Groupes algébriques et grands degrés de transcendance

par

MICHEL WALDSCHMIDT

Institut Henri Poincaré
Paris, France

Sommaire

§1. Introduction

On considère un sous-corps K de $\mathbf{C}$, de degré de transcendance $t \geqslant 0$ sur $\mathbf{Q}$, et un groupe algébrique commutatif connexe G de dimension $d>1$ défini sur K. On note $T_G(\mathbf{C})$ l'espace tangent à l'origine de $G(\mathbf{C})$, $\exp_G : T_G(\mathbf{C}) \to G(\mathbf{C})$ l'application exponentielle de $G(\mathbf{C})$, et Ω le noyau de $\exp_G$. Soit V un sous-espace vectoriel de $T_G(\mathbf{C})$ de dimension n sur $\mathbf{C}$, avec $1 \leqslant n < d$, tel que $\exp_G V$ soit dense pour la topologie de Zariski dans $G(\mathbf{C})$. On note $\varkappa = \mathrm{rg}_{\mathbf{Z}}\, \Omega \cap V$, où $\mathrm{rg}_{\mathbf{Z}}$ désigne le rang sur $\mathbf{Z}$. On définit $\varrho = \varrho(G)$ par : $\varrho = 1$ si G est linéaire, et $\varrho = 2$ sinon. Ainsi $\varkappa \leqslant \varrho n$.

Soit $Y=\mathbf{Z}y_1+\ldots+\mathbf{Z}y_m$ un sous-groupe de type fini de V de rang m sur $\mathbf{Z}$, tel que $\Gamma=\exp_G Y$ soit contenu dans $G(K)$. On désigne par ℓ le rang de Γ sur $\mathbf{Z}$, de sorte que $m-\ell=\mathrm{rg}_{\mathbf{Z}}\,\Omega\cap Y$ et $0\leqslant m-\ell\leqslant\varkappa$.

Si on choisit une base $v_1,\ldots,v_n$ de V sur $\mathbf{C}$, si $\mathscr{L}\colon\mathbf{C}^n\to T_G(\mathbf{C})$ désigne l'application linéaire associée :

$$\mathscr{L}(z_1,\ldots,z_n)=\sum_{\nu=1}^{n}z_\nu v_\nu,$$

et enfin si on pose $\mathscr{L}^{-1}(y_j)=u_j=(u_{j1},\ldots,u_{jn})$, $(1\leqslant j\leqslant m)$, on voit que la situation étudiée est celle d'un sous-groupe à n-paramètres $\varphi=\exp_G\circ\mathscr{L}$ de $G(\mathbf{C})$ dont l'image est dense dans $G(\mathbf{C})$, et dont les valeurs

$$\varphi(u_j)=\exp_G\left(\sum_{\nu=1}^{n}u_{j\nu}v_\nu\right),\quad(1\leqslant j\leqslant m)$$

en des points $u_1,\ldots,u_m$ $\mathbf{Q}$-linéairement indépendants de $\mathbf{C}^n$ sont dans $G(K)$.

On cherche à minorer t en fonction de n, ℓ, d et $\varkappa$. Commençons par regarder le cas $n=1$.

(a) *Sous-groupes à un paramètre.* Quand $n=1$, on a $V=\mathbf{C}v$, avec $v\in T_G(\mathbf{C})$, $v\neq 0$, et l'hypothèse que $\exp_G V$ est dense dans $G(\mathbf{C})$ signifie que pour tout sous-groupe algébrique H de G, avec $H\neq G$, on a $v\notin T_H(\mathbf{C})$.

La méthode de transcendance de Schneider [Wa1] § 4.2 permet de montrer :

$$si\ (\ell+\varkappa)\,d>\ell+dQ,\ alors\ t>0.$$

Quand on utilise, de plus, le critère de Gel'fond [Br] et un lemme de zéros de Masser et Wüstholz [MW1], on obtient (cf. [Wa2], (5.7)) :

$$si\ (\ell+\varkappa)\,d\geqslant 2(\ell+dQ),\ alors\ t>1.$$

Cet énoncé généralise des résultats d'indépendance algébrique sur les valeurs de la fonction exponentielle (Gel'fond, Shmelev, Tijdeman, Brownawell, ...) et de fonctions elliptiques (Brownawell-Kubota, Shmelev, Masser-Wüstholz, ...); cf. [Wa4] § I1 et I3.

