Indépendance algébrique et exponentielles en plusieurs variables

Michel WALDSCHMIDT

Résumé. On montre que certains corps engendrés sur $\mathbb{Q}$ par des nombres de la forme $\exp\langle x,y\rangle$, avec $x\in\mathbb{C}^n$ et $y\in\mathbb{C}^n$, ont un grand degré de transcendance.

§1. Introduction.

Soit n un entier ≥ 1. Quand $X=\mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$ est un sous-groupe de type fini de $\mathbb{C}^n$, on note

$$\mu(X)=\min_W(\mathrm{rang}_{\mathbb{Z}}\, X/X\cap W)/\dim_{\mathbb{C}}\mathbb{C}^n/W$$

quand W décrit les sous-espaces vectoriels de $\mathbb{C}^n$ sur $\mathbb{C}$ avec $W\neq\mathbb{C}^n$. Ainsi $\mu(X)\leq d/n$, et pour $n=1$ on a $\mu(X)=\mathrm{rang}_{\mathbb{Z}}X$.

On considère deux sous-groupes $X=\mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$ et $Y=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$ de $\mathbb{C}^n$. On note $\langle\ ,\ \rangle$ le produit scalaire usuel dans $\mathbb{C}^n$, on désigne par K le corps obtenu en adjoignant à $\mathbb{Q}$ les ℓd nombres

$$\exp\langle x_i,y_j\rangle, \qquad (1\leq i\leq d,\ 1\leq j\leq \ell),$$

et par t le degré de transcendance de K sur $\mathbb{Q}$.

On sait déjà [Wal 1] :

<u>si</u> $\mu(X)\mu(Y)>\mu(X)+\mu(Y)$, <u>alors</u> $t\geq 1$
<u>si</u> $\mu(X)\mu(Y)\geq 2(\mu(X)+\mu(Y))$, <u>alors</u> $t\geq 2$.

Il semble raisonnable d'espérer démontrer, dans un avenir assez proche, que l'hypothèse $\mu(X)\mu(Y)>\mu(X)+\mu(Y)$ implique

$$t+1>\mu(X)\mu(Y)/(\mu(X)+\mu(Y)).$$

Il y a encore deux obstacles pour y arriver. Le premier vient du critère d'indépendance algébrique de [W-Z] : au lieu d'avoir l'exposant $t+1$

qu'on attend, on a seulement un exposant qui croît exponentiellement avec t. La solution de ce problème pourrait venir de la voie ouverte par Philippon [P2].

Le deuxième obstacle est de nature technique. Curieusement, dans tous les développements actuels de la méthode de Gel'fond (voir un aperçu historique dans [Wal 2]), pour obtenir de grands degrés de transcendance on est conduit à imposer une hypothèse d'approximation diophantienne. Pour simplifier nous demanderons une inégalité légèrement plus restrictive que celle dont nous avons vraiment besoin.

1.1. <u>Pour tout</u> $\varepsilon > 0$, <u>il existe</u> $H_0(\varepsilon) > 0$ <u>tel que si</u> $\lambda_1,\ldots,\lambda_d$, $h_1,\ldots,h_\ell$ <u>sont des entiers rationnels vérifiant</u>

$$\max(|\lambda_1|,\ldots,|\lambda_d|,|h_1|,\ldots,|h_\ell|) = H > H_0(\varepsilon)$$

<u>et</u>

$$\langle \sum_{i=1}^{d} \lambda_i x_i \, , \, \sum_{j=1}^{\ell} h_j y_j \rangle = \xi \neq 0 ,$$

<u>alors</u>

$$|\xi| > \exp(-H^\varepsilon) .$$

Sous cette hypothèse nous démontrerons :

THÉORÈME 1.2. <u>Si</u> $\mu(X)+\mu(Y) \neq 0$, <u>on a</u>

$$2^t \geqslant \mu(X)\mu(Y)/(\mu(X)+\mu(Y)) .$$

En utilisant des travaux récents de Zhu Yao Chen, on peut remplacer 2^t par $2^{t-2}(2+\sqrt{3})$ quand $t \geqslant 2$. En particulier quand $n=1$ cela améliore les résultats antérieurs de Chudnovsky [C], Warkentin [War], Philippon-Reyssat [P1,R], Endell [E1,E2] et Nesterenko [N].

