Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 20 (1974)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: INITIATION AUX NOMBRES TRANSCENDANTS

Autor: Waldschmidt, Michel

Kapitel: II. Le théorème de Baker sur l'indépendance LINÉAIRE DE LOGARITHMES DE NOMBRES ALGÉBRIQUES

DOI: https://doi.org/10.5169/seals-46895

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

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

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

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 :

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

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

$$\int_0^1 \frac{dx}{1 + x^3} = \frac{1}{3} \left(\operatorname{Log} 2 + \frac{\pi}{\sqrt{3}}\right).$$

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* $\mathbf{C}$ *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

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

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, Log α_1 , ... , Log α_m, à coefficients algébriques, est non nulle, mais en plus il minorait une telle forme, en fonction des tailles des nombres α_1 , ... , α_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* α_1 , ... , α_m *des nombres algébriques dont les logarithmes sont* $\mathbf{Q}$*-linéairement indépendants. Alors* Log α_1 , ... , Log α_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, $P \in \mathbf{Q}[X_1 , ... , X_m]$ étant un polynôme non nul, si les nombres α_1 , ... , α_m sont suffisamment proches de 1 (d'autant plus proches que le degré total du polynôme est plus grand), alors P (Log α_1, ..., Log α_m) $\neq 0$ (on peut même minorer effectivement ce nombre). Par exemple, si q est un nombre entier, $q > e^{694}$, alors le nombre

$$\text{Log}\,(1+\frac{1}{q})\,.\quad \text{Log}\,(1-\frac{1}{q})$$

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

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

(qui a un degré de transcendance sur **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

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

que l'on notera

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

ainsi

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

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

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

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

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

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

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

et les fonctions $f_{s, \sigma_1, \ldots, \sigma_{m-1}}(Z)$ 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

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

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

(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 $x_0\, s_0\, (c s_0 + 1)^{m-1} \ll x_0\, s_o^m$.

Donc, à condition que

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

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

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

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 $0, \dots, x_0 - 1$, 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 $\mathbf{Q}(\operatorname{Log}\alpha_1, \dots, \operatorname{Log}\alpha_{m-1})$; 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* $f_{s,\sigma_1,\dots,\sigma_{m-1}}(x)$, *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* $f_{s,\sigma_1,\dots,\sigma_{m-1}}(Z)$, pour $0 \leqq s \leqq \frac{s_0}{2} - 1$, *admettent les zéros* $0, 1, \dots, x_0 - 1$, *d'ordre* $\frac{s_0}{2}$. On calcule donc les dérivées de ces fonctions: ce sont des polynômes en $\operatorname{Log} \alpha_1, \dots, \operatorname{Log} \alpha_{m-1}$, dont on cherche à exprimer les coefficients en fonction des

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

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

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

mais

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

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

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

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

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

Or on peut choisir $x_1, \dots, x_{l_0}$ tels que, en plus des propriétés précédentes, on ait

$$x_0\, s_0^m < x_{l_0}\,,$$

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 :

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

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 $p_h(\lambda_0)$, $1 \leqq h \leqq p, 0 \leqq \lambda_0 \leqq q_0 - 1$, 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*

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

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

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

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

§ 4. Démonstration du théorème de Baker

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

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

Soit

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

Considérons un polynôme

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

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

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

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

La relation (22) permet de remplacer

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

par:

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

c'est-à-dire d'écrire F sous la forme

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

où

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

Les dérivées de F vérifient les relations:

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

où

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

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)):

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

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:

$$G(\mathrm{Z}_0, \ldots, \mathrm{Z}_{m-1}) = \sum_{(\lambda)} p(\lambda)\, \mathrm{Z}_o^{\lambda_o} e^{\gamma_o \mathrm{Z}_o} \alpha_1^{\gamma_1 \mathrm{Z}_1} \ldots \alpha_{m-1}^{\gamma_{m-1}\mathrm{Z}_{m-1}}\,,$$

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:

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

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

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

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

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

$$D_{m-1}^{\sigma_{m-1} + \tau_{m-1}} G(Z, \ldots, Z),$$

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 $\geqq 0$, on note Λ_l l'ensemble des $(m+1)$-uples

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

d'entiers vérifiant

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

Construction de la fonction auxiliaire.

Il existe des éléments

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

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

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

et tels que les fonctions

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

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

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

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

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

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

soient entiers sur **Z**. Les conditions

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

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

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

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 :*

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

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

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

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 $\sigma_0 + \dots + \sigma_{m-1} \leq \dfrac{s_0}{2^l} - 1$, admet les zéros

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

d'ordre $\geq \dfrac{s_o}{2^l}$, 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:

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

Or:

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

Pour N assez grand, on obtient:

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

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 $\alpha_1, \dots, \alpha_m$, $\beta_0, \dots, \beta_{m-1}$; 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):

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

d'où:

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

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

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

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:

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

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

et le lemme 5 montrent que deux des nombres:

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

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

Le théorème 2 est donc démontré dans le cas où $2\,i\,\pi$, Log $\alpha_1, \dots,$ Log α_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

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

D'après (34), on a:

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

D'autre part:

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

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

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:

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

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

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

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).