à-dire d'écrire F sous la forme

$$(23) \qquad F(Z) = \sum_{(\lambda)} p(\lambda) Z^{\lambda_o} e^{\gamma_o Z} \alpha_1^{\gamma_1 Z} \ldots \alpha_{m-1}^{\gamma_{m-1}},$$

où

$$(24) \qquad \begin{cases} \gamma_0 = \lambda_m \beta_0 \\ \gamma_i = \lambda_i + \lambda_m \beta_i, \quad 1 \leq i \leq m-1. \end{cases}$$

Les dérivées de F vérifient les relations:

$$(25)\ \frac{d^s}{dZ^s} F = \sum_{\sigma_o+\ldots+\sigma_{m-1}=s} \frac{s\,!}{\sigma_0\,!\ldots\sigma_{m-1}!} (\mathrm{Log}\,\alpha_1)^{\sigma_1} \ldots (\mathrm{Log}\,\alpha_{m-1})^{\sigma_{m-1}} \,.\, F_{(\sigma)}(Z)\,,$$

où

$$(26) \qquad F_{(\sigma)}(Z) = \sum_{(\lambda)} p(\lambda) \frac{d^{\sigma_o}}{dZ^{\sigma_o}} (Z^{\lambda_o} e^{\lambda_m \beta_o Z}) \,.\, \gamma_1^{\sigma_1} \ldots \gamma_{m-1}^{\sigma_{m-1}} \,.\, \alpha_1^{\gamma_1 Z} \ldots \alpha_{m-1}^{\gamma_{m-1} Z}\,.$$

pour

$$(\sigma) = (\sigma_0, \ldots, \sigma_{m-1})\,.$$

(Avec les notations (17) précédentes, on a:

$$f_{s,\sigma_1,\ldots,\sigma_{m-1}} = \frac{s\,!}{\sigma_o!\ldots!\sigma_{m-1}} F_{\sigma_o,\ldots,\sigma_{m-1}}\,,$$

où $\sigma_0 = s - \sigma_1 - \ldots - \sigma_{m-1}$).

Les fonctions $F_{(\sigma)}$ sont reliées entre elles par des équations différentielles (qui généralisent (25)):

$$(27)\ \frac{d^t}{dZ^t} F_{(\sigma)} = \sum_{\tau_o+\ldots+\tau_{m-1}=t} \frac{t\,!}{\tau_o!\ldots\tau_{m-1}!} (\mathrm{Log}\,\alpha_1)^{\tau_1} \ldots (\mathrm{Log}\,\alpha_{m-1})^{\tau_{m-1}} \,.\, F_{(\sigma+\tau)}$$

où $(\sigma+\tau) = (\sigma_0+\tau_0, \ldots, \sigma_{m-1}+\tau_{m-1})\,.$

Ces relations (27) sont évidentes par le calcul à partir de (26) (cf. par exemple Fel'dman [2]), mais on peut donner une raison un peu plus profonde de leur existence de la manière suivante (cf. Baker [1]).

On définit une fonction $G(Z_0, \ldots, Z_{m-1})$ de m-1 variables complexes par:

$$G(Z_0, \ldots, Z_{m-1}) = \sum_{(\lambda)} p(\lambda)\, Z_o^{\lambda_o} e^{\gamma_o Z_o} \alpha_1^{\gamma_1 Z_1} \ldots \alpha_{m-1}^{\gamma_{m-1} Z_{m-1}}\,,$$

où $\gamma_0, \ldots, \gamma_{m-1}$ sont définis par (24).

