"Approximations diophantiennes et nombres transcendants"
Luminy, 1982
Progress in Mathematics
Birkhäuser (1983)

DÉPENDANCE DE LOGARITHMES DANS LES GROUPES ALGÉBRIQUES

M. WALDSCHMIDT

La conjecture de Leopoldt sur le rang p-adique du groupe des unités d'un corps de nombres algébriques peut être considérée comme un cas particulier de la conjecture suivante (cf. [7]).

Soient α_{ij} , $(1 \leqslant i \leqslant d \ , \ 1 \leqslant j \leqslant \ell)$ des nombres algébriques non nuls, ι un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}$, p un nombre premier, et ι_p un plongement de $\bar{\mathbb{Q}}$ dans $\mathbb{C}_p$. On suppose que les nombres $\iota_p \alpha_{ij}$ sont des unités p-adiques. Notons r_p le rang de la matrice $d \times \ell$

$$(\log_p \iota_p \alpha_{ij})_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant \ell} \ ,$$

et r° celui de

$$(\log |\iota \alpha_{ij}|)_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant \ell} \ .$$

Enfin désignons par r le minimum des rangs des matrices $(z_{ij})_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant \ell}$, quand (z_{ij}) décrit les éléments de $\mathbb{C}^{\ell d}$ tels qu'il existe $m \in \mathbb{Z}$, $m > 0$, avec

$$e^{z_{ij}} = \iota \alpha_{ij}^m \ , \qquad (1 \leqslant i \leqslant d \ , \ 1 \leqslant j \leqslant \ell).$$

Autrement dit

$$r = \min \operatorname{rang} (\log \iota \alpha_{ij}^m)_{1 \leqslant i \leqslant d, 1 \leqslant j \leqslant \ell} \ ,$$

quand m décrit les entiers strictement positifs, et, pour chaque (i,j), $\log \iota\alpha_{ij}^m$ décrit toutes les déterminations du logarithme de $\iota\alpha_{ij}^m$.

CONJECTURE : $r = r_p \geqslant r^\circ$.

Cette conjecture est en fait une conséquence de celles de Schanuel dans $\mathbb{C}$ et $\mathbb{C}_p$ (cf. [7]).

Nous avons montré dans [7] les inégalités

$$r_p \geqslant r/2 \ , \ r_p \geqslant r^\circ/2 \ , \ r \geqslant r_p/2 \ , \ r \geqslant r^\circ/2 \ ,$$

et aussi, pour deux nombres premiers p_1 et p_2 ,

$$r_{p_1} \geqslant r_{p_2}/2 \ .$$

La situation que nous venons de décrire concerne le groupe algébrique $\mathbb{G}_m^d$, produit de d copies du groupe multiplicatif $\mathbb{G}_m$, et le sous-groupe de $\bar{\mathbb{Q}}^{xd}$ engendré par les ℓ éléments

$$(\alpha_{1j},\dots,\alpha_{dj}) \in \bar{\mathbb{Q}}^{xd} \ , \qquad (1 \leqslant j \leqslant \ell).$$

Nous considérons plus généralement un groupe algébrique commutatif G de dimension $d \geqslant 1$ défini sur un corps de nombres K , et un sous-groupe de type fini Γ de $G(K)$ de rang $\ell \geqslant 1$. Nous allons construire un ensemble $\mathcal{S}$ de places de K , contenant toutes les places infinies, et contenant toutes les places de K sauf un nombre fini d'entre elles, et, pour chaque $v \in \mathcal{S}$, nous allons définir un nombre $r_v = r_v(\Gamma,G)$. Nous montrerons alors que si v_1 et v_2 sont deux éléments de $\mathcal{S}$, on a

$$r_{v_1} \geqslant r_{v_2}/3 \ .$$

Quand G est un groupe algébrique linéaire, ou encore une puissance d'une courbe elliptique ayant multiplication complexe, on peut remplacer le coefficient $1/3$ par $1/2$.

Voici la définition de r_v . Pour commencer soit K_v un complété de K en une place finie v ; nous supposons qu'il existe un sous-groupe compact de $G(K_v)$ contenant un sous-groupe Γ' d'indice fini de Γ , et nous définissons $\mathcal{S}$ comme l'ensemble des places archimédiennes et des places finies vérifiant cette condition. On note alors $r_v(\Gamma,G)$ la dimension du K_v-espace vectoriel engendré dans l'espace tangent à l'origine $T_G(K_v)$ par l'image de Γ' sous l'application logarithme de $G(K_v)$.

Pour une place infinie v de K , correspondant à un plongement de K dans $\mathbb{C}$, nous définissons $r_v(\Gamma,G)$ comme le minimum des dimensions des sous-$\mathbb{C}$-espaces vectoriels $\mathbb{C}t_1+\ldots+\mathbb{C}t_\ell$ de $T_G(\mathbb{C})$, quand $(t_1,\ldots,t_\ell)$ décrit les éléments de $(T_G(\mathbb{C}))^\ell$ tels que le sous-groupe de $G(\mathbb{C})$ engendré par les ℓ éléments

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

soit d'indice fini dans Γ .

Quand $G = \mathbb{G}_m^d$, on retrouve la situation précédente.

Il serait intéressant, dans le cas général, de savoir si $r_v(\Gamma,G)$ est en fait indépendant de $v \in \mathcal{S}$, et dans ce cas de donner une description "algébrique" de ce nombre.

Nous montrerons qu'il existe deux sous-groupes algébriques H et H' de G , définis sur K , de dimension respectivement $\delta < d$ et $\delta' > 0$, tels que, si λ (resp. λ') désigne le rang de $\Gamma \cap H$ (resp. $\Gamma \cap H'$), on ait

$$r_v(\Gamma,G) \geqslant d \, \frac{\ell-\lambda}{\ell-\lambda+2(d-\delta)}$$

et

$$r_v(\Gamma,G) \geqslant \ell \, \frac{\delta'}{\lambda'+2\delta'} .$$

Pour démontrer la première minoration, on utilisera le lemme de zéros de Masser et Wüstholz [3] et la fonction auxiliaire de [6], tandis que la deuxième minoration reposera sur un lemme d'interpolation de [2] et sur une nouvelle fonction auxiliaire. En fait quand v est une place

finie nous verrons que ces deux inégalités peuvent être déduites l'une de l'autre directement.

Nous utiliserons ces minorations pour établir les inégalités $r_{v_1} \geqslant r_{v_2}/3$. Quand v_1 et v_2 sont finies, on se ramène au cas $r_{v_2} = \ell$ et on montre qu'alors $\lambda' \leqslant \delta'$, donc la deuxième minoration donne $r_{v_1} \geqslant \ell/3$. Quand l'une au moins des places v_1 , v_2 est infinie, quelques arguments supplémentaires sont nécessaires pour tenir compte des périodes de l'exponentielle $\exp_G : T_G(\mathbb{C}) \longrightarrow G(\mathbb{C})$.

Le plan de ce travail est le suivant. Dans une première partie (§1) nous étudions les coefficients

$$\mu(\Gamma,G) = \min_H \frac{\ell-\lambda}{d-\delta} \quad \text{et} \quad \mu^*(\Gamma,G) = \max_{H'} \frac{\lambda'}{\delta'}$$

qui interviennent dans le lemme de zéros et dans le lemme d'interpolation respectivement. Ensuite nous étudions r_v pour une place v finie (§2), puis pour une place v infinie (§3). Enfin (§4), nous comparons r_{v_1} et r_{v_2} .

Il sera commode de définir un nombre ρ de la manière suivante : $\rho = 1$ si G est un groupe algébrique linéaire, $\rho = 2$ sinon. Ainsi le résultat principal (théorème 4.1) s'écrira :

$$r_{v_1}(\Gamma,G) \geqslant \frac{1}{\rho+1}\, r_{v_2}(\Gamma,G) \ .$$

§1. LE LEMME DE ZÉROS ET LE LEMME D'INTERPOLATION.

a) Définition de ω et ω^* .

Soient K un corps de caractéristique zéro, V une sous-variété quasi-projective de $\mathbb{P}_N(K)$, et E une partie finie non vide de V . On note $\omega(E,V)$ le plus petit des degrés des hypersurfaces de $\mathbb{P}_N(K)$ contenant E mais ne contenant pas V .

De plus, quand $\text{card } E \geqslant 2$, on note $\omega^*(E)$ le plus petit des entiers $D > 1$ ayant la propriété suivante : pour tout $\sigma \in E$, il existe une hypersurface algébrique de $\mathbb{P}_N(K)$, de degré $< D$, contenant $E-\{\sigma\}$ mais ne passant pas par σ .

Un "lemme de zéros" est une minoration de $\omega(E,V)$, tandis qu'un "lemme d'interpolation" est une majoration de $\omega^*(E)$. Nous nous intéresserons ici au cas où $V = G(K)$, G étant un groupe algébrique commutatif, et où l'ensemble E est de la forme

$$\Gamma(S) = \{h_1\gamma_1+\ldots+h_\ell\gamma_\ell \ ; \ (h_1,\ldots,h_\ell) \in \mathbb{Z}^\ell \ , \ 0 \leqslant h_j < S\} \ ,$$

avec

$$\Gamma = \mathbb{Z}\gamma_1+\ldots+\mathbb{Z}\gamma_\ell \subset G(K) \ .$$

b) Définition de μ et μ^* .

Soient G un groupe algébrique commutatif de dimension $d \geqslant 1$ défini sur un corps K de caractéristique nulle, et Γ un sous-groupe de type fini de $G(K)$, de rang ℓ sur $\mathbb{Z}$. On définit

$$\mu(\Gamma,G) = \min_H\{(\ell - \text{rang}_{\mathbb{Z}}\Gamma\cap H)/(d - \dim H)\}$$

quand H décrit les sous-groupes algébriques de G , définis sur K , et de dimension $< d$, et

$$\mu^*(\Gamma,G) = \max_{H'}\{(\text{rang}_{\mathbb{Z}}\Gamma\cap H')/\dim H'\} \ ,$$

quand H' décrit les sous-groupes algébriques de G, définis sur K, et de dimension > 0.

On a évidemment

$$\mu(\Gamma,G) \leqslant \frac{\ell}{d} \leqslant \mu^*(\Gamma,G) .$$

c) Les résultats de Masser-Wüstholz [3] et de Masser [2].

On considère de nouveau un groupe algébrique G commutatif connexe défini sur un corps K de caractéristique zéro, plongé comme variété quasi-projective dans un espace projectif $\mathbb{P}_N$. Comme dans [3], par abus de notation, on écrira G pour $G(K)$. On considère des éléments $\gamma_1,\ldots,\gamma_\ell$ linéairement indépendants sur $\mathbb{Z}$ dans G, on note Γ le sous-groupe de G qu'ils engendrent, et $\Gamma(S)$ la partie finie de Γ formée des combinaisons linéaires à coefficients entre 0 et S comme ci-dessus.

