Annals of Mathematics, 117 (1983), 627–657

Sous-groupes analytiques de groupes algébriques

Par MICHEL WALDSCHMIDT

Soient G un groupe algébrique défini sur la clôture algébrique $\overline{\mathbf{Q}}$ de $\mathbf{Q}$ dans $\mathbf{C}$, et φ: $\mathbf{C}^n \to G(\mathbf{C})$ un homomorphisme analytique. En général, $\varphi(\mathbf{C}^n)$ n'est pas un sous-groupe algébrique de $G(\mathbf{C})$, mais s'enroule autour de son adhérence de Zariski. Nous allons donner des conditions arithmétiques qui assurent que l'image est fermée.

Ce problème a été étudié d'abord par Lang [2, Chap. II] pour les sous-groupes à un paramètre. On sait maintenant que pour $n = 1$, il suffit qu'il existe 5 nombres complexes, linéairement indépendants sur $\mathbf{Z}$, dont les images par φ soient dans $G(\overline{\mathbf{Q}})$, pour assurer que $\varphi(\mathbf{C})$ est fermé (cf. [9, Th. 4.2.1]; l'hypothèse que G est commutatif et connexe n'est pas restrictive).

Dans le cas général ($n \geq 1$), les premiers résultats sur ce sujet ont été obtenus par Bombieri et Lang [1]. Les énoncés antérieurs de Lang [2] ne concernaient que les sous-groupes "normalisés" (voir aussi [9, Chap. 3 et 5]) dont nous ne parlerons pas ici. L'intérêt d'obtenir des résultats sans hypothèse de normalisation avait été souligné par Lang dans [2, pp. 20, 39 et 44]. Les énoncés de Bombieri et Lang [1] (voir aussi [9, §8.2]) imposaient des conditions sévères sur l'approximation diophantienne des logarithmes. Ces conditions provenaient d'une estimation analytique, le lemme de Schwarz.

En poursuivant la méthode de Bombieri et Lang, mais en remplaçant leur estimation analytique par un lemme de Schwarz conjectural, nous avons montré dans [9, Chap. 8] comment les hypothèses diophantiennes devraient pouvoir être remplacées par des conditions d'algèbre linéaire. Jusqu'à présent ce lemme de Schwarz n'a été démontré que dans quelques cas particuliers [9, Chap. 7].

Nous utilisons ici une approche différente, qui évite le lemme de Schwarz, mais qui utilise un résultat puissant, le "lemme de zéros" de Masser et Wüstholz [4]. Les résultats auxquels nous arrivons sont précisément ceux qui ont été conjecturés dans [9], notamment le problème 8.2.3 de [9]. Le cas $G = \mathbf{G}_m^d$ (où $\mathbf{G}_m$ est le groupe multiplicatif) avait été résolu dans [10], et nous généralisons ici la méthode de [10] pour l'adapter à un groupe algébrique quelconque.

Pour arriver à la conclusion que $\varphi(\mathbf{C}^n)$ est fermé, nous supposerons que $G(\overline{\mathbf{Q}})$ contient beaucoup de points de l'image de φ, disons $\varphi(Y) \subset G(\overline{\mathbf{Q}})$, où $Y = \mathbf{Z}y_1 + \cdots + \mathbf{Z}y_m$ est un sous-groupe de $\mathbf{C}^n$ de rang m sur $\mathbf{Z}$. Nous supposerons donc m grand: $m \geq 2n^2 + 2n + 1$. Quand G est une variété abélienne simple et que la différentielle de φ à l'origine est injective, cette hypothèse sur m suffit (on obtient dans ce cas $\varphi(\mathbf{C}^n) = G(\mathbf{C})$ et $\dim G = n$). Mais dans le cas général on voit facilement que cette hypothèse n'est pas suffisante. Le résultat que nous établirons montrera que la condition suivante suffit: on suppose que, pour tout sous-espace W de $\mathbf{C}^n$, $W \neq \mathbf{C}^n$, on a

$$\operatorname{rang}_{\mathbf{Z}}(Y/Y \cap W) > 2(n+1)\dim_{\mathbf{C}}(\mathbf{C}^n/W).$$

Autrement dit on demande à Y de ne pas avoir presque tous ses éléments dans un sous-espace strict de $\mathbf{C}^n$. Cette hypothèse implique (en prenant $W = 0$) $m > 2n(n+1)$. D'autre part pour $n = 1$ on retrouve l'énoncé que nous avions cité au début sur les sous-groupes à un paramètre. Si G est un groupe linéaire nous verrons que l'hypothèse précédente peut être remplacée par

$$\operatorname{rang}_{\mathbf{Z}}(Y/Y \cap W) > (n+1)\dim_{\mathbf{C}}(\mathbf{C}^n/W).$$

On peut obtenir des énoncés plus précis en tenant compte des périodes de φ. Les démonstrations que nous donnerons vont se faire par récurrence sur n, et pour cette récurrence il semble indispensable d'avoir des résultats plus fins quand φ est périodique. Bien entendu, cette difficulté disparait dans la cas p-adique.

Enfin la méthode que nous utilisons se prête très bien à l'étude de l'indépendance algébrique. Moyennant des hypothèses convenables, on peut remplacer partout $\overline{\mathbf{Q}}$ par une extension de $\mathbf{Q}$ de degré de transcendance 1.

Nous énonçons d'abord (§1) les principaux résultats, sans faire intervenir les périodes éventuelles de φ. Les énoncés plus précis seront donnés avec les démonstrations (§4), qui utiliseront d'une part une fonction auxiliaire (§2), d'autre part le lemme de zéros de Masser et Wüstholz (§3b), et enfin des propriétés des coefficients de Dirichlet généralisés (§3a et 3c). Au paragraphe 5 nous étudions l'indépendance algébrique, et au paragraphe 6 nous présentons des résultats complémentaires qui seront développés ailleurs.

Afin d'unifier les énoncés nous introduisons un nombre $\rho = \rho(G)$ défini par

$$\rho = \begin{cases} 1 & \text{si } G \text{ est linéaire} \\ 2 & \text{sinon.} \end{cases}$$

Quand φ: $\mathbf{C}^n \to G(\mathbf{C})$ est un homomorphisme analytique, on définit $\kappa = \kappa(\varphi)$

par

$$\kappa = \begin{cases} \operatorname{rang}_{\mathbf{C}} \ker \varphi & \text{si } \rho = 1, \\ \operatorname{rang}_{\mathbf{R}} \ker \varphi & \text{si } \rho = 2. \end{cases}$$

Ainsi $\kappa \leq \rho n$. Enfin les conditions suivantes sont équivalentes:

(i) La différentielle $\mathfrak{L}$: $\mathbf{C}^n \to T_G(\mathbf{C})$ de φ en 0 est injective,

(ii) $\ker \varphi$ est discret dans $\mathbf{C}^n$,

(iii) $\kappa = \operatorname{rang}_{\mathbf{Z}} \ker \varphi$.

Si ces conditions sont satisfaites, on dira, en suivant [1], que φ est un sous-groupe à n paramètres de G.

1. Dimension algébrique de sous-groupes analytiques de groupes algébriques

On considère un groupe algébrique G, défini sur $\overline{\mathbf{Q}}$, et un homomorphisme analytique φ: $\mathbf{C}^n \to G(\mathbf{C})$. On s'intéresse aux sous-groupes Y de $\mathbf{C}^n$, de type fini, tels que $\varphi(Y) \subset G(\overline{\mathbf{Q}})$.

Les notations seront les suivantes. L'espace tangent à l'origine de $G(\mathbf{C})$ sera noté $T_G(\mathbf{C})$, $\exp_G$: $T_G(\mathbf{C}) \to G(\mathbf{C})$ sera l'application exponentielle de G, et $\mathfrak{L}$: $\mathbf{C}^n \to T_G(\mathbf{C})$ la différentielle de φ en 0. Ainsi $\varphi = \exp_G \circ \mathfrak{L}$. Enfin m sera le rang sur $\mathbf{Z}$ de Y, et d la dimension de φ, c'est-à-dire la dimension algébrique de l'adhérence de Zariski $\overline{\varphi(\mathbf{C}^n)}$ sur $\overline{\mathbf{Q}}$ de $\varphi(\mathbf{C}^n)$. On a $\overline{\varphi(\mathbf{C}^n)} = H(\mathbf{C})$, où H est un groupe algébrique commutatif connexe défini sur $\overline{\mathbf{Q}}$.

Voici quelques exemples.

1. Soit A une variété abélienne simple définie sur $\overline{\mathbf{Q}}$. On considère des périodes $\omega_1, \ldots, \omega_n$ dans $T_A(\mathbf{C})$, c'est-à-dire des éléments du noyau de $\exp_A$. On pose $G = \mathbf{G}_a^n \times A$, où $\mathbf{G}_a$ est le groupe additif, et on définit φ: $\mathbf{C}^n \to G(\mathbf{C})$ par

$$\varphi(z) = \big(z, \exp_A(z_1\omega_1 + \cdots + z_n\omega_n)\big)$$

pour $z = (z_1, \ldots, z_n) \in \mathbf{C}^n$. On peut alors prendre $Y = \mathbf{Z}^n$. Puisque A est simple, il suffit que $\omega_1, \ldots, \omega_n$ ne soient pas tous nuls pour que la dimension algébrique de φ soit $n + \dim A$ (cf. [9, p. 28]).

2. Soit E une courbe elliptique ayant des multiplications complexes dans un corps imaginaire quadratique $k = \mathbf{Q}(\tau)$. Soient $u_1, \ldots, u_{d-1}$ des éléments de $T_E(\mathbf{C})$, linéairement indépendants sur k, tels que $\exp_E u_j \in E(\overline{\mathbf{Q}})$, $(1 \leq j < d)$. On prend $G = \mathbf{G}_a \times E^{d-1}$, $n = 1$, $m = 2$, $Y = \mathbf{Z} + \mathbf{Z}\tau$, et

$$\varphi(z) = (z, \exp_E zu_1, \ldots, \exp_E zu_{d-1}), \qquad (z \in \mathbf{C}).$$

3. Supposons G commutatif connexe de dimension $d \geq 1$, et prenons $n = d$. Nous choisissons un isomorphisme $\mathfrak{L}: \mathbf{C}^n \to T_G(\mathbf{C})$, (ce qui revient à choisir une base de $T_G(\mathbf{C})$). Comme $G(\overline{\mathbf{Q}})$ n'a pas un rang fini sur $\mathbf{Z}$, pour chaque $m \geq 1$ on peut choisir m éléments $\mathbf{Q}$-linéairement indépendants dans $\mathbf{C}^n$ dont les images par $\varphi = \exp_G \circ \mathfrak{L}$ sont dans $G(\overline{\mathbf{Q}})$.

Dans les deux premiers exemples, m est petit (mais d n'est pas borné), alors que dans le troisième, m est quelconque, mais $d = n$. On obtient des exemples moins triviaux, dans lesquels ni m, ni d ne sont bornés en fonction de n, en prenant des produits directs: si on part de deux exemples (G_1, φ_1, Y_1) et (G_2, φ_2, Y_2), on peut considérer $G = G_1 \times G_2$, $Y = Y_1 \times Y_2$, et $\varphi: \mathbf{C}^{n_1} \times \mathbf{C}^{n_2} \to G(\mathbf{C})$ défini par:

$$\varphi(z_1, z_2) = \big(\varphi_1(z_1), \varphi_2(z_2)\big).$$

Plus généralement, l'exemple 3 montre que, si $\varphi: \mathbf{C}^n \to G(\mathbf{C})$ est tel qu'il existe un sous-espace vectoriel V de $\mathbf{C}^n$, $V \neq 0$, pour lequel l'adhérence de Zariski sur $\overline{\mathbf{Q}}$ de $\varphi(V)$ dans G a une dimension algébrique égale à la dimension de V sur $\mathbf{C}$, alors le sous-groupe

$$\{y \in \mathbf{C}^n; \varphi(y) \in G(\overline{\mathbf{Q}})\}$$

de $\mathbf{C}^n$ n'a pas un rang fini sur $\mathbf{Z}$.

Dans le cas général, nous allons montrer que, si m et d sont suffisamment grands en fonction de n, alors

a) beaucoup de points de $\varphi(Y)$ sont dans un sous-groupe algébrique strict de G,

b) beaucoup de points de Y sont dans un sous-espace strict de $\mathbf{C}^n$, et

c) il existe un sous-espace strict de $\mathbf{C}^n$ tel que la dimension algébrique de son image par φ soit petite.