D'après (23), on a:

$$F(Z) = G(Z, \ldots, Z),$$

donc:

$$\frac{d^s}{dZ^s} F(Z) = \sum_{\sigma_0 + \ldots + \sigma_{m-1} = s} \frac{s!}{\sigma_0! \ldots \sigma_{m-1}!} \frac{\partial^s}{\partial Z_0^{\sigma_0} \ldots \partial Z_{m-1}^{\sigma_{m-1}}} G(Z, \ldots, Z).$$

Soit:

$$D_i = (\operatorname{Log} \alpha_i)^{-1} \cdot \frac{\partial}{\partial Z_i}, \quad (1 \leq i \leq m-1),$$

et

$$D_0 = \frac{\partial}{\partial Z_0}.$$

On a donc, d'après (25):

$$F_{(\sigma)}(Z) = D_0^{\sigma_0} \ldots D_{m-1}^{\sigma_{m-1}} G(Z, \ldots, Z),$$

et on en déduit immédiatement

$$\frac{d^t}{dZ^t} F_{(\sigma)}(Z) =$$

$$= \sum_{\tau_0 + \ldots + \tau_{m-1} = t} \frac{t!}{\tau_0! \ldots \tau_{m-1}!} \frac{\partial^{\tau_0}}{\partial Z_0^{\tau_0}} \ldots \frac{\partial^{\tau_{m-1}}}{\partial Z_{m-1}^{\tau_{m-1}}} \cdot D_0^{\sigma_0} \ldots D_{m-1}^{\sigma_{m-1}} G(Z, \ldots, Z)$$

$$= \sum_{\tau_0 + \ldots + \tau_{m-1} = t} \frac{t!}{\tau_0! \ldots \tau_{m-1}!} (\operatorname{Log} \alpha_1)^{\tau_1} \ldots (\operatorname{Log} \alpha_{m-1})^{\tau_{m-1}} \cdot D_0^{\sigma_0 + \tau_0} \ldots$$
$$D_{m-1}^{\sigma_{m-1} + \tau_{m-1}} G(Z, \ldots, Z),$$

ce qui est la relation (27).

Soit N un entier suffisamment grand; *on définit des fonctions* x_0, s_0, q_0, q, t_0 *de* N *par :*

(28) $x_0 = N^m; \quad s_0 = N^{2m}; \quad q_0 = 2N^{2m}; \quad q = N^{2m-1}; \quad t_0 = N^{\frac{1}{2}}.$

Si l est un entier ≥ 0, on note Λ_l l'ensemble des $(m+1)$-uples

$$(x, (\sigma)) = (x, \sigma_0, \ldots, \sigma_{m-1})$$

d'entiers vérifiant

$$0 \leqq x \leqq x_0 \, t_o^l - 1 \, ; \quad \sigma_i \geqq 0 \, ; \quad \sigma_0 + \ldots + \sigma_{m-1} \leqq \frac{s_0}{2^l} - 1 \, .$$

Construction de la fonction auxiliaire.

Il existe des éléments

$$p(\lambda_0, \ldots, \lambda_m) = p(\lambda) \, , \quad 0 \leqq \lambda_0 \leqq q_0 - 1 \, ; \quad 0 \leqq \lambda_i \leqq q - 1 \, (1 \leqq i \leqq m) \, ,$$

appartenant à K et entiers sur **Z**, *non tous nuls, de taille majorée par*

$$(29) \qquad t\big(p(\lambda)\big) \ll (q_0 + s_0) \text{ Log } q + q \, x_0 \ll N^{3m-1} \text{ Log} N \, ,$$

et tels que les fonctions

$$(26) \quad F_{(\sigma)}(Z) = \sum_{(\lambda)} p(\lambda) \sum_{\mu=0}^{\sigma} \frac{\sigma_0 \, !}{\mu!(\sigma_o - \mu)!} \cdot \frac{\lambda_0 \, !}{(\lambda_o - \mu)!} \cdot (\beta_0 \lambda_m)^{\sigma_o - \mu} \, .$$

$$(\lambda_1 + \beta_1 \lambda_m)^{\sigma_1} \ldots (\lambda_{m-1} + \beta_{m-1} \lambda_m)^{\sigma_{m-1}} \, . \, Z^{\lambda_o - \mu} \, . \, \alpha_1^{\lambda_1 Z} \ldots \alpha_m^{\lambda_m Z} \, ,$$

définies pour $(\sigma) = (\sigma_0, \ldots, \sigma_{m-1})$, $\sigma_i \geqq 0$, *vérifient*

$$(30) \qquad F_{(\sigma)}(x) = 0 \quad \textit{pour} \quad \big(x, (\sigma)\big) \in \Lambda_0 \, .$$