Il est facile de voir [3] qu'il existe une constante $c_1 > 0$, ne dépendant que de $\gamma_1,\ldots,\gamma_\ell$ et de G plongé dans $\mathbb{P}_N$ telle que, pour tout réel $S \geqslant 1$, on ait

$$\omega(\Gamma(S),G) \leqslant c_1 S^{\mu(\Gamma,G)} .$$

Par conséquent le lemme de zéros suivant [3] est le meilleur possible.

THEOREME 1.1 (Masser-Wüstholz [3]). *Il existe une constante $c_2 > 0$ telle que, pour tout réel $S \geqslant 1$, on ait*

$$\omega(\Gamma(S),G) \geqslant c_2 S^{\mu(\Gamma,G)} .$$

Le résultat principal de [3] est en fait un peu plus précis ; en particulier la constante c_2 y est donnée explicitement.

D'autre part il est facile de minorer ω^* : il existe une constante $c_3 > 0$ telle que pour tout réel $S \geqslant 1$ on ait

$$\omega^*(\Gamma(S)) \geqslant c_3 S^{\mu^*(\Gamma,G)} ,$$

et ainsi le lemme d'interpolation suivant [2] est le meilleur possible.

THEOREME 1.2 (Masser [2]). Il existe une constante $c_4 > 0$ telle que, pour tout réel $S \geq 1$, on ait

$$\omega^*(\Gamma(S)) \leq c_4 S^{\mu^*(\Gamma,G)} .$$

d) Etude du coefficient μ.

Nous reprenons les notations du b) ci-dessus ; en particulier il n'est pas utile ici de plonger G dans un espace projectif. Nous aurons besoin de quelques informations complémentaires, assez simples, sur μ.

Remarquons d'abord que si H est un sous-groupe algébrique de G, de dimension $< d$, défini sur K, alors

$$\mu(\Gamma/\Gamma\cap H, G/H) = \min_{H'}\{(\mathrm{rang}_{\mathbb{Z}}\Gamma/\Gamma\cap H')/\dim G/H'\} ,$$

quand H' décrit les sous-groupes algébriques de G, contenant H, de dimension $< d$, et définis sur K. En particulier

$$\mu(\Gamma/\Gamma\cap H, G/H) \geq \mu(\Gamma,G) .$$

LEMME 1.3. Soit H un sous-groupe algébrique de G, défini sur K, de dimension $\delta < d$, tel que

$$\mu(\Gamma,G) = (\ell-\lambda)/(d-\delta) ,$$

avec $\lambda = \mathrm{rang}_{\mathbb{Z}}\Gamma\cap H$. On suppose $\lambda > 0$. Alors

$$\mu(\Gamma\cap H, H) \geq \mu(\Gamma,G) .$$

Démonstration. Il suffit de reprendre la démonstration du lemme 1.3.2 de [5]. La condition $\lambda > 0$ assure $\delta > 0$.

Remarque. Il peut arriver que, pour tous les sous-groupes algébriques H de G vérifiant l'hypothèse du lemme 1.3, on ait

$$\mu(\Gamma\cap H,H) < \lambda/\delta .$$

C'est le cas par exemple pour $G = G_a^3$, $d = 3$, $\ell = 6$, et

$$\Gamma = \mathbb{Z}^3 + \mathbb{Z}(x_1,0,0) + \mathbb{Z}(x_2,0,0) + \mathbb{Z}(0,y,0) ,$$

avec $y \notin \mathbb{Q}$, et $1,x_1,x_2$ $\mathbb{Q}$-linéairement indépendants (avec $\mu(\Gamma,G) = 1$). Le lemme qui suit fournit un palliatif.

LEMME 1.4. *Il existe un entier* $\nu \geqslant 0$ *et des sous-groupes algébriques* H_i , $(0 \leqslant i \leqslant \nu+1)$ *de* G , *définis sur* K , *avec*

$$G = H_0 \supset H_1 \supset \ldots \supset H_{\nu+1} = 0 ,$$

de dimension respective

$$d = \delta_0 > \delta_1 > \ldots > \delta_{\nu+1} = 0 ,$$

tels que, si on note

$$\Gamma_i = \Gamma\cap H_i \quad , \quad \lambda_i = \operatorname{rang}_{\mathbb{Z}} \Gamma_i \quad , \quad (0 \leqslant i \leqslant \nu+1),$$

on ait

$$\mu(\Gamma_i,H_i) = (\lambda_i-\lambda_{i+1})/(\delta_i-\delta_{i+1}) \quad , \quad (0 \leqslant i \leqslant \nu),$$

avec, pour $1 \leqslant i \leqslant \nu$,

$$\frac{\lambda_i}{\delta_i} > \frac{\lambda_{i-1}}{\delta_{i-1}} \quad \text{et} \quad \mu(\Gamma_i,H_i) \geqslant \mu(\Gamma_{i-1},H_{i-1}) .$$

Démonstration. Supposons construits $H_0,\ldots,H_i$, avec $i \geqslant 0$. On considère deux cas. Si $\mu(\Gamma_i,H_i) = \lambda_i/\delta_i$, on choisit $\nu = i$. Sinon, on utilise la définition de μ : il existe un sous-groupe algébrique H_{i+1} de H_i , de dimension $\delta_{i+1} < \delta_i$, tel que

$$\mu(\Gamma_i,H_i) = (\lambda_i-\lambda_{i+1})/(\delta_i-\delta_{i+1}) ,$$

avec $\lambda_{i+1} = \operatorname{rang}_{\mathbb{Z}}\Gamma\cap H_{i+1}$. Alors

$$\frac{\lambda_i-\lambda_{i+1}}{\delta_i-\delta_{i+1}} < \frac{\lambda_i}{\delta_i} \quad \text{et} \quad \delta_{i+1} > 0 ,$$

donc

$$\lambda_{i+1}/\delta_{i+1} > \lambda_i/\delta_i .$$

De plus le lemme 1.3 implique $\mu(\Gamma_{i+1},H_{i+1}) \geqslant \mu(\Gamma_i,H_i)$. Enfin, comme $\delta_{i+1} < \delta_i$, la construction s'arrête pour un ν vérifiant $0 \leqslant \nu < d$.

e) Etude du coefficient μ^* .

Le coefficient μ^* jouit de propriétés analogues à celles du coefficient μ , à condition de changer le sens des inégalités, et de remplacer les sous-groupes par des quotients. Voici par exemple les énoncés correspondants aux lemmes 1.3 et 1.4. Comme les démonstrations sont similaires, nous les omettrons.

Si H est un sous-groupe algébrique de G , de dimension > 0 , défini sur K , alors

$$\mu^*(\Gamma \cap H,H) \leqslant \mu^*(\Gamma,G) .$$

LEMME 1.5. Soit H un sous-groupe algébrique de G , défini sur K , de dimension $\delta > 0$, tel que

$$\mu^*(\Gamma,G) = \frac{\lambda}{\delta} > \frac{\ell}{d} ,$$

avec $\lambda = \mathrm{rang}_{\mathbb{Z}} \Gamma \cap H$. Alors

$$\mu^*(\Gamma/\Gamma \cap H,G/H) \leqslant \mu^*(\Gamma,G) .$$

LEMME 1.6. Il existe un entier $\nu \geqslant 0$ et des sous-groupes algébriques H_i , $(0 \leqslant i \leqslant \nu+1)$ de G , définis sur K , avec

$$0 = H_0 \subset H_1 \subset \ldots \subset H_{\nu+1} = G ,$$

de dimension respective

$$0 = \delta_0 < \delta_1 < \ldots < \delta_{\nu+1} = d ,$$

tels que si on note

$$\Gamma_i = \Gamma \cap H_i \quad , \quad \lambda_i = \mathrm{rang}_{\mathbb{Z}} \Gamma_i \quad , \quad (0 \leqslant i \leqslant \nu+1),$$

on ait

$$\mu^*(\Gamma/\Gamma_i, G/H_i) = (\lambda_{i+1}-\lambda_i)/(\delta_{i+1}-\delta_i) ,$$

avec, pour $1 \leqslant i \leqslant \nu$,

(1.7) $$(\lambda_i-\lambda_{i-1})/(\delta_i-\delta_{i-1}) > (\ell-\lambda_{i-1})/(d-\delta_{i-1})$$

et

$$\mu^*(\Gamma/\Gamma_i, G/H_i) \leqslant \mu^*(\Gamma/\Gamma_{i-1}, G/H_{i-1}).$$

On notera que la condition (1.7) s'écrit de manière équivalente

$$(\ell-\lambda_i)/(d-\delta_i) < (\ell-\lambda_{i-1})/(d-\delta_{i-1}) .$$

§2. ÉTUDE LOCALE p-ADIQUE.

On désigne par k un corps non archimédien complet localement compact de caractéristique nulle et de caractéristique résiduelle $p \neq 0$. On note $\mathfrak{o}$ son anneau d'entiers, ∂ son degré sur $\mathbb{Q}_p$, et $|\ |$ sa valeur absolue normalisée par $|p| = p^{-1}$. De manière générale, nous utiliserons les notations de [1].

a) Définition de $r(\Gamma,G,k)$ et énoncé des résultats.

Soient G un groupe algébrique commutatif défini sur k, et soit Γ un sous-groupe de type fini de $G(k)$, de rang $\ell \geqslant 1$ sur $\mathbb{Z}$. On suppose qu'il existe un sous-groupe Γ' d'indice fini de Γ qui est contenu dans un sous-groupe compact de $G(k)$. On note $r(\Gamma,G,k)$ la dimension du k-espace vectoriel engendré, dans l'espace tangent à l'origine $T_G(k)$ de G, par l'image de Γ' sous l'application logarithme de G (cf. [1] §4.1).

Soit $\mathcal{V}$ un sous-groupe ouvert suffisamment petit de $G(k)$ sur lequel l'application logarithme de G induit un difféomorphisme à valeurs dans $T_G(k)$. Grâce à notre hypothèse $\mathcal{V} \cap \Gamma$ est un sous-groupe d'indice fini de Γ, donc on peut choisir $\gamma_1,\ldots,\gamma_\ell$ dans $\mathcal{V} \cap \Gamma$ linéairement indépendants sur $\mathbb{Z}$; si $t_1,\ldots,t_\ell$ sont leurs logarithmes dans $T_G(k)$, la dimension du k-espace vectoriel engendré par $t_1,\ldots,t_\ell$ est égale à $r(\Gamma,G,k)$. Ainsi $r(\Gamma,G,k)$ est le plus petit des entiers $n \geqslant 1$ pour lesquels il existe un homomorphisme analytique

$$\varphi : \mathfrak{o}^n \longrightarrow G(k)$$

avec la propriété que $\varphi(\mathfrak{o}^n) \cap \Gamma$ soit un sous-groupe d'indice fini de Γ.

