G. REVUZ

Équations diophantiennes exponentielles

Mémoires de la S. M. F., tome 37 (1974), p. 139-156
<http://www.numdam.org/item?id=MSMF_1974__37__139_0>

Journées arithmétiques [1973, Grenoble]
Bull. Soc. math. France,
Mémoire 37, 1974, p. 139-156

EQUATIONS DIOPHANTIENNES EXPONENTIELLES

par

G. REVUZ

-:-:-:-

En 1969, E.G. Straus posait, à Stony Brook [1], le problème de savoir si, étant donné deux entiers naturels θ et φ, tels que $\operatorname{Log}\theta/\operatorname{Log}\varphi$ soit irrationnel, il peut exister une infinité d'entiers naturels qui s'écrivent en base θ et en base φ avec des sommes de chiffres bornées. Ce problème se traduit immédiatement par celui de savoir si l'équation

$$\sum_{i=1}^{M} \lambda_i \theta^{m_i} = \sum_{j=1}^{N} \mu_j \varphi^{n_j}$$

où toutes les lettres représentent des entiers naturels et où $0 \leq \lambda_i \leq \theta - 1$, $0 \leq \mu_j \leq \varphi - 1$, peut avoir une infinité de solutions quand $\operatorname{Log}\theta/\operatorname{Log}\varphi$ est irrationnel.

Se plaçant dans un cadre un peu plus large, on peut se poser le problème d'étudier la finitude du nombre de solutions $(m_i, n_j) \in \mathbf{Z}^{M+N}$ de l'équation

$$\sum_{i=1}^{M} \lambda_i \theta^{m_i} = \sum_{j=1}^{N} \mu_j \varphi^{n_j} \qquad \text{(E)}$$

où λ_i $(1 \leq i \leq M)$ et μ_j $(1 \leq j \leq N)$ sont des nombres algébriques non nuls que l'on peut toujours supposer entiers et θ et φ des nombres algébriques quelconques.

Dans une note aux C.R. [2] j'avais établi la finitude du nombre de solutions de (E) dans un certain nombre de cas particuliers. Indépendamment E.G. Straus et H.G. Senge, dans [3] ont établi cette finitude dans le cas où θ et φ sont des P-V nombres, les solutions étant supposées à valeurs positives, (ce qui donne d'ailleurs la réponse au problème de numération initialement posé), et en ont déduit la solution d'un problème posé par Salem [4] concernant la limite pour u infini de $\prod_{k=0}^{\infty} \cos \pi u \theta^{-k} \times \prod_{k=0}^{\infty} \cos \pi u \varphi^{-k}$ quand θ et φ sont des P-V nombres. L'emploi conjugué des méthodes employées dans les deux travaux précédents permet de résoudre le problème en général.

Nous remarquons d'abord que si (E) admet une solution (m_i, n_j) annulant ses deux membres elle admet l'infinité de solutions $(m_i+k\ ,\ n_j+\ell)$ pour tous k et ℓ dans $\mathbb{Z}$. Nous convenons de ne nous intéresser qu'aux solutions qui n'annulent pas les deux membres. Nous constatons ensuite que si θ et φ sont liés par une relation $\theta^{x_o} = \varphi^{y_o}$ $(x_o \in \mathbb{Z}\ ,\ y_o \in \mathbb{Z})$ l'existence, pour (E), d'une solution (x_i, y_j) entraîne l'existence de l'infinité de solutions $(x_i+kx_o\ ,\ y_j+ky_o)$ où k décrit $\mathbb{Z}$. Notre but est de montrer que, en dehors de ce cas (qui inclut celui où θ ou φ serait racine de 1), (E) ne peut avoir une infinité de solutions, c'est-à-dire d'établir :

Théorème 1. <u>L'équation (E), où</u> λ_i $(1\le i\le M)$, μ_j $(1\le j\le N)$, θ <u>et</u> φ <u>sont des nombres algébriques, ne peut admettre une infinité de solutions en</u> $(m_i, n_j) \in \mathbb{Z}^{M+N}$, <u>n'annulant pas ses 2 membres, si</u> θ <u>et</u> φ <u>sont multiplicativement indépendants sur</u> $\mathbb{Z}$.

<u>Préliminaires</u> : Soit L la plus petite extension galoisienne contenant $Q(\lambda_i, \mu_j, \varphi, \theta)$ et $\Gamma = \text{gal}\, L/\mathbb{Q}$. Pour tout $\sigma \in \Gamma$, toute solution (m_i, n_j) de (E) doit aussi vérifier

$$\sum_{i=1}^{M} \sigma(\lambda_i)[\sigma(\theta)]^{m_i} = \sum_{j=1}^{N} \sigma(\mu_j)[\sigma(\varphi)]^{n_j} \qquad (\sigma(E))$$

Sur L est définie une famille de places P, et, à chacune d'elles est associée une valeur absolue $|\ |_P$ que nous supposerons normalisée de façon telle que ces valeurs absolues satisfassent à la formule du produit. Nous supposons que E (donc $\sigma(E)$) a une infinité de solutions.

Il existe une permutation π de $[1,2,\dots,M]$ et une permutation τ de $[1,2,\dots,N]$ telles que pour une infinité de solutions de (E) on ait :

$$m_{\pi(1)} \ge m_{\pi(2)} \ge \dots \ge m_{\pi(M)} \quad \text{et} \quad n_{\tau(1)} \ge n_{\tau(2)} \dots \ge n_{\tau(N)}\ .$$

On peut donc supposer qu'il existe une infinité de solutions telles que :

$$m_1 \ge m_2 \dots \ge m_M \quad \text{et} \quad n_1 \ge n_2 \ge \dots \ge n_N$$

et ne plus considérer que de telles solutions.

