Transcendance et exponentielles en plusieurs variables.

Waldschmidt, Michel

pp. 97 - 128

Invent. math. 63, 97–127 (1981)

Inventiones mathematicae

Transcendance et exponentielles en plusieurs variables

Michel Waldschmidt

Institut Henri Poincaré, 11, rue Pierre et Marie Curie,
F-75231 Paris Cedex 05, France

On considère d fonctions exponentielles en n variables

$$\exp\langle x_i, z\rangle, \quad (1 \leqq i \leqq d),$$

algébriquement indépendantes, qui prennent des valeurs algébriques sur un sous-groupe Y de $\mathbb{C}^n$ de rang ℓ. Pour pouvoir appliquer les méthodes transcendantes, on suppose

$$\ell d > n(\ell + d).$$

On montre alors que «la plupart» des x_i se trouvent dans un sous-espace propre W de $\mathbb{C}^n$, et que «la plupart» des éléments de Y sont dans l'orthogonal de W.

Cet énoncé permet de répondre à une question de Weil consistant à déterminer les caractères du groupe des classes d'idèles d'un corps de nombres pour lesquels les coefficients de la série L de Hecke sont algébriques [8].

L'analogue p-adique de ce résultat fournit l'énoncé de transcendance sollicité par Serre [5] p. III.20 dans son étude sur les représentations p-adiques des groupes de Galois de corps de nombres; il permet aussi de montrer que le rang p-adique du groupe des unités d'un corps de nombres est au moins égal à la moitié du nombre de Dirichlet.

La démonstration utilise essentiellement deux outils; d'une part une construction d'une fonction auxiliaire inspirée d'un travail antérieur en collaboration avec Mignotte [3], d'autre part un théorème récent de Masser sur les zéros de polynômes exponentiels [2].

Voici le plan de ce travail. La première partie concerne le cas complexe, la seconde le cas p-adique. Dans chacune de ces parties, au § 1 on donne les énoncés sur les exponentielles, et au § 2 on formule ces résultats en terme de minoration du rang de matrices dont les coefficients sont des logarithmes de nombres algébriques. Au § 3 on construit la fonction auxiliaire, qui permet d'appliquer le théorème de Masser (§ 4). La démonstration des théorèmes (§ 6 de la première partie et § 5 de la deuxième) requiert une étude du coefficient de Dirichlet généralisé $\mu(\Gamma)$, et du coefficient $\chi(Y, X)$ introduit par Masser (§ 5 de la

0020-9910/81/0063/0097/$06.20

première partie). Quelques résultats complémentaires sont indiqués à la fin de la première partie: au § 7 on introduit un coefficient $\theta(M)$ relatif à une matrice M (ce coefficient est utilisé dans la deuxième partie), et au § 8 on indique sans démonstration un résultat d'indépendance algébrique.

Première partie: le cas complexe

§ 1. Généralisation à plusieurs variables du théorème des six exponentielles

Le théorème des six exponentielles, dû à Siegel, Lang et Ramachandra (cf. [1] Chap. 2, [7] Cor. 1.7), est l'énoncé suivant. Soient x_1, x_2 deux nombres complexes $\mathbb{Q}$-linéairement indépendants, et y_1, y_2, y_3 trois nombres complexes $\mathbb{Q}$-linéairement indépendants. Alors l'un au moins des six nombres

$$\exp(x_i y_j), \qquad (i=1,2;\ j=1,2,3)$$

est transcendant.

Pour généraliser ce résultat aux exponentielles en plusieurs variables, nous noterons, pour $u=(u_1,\ldots,u_n)$ et $v=(v_1,\ldots,v_n)$ dans $\mathbb{C}^n$,

$$\langle u, v\rangle = \sum_{k=1}^{n} u_k v_k.$$

Théorème 1.1. *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 $\mathbb{C}^n$ de rang d et ℓ respectivement, avec $\ell d > n(\ell+d)$. On suppose que les $d\ell$ nombres*

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

sont algébriques.

Alors on peut écrire

$$X = X_1 \oplus X_2, \qquad Y = Y_1 \oplus Y_2,$$

où X_1, X_2, Y_1, Y_2 sont des sous-groupes de $\mathbb{C}^n$, de rang d_1, d_2, ℓ_1, ℓ_2 respectivement, avec

$$\langle X_1, Y_2\rangle = 0,$$

et, en désignant par n_1 la dimension du $\mathbb{C}$-espace vectoriel engendré par X_1,

$$d_1/n_1 > d/n \quad \text{et} \quad \ell_1 d_1 \leqq n_1(\ell_1+d_1).$$

En choisissant $d=n+1$, nous en déduirons le corollaire suivant (cf. [6] problèmes *B* et *C*).

Corollaire 1.2. *Soient $\alpha_{\nu,\mu}$, $(1\leqq \nu\leqq n,\ 1\leqq \mu\leqq m)$ des nombres algébriques non nuls, avec $m\geqq n^2+n+1$, et $\log\alpha_{\nu,\mu}$ des déterminations de leurs logarithmes. Soient $t_1,\ldots,t_n$ des nombres complexes. On suppose que les m nombres*

$$\prod_{\nu=1}^{n} \alpha_{\nu,\mu}^{t_\nu} = \exp\left(\sum_{\nu=1}^{n} t_\nu \log\alpha_{\nu,\mu}\right), \qquad (1\leqq \mu\leqq m)$$

sont algébriques.

a) *Si les m éléments de* $\mathbb{C}^n$

$$(\log \alpha_{1,\mu}, \ldots, \log \alpha_{n,\mu}), \quad (1 \leqq \mu \leqq m)$$

sont $\mathbb{Q}$*-linéairement indépendants, alors les nombres* $1, t_1, \ldots, t_n$ *sont* $\mathbb{Q}$*-linéairement dépendants.*

b) *Si les mn nombres complexes*

$$\log \alpha_{v,\mu}, \quad (1 \leqq v \leqq n;\ 1 \leqq \mu \leqq m)$$

sont $\mathbb{Q}$*-linéairement indépendants, alors les nombres* $t_1, \ldots, t_n$ *sont tous rationnels.*

En voici une conséquence. Soit k un corps de nombres; notons k_v, $(1 \leqq v \leqq n)$ les complétés de k pour les valuations archimédiennes, avec $k_v = \mathbb{R}$ pour $1 \leqq v \leqq r_1$, $k_v = \mathbb{C}$ pour $r_1 < v \leqq r_1 + r_2$, $n = r_1 + r_2$, et $[k : \mathbb{Q}] = r_1 + 2r_2$. Pour $\alpha \in k$, on note α_v l'image de α dans k_v. Soit $\mathfrak{f}$ un idéal entier non nul de k; on note $k^*(\mathfrak{f})$ le sous-groupe de k^* formé des α_1/α_2, où α_1 et α_2 décrivent les entiers de k congrus à 1 modulo $\mathfrak{f}$.

Corollaire 1.3. *Soient* $t_1, \ldots, t_n$ *des nombres complexes.*

a) *Si, pour tout* $\alpha \in k^*(\mathfrak{f})$, *on a*

$$\prod_{v=1}^{n} |\alpha_v|^{t_v} \in \overline{\mathbb{Q}}$$

alors $t_v \in \mathbb{Q}$ *pour tout* $v = 1, \ldots, n$.

b) *S'il existe un corps de nombres K tel que*

$$\prod_{v=1}^{n} |\alpha_v|^{t_v} \in K$$

pour tout $\alpha \in k^*(\mathfrak{f})$, *alors* $t_v \in \mathbb{Z}$ *pour* $1 \leqq v \leqq r_1$ *et* $t_v \in 2\mathbb{Z}$ *pour* $r_1 < v \leqq n$.

Le corollaire 1.3 apporte une réponse à un problème de Weil [8] p. 4: soit χ un «Grössencharakter» d'un corps de nombres k; si les valeurs de χ (sur les idéaux premiers au conducteur) sont des nombres algébriques, alors χ est de type (A) au sens de Weil; si les valeurs de χ sont dans une extension finie de $\mathbb{Q}$, alors χ est de type (A_0). En particulier, si les valeurs de χ sont des racines de l'unité, alors χ est d'ordre fini. On en déduira le corollaire suivant.

Corollaire 1.4. *Soit k un corps de nombres. Il existe un sous-groupe de type fini de* k^* *dont l'image est dense dans* $(k \otimes_{\mathbb{Q}} \mathbb{R})^*$.

Dans le cas où l'extension $k/\mathbb{Q}$ est abélienne, cet énoncé a été démontré par H.W. Lenstra Jr par des moyens purement algébriques, et par J.-L. Brylinski à l'aide du théorème de Baker, en réponse à une question posée par J.-L. Colliot-Thélène, D. Coray et J.-J. Sansuc.

Le théorème 1.1 et le corollaire 1.4 sont démontrés au § 6. Pour la démonstration des corollaires 1.2 et 1.3, nous renvoyons à [6]. Dans un exposé au Séminaire de Théorie des Nombres Delange Pisot Poitou en 1980 (Progress in Math., Birkhäuser Verlag), nous déduisons directement le corollaire 1.3 du théorème 1.1 et nous explicitons l'application au problème de Weil.

§ 2. Minoration du rang de matrices dont les coefficients sont des logarithmes de nombres algébriques

Soit $M=(u_{i,j})_{1\leqq i\leqq d,\ 1\leqq j\leqq \ell}$ une matrice $d\times\ell$ à coefficients dans un corps K; soit n un entier positif; les deux propriétés suivantes sont équivalentes:

(i) le rang de M est inférieur ou égal à n

(ii) il existe $x_1,\ldots,x_d$, $y_1,\ldots,y_\ell$ dans K^n tels que

$$u_{i,j}=\langle x_i,y_j\rangle,\quad (1\leqq i\leqq d,\ 1\leqq j\leqq \ell).$$

Pour $n=1$ on constate ainsi que le théorème des six exponentielles peut s'énoncer de la manière suivante.

Soit

$$M=\begin{pmatrix}\log\alpha_1 & \log\alpha_2 & \log\alpha_3\\ \log\beta_1 & \log\beta_2 & \log\beta_3\end{pmatrix}$$

une matrice 2×3 dont les coefficients sont des logarithmes de nombres algébriques. On suppose que les trois éléments de la première ligne sont $\mathbb{Q}$-linéairement indépendants, ainsi que les deux éléments de la première colonne. Alors le rang de la matrice M est égal à 2.

De même, on peut énoncer le théorème 1.1 sous la forme suivante.

Théorème 2.1. *On considère une matrice* $d\times\ell$

$$M=\begin{pmatrix}\log\alpha_{1,1} & \ldots & \log\alpha_{1,\ell}\\ \ldots & \ldots & \ldots\\ \log\alpha_{d,1} & \ldots & \log\alpha_{d,\ell}\end{pmatrix}$$

dont les coefficients sont des logarithmes de nombres algébriques. On suppose que les vecteurs lignes de M *sont* $\mathbb{Q}$*-linéairement indépendants dans* $\mathbb{C}^\ell$, *et que les vecteurs colonnes de* M *sont* $\mathbb{Q}$*-linéairement indépendants dans* $\mathbb{C}^d$. *Soit* r *le rang de* M. *On suppose* $r<d\ell/(d+\ell)$.