Preuve : Soit $\Delta \in K$, entier sur **Z** non nul, tel que

$$\Delta \, \beta_0 \, , \ldots , \Delta \, \beta_{m-1} \, , \quad \Delta \, \alpha_1 \, , \ldots , \Delta \, \alpha_m$$

soient entiers sur **Z**. Les conditions

$$\Delta^{s_o + q x_o m} \, . \, F_{(\sigma)}(x) = 0 \quad \text{pour} \quad \big(x, (\sigma)\big) \in \Lambda_0$$

forment un système de moins de $x_0 \, s_o^m$ équations à $q_0 \, q^m$ inconnues $p(\lambda_0, \ldots, \lambda_m)$, dont les coefficients sont des éléments de K, entiers sur **Z**, de taille majorée par

$$\ll (q_0 + s_0) \text{ Log } q + q \, x_0 \, .$$

Le lemme 2 fournit le résultat, grâce à la relation:

$$q_0 \, q^m = 2 \, x_0 \, s_o^m \, .$$

La récurrence.

Pour tout entier l, $0 \leqq l \leqq 5 \, m^2$; *on a :*

$$(31) \qquad F_{(\sigma)}(x) = 0 \quad \textit{pour} \quad \big(x, (\sigma)\big) \in \Lambda_l \, .$$

Cette relation est vraie par construction (30) pour $l = 0$. Supposons-la vraie pour $l - 1$:

$$F_{(\sigma)}(x) = 0 \quad \text{pour} \quad \begin{cases} x = 0, \ldots, x_0 t_o^{l-1} - 1 \\ \sigma_0 + \ldots + \sigma_{m-1} \leqq \dfrac{s_o}{2^{l-1}} - 1 . \end{cases}$$

Soit $(x, (\sigma)) \in \Lambda_l$. Nous allons majorer $|F_{(\sigma)}(x)|$, puis majorer $t(F_{(\sigma)}(x))$, et constater que la relation (4) n'est pas satisfaite, donc $F_{(\sigma)}(x) = 0$.

Majoration de $|F_{(\sigma)}(x)|$.

La fonction $F_{(\sigma)}$, pour $\sigma_0 + \ldots + \sigma_{m-1} \leqq \dfrac{s_0}{2^l} - 1$, admet les zéros

$$0, \ldots, x_0 t_o^{l-1} - 1 ,$$

d'ordre $\geqq \dfrac{s_o}{2^l}$, grâce à l'hypothèse de récurrence et aux relations (27).

Utilisons le lemme 1 avec $\lambda = N^{1/8}$, $s = 0$, $k = \dfrac{s_0}{2^l} x_0 t_o^{l-1}$.

Le nombre R défini par (1) vérifie $R \ll x_0 t_o^l N^{-1/4}$, donc, en utilisant (26), (28) et (29), on a:

$$\text{Log } |F_{(\sigma)}|_R \ll q R + (q_0 + s_0) \text{ Log } R \ll N^{3m + \frac{l}{2} - \frac{3}{4}} \text{ Log } N .$$

Or:

$$k \text{ Log } \lambda = \frac{1}{8} \frac{s_0}{2^l} x_0 t_o^{l-1} \text{ Log } N \gg N^{3m + \frac{l}{2} - \frac{1}{2}} . \text{Log } N .$$

Pour N assez grand, on obtient:

$$\text{(32)} \qquad \text{Log } |F_{(\sigma)}(x)| \leqq -N^{3m + \frac{l}{2} - \frac{1}{2}} .$$

Majoration de $t(F_{(\sigma)}(x))$.