On remarque ensuite que si, pour l'ensemble des solutions considérées une des différences $m_i - m_{i+1}$ restait bornée, pour une infinité de ces solutions cette différence aurait une même valeur a_i. On pourrait alors, dans le premier membre de (E) remplacer $\lambda_i\theta^{m_i} + \lambda_{i+1}\theta^{m_{i+1}}$ par le terme unique $\lambda'_{i+1}\theta^{m_{i+1}}$

en posant $\lambda'_{i+1} = \lambda_i \theta^{a_i} + \lambda_{i+1}$. Cette opération étant répétée autant de fois qu'il est nécessaire on arriverait à une équation du même type que E et pour laquelle les différences entre deux éléments consécutifs des solutions ne seraient pas bornées. Autrement dit, de l'infinité de solutions de (E) on pourrait extraire une suite S_k de solutions (tous les éléments de la solution, m_i et n_j, apparaissent alors comme des fonctions de k) et ces fonctions vérifient :

$$(1) \qquad \begin{aligned} &\forall i, \quad \lim_{k\to+\infty} (m_i - m_{i+1}) = +\infty \\ &\forall j, \quad \lim_{k\to\infty} (n_j - n_{j+1}) = +\infty \end{aligned}$$

Les deux membres de E (qui sont aussi des fonctions de k) seront désignés par A et B . m_1 et m_M ne peuvent être simultanément bornés ; il en est de même pour n_1 et n_N .

En posant au besoin $\theta' = \frac{1}{\theta}$, $m'_i = m_i$, pour tout i , on peut toujours se ramener au cas où

$$\lim_{k\to\infty} m_1 = +\infty$$

θ n'étant pas racine de 1 , il existe des places P pour lesquelles $|\theta|_P > 1$; pour une telle place $\lim_{k\to\infty} |A|_P = +\infty$, donc $\lim_{k\to\infty} |B|_P = +\infty$; donc ou bien $|\varphi|_P > 1$ et $\lim_{k\to\infty} n_1 = +\infty$, ou bien $|\varphi|_P < 1$ et $\lim_{k\to\infty} n_N = -\infty$. Si pour toutes les places P pour lesquelles $|\theta|_P > 1$, on était dans la deuxième de ces éventualités on poserait $\varphi' = \frac{1}{\varphi}$ et $m'_j = -m_j$ pour tout j . On peut donc toujours se ramener au cas où

$$(2) \qquad \lim_{k\to\infty} m_1 = \lim_{k\to\infty} n_1 = +\infty$$

et où <u>il existe au moins une place</u> P_o <u>pour laquelle</u> $|\theta|_{P_o} > 1$, $|\varphi|_{P_o} > 1$.

Nous allons maintenant <u>sous cette hypothèse, et sous celle que</u> (E) <u>admet une suite</u> S_k <u>de solutions satisfaisant à (1) et (2)</u>, établir un certain nombre de résultats intermédiaires.

Lemme 1. <u>Pour toute place</u> P <u>telle que</u> $|\theta|_P > 1$, $|\varphi|_P > 1$

$$(3) \qquad \lim_{k\to\infty} \frac{m_1}{n_1} = \frac{\log|\varphi|_P}{\log|\theta|_P}$$

Soit $\wp = \{P \,|\, |\theta|_P > 1 \, , \, |\varphi|_P > 1\}$. (3) résulte immédiatement du fait que, pour une valeur absolue non archimédienne, appartenant à $\wp$ et pour k assez grand

$$|A|_P = |\lambda_1|_P |\theta|_P^{m_1} \qquad |B|_P = |\mu_1|_P |\varphi|_P^{n_1}$$

et que, pour une valeur absolue archimédienne, appartenant à $\wp$, définie par $\sigma \in \Gamma$

$$\sigma(A) \sim \sigma(\lambda_1)[\sigma(\theta)]^{m_1}$$

$$\sigma(B) \sim \sigma(\mu_1)[\sigma(\varphi)]^{n_1}$$

quand k tend vers l'infini.

Si nous posons $\alpha = \lim_{k\to\infty} \frac{m_1}{n_1}$, le lemme peut s'exprimer sous la forme

$$\forall P \in \wp \, , \quad |\varphi|_P = |\theta|_P^{\alpha} \, .$$

Lemme 2.(1) <u>De la suite</u> S_k , <u>on peut extraire une suite</u> S_h <u>de solutions qui vérifient l'équation raccourcie</u>

$$\sum_{i=1}^{i_o} \lambda_i \theta^{m_i} = \sum_{j=1}^{j_o} \mu_j \varphi^{n_j} \quad , \quad i_o \le M \; , \quad j_o \le N \qquad (\mathcal{E})$$

<u>les solutions de cette suite satisfaisant à</u>

$$\forall i \quad 1 \le i \le i_o \quad \lim_{h\to\infty} \frac{m_i}{m_1} = 1$$

$$\forall j \quad 1 \le j \le j_o \quad \lim_{h\to\infty} \frac{n_j}{n_1} = 1 \, .$$

Remarquons en effet que les rapports $\frac{m_i}{m_1}$ et $\frac{n_j}{n_1}$ étant majorés par 1 , on peut, de la suite S_k considérée, extraire une suite S_h telle que chacun de ces rapports ait une limite l_i ou L_j et que ces limites vérifient

$$\forall i \; , \; \forall j \quad l_{i+1} \le l_i \le 1 \qquad L_{j+1} \le L_j \le 1 \, .$$

Soit alors i_o (resp. j_o) le plus grand indice i (resp. j) tel que $l_i = 1$ (resp. $L_j = 1$) . $(\mathcal{E})$ s'écrit alors sous la forme

(1) Ce lemme (qui joue un rôle essentiel) est dû à Straus et Senge.

$$\sum_{i=1}^{i_o} \lambda_i \theta^{m_i} + \varepsilon_A = \sum_{j=1}^{j_o} \mu_j \varphi^{n_j} + \varepsilon_B$$