Soit d la dimension de G. On a évidemment

$$r(\Gamma,G,k) \leqslant \min(\ell,d) .$$

D'autre part si k' est une extension finie de k, on a

$$r(\Gamma,G,k) = r(\Gamma,G,k')$$

(comparer avec la démonstration du corollaire 4.2.p de [6]). Si H est un sous-groupe algébrique de G défini sur k et contenant Γ, alors

$$r(\Gamma,G,k) = r(\Gamma,H,k) .$$

Enfin, si Γ est un sous-groupe fini de $G(k)$, nous poserons $r(\Gamma,G,k) = 0$.

Le résultat principal de ce §2 est le suivant.

THÉOREME 2.1. *On suppose que* G *est défini sur un corps de nombres* K *contenu dans* k, *et que* Γ *est contenu dans* $G(K)$. *On note*

$$r = r(\Gamma,G,k) , \quad \mu = \mu(\Gamma,G) , \quad \text{et} \quad \mu^* = \mu^*(\Gamma,G) .$$

Alors on a

$$r \geqslant d\mu/(\mu+\rho) \tag{2.2}$$

et

$$r \geqslant \ell/(\mu^*+\rho) . \tag{2.3}$$

Dans un premier temps, nous montrons qu'il suffit d'établir l'une des deux inégalités : l'autre s'en déduit comme corollaire. Puis nous donnons une démonstration de (2.2) en utilisant le lemme de zéros 1.1, et enfin nous donnons une (deuxième) démonstration de (2.3) en utilisant le lemme d'interpolation 1.2.

b) *Propriétés simples de* $r(\Gamma,G,k)$. *Equivalence entre* (2.2) *et* (2.3).

Pour alléger les notations nous noterons simplement $r(\Gamma,G)$, ou même $r(\Gamma)$, au lieu de $r(\Gamma,G,k)$.

LEMME 2.4. Soient G un groupe algébrique commutatif défini sur k, et Γ un sous-groupe de type fini de $G(k)$ de rang $\ell \geqslant 1$ sur $\mathbb{Z}$.

1. Si Γ_1 et Γ_2 sont deux sous-groupes de Γ tels que $\Gamma_1+\Gamma_2$ soit d'indice fini dans Γ, alors

$$r(\Gamma) \leqslant r(\Gamma_1) + r(\Gamma_2) .$$

2. Si H est un sous-groupe algébrique de G défini sur k, de dimension δ, et si $\lambda = \operatorname{rang}_{\mathbb{Z}} \Gamma \cap H$, alors

$$r(\Gamma) \leqslant \ell-\lambda+\delta .$$

En particulier, si $r(\Gamma) = d$, alors $\mu(\Gamma,G) \geqslant 1$, et si $r(\Gamma) = \ell$, alors $\mu^*(\Gamma,G) \leqslant 1$.

3. Si H est un sous-groupe algébrique de G défini sur k, alors

$$r(\Gamma,G) \geqslant r(\Gamma \cap H,H) + r(\Gamma/\Gamma \cap H,G/H) .$$

Démonstration. La propriété 1 revient à dire que pour une matrice M de la forme (M_1,M_2), on a $\operatorname{rang} M \leqslant \operatorname{rang} M_1 + \operatorname{rang} M_2$, et la propriété 3 résulte du fait que pour une matrice M de la forme

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

on a $\operatorname{rang} M \geqslant \operatorname{rang} A + \operatorname{rang} C$.

Pour démontrer 2, on utilise 1 avec $\Gamma_1 = \Gamma \cap H$, et on choisit Γ_2 de rang $\ell-\lambda$ tel que $\Gamma_1+\Gamma_2$ soit d'indice fini dans Γ. Comme $\Gamma_1 \subset H$, on a $r(\Gamma_1) \leqslant \dim H = \delta$. D'autre part $r(\Gamma_2) \leqslant \operatorname{rang}_{\mathbb{Z}} \Gamma_2 = \ell-\lambda$.

Du lemme 2.4 on déduit par récurrence :

LEMME 2.5. Si H_i, $(0 \leqslant i \leqslant \nu+1)$ sont des sous-groupes algébriques de G, définis sur k, avec

$$G = H_0 \supset H_1 \supset \ldots \supset H_{\nu+1} = 0 ,$$

alors

$$r(\Gamma,G) \geqslant \sum_{i=0}^{\nu} r(\Gamma\cap H_i/\Gamma\cap H_{i+1}, H_i/H_{i+1}) \ .$$

Enfin le lemme suivant est évident.

LEMME 2.6. Il existe un sous-groupe $\widetilde{\Gamma}$ de Γ tel que

$$\operatorname{rang}_{\mathbb{Z}} \widetilde{\Gamma} = r(\widetilde{\Gamma},G) = r(\Gamma,G) \ .$$

Démonstration de (2.2) $\Longrightarrow$ (2.3). Avec les notations du lemme 1.4, l'inégalité (2.2) entraîne

$$r(\Gamma_i/\Gamma_{i+1}, H_i/H_{i+1}) \geqslant (\delta_i-\delta_{i+1})\mu_i/(\mu_i+\rho), \quad (0\leqslant i<\nu),$$

avec

$$\mu_i = \mu(\Gamma_i/\Gamma_{i+1}, H_i/H_{i+1}) \ .$$

Mais on a

$$\mu_i \geqslant \mu(\Gamma_i,H_i) = (\lambda_i-\lambda_{i+1})/(\delta_i-\delta_{i+1}), \qquad (0\leqslant i<\nu).$$

De plus, pour $0\leqslant i<\nu$,

$$\lambda_\nu/\delta_\nu \geqslant (\lambda_i-\lambda_{i+1})/(\delta_i-\delta_{i+1}) \ ,$$

donc

$$(\delta_i-\delta_{i+1})/(\lambda_i-\lambda_{i+1}+\rho\delta_i-\rho\delta_{i+1}) \geqslant \delta_\nu/(\lambda_\nu+\rho\delta_\nu) \ .$$

Le lemme 2.5 donne alors

$$\begin{aligned} r(\Gamma,G) &\geqslant \sum_{i=0}^{\nu} (\lambda_i-\lambda_{i+1})(\delta_i-\delta_{i+1})/(\lambda_i-\lambda_{i+1}+\rho\delta_i-\rho\delta_{i+1}) \\ &\geqslant \ell\delta_\nu/(\lambda_\nu+\rho\delta_\nu) \\ &\geqslant \ell/(\mu^*+\rho). \end{aligned}$$

Démonstration de (2.3) $\Longrightarrow$ (2.2). On utilise de même le lemme 1.6 ; grâce à (2.3), on a

$$r(\Gamma_{i+1}/\Gamma_i, H_{i+1}/H_i) \geqslant (\lambda_{i+1}-\lambda_i)/(\mu_i^*+\rho) \ ,$$

avec

$$\mu_i^* = \mu^*(\Gamma_{i+1}/\Gamma_i, H_{i+1}/H_i) \leqslant \mu^*(\Gamma/\Gamma_i, G/H_i) \ .$$

Mais

$$(\ell-\lambda_\nu)/(d-\delta_\nu) \leqslant (\ell-\lambda_i)/(d-\delta_i) \leqslant (\lambda_i-\lambda_{i-1})/(\delta_i-\delta_{i-1}) \ ,$$

donc

$$(\lambda_{i+1}-\lambda_i)/(\lambda_{i+1}-\lambda_i+\rho\delta_{i+1}-\rho\delta_i) \geqslant (\ell-\lambda_\nu)/(\ell-\lambda_\nu+\rho d-\rho\delta_\nu) \ ,$$

et du lemme 2.5 on conclut

$$\begin{aligned} r(\Gamma,G) &\geqslant \sum_{i=0}^{\nu} (\lambda_{i+1}-\lambda_i)(\delta_{i+1}-\delta_i)/(\lambda_{i+1}-\lambda_i+\rho\delta_{i+1}-\rho\delta_i) \\ &\geqslant d(\ell-\lambda_\nu)/(\ell-\lambda_\nu+\rho d-\rho\delta_\nu) \\ &\geqslant d\mu/(\mu+\rho) \ . \end{aligned}$$

c) La première fonction auxiliaire. Démonstration de (2.2).

En plus du lemme de zéros 1.1, l'outil essentiel dans la démonstration de (2.2) est le théorème 3.1.p de [6] dont voici un léger raffinement.

PROPOSITION 2.7. *Soient* L *et* n *deux entiers positifs,* Δ , U , R , r *des nombres réels positifs, et* $\varphi_1,\dots,\varphi_L$ *des fonctions analytiques dans le polydisque* $B(0,R^+)$ *de* k^n . *On suppose* $R > r$ *et*

$$(2.8) \qquad \partial(U+\log p)(U+\log \frac{R}{r})^n \leqslant L\Delta(\log \frac{R}{r})^n \ .$$

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

$$-e^{\Delta} \leqslant q_\lambda \leqslant e^{\Delta} \ ,$$

tels que la fonction

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

vérifie

$$|F|_r \leqslant e^{-U} \cdot \max_{1\leqslant\lambda\leqslant L} |\varphi_\lambda|_R \ .$$

Démonstration. Si les fonctions $\varphi_1,\dots,\varphi_L$ sont toutes nulles, le résultat est banal. Sinon, quitte à remplacer chaque φ_λ par $\frac{1}{c}\varphi_\lambda$ avec $c = \max_{1\leqslant\lambda\leqslant L} |\varphi_\lambda|_R$, on peut supposer $\max_{1\leqslant\lambda\leqslant L} |\varphi_\lambda|_R = 1$. On reprend alors la démonstration de [6] p. 122-123, avec

$$T_o = U(\log \tfrac{R}{r})^{-1} \quad , \quad T < T_o+1 \ ,$$

et B est le plus petit entier $\geqslant U/\log p$. On a alors, avec les notations de [6],

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

$$\partial B(\log p)T^n < L\Delta \ ,$$

et

$$|F|_R \leqslant 1 \ .$$

On en déduit facilement la proposition 2.7.

Nous considérons maintenant un groupe algébrique commutatif. Pour obtenir un énoncé raffiné, nous l'écrivons sous la forme $G = \mathbb{G}_a^{d_o} \times G_1 \times G_2$, 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 $d_o = d_1 = 0$, $G = G_2$. Le seul autre cas que nous utiliserons ici est $G = G_1$, mais le cas général nous sera utile ailleurs.