Alors il existe deux matrices $P\in SL_d(\mathbb{Z})$ *et* $Q\in SL_\ell(\mathbb{Z})$ *telles que*

$$PMQ=\begin{pmatrix}M_1 & 0\\ * & M_2\end{pmatrix}$$

où M_1 *est une matrice* $d_1\times\ell_1$ *de rang* r_1 *avec*

$$d_1/r_1>d/r\quad et\quad \ell_1 d_1\leqq r_1(\ell_1+d_1).$$

Par exemple, si $M=(\log\alpha_{i,j})_{1\leqq i\leqq d,\ 1\leqq j\leqq\ell}$ est une matrice $d\times\ell$ dont les coefficients sont des logarithmes de nombres algébriques, et si les $d\ell$ nombres $\log\alpha_{i,j}$ $(1\leqq i\leqq d,\ 1\leqq j\leqq\ell)$ sont $\mathbb{Q}$-linéairement indépendants, alors le rang de M est supérieur ou égal à $\ell d/(\ell+d)$. En particulier, si $\ell\geqq d^2-d+1$, alors M est de rang d.

§ 3. Construction d'une fonction auxiliaire

Nous développons ici une remarque de [3] en construisant une fonction auxiliaire générale qui peut servir dans de nombreuses démonstrations de transcendance.

a) *Enoncés des résultats*
On choisit une norme $|.|$ dans $\mathbb{C}^n$; pour $R>0$, on note

$$B(0,R)=\{z\in\mathbb{C}^n;\ |z|\leqq R\}.$$

Quand f est une fonction complexe continue sur $B(0,R)$ on note

$$|f|_R=\sup\{|f(z)|;\ z\in B(0,R)\}.$$

Théorème 3.1. *Soient L et n deux entiers positifs, S, U, R, r des nombres réels positifs, et $\varphi_1,\ldots,\varphi_L$ des fonctions continues sur $B(0,R)$, analytiques à l'intérieur. On suppose*

$$3\leqq U,\ S\leqq U,\ e\leqq R/r\leqq e^U,\ \sum_{\lambda=1}^{L}|\varphi_\lambda|_R\leqq e^U,$$

et

$$(8U)^{n+1}\leqq LS\left(\operatorname{Log}\frac{R}{r}\right)^n.$$

Alors il existe des entiers rationnels $p_1,\ldots,p_L$, avec

$$0<\max_{1\leqq\lambda\leqq L}|p_\lambda|\leqq e^S,$$

tels que la fonction

$$F=\sum_{\lambda=1}^{L}p_\lambda\varphi_\lambda$$

vérifie

$$|F|_r\leqq e^{-U}.$$

Nous n'utiliserons ici que le corollaire suivant, obtenu en choisissant

$$\varphi_\lambda(z)=\exp\langle\lambda_1x_1+\ldots+\lambda_dx_d,z\rangle,\qquad(0\leqq\lambda_i\leqq D-1,\ 1\leqq i\leqq d),$$

avec

$$D=N^{n/(d-n)}(\log N)^{n+2},\qquad L=[D]^d,\ S=DN,$$

et

$$r=N,\ R=eN,\ U=N^{d/(d-n)}(\log N)^{d+2}.$$

Corollaire 3.2. *Soient $x_1,\ldots,x_d$ des éléments de $\mathbb{C}^n$, avec $d>n$. Il existe un entier $N_0>0$, et une suite $(P_N)_{N\geqq N_0}$ de polynômes non nuls de $\mathbb{Z}[T_1,\ldots,T_d]$, avec*

$$\deg_{T_i}P_N<N^{n/(d-n)}(\log N)^{n+2},\qquad(1\leqq i\leqq d)$$
$$\log H(P_N)\leqq N^{d/(d-n)}(\log N)^{n+2},$$

telle que les fonctions

$$F_N(z)=P_N(e^{\langle x_1,z\rangle},\ldots,e^{\langle x_d,z\rangle})$$

vérifient

$$|F_N|_N\leqq\exp\{-N^{d/(d-n)}(\log N)^{d+2}\}.$$

On a noté $H(P)$ la hauteur de $P\in\mathbb{Z}[T_1,\ldots,T_d]$, c'est-à-dire le maximum des valeurs absolues des coefficients de P.

b) *Un lemme de Siegel*

Nous utiliserons la version suivante du lemme de Siegel.

Lemme 3.3. *Soient S, U, V des nombres réels positifs, et $u_{i,j}$ $(1\leqq i\leqq v,\ 1\leqq j\leqq\mu)$ des nombres complexes. On suppose*

$$\sum_{i=1}^{v}|u_{i,j}|\leqq e^U,\qquad(1\leqq j\leqq\mu),$$

et

$$(\sqrt{2}\,e^{S+U+V}+1)^{2\mu}\leqq e^{vS}.$$

Alors il existe $(\xi_1,\ldots,\xi_v)\in\mathbb{Z}^v$ vérifiant

$$0<\max_{1\leqq i\leqq v}|\xi_i|\leqq e^S$$

et

$$\max_{1\leqq j\leqq\mu}\left|\sum_{i=1}^{v}u_{i,j}\xi_i\right|\leqq e^{-V}.$$

Démonstration. Quitte à multiplier les $u_{i,j}$ par e^{-U} et à remplacer V par $U+V$, on peut supposer $U=0$. Posons $X=[e^S]$. Grâce à l'hypothèse, il existe un entier ℓ vérifiant

$$\ell^{2\mu}<(X+1)^v\quad\text{et}\quad\sqrt{2}X/\ell\leqq e^{-V}.$$

On utilise alors le lemme 1 de [3] pour résoudre le système

$$\begin{cases}\max\limits_{1\leqq j\leqq\mu}\left|\sum\limits_{i=1}^{v}\mathrm{Re}\,(u_{i,j})\,\xi_i\right|\leqq X/\ell\\ \max\limits_{1\leqq j\leqq\mu}\left|\sum\limits_{i=1}^{v}\mathrm{Im}\,(u_{i,j})\,\xi_i\right|\leqq X/\ell.\end{cases}$$

c) *Formule d'interpolation*

Pour $\tau=(\tau_1,\ldots,\tau_n)\in\mathbb{N}^n$, on note $\tau!=\tau_1!\ldots\tau_n!$, $\|\tau\|=\tau_1+\ldots+\tau_n$, et $D^\tau=(\partial^{\tau_1}/\partial z_1^{\tau_1})\ldots(\partial^{\tau_n}/\partial z_n^{\tau_n})$.

Lemme 3.4. *Soient r et R deux nombres réels vérifiant $0<r<R$, T un entier positif, et F une fonction continue dans $B(0,R)$, analytique à l'intérieur. Alors*

$$|F|_r\leqq(1+T^{\frac{1}{2}})(r/R)^T|F|_R+\sum_{\|\tau\|<T}|D^\tau F(0)|\,r^{\|\tau\|}/\tau!$$

Démonstration. On tronque le développement de Taylor de F à l'origine: soit

$$G(z)=F(z)-\sum_{\|\tau\|<T}D^\tau F(0)\,z^\tau/\tau!.$$

Soit $z_0 \in \mathbb{C}^n$ avec $|z_0| = r$ tel que $|F(z_0)| = |F|_r$. On définit deux fonctions f et g d'une variable complexe w par

$$f(w) = F(z_0 w), \qquad g(w) = G(z_0 w).$$

Comme g a un zéro à l'origine d'ordre $\geqq T$, on a par le lemme de Schwarz

$$|g(1)| \leqq (r/R)^T |g|_{R/r}.$$

Notons

$$P(w) = f(w) - g(w) = \sum_{t=0}^{T-1} a_t w^t,$$

avec

$$a_t = \sum_{|\tau| = t} D^\tau F(0)\, z_0^\tau / \tau!, \qquad (0 \leqq t < T).$$

On a grâce à la relation de Parseval,

$$\begin{aligned} |P|_{R/r} &\leqq \sum_{t=0}^{T-1} |a_t| (R/r)^t \\ &\leqq T^{\frac{1}{2}} \left(\sum_{t=0}^{T-1} |a_t|^2 (R/r)^{2t} \right)^{\frac{1}{2}} \\ &\leqq T^{\frac{1}{2}} |f|_{R/r}, \end{aligned}$$

donc

$$|g|_{R/r} \leqq (1 + T^{\frac{1}{2}}) |f|_{R/r},$$

et finalement

$$|G(z_0)| \leqq (1 + T^{\frac{1}{2}})(r/R)^T |F|_R.$$

On obtient alors

$$\begin{aligned} |F|_r &= |F(z_0)| \\ &\leqq |G(z_0)| + \sum_{\|\tau\| < T} |D^\tau F(0)| |z_0|^{\|\tau\|} / \tau!, \end{aligned}$$

d'où le lemme 3.4.

d) *Démonstration du théorème 3.1.*
On définit un nombre réel T_0 par

$$T_0 = 4U / \log(R/r)$$

Remarquons que T_0 vérifie

$$4 \leqq T_0 \leqq 4U.$$

Soit T le plus petit entier $\geqq T_0$. On résout le système de

$$\binom{T+n-1}{n} < (T_0 + 1)^n$$

inéquations à L inconnues $p_1, \ldots, p_L$:

$$\left| \sum_{\lambda=1}^{L} p_\lambda D^\tau \varphi_\lambda(0)\, r^{\|\tau\|} / \tau! \right| \leqq \tfrac{1}{2}(1 + T_0)^{-n} e^{-U}, \qquad (\|\tau\| < T).$$

On a d'une part

$$\sum_{\lambda=1}^{L} |D^{\tau}\varphi_{\lambda}(0)|\, r^{\|\tau\|}/\tau! \leqq \sum_{\lambda=1}^{L} |\varphi_{\lambda}|_r \leqq e^U, \qquad (\|\tau\| < T),$$

et d'autre part

$$2\sqrt{2}(1+T_0)^n e^{3U} + 1 \leqq e^{(2n+3)U}$$

et

$$2(2n+3)\,U(1+T_0)^n \leqq 2^{n+3}\, T_0^n U \leqq LS.$$

Le lemme 3.3 montre l'existence d'une solution non triviale $(p_1, \ldots, p_L) \in \mathbb{Z}^L$ avec

$$\max_{1 \leqq \lambda \leqq L} |p_{\lambda}| \leqq e^S.$$

Alors la fonction

$$F = \sum_{\lambda=1}^{L} p_{\lambda}\varphi_{\lambda}$$

vérifie

$$\sum_{\|\tau\| < T} |D^{\tau}F(0)|\, r^{\|\tau\|}/\tau! \leqq \tfrac{1}{2} e^{-U}.$$

Des inégalités

$$|F|_R \leqq \sum_{\lambda=1}^{L} |p_{\lambda}|\,|\varphi_{\lambda}|_R \leqq e^{S+U} \leqq e^{2U}$$

et

$$1 + T^{\frac{1}{2}} \leqq 2 + 2\sqrt{U} \leqq \tfrac{1}{2} e^U$$

on déduit

$$(1+T^{\frac{1}{2}})(r/R)^T |F|_R \leqq \tfrac{1}{2} e^{3U} (R/r)^{-T_0} \leqq \tfrac{1}{2} e^{-U},$$

et le lemme 3.4 donne le résultat annoncé.

§ 4. Théorème de Masser et conséquences

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 $\mathbb{C}^n$ de rang d et ℓ respectivement. Dans [2], Masser définit

$$\chi(Y, X) = \min_{X', Y'} \{(\ell - \operatorname{rang}_{\mathbb{Z}} Y')/\operatorname{rang}_{\mathbb{Z}} X'\},$$

où X' décrit les sous-$\mathbb{Z}$-modules de X, et Y' les sous-$\mathbb{Z}$-modules de Y, avec $X' \neq 0$ et $\langle X', Y' \rangle \subseteq 2i\pi\mathbb{Z}$.