Voici l'énoncé précis.

THÉORÈME 1.1. *Soient G un groupe algébrique défini sur $\overline{\mathbf{Q}}$ de dimension d, φ: $\mathbf{C}^n \to G(\mathbf{C})$ un sous-groupe à n paramètres de G, de dimension d, et Y un sous-groupe de $\mathbf{C}^n$ de rang m sur $\mathbf{Z}$ tel que $\varphi(Y) \subset G(\overline{\mathbf{Q}})$. On note $\rho = \rho(G)$ et on suppose*

$$md > n(m + d\rho).$$

Alors il existe un sous-espace vectoriel V de $\mathbf{C}^n$ tel que, si H désigne l'adhérence de Zariski sur $\overline{\mathbf{Q}}$ de $\varphi(V)$, et si on note

$$n_1 = \dim_{\mathbf{C}}(\mathbf{C}^n/V),\ d_1 = \dim(G/H),\ et\ m_1 = \operatorname{rang}_{\mathbf{Z}}(Y/Y \cap V),$$

on ait

$$n_1 > 0,\ d_1/n_1 > d/n,\ et\ m_1 d_1 \leq n_1(m_1 + d_1\rho).$$

Ces inégalités impliquent

$$\frac{\operatorname{rang}_{\mathbf{Z}}(Y/Y \cap V)}{\dim_{\mathbf{C}}(\mathbf{C}^n/V)} = \frac{m_1}{n_1} < \frac{d\rho}{d-n}.$$

De plus, si on note $\Gamma = \varphi(Y)$, on a

$$\frac{\operatorname{rang}_{\mathbf{Z}}(\Gamma/\Gamma \cap H)}{\dim(G/H)} \leq \frac{m_1}{d_1} < \frac{n\rho}{d-n}.$$

Choisissons un sous-espace V_1 supplémentaire de V dans $\mathbf{C}^n$, écrivons $V_2 = V$, et définissons φ_1 et φ_2, homomorphismes de $\mathbf{C}^n$ dans $G(\mathbf{C})$, par

$$\varphi_1(v_1 + v_2) = \varphi(v_1), \varphi_2(v_1 + v_2) = \varphi(v_2), \qquad (v_1 \in V_1, v_2 \in V_2).$$

Alors H est l'adhérence de Zariski sur $\overline{\mathbf{Q}}$ de $\varphi_2(\mathbf{C}^n)$, donc φ_2 a une dimension algébrique égale à $d - d_1$. D'autre part, si on note $Y_2 = Y \cap V_2$, on peut choisir un sous-groupe Y_1 de Y tel que $Y = Y_1 \oplus Y_2$, et on a

$$\varphi_1(Y_2) = 0, \text{ et } \operatorname{rang}_{\mathbf{Z}} Y_1 = m_1.$$

Quand $G = \mathbf{G}_m^d$, on retrouve le théorème 1.1 de [10] en choisissant

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

et en utilisant les caractérisations classiques des sous-groupes algébriques de $\mathbf{G}_m^d$ (par exemple [4, §7]).

COROLLAIRE 1.2. *Soient A une variété abélienne simple de dimension d définie sur $\overline{\mathbf{Q}}$, φ: $\mathbf{C}^n \to A(\mathbf{C})$ un sous-groupe à n paramètres de A, et Y un sous-groupe de $\mathbf{C}^n$ de rang m sur $\mathbf{Z}$ tel que $\varphi(Y) \subset A(\overline{\mathbf{Q}})$. Alors*

$$md \leq n(m + 2d).$$

En particulier, si $m \geq 2n^2 + 2n + 1$, on trouve $d < n + 1$, donc $d = n$, et $\varphi(\mathbf{C}^n) = A(\mathbf{C})$.

COROLLAIRE 1.3. *Soient G un groupe algébrique défini sur $\overline{\mathbf{Q}}$, φ: $\mathbf{C}^n \to G(\mathbf{C})$ un homomorphisme analytique de dimension $d > n$, et Y un sous-groupe de $\mathbf{C}^n$ tel que $\varphi(Y) \subset G(\overline{\mathbf{Q}})$. Alors il existe un sous-espace vectoriel V de $\mathbf{C}^n$, $V \neq \mathbf{C}^n$, tel que*

$$\operatorname{rang}_{\mathbf{Z}}(Y/Y \cap V) \leq \frac{d\rho}{d-n} \dim_{\mathbf{C}}(\mathbf{C}^n/V).$$

Pour obtenir le corollaire 1.3, on remarque d'abord qu'il n'y a pas de restriction à supposer que φ est un sous-groupe à n paramètres; on applique ensuite le théorème 1.1 à chaque sous-groupe de rang fini de Y; on utilise enfin un argument de compacité. En fait nous établirons d'abord le corollaire 1.3 (quand Y est de type fini), et nous en déduirons le théorème 1.1 (cf. §4). Ce corollaire 1.3 répond au problème 8.2.3 de [9]. Enfin, en remarquant que la quantité $d/(d-n)$, avec $d > n$, est maximale pour $d = n+1$, on obtient le résultat annoncé dans l'introduction.

COROLLAIRE 1.4. *Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur $\overline{\mathbf{Q}}$, de dimensions respectives d' et d'', avec $d' < d''$. Soit ψ: $G'(\mathbf{C}) \to G''(\mathbf{C})$ un homomorphisme analytique dont la différentielle à l'origine $\mathfrak{L}$: $T_{G'}(\mathbf{C}) \to T_{G''}(\mathbf{C})$ est injective, et soit Γ'' un sous-groupe de type fini de $G''(\overline{\mathbf{Q}})$ contenu dans l'image de ψ. Alors il existe un sous-groupe algébrique H'' de G'', $H'' \neq G''$, tel que*

$$\frac{\operatorname{rang}_{\mathbf{Z}}(\Gamma''/\Gamma''\cap H'')}{\dim(G''/H'')} \leq \frac{d'\rho''}{d''-d'},$$

où $\rho'' = \rho(G'')$.

En particulier, si G'' est une variété abélienne simple, la conclusion s'écrit

$$\operatorname{rang}_{\mathbf{Z}}\Gamma'' \leq 2d'd''/(d'-d'').$$

Le corollaire 1.4 se déduit du théorème 1.1 en prenant $\varphi = \psi \circ \exp_{G'}$ et $n = d'$. On peut raffiner le corollaire 1.4 en supposant $\Gamma'' \subset \psi(G'(\overline{\mathbf{Q}}))$; pour cela, on considère l'homomorphisme analytique de $T_{G'}(\mathbf{C})$ dans $G'(\mathbf{C}) \times G''(\mathbf{C})$ défini par

$$z \mapsto (\exp_{G'}(z), \psi \circ \exp_{G'}(z))$$

(cf. [9, corollaire 4.2.5]).

2. Construction d'une fonction auxiliaire avec des périodes

Nous modifions la construction de [10, §3] en tenant compte des périodes éventuelles de nos fonctions. Pour $z = (z_1, \ldots, z_n) \in \mathbf{C}^n$, nous notons

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

(c'est aussi le choix qui est fait implicitement dans [10, p. 101]. Pour $R > 0$, on désigne par $B(0, R)$ le polydisque fermé de centre 0 et de rayon R:

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

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

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

a) *Enoncé.*

PROPOSITION 2.1. *Soient θ une fonction thêta holomorphe relative à un réseau de $\mathbf{C}^g$, avec $\theta(0) \neq 0$, $\mathfrak{L}$: $\mathbf{C}^n \to \mathbf{C}^g$ une application linéaire, et $\sigma = \theta \circ \mathfrak{L}$. Soient $\omega_1, \ldots, \omega_\kappa$ (avec $0 \leq \kappa \leq 2n$) des éléments $\mathbf{R}$-linéairement indépendants de $\mathbf{C}^n$. Il existe deux constantes c_1, c_2 positives ayant les propriétés suivantes.*

Soient $L \geq 1$, $D \geq 0$ *des nombres entiers,* Δ, U, R, r *des nombres réels positifs, et* $\varphi_1, \ldots, \varphi_L$ *des fonctions méromorphes dans* $\mathbf{C}^n$, *admettant* $\omega_1, \ldots, \omega_\kappa$ *comme périodes. On suppose que les fonctions* $\psi_\lambda = \sigma^D \varphi_\lambda$, $(1 \leq \lambda \leq L)$ *sont entières. D'autre part on suppose*

$$U \geq \Delta, R/r \geq c_1, r \geq c_1, U \geq r^2 \log(R/r), U \geq Dr^2, \sum_{\lambda=1}^{L} |\psi_\lambda|_R \leq e^U,$$

et

$$c_2 U^{n+1} \leq L \Delta r^\kappa (\log R/r)^n.$$

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

$$0 < \max_{1 \leq \lambda \leq L} |p_\lambda| \leq e^\Delta,$$

tels que la fonction

$$\Psi = \sum_{\lambda=1}^{L} p_\lambda \psi_\lambda$$

vérifie

$$|\Psi|_r \leq e^{-U}.$$

Quand il n'y a pas de périodes, c'est-à-dire quand $\kappa = 0$, on peut appliquer le théorème 3.1. de [10], et on trouve le résultat avec $c_1 = 3$, $c_2 = 8^{n+1}$.

b) *Lemmes auxiliaires.* Nous aurons besoin des deux lemmes suivants. Le premier permet de rester suffisamment loin des pôles, grâce à la forme particulière du dénominateur, et le second donne une formule d'interpolation.

LEMME 2.2. *Soient* θ *une fonction thêta holomorphe relative à un réseau de* $\mathbf{C}^g$, *avec* $\theta(0) \neq 0$, $\mathfrak{L}\colon \mathbf{C}^n \to \mathbf{C}^g$ *une application linéaire non nulle, et* $\Lambda = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_m$ *un sous-groupe de type fini de* $\mathbf{C}^n$. *Il existe deux constantes* c' *et* c'' *positives, et deux sous-ensembles* $\mathfrak{T}$ *et* F *de* Λ, *avec* F *fini et*

$$\Lambda = \mathfrak{T} + F = \{t + f; t \in \mathfrak{T}, f \in F\},$$

tels que, pour tout réel $S \geq 1$, *si on note*

$$\Lambda(S) = \{h_1\omega_1 + \cdots + h_m\omega_m; (h_1, \ldots, h_m) \in \mathbf{Z}^m, 0 \leq h_j \leq S\},$$

on ait

$$|\theta \circ \mathfrak{L}(z)| \geq \exp(-c'' S^2)$$

pour tout $z \in \mathbf{C}^n$ *vérifiant*

$$\operatorname{dist}(z, \Lambda(S) \cap \mathfrak{T}) \leq c'.$$

Démonstration. On note Ω le réseau de $\mathbf{C}^g$ associé à θ, $s\colon \mathbf{C}^g \to \mathbf{C}^g/\Omega$ la surjection canonique, Δ un polydisque fermé de $\mathbf{C}^g$, de centre 0 et de rayon $\delta > 0$ sur lequel θ ne s'annule pas, et Δ' le polydisque fermé de centre 0 et de rayon $\delta/2$. On définit ensuite

$$\mathfrak{T} = \{\omega \in \Lambda, s \circ \mathfrak{L}(\omega) \in s(\Delta')\},$$

et on choisit $c' > 0$ tel que

$$z \in \mathbf{C}^n,\ |z| \leq c' \quad \text{implique} \quad |\mathfrak{L}(z)| \leq \delta/2.$$

Alors pour $\omega \in \mathfrak{T}$ et $|z - \omega| < c'$, on a $s \circ \mathfrak{L}(z) \in s(\Delta)$, et la conclusion s'obtient comme dans [9, lemme 1.2.2].

En combinant les arguments de [9, §7.3] (voir aussi [10, lemme 3.4]) avec un théorème de Masser [3, Théorème A] sur l'interpolation polynomiale, nous allons établir le résultat suivant (théorème 7.4.13 de [9]).