PROPOSITION 2.8. *Soient* d_o, d_1, d_2 *des entiers* $\geqslant 0$, *avec* $d = d_o + d_1 + d_2 \geqslant 1$, K *un corps de nombres contenu dans* k, G_1 *et* G_2 *deux groupes algébriques commutatifs définis sur* K *de dimension respective* d_1 *et* d_2, *et enfin* $G = \mathbb{G}_a^{d_o} \times G_1 \times G_2$. *On suppose que* G_1 *est linéaire. Soit* $\varphi : \mathbb{C}^n \longrightarrow G(k)$ *un homomorphisme analytique, avec* $0 < n < d$. *Soit* Y *un sous-groupe de type fini de* $p\mathbb{C}^n$ *tel que* $\varphi(Y)$ *soit contenu dans* $G(K)$. *Soit* $y_1,\dots,y_\ell$ *une base de* Y *sur* $\mathbb{Z}$; *pour* S *réel* $\geqslant 0$, *notons*

$$Y(S) = \{h_1y_1+\ldots+h_\ell y_\ell \ ; \ (h_1,\ldots,h_\ell) \in \mathbb{Z}^\ell \ , \ 0 \leqslant h_j < S\} \ .$$

Alors il existe un entier $N \geqslant 1$, un plongement quasi-projectif de G dans $\mathbb{A}_{d_o} \times \mathbb{A}_{d_1} \times \mathbb{P}_N$, une constante $C > 0$, et une suite $(P_S)_{S \geqslant S_o}$ de polynômes de

$$\mathbb{Z}[U_1,\ldots,U_{d_o},V_1,\ldots,V_{d_1},W_o,\ldots,W_N] \ ,$$

où P_S a un degré $\leqslant D_o$ par rapport à chaque variable $U_1,\ldots,U_{d_o}$, un degré $\leqslant D_1$ par rapport à chaque variable $V_1,\ldots,V_{d_1}$, et P_S est homogène de degré $\leqslant D_2$ en les variables $W_o,\ldots,W_N$, avec

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

où

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

tels que P_S s'annule sur $\varphi(Y(S))$, mais ne s'annule pas partout sur $G(K)$.

Quand G est linéaire, on peut choisir $d_o = d_2 = 0$, $d = d_1$, $G = G_1$, et on obtient un polynôme P_S de degré $\leqslant D_1$ avec

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

D'autre part, si G est quelconque et que l'on choisisse $d_o = d_1 = 0$, $d = d_2$, $G = G_2$, on obtient un polynôme homogène P_S, de degré $\leqslant D_2$, avec

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

Démonstration de la proposition 2.8. Il est utile d'effectuer quelques réductions préliminaires. D'abord on peut supposer que le seul sous-groupe algébrique de G défini sur K et contenant $\varphi(\mathbb{G}^n)$ est G lui-même. En effet, si ce n'était pas le cas, il existerait un polynôme à coefficients dans K, nul sur $\varphi(Y)$ mais pas sur $G(K)$. En prenant la norme sur $\mathbb{Q}$ et en multipliant par un entier positif on

obtient un polynôme à coefficients dans $\mathbb{Z}$.

En particulier on supposera que G est connexe, et que $d_o < n$. On remarque alors que D_1 tend vers l'infini avec S :

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

Nous supposerons aussi que l'on a ou bien $d_2 = 0$, ou bien

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

Cela n'est pas restrictif : en effet, si D_2 ne vérifiait pas cette minoration, alors on aurait $2d_o+d_1 \geqslant 2n$, et $d_o+d_1 > n$, donc

$$(2d_2+d_1)/(d_o+d_1+d_2-n) \geqslant d_1/(d_o+d_1-n) ;$$

on construit dans ce cas un polynôme P_S indépendant des variables $W_o,\ldots,W_N$.

D'autre part dans l'énoncé de la proposition 2.8 on peut remplacer K et k par des extensions finies sans perte de généralité. On peut alors choisir un plongement de G_2 dans un espace projectif $\mathbb{P}_N$, défini sur K , ayant les propriétés requises au §4.1 de [1]. L'existence d'un tel plongement a été démontrée par Serre [4]. L'homomorphisme analytique $\varphi : \mathbb{C}^n \longrightarrow G(k)$ est alors représenté par des coordonnées

$$(\lambda_1,\ldots,\lambda_{d_o},\mu_1,\ldots,\mu_{d_1},\psi_o,\ldots,\psi_N)$$

où les λ_i sont des formes linéaires en $z = (z_1,\ldots,z_n)$, les μ_i et ψ_j sont des fonctions strictement analytiques sur $\mathbb{C}^n$, et $\{\mu_1,\ldots,\mu_{d_1}\}$ (resp. $\{\frac{\psi_1}{\psi_o},\ldots,\frac{\psi_N}{\psi_o}\}$) est un système d'ordre arithmétique fonctionnel fini avec $\rho = 1$ (resp. $\rho = 2$) pour lequel tout point de $\mathbb{C}^n$ est régulier (cf. [1]). Enfin, grâce à la première réduction ci-dessus, on peut supposer que les fonctions

$$\lambda_1,\ldots,\lambda_{d_o},\mu_1,\ldots,\mu_{d_1},\psi_1/\psi_o,\ldots,\psi_{d_2}/\psi_o$$

sont algébriquement indépendantes sur K .

On choisit d'abord un entier ν suffisamment grand, puis un entier S_o suffisamment grand (dépendant de ν) ; enfin soit S un réel $\geqslant S_o$. On définit un réel $\Delta > 0$ par

$$\Delta^{d-n} = \nu^{n+2} S^{2d_2+d_1} (\log S)^{d_o} ,$$

et on définit des réels D_o , D_1 , D_2 par

$$D_o \log S = D_1 S = D_2 S^2 = \Delta .$$

Premier pas. Il existe un polynôme non nul P_S dans l'anneau

$$\mathbb{Z}[U_1,\dots,U_{d_o},V_1,\dots,V_{d_1},W_o,\dots,W_{d_2}] ,$$

de degré $\leqslant D_o$ en $U_1,\dots,U_{d_o}$, de degré $\leqslant D_1$ en $V_1,\dots,V_{d_1}$, et homogène de degré $D_2^o \leqslant D_2$ en $W_o,\dots,W_{d_2}$, dont les coefficients sont des entiers rationnels dont la valeur absolue (ordinaire) est majorée par e^{Δ} , tel que la fonction

$$F_S = P_S(\lambda_1,\dots,\lambda_{d_o},\mu_1,\dots,\mu_{d_1},\psi_o,\dots,\psi_{d_2})$$

vérifie

$$|F_S|_{1/p} \leqslant e^{-\nu\Delta} .$$

Ce premier pas est purement analytique et ne fait pas intervenir le corps de nombres K . On utilise la proposition 2.7 avec

$$U = \nu\Delta \ , \ R = 1 \ , \ r = 1/p \ , \ L \geqslant D_o^{d_o} D_1^{d_1} D_2^{d_2} (d_2+1)^{-d_2} ,$$

et les φ_j sont des monômes en $\lambda_1,\dots,\lambda_{d_o},\mu_1,\dots,\mu_{d_1}$, $\psi_o,\dots,\psi_{d_2}$, de degrés respectifs $\leqslant D_o, D_1, D_2$; ainsi

$$|\varphi_j|_1 \leqslant p^{\Delta} .$$

Deuxième pas. Pour tout $y \in Y(S)$, on a $F_S(y) = 0$.

Comme la fonction ψ_o n'a pas de zéros dans $\mathfrak{O}$, le nombre

$$\alpha = \psi_o(y)^{-D_2^o} F_S(y)$$

est bien défini, et appartient à K. Grâce à la construction de F_S on a

$$|\alpha| \leqslant e^{-\frac{1}{2}\nu\Delta} .$$

D'autre part, d'après [1], α a une hauteur majorée par $\exp(\nu\Delta/3)$. La formule du produit implique alors $\alpha = 0$.

La proposition 2.8 est ainsi démontrée. Nous déduisons alors de 1.1 le corollaire suivant, qui est clairement équivalent à l'inégalité (2.2).

COROLLAIRE 2.9. Soient K un corps de nombres contenu dans k, G un groupe algébrique commutatif défini sur K de dimension $d \geqslant 1$, $\varphi : \mathfrak{O}^n \longrightarrow G(k)$ un homomorphisme analytique avec $n < d$, et Γ un sous-groupe de type fini de $\varphi(\mathfrak{O}^n) \cap G(K)$. Alors

$$\mu(\Gamma, G) \leqslant \rho n/(d-n) .$$

Par exemple si G est une variété abélienne simple, alors $\varphi(\mathfrak{O}^n) \cap G(K)$ a un rang sur $\mathbb{Z}$ fini $\leqslant 2nd/(d-n)$.

d) La deuxième fonction auxiliaire. Démonstration de (2.3).

Nous avons déjà démontré (2.3), puisque nous l'avons déduit de (2.2), et que nous avons établi (2.2) grâce à la première fonction auxiliaire. Néanmoins il est intéressant de donner une deuxième démonstration de (2.3), en utilisant le lemme d'interpolation 1.2 et la nouvelle fonction auxiliaire suivante.

PROPOSITION 2.10. Soient N et n deux entiers positifs, Δ, U, R, r des nombres réels positifs, et $\zeta_1, \ldots, \zeta_N$

des éléments de k^n . On suppose

$$R > r\ ,\quad \max_{1\leqslant\nu\leqslant N} |\zeta_\nu| \leqslant r\ ,$$

et

$$\partial(U+\log p)(U+\log \tfrac{R}{r})^n < N\Delta(\log \tfrac{R}{r})^n\ .$$

Alors il existe des entiers positifs $q_1,\dots,q_N$, non tous nuls, avec

$$-e^{\Delta} < q_\nu < e^{\Delta}\ ,$$

tels que pour toute fonction φ analytique dans le polydisque $B(0,R^+)$ de k^n , on ait

$$|\sum_{\nu=1}^{N} q_\nu \varphi(\zeta_\nu)| < e^{-U}|\varphi|_R\ .$$

Démonstration. On définit $T_o = U(\log R/r)^{-1}$. Soit T la partie entière de T_o+1 . On note, pour $z = (z_1,\dots,z_n) \in k^n$, et $t = (t_1,\dots,t_n) \in \mathbb{N}^n$,

$$z^t = z_1^{t_1}\dots z_n^{t_n} \quad \text{et} \quad \|t\| = t_1+\dots+t_n\ .$$

On considère le système de

$$\binom{T+n-1}{n} \leqslant (T_o+1)^n$$

inéquations à N inconnues $q_1,\dots,q_N$:

$$|c_t \sum_{\nu=1}^{N} q_\nu \zeta_\nu^t| < e^{-U}\ ,\qquad (t\in\mathbb{N}^n\ ,\ \|t\| < T)\ ,$$

où les $c_t \in k$ sont choisis de telle sorte que

$$|c_t\zeta_\nu^t| \leqslant 1 \quad \text{et} \quad |c_t| > r^{-\|t\|}\ ,\quad (1\leqslant\nu\leqslant N\ ,\ \|t\| < T)\ .$$

On utilise le lemme 3.3.p de [6] avec

$$e^{\Delta}-1 \leqslant A < e^{\Delta}\ ,\quad \frac{U}{\log p} < B \leqslant \frac{U}{\log p}+1\ ,\quad \mu \leqslant (T_o+1)^n\ .$$

Ainsi

$$p^{\partial B\mu} \leqslant \exp\{\partial(U+\log p)(1+\frac{U}{\log R/r})^n\} < e^{N\Delta} \leqslant (A+1)^N\ .$$

On trouve ainsi $q_1,\dots,q_N$, non tous nuls, entre $-e^{\Delta}$ et e^{Δ} .