Voici un autre corollaire qui fait intervenir plusieurs variables. Soit K un sous-corps de $\mathbb{C}$ de degré de transcendance $t \geqslant 0$ sur $\mathbb{Q}$, et soient α_{ij}, $(1 \leqslant i,j \leqslant m)$ m^2 éléments multiplicativement indépendants de K^*. On suppose que pour tout $\varepsilon > 0$ il existe $H_0(\varepsilon) > 0$ tel que pour tout $h_{ij} \in \mathbb{Z}$, $(1 \leqslant i , j \leqslant m)$ vérifiant

$$\max_{1 \leqslant i,j \leqslant m} |h_{ij}| = H \geqslant H_0(\varepsilon)$$

on ait

$$\left|1 - \prod_{i=1}^{m} \prod_{j=1}^{m} \alpha_{ij}^{h_{ij}}\right| > \exp(-H^\varepsilon) .$$

Pour $1 \leqslant i , j \leqslant m$ on choisit une détermination $\log \alpha_{ij}$ du logarithme de α_{ij}.

COROLLAIRE 1.3. <u>Le rang</u> r <u>de la matrice</u> $(\log \alpha_{ij})_{1\leq i,j\leq m}$ <u>vérifie</u>

$$r \geq m/2^{t+1} .$$

Dans le cas $t=0$ on retrouve un résultat de [Wal 1] §7. Le cas général se démontre de la même manière.

Il n'y a pas de difficulté à donner des analogues p-adiques de ces résultats.

Voici le plan de cet exposé. Au §2 on énonce un résultat plus précis que le théorème 1.2, en y remplaçant 2^t par un nombre $J(K)$ (vérifiant $J(K) \leq 2^t$ d'après le critère d'indépendance algébrique de [W-Z]). La définition de $J(K)$ nous amène à choisir une base de transcendance $\theta_1,\ldots,\theta_t$ de K sur $\mathbb{Q}$, et à lui faire subir des petites perturbations (§3). On montre au §4 comment intervient l'hypothèse technique (1.1). On introduit ensuite une fonction auxiliaire (§5) pour terminer la démonstration au §6.

Quelques mots sur la démonstration. On ne dispose pas, actuellement, de "lemme de petites valeurs" (analogue au théorème de Tijdeman) pour les polynômes exponentiels en plusieurs variables. Pour cette raison les méthodes développées dans [C,E1,E2,N,P1,R,War] ne s'appliquent pas immédiatement ici. On pourrait en revanche utiliser la méthode de Masser et Wüstholz dans [M-W], mais le résultat serait légèrement moins précis que notre théorème 1.2.

Nous utiliserons ici un mélange de ces différentes méthodes, faisant intervenir à la fois un critère d'indépendance algébrique, et un lemme de zéros sous une forme raffinée due à Masser et Wüstholz [M-W]. Notre démonstration permet de travailler avec un groupe algébrique commutatif G quelconque (au lieu de $\mathbb{G}_m^d$). Nous indiquerons (sans démonstration) un résultat dans cette direction au §7.

§2. <u>Le critère d'indépendance algébrique et le coefficient</u> J .

Quand $P \in \mathbb{C}[X_1,\ldots,X_n]$ est un polynôme non nul en n variables à coefficients complexes, on note $H(P)$ sa hauteur (maximum des modules de ses coefficients), $d(P)$ le maximum de ses degrés partiels, et $t(P)$ la taille de P :

$$t(P) = \max(\log H(P), 1+d(P)) .$$

Soient $\theta_1,\ldots,\theta_t$ des nombres complexes, $t \geq 1$. On désigne par $A(\theta_1,\ldots,\theta_t)$ l'ensemble des nombres réels $\eta \geq 1$ ayant la propriété suivante : il existe une constante $T_0 > 0$ telle que pour tout $T \geq T_0$

et tout $(\tilde{\theta}_1,\dots,\tilde{\theta}_t) \in \mathbb{C}^t$ vérifiant

$$\max_{1\leq i\leq t} |\theta_i-\tilde{\theta}_i| < \exp(-2T^{\eta}) ,$$

il existe un polynôme $P\in \mathbb{Z}[X_1,\dots,X_t]$ de taille $\leq T$ avec

$$0 < |P(\tilde{\theta}_1,\dots,\tilde{\theta}_t)| < \exp(-T^{\eta}) .$$

Si l'ensemble $A(\theta_1,\dots,\theta_t)$ est vide, on pose $J(\theta_1,\dots,\theta_t) = 1$. S'il n'est pas vide, on désigne par $J(\theta_1,\dots,\theta_t)$ sa borne supérieure.