Pour N entier $\geqq 1$, notons

$$Y_N = \{m_1 y_1 + \ldots + m_{\ell} y_{\ell};\ m_j \in \mathbb{Z},\ 0 \leqq m_j \leqq N,\ (1 \leqq j \leqq \ell)\}.$$

Le théorème suivant de Masser [2] va jouer un rôle fundamental.

Théorème 4.1. (Masser). *Soit* $P \in \mathbb{C}[T_1, \ldots, T_d]$ *un polynôme non nul de degré total au plus* D, *avec* $D \geqq 1$. *Soit* N *un entier positif. Si la fonction*

$$\phi(z) = P(e^{\langle x_1, z\rangle}, \ldots, e^{\langle x_d, z\rangle})$$

vérifie

$$\phi(y) = 0 \quad \textit{pour tout } y \in Y_N,$$

alors

$$D \geqq (N/d)^{\chi(Y,X)}.$$

En utilisant le corollaire 3.2, nous allons en déduire:

Corollaire 4.2. *Si les nombres*

$$\exp\langle x_i, y_j\rangle \quad (1 \leqq i \leqq d,\ 1 \leqq j \leqq \ell)$$

sont tous algébriques, et si $d > n$, *alors*

$$\chi(Y, X) \leqq n/(d-n).$$

Démonstration du corollaire 4.2. Quitte à multiplier tous les x_i par $\sum_{j=1}^{\ell} |y_j|$ et à diviser tous les y_j par ce même nombre, on peut supposer $\sum_{j=1}^{\ell} |y_j| = 1$, de sorte que Y_N soit contenu dans $B(0, N)$.

Comme le degré total du polynôme P_N (construit au corollaire 3.2) est majoré par

$$dN^{n/(d-n)}(\log N)^{n+2},$$

il suffit de vérifier que les nombres $F_N(y)$, $(y \in Y_N)$ sont nuls quand N est suffisamment grand.

Notons $\alpha_{i,j} = \exp\langle x_i, y_j\rangle$, $(1 \leqq i \leqq d,\ 1 \leqq j \leqq \ell)$, et, pour N suffisamment grand,

$$S = N^{d/(d-n)}(\log N)^{n+2}, \qquad U = N^{d/(d-n)}(\log N)^{d+2}.$$

Soit $y = m_1 y_1 + \ldots + m_\ell y_\ell \in Y_N$. On a

$$F_N(y) = \sum_{\lambda_1} \ldots \sum_{\lambda_d} p(\lambda_1, \ldots, \lambda_d) \prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{i,j}^{\lambda_i m_j}.$$

Les conjugués de $F_N(y)$ sur $\mathbb{Q}$ ont un module majoré par $\exp(c_1 S)$, où c_1 ne dépend pas de N. Comme $|F_N(y)| \leqq e^{-U}$, on en déduit que la norme de $F_N(y)$ sur $\mathbb{Q}$ a une valeur absolue majorée par $\exp(-U/2)$. Mais cette norme est un nombre rationnel dont un dénominateur est majoré par $\exp(c_2 S)$. Comme $U > 2c_2 S$ pour N suffisamment grand, on en déduit $F_N(y) = 0$.

§ 5. Etude des coefficients μ et χ

a) Le coefficient de Dirichlet généralisé $\mu(\Gamma)$

Soient K un corps de caractéristique nulle, V un espace vectoriel sur K de dimension finie n, Γ un sous-groupe de type fini de V de rang ℓ sur $\mathbb{Z}$, et $\gamma_1, \ldots, \gamma_s$ (avec $s \geqq \ell$) un système générateur de Γ sur $\mathbb{Z}$. On note G l'application

linéaire de K^s dans V définie par

$$G(t_1, \ldots, t_s) = t_1\gamma_1 + \ldots + t_s\gamma_s.$$

Quand on choisit une base $(e_1, \ldots, e_n)$ de V sur K, pour $x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{i=1}^{n} y_i e_i$ dans V, on note

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Remarquons d'abord que, si λ et ρ sont deux nombres entiers, $0 \leqq \lambda \leqq \ell$, $0 \leqq \rho \leqq n$, alors les propriétés suivantes sont équivalentes:

(i) il existe un sous-espace W de V de dimension ρ tel que $\mathrm{rang}_{\mathbb{Z}} \Gamma \cap W = \lambda$

(ii) on choisit une base de V sur K; il existe un sous-espace vectoriel V' de V de codimension ρ, et un sous-groupe Γ' de Γ de rang λ tels que $\langle \Gamma', V' \rangle = 0$.

(iii) il existe un sous-K-espace vectoriel S de K^s, rationnel sur $\mathbb{Q}$, de dimension λ, tel que $\dim_K G(S) = \rho$.

On définit alors (cf. [7] § 1.3):

$$\mu(\Gamma) = \mu(\Gamma, V) = \min\{(\ell - \lambda)/(n - \rho)\},$$

où λ et ρ parcourent les entiers vérifiant les conditions précédentes, avec $\rho < n$.

Lemme 5.1. *Soit Γ un sous-groupe de type fini de V, de rang ℓ sur $\mathbb{Z}$. On suppose $\mu(\Gamma) < \ell/n$. Alors il existe un sous-espace W de V, de dimension $n' > 0$, et un sous-groupe Γ' de $\Gamma \cap W$, de rang l' sur $\mathbb{Z}$, tels que*

$$\mu(\Gamma', W) = \ell'/n' > \ell/n.$$

Démonstration. Voir [7] lemme 1.3.1.

Lemme 5.2. *Soient X et Y deux sous-groupes de type fini de K^n, de rang d et ℓ respectivement. Il existe un entier positif $n' \leqq n$, et deux sous-groupes X' et Y' de $K^{n'}$, de rang d' et ℓ' respectivement, tels que*

$$\mu(X', K^{n'}) = d'/n' \geqq d/n,$$
$$\mu(Y', K^{n'}) = \ell'/n' \geqq \mu(Y, K^n),$$

et

$$\langle X', Y' \rangle \subseteq \langle X, Y \rangle.$$

Démonstration. Le lemme est banal si $\mu(X, K^n) = d/n$ et $\mu(Y, K^n) = \ell/n$. En particulier on peut supposer $n \geqq 2$. On démontre le résultat par récurrence sur n en distingant deux cas.

Premier cas. $\mu(X, K^n) < d/n$.

On utilise le lemme 5.1: il existe un sous-espace V_1 de K^n, de dimension $n_1 < n$, et un sous-groupe X_1 de $V_1 \cap X$, de rang d_1 sur $\mathbb{Z}$, tels que

$$\mu(X_1, V_1) = d_1/n_1 > d/n.$$

Soit $(v_1, \ldots, v_{n_1})$ une base de V_1 sur K, par laquelle on identifie V_1 à K^{n_1}, et soit Y_1 l'image de Y dans K^{n_1} par la projection

$$K^n \to K^{n_1}$$
$$z \mapsto (\langle z, v_\nu \rangle)_{1 \leqq \nu \leqq n_1}$$

Alors

$$\langle X_1, Y_1 \rangle \subseteq \langle X, Y \rangle,$$

et

$$\mu(Y_1, K^{n_1}) \geqq \mu(Y, K^n).$$

L'hypothèse de récurrence donne alors le résultat annoncé.

Deuxième cas. $\mu(X, K^n) = d/n$ *et* $\mu(Y, K^n) < \ell/n$.

On utilise de nouveau le lemme 5.1: il existe un sous-espace V_2 de K^n de dimension $n_2 < n$ et un sous-groupe Y_2 de $V_2 \cap Y$ de rang ℓ_2 sur $\mathbb{Z}$ tels que

$$\mu(Y_2, V_2) = \ell_2/n_2 > \ell/n > \mu(Y, K^n).$$

On choisit une base de V_2, et on considère la projection X_2 de X dans K^{n_2}. On a alors

$$\langle X_2, Y_2 \rangle \subseteq \langle X, Y \rangle,$$

et

$$\mu(X_2, K^{n_2}) \geqq \mu(X, K^n) = d/n.$$

On utilise alors l'hypothèse de récurrence, et on en déduit le lemme 5.2.

Nous utiliserons enfin la remarque suivante, conernant le cas $K = \mathbb{R}$ (cf. [7] p. 36): un sous-groupe de type fini Γ de $\mathbb{R}^n$ est dense dans $\mathbb{R}^n$ si et seulement si $\mu(\Gamma, \mathbb{R}^n) > 1$. Cette remarque résulte par exemple de la classification des sous-groupes fermés des espaces vectoriels réels de dimension finie (cf. Bourbaki, Top. Gén., Chap. VII § 1 ex 9).

b) Propriétés du coefficient $\chi(Y, X)$

Nous utiliserons le lien suivant entre les coefficients μ et χ.

Lemme 5.3. *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* $\mathbb{C}^n$, *de rang* d *et* ℓ *respectivement. On suppose* $\mu(X) = d/n > 1$ *et* $\mu(Y) \geqq d/(d-n)$. *Alors*

$$\chi(Y, X) \geqq \frac{n}{d} \mu(Y).$$

Par exemple si $\mu(X) = d/n$ et $\mu(Y) = \ell/n$ avec $\frac{1}{\ell} + \frac{1}{d} \leqq \frac{1}{n}$, alors $\chi(Y, X) = \ell/d$. Le lemme 5.3 résulte de l'énoncé plus précis suivant.

Lemme 5.4. *Soient* K *un corps de caractéristique nulle,* n *un entier positif,* X *et* Y *deux sous-groupes de type fini de* K^n, *de rang* d *et* ℓ *respectivement,* X' *un sous-groupe de* X *de rang* r, *et* Y' *un sous-groupe de* Y *de rang* s. *On suppose*

$$\mu(X)\,\mu(Y) \geqq \mu(X) + \mu(Y)$$

et

$$\mathrm{rang}_{\mathbb{Z}}(\langle X', Y'\rangle) \leqq 1.$$

Alors

$$(d-r)\,\mu(Y)+(\ell-s)\,\mu(X) \geqq n\,\mu(X)\,\mu(Y).$$

En particulier, si, de plus, on a $\mu(X)=d/n$ et $\mu(Y)=\ell/n$, alors

$$\frac{r}{d}+\frac{s}{\ell} \leqq 1.$$

Démonstration du lemme 5.4. On peut évidemment supposer $s \geqq 1$ et $r \geqq 1$. On choisit une base $x_1, \ldots, x_r$ de X' sur $\mathbb{Z}$, et une base $y_1, \ldots, y_s$ de Y' sur $\mathbb{Z}$, que l'on numérote de telle sorte que, si ρ est le rang de la matrice

$$(\langle x_i, y_j\rangle)_{1 \leqq i \leqq r,\, 1 \leqq j \leqq s}$$

on ait

$$\det(\langle x_h, y_k\rangle)_{1 \leqq h,k \leqq \rho} \neq 0.$$

Soient $a_{j,k} \in \mathbb{Z}$, $(1 \leqq j \leqq s,\ 0 \leqq k \leqq \rho)$, avec $a_{j,0} \neq 0$, $(1 \leqq j \leqq s)$ tels que

$$a_{j,0}\langle x_i, y_j\rangle = \sum_{k=1}^{\rho} a_{j,k}\langle x_i, y_k\rangle, \qquad (1 \leqq i \leqq r,\ 1 \leqq j \leqq s).$$