LEMME 2.3. *Soient ϑ, r_1, r, R des nombres réels, avec $\vartheta > 0$, $0 < r_1 \leq r \leq R$, T un entier positif, et $\mathfrak{S}$ un sous-ensemble fini du polydisque $B(0, r_1)$ de $\mathbf{C}^n$. On note*

$$\delta = \min\{|s - s'|;\ s \in \mathfrak{S}, s' \in \mathfrak{S}, s \neq s'\},$$

et on suppose

$$T \leq 2^{-7n}(\delta/r_1)^{2n-2}\operatorname{Card}\mathfrak{S}$$

et

$$\vartheta^2 \leq n^{-n}(\delta/r_1)^{2n}\operatorname{Card}\mathfrak{S}.$$

Alors, pour toute fonction F continue sur $B(0, R)$ et analytique à l'intérieur, on a

$$|F|_r \leq (cr/R)^T|F|_R + (cr/r_1)^T \max_{s\in\mathfrak{S}}|F(s)|,$$

où

$$c = 2 + 2(2^{10n}\vartheta^{-1})^n.$$

Démonstration. On écrit $F = P + G$, où P est un polynôme de degré total $< T$, et G a un zéro à l'origine d'ordre $\geq T$. Grâce au théorème A de [3], on obtient

$$|P|_{r_1} \leq (2^{10n}\vartheta^{-1})^{nT} \max_{s\in\mathfrak{S}}|P(s)|.$$

Soit $z_0 \in \mathbf{C}^n$, avec $|z_0| = r$ et $|P|_r = |P(z_0)|$, et soit $Q(t) = t^{T-1}P(z_0/t) \in \mathbf{C}[t]$. Le principe du maximum donne $|Q(1)| \leq |Q|_{r/r_1}$, donc

$$|P|_r \leq (r/r_1)^{T-1}|P|_{r_1}.$$

D'autre part

$$|P(s)| \leq |F(s)| + |G|_{r_1} \qquad \text{pour tout } s \in \mathfrak{S}.$$

Enfin, pour $0 \leq \rho \leq R$, on trouve, comme dans [10] (démonstration du lemme 3.4):

$$|G|_\rho \leq (\rho/R)^T |G|_R, \text{ et } |G|_R \leq |P|_R + |F|_R \leq (1 + T^{1/2})|F|_R.$$

Alors

$$\begin{aligned}|F|_r &\leq |P|_r + |G|_r \\ &\leq (r/r_1)^T (2^{10n}\vartheta^{-1})^{nT}\Big(|G|_{r_1} + \max_{s\in\mathfrak{S}}|F(s)|\Big) + |G|_r\end{aligned}$$

et on en déduit l'inégalité annoncée.

c) *Démonstration de la proposition* 2.1. On complète $\omega_1, \ldots, \omega_\kappa$ en une base $(\omega_1, \ldots, \omega_{2n})$ de $\mathbf{C}^n$ sur $\mathbf{R}$. Les constantes positives $c_3, \ldots, c_8$ ne dépendront que de $n, g, \mathfrak{L}, \theta, \omega_1, \ldots, \omega_{2n}$. Soit ν un entier suffisamment grand; on va démontrer la proposition avec $c_1 = \nu$, $c_2 = \nu^{n+2}$.

On utilise le lemme 2.2 avec $m = 2n$, et on note

$$\Lambda' = \mathbf{Z}\omega_1 + \cdots + \mathbf{Z}\omega_\kappa, \Lambda'' = \mathbf{Z}\omega_{\kappa+1} + \cdots + \mathbf{Z}\omega_{2n}.$$

Ainsi $\Lambda = \Lambda' + \Lambda''$, et, avec des notations évidentes, pour chaque $S > 0$, $\Lambda(S) = \Lambda'(S) + \Lambda''(S)$. On pose $T = 4U/\log(R/r)$, $T_0 = \nu T$, et on désigne par $\mathfrak{S}$ l'ensemble des $\lambda_1 + rT_0^{-1/2}\lambda_2$, pour

$$\lambda_1 \in \Lambda''(r/c_3) \cap \mathfrak{T}, \lambda_2 \in \Lambda\big(T_0^{1/2}/rc_4\big).$$

On choisit ici

$$c_3 = 1 + \sum_{i=1}^{2n} |\omega_i|, \; c_4 = c_3 \max(2, 1/c');$$

$\mathfrak{T}$ et c' sont définis au lemme 2.2. Ainsi $\mathfrak{S}$ est contenu dans $B(0, r)$. On considère le système d'inéquations

$$\left|\sum_{\lambda=1}^{L} p_\lambda \psi_\lambda(s)\right| < e^{-\nu U}, \qquad (s \in \mathfrak{S}),$$

dont les inconnues sont $p_1, \ldots, p_L$. Le nombre de ces inéquations est majoré par

$$r^{2n-\kappa}\big(T_0^{1/2}/r\big)^{2n} = T_0^n r^{-\kappa}.$$

Les inégalités

$$1 + \sqrt{2}\, e^{(\nu+2)U} \leq e^{2\nu U}$$

et

$$4\nu U T_0^n r^{-\kappa} < L\,\Delta,$$

jointes au lemme 3.3 de [10], permettent de trouver une solution non triviale dans $\mathbf{Z}$ avec $|p_\lambda| \leq e^\Delta$. Posons alors

$$\Phi = \sum_{\lambda=1}^{L} p_\lambda \varphi_\lambda,\ \Psi = \sigma^D \Phi = \sum_{\lambda=1}^{L} p_\lambda \psi_\lambda.$$

La périodicité des φ_λ donne:

$$\Psi(z+\omega) = \big(\sigma(z+\omega)/\sigma(z)\big)^D \Psi(z) \qquad \text{pour tout } \omega \in \Lambda'.$$

Grâce au lemme 2.2, on a, pour $s \in \mathcal{S}$,

$$|\sigma(s)| \geq \exp\big(-c_5 r^2\big).$$

Soit $\mathcal{S}'$ l'ensemble des $s + \omega$, s décrivant $\mathcal{S}$ et ω décrivant $\Lambda'(r/c_3)$. Pour tout $s' \in \mathcal{S}'$, on obtient

$$|\Psi(s')| \leq e^{-\nu U/2}.$$

On vérifie de plus (cf. [9, lemme 1.1.8]), en utilisant l'hypothèse $U \geq r^2(\log(R/r)$,

$$\operatorname{Card} \mathcal{S}' \geq c_6 T_0^n,$$

et aussi

$$\delta = \min\{|s' - s''|;\, s' \in \mathcal{S}',\, s'' \in \mathcal{S}',\, s' \neq s''\} \geq c_7 r T_0^{-1/2}.$$

On utilise maintenant le lemme 2.3, avec $F = \Psi$, $\vartheta \geq c_8$, $r = r_1$, et avec l'ensemble $\mathcal{S}'$, et on trouve

$$|\Psi|_r \leq (cr/R)^T e^{\Delta + U} + c^T e^{-\nu U/2} \leq e^{-U}.$$

Remarque. Si, dans la proposition 2.1, on suppose $\omega_1, \ldots, \omega_\kappa$ linéairement indépendants sur $\mathbf{C}$, alors on peut remplacer l'hypothèse $U \geq r^2 \log(R/r)$ par $U \geq r \log(R/r)$. Pour cela, dans la démonstration, on remplace le lemme 2.3 par le théorème 7.3.4 de [9].

d) *Application aux groupes algébriques.* Considérons maintenant un groupe algébrique commutatif G.

Pour obtenir un énoncé raffiné, nous écrivons G sous la forme $\mathbf{G}_a^{d_0} \times G_1 \times G_2$, où G_1 est un groupe linéaire de dimension d_1, et G_2 est quelconque. Cela ne restreint pas la généralité, puisque l'on peut choisir $d_0 = d_1 = 0$, $G = G_2$. Le seul autre cas que nous utiliserons ici est $G = G_1$, mais le cas général nous sera utile ailleurs.

PROPOSITION 2.4. *Soient* $d_0 \geq 0$, $d_1 \geq 0$, $d_2 \geq 0$, $n \geq 1$ *des entiers*, $d = d_0 + d_1 + d_2$, *avec* $n < d$. *Soient* G_1 *et* G_2 *deux groupes algébriques commutatifs définis sur* $\overline{\mathbf{Q}}$, *de dimensions respectives* d_1 *et* d_2, G_1 *étant linéaire. On pose* $G = \mathbf{G}_a^{d_0} \times G_1 \times G_2$.

Soient φ *un sous-groupe à* n *paramètres de* G, κ *le rang sur* $\mathbf{Z}$ *de son noyau, et* $y_1, \ldots, y_m$ *des éléments* $\mathbf{Q}$*-linéairement indépendants de* $\mathbf{C}^n$ *dont les images par* φ *sont dans* $G(\overline{\mathbf{Q}})$.

Il existe un plongement de $G(\overline{\mathbf{Q}})$ *dans* $\mathbf{A}_{d_0+d_1}(\overline{\mathbf{Q}}) \times \mathbf{P}_N(\overline{\mathbf{Q}})$, *une constante* $C > 0$, *et une suite* $(P_S)_{S \geq S_0}$ *de polynômes de l'anneau*

$$\mathbf{Z}\left[U_1, \ldots, U_{d_0}, V_1, \ldots, V_{d_1}, W_0, \ldots, W_N\right],$$

P_S *étant de degré* $\leq D_0$ *en les variables* $U_1, \ldots, U_{d_0}$, *de degré* $\leq D_1$ *en* $V_1, \ldots, V_{d_1}$, *et homogène de degré* $\leq D_2$ *en* $W_0, \ldots, W_N$, *avec*

$$D_0 \log S = D_1 S = D_2 S^2 = \Delta,$$

où Δ *est défini par*

$$\Delta^{d-n} = C S^{2d_2+d_1-\kappa} (\log S)^{d_0},$$

et enfin P_S *s'annule en chaque point de l'image par* φ *de l'ensemble*

$$Y(S) = \left\{h_1 y_1 + \cdots + h_m y_m;\ (h_1, \ldots, h_m) \in \mathbf{Z}^m, 0 \leq h_j \leq S\right\},$$

mais P_S *ne s'annule pas partout sur* $G(\overline{\mathbf{Q}})$.

Le principe des tiroirs, utilisé de la manière habituelle, ne permet de trouver un tel polynôme que sous l'hypothèse supplémentaire

$$D_0^{d_0} D_1^{d_1} D_2^{d_2} \geq C' S^m.$$

Mais le point essentiel ici est que les exposants de S qui interviennent ne dépendent pas de m (seul C peut dépendre de m).

La démonstration fournira, en plus, une majoration pour les coefficients de P_S: leur valeur absolue sera majorée par e^{Δ}.

Quand G est linéaire, on peut choisir $d_2 = 0$. La construction donne alors un polynôme indépendant des variables $W_0, \ldots, W_N$. Si, de plus, on choisit $d_0 = 0$, c'est-à-dire $d = d_1$ et $G = G_1$, alors on obtient un polynôme en d_1 variables, de degré $\leq D_1$, avec

$$D_1 = C'' S^{(n-\kappa)/(d-n)}.$$

Si G est quelconque et que l'on choisisse $d_0 = d_1 = 0$, $d = d_2$, $G = G_2$, on obtient un polynôme homogène P_S, de degré $\leq D_2$, avec

$$D_2 = C'' S^{(2n-\kappa)/(d-n)}.$$

Démonstration de la proposition 2.4. Il est utile d'effectuer quelques réductions préliminaires. D'abord on peut supposer que G est l'adhérence de Zariski sur $\overline{\mathbf{Q}}$ de $\varphi(\mathbf{C}^n)$. En effet, si ce n'était pas le cas, il existerait un polynôme à coefficients algébriques, nul sur $\varphi(\mathbf{C}^n)$, mais pas sur $G(\overline{\mathbf{Q}})$. En prenant la norme sur $\mathbf{Q}$ et en multipliant par un entier positif, on obtient un polynôme à coefficients dans $\mathbf{Z}$, indépendant de S, ayant les propriétés requises.