Quand K est un sous-corps de $\mathbb{C}$ de degré de transcendance $t\geq 1$ sur $\mathbb{Q}$, on note $J(K)$ la borne supérieure des nombres $J(\theta_1,\dots,\theta_t)$, quand $(\theta_1,\dots,\theta_t)$ décrit les bases de transcendance de K sur $\mathbb{Q}$. Du théorème de [W-Z] on déduit

$$J(K) \leq 2^t .$$

Le théorème 1.2 est donc une conséquence de l'énoncé suivant

THÉORÈME 2.1. Soient $x_1,\dots,x_d,y_1,\dots,y_\ell$ des éléments de $\mathbb{C}^n$ vérifiant l'hypothèse (1.1), et tels que les sous-groupes $X = \mathbb{Z}x_1+\dots+\mathbb{Z}x_d$ et $Y = \mathbb{Z}y_1+\dots+\mathbb{Z}y_\ell$ satisfassent $\mu(X)+\mu(Y) \neq 0$. Soit K un sous-corps de $\mathbb{C}$, de degré de transcendance fini sur $\mathbb{Q}$, contenant les ℓd nombres

$$\exp \langle x_i,y_j\rangle , \qquad (1\leq i\leq d , 1\leq j\leq \ell).$$

Alors

$$J(K) \geq \mu(X)\mu(Y)/(\mu(X)+\mu(Y)) .$$

Les méthodes développées par R. Endell dans [E2] pourraient conduire à une inégalité stricte, au moins dans le cas $n=1$.

Le théorème 2.1 contient plus d'information que le théorème 1.2. Par exemple quand on suppose $\mu(X)\mu(Y) > \mu(X)+\mu(Y)$ l'inégalité $J(K) > 1$ que l'on déduit du théorème 2.1 se traduit par un résultat d'approximation simultanée des ℓd nombres $\exp \langle x_i,y_j\rangle$ par des nombres algébriques (cf. [W-Z] lemme 4.1).

§3. Petites perturbations.

On considère une extension K de $\mathbb{Q}$ de type fini, et une base de transcendance $\theta_1,\dots,\theta_t$ de K sur $\mathbb{Q}$. Soit $\theta_{t+1}\in K$ tel que $K = \mathbb{Q}(\theta_1,\dots,\theta_{t+1})$, et soit $B\in\mathbb{Q}(\theta_1,\dots,\theta_t)[X]$ le polynôme irréductible unitaire de θ_{t+1} sur $\mathbb{Q}(\theta_1,\dots,\theta_t)$. Quitte à multiplier θ_{t+1} par un élément non nul de l'anneau $A_o = \mathbb{Z}[\theta_1,\dots,\theta_t]$ (un "dénominateur" commun des coefficients de B), on peut supposer de plus $B \in A_o[X]$. Pour utiliser la définition de J (§2), on est amené à considérer des éléments $\tilde{\theta}_1,\dots,\tilde{\theta}_t$ de $\mathbb{C}$, proches respectivement de $\theta_1,\dots,\theta_t$:

$$\max_{1\leqslant i\leqslant t} |\theta_i-\tilde{\theta}_i| < \varepsilon .$$

Pour $\varepsilon > 0$ suffisamment petit (dépendant de $\theta_1,\dots,\theta_{t+1}$), le polynôme unitaire $B(\tilde{\theta}_1,\dots,\tilde{\theta}_t,X) \in \mathbb{C}[X]$ a exactement une racine $\tilde{\theta}_{t+1}$ à distance minimale de θ_{t+1}, cette racine est simple, et

$$|\theta_{t+1}-\tilde{\theta}_{t+1}| \leqslant c\varepsilon$$

où c ne dépend que de $\theta_1,\dots,\theta_{t+1}$. On peut le voir par exemple en considérant le semi-résultant du polynôme $B(\tilde{\theta}_1,\dots,\tilde{\theta}_t,X)$ avec lui-même (cf. [R] lemme 3.7). On note $\tilde{K}$ le corps $\mathbb{Q}(\tilde{\theta}_1,\dots,\tilde{\theta}_{t+1})$.

Prenons maintenant $x_1,\dots,x_d$, $y_1,\dots,y_\ell$ dans $\mathbb{C}^n$ tels que les nombres $\gamma_{ij} = \exp\langle x_i,y_j\rangle$, $(1\leqslant i\leqslant d$, $1\leqslant j\leqslant \ell)$ appartiennent tous à K^*. On écrit ces nombres comme des fractions rationnelles en $\theta_1,\dots,\theta_{t+1}$:

$$\gamma_{ij} = \frac{a_{ij}}{b_{ij}}(\theta_1,\dots,\theta_{t+1}), \qquad (1\leqslant i\leqslant d,\ 1\leqslant j\leqslant \ell)$$

où a_{ij} et b_{ij} sont des éléments de $\mathbb{Z}[X_1,\dots,X_{t+1}]$, non nuls au point $\theta_1,\dots,\theta_{t+1}$. Pour ε suffisamment petit (dépendant de $\theta_1,\dots,\theta_{t+1}$, et des a_{ij} et b_{ij}) les nombres $a_{ij}(\tilde{\theta}_1,\dots,\tilde{\theta}_{t+1})$ et $b_{ij}(\tilde{\theta}_1,\dots,\tilde{\theta}_{t+1})$ sont tous différents de 0, et on peut définir

$$\tilde{\gamma}_{ij} = \frac{a_{ij}}{b_{ij}}(\tilde{\theta}_1,\dots,\tilde{\theta}_{t+1}) \in \tilde{K}^*, \qquad (1\leqslant i\leqslant d,\ 1\leqslant j\leqslant \ell) .$$

On pose ensuite $\tilde{\gamma}_j = (\tilde{\gamma}_{1j},\dots,\tilde{\gamma}_{dj}) \in \tilde{K}^{*d}$, $(1\leqslant j\leqslant \ell)$.