On remarque que $\Delta^{s_o + q x_o t_o^l m}$ est un dénominateur de $F_{(\sigma)}(x)$, si Δ est un dénominateur de $\alpha_1, \ldots, \alpha_m, \beta_0, \ldots, \beta_{m-1}$; le calcul de la taille de $F_{(\sigma)}(x)$ s'effectue alors comme on l'a fait lors de la construction des $F_{(\sigma)}$; on a, grâce à (26), (28) et (29):

$$t(F_{(\sigma)}(x)) \ll (q_0 + s_0) \text{ Log } x_0 + q x_0 t_o^l ,$$

d'où:

$$(33) \qquad t\big(F_{(\sigma)}(x)\big) \ll N^{3m+\frac{l}{2}-1} \operatorname{Log} N .$$

Comme on le désirait, la relation (4) n'est pas vérifiée pour $\alpha = F_{(\sigma)}(x)$, grâce à (32) et (33), donc:

$$(31) \qquad F_{(\sigma)}(x) = 0 \quad \text{pour} \quad \big(x,(\sigma)\big) \in \Lambda_l .$$

Conclusion. Pour $l_0 = 5\,m^2$ dans (31), on constate que la fonction $F = F_{(0)}$ vérifie:

$$(34) \qquad \frac{d^s}{d\,Z^s} F(x) = 0 \quad \text{pour} \quad \begin{cases} x = 0\,, \dots , x_0\, t_o^{l_o} - 1 \\ s = 0\,, \dots , \dfrac{s_0}{2^{l_o}} - 1\,. \end{cases}$$

Comme:

$$x_0 t_o^{l_o} = N^{\frac{5}{2}m^2+m} > 2\,N^{2m^2+m} = q_0\, q^m ,$$

les équations:

$$F(x) = \sum_{(\lambda)} p(\lambda)\, x^{\lambda_o} . (\alpha_1^{\lambda_1} \dots \alpha_m^{\lambda_m})^x = 0$$

$$\text{pour } x = 0\,, \dots , q_0\, q^m - 1$$

et le lemme 5 montrent que deux des nombres:

$$\alpha_1^{\lambda_1} \dots \alpha_m^{\lambda_m} , \quad 0 \leqq \lambda_i \leqq q - 1 ,$$

sont égaux, donc que les nombres $\alpha_1 , \dots , \alpha_m$ sont multiplicativement dépendants.

Le théorème 2 est donc démontré dans le cas où $2\,i\,\pi$, $\operatorname{Log} \alpha_1 , \dots , \operatorname{Log} \alpha_m$ *sont* **Q***-linéairement indépendants.*

Indiquons pour terminer comment s'effectue la démonstration dans le cas général, à partir du lemme 4 ou de la relation (20).

Soit

$$R = x_0\, t_o^{l_o} , \quad \textit{et} \quad \Delta = \max_{0 \leqq \lambda_i \leqq q-1} (\lambda_1 \operatorname{Log} \alpha_1 + \dots + \lambda_m \operatorname{Log} \alpha_m) .$$

D'après (34), on a:

$$N(R,F) \geqq \frac{s_0}{2^{l_o}} . x_0\, t_o^{l_o} = \frac{1}{2^{5m^2}} . N^{\frac{5}{2}m^2+3m} .$$

D'autre part:

$$q_0\, q^m = N^{2m^2+m}, \quad \text{et} \quad R\varDelta \ll q\, x_0\, t_o^{l_o} = N^{\frac{5}{2}m^2+3m-1}.$$

On obtient alors une contradiction à la fois avec la relation $N(R,F) \leq 3(q_0 q^m - 1) + 4\, R\varDelta$ du lemme 4, et avec la majoration (20) (avec $n = q_0\, q^m$; choisir par exemple $\lambda = \dfrac{1}{6\,m^2}$).

