

I. Le Théorème de Gel'fond et Schneider SUR LA TRANSCENDANCE DE a^b

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **20 (1974)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 $e^{\alpha_1}, \dots, e^{\alpha_n}$, où $\alpha_1, \dots, \alpha_n$ sont des nombres algébriques \mathbf{Q} -linéairement indépendants.

En 1900, donc, dans son exposé « Mathematische Probleme » (voir: D. Hilbert, *Gesammelte Abhandlungen*, 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 Transzendenz 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 :*

$$a^b = \exp(b \cdot \text{Log } a)$$

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 \mathbb{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:

$$\text{Log } 2. \quad \text{Log } 3 ,$$

et

— *l'indépendance 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 $a^b = \exp(b \cdot \text{Log } a)$). 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 $K = \mathbf{Q}(a, b, a^b)$.

Les deux fonctions

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

sont algébriquement indépendantes (sur \mathbf{C}), prennent leurs valeurs dans K aux points $Z = n$. $\log a, n \in \mathbf{Z}$, 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 $Z = n + mb, (n, m) \in \mathbf{Z} \times \mathbf{Z}$. *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, \dots, 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 :

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

à coefficients algébriques, tel que la fonction entière $F = P(f_1, \dots, f_d)$ 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 $O(R^\rho)$; 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 $s \geq 0$ le plus petit entier tel que

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

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

$$(1) \quad R = \lambda^2 |x_0| + (\lambda^2 + 1) \cdot \sup_{1 \leq h \leq k} |x_h|.$$

Si la fonction F vérifie :

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

alors on a :

$$(3) \quad |F^{(s)}(x_0)| \leq \lambda^{-k}.$$

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

$$|G(x_0)| \leq |G|_R \cdot \frac{|Q(x_0)|}{|Q|_R}.$$

Le choix (1) de R permet la majoration :

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

donc :

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

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

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

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 $d \cdot \gamma$ soit entier algébrique non nul). La norme de $d \cdot \gamma$ 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 minoration, 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:

$$f(x) \ll g(x) \text{ pour } x \rightarrow +\infty$$

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

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

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 $\rho \geq 0$ un nombre réel, tels que:

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

(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 :

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

b) *Taille d'un nombre algébrique*

Précisons 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 da 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 $\sigma_1, \dots, \sigma_n$ (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

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

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 :

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

En effet, le nombre

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

($N_{K/\mathbf{Q}}$ 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 :

$$\text{Log } | \sigma_i(a) | \geq -n \cdot d(a) - (n-1) \text{Log } \| a \| ,$$

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

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

Nous aurons à utiliser les propriétés suivantes de la taille :

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

$$\begin{aligned} t(a_1 \dots a_k) &\leq t(a_1) + \dots + t(a_k) ; \\ t(a_1 + \dots + a_k) &\leq \text{Log } k + t(a_1) + \dots + t(a_k) ; \end{aligned}$$

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

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

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 ≥ 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

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

Enfin soit

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

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

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

et

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

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, \dots, x_n) du système (5) résulte de la non injectivité de l'application :

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

définie par

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

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 $A = \max |a_{i,j}| \geq 1$. Etant donnés deux entiers positifs m et B , on définit l'ensemble

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

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:

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

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 $L : \mathbf{Z}(n, B) \rightarrow \mathbf{Z}(r, nAB)$ 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

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

Alors $(x_j) = (y_j - Z_j)$ vérifie

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

et

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

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

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

Comme $\omega_h \cdot \omega_{h'}$ 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

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

Soit

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

On décompose les éléments $d_i \cdot a_{i,j}$ dans la base $(\omega_1, \dots, \omega_\delta)$: 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

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

on a de plus

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

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

Déterminer des éléments x_1, \dots, 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

$$\sum_{j=1}^n \sum_{h=1}^{\delta} \left(\sum_{h'=1}^{\delta} \alpha_{i,j,h'} \cdot \Omega_{h',h,k} \right) \cdot \xi_{j,h} = 0$$

$$1 \leq i \leq r, \quad 1 \leq k \leq \delta.$$

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

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

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

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

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

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

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

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, \dots, b_l des nombres complexes. Les fonctions :

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

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

$$b_1, \dots, b_l$$

sont \mathbf{Q} -linéairement indépendants.

Il revient au même de dire que si W_1, \dots, 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

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

n'est pas identiquement nulle.

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

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

avec

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

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

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

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

$$a^b = \exp(b \cdot \text{Log } a)$$

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

$$f(N) \ll g(N) \text{ pour } N \rightarrow +\infty.$$

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

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

Nous justifierons ce choix à la fin de la démonstration.

Premier pas. — Il existe des éléments de K

$$a_{i,j}(N), \quad (1 \leq i \leq p(N), 1 \leq j \leq q(N)),$$

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

$$(9) \quad \max_{i,j} \text{Log} \| a_{i,j}(N) \| \ll p(N) \text{Log } q(N) + N^2 \cdot q(N) \ll N^3 \cdot \text{Log } N,$$

tels que la fonction :

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

vérifie :

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

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

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

$$1 \leq \lambda \leq N^2, \quad 1 \leq \mu \leq N^2,$$

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

$$t((\lambda + \mu b)^{i-1} \cdot a^{j\lambda} \cdot (a^{bj})^\mu) \ll p(N) \cdot \text{Log } q(N) + N^2 q(N).$$

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

$$(\lambda + \mu b)^{i-1} \cdot a^{j\lambda} \cdot (a^{bj})^\mu.$$

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

- 1) $F_N(\lambda + \mu b) = 0$ pour $1 \leq \lambda \leq M(N)$, $1 \leq \mu \leq M(N)$
- 2) Il existe $(\lambda_1, \mu_1) \in \mathbf{Z} \times \mathbf{Z}$, $1 \leq \lambda_1 \leq M(N) + 1$,
 $1 \leq \mu_1 \leq M(N) + 1$,

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

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

(i.e. elle est d'ordre ≤ 1), donc le nombre de ses zéros dans un disque $|Z| \leq R$ est majoré par $\ll R$ pour $R \rightarrow +\infty$ (Les constantes impliquées pour $R \rightarrow +\infty$ 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 :

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

On utilise le lemme 1 avec

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

(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 :

$$\text{Log } |F|_R \leq k \text{Log } \lambda = \frac{1}{8} M(N)^2 \cdot \text{Log } M(N)$$

pour

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

Or pour cette valeur de R on a :

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

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

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

Quatrième pas. — La taille de γ vérifie

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

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

$$(13) \quad \text{Log } |\gamma| \gg -M(N)^{3/2} \cdot \text{Log } (M(N)).$$

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

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

est entier sur \mathbf{Z} , donc

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

D'autre part la majoration

$$\text{Log } \|\gamma\| \ll p(N) \cdot \text{Log } M(N) + M(N) q(N)$$

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

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

$$p(N) \cdot q(N) \geq 2N^4 .$$

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

II. LE THÉORÈME DE BAKER SUR L'INDÉPENDANCE LINÉAIRE DE LOGARITHMES DE NOMBRES ALGÈBRIQUES.

§ 1. ÉNONCÉ 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 $\alpha_1, \dots, \alpha_m$ des nombres algébriques dont les logarithmes sont \mathbf{Q} -linéairement indépendants.*