Quand E est un sous-ensemble fini de $\mathbb{C}^{*d}$, on note $\omega(E)$ le plus petit des degrés des polynômes non nuls de $\mathbb{C}[X_1,\dots,X_d]$ qui s'annulent sur E (il s'agit du degré total).

Au paragraphe 6 on démontrera le résultat suivant.

PROPOSITION 3.1. _On suppose qu'il existe_ $S_o > 0$ _tel que pour tout_ $S \geqslant S_o$ _et pour tout_ $(\tilde{\theta}_1,\dots,\tilde{\theta}_t) \in \mathbb{C}^t$ _vérifiant_

$$\max_{1\leqslant i\leqslant t} |\theta_i-\tilde{\theta}_i| \leqslant \exp(-S) ,$$

le sous-ensemble $\tilde{\Gamma}(S)$ _de_ $\mathbb{C}^{*d}$ _formé des éléments_

$$\tilde{\gamma}_1^{h_1}\cdots\tilde{\gamma}_\ell^{h_\ell} = \left(\prod_{j=1}^{\ell} \tilde{\gamma}_{1j}^{h_j},\ldots,\prod_{j=1}^{\ell} \tilde{\gamma}_{dj}^{h_j}\right) , \quad (h_1,\ldots,h_\ell)\in\mathbb{Z}^\ell , \quad 0 \leqslant h_j \leqslant S$$

<u>vérifie</u>

$$(3.2) \qquad \omega(\tilde{\Gamma}(S)) \geqslant (S/d)^{\ell/d} .$$

<u>Si</u> $X = \mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$ <u>et</u> $Y = \mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$ <u>satisfont</u> $\mu(X)=d/n$ <u>et</u> $\mu(Y)=\ell/n$, <u>alors</u>

$$J(\theta_1,\ldots,\theta_t) \geqslant \ell d/n(\ell+d) .$$

Au paragraphe suivant on montre que la proposition 3.1 implique le théorème 2.1.

§4. <u>Utilisation de l'hypothèse technique</u> (1.1).

Montrons d'abord qu'il n'y a pas de restriction, pour le théorème 2.1, à supposer $\mu(X)=d/n$ et $\mu(Y)=\ell/n$. On se ramène déjà au cas où $\operatorname{rang}_{\mathbb{Z}} X = d$ et $\operatorname{rang}_{\mathbb{Z}} Y = \ell$, de manière évidente. On utilise ensuite le lemme 5.2 de [Wal 1] : il existe $n' \geqslant 1$, $X' \subseteq \mathbb{C}^{n'}$ et $Y' \subseteq \mathbb{C}^{n'}$, avec $\operatorname{rang}_{\mathbb{Z}} X' = d'$, $\operatorname{rang}_{\mathbb{Z}} Y' = \ell'$, $\mu(X') = d'/n' \geqslant \mu(X)$, $\mu(Y') = \ell'/n' \geqslant \mu(Y)$, et $\langle X',Y'\rangle \subseteq \langle X,Y\rangle$. Alors

$$\ell'd'/n'(\ell'+d') \geqslant \mu(X)\mu(Y)/(\mu(X)+\mu(Y)) ,$$

et l'hypothèse (1.1) pour X et Y implique la même hypothèse pour X' et Y'. Ainsi, quitte à remplacer X et Y par X' et Y', on peut supposer $\mu(X)=d/n$ et $\mu(Y)=\ell/n$.

Pour déduire le théorème 2.1 de la proposition 3.1, il ne reste plus qu'à vérifier l'hypothèse (3.2) en utilisant (1.1). C'est l'objet du lemme suivant.

LEMME 4.1. <u>Soient</u> $x_1,\ldots,x_d$, $y_1,\ldots,y_\ell$ <u>des éléments de</u> $\mathbb{C}^n$ <u>vérifiant la condition</u> (1.1), <u>avec</u> $\ell d \geqslant n(\ell+d)$ <u>et tels que</u> $X = \mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$ <u>et</u> $Y = \mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$ <u>satisfassent</u> $\mu(X)=d/n$ <u>et</u> $\mu(Y)=\ell/n$. <u>Soit</u> $\varepsilon > 0$. <u>Il existe</u> $S_0(\varepsilon) > 0$ <u>tel que pour tout</u> $S \geqslant S_0(\varepsilon)$ <u>et pour tout</u> $z_{ij}\in\mathbb{C}$, $(1 \leqslant i \leqslant d$, $1 \leqslant j \leqslant \ell)$ <u>avec</u>

$$\max_{i,j} |z_{ij} - \langle x_i,y_j\rangle| < \exp(-S^\varepsilon) ,$$

<u>l'ensemble</u>

$$E = \left\{\left(\prod_{j=1}^{\ell} e^{h_j z_{1j}},\ldots,\prod_{j=1}^{\ell} e^{h_j z_{dj}}\right)\in\mathbb{C}^{\times d} ; (h_1,\ldots,h_\ell)\in\mathbb{Z}^\ell , 0 \leqslant h_j \leqslant S\right\}$$