ε_A (resp. ε_B) désignant la somme des termes de rang supérieur à i_o (resp. j_o) dans A (resp. B), puis, sous la forme

(4) $$1 - \rho\varphi^{n_{j_o}} \theta^{-m_{i_o}} = \frac{\varepsilon_B - \varepsilon_A}{A}$$

avec $$\rho = \sum_{j=1}^{j_o} \mu_j \varphi^{n_j - n_{j_o}} \Big/ \sum_{i=1}^{i_o} \lambda_i \theta^{m_i - m_{i_o}} .$$

Un lemme dû à Straus et Senge (cf. [3]) permet alors, pour une valeur absolue quelconque, associée à une place P_o, de minorer le premier membre de (4) si celui-ci est différent de 0 : étant donné un corps L de degré fini sur Q et, un nombre ζ, algébrique sur L, des nombres $\theta_1, \ldots, \theta_r$ de L et $\delta > 0$ arbitraire, il n'existe qu'un nombre fini d'éléments $\rho \in L$ et un nombre fini d'entiers naturels $m_1, \ldots, m_r$ tels que

$$0 < |\zeta - \theta_1^{m_1} \ldots \theta_r^{m_r} \rho|_{P_o} < \frac{C}{H(\theta_1)^{m_1\delta} \ldots H(\theta_r)^{m_r\delta} H(\rho)^{2+\delta}}$$

C étant une constante et la hauteur $H(\alpha)$ étant définie pour tout $\alpha \in L$ par

$$H(\alpha) = \prod_P \max(1, |\alpha|_P)$$

le produit étant étendu à l'ensemble des valeurs absolues normalisées. Nous appliquons ce lemme en prenant $\zeta = 1$, φ et $1/\theta$ pour nombres θ_1, θ_2. Il résulte de ce lemme que pour k (et donc m_{i_o} et n_{j_o}) suffisamment grand, on a :

(5) $$|1 - \rho\varphi^{n_{j_o}} \theta^{-m_{i_o}}|_{P_o} > \frac{C}{H(\varphi)^{n_{j_o}\delta} H(\frac{1}{\theta})^{m_{i_o}\delta} H(\rho)^{2+\delta}}$$

Désignons par $\mathcal{P}_\theta$ (resp. $\mathcal{P}_\varphi$) l'ensemble des places donnant à θ (resp. φ) des valeurs absolues supérieures à 1 et posons

$$H(\varphi) = \prod_{P \in \mathcal{P}_\varphi} |\varphi|_P = b$$

$$H(\tfrac{1}{\theta}) = H(\theta) = \prod_{P \in \mathcal{P}_\theta} |\theta|_P = a$$

(l'égalité des hauteurs d'un nombre et de son inverse résultant de la formule du produit).

Pour évaluer $H(\rho)$ remarquons d'abord que pour tout couple de nombres a et a' de L, $H(aa') \leq H(a).H(a')$. D'où, en désignant par ψ et χ le numérateur et le dénominateur de ρ

$$H(\rho) \leq H(\psi).H(\frac{1}{\chi}) = H(\psi).H(\chi) .$$

Or, pour toute place $P \notin \mathcal{P}_\varphi$, ψ a des valeurs absolues bornées. Il existe donc une constante C_1 telle que

$$H(\psi) \leq C_1 \prod_{P \in \mathcal{P}_\varphi} |\psi|_P \quad ;$$

pour toute place $P \in \mathcal{P}_\varphi$ définissant une valeur absolue non archimédienne

$$|\psi|_P = |\mu_1|_P |\varphi|_P^{n_1 - n_{j_o}}$$

dès que k est assez grand ; et pour toute place $P \in \mathcal{P}_\varphi$, définie par $\sigma \in \Gamma$,

$$\psi \sim \sigma(\mu_1)\sigma(\varphi)^{n_1 - n_{j_o}}$$

quand k tend vers l'infini ; donc il existe une constante C_σ telle que

$$|\psi|_P \leq C_\sigma |\varphi|_P^{n_1 - n_{j_o}} .$$

Finalement,

$$H(\psi) \leq C'_1 \prod_{\mathfrak{p} \in \mathcal{P}_\varphi} |\varphi|_P^{n_1 - n_{j_o}} = C'_1 b^{n_1 - n_{j_o}}$$

(C'_1, comme toutes les lettres C indexées qui apparaîtront dans la suite du calcul désignant des constantes).

De même,

$$H(\chi) \leq C'_2 \prod_{\mathfrak{p} \in \mathcal{P}_\theta} |\theta|_P^{m_1 - m_{i_o}} = C'_2 a^{m_1 - m_{i_o}} .$$

Or, on a

$$m_1 = n_1 \alpha(1+\varepsilon)$$

$$m_{i_o} = n_{j_o} \alpha(1+\varepsilon')$$

$$m_1 - m_{i_o} = m_{i_o} \varepsilon_1$$

$$n_1 - n_{j_o} = n_{j_o} \varepsilon_2$$

les lettres ε , ε' , ε_1 , ε_2 désignant des fonctions de k tendant vers 0 quand k tend vers l'infini. Ceci permet d'écrire

$$H(\rho) \leq C_1'C_2' b^{n_{j_o}\varepsilon_2} a^{n_{j_o}\varepsilon_1(1+\varepsilon')} = C_1'C_2' b^{n_{j_o}} a^{n_{j_o}\eta}$$

avec $\lim_{k\to\infty} \eta = 0$. En reportant ces expressions dans (5) on trouve

$$(6) \qquad |1-\rho\varphi^{n_{j_o}}\theta^{-m_{i_o}}| > \frac{C_3}{b^{n_{j_o}\delta} a^{n_{j_o}(1+\varepsilon')\delta} b^{n_{j_o}\varepsilon_2} a^{n_{j_o}\eta}} > \frac{C_3}{b^{n_{j_o}\delta} a^{2n_{j_o}\delta} b^{n_{j_o}\varepsilon_2} a^{n_{j_o}\eta}}$$