Pour $\rho < j \leqq s$, on définit

$$\tilde{y}_j = a_{j,0}\, y_j - \sum_{k=1}^{\rho} a_{j,k} y_k.$$

Ainsi

$$\langle x_i, \tilde{y}_j\rangle = 0, \qquad (1 \leqq i \leqq r,\ \rho < j \leqq s).$$

Soit W le sous-espace de K^n engendré par $\tilde{y}_{\rho+1}, \ldots, \tilde{y}_s$. Comme $y_1, \ldots, y_\rho$ sont K-linéairement indépendants, et que

$$W \cap (K y_1 + \ldots + K y_\rho) = 0,$$

on a

$$\dim_K W = \omega - \rho,$$

où

$$\omega = \dim_K K \cdot Y'.$$

D'autre part $\tilde{y}_{\rho+1}, \ldots, \tilde{y}_s$ sont $\mathbb{Q}$-linéairement indépendants, donc

$$\mathrm{rang}_{\mathbb{Z}}\, Y \cap W \geqq s - \rho.$$

Enfin, comme $r \geqq 1$, on a $\omega - \rho < n$. D'où

$$\mu(Y) \leqq (\ell - s + \rho)/(n - \omega + \rho).$$

De même

$$\mu(X) \leqq (d - r + \rho)/(n - v + \rho),$$

où

$$v = \dim_K K \cdot X'.$$

On vérifie facilement que $\dim_K(KX' \cap KY') \leqq \rho$, donc

$$\omega + v - \rho \leqq \dim_K(KX' + KY') \leqq n.$$

On en déduit

$$(d-r)\mu(Y) + (\ell - s)\mu(X) \geqq n\mu(X)\mu(Y) + \rho(\mu(X)\mu(Y) - \mu(X) - \mu(Y)),$$

d'où le lemme 5.4.

§ 6. Démonstrations

a) Démonstration du théorème 1.1.

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 $\mathbb{C}^n$ de rang d et ℓ respectivement. Supposons que les nombres

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

soient tous algébriques.

Nous montrons d'abord le résultat suivant.

Proposition 6.1. *Si $d > n$, alors $\mu(Y) \leqq d/(d-n)$.*

Démonstration de la proposition 6.1. Le lemme 5.2 permet de construire deux sous-groupes X' et Y' de $\mathbb{C}^{n'}$, de rang d' et ℓ' respectivement, avec

$$\mu(X') = d'/n' \geqq d/n, \qquad \mu(Y') = \ell'/n' \geqq \mu(Y),$$

et

$$\exp\langle X', Y'\rangle \subset \overline{\mathbb{Q}}.$$

Supposons $d > n$ et $\mu(Y) > d/(d-n)$. Alors

$$\ell'/n' > d/(d-n) \geqq d'/(d'-n'),$$

donc

$$d'\ell' > n'(d' + \ell').$$

Le lemme 5.3 donne alors

$$\chi(X', Y') = \ell'/d' > n'/(d'-n'),$$

ce qui contredit le corollaire 4.2.

Remarque. Les «conséquences d'un lemme de Schwarz conjectural» de [6] § 3 sont donc toutes établies, en particulier les corollaires 1.2 et 1.3 sont maintenant démontrés. Mais ce lemme de Schwarz conjectural [7] (7.1.2) n'est toujours pas démontré.

Néanmoins on peut espérer que la méthode présentée ici, jointe aux travaux en cours de Masser et Wüstholz sur les lemmes de zéros dans les groupes algébriques, permettra de résoudre les autres problèmes des § 8.1 et § 8.2 de [7].

Démonstration du théorème 1.1. Sous les hypothèses du théorème 1.1, on déduit de la proposition 6.1 l'inégalité $\mu(X) < d/n$. D'après le lemme 5.1, il existe un sous-espace W de $\mathbb{C}^n$, de dimension n_1, et un sous-groupe X_1 de $X \cap W$, de rang

d_1 tels que

$$\mu(X_1, W) = d_1/n_1 > d/n.$$

On peut évidemment choisir un tel X_1 qui soit facteur direct dans X, et on note $X = X_1 \oplus X_2$, où X_2 est de rang $d_2 = d - d_1$.

On note V l'orthogonal de W, $Y_2 = Y \cap V$, et ℓ_2 le rang de Y_2. On a $Y = Y_1 \oplus Y_2$, où Y_1 est de rang $\ell_1 = \ell - \ell_2$.

On identifie $\mathbb{C}^n/V$ à W, et on note $s: \mathbb{C}^n \to \mathbb{C}^n/V$ la surjection canonique. Alors

$$\operatorname{rang}_{\mathbb{Z}} s(Y) = \ell - \operatorname{rang}_{\mathbb{Z}} Y \cap V = \ell_1.$$

Comme

$$\exp\langle s(Y), X_1\rangle \subset \overline{\mathbb{Q}}$$

et que $\mu(X_1) = d_1/n_1$, on déduit de la proposition 6.1

$$\ell_1 d_1 \leqq n_1(\ell_1 + d_1),$$

d'où le théorème 1.1.

Remarque. Des inégalités

$$d_1/n_1 > d/n \quad \text{et} \quad \ell_1 d_1 \leqq n_1(\ell_1 + d_1)$$

on déduit

$$\mu(Y) \leqq \ell_1/n_1 \leqq d_1/(d_1 - n_1) < d/(d-n) < \ell/n,$$

donc, en désignant par n_2 la dimension du $\mathbb{C}$-espace vectoriel engendré par Y_2,

$$\ell_2/n_2 \geqq (\ell - \ell_1)/(n - n_1) > \ell/n.$$

On notera au passage que l'on a obtenu l'inégalité stricte dans la proposition 6.1 :

$$\mu(Y) < d/(d-n).$$

b) Démonstration du corollaire 1.4.

Soit k un corps de nombres. L'équivalence entre les trois propriétés suivantes a été remarquée par H.W. Lenstra, Jr.

(i) Il existe un sous-groupe de type fini de k^* qui est dense dans $(k \otimes_{\mathbb{Q}} \mathbb{R})^*$.

(ii) Tout caractère continu $\chi: (k \otimes_{\mathbb{Q}} \mathbb{R})^* \to \mathbb{C}^*$ envoyant k^* dans l'ensemble des racines de l'unité est d'ordre fini

(iii) Tout caractère de Hecke de k qui, considéré comme fonction sur les idéaux, a ses valeurs dans les racines de l'unité, est d'ordre fini.

Comme (ii) et (iii) sont des conséquences du corollaire 1.3, il suffit pour établir le corollaire 1.4 de vérifier l'implication (ii) $\Rightarrow$ (i).

On considère la suite exacte

$$0 \to (2i\pi\mathbb{Z})^{r_2} \to k \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\exp} (k \otimes_{\mathbb{Q}} \mathbb{R})^* \to (\mathbb{Z}/2\mathbb{Z})^{r_1} \to 0,$$

on note V le $\mathbb{R}$-espace vectoriel $k \otimes_{\mathbb{Q}} \mathbb{R}$, et G le sous-groupe de V image inverse de k^* par l'exponentielle. Soit W un hyperplan de V. De la propriété (ii) on

déduit que l'image de G dans V/W a un rang $\geqq 2$. Donc il existe un sous-groupe Γ de G, de type fini, tel que $\mu(\Gamma)>1$ (cf. [6], § 2b). Alors Γ est dense dans V, et il suffit de considérer l'image de Γ dans $(k\otimes_{\mathbb{Q}}\mathbb{R})^*$.

Remarque. Le corollaire 1.2 permet de montrer (cf. [6] § 3) que si $L: k^* \to \mathbb{R}^n$ est le plongement logarithmique d'un corps de nombres k, avec $n=r_1+r_2$, et si H est un hyperplan de $\mathbb{R}^n$, alors le rang sur $\mathbb{Z}$ de $L(k^*)/H\cap L(k^*)$ est infini.

c) Démonstration du théorème 2.1.

Comme la matrice M est de rang r, il existe deux applications linéaires surjectives $\xi: \mathbb{C}^d \to \mathbb{C}^r$ et $\eta: \mathbb{C}^\ell \to \mathbb{C}^r$ telles que ${}^t\xi \circ \eta: \mathbb{C}^\ell \to \mathbb{C}^d$ soit l'application linéaire associée à M dans les bases canoniques.

Notons

$$X=\xi(\mathbb{Z}^d)=\mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$$

et

$$Y=\eta(\mathbb{Z}^\ell)=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$$

où $(x_1,\ldots,x_d)$ est l'image par ξ de la base canonique de $\mathbb{C}^d$, et $(y_1,\ldots,y_\ell)$ est l'image par η de la base canonique de $\mathbb{C}^\ell$. Alors on a

$$\langle x_i, y_j\rangle = \log \alpha_{i,j}, \qquad (1\leqq i\leqq d,\ 1\leqq j\leqq \ell).$$

Comme les lignes de M sont $\mathbb{Q}$-linéairement indépendantes, le rang de X sur $\mathbb{Z}$ est égal à d; de même, comme les colonnes de M sont $\mathbb{Q}$-linéairement indépendantes, le rang de Y sur $\mathbb{Z}$ est égal à ℓ. Grâce au théorème 1.1 on peut écrire

$$X=\mathbb{Z}x'_1+\ldots+\mathbb{Z}x'_d \quad \text{et} \quad Y=\mathbb{Z}y'_1+\ldots+\mathbb{Z}y'_\ell,$$

avec

$$\langle x'_i, y'_j\rangle = 0, \qquad (1\leqq i\leqq d_1,\ \ell_2<j\leqq \ell),$$

et

$$d_1/n_1 > d/r, \qquad \ell_1 d_1 \leqq n_1(\ell_1+d_1),$$

où n_1 est la dimension du $\mathbb{C}$-espace vectoriel engendré par $x_1,\ldots,x_{d_1}$. On définit $P\in SL_d(\mathbb{Z})$ et $Q\in SL_\ell(\mathbb{Z})$ par

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_d \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \quad \text{et} \quad (y'_1,\ldots,y'_\ell)=(y_1,\ldots,y_\ell)Q.$$

Alors

$$PMQ=(\langle x'_i, y'_j\rangle)_{1\leqq i\leqq d,\ 1\leqq j\leqq \ell}.$$

Comme η est surjective, Y contient une base de $\mathbb{C}^r$ sur $\mathbb{C}$, donc la matrice

$$M_1=(\langle x'_i, y'_j\rangle)_{1\leqq i\leqq d_1,\ 1\leqq j\leqq \ell_1}$$

a un rang égal à n_1.

Cela démontre le théorème 2.1.

Remarque. Pour appliquer le théorème 2.1 à une matrice $M=(\log\alpha_{i,j})$ de rang r pour laquelle on ne suppose pas les vecteurs lignes et les vecteurs colonnes linéairement indépendants sur $\mathbb{Q}$, on utilise la remarque suivante: si d' est le

rang sur $\mathbb{Z}$ des vecteurs lignes, et ℓ' le rang sur $\mathbb{Z}$ des vecteurs colonnes, alors il existe $P \in SL_d(\mathbb{Z})$ et $Q \in SL_\ell(\mathbb{Z})$ tels que

$$PMQ = \begin{pmatrix} 0 & 0 \\ M' & 0 \end{pmatrix}$$

où M' est une matrice $d' \times \ell'$ de rang r dont les lignes et les colonnes sont $\mathbb{Q}$-linéairement indépendantes.