Soit maintenant φ une fonction analytique dans $B(0,R^+)$, avec $|\varphi|_R \leqslant 1$. On tronque le développement de Taylor de φ à l'origine sous la forme

$$\varphi = P+G ,$$

où P est un polynôme de degré $< T$, et G a un zéro à l'origine d'ordre $\geqslant T$. On a

$$|\sum_{\nu=1}^{N} q_\nu G(\zeta_\nu)| \leqslant \max_{1\leqslant\nu\leqslant N} |G(\zeta_\nu)| \leqslant |G|_r \leqslant (r/R)^T |\varphi|_R < e^{-U} ,$$

et

$$|\sum_{\nu=1}^{N} q_\nu P(\zeta_\nu)| \leqslant \max_{|t|<T} |\frac{1}{t!} D^t\varphi(0) \sum_{\nu=1}^{N} q_\nu \zeta_\nu^t| \leqslant |\varphi|_r e^{-U} \leqslant e^{-U}.$$

D'où

$$|\sum_{\nu=1}^{N} q_\nu \varphi(\zeta_\nu)| < e^{-U} .$$

Par homogénéité, on en déduit la proposition 2.10 pour toute fonction φ analytique dans $B(0,R^+)$.

De la même manière que nous avons déduit 2.8 de 2.7, on obtient comme conséquence de 2.10 la proposition suivante.

PROPOSITION 2.11. Sous les hypothèses de la proposition 2.8, il existe un plongement de G dans $\mathbb{A}_{d_0} \times \mathbb{A}_{d_1} \times \mathbb{P}_N$, une constante $C > 0$, et, pour chaque réel S suffisamment grand, des entiers rationnels q_γ , indexés par γ dans $\Gamma(S) = \varphi(Y(S))$, non tous nuls, avec la propriété suivante. Pour tout polynôme P de l'anneau

$$\mathbb{Z}[U_1,\dots,U_{d_0},V_1,\dots,V_{d_1},W_0,\dots,W_N] ,$$

de degré $\leqslant D_0$ en $U_1,\dots,U_{d_0}$, de degré $\leqslant D_1$ en $V_1,\dots,V_{d_1}$, et homogène de degré $\leqslant D_2$ en $W_0,\dots,W_N$, avec

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

où

$$\Delta^n = CS^{\ell} ,$$

on a

$$\sum_{\gamma \in \Gamma(S)} q_\gamma P(\gamma) = 0 .$$

Le lemme d'interpolation 1.2 donne alors l'énoncé suivant équivalent à (2.3) :

COROLLAIRE 2.12. Sous les hypothèses du corollaire 2.9, on a

$$\mu^*(\Gamma,G) \geqslant \frac{\ell}{n} - \rho .$$

Bien entendu, l'étude faite au §2 b ci-dessus montre que les corollaires 2.9 et 2.12 peuvent être déduits l'un de l'autre.

e) Compléments.

Comme on a toujours $\mu(\Gamma,G) \leqslant \ell/d$ (resp. $\mu^*(\Gamma,G) \geqslant \ell/d$), le corollaire 2.9 (resp. 2.12) n'est intéressant que si

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

Supposons $\mu(\Gamma,G) = \ell/d$, ce qui équivaut à $\mu^*(\Gamma,G) = \ell/d$. Alors les inégalités (2.2) et (2.3) s'écrivent sous la même forme :

$$r(\Gamma,G) \geqslant \ell d/(\ell + d\rho) .$$

Il serait intéressant de décrire plus complètement la situation, au moins d'un point de vue conjectural. Dans [7] §3 est décrit un exemple, dû à M. Langevin, dans lequel

$$G = \mathfrak{G}_m^d , \quad \rho = 1 , \quad \ell = d , \quad \mu(\Gamma,G) = 1 ,$$

et

$$r(\Gamma,G) = \frac{2}{3} d ,$$

ceci pour chaque entier d positif divisible par 3 . La même construction donne, quand d est un entier positif divisible par 3 et E une courbe elliptique (définie sur

un corps de nombres K contenu dans k) ayant des endomorphismes non triviaux, un exemple avec

$$G = E^d \ , \ \rho = 2 \ , \ \ell = 2d \ , \ \mu(\Gamma, G) = 2 \ ,$$

et

$$r(\Gamma, G) = \frac{2}{3} \, d \ .$$

§3. LE CAS COMPLEXE.

On désigne par G un groupe algébrique commutatif défini sur $\mathbb{C}$ de dimension $d \geqslant 1$, et par Γ un sous-groupe de type fini de $G(\mathbb{C})$ de rang ℓ sur $\mathbb{Z}$.

a) Définition de $r(\Gamma,G,\mathbb{C})$ et énoncé des résultats.

Notons $T_G(\mathbb{C})$ l'espace tangent à l'origine de $G(\mathbb{C})$, et $\exp_G : T_G(\mathbb{C}) \longrightarrow G(\mathbb{C})$ l'application exponentielle de $G(\mathbb{C})$. Il existe des éléments $t_1,\ldots,t_\ell$ de $T_G(\mathbb{C})$ dont les images par $\exp_G$ engendrent un sous-groupe d'indice fini de Γ. On définit alors $r(\Gamma,G,\mathbb{C})$ comme le minimum des nombres $\dim_{\mathbb{C}}(\mathbb{C}t_1+\ldots+\mathbb{C}t_\ell)$, quand $(t_1,\ldots,t_\ell)$ décrit les éléments de $(T_G(\mathbb{C}))^\ell$ vérifiant cette propriété.

Si G° désigne la composante connexe de l'élément neutre dans G, on a

$$r(\Gamma,G,\mathbb{C}) = r(\Gamma\cap G^\circ,G^\circ,\mathbb{C}) .$$

Si $\ell = 0$, c'est-à-dire si Γ est un sous-groupe fini de $G(\mathbb{C})$, alors $r(\Gamma,G,\mathbb{C}) = 0$.

Si $\ell \geqslant 1$, $r(\Gamma,G,\mathbb{C})$ est le plus petit des entiers $n \geqslant 1$ tels qu'il existe un homomorphisme analytique $\varphi : \mathbb{C}^n \longrightarrow G(\mathbb{C})$ pour lequel $\varphi(\mathbb{C}^n)\cap\Gamma$ soit un sous-groupe d'indice fini de Γ.

Ainsi dans tous les cas

$$r(\Gamma,G,\mathbb{C}) \leqslant \min(\ell,d) .$$

D'autre part $r(\Gamma,G,\mathbb{C})$ est majoré par la dimension du $\mathbb{C}$-espace vectoriel engendré dans $T_G(\mathbb{C})$ par $\exp_G^{-1}(\Gamma)$. Cette majoration peut être stricte : par exemple, si G est une variété abélienne, $\exp_G^{-1}(0)$ contient une base de $T_G(\mathbb{C})$.

Le résultat principal de ce §3 est le suivant. On désigne par $\bar{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$.

THÉORÈME 3.1. On suppose que G est défini sur $\bar{\mathbb{Q}}$, et que Γ est contenu dans $G(\bar{\mathbb{Q}})$. On note

$$r = r(\Gamma,G,\mathbb{C}) \ , \ \mu = \mu(\Gamma,G) \ , \ \mu^* = \mu^*(\Gamma,G) \ .$$

Alors on a

$$r \geqslant d\mu/(\mu+\rho) \tag{3.2}$$

et

$$r \geqslant \ell/(\mu^*+\rho) \ . \tag{3.3}$$

Le plan de ce §3 est le suivant. Nous reprenons d'abord rapidement la méthode du §2 c pour démontrer (3.2), puis celle du §2 d pour (3.3). Nous verrons ensuite pourquoi les résultats du §2 b ne s'étendent pas au cas complexe. Pour y remédier, nous montrerons comment il convient de choisir les logarithmes.

b) Démonstration de (3.2).

On utilise le théorème 3.1 de [6] et le lemme de zéros 1.1 pour démontrer la proposition suivante, analogue complexe de 2.8.

PROPOSITION 3.4. On écrit G sous la forme $G = \mathbb{G}_a^{d_o} \times G_1 \times G_2$, où G_1 est linéaire de dimension d_1 et G_2 est de dimension d_2, tous deux définis sur $\bar{\mathbb{Q}}$. Soit $\varphi : \mathbb{C}^n \longrightarrow G(\mathbb{C})$ un homomorphisme analytique, avec $n < d$. Soient $y_1,\dots,y_\ell$ des éléments $\mathbb{Q}$-linéairement indépendants de $\mathbb{C}^n$ dont les images par φ sont dans $G(\bar{\mathbb{Q}})$. On note $Y = \mathbb{Z}y_1+\dots+\mathbb{Z}y_\ell$, et on définit $Y(S)$, pour S réel $\geqslant 0$, comme d'habitude.

Alors il existe un plongement de $G(\mathbb{C})$ dans $\mathbb{C}^{d_o} \times \mathbb{C}^{d_1} \times \mathbb{P}_N(\mathbb{C})$, une constante $C > 0$, et une suite $(P_S)_{S \geqslant S_o}$ de polynômes de l'anneau

$$\mathbb{Z}[U_1,\dots,U_{d_o},V_1,\dots,V_{d_1},W_o,\dots,W_N] \ ,$$

P_S étant de degré $\leqslant D_o$ en les U_i , $\leqslant D_1$ en les V_i , et homogène de degré $\leqslant D_2$ en les W_i , avec

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

où

$$\Delta^{d-n} = CS^{2d_2+d_1}(\log S)^{d_o} ,$$

tels que P_S s'annule sur $\varphi(Y(S))$ mais pas sur tout $G(\bar{\mathbb{Q}})$.