Majorons maintenant le deuxième membre de (4) :

$$|\varepsilon_B - \varepsilon_A|_{P_o} < 2\max(|\varepsilon_B|_{P_o}, |\varepsilon_A|_{P_o}) .$$

De la définition de i_o et j_o résulte qu'il existe une constante $f < 1$ telle que

$$m_{i_o+1} < fm_{i_o}$$

$$n_{j_o+1} < fn_{j_o}$$

et il existe alors des constantes C' et C'' telles que

$$|\varepsilon_A|_{P_o} < C'|\theta|_{P_o}^{fm_{i_o}} < C|\varphi|_{P_o}^{fn_{j_o}(1+\varepsilon')}$$

$$|\varepsilon_B|_{P_o} < C''|\varphi|_{P_o}^{fn_{j_o}}$$

Il vient alors

$$|\varepsilon_B - \varepsilon_A| < 2\max(C', C'')|\varphi|_{P_o}^{fn_{j_o}(1+|\varepsilon'|)}$$

$$= C_4|\varphi|_{P_o}^{fn_{j_o}(1+|\varepsilon'|)} .$$

D'autre part, pour k assez grand

$$|A|_{P_o} > C_5|\theta|_{P_o}^{m_1} = C_5|\varphi|^{n_{j_o}(1+\varepsilon)(1+\varepsilon_2)} \quad ;$$

quand k tend vers l'infini les exposants de $|\varphi|^{n_{j_o}}$ dans les deux formules précédentes tendent respectivement vers f et 1 ; f étant strictement < 1, pour k assez grand, leur différence dépassera $\frac{1-f}{2}$. On aura donc

$$(7) \qquad \left|\frac{\varepsilon_B-\varepsilon_A}{A}\right|_{P_o} < \frac{C_4}{C_5}|\varphi|_{P_o}^{n_{j_o}\frac{f-1}{2}}$$

De (4), (6), (7) résulte alors

$$\frac{C_4}{C_5}|\varphi|_{P_o}^{n_{j_o}\frac{f-1}{2}} > \frac{C_3}{b^{n_{j_o}\delta}a^{2n_{j_o}\delta}b^{n_{j_o}\varepsilon}2_a^{n_{j_o}\eta}}$$

$$|\varphi|_{P_o}^{\frac{f-1}{2}} > \frac{C_6}{b^{\delta}a^{2\delta}b^{\varepsilon}2_a^{\eta}}$$

$\dfrac{C_6^{\frac{1}{n_{j_o}}}}{b^{\varepsilon}2_a^{\eta}}$ tend vers 1 quand k tend vers l'infini ; $|\varphi|_{P_o}^{\frac{f-1}{2}}$ est strictement inférieur à 1 ; cette inégalité est donc impossible pour δ arbitraire. L'égalité (4) n'est donc possible que si ses deux membres sont nuls, ce qui établit le lemme 2.

On en déduit :

Corollaire. <u>Toute place</u> P <u>qui rend</u> $|\theta|_P > 1$, <u>rend aussi</u> $|\varphi|_P > 1$ (c'est évident puisque, dans le cas contraire on aurait $\lim\limits_{h\to\infty}|A|_P = +\infty$, et $\lim\limits_{h\to\infty}|B|_P = 0$).

Nous allons maintenant comparer toutes les valeurs absolues de θ et de φ en distinguant le cas des valeurs absolues non archimédiennes ou archimédiennes.

Lemme 3. <u>Il existe</u> α, <u>ne dépendant pas de</u> $\mathfrak{p}$, <u>tel que pour tout idéal</u> $\mathfrak{p}$ <u>de l'anneau des entiers de</u> L

$$(8) \qquad |\varphi|_{\mathfrak{p}} = |\theta|_{\mathfrak{p}}^{\alpha}$$

Posons

$$\mathcal{P}_1 = \{\mathfrak{p} \mid |\theta|_{\mathfrak{p}} > 1 \, , \, |\varphi|_{\mathfrak{p}} > 1\}$$

$$\mathcal{P}_2 = \{\mathfrak{p} \mid |\theta|_{\mathfrak{p}} = 1 \, , \, |\varphi|_{\mathfrak{p}} = 1\}$$

$$\mathcal{P}_3 = \{\mathfrak{p} \mid |\theta|_{\mathfrak{p}} < 1 \, , \, |\varphi|_{\mathfrak{p}} < 1\}$$

(8) est déjà montrée pour $\mathfrak{p} \in \mathcal{P}_1$, est trivialement vraie pour $\mathfrak{p} \in \mathcal{P}_2$, et, pour $\mathfrak{p} \in \mathcal{P}_3$, résulte du fait que

$$\forall \mathfrak{p} \in \mathcal{P}_3 \quad \frac{\log|\varphi|_{\mathfrak{p}}}{\log|\theta|_{\mathfrak{p}}} = \lim_{h\to\infty} \frac{m_{i_o}}{n_{j_o}} = \alpha \, .$$

Il nous reste à établir que tous les idéaux de L se partagent entre $\mathcal{P}_1$, $\mathcal{P}_2$ et $\mathcal{P}_3$, c'est-à-dire que $|\varphi|_{\mathfrak{p}} = 1$ (qui entraîne a priori $|\theta|_{\mathfrak{p}} \leq 1$) entraîne, en fait $|\theta|_{\mathfrak{p}} = 1$.

Soit donc $\mathfrak{p}_o$ tel que $|\varphi|_{\mathfrak{p}_o} = 1$. En tenant compte de ce que $|\theta|_{\mathfrak{p}_o} \leq 1$, et de ce que nous avons supposé les coefficients λ_i et μ_j entiers, on peut écrire

$$|\theta|_{\mathfrak{p}_o}^{m_{i_o}} \geq |A|_{\mathfrak{p}_o} = |B|_{\mathfrak{p}_o} = |\psi|_{\mathfrak{p}_o} \, ,$$

$\psi = \sum_{j=1}^{j_o} \mu_j \varphi^{n_j - n_{j_o}}$ étant le nombre étudié lors de la démonstration du lemme 2.