En particulier on supposera que G est connexe, et que $d_0 \leq n$. On a aussi $\kappa \leq 2n - d_0$, mais on va se ramener à une condition plus forte.

a) Supposons $d_2 = 0$. Comme $\mathcal{L}$ est injective, le noyau de φ est engendré comme $\mathbf{Z}$-module par κ éléments de $\mathbf{C}^n$ linéairement indépendants sur $\mathbf{C}$. Nous allons nous ramener à $\kappa = 0$. Supposons donc la proposition 2.4 démontrée quand $\kappa = 0$. Maintenant, si $\kappa > 0$, φ se factorise en un homomorphisme de

$$\mathbf{C}^n/\ker\varphi \cong \mathbf{C}^{n-\kappa} \times (\mathbf{C}^{\times})^{\kappa}$$

dans $G(\mathbf{C})$, et on considère la restriction φ' de cet homomorphisme à $\mathbf{C}^{n-\kappa}$. Pour φ' et pour l'adhérence de Zariski G' de $\varphi'(\mathbf{C}^{n-\kappa})$, on a

$$\kappa' = 0, d_0' = d_0, d_1' = d_1 - \kappa, d' = d - \kappa, n' = n - \kappa.$$

Par hypothèse on peut appliquer la proposition 2.4 (avec $\kappa' = d_2' = 0$) à φ' pour trouver la constante C' (permettant de définir Δ') et un polynôme (ne dépendant en fait que des $d - \kappa$ variables $U_1, \ldots, U_{d_0}, V_1, \ldots, V_{d_1-\kappa}$). On choisit enfin $C = C'$, de sorte que $\Delta' = \Delta$.

b) On va montrer qu'on peut toujours supposer soit $d_2 = 0$, soit $2n \geq d_1 + 2d_0 + \kappa$. Dans le cas contraire, notons $s\colon T_G(\mathbf{C}) \to T_{G/G_2}(\mathbf{C})$, et $p\colon \mathbf{C}^n \to \mathbf{C}^n/V$ les surjections canoniques, où V est le noyau de $s \circ \mathcal{L}$, n_2 la dimension de V, Λ le noyau de φ, et λ_1 (resp. λ_2) le rang sur $\mathbf{Z}$ de $\Lambda/\Lambda \cap V$ (resp. de $\Lambda \cap V$). On a

$$\kappa = \lambda_1 + \lambda_2, \lambda_2 \leq 2n_2, \text{et } n_2 \leq d_2,$$

car la restriction de $\mathcal{L}$ à V est une injection de V dans $T_{G_2}(\mathbf{C})$.

Soit φ' le sous-groupe à $n - n_2$ paramètres de G/G_2 rendant commutatif le diagramme:

$$\begin{tikzcd}
\mathbf{C}^n \arrow[r, "\mathcal{L}"] \arrow[dd, "p"'] \arrow[dr, "\varphi"'] & T_G(\mathbf{C}) \arrow[r, "s"] \arrow[d] & T_{G/G_2}(\mathbf{C}) \arrow[dd] \\
 & G(\mathbf{C}) \arrow[dr] & \\
\mathbf{C}^n/V \arrow[rr, "\varphi'"'] & & G/G_2(\mathbf{C}).
\end{tikzcd}$$

Le noyau de φ' est engendré comme $\mathbf{Z}$-module par des éléments linéairement indépendants sur $\mathbf{C}$. Soit $n_0 = n - n_1 - n_2$. On vérifie alors facilement les inégalités

$$n_0 \geq d_0, n_0 + n_1 \leq d_0 + d_1, d_1 \geq n_1, \lambda_1 \leq n_1.$$

En particulier on a $\kappa \leq n_1 + 2n_2$. Grâce à l'hypothèse $2n < d_1 + 2d_0 + \kappa$, on en conclut $d_0 + d_1 > n_0 + n_1$. On pourra alors, grâce à la proposition 2.4 dans le cas $d_2 = 0$ appliquée à φ', construire P_S indépendant des variables $W_0, \ldots, W_N$, avec des degrés majorés par D_0' et D_1', avec

$$D_0' \log S = D_1' S = \Delta',$$

où Δ' est défini par

$$\Delta'^{d_0 + d_1 - n_0 - n_1} = CS^{d_1 - n_1} (\log S)^{d_0}.$$

Mais on vérifie

$$(d_1 - n_1)/(d_0 + d_1 - n_0 - n_1) \leq (2d_2 + d_1 - \kappa)/(d - n),$$

et $\Delta' \leq \Delta$.

c) Dans le cas $d_0 = 0$, l'argument de b) permet de se ramener soit à $d_2 = 0$, soit à $2n > d_1 + \kappa$.

Ces trois réductions a), b), c), montrent qu'on aura toujours

$$D_1 \geq C''(\log S)^{n/(d-n)},$$

et, de plus, on aura soit $d_2 = 0$, soit

$$D_2 \geq C''(\log S)^{1/(d-n)}.$$

On utilise maintenant l'existence, démontrée par Serre [8], d'un plongement de G_2 dans un espace projectif $\mathbf{P}_N$, défini sur $\overline{\mathbf{Q}}$, dans lequel l'application exponentielle de G_2 est représentée par $N + 1$ fonctions entières d'ordre ≤ 2, la première, qui ne s'annule pas à l'origine, étant composée d'une fonction thêta holomorphe relative à un réseau d'un espace $\mathbf{C}^g$, et d'une application linéaire de $T_{G_2}(\mathbf{C})$ dans $\mathbf{C}^g$. Alors l'homomorphisme φ: $\mathbf{C}^n \to G(\mathbf{C})$ peut être représenté par des coordonnées

$$(\lambda_1, \ldots, \lambda_{d_0}, \mu_1, \ldots, \mu_{d_1}, \psi_0, \ldots, \psi_N),$$

avec les propriétés suivantes:

a) Pour $1 \leq i \leq d_0$, $\lambda_i(z) = z_i$.

b) Soit δ l'entier tel que $G_1(\overline{\mathbf{Q}}) = \overline{\mathbf{Q}}^\delta \times \overline{\mathbf{Q}}^{\times d_1 - \delta}$, $(0 \leq \delta \leq d_1)$. Pour $1 \leq i \leq \delta$, on a $\mu_i(z) = z_{d_0 + i}$, et pour $\delta < i \leq d_1$ on a $\mu_i(z) = \exp\langle x_i, z \rangle$, avec $x_i \in \mathbf{C}^n$.

c) Les fonctions $\psi_0, \ldots, \psi_N$ sont entières dans $\mathbf{C}^n$, d'ordre ≤ 2. De plus ψ_0 est composée d'une fonction thêta non nulle à l'origine, et d'une application linéaire de $\mathbf{C}^n$ dans $\mathbf{C}^g$.

d) Enfin on peut supposer que les fonctions

$$\lambda_1,\ldots,\lambda_{d_0},\mu_1,\ldots,\mu_{d_1},\psi_1/\psi_0,\ldots,\psi_{d_2}/\psi_0$$

sont algébriquement indépendantes sur $\overline{\mathbf{Q}}$.

On utilisera aussi la majoration de la hauteur sur $G_2(\overline{\mathbf{Q}})$, relative au plongement précédent, donnée par Serre dans [8, Prop. 5, p. 197].

Soit K un corps de nombres sur lequel G est défini, tel que $\varphi(Y)\subset G(K)$, tel que le plongement précédent de G_2 dans $\mathbf{P}_N$ soit défini sur K, et tel que $G_1(K)$ soit un produit $K^\delta\times(K^\times)^{d_1-\delta}$. On identifie alors $G(K)$ à un sous-ensemble de $K^{d_0+d_1}\times\mathbf{P}_N(K)$.

D'après le lemme 1.2.2 de [9], il existe deux sous-ensembles $\mathfrak{T}$ et F de $Y=\mathbf{Z}y_1+\cdots+\mathbf{Z}y_m$, avec F fini, tels que

$$Y=\mathfrak{T}+F=\{t+f,t\in\mathfrak{T},f\in F\},$$

et

$$|\psi_0(t)|\geq-cS^2\qquad\text{pour } t\in Y(S)\cap\mathfrak{T},\ S\geq 1,$$

où c ne dépend pas de S (le lemme 2.2 ci-dessus donne un résultat un peu plus précis).

On choisit maintenant un entier ν suffisamment grand, puis un entier S_0 suffisamment grand (dépendant de ν), et on va construire P_S pour chaque réel $S\geq S_0$, avec $C=\nu^{8d}$. Cette construction va se faire en trois étapes.

Première étape. On construit un polynôme non nul

$$Q_S\in\mathbf{Z}\left[U_1,\ldots,U_{d_0},V_1,\ldots,V_{d_1},W_0,\ldots,W_{d_2}\right],$$

dont le degré en $U_1,\ldots,U_{d_0}$ *est majoré par* D_0/ν, *le degré en* $V_1,\ldots,V_{d_1}$ *est majoré par* D_1/ν, *et qui est homogène de degré* D_2° *en* $W_0,\ldots,W_{d_2}$, *avec* $D_2^\circ\leq D_2/\nu$, *tel que la fonction entière dans* $\mathbf{C}^n$:

$$\Psi_S=Q_S\left(\lambda_1,\ldots,\lambda_{d_0},\mu_1,\ldots,\mu_{d_1},\psi_0,\ldots,\psi_{d_2}\right)$$

vérifie

$$|\Psi_S(z)|\leq e^{-\nu^6\Delta}\qquad\qquad \textit{pour } |z|\leq\nu^2S.$$

De plus, les coefficients de Q_S *ont une valeur absolue majorée par* $e^{\Delta/\nu}$.

Supposons d'abord $d_2\geq 1$. On va utiliser la proposition 2.1, avec $r=\nu^2S$, $R=\nu r$, $\sigma=\psi_0$, et $U=\nu^6\Delta$. L'entier L est le nombre de monomes en $U_1,\ldots,U_{d_0},V_1,\ldots,V_{d_1},W_0,\ldots,W_{d_2}$, vérifiant les conditions de degrés et d'homogénéité requises. Ainsi

$$L>D_0^{d_0}D_1^{d_1}D_2^{d_2}\nu^{-d}(d_2+1)^{-d_2}.$$

On en déduit

$$L > c_2 C^{-1} \nu^{6n+7-2\kappa} (\log \nu)^{-n} D_0^{d_0} D_1^{d_1} D_2^{d_2},$$

ce qui permet de vérifier la condition

$$c_2 U^{n+1} < L(\Delta/\nu) r^{\kappa} \left(\log \frac{R}{r}\right)^n.$$

On utilise maintenant l'hypothèse $d_2 \geq 1$: grâce à une réduction précédente, on a $2n \geq d_1 + 2d_0 - \kappa$, ce qui donne bien $U \geq r^2 \log(R/r)$.

Dans le cas $d_2 = 0$, seul le dernier argument peut tomber en défaut. Mais, comme $D = \kappa = 0$, il suffit d'utiliser soit la remarque qui suit la démonstration de la proposition 2.1 (fin du §c ci-dessus), soit, plus simplement, le théorème 3.1 de [10].

Deuxième étape. On vérifie $\Psi_S(t) = 0$ pour $t \in Y(\nu S) \cap \mathfrak{T}$. Pour cela considérons la fonction méromorphe

$$\Phi_S = \psi_0^{-D_2^0} \Psi_S.$$

Le nombre $\Phi_S(t)$ appartient à K, et grâce au choix de l'ensemble $\mathfrak{T}$, on déduit de la première étape

$$|\Phi_S(t)| \leq e^{-\nu^5 \Delta}.$$

On multiplie par un dénominateur, et on prend la norme sur $\mathbf{Q}$. La majoration de la hauteur citée plus haut montre qu'on obtient un entier rationnel de valeur absolue inférieure à 1.

Troisième étape. Construction de P_S. On utilise le fait que, pour $\gamma \in G_2(K)$, la translation $g \mapsto \gamma + g$ est un isomorphisme de G sur G, défini sur K. Il en résulte facilement qu'il existe un entier $a > 0$, ne dépendant que du plongement de G_2 dans $\mathbf{P}_N$, tel que, si H est une hypersurface de $\mathbf{P}_N$, définie sur K, de degré disons D, et ne contenant pas $G_2(\overline{\mathbf{Q}})$, alors il existe une hypersurface de $\mathbf{P}_N$, définie sur K, de degré $\leq aD$, contenant $\gamma + H \cap G_2$, et ne contenant pas tout $G_2(\overline{\mathbf{Q}})$. (Comparer avec [4], §2).