<u>vérifie</u>

$$\omega(E) \geq (S/d)^{\ell/d} .$$

Démonstration du lemme 4.1.

Supposons que la conclusion ne soit pas vérifiée. D'un lemme de zéros de Masser [M] on déduit qu'il existe deux entiers r et k vérifiant $1 \leq r \leq d$, $1 \leq k \leq \ell$, $\ell r+kd > \ell d$, il existe des éléments $\lambda^{(1)},\ldots,\lambda^{(r)}$ de $\mathbb{Z}^d$, linéairement indépendants sur $\mathbb{Z}$, avec $\lambda^{(\rho)} = (\lambda_1^{(\rho)},\ldots,\lambda_d^{(\rho)})$, $(1 \leq \rho \leq r)$, et enfin des éléments $h^{(1)},\ldots,h^{(k)}$ de $\mathbb{Z}^\ell$, linéairement indépendants sur $\mathbb{Z}$, avec $h^{(\varkappa)} = (h_1^{(\varkappa)},\ldots,h_\ell^{(\varkappa)})$, $(1 \leq \varkappa \leq k)$, vérifiant

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} e^{\lambda_i^{(\rho)} h_j^{(\varkappa)} z_{ij}} = 1 , \qquad (1 \leq \rho \leq r \ , \ 1 \leq \varkappa \leq k).$$

De plus, le raffinement de ce résultat donné par Masser et Wüstholz dans [M-W] permet de choisir ces $\lambda^{(\rho)}$ et ces $h^{(\varkappa)}$ de telle sorte que

$$\max_{1\leq i\leq d} |\lambda_i^{(\rho)}| \leq (S/d)^{\ell\rho/d} \quad , \quad \max_{1\leq j\leq \ell} |h_j^{(\varkappa)}| \leq (S/d)^{\ell r/d}$$

pour $1 \leq \rho \leq r$, $1 \leq \varkappa \leq k$.

Pour $1 \leq \rho \leq r$ et $1 \leq \varkappa \leq k$, notons

$$x'_\rho = \sum_{i=1}^{d} \lambda_i^{(\rho)} x_i \quad , \quad y'_\varkappa = \sum_{j=1}^{\ell} h_j^{(\varkappa)} y_j \ ,$$

et

$$m_{\rho,\varkappa} = \frac{1}{2i\pi} \sum_{i=1}^{d} \sum_{j=1}^{\ell} \lambda_i^{(\rho)} h_j^{(\varkappa)} z_{ij} .$$

Ainsi $m_{\rho,\varkappa} \in \mathbb{Z}$, et $|m_{\rho,\varkappa}| \leq S^{2\ell}$ pour $S \geq S_0(\varepsilon)$ suffisamment grand. Soit s le rang de la matrice $(m_{\rho,\varkappa})_{1\leq\rho\leq r, 1\leq\varkappa\leq k}$. On suppose que la numérotation des $\lambda^{(\rho)}$ et des $h^{(\varkappa)}$ a été choisie de telle sorte que le déterminant de la matrice $(m_{\rho,\varkappa})_{1\leq\rho,\varkappa\leq s}$ ne soit pas nul.

Il existe des entiers rationnels $a_{\sigma,\varkappa}$, $(0 \leq \sigma \leq s \ , \ 1 \leq \varkappa \leq k)$ avec $a_{0,\varkappa} \neq 0$, $(1 \leq \varkappa \leq k)$, et

$$a_{0,\varkappa} m_{\rho,\varkappa} = \sum_{\sigma=1}^{s} a_{\sigma,\varkappa} m_{\rho,\sigma} \ , \qquad (1 \leq \rho \leq r \ , \ 1 \leq \varkappa \leq k).$$

On peut choisir pour $a_{\sigma,\varkappa}$ des mineurs de la matrice $(m_{\rho,\varkappa})_{1\leq\rho\leq r, 1\leq\varkappa\leq k}$, donc

$$|a_{\sigma,\varkappa}| \leq s! \ S^{2\ell s} \leq d! \ S^{2\ell d} ,$$

pour $0 \leq \sigma \leq s$, $1 \leq \varkappa \leq k$. Pour $\sigma < \varkappa \leq k$, on définit

$$y''_\varkappa = a_{o\varkappa}\, y'_\varkappa - \sum_{\sigma=1}^{s} a_{\sigma,\varkappa}\, y'_\sigma .$$