§ 7. Compléments

a) Définition et propriétés élémentaires du coefficient θ

Soient K un corps de caractéristique 0, ℓ et d deux entiers positifs, et M une matrice $d \times \ell$ à coefficients dans K, que l'on identifie avec l'application linéaire correspondante $K^\ell \to K^d$ dans les bases canoniques. Soit $Z = \mathbb{Z}z_1 + \ldots + \mathbb{Z}z_\ell$ le sous-groupe de K^d engendré par les colonnes de M:

$$z_j = (u_{1,j}, \ldots, u_{d,j}), \quad (1 \leqq j \leqq \ell).$$

Soient λ et δ deux entiers positifs ou nuls. Les propriétés suivantes sont équivalentes:

(i) Il existe $P \in SL_d(\mathbb{Z})$ et $Q \in SL_\ell(\mathbb{Z})$ tels que

$$PMQ = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

où C est une matrice $\delta \times \lambda$.

(ii) Il existe un sous-espace S de K^ℓ, rationnel sur $\mathbb{Q}$, de dimension λ, et un sous-espace T de K^d, rationnel sur $\mathbb{Q}$, de dimension δ, tels que

$$M(S) \subseteq T.$$

(iii) Il existe un sous-espace T de K^d, rationnel sur $\mathbb{Q}$, de dimension δ, tel que

$$\operatorname{rang}_{\mathbb{Z}} Z \cap T \geqq \lambda - \ell + \operatorname{rang}_{\mathbb{Z}} Z.$$

Définition. On définit les nombres $\theta(M)$ et $\theta(Z)$ par

$$\theta(M) = \theta(Z) = \min \{(\ell - \lambda)/(d - \delta)\},$$

où λ et δ décrivent les entiers vérifiant les conditions précédentes avec $\delta \neq d$.

Remarques. 1. On a $\theta(M) = 0$ si et seulement si les d lignes de M

$$(u_{i,1}, \ldots, u_{i,\ell}) \in K^\ell, \quad (1 \leqq i \leqq d)$$

sont $\mathbb{Q}$-linéairement dépendantes.

2. On a

$$\theta(M) \leqq \frac{1}{d} \operatorname{rang}_{\mathbb{Z}} Z.$$

3. Les conditions $\theta(M)=\ell/d$ et $\theta({}^tM)=d/\ell$ sont équivalentes.

4. On a

$$\mu(Z)\leqq\theta(M).$$

5. Si r est le rang de M, avec les notations précédentes on a $r\leqq\ell-\lambda+\delta$. En particulier, si $r=d$, alors $\theta(M)\geqq 1$; autrement dit si $\theta(M)<1$, alors $\mu(Z)=0$.

6. Supposons $M=(\langle x_i, y_j\rangle)_{1\leqq i\leqq d,\,1\leqq j\leqq\ell}$, où $X=\mathbb{Z}x_1+\ldots+\mathbb{Z}x_d$ et $Y=\mathbb{Z}y_1+\ldots+\mathbb{Z}y_\ell$ sont deux sous-groupes de $\mathbb{C}^n$. Alors $\theta(M)=\chi_0(Y,X)$, où χ_0 est défini de façon analogue à χ (cf. § 4), mais en remplaçant $2i\pi\mathbb{Z}$ par 0.

7. Si $p_1,\ldots,p_{d+\ell}$ sont des nombres premiers deux-à-deux distincts, et $d\geqq 2$, alors la matrice

$$M=(\sqrt[]{p_ip_{d+j}})_{1\leqq i\leqq d,\,1\leqq j\leqq\ell}$$

a pour rang 1, et vérifie

$$\theta(M)=\ell/d,\qquad \mu(Z)=0.$$

Les remarques 4 et 5 conduisent à des majorations de $\mu(Z)$ et du rang de M en fonction de $\theta(M)$. La remarque 7 montre qu'il n'y a pas, en général, d'inégalité dans l'autre sens. Néanmoins nous allons voir que si les coefficients de M sont des logarithmes de nombres algébriques, alors le théorème 2.1 permet de minorer $\mu(Z)$ et r en fonction de $\theta(M)$. Minorer μ ou r est un problème de transcendance (ou même d'indépendance algébrique de logarithmes), alors que minorer θ est un problème d'irrationalité, ou plus précisément d'indépendance linéaire sur $\mathbb{Q}$.

b) Compléments au corollaire 1.2.

L'énoncé suivant précise le corollaire 1.2.

Corollaire 7.1. *Soient X et Y deux sous-groupes de type fini de $\mathbb{C}^n$ tels que*

$$\exp\langle x, y\rangle\in\overline{\mathbb{Q}}$$

pour tout $x\in X$ et tout $y\in Y$. On suppose que X contient $\mathbb{Z}^n$, et que le rang de Y est $\geqq n^2+n+1$.

a) *Alors il existe $a\in\mathbb{Z}^n$, $a\neq 0$, tel que*

$$\langle a, x\rangle\in\mathbb{Z}$$

pour tout $x\in X$.

b) *Si, de plus, le rang de X est $\geqq n+1$, alors $\theta(Y)\leqq n$.*

Démonstration. a) Notons d le rang de X, et ℓ le rang de Y. Si $d=n$, l'énoncé est banal. Si $d\geqq n+1$, d'après la proposition 6.1 en permutant X et Y on a

$$\mu(X)\leqq\ell/(\ell-n)\leqq 1+\frac{n}{n^2+1}<1+(1/n),$$

donc $\mu(X)=1$. L'énoncé a) s'en déduit.

b) On peut supposer $d=n+1$. Avec les notations du théorème 1.1, soit W l'espace engendré par X_1 sur $\mathbb{C}$. On obtient alors

$$d_1=n_1+1,\qquad \text{et } \operatorname{rang}_{\mathbb{Z}} W\cap\mathbb{Z}^n=\dim_{\mathbb{C}} W,$$

donc W est rationnel sur $\mathbb{Q}$. Comme

$$\operatorname{rang}_{\mathbb{Z}} Y \cap W^{\perp} \geqq \ell - \ell_1,$$

on a

$$\theta(Y) \leqq \ell_1/n_1 \leqq d_1/(d_1 - n_1) = n_1 + 1 \leqq n.$$

Remarque. On peut apporter d'autres précisions au corollaire 1.2. Par exemple soit P l'ensemble des nombres premiers. Soient $t_1, \ldots, t_n$ des nombres complexes. On suppose qu'il existe une infinité de $(p_1, \ldots, p_n) \in P^n$ vérifiant

$$p_1^{t_1} \ldots p_n^{t_n} \in \overline{\mathbb{Q}}.$$

Alors il existe une partie non vide J de $\{1, \ldots, n\}$ telle que

$$\sum_{j \in J} t_j \in \mathbb{Q}.$$

c) Minoration de r en fonction de θ

Voici une conséquence du théorème 2.1.

Corollaire 7.2. *Soit $M = (\log \alpha_{i,j})_{1 \leqq i \leqq d,\, 1 \leqq j \leqq \ell}$ une matrice $d \times \ell$ dont les coefficients sont des logarithmes de nombres algébriques. Soit r le rang de M, et soit $\theta = \theta(M)$. Alors*

$$r \geqq d\theta/(1+\theta).$$

Remarque. Nous obtiendrons l'inégalité stricte dans le cas où $r < \ell d/(\ell + d)$ et où les ℓ vecteurs colonnes de M sont $\mathbb{Q}$-linéairement indépendants dans $\mathbb{C}^d$.

Démonstration. Grâce à la remarque à la fin du § 6, on peut supposer que les lignes de M sont $\mathbb{Q}$-linéairement indépendantes, et aussi que les colonnes de M sont $\mathbb{Q}$-linéairement indépendantes. Si $r \geqq \ell d/(\ell + d)$, le résultat est clair. Sinon, on utilise le théorème 2.1 :

$$\theta \leqq \ell_1/d_1 \leqq r_1/(d_1 - r_1) < r/(d-r).$$

d) Minoration de μ en fonction de θ

Le théorème 2.1 permet de minorer $\mu(Z)$ en fonction de $\theta(Z)$ quand Z est un sous-groupe de type fini de $\mathbb{C}^d$ engendré par des points dont les coordonnées sont des logarithmes de nombres algébriques. Voici quelques exemples.

Corollaire 7.3. *Soit Z un sous-groupe de $\mathbb{C}^d$ de rang ℓ engendré par des points de $\mathbb{C}^d$ dont les composantes sont des logarithmes de nombres algébriques.*

a) *Si $\ell \geqq d^2 - d + 1$ et $\theta(Z) \geqq d - 1$, alors $\mu(Z) > 0$.*

b) *Si $\ell \geqq d^2 - d + 2$ et $\theta(Z) > d - 1$, alors $\mu(Z) > 1$.*

c) *Si $\ell \geqq d^2$ et $\theta(Z) \geqq d - 1$, alors $\mu(Z) = \theta(Z)$.*

Démonstration. a) Si $\mu(Z) = 0$ et $\ell > d(d-1)$, on a, avec les notations du corollaire 7.2 et en utilisant la remarque qui le suit,

$$r \leqq d - 1 < \ell d/(\ell + d), \quad \text{donc } \theta(Z) < r/(d-r) \leqq d - 1.$$

b) Supposons $\mu(Z)=1$ et $\ell-1>d(d-1)$. Alors on a $Z=Z_1\oplus Z_2$, où Z_2 est de rang $\ell-1$ et engendre un $\mathbb{C}$-espace vectoriel de $\mathbb{C}^d$ de codimension 1. Utilisant a), on peut écrire

$$\theta(Z_2)=\lambda/\delta<d-1 \quad \text{et} \quad \theta(Z)\leqq(\lambda+1)/\delta.$$

Mais la condition $\lambda<\delta(d-1)$ s'écrit aussi $\lambda\leqq\delta(d-1)-1$, donc $\theta(Z)\leqq d-1$.

c) Supposons $\ell\geqq d^2$ et $\mu(Z)<\theta(Z)$. Soit W un sous-espace de $\mathbb{C}^n$, de dimension r, avec $1\leqq r<d$, tel que

$$\mu(Z)=(\ell-\lambda)/(d-r), \quad \text{où} \quad \lambda=\operatorname{rang}_{\mathbb{Z}} Z\cap W.$$

Après une permutation éventuelle de la base canonique de $\mathbb{C}^d$, on peut construire une base $v_1,\ldots,v_{d-r}$ de l'orthogonal V de W de la forme

$$v_h=(v_{h,1},\ldots,v_{h,r},\delta_{h,1},\ldots,\delta_{h,d-r}), \quad (1\leqq h\leqq d-r),$$

où $\delta_{h,k}$ est le symbole de Kronecker. Soit $p:\mathbb{C}^d\to\mathbb{C}^r$ la projection sur les r première coordonnées. La restriction de p à W est un isomorphisme de W sur $\mathbb{C}^r$. Le sous-groupe $Y=p(Z\cap W)$ de $\mathbb{C}^r$ a donc pour rang λ, et on a

$$\lambda>\ell r/d\geqq dr\geqq r(r+1).$$

On définit

$$X=\mathbb{Z}^r+\mathbb{Z}p(v_1)+\ldots+\mathbb{Z}p(v_{d-r}).$$

Comme $\mu(Z)<\theta(Z)$, V n'est pas rationnel sur $\mathbb{Q}$, c'est-à-dire $\operatorname{rang}_{\mathbb{Z}} X\geqq r+1$. Alors le corollaire 7.1 b implique $\theta(Y)\leqq r$. On écrit donc $Y=Y_1\oplus Y_2$, où le rang λ_1 de Y_1 sur $\mathbb{Z}$ vérifie $1\leqq\lambda_1\leqq\delta r$, δ étant la codimension du $\mathbb{C}$-espace vectoriel E engendré par Y_1 dans $\mathbb{C}^r$; de plus E est rationnel sur $\mathbb{Q}$. On choisit une telle décomposition avec δ maximal. On a

$$\delta\leqq r-1, \quad \text{et} \quad \operatorname{rang}_{\mathbb{Z}} Y_2=\lambda-\lambda_1>r.$$