L'ensemble des zéros de Q_S dans $\mathbf{A}_{d_0+d_1} \times \mathbf{P}_N$ est une hypersurface qui ne contient pas $G(\overline{\mathbf{Q}})$, mais qui contient l'image par φ de $Y(\nu S) \cap \mathfrak{T}$. Pour chaque $f \in F$, il existe donc un polynôme $R_{S,f} \in K[U_1, \ldots, U_{d_0}, V_1, \ldots, V_{d_1}, W_0, \ldots, W_N]$, de degré en $U_1, \ldots, U_{d_0}$ majoré par D_0/ν, de degré en $V_1, \ldots, V_{d_1}$ majoré par D_1/ν, et homogène en $W_0, \ldots, W_N$ de degré $\leq aD_2/\nu$, qui ne s'annule pas partout sur $G(\overline{\mathbf{Q}})$, mais qui s'annule en $\varphi(f + y)$ pour $y \in Y(\nu S) \cap \mathfrak{T}$.

On considère alors le polynôme

$$\prod_{f \in F} R_{S,f} \in K\left[U_1,\ldots, U_{d_0}, V_1,\ldots, V_{d_1}, W_0,\ldots, W_N\right],$$

on prend sa norme sur $\mathbf{Q}$, on multiplie par un dénominateur, et on obtient le polynôme P_S cherché.

3. Les coefficients de Dirichlet généralisés

On désigne par K un corps de caractéristique nulle, et par G un groupe algébrique commutatif défini sur K de dimension $d \geq 1$.

Nous rappelons la définition du coefficient $\mu(Y, K^n)$ (cf. [9]) quand Y est un sous-groupe de type fini de K^n, et nous en considérons deux généralisations: la première est le coefficient $\mu(\Gamma, G)$ de [4] quand Γ est un sous-groupe de type fini de $G(K)$; la seconde est un nouveau coefficient $\mu(\varphi)$, quand K est plongé dans $\mathbf{C}$ et φ: $\mathbf{C}^n \to G(\mathbf{C})$ est un homomorphisme analytique.

Nous énonçons ensuite le lemme de zéros de Masser et Wüstholz [4], puis nous donnons quelques lemmes auxiliaires.

a) *Définitions.* Soit Y un sous-groupe de type fini de K^n. On définit (cf. [9]):

$$\mu(Y, K^n) = \min\{\mathrm{rang}_{\mathbf{Z}}(Y/Y \cap W)/\dim_K(K^n/W)\},$$

quand W décrit les sous-espaces vectoriels de K^n, avec $W \neq K^n$. Plus généralement, si Γ est un sous-groupe de type fini de $G(K)$, on définit (cf. [4]):

$$\mu(\Gamma, G) = \min\{\mathrm{rang}_{\mathbf{Z}}(\Gamma/\Gamma \cap H)/\dim(G/H)\},$$

quand H décrit les sous-groupes algébriques de G, définis sur K, de dimension algébrique strictement inférieure à celle de G.

Enfin, si K est plongé dans $\mathbf{C}$, et si φ: $\mathbf{C}^n \to G(\mathbf{C})$ est un homomorphisme analytique, nous noterons

$$\mu(\varphi) = \min\{\dim \overline{\varphi(V)}/\dim V\},$$

quand V décrit les sous-espaces vectoriels non nuls de $\mathbf{C}^n$, et $\dim \overline{\varphi(V)}$ est la dimension de l'adhérence de Zariski sur K de $\varphi(V)$ (c'est donc la dimension de la restriction de φ à V).

Si $x_1,\ldots, x_d$ sont des éléments de $\mathbf{C}^n$, et si $X = \mathbf{Z}x_1 + \cdots + \mathbf{Z}x_d$, on a

$$\mu(X, \mathbf{C}^n) = \mu(\varphi),$$

où φ désigne l'homomorphisme de $\mathbf{C}^n$ dans $(\mathbf{C}^\times)^d$ défini par

$$\varphi(z) = \left(e^{\langle x_1, z\rangle},\ldots, e^{\langle x_d, z\rangle}\right), \qquad (z \in \mathbf{C}^n)$$

(cf. [9], p. 57).

b) *Le lemme de zéros de Masser et Wüstholz.* L'énoncé suivant se déduit du théorème principal de [4].

THÉORÈME 3.1. (*Masser, Wüstholz*). *On considère un plongement de G dans un espace projectif $\mathbf{P}_N$ défini sur K. Il existe une constante $c > 0$ ayant la propriété suivante.*

Soient $\gamma_1, \ldots, \gamma_m$ des éléments de $G(K)$. Notons $\Gamma = \mathbf{Z}\gamma_1 + \cdots + \mathbf{Z}\gamma_m$, et $\mu = \mu(\Gamma, G)$. Soit S un nombre réel ≥ 0. Alors toute hypersurface de $\mathbf{P}_N$, ne contenant pas $G(K)$, et passant par tous les points

$$h_1\gamma_1 + \cdots + h_m\gamma_m, \quad (h_1, \ldots, h_m) \in \mathbf{Z}^m, 0 \leq h_j \leq S, (1 \leq j \leq m)$$

a un degré D minoré par:

$$D \geq c(S/d)^{\mu}.$$

c) *Lemmes auxiliaires.* Les lemmes qui suivent seront utiles dans la démonstration du théorème 1.1, au paragraphe 4. Le premier lemme est essentiellement le lemme 1.3.1 de [9] (voir aussi [10], lemme 5.1).

LEMME 3.2. *Soit Y un sous-groupe de K^n, de rang m sur $\mathbf{Z}$, tel que $\mu(Y, K^n) < m/n$. Alors il existe un sous-espace W de $\mathbf{C}^n$, de dimension $n' > 0$, tel que, si on note $Y' = Y \cap W$, et si m' est le rang de Y' sur $\mathbf{Z}$, on ait*

$$\mu(Y', W) = m'/n' > m/n.$$

On peut étendre ce lemme aux coefficients $\mu(\Gamma, G)$ et $\mu(\varphi)$. Nous n'utiliserons ici que cette deuxième généralisation, dont voici l'énoncé précis et la démonstration.

LEMME 3.3. *Supposons K plongé dans $\mathbf{C}$. Soit φ: $\mathbf{C}^n \to G(\mathbf{C})$ un homomorphisme analytique, de dimension d (où $d = \dim G$), tel que $\mu(\varphi) < d/n$. Alors il existe un sous-espace vectoriel V de $\mathbf{C}^n$, de codimension $n' > 0$ dans $\mathbf{C}^n$, tel que, si H désigne l'adhérence de Zariski sur K de $\varphi(V)$, d' la codimension dans G de H, et ψ l'homomorphisme analytique de $\mathbf{C}^n/V$ dans $G/H(\mathbf{C})$ rendant commutatif le diagramme:*

$$\begin{tikzcd} \mathbf{C}^n \arrow[r, "\varphi"] \arrow[d, "p"'] & G(\mathbf{C}) \arrow[d, "s"] \\ \mathbf{C}^n/V \arrow[r, "\psi"] & G/H(\mathbf{C}) \end{tikzcd}$$

(*où p et s sont les surjections canoniques*), *on ait*

$$\mu(\psi) = d'/n' > d/n.$$

De plus, ψ est un sous-groupe à n' paramètres.

Démonstration. On va démontrer le lemme 3.3 par récurrence sur n. Pour $n = 1$, l'hypothèse $\mu(\varphi) < d/n$ n'est jamais satisfaite, et il n'y a rien à démontrer.

Supposons donc $\mu(\varphi) < d/n$. Soit V un sous-espace de $\mathbf{C}^n$, vérifiant

$$\dim \overline{\varphi(V)} < \frac{d}{n} \dim V,$$

et maximal pour cette propriété. Montrons que V convient. On a

$$\frac{d - d'}{n - n'} < \frac{d}{n},$$

c'est-à-dire $d'/n' > d/n$. Montrons maintenant $\mu(\psi) = d'/n'$. Si ce n'était pas vrai, les inégalités $n' < nd'/d \leq n$ permettraient d'utiliser l'hypothèse de récurrence, donc de trouver un sous-espace V_1 de $\mathbf{C}^n$, contenant strictement V, tel que, si on note H_1/H l'adhérence de Zariski sur K de $\psi(V_1/V)$, et

$$n_1' = \dim_{\mathbf{C}}(\mathbf{C}^n/V_1), \qquad d_1' = \dim(G/H_1),$$

on ait

$$d_1' > n_1'd'/n' > n_1'd/n.$$

Mais alors $\varphi(V_1) \subset H_1$, donc

$$\dim \overline{\varphi(V_1)} \leq d - d_1' < \frac{d}{n}(n - n_1') = \frac{d}{n} \dim V_1,$$

ce qui contredit le fait que V avait été choisi maximal. Enfin, pour cette même raison, V est le noyau de l'application linéaire $\mathbf{C}^n \to T_{G/H}(\mathbf{C})$ tangente à $\psi \circ p = s \circ \varphi$.

Remarque. En reprenant la démonstration du lemme 5.2 de [10], on peut établir le résultat suivant. *Si φ: $\mathbf{C}^n \to G(\mathbf{C})$ est un homomorphisme analytique et Y un sous-groupe de $\mathbf{C}^n$ de type fini et de rang m sur $\mathbf{Z}$ tel que $\varphi(Y) \subset G(K)$, alors il existe deux sous-espace V_1, V_2 de $\mathbf{C}^n$, et deux sous-groupes algébriques H_1 et H_2 de G définis sur K, avec*

$$0 \subseteq V_2 \subsetneq V_1 \subseteq \mathbf{C}^n, 0 \subseteq H_2 \subsetneq H_1 \subseteq G, \varphi(V_1) \subset H_1, \varphi(V_2) \subset H_2,$$

tels que, si ψ désigne l'homomorphisme rendant commutatif le diagramme

$$\begin{array}{ccc} V_1 & \xrightarrow{\varphi | V_1} & H_1(\mathbf{C}) \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle s} \\ V_1/V_2 & \xrightarrow{\psi} & H_1/H_2(\mathbf{C}) \end{array}$$

(*où p et s sont les surjections canoniques*), *on ait*

$$\mu(\psi) = \delta/\nu \geq d/n, \mu(p(Y \cap V_1), V_1/V_2) = \lambda/\nu \geq \mu(Y, \mathbf{C}^n),$$

où

$$\delta = \dim H_1/H_2, \nu = \dim V_1/V_2, \textit{et } \lambda = \operatorname{rang}_{\mathbf{Z}} p(Y \cap V_1).$$

De plus, si on suppose $\mu(\varphi) = d/n$, alors on peut démontrer

$$\mu(\varphi(Y), G) \geq \frac{n}{d}(\mu(Y, \mathbf{C}^n) - 2).$$

Si on voulait compléter la démonstration du théorème 1.1 en utilisant la méthode de [10], il suffirait de vérifier que les hypothèses $\mu(\varphi) = d/n$ et $\ell d > n(\ell + d\rho - \kappa)$, avec $\ell = \operatorname{rang}_{\mathbf{Z}}\varphi(Y)$ et $\kappa = \kappa(\varphi)$, impliquent

$$\mu(\varphi(Y), G) \geq \frac{n}{d}\left(\mu(Y, \mathbf{C}^n) - \frac{\kappa}{n}\right).$$

Cette inégalité a été vérifiée dans [10], (lemme 5.3) dans le cas $G = \mathbf{G}_m^d$. Un énoncé plus général a été obtenu par P. Philippon, qui permet de résoudre le cas $G = E^d$, quand E est une courbe elliptique, sous l'hypothèse un peu plus restrictive $\ell d > 2n(\ell + d)$. Ici nous utiliserons une approche différente.