Remarque sur le choix (28) *des fonctions* x_0, s_0, q_0, q, t_0 *de* N

Les seules propriétés requises pour ces fonctions sont les suivantes: ce sont des fonctions monotones croissantes, tendant vers $+\infty$ avec N, et vérifiant:

$$\begin{cases} q_0\, q^m = 2\, x_0\, s_o^m\,; \\ \dfrac{(q_0+s_0)\ \mathrm{Log}\ (x_0 t_0) + q\, x_0\, t_0}{x_0\, s_0} \to 0 \quad \text{quand} \quad N \to +\infty \\ \mathrm{Log}\ t_0 \geq \varepsilon\ \mathrm{Log}\ s_0\,, \quad \text{où} \quad \varepsilon > 0 \text{ ne dépend pas de N.} \end{cases}$$

Par exemple, un autre choix possible est le suivant (Fel'dman, [2]):

$$\begin{cases} q_0 = 2\,.\,N\,.\,(\mathrm{Log}\,N)^\delta\,; & q = (\mathrm{Log}\,N)^{1+2\delta-\frac{\delta}{m}}\,; \\ x_0 = N\,; & s_0 = (\mathrm{Log}\,N)^{1+2\delta}\,; \\ t_0 = (\mathrm{Log}\,N)^{\frac{\delta}{3m}}\,; & \end{cases}$$

avec $\delta > 0$ indépendant de N.

Le choix de ces fonctions est particulièrement important lorsqu'il s'agit d'établir des énoncés effectifs.

Utilisation d'une méthode élémentaire de Gel'fond dans la démonstration des théorèmes 1 *et* 2.

Nous terminerons en remarquant que la méthode exposée par Gel'fond au chapitre 12 de [6], permet de modifier les démonstrations (dans le cas réel) de manière à ne plus utiliser le principe du maximum pour démontrer l'analogue réel du lemme 1; le seul outil analytique qui intervienne est alors le théorème de Rolle (cf. Groupe d'Etude de Théorie des Nombres, exposés n° 1 (16 octobre 1972) et n° 5.(27 novembre 1972), Paris).

RÉFÉRENCES

[1] BAKER, A. Linear forms in the logarithms of algebraic numbers: I. *Mathematika, 13* (1966), 204-216; II, *id., 14* (1967), 102-107; III, *id., 14* (1967), 220-228; IV, *id., 15* (1968), 204-216.
[2] FEL'DMAN, N. I. Estimate for a linear form of logarithms of algebraic numbers. *Mat. Sbornik, 76* (118) (1968), 304-319 (trad. angl., *Math. U.S.S.R. Sbornik, 5* (1968), 291-307).
[3] —— Improved estimate for a linear form of the logarithms of algebraic numbers. *Mat. Sbornik, 77* (119) (1968), 423-436 (trad. angl., *Math. U.S.S.R. Sbornik, 6* (1968), 393-406).
[4] —— and A. B. SHIDLOVSKII. The development and present state of the theory of transcendental numbers. *Usp. Mat. Nauk. S.S.S.R., 22* (1967), 3-81 (trad. angl., *Russian Math. Surveys, 22* (1967), 1-79).
[5] GEL'FOND, A. O. Transcendental and algebraic numbers. *Gosudarstv. Izdat. Tekn.-Teor. Lit.*, Moscou, 1952 (trad. angl., Dover Publ., New York, 1960).
[6] —— et Yu. V. LINNIK. Méthodes élémentaires dans la théorie analytique des nombres. *Gusudarstv. Izdat. Fiz.-mat. Lit.*, Moscou 1962 (trad. franç. Gauthier-Villars, Paris, 1969).
[7] LANG, S. *Introduction to transcendental numbers*. Addison-Wesley, Reading (Mass.), 1966.
[8] —— Transcendental numbers and diophantine approximations. *Bull. Amer. Math. Soc. 77* (1971), 635-677. ;
[9] RAMACHANDRA, K. *Lectures on transcendental numbers*. The Ramanujan Institute, Madras, 1969.
[10] SCHNEIDER, Th. *Einführung in die transzendenten Zahlen*. Springer, Berlin, 1957, (trad. franç., Gauthier-Villars, Paris, 1959).
[11] SIEGEL, C. L. Transcendental numbers. *Ann. of Math. Studies*, n° 16; Princeton Univ. Press, 1949.

(Reçu le 14 juin 1973)

Université de Paris-Sud
Centre d'Orsay
Mathématiques, bât. 425
F-91405 Orsay

vide-leer-empty