En désignant par $P_{\mathfrak{p}_o}$ la place définie par l'idéal $\mathfrak{p}_o$ on peut affirmer, du fait de la formule du produit

$$|\psi|_{\mathfrak{p}_o} = \frac{1}{\prod_{P \neq P_{\mathfrak{p}_o}} |\psi|_{\mathfrak{p}}} \geq \frac{1}{H|\psi|} \geq \frac{1}{C'_1 b^{n_1 - n_{j_o}}}$$

D'où

$$|\theta|_o^{m_{i_o}} \geq \frac{1}{C'_1 b^{\frac{m_{i_o}}{\alpha} \frac{\epsilon_2}{1+\epsilon'}}}$$

$$|\theta|_{\mathfrak{p}_o} \geq \frac{1}{C_1'^{\frac{1}{m_{i_o}}} b^{\eta'}} \qquad \text{avec} \quad \eta' = \frac{\epsilon_2}{1+\epsilon'} \frac{1}{\alpha} \, .$$

Quand h tend vers l'infini, le deuxième membre de cette inégalité tend vers 1. On en conclut $|\theta|_{\mathfrak{p}_o} = 1$.

Ceci termine la démonstration du lemme 3 dont il résulte, en particulier, que θ et φ sont, ou ne sont pas, simultanément, des unités.

Lemme 4. <u>Pour tout</u> $\sigma \in \Gamma$, $|\sigma(\varphi)| = |\sigma(\theta)|^{\alpha}$ (9).

Posons

$$\Gamma_1 = \{\sigma \in \Gamma \mid |\sigma(\theta)| > 1 \ , \ |\sigma(\varphi)| > 1\}$$
$$\Gamma_2 = \{\sigma \in \Gamma \mid |\sigma(\theta)| = 1 \ , \ |\sigma(\varphi)| = 1\}$$
$$\Gamma_3 = \{\sigma \in \Gamma \mid |\sigma(\theta)| < 1 \ , \ |\sigma(\varphi)| < 1\}$$

(9) est déjà montrée pour $\sigma \in \Gamma_1$, est trivialement vraie pour $\sigma \in \Gamma_2$, et, pour $\sigma \in \Gamma_3$, résulte du fait que

$$\forall \sigma \in \Gamma_3 \quad \frac{\log|\sigma(\varphi)|}{\log|\sigma(\theta)|} = \lim_{h\to\infty} \frac{m_{i_0}}{n_{j_0}} = \alpha \ .$$

Il nous reste à établir que les automorphismes σ se partagent entre $\Gamma_1, \Gamma_2, \Gamma_3$.

Supposons donc qu'il existe $\sigma \in \Gamma$ tel que $|\sigma(\theta)| < 1$, $|\sigma(\varphi)| = 1$. Nous distinguerons deux cas suivant que θ et φ ont, tous deux des conjugués de module 1 (cas i) ou que seul φ en a (cas ii).

Cas i) θ et φ ont, tous deux des conjugués de module 1. Dans ce cas leurs polynômes minimaux P_θ, et P_φ (distincts ou confondus) sont des polynômes réciproques. Soient Q_θ et Q_φ leurs polynômes résolvants (polynômes dont les racines sont $z_0 + \frac{1}{z_0}$, pour tout z_0 racine de P_θ ou de P_φ) et considérons le sous-groupe g de Γ qui laisse invariant le corps engendré par les racines de Q_θ et de Q_φ ; tout automorphisme appartenant à g transforme une racine de P_θ ou de P_φ soit en elle-même soit en son inverse ; on peut choisir $\tau \in g$ tel que $\sigma(\theta)$ ne soit pas invariant ; on aura alors $|\tau\sigma(\theta)| = \dfrac{1}{|\sigma(\theta)|} > 1$, $|\tau\sigma(\varphi)| = 1$, c'est-à-dire que nous tomberons sur un cas d'impossibilité ; un tel automorphisme σ ne peut donc exister.

Cas ii) θ n'a aucun conjugué de module 1. φ a encore un polynôme minimal réciproque, donc 1 pour norme et comme sa norme dans L/Q est une puissance de sa norme absolue

$$\prod_{\sigma\in\Gamma} |\sigma(\varphi)| = 1 \ .$$

Mais alors, on déduit de la formule du produit

$$\prod_{\mathfrak{p}} |\varphi|_{\mathfrak{p}} = 1$$

le produit étant étendu à tous les idéaux de l'anneau des entiers de L . On déduit alors du lemme 3

$$\prod_p |\theta|_p = 1$$

donc

(10) $$\prod_{\sigma\in\Gamma} |\sigma(\theta)| = 1 \ .$$

Or, les $\sigma \in \Gamma$ qui ne rendent pas, a priori impossible l'existence de la suite S_h de solutions de $\sigma(\mathcal{E})$ se répartissent entre $\Gamma_1, \Gamma_2, \Gamma_3$ et

$$\Gamma_4 = \{\sigma \in \Gamma \mid |\sigma(\theta)| < 1 \ , \ |\sigma(\varphi)| = 1\}$$

donc

$$\prod_{\sigma\in\Gamma} |\sigma(\varphi)| = \prod_{\sigma\in\Gamma_1\cup\Gamma_3} |\sigma(\varphi)| = 1 \ .$$

Mais alors $\prod_{\sigma\in\Gamma_1\cup\Gamma_3} |\sigma(\theta)| = 1$ (puisque ce nombre est égal à la puissance $\frac{1}{\alpha}$-ième du précédent) ce qui, rapprochée de (10), montre que $\prod_{\sigma\in\Gamma_4} |\sigma(\theta)| = 1$

donc $\Gamma_4 = \emptyset$, ce qui achève d'établir le lemme 4.