4. Démonstrations

Dans tout ce paragraphe 4, on désigne par G un groupe algébrique commutatif défini sur $\overline{\mathbf{Q}}$ de dimension $d \geq 1$, par φ: $\mathbf{C}^n \to G(\mathbf{C})$ un homomorphisme analytique de dimension d, et par Y un sous-groupe de type fini de $\mathbf{C}^n$ tel que $\Gamma = \varphi(Y)$ soit contenu dans $G(\overline{\mathbf{Q}})$. De plus, m sera le rang de Y sur $\mathbf{Z}$, ℓ le rang de Γ sur $\mathbf{Z}$, $\mathfrak{L}$: $\mathbf{C}^n \to T_G(\mathbf{C})$ la différentielle de φ en 0, et $\rho = \rho(G)$, $\kappa = \kappa(\varphi)$.

a) *On suppose $\mathfrak{L}$ injective et $d > n$. Alors*

(4.1) $$\mu(\Gamma, G) \leq (n\rho - \kappa)/(d - n).$$

Cette inégalité est une conséquence immédiate du théorème 3.1 combiné à la proposition 2.4 (avec $d_0 = 0$, et $d_1 = d$, $d_2 = 0$ si $\rho = 1$, $d_1 = 0$, $d_2 = d$ si $\rho = 2$).

b) *On suppose $d > n$. Alors*

(4.2) $$\mu(Y, \mathbf{C}^n) \leq (d\rho - \kappa)/(d - n).$$

Montrons d'abord qu'il n'y a pas de restriction à supposer $\mathfrak{L}$ injectif. En effet, si $W = \ker \mathfrak{L}$ n'est pas réduit à 0, et si on note $\mathfrak{L}'$: $\mathbf{C}^n/W \to T_G(\mathbf{C})$ l'application linéaire quotient, et $\varphi' = \exp_G \circ \mathfrak{L}'$, avec $\kappa' = \operatorname{rang}_{\mathbf{Z}} \ker \varphi'$, on a

$$\kappa' \leq \rho n', \text{et } \kappa - \kappa' \leq (n - n')\rho, \text{avec } n' = \dim_{\mathbf{C}}(\mathbf{C}^n/W),$$

donc

$$(d\rho - \kappa')/(d - n') \le (d\rho - \kappa)/(d - n);$$

d'autre part

$$\mu(Y, \mathbf{C}^n) \le \mu(Y/Y \cap W, \mathbf{C}^n/W).$$

Enfin $\dim \varphi' = \dim \varphi = d$. Il suffit alors de démontrer

$$\mu(Y/Y \cap W, \mathbf{C}^n/W) \le (d\rho - \kappa')/(d - n').$$

On suppose donc $\mathfrak{L}$ injectif. Comme nous l'avons déjà vu, cela signifie

$$\kappa = \operatorname{rang}_{\mathbf{Z}} \ker \varphi.$$

Quitte à remplacer Y par $Y + \ker \varphi$, on peut supposer $Y \supset \ker \varphi$, donc $m = \ell + \kappa$. Notons $\mu(\Gamma, G) = \ell_1/d_1$, où $d_1 = \dim(G/H) > 0, \ell_1 = \operatorname{rang}_{\mathbf{Z}} \Gamma/\Gamma \cap H$, et H est un sous-groupe algébrique de G défini sur $\overline{\mathbf{Q}}$. D'après (4.1):

$$\ell_1/d_1 \le (n\rho - \kappa)/(d - n).$$

Si $d_1 = d$, alors $\ell_1 = \ell$ et

$$\mu(Y, \mathbf{C}^n) \le (\ell + \kappa)/n \le (d\rho - \kappa)/(d - n).$$

On supposera donc $0 < d_1 < d$. On considère le diagramme commutatif

$$\begin{tikzcd} \mathbf{C}^n \arrow[r, "\mathfrak{L}"] \arrow[dr, "\varphi"'] & T_G(\mathbf{C}) \arrow[r, "p_H"] \arrow[d] & T_{G/H}(\mathbf{C}) \arrow[d] \\ & G(\mathbf{C}) \arrow[r, "s_H"] & G/H(\mathbf{C}) \end{tikzcd}$$

où p_H et s_H sont les surjections canoniques, et les flèches verticales sont les exponentielles. Soit V le noyau de $p_H \circ \mathfrak{L}$. Comme $\varphi(\mathbf{C}^n)$ n'est pas contenu dans $H(\mathbf{C})$, on a $V \neq \mathbf{C}^n$. Enfin on note $Y' = Y \cap \varphi^{-1}(H)$. Ainsi le rang de Y' sur $\mathbf{Z}$ est $\ell + \kappa - \ell_1$.

1. On va d'abord montrer que si $V = 0$, on a

$$(\ell + \kappa)/n \le (d\rho - \kappa)/(d - n).$$

Supposons donc $p_H \circ \mathfrak{L}$ injective. Alors $n \le d_1$, et comme

$$p_H \circ \mathfrak{L}(Y') \subset \ker \exp_{G/H},$$

le rang de Y' est majoré par ρn, c'est-à-dire

$$\ell + \kappa \le \ell_1 + \rho n \le d_1 \frac{n\rho - \kappa}{d - n} + n\rho.$$

Si $d_1 = n$, on obtient

$$(\ell + \kappa)/n \leq \rho + \frac{n\rho - \kappa}{d - n} = (d\rho - \kappa)/(d - n).$$

Si $d_1 > n$, l'inégalité (4.1), appliquée à $\varphi_1 = s_H \circ \varphi$, avec $\rho(G/H) \leq \rho(G) = \rho$, et compte tenu du fait que $\dim \varphi_1 = \dim G/H = d_1$, donne

$$\mu(\Gamma/\Gamma \cap H, G/H) \leq (n\rho - \kappa_1)/(d_1 - n),$$

où $\kappa_1 = \operatorname{rang}_{\mathbf{Z}} \ker \varphi_1$. On a d'une part

$$\mu(\Gamma, G) \leq \mu(\Gamma/\Gamma \cap H, G/H),$$

avec, rappelons-le, $\mu(\Gamma, G) = \ell_1/d_1$, et d'autre part

$$Y' \subset \ker \varphi_1, \text{ donc } \kappa_1 \geq \ell + \kappa - \ell_1.$$

Alors

$$(d_1 - n)(\ell + \kappa - \kappa_1) \leq (d_1 - n)\ell_1 \leq d_1(n\rho - \kappa_1),$$

donc

$$d_1(\ell + \kappa - n\rho) \leq n(\ell + \kappa - \kappa_1) \leq n\ell_1 \leq n d_1 \ell/d,$$

et

$$d(\ell + \kappa - n\rho) \leq n\ell.$$

Finalement

$$(\ell + \kappa)/n \leq (d\rho - \kappa)/(d - n).$$

2. Ainsi le cas $V = 0$ est résolu. En particulier l'inégalité (4.2) est démontrée pour $n = 1$. On peut alors maintenant procéder par récurrence sur n, et supposer $V \neq 0$.

Notons p_V: $\mathbf{C}^n \to \mathbf{C}^n/V$ la surjection canonique. Il existe un homomorphisme injectif $\mathfrak{L}_1$: $\mathbf{C}^n/V \to T_{G/H}(\mathbf{C})$ tel que $\mathfrak{L}_1 \circ p_V = p_H \circ \mathfrak{L}$. Soit $\varphi_1 = \exp_{G/H} \circ \mathfrak{L}_1$: le diagramme

$$\begin{tikzcd} \mathbf{C}^n \arrow[r, "p_H \circ \mathfrak{L}"] \arrow[d, "p_V"'] & T_{G/H}(\mathbf{C}) \arrow[d, "\exp_{G/H}"] \\ \mathbf{C}^n/V \arrow[ur, "\mathfrak{L}_1"] \arrow[r, "\varphi_1"'] & G/H(\mathbf{C}) \end{tikzcd}$$

est commutatif. Notons $n_1 = n - \dim V$, $\kappa_1 = \operatorname{rang}_{\mathbf{Z}} \ker \varphi_1$, $Y_1 = p_V(Y)$, $Y_1' = p_V(Y')$, et $\lambda = \operatorname{rang}_{\mathbf{Z}} Y \cap V$. Ainsi, puisque $\varphi(V) \subset H$, on a $Y' \cap V = Y \cap V$,

$$\operatorname{rang}_{\mathbf{Z}} Y_1 = \ell + \kappa - \lambda, \ \operatorname{rang}_{\mathbf{Z}} Y_1' = \ell + \kappa - \lambda - \ell_1,$$

et, comme $Y_1' \subset \ker \varphi_1$,

$$\ell + \kappa - \lambda - \ell_1 \leq \kappa_1.$$

Remarquons que

$$\mu(Y, \mathbf{C}^n) \leq \mu(Y_1, \mathbf{C}^n/V) \leq (\ell + \kappa - \lambda)/n_1.$$

3. Supposons d'abord $d_1 = n_1$. Comme $\mathfrak{L}_1(\ker \varphi_1) \subset \ker \exp_{G/H}$, on a $\kappa_1 \leq n_1\rho$, et

$$(\ell + \kappa - \lambda)/n_1 \leq \rho + (\ell_1/n_1) \leq \rho + (n\rho - \kappa)/(d - n)$$
$$= (d\rho - \kappa)/(d - n),$$

et (4.2) en résulte.

4. Supposons maintenant $d_1 > n_1$. Grâce à l'hypothèse de récurrence et à l'inégalité $\rho(G/H) \leq \rho$, on a

$$\mu(Y_1, \mathbf{C}^n/V) \leq (d_1\rho - \kappa_1)/(d_1 - n_1);$$

on peut donc supposer

$$(d\rho - \kappa)/(d - n) \leq (d_1\rho - \kappa_1)/(d_1 - n_1),$$

ce qui s'écrit

$$d_1 n + \frac{\kappa_1}{\rho}(d - n) \leq dn_1 + \frac{\kappa}{\rho}(d_1 - n_1).$$

Alors on a

$$\ell + \kappa - \lambda - \kappa_1 \leq \ell_1$$

$$\leq d_1(n\rho - \kappa)/ (d - n)$$
$$\leq \frac{\rho}{d-n}\left(dn_1 + \frac{\kappa}{\rho}(d_1 - n_1) - \frac{\kappa_1}{\rho}(d - n)\right) - \frac{d_1\kappa}{d-n}$$
$$\leq \frac{d\rho n_1 - \kappa n_1}{d - n} - \kappa_1,$$

d'où

$$(l + \kappa - \lambda)/n_1 \leq (d\rho - \kappa)/(d - n),$$

ce qui termine la démonstration de (4.2).

Le corollaire 1.3 est une conséquence de (4.2): les trois hypothèses G commutatif, $\dim \varphi = \dim G$, et Y de type fini, ne font pas perdre de généralité.

c) *On suppose* $\mathfrak{L}$ *injective et* $m > n\rho$. *Alors*

(4.3) $$\mu(\varphi) \leq m/(m - n\rho).$$

Si $\mu(\varphi) \leq 1$, le résultat est banal. Supposons $\mu(\varphi) > 1$, donc $d > n$. On va démontrer (4.3) par récurrence sur n. Pour $n = 1$, on a $\mu(\varphi) = d$, et $\mu(Y, \mathbf{C}) = m$, donc (4.3) résulte de (4.2). Pour $n \geq 2$, on considère deux cas.

1. Si $\mu(Y, \mathbf{C}^n) = m/n$, on a grâce à (4.2)

$$m/n \leq d\rho/(d-n),$$

donc

$$\mu(\varphi) \leq d/n \leq m/(m - n\rho).$$

2. Si $\mu(Y, \mathbf{C}^n) < m/n$, le lemme 3.2 montre qu'il existe un sous-espace W de $\mathbf{C}^n$, de dimension $n' > 0$, tel que

$$\mu(Y', W) = m'/n' > m/n,$$

avec $Y' = Y \cap W$, $m' = \operatorname{rang}_{\mathbf{Z}} Y'$. On a alors $n' < n$, et on peut utiliser l'hypothèse de récurrence pour la restriction φ' de φ à W. On a $m'/n' > m/n > \rho$, donc

$$\mu(\varphi') \leq m'/(m' - n'\rho) \leq m/(m - n\rho).$$

Mais $\mu(\varphi) \leq \mu(\varphi')$. On en déduit (4.3).

d) *Démonstration du théorème* 1.1. Sous les hypothèses du théorème 1.1, on a $m > n\rho$ et $m/(m - n\rho) < d/n$, donc (4.3) implique $\mu(\varphi) < d/n$. Le lemme 3.3 permet de trouver un sous-espace V de $\mathbf{C}^n$, de codimension $n_1 > 0$, tel que l'adhérence de Zariski H de $\varphi(V)$ ait une codimension $d_1 > dn_1/n$, et que l'homomorphisme φ_1: $\mathbf{C}^n/V \to G/H$ défini par passage au quotient satisfasse $\mu(\varphi_1) = d_1/n_1$. En appliquant (4.3) à φ_1, on trouve que le rang m_1 de $Y/Y \cap V$ vérifie

$$(m_1 - n_1\rho_1)d_1 \leq m_1 n_1,$$

avec $\rho_1 = \rho(G/H)$. Comme $\rho_1 \leq \rho$, cela termine la démonstration du théorème 1.1.