Ainsi pour $1 \leqslant \rho \leqslant r$ et $s < \varkappa \leqslant k$ on a

$$\langle x'_\rho, y''_\varkappa\rangle = a_{o\varkappa}\, \langle x'_\rho, y'_j\rangle - \sum_{\sigma=1}^{s} a_{\sigma\varkappa}\, \langle x'_\rho, y'_\sigma\rangle ,$$

donc

$$|\langle x'_\rho, y''_\varkappa\rangle| < \exp(-\tfrac{1}{2}S^\varepsilon) .$$

L'hypothèse (1.1) implique alors $\langle x'_\rho, y''_\varkappa\rangle = 0$, pour $1 \leqslant \rho \leqslant r$, $s < \varkappa \leqslant k$. On termine la démonstration comme celle du lemme 5.4 de [Wal 1] pour obtenir une contradiction.

§5. La fonction auxiliaire.

Soient d et n deux entiers, $d > n \geqslant 1$, $x_1,\dots,x_d$ des éléments de $\mathbb{C}^n$, c_o un nombre réel suffisamment grand, T_o un nombre réel encore plus grand. Pour chaque $T \geqslant T_o$ on définit N , S , D , U par

$$T = N^{\ell+d} \ , \ S = N^d \ , \ D = c_o^{-1} N^\ell \ , \ U^{n+1} c_o^{d+2} = N^{\ell d+\ell+d} .$$

Enfin soit $V \geqslant 25\, c_o\, T$.

Pour $t = (t_1,\dots,t_n) \in \mathbb{C}^n$ on note $|t| = \max_{1\leqslant i\leqslant n} |t_i|$.

PROPOSITION 5.1. <u>Il existe un polynôme non nul</u> $F \in \mathbb{Z}[X_1,\dots,X_d]$ <u>de degré</u> $\leqslant D$ <u>en chaque</u> X_i <u>et de taille</u> $\leqslant c_o^{-1}\, T$, <u>tel que la fonction</u>

$$\Phi(z_1,\dots,z_d) = F(e^{z_1},\dots,e^{z_d})$$

<u>vérifie la propriété suivante</u> : <u>pour tout</u> $z = (z_1,\dots,z_d) \in \mathbb{C}^d$ <u>tel qu'il existe</u> $t = (t_1,\dots,t_n) \in \mathbb{C}^n$ <u>avec</u>

$$|t| \leqslant c_o\, S \ , \ \underline{\text{et}} \ \max_{1\leqslant i\leqslant d} |z_i - \langle x_i, t\rangle| \leqslant e^{-V} ,$$

<u>on a</u>

$$|\Phi(z)| \leqslant e^{-U} + e^{-\frac{23}{24}V} .$$

<u>Démonstration</u>.

On construit le polynôme F de telle sorte que la fonction

$$\psi(t) = \Phi(\langle x_1, t\rangle,\dots,\langle x_d, t\rangle)$$

satisfasse

$$|\psi(t)| \leqslant e^{-U}$$

pour tout $t \in \mathbb{C}^n$ vérifiant $|t| \leqslant c_o S$. Il suffit d'appliquer le théorème 3.1 de [Wal 1] aux fonctions

$$\exp \langle \sum_{i=1}^{d} \lambda_i x_i , t \rangle , \qquad (0 \leqslant \lambda_i \leqslant D),$$

avec $L = ([D]+1)^d$, $r = c_o S$, $R = er$ (le paramètre noté S dans [Wal 1] §3 est ici $c_o^{-1} T$).

Maintenant soit $t \in \mathbb{C}^n$, avec $|t| \leqslant c_o S$, et soit $z = (z_1,\ldots,z_d) \in \mathbb{C}^d$ avec

$$\max_{1 \leqslant i \leqslant d} |z_i - \langle x_i , t \rangle| \leqslant e^{-V} .$$

On va vérifier

$$|\Phi(z) - \psi(t)| \leqslant e^{-\frac{23}{24}V} .$$

On écrit

$$F(X_1,\ldots,X_d) = \sum_{\lambda} p_\lambda \prod_{i=1}^{d} X_i^{\lambda_i} ,$$

avec $\lambda = (\lambda_1,\ldots,\lambda_d)$, $0 \leqslant \lambda_i \leqslant D$. Alors

$$\Phi(z) - \psi(t) = \sum_{\lambda} p_\lambda \, (e^{u_\lambda} - e^{v_\lambda})$$

où

$$u_\lambda = \sum_{i=1}^{d} \lambda_i z_i \quad , \quad v_\lambda = \langle \sum_{i=1}^{d} \lambda_i x_i , t \rangle .$$

Mais pour u et v dans $\mathbb{C}$ on a

$$|e^u - e^v| \leqslant |e^v| . e^{|u-v|} . |u-v| .$$

D'où

$$|\Phi(z) - \psi(t)| \leqslant L . e^{c_o T} . e^{-V} \leqslant e^{-\frac{23}{24}V} .$$

§6. <u>Fin de la démonstration de la proposition</u> 5.1.