<u>Fin de la démonstration du théorème I quand</u> θ <u>et</u> φ <u>ne sont pas des unités</u>.

$\mathcal{P}_1 \cup \mathcal{P}_3 \neq \emptyset$; α , rapport de deux valuations, est alors rationnel. Posons,

$$\alpha = \frac{s}{r} (r \in \mathbb{N}, s \in \mathbb{N}) \ .$$

On a alors,

$$\theta^s = \varphi^r u \quad \text{avec} \quad |u| = 1 \ .$$

Mais du lemme 2 on déduit :

$$\forall \sigma \in \Gamma \qquad |\sigma(u)| = 1$$

et du lemme 3

$$\forall p \qquad |u|_p = 1 \ .$$

De l'ensemble de ces propriétés résulte que u est une racine de 1 ; si $k \in \mathbb{N}$ est tel que $u^k = 1$ on a :

$$\theta^{sk} = \varphi^{rk}$$

ce qui établit la dépendance multiplicative de θ et de φ .

Fin de la démonstration du théorème I quand θ et φ sont des unités.

L'hypothèse que θ et φ sont des unités entraînent que, pour un σ au moins, on ait $|\sigma(\theta)| > 1$, $|\sigma(\varphi)| > 1$, on peut toujours supposer

$$|\theta| > 1 \ , \quad |\varphi| > 1 \ .$$

On aura alors

$$\lim_{h\to\infty} \frac{\theta^{m_1}}{\varphi^{n_1}} = \frac{\mu_1}{\lambda_1} \ .$$

Pour h suffisamment grand, l'unité $\theta^{m_1}/\varphi^{n_1}$ appartient donc à un compact. Examinons ses conjugués :

$$\forall\sigma \in \Gamma \quad |\sigma(\frac{\theta^{m_1}}{\varphi^{n_1}})| = \frac{|\sigma(\theta)|^{m_1}}{|\sigma(\varphi)|^{n_1}} = |\sigma(\theta)|^{m_1-n_1\alpha}$$

en particulier

$$\frac{|\theta|^{m_1}}{|\varphi|^{n_1}} = |\theta|^{m_1-n_1\alpha}$$

d'où

$$\lim_{h\to\infty} (m_1 - n_1\alpha) = \frac{\mathrm{Log}|{}^{\mu_1}/\lambda_1|}{\mathrm{Log}|\theta|}$$

$m_1 - n_1\alpha$ tend donc vers une limite finie, soit β ; et alors

$$\lim_{h\to\infty} |\sigma(\frac{\theta^{m_1}}{\varphi^{n_1}})| = |\sigma(\theta)|^{\beta} \ .$$

Tous les conjugués de $\theta^{m_1}/\varphi^{n_1}$ appartiennent donc à un compact, pour h suffisamment grand ; dans ces conditions le polynôme caractéristique de l'entier $\theta^{m_1}/\varphi^{n_1}$ a des coefficients qui ne peuvent prendre qu'un nombre fini de valeurs ; $\theta^{m_1}/\varphi^{n_1}$ ne peut donc aussi prendre qu'un nombre fini de valeurs. Pour 2 éléments de la suite S_h au moins, ce rapport est le même : $\theta^{m_1}/\varphi^{n_1} = \theta^{m'_1}/\varphi^{n'_1}$; θ et φ sont multiplicativement dépendants sur $\mathbf{Z}$.

Nous allons maintenant étudier une équation diophantienne exponentielle à trois bases et généraliser à son sujet un résultat de Gelfond [5].

Théorème II. L'équation

$$\lambda a^x + \mu b^y + \nu c^z = 0 \qquad \text{(E)}$$

où λ , μ , ν , a , b , c sont six nombres algébriques non nuls, ne peut avoir une infinité de solutions en $(x,y,z) \in Z^3$, en dehors du cas où a , b , c sont deux à deux multiplicativement dépendants.

Nous montrerons d'abord :

Lemme 1. Si (E) a une infinité de solutions et si deux des bases a , b , c sont multiplicativement dépendantes, alors ces trois bases sont deux à deux multiplicativement dépendantes.

Supposons en effet qu'il existe x_o et y_o dans Z tels que

$$a^{x_o} = b^{y_o}$$

(on peut toujours choisir le couple x_o , y_o de façon que x_o soit positif) et soit d tel que $d^{x_o} = b$. On a alors

$$(a/d^{y_o})^{x_o} = 1$$

d'où

$$a = d^{y_o}\zeta$$

ζ étant une racine x_o-ième de 1 . Mais alors (E) s'écrit

$$\lambda\zeta^x d^{y_o x} + \mu d^{x_o y} + \nu c^z = 0$$

ζ^x ne pouvant prendre que x_o valeurs différentes, pour une infinité de solutions, ce nombre a la même valeur ζ_o ; et ces solutions vérifient :

$$\lambda' d^{x'} + \mu d^{y'} + \nu c^z = 0$$

avec $\lambda' = \lambda\zeta_o$, $x' = y_o x$, $y' = x_o y$; on sait qu'une telle équation exponentielle à deux bases ne peut avoir une infinité de solutions en vertu du théorème I que si c et d , donc c et b sont multiplicativement dépendants ce qui établit le lemme.

Pour démontrer, par l'absurde, le théorème II nous supposons alors que (E) a une infinité de solutions et qu'il n'existe pas, entre les trois bases, deux relations de dépendance linéaire ; il résulte alors du lemme 1 qu'il n'y en a aucune, donc que a , b et c sont deux à deux multiplicativement indépendants.

Nous nous placerons donc dorénavant dans l'hypothèse : a , b et c sont deux à deux multiplicativement indépendants et E a une infinité de solutions et c'est à partir de cette double hypothèse que nous allons chercher à aboutir à une contradiction.

Préliminaires.