La démonstration de la proposition 3.4 est analogue à celle de la proposition 2.8 ; essentiellement on remplace les arguments tirés de [1] par ceux utilisés dans [5] , notamment au §4.3. Ainsi on choisit $\psi_o = \theta \circ p$, où θ est une fonction thêta relative à un réseau d'un espace $\mathbb{C}^g$, et $p : \mathbb{C}^n \longrightarrow \mathbb{C}^g$ est une application linéaire. De plus on demande aux fonctions $\psi_o, \ldots, \psi_N$ d'être entières dans $\mathbb{C}^n$, d'ordre $\leqslant 2$. Tout cela est possible grâce à [4].

En combinant le théorème 1.1 et la proposition 3.4, on obtient l'énoncé suivant, équivalent à 3.2.

COROLLAIRE 3.5. Soit $\varphi : \mathbb{C}^n \longrightarrow G(\mathbb{C})$ un homomorphisme analytique. On suppose G défini sur $\bar{\mathbb{Q}}$ et Γ contenu dans $\varphi(\mathbb{C}^n) \cap G(\bar{\mathbb{Q}})$. Alors

$$\mu(\Gamma, G) \leqslant \rho n/(d-n) .$$

Remarque. On peut raffiner la proposition 3.4 en remplaçant la définition de Δ par

$$\Delta^{d-n} = CS^{2d_2+d_1-\varkappa}(\log S)^{d_o} ,$$

où $\varkappa$ est la dimension du $\mathbb{C}$-espace vectoriel engendré par le noyau de φ . On en déduit un raffinement correspondant de 3.5 :

$$\mu(\Gamma, G) \leqslant (\rho n - \varkappa)/(d-n) .$$

Pour cela, on modifie la construction de la fonction auxiliaire (théorème 3.1 de [6]) en tenant compte des périodes.

Comme la démonstration est plus compliquée, nous ne la donnons pas ici, et nous n'utiliserons pas ce raffinement.

c) La deuxième fonction auxiliaire. Démonstration de (3.3).

Voici l'analogue complexe de la proposition 2.10.

PROPOSITION 3.6. Soient N et n deux entiers positifs, Δ , U , R , r des nombres réels positifs, et $\zeta_1,\ldots,\zeta_N$ des points de $\mathbb{C}^n$. On suppose

$$U \geqslant 3 \ , \ U \geqslant \Delta \ , \ R/r > e \ , \ e^U \geqslant NR/r \ , \ \max_{1\leqslant\nu\leqslant N} |\zeta_\nu| < r \ ,$$

et

$$(8U)^{n+1} \leqslant N\Delta(\operatorname{Log}\frac{R}{r})^n \ .$$

Alors il existe des entiers rationnels $q_1,\ldots,q_N$, avec

$$0 < \max_{1\leqslant\nu\leqslant N} |q_\nu| \leqslant e^\Delta \ ,$$

tels que pour toute fonction φ analytique dans $B(0,R)$ on ait

$$\Big|\sum_{\nu=1}^{N} q_\nu \varphi(\zeta_\nu)\Big| \leqslant e^{-2U}|\varphi|_R \ .$$

Démonstration. On définit un nombre réel $T_o \geqslant 0$ par la condition $(R/r)^{T_o} = Ne^{4U}$. On a ainsi $4 \leqslant T_o \leqslant 5U-1$. Soit T le plus petit entier $\geqslant T_o$. On résout le système d'inéquations

$$\Big|\sum_{\nu=1}^{N} q_\nu \zeta_\nu^t\Big| \leqslant \tfrac{1}{2}(1+T_o)^{-n} R^{\|t\|} e^{-2U} \ , \quad (t \in \mathbb{N}^n \ , \ \|t\| < T).$$

On utilise pour cela le lemme 3.3 de [6] et les inégalités

$$\sum_{\nu=1}^{N} |\zeta_\nu^t| \leqslant N R^{\|t\|} \ ,$$

$$2\sqrt{2}(1+T_o)^n N e^{\Delta+3U} + 1 \leqslant e^{(n+5)U} \ ,$$

et

$$2(n+5)U(1+T_o)^n \leqslant N\Delta \ .$$

Alors on peut trouver $(q_1,\dots,q_N) \in \mathbb{Z}^N$, $\neq (0,\dots,0)$, et $|q_\nu| \leqslant e^{\Delta}$.

Soit maintenant φ analytique dans $B(0,R)$, et vérifiant $|\varphi|_R \leqslant e^U$. On écrit $\varphi = P+G$, où P est un polynôme de degré $< T$, et G a un zéro à l'origine d'ordre $\geqslant T$. On a (cf. [6] démonstration du lemme 3.4) :

$$|G|_R \leqslant (1+T^{\frac{1}{2}})|\varphi|_R ,$$

$$|G(\zeta_\nu)| \leqslant (r/R)^T (1+T^{\frac{1}{2}})|\varphi|_R ,$$

et, comme $2(1+T^{\frac{1}{2}}) \leqslant e^U$,

$$|\sum_{\nu=1}^{N} q_\nu G(\zeta_\nu)| \leqslant N\, e^{\Delta+U}(1+T^{\frac{1}{2}})(r/R)^T \leqslant \tfrac{1}{2}e^{-U} .$$

D'autre part si on écrit

$$P(z) = \sum_{\|t\|<T} c_t z^t ,$$

on a

$$\sum_{\nu=1}^{N} q_\nu P(\zeta_\nu) = \sum_{\|t\|<T} c_t \sum_{\nu=1}^{N} q_\nu \zeta_\nu^t ,$$

donc

$$|\sum_{\nu=1}^{N} q_\nu P(\zeta_\nu)| \leqslant (T_o+1)^n \Big(\max_{\|t\|<T} |c_t| R^{\|t\|}\Big).\tfrac{1}{2}(1+T_o)^{-n} e^{-2U}$$
$$\leqslant \tfrac{1}{2}e^{-U} ,$$

grâce aux inégalités de Cauchy. La proposition 3.6 est ainsi démontrée sous l'hypothèse $|\varphi|_R = e^U$, et le cas général s'en déduit par homogénéité.

On en déduit le résultat suivant : dans l'énoncé de la proposition 2.11, on peut remplacer : "Sous les hypothèses de la proposition 2.8" par : "Sous les hypothèses de la proposition 3.4", à condition d'ajouter la condition :

$$Y \cap \ker \varphi = (0) .$$

Cette condition supplémentaire est évidemment nécessaire : elle permet d'indexer les q_γ par γ dans $\Gamma(S) = \varphi(Y(S))$.

On obtient alors (3.3) sous la forme équivalente suivante :

COROLLAIRE 3.7. Sous les hypothèses du corollaire 3.5, on a

$$\mu^*(\Gamma,G) \geqslant \frac{\ell}{n}-\rho \ .$$

Remarque. Ici aussi on peut tenir compte des périodes de φ, en raffinant la proposition 3.6. Alors, si $\varkappa$ est la dimension du $\mathbb{C}$-espace vectoriel engendré par le noyau de φ, on peut préciser 3.7 :

$$\mu^*(\Gamma,G) \geqslant \frac{\ell+\varkappa}{n}-\rho \ ,$$

et, dans l'analogue complexe de 2.11, on peut remplacer la définition de Δ par

$$\Delta^n = CS^{\ell+\varkappa} \ .$$

d) Un problème dû aux périodes.

La partie 3 du lemme 2.4 ne s'étend pas au cas complexe. Voici un exemple dans lequel Γ est contenu dans un sous-groupe algébrique H de G, et

$$r(\Gamma,G,\mathbb{C}) < r(\Gamma,H,\mathbb{C}) \ .$$

On choisit $H = \mathbb{G}_a^2$, et G est une extension d'une courbe elliptique E par $\mathbb{G}_a^2$ (cf. [4] §3.3 p. 199). On écrit les éléments de l'espace tangent $T_G(\mathbb{C})$ sous la forme (z,z',u), avec $(z,z') \in T_H(\mathbb{C}) \cong \mathbb{C}^2$ et $u \in T_E(\mathbb{C}) \cong \mathbb{C}$. Soit (ω_1,ω_2) un couple fondamental de périodes de $\exp_E$ dans $T_E(\mathbb{C})$, et soit $\tau = \omega_2/\omega_1$. On choisit pour G l'extension pour laquelle

$$\exp(z+\eta_i,z'+\eta_i,u+\omega_i) = \exp(z,z',u) \ , \quad (i=1,2),$$

avec

$$\eta_i = 2\zeta(\omega_i/2) \ , \ (i=1,2) \ , \ \eta_2-\tau\eta_1 = 2i\pi/\omega_1 \ ;$$

(cf. [4] p. 199). On choisit $\Gamma = \mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2 \subset G(\mathbb{C})$, avec

$$\gamma_1 = \exp_G(\eta_1, \eta_2/\tau, \omega_1) \ , \ \gamma_2 = \exp_G(\tau\eta_1, \eta_2, \omega_2) \ .$$

Comme la matrice

$$\begin{pmatrix} \eta_1 & \tau\eta_1 \\ \eta_2/\tau & \eta_2 \\ \omega_1 & \omega_2 \end{pmatrix}$$

a pour rang 1 , on a $r(\Gamma, G, \mathbb{C}) = 1$. Mais $\Gamma \subset H$, car

$$\gamma_1 = \exp_G(0, \tfrac{1}{\tau}\eta_2 - \eta_1, 0) \ , \ \gamma_2 = \exp_G(\tau\eta_1 - \eta_2, 0, 0) \ ,$$

et comme la matrice

$$\begin{pmatrix} 0 & \frac{1}{\tau}\eta_2 - \eta_1 \\ \tau\eta_1 - \eta_2 & 0 \end{pmatrix}$$

a pour rang 2 , et que $\exp_H$ n'a pas de périodes, on a $r(\Gamma, H, \mathbb{C}) = 2$.

Remarque. Dans le cas général $\Gamma \subset H \subset G$, on peut montrer :

$$\tfrac{1}{2} r(\Gamma, H) \leqslant r(\Gamma, G) \leqslant r(\Gamma, H) \ .$$

e) Sur le choix des logarithmes.