On considère l'image $\bar{Y}_2$ de Y_2 par un isomorphisme $E\to\mathbb{C}^{r-\delta}$ défini sur $\mathbb{Q}$. Comme δ est maximal, on a $\theta(\bar{Y}_2)>r$. En utilisant encore une fois le corollaire 7.1 b, on peut écrire $Z\cap W=Z_1\oplus Z_2$, où Z_1 a pour rang λ_1 et Z_2 engendre un $\mathbb{C}$-espace vectoriel rationnel sur $\mathbb{Q}$ de codimension $d-r+\delta$ dans $\mathbb{C}^d$. Alors on obtient

$$\theta(Z)\leqq(\ell-\lambda+\lambda_1)/(d-r+\delta)$$

Mais l'inégalité

$$\theta(Z)>(\ell-\lambda)/(d-r)$$

implique alors

$$\delta(\ell-\lambda)<\lambda_1(d-r),$$

donc

$$\delta(\ell-\lambda+\lambda_1)<\lambda_1(d-r+\delta),$$

et

$$\theta(Z)<\lambda_1/\delta\leqq r\leqq d-1,$$

ce qui termine la démonstration.

e) Densité

Du corollaire 7.3b on déduit:

Corollaire 7.4. *Soient* $\alpha_{i,j}$, $(1 \leqq i \leqq d,\ 1 \leqq j \leqq \ell)$ *des nombres algébriques positifs multiplicativement indépendants, avec* $\ell \geqq d^2 - d + 2$. *Alors le sous-groupe de* $(\mathbb{R}_+^*)^d$ *engendré par les* ℓ *éléments*

$$(\alpha_{1,j}, \ldots, \alpha_{d,j}), \qquad (1 \leqq j \leqq \ell)$$

est dense dans $(\mathbb{R}_+^*)^d$.

§ 8. Indépendance algébrique

La méthode présentée ici permet d'obtenir des résultats d'indépendance algébrique. Pour cela on construit d'abord une fonction auxiliaire plus générale que celle du théorème 3.1, en choisissant les p_λ dans un anneau $\mathbb{Z}[\theta_1, \ldots, \theta_q]$, où $\theta_1, \ldots, \theta_q$ sont des nombres complexes. Si S est une borne pour la hauteur et D une borne pour le degré des p_λ (considérés comme polynômes en $\theta_1, \ldots, \theta_q$), on remplace dans le théorème 3.1 l'hypothèse

$$(8U)^{n+1} \leqq LS(\operatorname{Log} R/r)^n$$

par

$$c_0 U^{n+1} \leqq LSD^q(\operatorname{Log} R/r)^n,$$

où c_0 est une constante ne dépendant que de $\theta_1, \ldots, \theta_q$ et n.

Nous donnons ici seulement un exemple utilisant le théorème 4.1 de Masser. Pour le théorème 8.1 et le corollaire 8.2, nous désignons par $X = \mathbb{Z}x_1 + \ldots + \mathbb{Z}x_d$ un sous-groupe de $\mathbb{C}^n$ de rang d, et par $Y = \mathbb{Z}y_1 + \ldots + \mathbb{Z}y_\ell$ un sous-groupe de $\mathbb{C}^n$ de rang ℓ.

Théorème 8.1. *Soit* $\theta_1, \ldots, \theta_q$ *une base de transcendance sur* $\mathbb{Q}$ *du corps obtenu en adjoignant à* $\mathbb{Q}$ *les* $d\ell$ *nombres*

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

Notons $\chi = \chi(Y, X)$, *et*

$$\kappa = \left(q + 1 + \frac{d\chi}{\chi + 1}\right) \Big/ (n+1).$$

On suppose $q \geqq 1$.

Alors il existe une suite $(P_N)_{N \geqq N_0}$ *de polynômes non nuls de* $\mathbb{Z}[T_1, \ldots, T_q]$ *vérifiant*

$$\deg_{T_h} P_N \leqq N, \qquad (1 \leqq h \leqq q),$$
$$\log H(P_N) \leqq N,$$

et

$$\log |P_N(\theta_1, \ldots, \theta_q)| \leqq -N^\kappa (\log N)^{n/(n+2)}.$$

Grâce à un critère de Gel'fond [1] p. 55, on en déduit le corollaire suivant.

Corollaire 8.2. *On suppose* $\ell d \geqq 2n(\ell + d)$, *Si le corps obtenu en adjoignant à* $\mathbb{Q}$ *les* ℓd *nombres*

$$\exp \langle x_i, y_j \rangle, \quad (1 \leqq i \leqq d, 1 \leqq j \leqq \ell)$$

a un degré de transcendance $\leqq 1$ *sur* $\mathbb{Q}$, *alors on a*

$$X = X_1 \oplus X_2, \quad Y = Y_1 \oplus Y_2,$$

où X_1 *est un sous-groupe de* X *de rang* d_1, *et* Y_1 *un sous-groupe de* Y *de rang* ℓ_1, *avec*

$$\langle X_1, Y_2 \rangle = 0, \quad d_1/n_1 > d/n, \quad \text{et} \quad \ell_1 d_1 < 2n_1(\ell_1 + d_1),$$

n_1 *désignant la dimension du* $\mathbb{C}$*-espace vectoriel engendré par* X_1.

Deuxième Partie: Le cas *p*-adique

Dans toute cette deuxième partie, on désigne par K un corps valué non archimédien complet de caractéristique nulle et de caractéristique résiduelle $p \neq 0$. On normalise sa valuation v par $v(p) = 1$, et sa valeur absolue par

$$|x| = p^{-v(x)} \quad \text{pour } x \in K.$$

On note $\mathcal{O}$ l'anneau des entiers, $\mathcal{M}$ l'idéal de valuation, et $\mathcal{U}$ le groupe des unités de K:

$$\mathcal{O} = \{x \in K, v(x) \geqq 0\},$$
$$\mathcal{M} = \{x \in K, v(x) > 0\},$$
$$\mathcal{U} = \{x \in K, v(x) = 0\}.$$

Pour $x \in \mathcal{M}$, on définit le logarithme p-adique de $1 + x$ par la série convergente

$$\log_p(1 + x) = \sum_{m \geqq 1} (-1)^{m-1} x^m/m.$$

La fonction $\log_p$ definit un homomorphisme continu du groupe multiplicatif $1 + \mathcal{M}$ dans le groupe additif K.

Soit Ω_p une clôture algébrique du corps $\mathbb{Q}_p$ des nombres p-adiques. On prolonge le logarithme p-adique en un homomorphisme continu de Ω_p^* dans Ω_p tel que $\log_p p = 0$. Cela permet en particulier de définir $\log_p \alpha$ quand α est un élément non nul de K algébrique sur $\mathbb{Q}$.

Si on désigne par

$$E = \{z \in K, v(z) > 1/(p-1)\}$$

le domaine de convergence de la série exponentielle

$$\exp z = \sum_{m \geqq 0} z^m/m!,$$

pour $z \in E$ on a

$$v(1 - \exp z) = v(z), \quad \log_p(\exp z) = z,$$

et pour $x \in E$ on a

$$v(\log_p(1+x)) = v(x), \qquad \exp(\log_p(1+x)) = 1+x.$$

Ainsi la fonction exp définit un isomorphisme du groupe additif E sur le groupe multiplicatif $1+E$, l'isomorphisme réciproque étant la restriction du logarithme p-adique à $1+E$.

Une référence générale pour les problèmes que nous allons considérer est l'appendice I de [7] par Bertrand.

§ 1. Généralisation à plusieurs variables du théorème p-adique des six exponentielles

L'analogue p-adique du théorème des six exponentielles s'énonce ainsi (cf. [1] Appendice Th. 1, [4] Th. 1, [5] § 3.3 Prop. 1):

si x_1, x_2 sont deux éléments $\mathbb{Q}$-linéairement indépendants de K, et y_1, y_2, y_3 trois éléments $\mathbb{Q}$-linéairement indépendants de K, tels que

$$x_i y_j \in E \quad \text{pour } i=1,2 \text{ et } j=1,2,3,$$

alors un au moins des six nombres

$$\exp(x_i y_j) \quad (i=1,2;\ j=1,2,3)$$

est transcendant.

En voici une généralisation à plusieurs variables.

Théorème 1.1.p. *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 K^n de rang d et ℓ respectivement, avec $\ell d > n(\ell + d)$, et $\langle X, Y\rangle \subset E$. On suppose que les nombres*

$$\exp\langle x, y\rangle, \quad (x \in X,\ y \in Y)$$

sont tous algébriques.

Alors on peut écrire

$$X = X_1 \oplus X_2, \qquad Y = Y_1 \oplus Y_2,$$

avec

$$\langle X_1, Y_2\rangle = 0,$$

et, en désignant par d_1 le rang de X_1, par ℓ_1 le rang de Y_1, et par n_1 la dimension du K-espace vectoriel engendré par X_1,

$$d_1/n_1 > d/n, \quad \text{et} \quad \ell_1 d_1 \leqq n_1(\ell_1 + d_1).$$

Le cas particulier $d = n+1$ s'énonce ainsi.

Corollaire 1.2.p. *Soient $\alpha_{\nu,\mu}$, $(1 \leqq \nu \leqq n,\ 1 \leqq \mu \leqq m)$ des éléments non nuls de K algébriques sur $\mathbb{Q}$, avec $m \geqq n^2 + n + 1$. Soient $t_1, \ldots, t_n$ des éléments de K, avec*

$$\sum_{\nu=1}^{n} t_\nu \log_p \alpha_{\nu,\mu} \in E \quad \text{pour } 1 \leqq \mu \leqq m.$$

On suppose que les m nombres

$$\prod_{\nu=1}^{n} \alpha_{\nu,\mu}^{t_\nu} = \exp\left(\sum_{\nu=1}^{n} t_\nu \log_p \alpha_{\nu,\mu}\right), \quad (1 \leqq \mu \leqq m)$$

sont algébriques.

a) *Si les m éléments de* K^n

$$(\log_p \alpha_{1,\mu}, \ldots, \log_p \alpha_{n,\mu}) \quad (1 \leqq \mu \leqq m)$$

sont $\mathbb{Q}$*-linéairement indépendants, alors* $1, t_1, \ldots, t_n$ *sont* $\mathbb{Q}$*-linéairement dépendants.*

b) *Si de plus la matrice*

$$M = (\log_p \alpha_{\nu,\mu})_{1 \leqq \nu \leqq n,\, 1 \leqq \mu \leqq m}$$

vérifie

$$\theta(M) > n,$$

alors $t_1, \ldots, t_n$ *sont tous rationnels.*

Le corollaire 1.2.p permet de montrer que, si ρ est une représentation p-adique semi-simple abélienne et rationnelle du groupe de Galois absolu d'un corps de nombres k, alors ρ est localement algébrique au sens de [5]. Cet énoncé, quand k est composé d'extensions quadratiques de $\mathbb{Q}$, a été déduit par Serre du théorème p-adique des six exponentielles [5]. Pour le cas général, voir un exposé de Henniart au séminaire de théorie des nombres Delange Pisot Poitou en 1980/81 (Progress in Math., Birkhäuser Verlag).