5. Indépendance algébrique

Nous étudions ce qui se passe quand on remplace, dans ce qui précède, le corps $\overline{\mathbf{Q}}$ des nombres algébriques par une extension de $\mathbf{Q}$ de degré de transcendance 1. Le cas de $\mathbf{G}_m^d$ avait été esquissé dans [10, §8].

a) *Enoncé des résultats.* On désigne donc par K un sous-corps de $\mathbf{C}$ de degré de transcendance 1 sur $\mathbf{Q}$. Voici alors l'énoncé correspondant au théorème 1.1.

THÉORÈME 5.1. *Soient G un groupe algébrique de dimension d défini sur K, φ: $\mathbf{C}^n \to G(\mathbf{C})$ un sous-groupe à n paramètres de dimension d, et Y un sous-groupe de $\mathbf{C}^n$ de rang m sur $\mathbf{Z}$ tel que $\Gamma = \varphi(Y)$ soit contenu dans $G(K)$. On suppose*

$$md \geq 2n(m + d\rho).$$

Alors il existe un sous-espace vectoriel V de $\mathbf{C}^n$ tel que, si H désigne l'adhérence de Zariski sur K de $\varphi(V)$, et si on note

$$n_1 = \dim_{\mathbf{C}}(\mathbf{C}^n/V),\ d_1 = \dim(G/H),\ et\ m_1 = \mathrm{rang}_{\mathbf{Z}}(Y/Y \cap V),$$

on ait

$$n_1 > 0,\ d_1/n_1 > d/n,\ et\ m_1 d_1 < 2n_1(m_1 + d_1\rho).$$

En particulier on en déduit

$$\mu(\Gamma, G) < 2n\rho/(d - 2n)$$

et

$$\mu(Y, \mathbf{C}^n) < 2d\rho/(d - 2n).$$

Dans le cas $n = 1$, cette dernière inégalité s'énonce ainsi.

COROLLAIRE 5.2. *Soient G un groupe algébrique défini sur K, φ: $\mathbf{C} \to G(\mathbf{C})$ un sous-groupe à un paramètre de dimension algébrique $d \geq 3$, et Y un sous-groupe de $\mathbf{C}$ tel que $\varphi(Y) \subset G(K)$. Alors Y a un rang fini sur $\mathbf{Z}$, majoré par*

$$\mathrm{rang}_{\mathbf{Z}} Y < 2d\rho/(d - 2).$$

En particulier $\mathrm{rang}_{\mathbf{Z}} Y \leq 11$. Ce corollaire 5.2 contient des résultats d'indépendance sur les valeurs de la fonction exponentielle (Brownawell, Gel'fond, Smelev, Tijdeman, Waldschmidt, Wallisser) et sur les valeurs de fonctions elliptiques (Brownawell-Kubota, et Masser-Wüstholz; voir [5]).

COROLLAIRE 5.3. *Soient A une variété abélienne simple de dimension d définie sur K, φ: $\mathbf{C}^n \to A(\mathbf{C})$ un sous-groupe à n paramètres de A, et Y un sous-groupe de K^n de rang m sur $\mathbf{Z}$ tel que $\varphi(Y) \subset A(K)$. Alors*

$$md < 2n(m + 2d).$$

COROLLAIRE 5.4. *Soient G' et G'' deux groupes algébriques commutatifs connexes définis sur K, de dimensions respectives d' et d'', avec $d'' > 2d'$. Soit ψ: $G'(\mathbf{C}) \to G''(\mathbf{C})$ un homomorphisme analytique dont la différentielle à l'origine est injective. Soit Γ'' un sous-groupe de type fini de $G''(K)$ contenu dans l'image de ψ. Alors*

$$\mu(\Gamma'', G'') < 2d'\rho''/(d'' - 2d').$$

b) *Démonstrations.* La première étape de la démonstration du théorème 5.1 peut être faite sur une extension de $\mathbf{Q}$ de degré de transcendance fini quelconque.

PROPOSITION 5.5. *Soit K un sous-corps de $\mathbf{C}$ de degré de transcendance $q \geq 1$ sur $\mathbf{Q}$. On considère une base de transcendance $\theta_1, \ldots, \theta_q$ de K sur $\mathbf{Q}$. Soient G un groupe algébrique de dimension $d \geq 1$ défini sur K, φ: $\mathbf{C}^n \to G(\mathbf{C})$ un sous-groupe à n paramètres de G, et Γ un sous-groupe de type fini de $G(K)$ contenu dans $\varphi(\mathbf{C}^n)$. Notons*

$$\kappa = \kappa(\varphi), \mu = \mu(\Gamma, G), \gamma = \left(q + 1 + \frac{d\mu + \kappa}{\mu + \rho}\right) \Big/ (n + 1).$$

Alors il existe une suite $(P_N)_{N \geq N_0}$ de polynômes non nuls de $\mathbf{Z}[X_1, \ldots, X_q]$, vérifiant

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

et

$$\log|P_N(\theta_1, \ldots, \theta_q)| \leq - CN^{\gamma}(\log N)^{n/(n+1)},$$

où C ne dépend pas de N.

On a noté $H(P)$ la hauteur usuelle (= maximum des valeurs absolues des coefficients) du polynôme P. On notera que la conclusion est banale si $\gamma < q + 1$, c'est-à-dire si $(d - q - 1)\mu < \rho n(q + 1)$.

Pour démontrer la proposition 5.5, il est utile de remarquer d'abord que la proposition 2.1 (ou le théorème 3.1 de [10]) permet de construire une fonction auxiliaire à coefficients p_λ dans $\mathbf{Z}[\theta_1, \ldots, \theta_q]$: il suffit pour cela de l'appliquer aux fonctions

$$\theta_1^{\lambda_1} \ldots \theta_q^{\lambda_q} \varphi_\lambda, \qquad (1 \leq \lambda \leq L; 0 \leq \lambda_h \leq N, 1 \leq h \leq q).$$

L'hypothèse

$$c_2 U^{n+1} \leq L \,\Delta\, r^{\kappa} (\log R/r)^n$$

peut alors être remplacée par la condition plus faible

$$c_2' U^{n+1} \leq L \,\Delta\, N^q r^{\kappa} (\log R/r)^n.$$

On reprend ensuite la démonstration de la proposition 2.4, et le lemme de zéros 3.1 assure $P_N \neq 0$.

La suite de la démonstration du théorème 5.1 se fait alors comme au paragraphe 4: avec les notations du théorème 5.1, on démontre successivement

a) *si $\mathfrak{L}$ est injective, et $d > 2n$, alors*

$$\mu(\Gamma, G) < (2n\rho - \kappa)/(d - 2n). \tag{5.6}$$

Cette inégalité résulte de la proposition 5.5 et du critère de Gel'fond [2], p. 55.

b) *On suppose* $d > 2n$. *Alors*

$$\mu(Y, \mathbf{C}^n) < 2(d\rho - \kappa)/(d - 2n). \tag{5.7}$$

En particulier, pour $n = 1$, on trouve

$$(\ell + \kappa)d < 2\ell + 2d\rho,$$

ce qui améliore légérement le corollaire 5.2 (puisque $\ell \leq m \leq \ell + \kappa$).

c) *On suppose* $\mathfrak{L}$ *injective et* $m > 2n\rho$. *Alors*

$$\mu(\varphi) < 2m/(m - 2n\rho). \tag{5.8}$$

La fin de la démonstration du théorème 5.1 se fait comme au paragraphe 4.

6. Compléments

Nous terminons par quelques résultats complémentaires qui seront développés ailleurs. Nous étudions d'abord un analogue, pour les groupes algébriques, de la conjecture de Leopoldt sur le rang p-adique du groupe des unités d'un corps de nombres; il s'agit donc d'un problème d'indépendance algébrique de logarithmes. Nous considérons ensuite un problème d'indépendance linéaire de logarithmes. Le point de vue sous lequel nous abordons ces deux problèmes efface les périodes; en effet, la périodicité de φ n'apparaît pas dans le coefficient $\mu(\Gamma, G)$. Si on veut des énoncés qui en tiennent compte, il convient de s'intéresser plutôt à $\mu(Y, \mathbf{C}^n)$. Dans cette direction, nous regarderons quels résultats on peut espérer, soit en utilisant un lemme de Schwarz conjectural, soit en utilisant des lemmes de zéros multihomogènes. Nous donnerons ensuite un résultat quantitatif. Enfin nous reviendrons sur l'indépendance algébrique.

a) *Un analogue de la conjecture de Leopoldt pour les groupes algébriques.* Soient G un groupe algébrique commutatif de dimension $d \geq 1$ défini sur un corps de nombres K, et Γ un sous-groupe de type fini de $G(K)$, de rang $\ell \geq 1$.

Soit d'abord v une place infinie de K, correspondant à un plongement de K dans $\mathbf{C}$ (via $\mathbf{R}$ si v est réelle). Notons $r_v(\Gamma, G)$ le minimum des dimensions des sous-$\mathbf{C}$-espaces vectoriels $\mathbf{C}t_1 + \cdots + \mathbf{C}t_\ell$ de $T_G(\mathbf{C})$, quand $(t_1, \ldots, t_\ell)$ décrit les éléments de $(T_G(\mathbf{C}))^\ell$ tels que le sous-groupe de $G(\mathbf{C})$ engendré par les éléments

$$\gamma_j = \exp_G t_j, \qquad (1 \leq j \leq \ell)$$

soit un sous-groupe d'indice fini de Γ.

Du théorème 1.1 on déduit

$$r_v(\Gamma, G) \geq d\mu/(\mu + \rho), \qquad \text{avec } \mu = \mu(\Gamma, G). \tag{6.1}$$

On peut démontrer un analogue p-adique de ce résultat. Pour cela, soit K_v un complété de K en une place finie v. *Supposons* qu'il existe un sous-groupe compact de $G(K_v)$ contenant un sous-groupe Γ' d'indice fini de Γ. Nous désignerons par S l'ensemble formé des places archimédiennes de K, et des places finies de K vérifiant cette condition. Alors, pour v finie dans S, nous notons $r_v(\Gamma, G)$ la dimension du K_v-espace vectoriel engendré dans $T_G(K_v)$ par l'image de Γ' sous l'application logarithme de $G(K_v)$. Dans ces conditions l'inégalité (6.1) est valable pour tout $v \in S$.

Il serait intéressant de savoir si $r_v(\Gamma, G)$ dépend effectivement de v. On peut espérer que non. Dans cette direction, on peut montrer

$$r_{v_1}(\Gamma, G) \geq \frac{1}{\rho + 1} r_{v_2}(\Gamma, G) \qquad \text{pour } v_1 \text{ et } v_2 \text{ dans } S. \tag{6.2}$$

Dans le cas $G = \mathbf{G}_m^d$, cette inégalité (6.2) donne une minoration pour le rang p-adique du groupe des unités d'un corps de nombres [10].

b) *Indépendance linéaire de logarithmes.* Gardons les notations précédentes, et dans la définition de $r_v(\Gamma, G)$, au lieu de considérer la dimension du $\mathbf{C}$ (resp. du K_v) espace vectoriel engendré par les logarithmes dans l'espace tangent, regardons la dimension du K-espace vectoriel. On obtient un nombre $\tilde{r}_v(\Gamma, G)$, pour $v \in S$, et on peut montrer

$$\tilde{r}_{v_1}(\Gamma, G) \geq \frac{1}{\rho} \tilde{r}_{v_2}(\Gamma, G) \qquad \text{pour } v_1 \text{ et } v_2 \text{ dans } S. \tag{6.3}$$

Les résultats de Baker, Bertrand et Masser notamment fournissent de nombreux exemples de groupes algébriques G pour lesquels $\tilde{r}_v(\Gamma, G)$ est indépendant de $v \in S$.

La démonstration de (6.2) repose sur (6.1). De même, pour démontrer (6.3), on utilise la minoration suivante:

$$\tilde{r}_v(\Gamma, G) \geq \frac{1}{\rho} \operatorname{rang}_{\mathbf{Z}}(\Gamma/\Gamma \cap L_u) \qquad \text{pour tout } v \in S, \tag{6.4}$$

où L_u désigne le plus grand sous-groupe linéaire unipotent de G.