Au §4, nous aurons besoin des résultats du §2 b , notamment du lemme 2.6. Pour remplacer ces résultats dans le cas complexe, il faudra choisir convenablement les logarithmes. Commençons par exposer la situation dans le cas particulier $G = \mathbb{G}_m^d$. Ainsi Γ est un sous-groupe de type fini de $\mathbb{C}^{xd}$, de rang ℓ . Le problème consiste à trouver des nombres complexes z_{ij} , $(1 \leqslant i \leqslant d \ , \ 1 \leqslant j \leqslant \ell)$, avec les propriétés suivantes : si on note $\gamma_{ij} = \exp(z_{ij})$, et $\gamma_j = (\gamma_{1j}, \ldots, \gamma_{dj}) \in \mathbb{C}^{xd}$, $(1 \leqslant j \leqslant \ell)$, alors

1) le sous-groupe de $\mathbb{C}^{xd}$ engendré par $\gamma_1, \ldots, \gamma_\ell$ est un sous-groupe d'indice fini de Γ ;

2) si $p_1, \ldots, p_d, q_1, \ldots, q_\ell$ sont des entiers rationnels tels

que

$$\prod_{i=1}^{d}\prod_{j=1}^{\ell}\gamma_{ij}^{p_iq_j} = 1 ,$$

alors

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell} p_iq_jz_{ij} = 0 .$$

Rappelons la solution donnée dans [7]. On choisit des éléments $\gamma_1^\circ,\dots,\gamma_\ell^\circ$ dans Γ, $\mathbb{Q}$-linéairement indépendants, on écrit $\gamma_j^\circ = (\gamma_{ij}^\circ)_{1\leqslant i\leqslant d}$, et on considère le sous-groupe de $\mathbb{C}^\times$ engendré par les ℓd nombres γ_{ij}°. Soit a l'ordre du sous-groupe de torsion. Les ℓd nombres $(\gamma_{ij}^\circ)^a$ engendrent un sous-groupe libre de $\mathbb{C}^\times$. On choisit une base (δ_s), et on écrit les $\gamma_{ij} = (\gamma_{ij}^\circ)^a$ dans cette base :

$$\gamma_{ij} = \prod_s \delta_s^{a_{ijs}} , \quad (1\leqslant i\leqslant d , \ 1\leqslant j\leqslant \ell) .$$

On choisit des nombres complexes z_s tels que $\exp(z_s) = \delta_s$, et on définit

$$z_{ij} = \sum_s a_{ijs}z_s , \ (1\leqslant i\leqslant d , \ 1\leqslant j\leqslant \ell) .$$

Alors $\exp(z_{ij}) = \gamma_{ij}$, et la condition

$$\prod_{i=1}^{d}\prod_{j=1}^{\ell}\prod_s \delta_s^{a_{ijs}p_iq_j} = 1$$

implique, puisque les δ_s sont multiplicativement indépendants,

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell} a_{ijs}p_iq_j = 0$$

pour tout s, donc

$$\sum_{i=1}^{d}\sum_{j=1}^{\ell} p_iq_jz_{ij} = 0 .$$

Nous allons modifier cet argument pour l'étendre au cas d'un groupe algébrique commutatif quelconque. Essentiellement, au lieu de considérer le sous-groupe de $\mathbb{C}^\times$ engendré par les ℓd nombres γ_{ij}°, on va considérer le sous-groupe de $\mathbb{C}^{\times\ell d}$ engendré par le point $(\gamma_{ij}^\circ)_{1\leqslant i\leqslant d,1\leqslant j\leqslant \ell}$.

LEMME 3.8. On suppose $\ell \geqslant 1$. Il existe $t_1,\dots,t_\ell$ dans $T_G(\mathbb{C})$ tels que les points $\gamma_j = \exp_G t_j$, $(1 \leqslant j \leqslant \ell)$ de $G(\mathbb{C})$ engendrent un sous-groupe d'indice fini de Γ , et tels que pour tout sous-groupe algébrique H de G et tout $t \in \mathbb{Z}t_1+\dots+\mathbb{Z}t_\ell$, la condition $\exp_G t \in H$ implique $t \in T_H$.

La conclusion entraîne, et, si H est connexe, équivaut à :

$$(\mathbb{Z}t_1+\dots+\mathbb{Z}t_\ell) \cap (T_H+\ker \exp_G) \subset T_H \ .$$

D'autre part le sous-groupe Γ' de Γ engendré par $\gamma_1,\dots,\gamma_\ell$ possède alors la propriété que pour tout sous-groupe algébrique H de G , $\Gamma'/\Gamma' \cap H$ est sans torsion.

Démonstration du lemme 3.8. Commençons par traiter le cas $\ell = 1$. On veut trouver $t \in T_G$ tel que $\gamma = \exp_G t$ soit un point de Γ , non de torsion, et tel que les conditions $\gamma \in H$ et $t \in T_H$ soient équivalentes pour chaque sous-groupe algébrique H de G . Pour cela on prend l'adhérence de Zariski Z de Γ dans G ; c'est un sous-groupe algébrique de G , et on note H_o la composante connexe de Z contenant l'élément neutre. Alors $\Gamma \cap H_o$ est un sous-groupe d'indice fini de Γ . On choisit $\gamma \in \Gamma \cap H_o$, non de torsion, puis on choisit un élément t dans

$$\exp_{H_o}^{-1}\gamma = \exp_G^{-1}\gamma \cap T_{H_o} \ .$$

Alors

$$\gamma \in H \Longrightarrow H_o \subset H \Longrightarrow T_{H_o} \subset T_H \Longrightarrow t \in T_H \ .$$

Pour ℓ quelconque, on considère ℓ éléments $\gamma_1^o,\dots,\gamma_\ell^o$ de Γ linéairement indépendants sur $\mathbb{Z}$. Dans G^ℓ , on considère l'adhérence de Zariski Z de $\mathbb{Z}\gamma^o$, où $\gamma^o = (\gamma_1^o,\dots,\gamma_\ell^o)$, on note H_o la composante connexe de l'élément neutre de Z , et dans son espace tangent T_{H_o} on choisit un élément t dont l'image γ par $\exp_{G^\ell}$ est un élément du sous-groupe engendré par γ^o , et n'est pas de torsion (c'est possible puisque γ^o lui-même n'est pas de

torsion dans G). En identifiant T_{G^ℓ} et T_G^ℓ, on écrit $t = (t_1,\dots,t_\ell)$, avec $t_j \in T_G$. Montrons que ces éléments $t_1,\dots,t_\ell$ vérifient les propriétés annoncées.

Il est clair que les $\gamma_j = \exp_G t_j$ engendrent un sous-groupe d'indice fini de Γ. Maintenant si $(h_1,\dots,h_\ell) \in \mathbb{Z}^\ell$ et $H \subset G$ sont tels que

$$\gamma_1^{h_1}\dots\gamma_\ell^{h_\ell} \in H ,$$

alors le sous-groupe algébrique

$$\widetilde{H} = \{(g_1,\dots,g_\ell) \in G^\ell \ , \ g_1^{h_1}\dots g_\ell^{h_\ell} \in H\}$$

de G^ℓ contient γ, donc $t \in T_{\widetilde{H}}$, c'est-à-dire $h_1t_1+\dots+h_\ell t_\ell \in T_H$.

Ceci termine la démonstration du lemme 3.8.

Voici, avec ce choix des logarithmes, l'analogue complexe de la deuxième partie du lemme 2.4.

LEMME 3.9. *Soient H un sous-groupe algébrique connexe de G, de dimension δ, et $t_1,\dots,t_\ell$ des éléments de $T_G(\mathbb{C})$, dont les images par $\exp_G$ appartiennent à Γ, et tels que*

$$(\mathbb{Z}t_1+\dots+\mathbb{Z}t_\ell) \cap (T_H+\ker \exp_G) \subset T_H .$$

Notons λ le rang de $\Gamma \cap H$ sur $\mathbb{Z}$. Alors

$$\dim_{\mathbb{C}}(\mathbb{C}t_1+\dots+\mathbb{C}t_\ell) \leqslant \ell-\lambda+\delta .$$

Démonstration. Notons Γ' le sous-groupe de Γ engendré par les ℓ points $\gamma_j = \exp_G t_j$, $(1 \leqslant j \leqslant \ell)$, avec $\ell' = \operatorname{rang}_{\mathbb{Z}}\Gamma'$, et $\lambda' = \operatorname{rang}_{\mathbb{Z}}\Gamma' \cap H$. On considère des entiers rationnels a_{sj}, $(1 \leqslant s \leqslant \ell' \ , \ 1 \leqslant j \leqslant \ell)$, tels que, si on note

$$\gamma'_s = \prod_{j=1}^{\ell} \gamma_j^{a_{sj}} \ , \quad (1 \leqslant s \leqslant \ell') ,$$

alors $\gamma'_1,\dots,\gamma'_{\lambda'}$ engendrent un sous-groupe d'indice fini de $\Gamma' \cap H$, tandis que les images modulo H de

$\gamma'_{\lambda'+1},\ldots,\gamma'_{\ell'}$ engendrent un sous-groupe d'indice fini de $\Gamma'/\Gamma'\cap H$. En particulier $\gamma'_1,\ldots,\gamma'_{\ell'}$ engendrent un sous-groupe d'indice fini de Γ' , donc la matrice (a_{sj}) a pour rang ℓ' . De l'hypothèse sur les t_j on déduit

$$\sum_{j=1}^{\ell} a_{sj}\, t_j \in T_H \qquad \text{pour } 1 \leqslant s \leqslant \lambda' ,$$

donc l'espace vectoriel engendré sur $\mathbb{C}$ par les ℓ' éléments

$$\sum_{j=1}^{\ell} a_{sj}\, t_j , \qquad (1 \leqslant s \leqslant \ell')$$

a une dimension $\leqslant \delta+\ell'-\lambda' \leqslant \delta+\ell-\lambda$.

§4. ÉTUDE GLOBALE.

Soient K un corps de nombres, G un groupe algébrique commutatif défini sur K de dimension $d \geqslant 1$, et Γ un sous-groupe de type fini de $G(K)$, de rang ℓ sur $\mathbb{Z}$.

a) Définition de $r_v(\Gamma,G)$ et énoncé du théorème principal.

On note $\mathcal{S}$ l'ensemble formé des places archimédiennes de K, et des places finies de K pour lesquelles Γ possède un sous-groupe d'indice fini contenu dans un sous-groupe compact de $G(K_v)$.

Quand $v \in \mathcal{S}$ est une place finie, on notera $r_v(\Gamma,G)$ le nombre $r(\Gamma,G,K_v)$ introduit au §2. De même, si v est une place infinie, on lui associe un plongement de K dans $\mathbb{C}$ (via un plongement de $\mathbb{R}$ dans $\mathbb{C}$ si v est réelle) ; par ce plongement G est défini sur $\mathbb{C}$ et on note $r_v(\Gamma,G)$ le nombre $r(\Gamma,G,\mathbb{C})$ correspondant introduit au §3.