§ 2. Dépendance de logarithmes *p*-adiques de nombres algébriques

Voici l'analogue p-adique du corollaire 7.2 de la première partie.

Théorème 2.1.p. *Soient* $\alpha_{i,j}$ *des éléments non nuls de K algébriques sur* $\mathbb{Q}$. *Soit* r_p *le rang de la matrice*

$$M_p = (\log_p \alpha_{i,j})_{1 \leqq i \leqq d,\, 1 \leqq j \leqq \ell}.$$

Alors

$$r_p \geqq d\,\theta(M_p)/(1 + \theta(M_p)).$$

Nous en déduirons (au § 5) le corollaire suivant.

Corollaire 2.2.p. *Soient k un corps de nombres,* φ *un plongement de k dans* $\mathbb{C}$, *et* φ_p *un plongement de k dans K. Soient* $\alpha_{i,j}$ *des éléments de k tels que*

$$\varphi_p \alpha_{i,j} \in \mathscr{U} \quad \text{pour } 1 \leqq i \leqq d,\ 1 \leqq j \leqq \ell.$$

On note r le rang de la matrice

$$M = (\log |\varphi \alpha_{i,j}|)_{1 \leqq i \leqq d,\, 1 \leqq j \leqq \ell},$$

où log *désigne le logarithme usuel, et* r_p *le rang de la matrice*

$$M_p = (\log_p \varphi_p \alpha_{i,j})_{1 \leqq i \leqq d,\, 1 \leqq j \leqq \ell}.$$

Alors

$$r_p \geqq r/2.$$

Ainsi le rang p-adique du groupe des unités d'un corps de nombres est au moins égal à la moitié du nombre de Dirichlet. La conjecture de Leopoldt stipule que ces deux nombres doivent être égaux. D'autres minorations du rang p-adique du groupe des unités sont dues à Ax et Brumer, et, plus récemment, à Kisilevsky et Wales, et à M. Emsalem.

Nous verrons d'autre part que la conjecture de Schanuel p-adique permettrait de montrer, sous les hypothèses du corollaire 2.2.p, l'inégalité $r_p \geqq r$.

§ 3. Construction d'une fonction auxiliaire

Pour R réel positif, on désigne par

$$B(0, R^+) = \{z \in K^n, |z| \leqq R\}$$

le polydisque circonférencié de rayon R, où

$$|z| = \max_{1 \leqq \nu \leqq n} |z_\nu|$$

désigne la norme ultramétrique sur K^n.

On dira qu'une fonction f définie sur $B(0, R^+)$ et à valeurs dans K est analytique dans ce polydisque si

$$f(z) = \sum_{\tau \in \mathbb{N}^n} a_\tau z^\tau \quad \text{pour } z \in B(0, R^+),$$

où

$$\lim_{\|\tau\| \to \infty} |a_\tau| R^{\|\tau\|} = 0.$$

Pour $0 \leqq r \leqq R$ on pose

$$|f|_r = \sup_{\tau \in \mathbb{N}^n} (|a_\tau| r^{\|\tau\|}),$$

et on a

$$|f(z)| \leqq |f|_r \quad \text{pour } z \in B(0, r^+).$$

De plus, si la valuation de K est dense, on a

$$|f|_r = \sup \{|f(z)|,\ z \in B(0, r^+)\}.$$

Dans tout ce paragraphe 3, nous supposons que K est localement compact, et nous notons δ son degré sur $\mathbb{Q}_p$.

a) Enoncés des résultats

Voici d'abord la fonction auxiliaire.

Théorème 3.1.p. *Soient L et n deux entiers positifs, S, U, R, r des nombres réels positifs, et $\varphi_1, \ldots, \varphi_L$ des fonctions analytiques dans le polydisque $B(0, R^+)$ de K^n.*

On suppose

$$\log p \leqq U, \quad S \leqq U, \quad 1 < R/r \leqq e^U,$$
$$|\varphi_\lambda|_R \leqq e^U, \quad (1 \leqq \lambda \leqq L),$$

et

$$\delta(4U)^{n+1} \leqq LS\left(\log \frac{R}{r}\right)^n.$$

Alors il existe des entiers rationnels non tous nuls $q_1, \ldots, q_L$, *avec*

$$-e^S \leqq q_\lambda \leqq e^S, \quad (1 \leqq \lambda \leqq L),$$

tels que la fonction

$$F = \sum_{\lambda=1}^{L} q_\lambda \varphi_\lambda$$

vérifie

$$|F|_r \leqq e^{-U}$$

Nous allons en déduire le corollaire suivant.

Corollaire 3.2.p. *Soient* $x_1, \ldots, x_d$ *des éléments de* K^n, *avec* $d > n$. *Soit* r *un nombre réel positif tel que pour tout* $z \in B(0, r^+)$, *on ait*

$$\langle x_i, z \rangle \in E \quad \text{pour } 1 \leqq i \leqq d.$$

Il existe un entier $N_0 > 0$ *et une suite* $(P_N)_{N \geqq N_0}$ *de polynômes non nuls de* $\mathbb{Z}[T_1, \ldots, T_d]$, *avec*

$$\deg_{T_i} P_N < N^{n/(d-n)}(\log N)^{n+2}, \quad (1 \leqq i \leqq d),$$

et

$$\log H(P_N) \leqq N^{d/(d-n)}(\log N)^{n+2},$$

telle que les fonctions

$$F_N(z) = P_N(\exp\langle x_1, z\rangle, \ldots, \exp\langle x_d, z\rangle)$$

vérifient

$$|F_N|_r \leqq \exp\{-N^{d/(d-n)}(\log N)^{d+2}\}.$$

Démonstration du corollaire 3.2.p. On choisit un nombre $R > r$ tel que le polydisque $B(0, R^+)$ soit contenu dans

$$\{z \in K^n;\ \langle x_i, z\rangle \in E \text{ pour } 1 \leqq i \leqq d\}.$$

Notons que les valeurs de la fonction exponentielle sont des unités. Le reste de la démonstration est identique à celle du corollaire 3.2 de la première partie.

b) Un lemme de Siegel

Rappelons que $\mathcal{O}$ désigne l'anneau de valuation de K.

Lemme 3.3.p. *Soient* A *et* B *deux entiers positifs, et* $u_{i,j}$, $(1 \leqq i \leqq \nu,\ 1 \leqq j \leqq \mu)$ *des éléments de* $\mathcal{O}$. *On suppose*

$$p^{\delta B \mu} < (A+1)^\nu.$$

Alors il existe des entiers rationnels $a_1, \ldots, a_v$, *non tous nuls, vérifiant*

$$-A \leqq a_i \leqq A, \qquad (1 \leqq i \leqq v),$$

tels que

$$v\left(\sum_{i=1}^{v} u_{i,j} a_i\right) \geqq B \qquad \textit{pour } 1 \leqq j \leqq \mu.$$

Démonstration. Si π est une uniformisante de K, e l'indice de ramification de K sur $\mathbb{Q}_p$, et g le degré résiduel, on a

$$\delta = eg, \qquad v(\pi) = 1/e,$$

et le corps des restes de K est un corps fini à $q = p^g$ éléments. Soit $h = Be$. Il y a q^h classes résiduelles dans $\mathcal{O}$ modulo π^h. Considérons les $(A+1)^v$ éléments de K^μ:

$$\left(\sum_{i=1}^{v} u_{i,j} a_i\right)_{1 \leqq j \leqq \mu}, \qquad (0 \leqq a_i \leqq A,\ a_i \in \mathbb{Z}).$$

Comme

$$q^{h\mu} < (A+1)^v,$$

le principe des tiroirs montre qu'il existe $a' \in \mathbb{Z}^v$ et $a'' \in \mathbb{Z}^v$ avec

$$a' \neq a'', \qquad 0 \leqq a_i' \leqq A, \qquad 0 \leqq a_i'' \leqq A,$$

et

$$\sum_{i=1}^{v} u_{i,j} a_i' \equiv \sum_{i=1}^{v} u_{i,j} a_i'' \bmod \pi^h, \qquad (1 \leqq j \leqq \mu).$$

On pose alors

$$a_i = a_i' - a_i'', \qquad (1 \leqq i \leqq v).$$

c) Formule d'interpolation

Lemme 3.4.p. *Soient r et R des nombres réels avec $0 < r < R$, T un entier positif, et F une fonction analytique dans le polydisque $B(0, R^+)$ de K^n. Alors*

$$|F|_r \leqq \max\{(r/R)^T |F|_R;\ \max_{\|\tau\| < T} |D^\tau F(0)| r^{\|\tau\|} / |\tau!|\}.$$

Démonstration. Il suffit de remarquer que pour $\|\tau\| \geqq T$, on a $r^{\|\tau\|} \leqq (r/R)^T R^{\|\tau\|}$.

d) Démonstration du théorème 3.1.p.

On définit un nombre réel T_0 par

$$(R/r)^{T_0} = e^{3U},$$

et on désigne par T le plus petit entier $\geqq T_0$. L'hypothèse $R/r \leqq e^U$ implique $T_0 \geqq 3$, donc $T < T_0 + 1 \leqq \frac{4}{3} T_0$. On va construire les entiers $q_1, \ldots, q_L$ de telle sorte que la fonction

$$F = q_1 \varphi_1 + \ldots + q_L \varphi_L$$

vérifie

$$|D^\tau F(0)| r^{\|\tau\|}/|\tau!| \leqq e^{-U} \quad \text{pour} \quad \|\tau\| < T.$$

Pour cela on choisit des éléments $c_\tau \in K$ vérifiant

$$|D^\tau \varphi_\lambda(0) c_\tau/\tau!| \leqq 1$$

et

$$|c_\tau| \geqq e^{-U\|\tau\|},$$

et on considère le système d'inéquations

$$\left| \sum_{\lambda=1}^{L} q_\lambda D^\tau \varphi_\lambda(0)\, c_\tau/\tau! \right| \leqq p^{-B}, \quad (\|\tau\| < T),$$

où B est de plus petit entier $\geqq 2U/\log p$. Comme $U \geqq \log p$, on a $B < 3U/\log p$ et

$$B(\log p)\, T^n < LS.$$

On peut donc utiliser le lemme 3.3.p avec

$$\mu = \binom{T+n-1}{n} \leqq T^n, \quad v = L, \quad A = [e^S],$$

et on obtient une solution non triviale $q_1, \ldots, q_L$ avec

$$-e^S \leqq q_\lambda \leqq e^S \quad (1 \leqq \lambda \leqq L).$$

Des inégalités

$$|F|_R \leqq e^{S+U} \leqq e^{2U}$$

on déduit

$$(r/R)^T |F|_R \leqq e^{-U},$$

et le lemme 3.4.p permet de conclure.

§ 4. Théorème de Masser et conséquences

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 K^n de rang d et ℓ respectivement. Notons

$$\chi_0(Y, X) = \min_{X', Y'} \{(\ell - \operatorname{rang}_{\mathbb{Z}} Y')/\operatorname{rang}_{\mathbb{Z}} X'\},$$

où X' décrit les sous-$\mathbb{Z}$-modules de X, et Y' les sous-$\mathbb{Z}$-modules de Y, avec $X' \neq 0$ et $\langle X', Y' \rangle = 0$.