On va d'abord montrer, sous les hypothèses de la proposition 3.1, l'inégalité :

(6.1) $$J(\theta_1,\ldots,\theta_t) \geqslant (\ell d+\ell+d)/(n+1)(\ell+d) .$$

Comme $J(\theta_1,\ldots,\theta_t) \geq 1$, cela revient à choisir un nombre réel η vérifiant

$$1 \leq \eta < (\ell d+\ell+d)/(n+1)(\ell+d)$$

puis à construire, pour chaque $T \geq T_o$ et chaque $(\tilde{\theta}_1,\ldots,\tilde{\theta}_t) \in \mathbb{C}^t$ vérifiant

$$\max_{1\leq i\leq t} |\theta_i-\tilde{\theta}_i| < \exp(-2T^\eta) ,$$

un polynôme non nul $P \in \mathbb{Z}[X_1,\ldots,X_t]$ de taille $\leq T$ tel que

$$0 < |P(\tilde{\theta}_1,\ldots,\tilde{\theta}_t)| < \exp(-T^\eta) .$$

Posons $\varepsilon = 1/14$. On commence par choisir comme au §3 la racine $\tilde{\theta}_{t+1}$ de $B(\tilde{\theta}_1,\ldots,\tilde{\theta}_t,X)$ qui vérifie

$$|\theta_{t+1}-\tilde{\theta}_{t+1}| < \exp(-(2-\varepsilon)T^\eta) ,$$

et à en déduire $\tilde{\gamma}_{ij} \in \tilde{K}^\times$ avec

$$|\tilde{\gamma}_{ij}-\gamma_{ij}| < \exp(-(2-2\varepsilon)T^\eta) .$$

Reprenons le polynôme $F \in \mathbb{Z}[X_1,\ldots,X_d]$ construit à la proposition 5.1. L'hypothèse (3.2) montre qu'il existe $(h_1,\ldots,h_\ell) \in \mathbb{Z}^\ell$, $0 \leq h_j \leq S$, tel que le nombre

$$\xi = F(\tilde{\gamma}_1^{h_1}\ldots\tilde{\gamma}_\ell^{h_\ell})$$

ne soit pas nul. On choisit $z_{ij} \in \mathbb{C}$, $(1 \leq i \leq d , 1 \leq j \leq \ell)$ vérifiant $\exp z_{ij} = \tilde{\gamma}_{ij}$ et

$$|z_{ij} - \langle x_i,y_j\rangle| \leq \exp(-(2-3\varepsilon)T^\eta) .$$

Ainsi en posant

$$z_i = \sum_{j=1}^{\ell} h_j z_{ij} , \quad (1 \leq i \leq d) , \quad z = (z_1,\ldots,z_d), \ t = \sum_{j=1}^{\ell} h_j y_j ,$$

on trouve $\xi = \Phi(z)$, et

$$|t| \leq c_o S \quad \text{et} \quad \max_{1\leq i\leq d} |z_i - \langle x_i,t\rangle| \leq \exp(-(2-4\varepsilon)T^\eta) .$$

La proposition 5.1, avec $V = (2-4\varepsilon)T^\eta$, implique

$$0 < |\xi| < \exp(-(2-5\varepsilon)T^\eta) .$$

On définit $Q \in \mathbb{Z}[X_1,\ldots,X_{t+1}]$ par

$$Q = \sum_{\lambda} p_{\lambda} \prod_{i=1}^{d} \prod_{j=1}^{\ell} a_{ij}^{\lambda_i h_j} b_{ij}^{[D][S]-\lambda_i h_j} .$$

Ainsi

$$Q(\tilde{\theta}_1,\ldots,\tilde{\theta}_{t+1}) = \xi \prod_{i=1}^{d} \prod_{j=1}^{\ell} b_{ij}(\tilde{\theta}_1,\ldots,\tilde{\theta}_{t+1})^{[D][S]} ,$$

et donc

$$0 < |Q(\tilde{\theta}_1,\ldots,\tilde{\theta}_{t+1})| \leqslant \exp(-(2-6\varepsilon)T^{\eta}) .$$

D'autre part

$$t(Q) \leqslant c_o^{1/2} DS = T/c_o^{1/2} .$$

Posons $R(X) = Q(\tilde{\theta}_1,\ldots,\tilde{\theta}_t,X)$. Si le polynôme R est constant, on prend $P(X_1,\ldots,X_t) = Q(X_1,\ldots,X_t,0)$. Si $\deg R \geqslant 1$, on considère le semi-résultant de $R(X)$ et de $B(\tilde{\theta}_1,\ldots,\tilde{\theta}_t,X)$; on trouve ainsi (cf. [W-Z] lemmes 2.3 et 2.4) un polynôme non nul $P \in \mathbb{Z}[X_1,\ldots,X_t]$, vérifiant $t(P) \leqslant T$ et

$$0 < |P(\tilde{\theta}_1,\ldots,\tilde{\theta}_t)| \leqslant \exp(-(2-7\varepsilon)T^{\eta}) .$$

On en déduit (6.1).