Pour $\rho = 1$, l'inégalité (6.4) est une conséquence du théorème de Baker sur l'indépendance linéaire (sur $\overline{\mathbf{Q}}$) de logarithmes usuels (voir [9], théorème 2.5.1). Pour $\rho = 2$, on démontre (6.4) en étudiant les points algébriques sur le graphe d'un homomorphisme analytique (cf. (6.7) ci-dessous).

c) *Lemme de Schwarz, et lemmes de zéros multihomogènes.* Avec les hypothèses de la proposition 2.4, supposons que la dimension algébrique de φ soit égale à d. En utilisant la méthode de [9, Chap. 8], on voit facilement que le lemme de Schwarz conjecturé dans [9, (7.1.10)] permettrait de démontrer l'inégalité suivante:

CONJECTURE 6.5. *Si $d > n$, alors*

$$\mu(Y, \mathbf{C}^n) \leq (d_1 + 2d_2 - \kappa)/(d - n).$$

Comme le lemme de Schwarz est vrai en une variable, on a, pour $n = 1$ et $d \geq 2$,

$$\operatorname{rang}_{\mathbf{Z}} Y \leq (d_1 + 2d_2 - \kappa)/(d - 1). \tag{6.6}$$

En fait, on constate facilement que cette inégalité (6.6) résume les résultats du Chapitre 4 de [9].

L'inégalité (4.2) correspond aux deux cas particuliers suivants de la conjecture 6.5:

$$d_0 = d_2 = 0,\ d_1 = d \text{ (pour } \rho = 1)$$

et

$$d_0 = d_1 = 0,\ d_2 = d \text{ (pour } \rho = 2).$$

Pour démontrer le cas général de la conjecture 6.5 par la méthode présentée ici, il semble nécessaire de disposer de lemmes de zéros plus précis que ceux de [4]. Ainsi, en utilisant une version raffinée, due à Masser et Wüstholz, du théorème B de [4], on peut démontrer le cas particulier suivant de 6.5, correspondant à $d_0 = n$, et $d_1 = 0$ ou $d_2 = 0$ (voir [9], théorème 6.3.2 et théorème 8.1.1):

(6.7) *Soient φ: $\mathbf{C}^n \to G(\mathbf{C})$ un homomorphisme analytique, et Y un sous-groupe de $\overline{\mathbf{Q}}^n$ de rang $\geq \rho n + 1$ sur $\mathbf{Z}$, tel que $\varphi(Y) \subset G(\overline{\mathbf{Q}})$. Alors il existe $y \in Y$, $y \neq 0$, tel que l'homomorphisme $t \mapsto \varphi(yt)$ de $\mathbf{C}$ dans $G(\mathbf{C})$ soit rationnel.*

On peut poser un problème analogue à (6.5) dans lequel on remplace $\overline{\mathbf{Q}}$ par une extension de $\mathbf{Q}$ de degré de transcendance fini $q \geq 1$, mais il n'y a que dans le cas $q = 1$ que la méthode actuelle semble suffisante; la conclusion devrait être: pour $d > 2n$ et $q = 1$,

$$\mu(Y, \mathbf{C}^n) < 2(d_1 + 2d_2 - \kappa)/(d - 2n).$$

Enfin les théorèmes A et C de [4] devraient permettre d'obtenir de nouveaux énoncés de transcendance et d'indépendance algébrique avec des hypothèses de normalisation.

d) *Approximation diophantienne.* Soient $\log \alpha_1, \ldots, \log \alpha_{n+1}$ des logarithmes complexes de nombres algébriques $\alpha_1, \ldots, \alpha_n$ non nuls, et soient $\beta_1, \ldots, \beta_n$ des nombres algébriques. Posons

$$\Lambda = \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n - \log \alpha_{n+1}.$$

En notant $(e_1, \ldots, e_n)$ la base canonique de $\mathbf{C}^n$, on définit des éléments $t_1, \ldots, t_{n+1}$ de $\mathbf{C}^{n+1}$ par

$$t_j = \left(e_j, \log \alpha_j\right) \quad \text{pour } 1 \leq j \leq n,$$

et

$$t_{n+1} = (\beta_1, \ldots, \beta_n, \log \alpha_{n+1}).$$

Alors la condition $\Lambda \neq 0$ équivaut à dire que $t_1, \ldots, t_{n+1}$ sont **C**-linéairement indépendants, et minorer $|\Lambda|$ équivaut à minorer

$$\Delta_V = \sum_{j=1}^{n+1} \operatorname{dist}\left(t_j, V\right),$$

quand V est un sous-espace vectoriel de $\mathbf{C}^{n+1}$ de dimension n sur $\mathbf{C}$, et $\operatorname{dist}(t, V)$ est la distance, dans $\mathbf{C}^{n+1}$, de t à V. Plus précisément, avec la norme

$$|z| = \max_{1 \leq j \leq n+1} |z_j| \quad \text{pour } z = \left(z_1, \ldots, z_{n+1}\right) \in \mathbf{C}^{n+1},$$

on a d'une part

$$\operatorname{dist}\left(t_{n+1}, \mathbf{C}t_1 + \cdots + \mathbf{C}t_n\right) \leq |\Lambda|,$$

et, d'autre part, pour tout sous-espace V de codimension 1 dans $\mathbf{C}^{n+1}$,

$$|\Lambda| \leq 2\left(1 + \sum_{j=1}^{n} |\beta_j|\right)\left(1 + \sum_{j=1}^{n+1} |\log \alpha_j|\right) \Delta_V.$$

Les hypothèses arithmétiques sur $\alpha_1, \ldots, \alpha_{n+1}, \beta_1, \ldots, \beta_n$ se traduisent par le fait que si $G = \mathbf{G}_a^n \times \mathbf{G}_m$, le sous-groupe Γ de $G(\mathbf{C})$ engendré par les points $\gamma_j = \exp_G t_j$ est en fait contenu dans $G(\overline{\mathbf{Q}})$; ici, pour $z = (z_1, \ldots, z_{n+1}) \in \mathbf{C}^{n+1}$, on a noté (abusivement) $\exp_G z = (z_1, \ldots, z_n, \exp(z_{n+1}))$.

Considérons maintenant un groupe algébrique commutatif G défini sur $\overline{\mathbf{Q}}$, et des éléments $t_1, \ldots, t_\ell$ de $T_G(\mathbf{C})$ dont les images par $\exp_G$ sont dans $G(\overline{\mathbf{Q}})$. Notons r la dimension du **C**-espace vectoriel engendré par $t_1, \ldots, t_\ell$. Le problème consiste à minorer

$$\sum_{j=1}^{\ell} \operatorname{dist}\left(t_j, V\right)$$

quand V est un sous-espace vectoriel de $T_G(\mathbf{C})$ de dimension $< r$ sur $\mathbf{C}$, et la distance est relative au choix d'une base de T_G.

Dans cette direction, on peut montrer que si la dimension n de V sur $\mathbf{C}$ vérifie

$$n < d\mu/(\mu + \rho),$$

avec $\mu = \mu(\Gamma, G)$, on a

(6.8) $$\sum_{j=1}^{\ell} \operatorname{dist}(t_j, V) > \exp(-C(\log A)^{\gamma}),$$

avec

$$\gamma = d\mu/(d\mu - n(\mu + \rho)),$$

et

$$A = \max_{1 \le j \le \ell} \max(e, H(\gamma_j), \exp|t_j|),$$

où H est la hauteur absolue sur l'espace projectif $\mathbf{P}_N(\overline{\mathbf{Q}})$ dans lequel on a plongé $G(\overline{\mathbf{Q}})$.

Des versions raffinées de (6.8) conduisent à de nouvelles minorations de formes linéaires de logarithmes. Le cas d'une courbe elliptique avec multiplications complexes (c'est-à-dire ici $G = \mathbf{G}_a^n \times E$) a été explicité par Yu Kun Rui. D'autre part le choix $G = \mathbf{G}_m^d$ donne des versions effective du théorème 1.1 de [10]; pour $n = 1$, on obtient une minoration de la forme

$$\sum_{i=2}^{d} \sum_{j=2}^{\ell} \left| \frac{\log \alpha_{ij}}{\log \alpha_{1j}} - \frac{\log \alpha_{i1}}{\log \alpha_{11}} \right| > \exp\{-C(\log A)^{\gamma}\},$$

avec $\gamma = \ell d/(\ell d - \ell - d)$, où les α_{ij}, $(1 \le i \le d,\ 1 \le j \le \ell$, et $\ell d > \ell + d)$ sont des nombres algébriques non nuls de hauteur $\le A$, avec $|\log \alpha_{ij}| \le \log A$, et de plus

$$\log \alpha_{11}, \ldots, \log \alpha_{1\ell} \text{ sont } \mathbf{Q}\text{-linéairement indépendants},$$

et

$$\log \alpha_{11}, \ldots, \log \alpha_{d1} \text{ sont } \mathbf{Q}\text{-linéairement indépendants}.$$

On en déduit des résultats antérieurs (Shorey, Srinivasan, Mignotte et Waldschmidt) sur l'approximation simultanée de nombres de la forme $\exp(x_i y_j)$, $(x_i \in \mathbf{C},\ y_j \in \mathbf{C})$ par des nombres algébriques.

e) *Indépendance algébrique.* Soient K un sous-corps de $\mathbf{C}$ de type fini sur $\mathbf{Q}$ et de degré de transcendance $q \ge 0$ sur $\mathbf{Q}$, et G un groupe algébrique commutatif défini sur K, de dimension $d \ge 1$. On considère un sous-groupe à n paramètres $\varphi\colon \mathbf{C}^n \to G(\mathbf{C})$ de G, et un sous-groupe Γ de $\varphi(\mathbf{C}^n) \cap G(K)$. On note $\rho = \rho(G)$, $\kappa = \kappa(\varphi)$, et $\mu = \mu(\Gamma, G)$.

Il semble raisonnable d'espérer, dans ces conditions, l'inégalité

(6.9) $\kappa + d\mu \le n(q+1)(\mu + \rho)$, avec l'inégalité stricte si $q > 0$, qui généraliserait (4.1) (correspondant à $q = 0$) et (5.6) (correspondant à $q = 1$). Des progrès récents en direction de (6.9) ont été obtenus par P. Philippon [7].

Si on suppose que le corps K a un type de transcendance $\leq \tau$ (cf. [2], Chap. 5), les méthodes précédentes conduisent à l'inégalité

$$\kappa + d\mu \leq n\tau(\mu + \rho) + (\mu + \rho)(\tau - q - 1), \text{ avec l'inégalité stricte si } \tau > 1.$$

On utilise alors la remarque suivante (cf. [6], §6β): si on remplace G par une puissance de G, et φ par la même puissance de φ, on voit que κ, d, n sont homogènes de poids 1, tandis que ρ, μ, τ, q sont invariants (homogènes de poids 0), d'où

$$\kappa + d\mu \leq n\tau(\mu + \rho).$$

INSTITUT HENRI POINCARÉ, PARIS, FRANCE

REFERENCES

[1] E. BOMBIERI and S. LANG, Analytic subgroups of group varieties, Invent. Math. 11 (1970), 1–14.
[2] S. LANG, *Introduction to Transcendental Numbers*, Addison-Wesley, 1966.
[3] D. W. MASSER, Polynomial interpolation in several complex variables, J. Approximation Theory, **24** (1978), 18–34.
[4] D. W. MASSER AND G. WÜSTHOLZ, Zero estimates on group varieties I, Invent. Math. **64** (1981), 489-516.
[5] ______ Algebraic independence properties of values of elliptic functions, Proc. Exeter Journées Arithmétiques 1980, ed. J. V. Armitage, Cambridge, England (1982), 360–363.
[6] P. PHILIPPON, Indépendance algébrique de valeurs de fonctions exponentielles p-adiques, J. Reine Angew. Math., **329** (1981), 42–51.
[7] ______, Indépendance algébrique et variétés abéliennes; C. R. Acad. Sc. Paris, Sér. A, **294** (1982), 257–259.
[8] J-P. SERRE, Quelques propriétés des groupes algébriques commutatifs; Appendice 2 de [9].
[9] M. WALDSCHMIDT, Nombres transcendants et groupes algébriques, Astérisque, 69–70, Soc. Math. France 1979.
[10] ______, Transcendance et exponentielles en plusieurs variables, Invent. Math. **63** (1981), 97–127.

(Received December 28, 1981)