Notons d'abord que l'hypothèse d'indépendance multiplicative des bases entraîne qu'aucune d'elles n'est racine de 1 . Soit ensuite L la plus petite extension galoisienne contenant $\mathbb{Q}(a,b,c,\lambda,\mu,\nu)$; L est muni d'un système complet de places P et nous supposons les valeurs absolues correspondantes normalisées de façon à satisfaire à la formule du produit. (E) ayant une infinité de solutions, aucun des trois nombres x,y,z ne peut rester borné ; si en effet l'un d'eux l'était, pour une infinité de solutions, il garderait la même valeur et ces solutions vérifieraient une équation exponentielle à deux bases, ce qui contredirait encore le théorème I.

En posant, au besoin, $a' = \frac{1}{a}$, $x' = -x$ (ou l'analogue pour b et c) on peut toujours supposer que l'ensemble des x , celui des y et celui des z (tels que (x,y,z) soit solution) ne sont pas majorés ; on peut alors de l'infinité de solutions supposée extraire une suite S_h de solutions $(x,y,z$ deviennent alors des fonctions de h) ces solutions vérifiant

$$\lim_{h\to\infty} x = \lim_{h\to\infty} y = \lim_{h\to\infty} z = +\infty .$$

Comparaison des diverses valeurs absolues des 3 bases.

Supposons que, pour, une infinité de solutions appartenant à S_h on ait, pour une place P fixée

$$(1) \qquad |\lambda a^x|_P \geq |\mu b^y|_P \geq |\nu c^z|_P .$$

Supposons d'abord $|a|_P > 1$. Il en résulte que $\lim_{h\to\infty} |\lambda a^x|_P = +\infty$. Les deux autres termes de (E) ne peuvent donc restées bornés simultanément ; il en résulte déjà que $|b|_P > 1$. Ecrivons alors (E) sous la forme

$$(2) \qquad b^y a^{-x} + \frac{\lambda}{\mu} = \frac{\nu}{\mu} c^z a^{-x} .$$

Un théorème de Gelfond [6] sur l'approximation ordinaire ou $\mathfrak{p}$-adique d'un nombre algébrique (ici $\frac{\lambda}{\mu}$) par un produit de nombres algébriques (ici a et b) multiplicativement indépendants sur Z permet alors d'écrire, que pour h assez grand

$$|\frac{\nu}{\mu}c^{z}a^{-x}|_{P} > e^{-\delta\,\sup(x,y)} \geq e^{-\delta' x}$$

(δ et δ' réesl positifs arbitraires).

(Car de $|\lambda a^{x}|_{P} > |\mu b^{y}|_{P}$ on déduit que le rapport y/x est majoré, donc $\mathrm{Sup}(x,y) \ll x$).

Cette inégalité s'écrit

$$K + z\log|c|_{P} > x(\log|a|_{P} - \delta') \qquad \text{(K constante)}$$

et ceci exige $|c|_{P} > 1$.

Si on était parti de l'hypothèse $|b|_{P} > 1$, on aurait déduit de (1) , $|a|_{P} > 1$ et on serait retombé sur le cas précédent. Enfin $|c|_{P} > 1$ entraîne $|a|_{P} > 1$, $|b|_{P} > 1$

D'autre part, en rapprochant (1) de (3) on a :

$$K' + x\log|a|_{P} > K + z\log|c|_{P} > x(\log|a|_{P} - \delta)$$

et on en déduit

(3) $$\lim_{h\to\infty} \frac{x}{z} = \frac{\log|c|_{P}}{\log|a|_{P}} .$$

De même, en écrivant (E) sous la forme

$$c^{z}a^{-x} + \frac{\lambda}{\nu} = \frac{\mu}{\nu}b^{y}a^{-x}$$

d'où on déduit

$$K + y\log|b|_{P} > x(\log|a|_{P} - \delta')$$

on arrive à

(4) $$\lim_{h\to\infty} \frac{x}{y} = \frac{\log|b|_{P}}{\log|a|_{P}} .$$

La symétrie des résultats obtenus montre qu'il sont indépendants de l'hypothèse provisoire (1). Si nous remarquons enfin que

$$\mathcal{P}_{1} = \{P \mid |a|_{P} > 1 \;,\; |b|_{P} > 1 \;,\; |c|_{P} > 1\} \neq \emptyset$$

du fait de la formule du produit, puisque a,b,c ne sont pas des racines de 1, nous pouvons conclure :

<u>Pour toute place</u> P <u>de</u> L, <u>les trois valeurs absolues</u> $|a|_P$, $|b|_P$, $|c|_P$ <u>sont, ou ne sont pas, simultanément supérieures à</u> 1. <u>Quand</u> h <u>tend vers l'infini les rapports</u> x/y <u>et</u> x/z <u>tendent vers des limites finies non nulles</u> α <u>et</u> β <u>qui sont respectivement la valeur commune des rapports</u>

$$\frac{\log|b|_P}{\log|a|_P} \quad \underline{\text{et}} \quad \frac{\log|c|_P}{\log|a|_P},$$

<u>pour toute place</u> P <u>de</u> $\mathcal{P}_1$.