Pour terminer la démonstration de la proposition 3.1 on utilise l'astuce de Landau-Philippon [P1] : on applique (6.1) aux sous-groupes X^k et Y^k de $(\mathbb{C}^n)^k$ pour k entier positif. L'hypothèse (3.2) étant stable par puissance cartésienne, on trouve

$$J(\theta_1,\ldots,\theta_t) \geqslant (k\ell d+\ell+d)/(kn+1)(\ell+d) ,$$

puis on fait tendre k vers l'infini.

§7. Compléments.

La démonstration que nous venons de présenter permet d'étudier, plus généralement, les sous-groupes à n paramètres de groupes algébriques définis sur une extension de $\mathbb{Q}$ de type fini. Nous nous contenterons, ici, de donner une généralisation en plusieurs variables du théorème principal de [M-W].

Soit $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3, n'ayant pas de multiplication complexe, et soient $X = \mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$ et $Y = \mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$ deux sous-groupes de type fini de $\mathbb{C}^n$ vérifiant la condition technique (1.1). Soit K le sous-corps de $\mathbb{C}$ obtenu en adjoignant à $\mathbb{Q}$ les nombres g_2, g_3, et les valeurs de $\wp$

aux points $\langle x_i, y_j \rangle$, $(1 \leqslant i \leqslant d$, $1 \leqslant j \leqslant \ell)$ qui ne sont pas pôles de P. Enfin soit t le degré de transcendance de K sur $\mathbb{Q}$.

THÉORÈME 7.1. <u>Si</u> $\mu(X)+\mu(Y) \neq 0$, <u>alors</u>

$$2^t \geqslant \mu(X)\mu(Y)/(2\mu(X)+\mu(Y)) .$$

Bibliographie

[C] G.V. ČUDNOVSKII.- Some analytic methods in the theory of transcendental numbers. Inst. Math., Ukr S.S.R. Acad. Sci., Preprints IM 74-8 et 74-9, Kiev 1974.

[E1] R. ENDELL.- Zur algebraischen Unabhängigkeit gewisser Werte der Exponentialfunktion (nach Chudnovsky). Diplomarbeit, Düsseldorf, 1981.

[E2] R. ENDELL.- Zur algebraischen Unabhängigkeit gewisser Werte der Exponentialfunktion, 1983, Noordwijkerhout, même volume.

[M] D.W. MASSER.- On polynomials and exponential polynomials in several complex variables. Invent. Math., 63 (1981), 81-95.

[M-W] D.W. MASSER and G. WÜSTHOLZ.- Fields of large transcendence degree generated by values of elliptic functions. Invent. Math., 72 (1983), 407-464.

[N] Ju.V. NESTERENKO.- On the algebraical independence of algebraic numbers to algebraic powers, in : "Approximations diophantiennes et nombres transcendants". Luminy 1982, Progress in Math. 31, Birkhäuser (1983), 199-220.

[P1] P. PHILIPPON.- Indépendance algébrique des valeurs de fonctions exponentielles p-adiques. J. reine angew. Math., 329 (1981), 42-51.

[P2] P. PHILIPPON.- Pour une théorie de l'indépendance algébrique. Thèse, Orsay, 1983 (à paraître).

[R] E. REYSSAT.- Un critère d'indépendance algébrique. J. reine angew. Math., 329 (1981), 66-81.

[Wal 1] M. WALDSCHMIDT.- Transcendance et exponentielles en plusieurs variables. Invent. Math., 63 (1981), 97-127.

[Wal 2] M. WALDSCHMIDT.- Algebraic independence of transcendental numbers. Gel'fond's method and its developments, à paraître.

[W-Z] M. WALDSCHMIDT et ZHU Yao Chen.- Une généralisation en plusieurs variables d'un critère de transcendance de Gel'fond, C. R. Acad. Sc. Paris, Ser. I, 297 (1983), 229-232.

[War] P. WARKENTIN.- Algebraische Unabhängigkeit gewisser p-adischer Zahlen. Diplomarbeit, Freiburg i. Br., 1978.

Michel WALDSCHMIDT
Institut Henri Poincaré
11, rue Pierre et Marie Curie
75231 PARIS CEDEX 05