Pour N entier positif notons

$$Y_N = \{m_1 y_1 + \ldots + m_\ell y_\ell;\ m_j \in \mathbb{Z},\ 0 \leqq m_j \leqq N,\ (1 \leqq j \leqq \ell)\}.$$

Nous utiliserons le corollaire suivant de la proposition de [2] (cf. l'avant dernière remarque du § 7 de [2]).

Théorème 4.1.p. (Masser). *On suppose* $\langle X, Y\rangle \subset E$. *Soit* $P \in K[T_1, \ldots, T_d]$ *un polynôme non nul de degré total au plus D, avec* $D \geqq 1$. *Soit N un entier positif. Si la fonction*

$$\phi(z) = P(\exp\langle x_1, z\rangle, \ldots, \exp\langle x_d, z\rangle)$$

vérifie

$$\phi(y) = 0 \quad \textit{pour tout } y \in Y_N,$$

alors

$$D \geqq (N/d)^{\chi_0(Y,X)}.$$

En combinant ce résultat avec le corollaire 3.2.p, nous allons obtenir l'énoncé suivant.

Corollaire 4.2.p. *On suppose*

$$\langle X, Y\rangle \subset E, \quad d > n \quad \textit{et} \quad \mu(Y) > 0.$$

Si les nombres

$$\exp\langle x_i, y_j\rangle, \quad (1 \leqq i \leqq d, 1 \leqq j \leqq \ell)$$

sont tous algébriques, alors

$$\chi_0(Y, X) \leqq n/(d-n).$$

Démonstration du corollaire 4.2.p. Comme le corps K n'est pas supposé localement compact, il faut quelques précautions pour utiliser le corollaire 3.2.p.

L'hypothèse $\mu(Y) > 0$ permet de choisir n éléments $e_1, \ldots, e_n$ de Y linéairement indépendants sur K. Soit $(f_1, \ldots, f_n)$ la base de K^n duale de $(e_1, \ldots, e_n)$:

$$\langle e_h, f_k\rangle = \delta_{h,k}, \quad (1 \leqq h,\ k \leqq n),$$

où $\delta_{h,k}$ est le symbole de Kronecker. On définit des éléments $x'_1, \ldots, x'_d$ et $y'_1, \ldots, y'_\ell$ de K^n par

$$x'_i = (\langle x_i, e_h\rangle)_{1 \leqq h \leqq n}, \quad (1 \leqq i \leqq d)$$

et

$$y'_j = (\langle y_j, f_k\rangle)_{1 \leqq k \leqq n}, \quad (1 \leqq j \leqq \ell).$$

Ainsi

$$\langle x'_i, y'_j\rangle = \langle x_i, y_j\rangle, \quad (1 \leqq i \leqq d,\ 1 \leqq j \leqq \ell).$$

Soit a un entier rationnel tel que les éléments $x''_1, \ldots, x''_d$ de K^n définis par

$$x''_i = p^a x'_i, \quad (1 \leqq i \leqq d)$$

vérifient

$$|x''_i| < p^{-1/(p-1)}, \quad (1 \leqq i \leqq d),$$

et soit b un entier rationnel tel que les éléments $y''_1, \ldots, y''_\ell$ de K^n définis par

$$y''_j = p^b y'_j, \quad (1 \leqq j \leqq \ell)$$

vérifient

$$|y''_j| \leqq 1, \quad (1 \leqq j \leqq \ell).$$

On pose

$$X'' = \mathbb{Z}x_1'' + \ldots + \mathbb{Z}x_d''$$

et

$$Y'' = \mathbb{Z}y_1'' + \ldots + \mathbb{Z}y_\ell''.$$

On a évidemment

$$\operatorname{rang}_{\mathbb{Z}} X'' = d, \quad \operatorname{rang}_{\mathbb{Z}} Y'' = \ell, \quad \chi_0(Y'', X'') = \chi_0(Y, X),$$

et

$$\exp\langle x_i'', y_j''\rangle \in \overline{\mathbb{Q}}, \quad (1 \leqq i \leqq d,\ 1 \leqq j \leqq \ell).$$

De plus le corps K_0 obtenu en adjoignant à $\mathbb{Q}_p$ les dn nombres

$$\langle x_i, e_h\rangle, \quad (1 \leqq i \leqq d,\ 1 \leqq h \leqq n)$$

est localement compact, et $x_i'' \in K_0^n$, $(1 \leqq i \leqq d)$. On peut maintenant utiliser le corollaire 3.2.p avec $r=1$, en y remplaçant K par K_0 et x_i par x_i''. La fonction F_N ainsi construite induit une fonction analytique sur le polydisque unité de K^n, et on obtient comme dans la première partie

$$F_N(y) = 0 \quad \text{pour } y \in Y_N''.$$

Le théorème 4.1.p implique alors

$$\chi_0(Y'', X'') \leqq n/(d-n).$$

Le corollaire 4.2.p en résulte.

§ 5. Démonstrations

a) Démonstrations des énoncés 1.1.p, 1.2.p et 2.1.p.

Le théorème 1.1.p se déduit du corollaire 4.2.p grâce aux arguments donnés dans la première partie (§ 6a). (Le remplacement de χ par χ_0 permet d'ailleurs de simplifier cette démonstration pour le cas p-adique).

Il en est de même pour la démonstration du corollaire 1.2.p (cf. première partie, § 7b) et pour celle du théorème 2.1.p (cf. première partie § 6c et § 7c), une fois que l'on s'est ramené au cas où les nombres algébriques $\alpha_{\nu,\mu}$ ou $\alpha_{i,j}$ appartiennent à $1+E$, ce que l'on peut réaliser grâce à la remarque suivante.

Soit α un élément non nul de K, algébrique sur $\mathbb{Q}$. Soit a un entier rationnel tel que $p^a \log_p \alpha \in E$ (il suffit de prendre a suffisamment grand). Alors le nombre

$$\tilde{\alpha} = \exp(p^a \log_p \alpha)$$

est algébrique sur $\mathbb{Q}$, appartient à $1+E$, et vérifie

$$\log_p \tilde{\alpha} = p^a \log_p \alpha.$$

(On notera que si, par exemple, $\alpha \notin 1+\mathscr{M}$, alors $\tilde{\alpha} \neq \alpha^{p^a}$.)

b) Lien avec le théorème 2 de Serre [4]

Soit G un groupe topologique isomorphe à $(\mathbb{Z}_p)^r$, où $\mathbb{Z}_p$ désigne le groupe des entiers p-adiques. Soit A un sous-groupe libre de type fini de G de rang a. On définit

$$\mu = \mu(A, G) = \min_W \{(\operatorname{rang} A \cap W)/\operatorname{codim} W\},$$

où W décrit les sous-$\mathbb{Z}_p$-modules de G, avec $W \neq G$.

Soient e_i, $(1 \leqq i \leqq b)$ des homomorphismes continus de G dans K^*. L'analogue p-adique de la proposition 6.1 donne l'énoncé suivant.

Proposition 5.1.p. *Supposons que tous les $e_i(x)$, $(x \in A,\ 1 \leqq i \leqq b)$ soient algébriques sur $\mathbb{Q}$. Si $\mu > 1$ et $b > \mu r/(1-\mu)$, alors les e_i sont multiplicativement dépendants.*

Pour en déduire le théorème 2 de [4], il suffit de remarquer que si A est λ-dense dans G au sens de [4], alors $\lambda\mu \geqq 1$ (cf. Bertrand. Appendice I de [7], § 2.2 et § 2.3).

c) Démonstration du corollaire 2.2.p

Nous commençons par démontrer le lemme suivant.

Lemme 5.2.p. *Sous les hypothèses du corollaire* 2.2.p., *on a*

$$\theta(M_p) \geqq \theta(M).$$

Démonstration du lemme 5.2.p. Si $a_{i,j}$ sont des nombres rationnels pour lesquels

$$\sum_{i=1}^{d} \sum_{j=1}^{\ell} a_{i,j} \log_p \varphi_p \alpha_{i,j} = 0,$$

alors le nombre

$$\prod_{i=1}^{d} \prod_{j=1}^{\ell} \alpha_{i,j}^{a_{i,j}}$$

est une racine de l'unité (on a supposé $\varphi_p \alpha_{i,j} \in \mathscr{U}$), donc

$$\sum_{i=1}^{d} \sum_{j=1}^{\ell} a_{i,j} \log |\varphi \alpha_{i,j}| = 0.$$

Le lemme 5.2.p en résulte.

Démonstration du corollaire 2.2.p. On extrait de M une matrice carrée $r \times r$ inversible que l'on note

$$M' = (\log |\varphi \beta_{s,t}|)_{1 \leqq s,\, t \leqq r}.$$

On considère la matrice carrée correspondante extraite de M_p:

$$M'_p = (\log_p \varphi_p \beta_{s,t})_{1 \leqq s,\, t \leqq r}.$$

Comme M' est inversible on a $\theta(M') = 1$, et le lemme 5.2.p entraîne $\theta(M'_p) = 1$. Alors du théorème 2.1.p on déduit

$$\operatorname{rang} M_p \geqq \operatorname{rang} M'_p \geqq r\theta(M'_p)/(1 + \theta(M'_p)) = r/2.$$

Pour terminer voici l' analogue p-adique de la conjecture de Schanuel.

Conjecture de Schanuel p-adique. *Soient $x_1, \ldots, x_n$ des éléments de E linéairement indépendants sur $\mathbb{Q}$. Alors le degré de transcendance sur $\mathbb{Q}$ du corps*

$$\mathbb{Q}(x_1, \ldots, x_n, \exp x_1, \ldots, \exp x_n)$$

est supérieur ou égal à n.

On déduit de cette conjecture que si $\alpha_1, \ldots, \alpha_m$ sont des éléments de K^* algébriques sur $\mathbb{Q}$, l'idéal des $P \in \mathbb{Q}[X_1, \ldots, X_m]$ tels que

$$P(\log_p \alpha_1, \ldots, \log_p \alpha_m) = 0$$

est engendré par des formes linéaires. Il en résulte facilement que sous les hypothèses du corollaire 2.2.p. la conjecture de Schanuel p-adique implique $r_p \geqq r$.

References

1. Lang, S.: Introduction to transcendental numbers, Reading, Mass.: Addison-Wesley 1966
2. Masser, D.W.: On polynomials and exponential polynomials in several complex variables. Invent. math. **63**, 81–95 (1981)
3. Mignotte, M., Waldschmidt, M.: Approximation des valeurs de fonctions transcendantes, Koninkl. Nederl. Akad. van Wet., Proc. Ser. A, **78**, 213–223 (1975)
4. Serre, J-P.: Dépendance d'exponentielles p-adiques. Séminaire Delange Pisot Poitou (Théorie des Nombres), 7è année, n° 15 (1965/66)
5. Serre, J-P.: Abelian ℓ-adic representations and elliptic curves. New York: Benjamin 1968
6. Waldschmidt, M.: Propriétés arithmétiques de fonctions de plusieurs variables. Séminaire P. Lelong-H. Skoda (Analyse), 19è année, n° 20 (1978/79): Lecture Notes in Math., vol. 822, p. 332–356 (1980)
7. Waldschmidt, M.: Nombres transcendants et groupes algébriques, Astérisque 69–70 (Société Mathématique de France) 1979
8. Weil, A.: On a certain type of characters of the idèle class-group of an algebraic number field; Proc. Intern. Symp. Alg. Geom., Tokyo Nikko 1955, Tokyo (1956)

Reçu le 20 Septembre 1980