Examinons maintenant les autres valeurs absolues de a,b,c. Soit P une place n'appartenant pas à $\mathcal{P}_1$ et faisons à nouveau, pour cette place, l'hypothèse (1).

$$|a|_P < 1 \Rightarrow \lim_{h\to\infty} |\lambda a^x|_P = 0 \Rightarrow \begin{matrix} \lim|\mu b^y|_P = 0 \Rightarrow |b|_P < 1 \\ \lim|\nu c^z|_P = 0 \Rightarrow |c|_P < 1 \end{matrix}$$

Supposons maintenant $|c|_P < 1$. Ecrivons encore (E) sous la forme (2) et déduisons en (3). Cette inégalité est impossible si $|a|_P > 1$ et, si $|a|_P = 1$, on en déduirait $\lim_{h\to\infty} z/x = 0$, contrairement à ce qui a été montré. Enfin $|b|_P < 1$ entraîne $|c|_P < 1$, ce qui nous ramène au cas précédent. D'autre part nous obtiendrons, de la même façon que ci-dessus, les formules (3) et (4), et la symétrie des résultats obtenus montre qu'ils sont encore indépendants de l'hypothèse (1). Nous sommes donc en mesure de généraliser le résultat énoncé ci-dessus et d'énoncer :

Lemme 2. <u>Toutes les places de</u> L <u>se partagent entre</u> $\mathcal{P}_1$,

$$\mathcal{P}_2 = \{P \mid |a|_P = |b|_P = |c|_P = 1\} \quad \underline{\text{et}} \quad \mathcal{P}_3 = \{P \mid |a|_P < 1,\ |b|_P < 1,\ |c|_P < 1\}$$

<u>et il existe deux réels non nuls</u> α <u>et</u> β <u>tels que pour toute place</u> P <u>on ait</u>

$$|b|_P = |a|_P^{\alpha}, \quad |c|_P = |a|_P^{\beta}.$$

(Ces égalités démontrées pour les places de $\mathcal{P}_1$ et $\mathcal{P}_3$ étant trivialement vraies pour celles de $\mathcal{P}_2$). Il résulte en particulier de ce lemme que a,b,c sont (ou ne sont pas) simultanément des unités.

Fin de la démonstration quand les bases ne sont pas des unités.

Dans ce cas α, rapport de deux valuations est un rationnel r/s. D'autre part on peut poser $b^s = a^r u$, et il résulte du lemme que, pour toute place P, $|u|_P = 1$; u est donc une racine de l'unité. Soit k tel que $u^k = 1$. On arrive à

$$b^{sk} = a^{rk} \quad (sk \in Z\ ,\ rk \in Z)\ .$$

Ceci contredit l'hypothèse d'indépendance multiplicative de a et b et termine, dans ce cas, la démonstration. (On montrerait de même la dépendance de a et c mais ce n'est pas nécessaire).

Fin de la démonstration quand les bases sont des unités.

Dans ce cas, toutes les places finies sont dans $\mathcal{P}_2$, et toutes les valeurs absolues archimédiennes sont définies par des automorphismes de $\Gamma = \mathrm{gal}\, L/\mathbb{Q}$ qui se partagent entre les sous-ensembles $\Gamma_1, \Gamma_2, \Gamma_3$ de Γ, définissant respectivement des places appartenant à $\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3$. En outre (formule du produit) Γ_1 n'est pas vide. Soit σ un de ses éléments. Pour une infinité de solutions appartenant à S_h, l'ordre des trois nombres $|\sigma(a)^x|$, $|\sigma(b)^y|$, $|\sigma(c)^z|$ est le même. Supposons que ce soit

$$|\sigma(a)^x| \geq |\sigma(b)^y| \geq |\sigma(c)^z|\ . \tag{5}$$

Considérons alors

$$\zeta = \sigma(c)^z/\sigma(b)^y\ .$$

Ce nombre est un entier de module inférieur à 1. Etudions ses conjugués. Pour tout $\tau \in \Gamma_1$ on a, en vertu du lemme,

$$\frac{\log|\tau(a)|}{\log|\tau(b)|} = \frac{\log|\sigma(a)|}{\log|\sigma(b)|}\ ,\quad \frac{\log|\tau(a)|}{\log|\tau(c)|} = \frac{\log|\sigma(a)|}{\log|\sigma(c)|} \tag{6}$$

donc

$$|\tau(a)^x| \geq |\tau(b)^y| \geq |\tau(c)^z|$$

et

$$|\tau(\zeta)| \leq 1\ .$$

Pour $\tau \in \Gamma_2$ $\qquad |\tau(\zeta)| = 1\ .$

Pour $\tau \in \Gamma_3$ on déduit, au contraire, de (6) :

$$|\tau(a)^x| \leq |\tau(b)^y| \leq |\tau(c)^z| \quad ;$$

mais $\tau(a)$, $\tau(b)$, $\tau(c)$ vérifient

$$\tau(\lambda)\tau(a)^x\tau(b)^{-y} + \tau(\mu) + \tau(\nu)\tau(\zeta) = 0$$

et comme $|\tau(a)^x\tau(b)^{-y}| < 1$ et $\tau(\nu) \neq 0$, il résulte de cette égalité que $\tau(\zeta)$ est borné. Pour h suffisamment grand les solutions de la sous-suite satisfaisant à (5) sont donc telles que ζ et tous ses conjugués appartiennent à un compact. Il en résulte, en raisonnant comme lors de la démonstration du théorème I, que ζ ne peut prendre qu'un nombre fini de valeurs et on en déduit la dépendance multiplicative de b et c , donc la contradiction cherchée.

-:-:-:-

BIBLIOGRAPHIE

[1] E.G. STRAUS - Symposium on number theory - Stony Brook. Juillet 1969. Problems section.

[2] G. REVUZ - Comptes rendus, 274, série A, 1972, p. 141.

[3] H.G. SENGE et E.G. STRAUS - Proceedings Washington state conference on number theory - Pulmann Washington, 1971, pp. 55-67.

[4] R. SALEM - Algebraic numbers and Fourier Analysis, Heath, 1963, p. 62.

[5] GELFOND - Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier. Mat. Sbornik, nouvelle série, t. 7, 1940, p. 7-25. Résultat cité par SCHNEIDER dans "Einführung in die Transzendenten Zahlen", p. 110.

[6] GELFOND - Transcendental and algebraic numbers. Th. 3, p. 28 de la traduction ~~anglaise~~. Dover Pub., 1960.

-:-:-:-

Département de Mathématiques,
Université de Poitiers,
40, avenue du Recteur Pineau,
86022 POITIERS