THÉORÈME 4.1. Si v_1 et v_2 sont deux éléments de $\mathcal{S}$, on a

$$r_{v_1}(\Gamma,G) \geqslant \frac{1}{\rho+1}\, r_{v_2}(\Gamma,G) .$$

Nous démontrons d'abord ce théorème, puis nous y apportons quelques compléments.

b) Démonstration du théorème 4.1.

Supposons pour commencer v_2 finie. Le lemme 2.6 permet d'extraire de Γ un sous-groupe $\tilde{\Gamma}$ vérifiant

$$\operatorname{rang}_{\mathbb{Z}} \tilde{\Gamma} = r_{v_2}(\tilde{\Gamma},G) = r_{v_2}(\Gamma,G) .$$

Alors la partie 2 du lemme 2.4 entraîne

$$\mu^*(\tilde{\Gamma},G) \leqslant 1 .$$

Finalement, le théorème 2.1 si v_1 est finie, et 3.1 si

v_1 est infinie, donne

$$r_{v_1}(\tilde{\Gamma},G) \geqslant \frac{1}{\rho+1} \operatorname{rang}_{\mathbb{Z}} \tilde{\Gamma} .$$

Comme $\tilde{\Gamma} \subset \Gamma$, on a $r_{v_1}(\tilde{\Gamma},G) \leqslant r_{v_1}(\Gamma,G)$, et le théorème 4.1 est démontré pour le cas où v_2 est finie.

Supposons maintenant v_2 infinie. Soient $t_1,\dots,t_\ell$ des éléments de $T_G(\mathbb{C})$ vérifiant les propriétés indiquées au lemme 3.8, et soit r la dimension du $\mathbb{C}$-espace vectoriel engendré par $t_1,\dots,t_\ell$. On a évidemment $r \geqslant r_{v_2}(\Gamma,G)$. On extrait de l'ensemble $t_1,\dots,t_\ell$ un système libre sur $\mathbb{C}$, disons $\tilde{t}_1,\dots,\tilde{t}_r$, et on note $\tilde{\Gamma}$ le sous-groupe de Γ engendré par les $\tilde{\gamma}_j = \exp_G \tilde{t}_j$, $(1 \leqslant j \leqslant r)$. Comme $\tilde{\Gamma}$ est de rang r sur $\mathbb{Z}$, le lemme 3.9 montre que $\mu^*(\tilde{\Gamma},G) \leqslant 1$. On utilise maintenant pour $\tilde{\Gamma}$ le théorème 2.1 si v_1 est finie, et le théorème 3.1 si v_1 est infinie :

$$r_{v_1}(\tilde{\Gamma},G) \geqslant r/(\rho+1) ,$$

d'où

$$r_{v_1}(\Gamma,G) \geqslant r_{v_1}(\tilde{\Gamma},G) \geqslant r/(\rho+1) \geqslant r_{v_2}(\Gamma,G)/(\rho+1) ,$$

ce qui démontre le théorème 4.1.

c) <u>Produits de groupes algébriques de dimension</u> 1 .

Considérons d'abord le cas $G = \mathbb{G}_m^d$. Soient $\gamma_1,\dots,\gamma_\ell$ des éléments linéairement indépendants sur $\mathbb{Z}$ (c'est-à-dire multiplicativement indépendants) de Γ. Ecrivons $\gamma_j = (\gamma_{ij})_{1 \leqslant i \leqslant d}$, avec $\gamma_{ij} \in K^\times$. Soit M la matrice (γ_{ij}) à d lignes et ℓ colonnes. Alors le nombre $\mu(\Gamma,\mathbb{G}_m^d)$ coïncide avec le coefficient $\theta(M,K^\times)$ introduit dans [7] (cf. [3] §7 et [7] §5), et $\mu^*(\Gamma,\mathbb{G}_m^d)$ n'est autre que $\theta({}^tM,K^\times)$, où ${}^tM$ est la matrice transposée de M (voir aussi [6] §7 et [5] remarque 1.3.9). Dans ce cas particulier, l'inégalité (2.2) coïncide avec le théorème 4.1 de [7], et pour obtenir l'équivalence avec (2.3) il suffit de transposer

la matrice, c'est-à-dire de considérer le sous-groupe de $K^{x\ell}$ engendré par les vecteurs lignes de M. De même l'énoncé (3.5) coïncide avec le corollaire 4.2 de [6], et l'équivalence entre (3.2) et (3.3) est ici évidente.

Supposons, un peu plus généralement, que G soit produit de groupes algébriques de dimension 1. Ecrivons $G = \mathbb{G}_a^{d_o} \times \mathbb{G}_m^{d_1} \times E_2^{d_2} \times \ldots \times E_h^{d_h}$, où $h \geqslant 1$, $d_o \geqslant 0$, $d_1 \geqslant 0$, $d_2 \geqslant 1, \ldots, d_h \geqslant 1$ sont des entiers rationnels et $E_2, \ldots, E_h$ sont des courbes elliptiques définies sur K et deux-à-deux non isogènes. Considérons un plongement de K dans $\mathbb{C}$. La condition sur $t_1, \ldots, t_\ell$ donnée dans le lemme 3.8 peut être explicitée de la manière suivante. Ecrivons $t_j = (u_{sij})$, et $\exp_G t_j = \gamma_j = (\gamma_{sij})$ avec, pour $1 \leqslant j \leqslant \ell$,

$$u_{oij} = \gamma_{oij} \in K, \qquad (1 \leqslant i \leqslant d_o),$$

$$e^{u_{1ij}} = \gamma_{1ij} \in K^x, \qquad (1 \leqslant i \leqslant d_1),$$

et, pour $2 \leqslant s \leqslant h$,

$$\exp_{E_s} u_{sij} = \gamma_{sij} \in E_s(K), \qquad (1 \leqslant i \leqslant d_s).$$

Pour $s = 1$, on demande que toute relation de la forme

$$\prod_{i=1}^{d_1} \prod_{j=1}^{\ell} \gamma_{1ij}^{a_i b_j} = 1$$

avec des entiers rationnels a_i, b_j implique

$$\sum_{i=1}^{d_1} \sum_{j=1}^{\ell} a_i b_j u_{1ij} = 0.$$

Pour $2 \leqslant s \leqslant h$, en notant A_s l'anneau des endomorphismes de E_s, on demande que toute relation dans $E_s(\mathbb{C})$ de la forme

$$\sum_{i=1}^{d_s} \sum_{j=1}^{\ell} a_i b_j \gamma_{sij} = 0$$

avec a_i et b_j dans A_s implique

$$\sum_{i=1}^{d_s} \sum_{j=1}^{\ell} a_i b_j u_{sij} = 0.$$

L'équivalence entre ces conditions et celle du lemme 3.8 repose sur le théorème de Kolchin (voir [3] §8).

Notons alors M la matrice (u_{sij}) à d lignes (indexées par (s,i)) et ℓ colonnes (indexées par j). La démonstration du théorème 4.1 montre que pour tout $v \in \mathcal{S}$, on a

$$r_v(\Gamma,G) \geqslant \tfrac{1}{3} \operatorname{rang} M .$$

Bien entendu, si $h=1$, c'est-à-dire si $G = \mathbb{G}_a^{d_0} \times \mathbb{G}_m^{d_1}$, on peut remplacer $1/3$ par $1/2$. Nous allons voir qu'il en est de même quand $G = E^d$ où E est une courbe elliptique ayant multiplication complexe, et aussi que dans ce cas on a

$$r_{v_1}(\Gamma,E^d) \geqslant \tfrac{1}{2} r_{v_2}(\Gamma,E^d) \tag{4.2}$$

pour tout v_1, v_2 dans $\mathcal{S}$.

Démontrons d'abord (4.2) dans le cas où v_2 est finie. Comme G est un produit de groupes algébriques de dimension 1, on peut supposer $r_{v_2}(\Gamma,G) = d$ (cela revient à extraire d'une matrice un nombre maximal de lignes indépendantes, c'est-à-dire ici à considérer un sous-produit de $E \times \ldots \times E = E^d$). D'autre part, en notant A l'anneau des endomorphismes de E, on ne modifie pas $r_v(\Gamma,E^d)$ si on remplace Γ par le sous-A-module qu'il engendre ; on supposera donc Γ stable par A. Si H est un sous-groupe algébrique de E^d défini sur K de dimension δ, et si $\lambda = \operatorname{rang}_{\mathbb{Z}} \Gamma \cap H$, alors, comme H est stable par A, $\Gamma \cap H$ est un A-module de rang $\lambda/2$, et $\Gamma/\Gamma \cap H$ est un A-module de rang $(\ell-\lambda)/2$. On obtient (comparer avec le lemme 2.4) :

$$r_{v_2}(\Gamma,E^d) \leqslant \delta + (\ell-\lambda)/2 ,$$

donc $\mu(\Gamma,G) \geqslant 2$. L'inégalité (4.2) résulte alors du théorème 2.1 si v_1 est finie, et du théorème 3.1 sinon.

Quand v_2 est infinie, correspondant à un plongement de K dans $\mathbb{C}$, l'inégalité (4.2) est légèrement moins précise que l'inégalité annoncée

$$r_v(\Gamma,G) \geqslant \frac{1}{2} \text{ rang } M .$$

Pour démontrer celle-ci on se ramène au cas où M est de rang d (cela n'affecte pas les conditions sur les u_{sij}), puis où Γ est stable par $A = \text{End } E$. Comme ci-dessus on obtient $u(\Gamma,G) \geqslant 2$ (comparer avec le lemme 3.9), et l'inégalité (2.2) ou (2.3) permet de conclure.

BIBLIOGRAPHIE

[1] D. BERTRAND.- Problèmes locaux. Appendice 1 de [5].

[2] D.W. MASSER.- Interpolation on group varieties. (Dans ce volume).

[3] D.W. MASSER and G. WÜSTHOLZ.- Zero estimates in group varieties. Invent. Math., 64 (1981), 489-516.

[4] J.-P. SERRE.- Quelques propriétés des groupes algébriques commutatifs. Appendice 2 de [5].

[5] M. WALDSCHMIDT.- Nombres transcendants et groupes algébriques. Astérisque (Soc. Math. France) 69-70 (1979).

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

[7] M. WALDSCHMIDT.- A lower bound for the p-adic rank of the units of an algebraic number field. Coll. Number Theory, Janos Bolyai Math. Soc., Budapest, July 1981. Topics in classical number theory vol. 34.

(Texte reçu le 15 juillet 1982)

M. WALDSCHMIDT
Institut Henri Poincaré
11, rue Pierre et Marie Curie
75231 Paris Cédex 05
(France)