D'aprés la conjecture (6.9) de [Wa2], on devrait avoir :

$$si\ (\ell+\varkappa)\,d>\ell+dQ,\ alors\ t+1>(\ell+\varkappa)\,d/(\ell+dQ). \tag{1.1}$$

Philippon a déjà obtenu l'inégalité

$$t+1\geqslant(\ell+\varkappa)\,d/(\ell+dQ) \tag{1.2}$$

dans plusieurs cas particuliers : d'abord quand G est une variété abélienne, moyennant une hypothèse sur l'action des endomorphismes [P2, P3], puis quand G est un groupe linéaire [P4] (l'hypothèse que G est linéaire lui permet d'utiliser un résultat de Tijdeman — cf. [Br] — sur les petites valeurs de polynômes exponentiels). L'outil principal de Philippon est son très bon critère d'indépendance algébrique (voir ci-dessous § 2).

Ici, nous établirons (1.2) pour un groupe algébrique commutatif G quelconque, mais avec une hypothèse technique supplémentaire. Dans la deuxième partie de ce travail, nous verrons plusieurs exemples où cette hypothèse prend une forme familière. Par exemple dans le cas linéaire, elle se réduit à des mesures d'indépendance linéaire qui apparaissent dans tout les travaux sur cette question [Br, P4, Wa4].

(b) *Sous-groupes à plusieurs paramètres.* Dans le cas $n>1$, on peut avoir $t=0$ sans que m et d soient bornés en fonction de n (cf. [Wa2] § 1). Mais on obtient une situation analogue à celle du cas $n=1$ si on remplace le nombre $m=\mathrm{rg}_{\mathbf{Z}} Y$ par le coefficient de Dirichlet généralisé [Wa1] § 1.3 :

$$\mu(Y, V) = \min_{W} \{(\mathrm{rg}_{\mathbf{Z}} Y/Y \cap W)/\dim_{\mathbf{C}} V/W\},$$

où W décrit les sous-espaces vectoriels de V sur $\mathbf{C}$ avec $W \neq V$, et $\dim_{\mathbf{C}}$ désigne la dimension d'un $\mathbf{C}$-espace vectoriel. On a évidemment $\mu(Y, V) \leqslant m/n$, et si $n=1$ on a $\mu(Y, V)=m$.

On déduit de [Wa2], en posant $\mu(Y)=\mu(Y, V)$:

$$\text{si } d\mu(Y) > n\mu(Y)+d\varrho-\varkappa, \text{ alors } t>0,$$

et

$$\text{si } d\mu(Y) \geqslant 2(n\mu(Y)+d\varrho-\varkappa), \text{ alors } t>1.$$

Notre but est d'établir l'inégalité :

$$t+1 \geqslant d\mu(Y)/(n\mu(Y)+d\varrho-\varkappa). \tag{1.3}$$

Quand $n=1$, on retrouve (1.2) en appliquant (1.3) à $\tilde{Y}=Y+V\cap\Omega$, avec $\mu(\tilde{Y})=\ell+\varkappa$, et $\exp_G \tilde{Y}=\exp_G Y=\Gamma\subset G(K)$.

Pour établir (1.3), la méthode que nous utiliserons nécessite une hypothèse technique (cf. § 9) qu'il est plus facile de vérifier quand G est défini sur le corps $\bar{\mathbf{Q}}$ des nombres algébriques. Donnons-en déjà un exemple.

(c) *Un corollaire du théorème principal.* Le théorème principal est énoncé au § 3. Mais en voici déjà une conséquence.

On plonge G comme sous-variété quasi-projective d'un espace projectif $\mathbf{P}_N$ sur K, et on dira, suivant [MW2], qu'un sous-groupe algébrique H de G peut être défini par des équations de degré $\leqslant M$ s'il existe des hypersurfaces $Z_1, \ldots, Z_k$ de $\mathbf{P}_N$, de degrés $\leqslant M$, telles que

$$H = G \cap Z_1 \cap \ldots \cap Z_k.$$

D'autre part, quand $\Gamma = \mathbf{Z}\gamma_1 + \ldots + \mathbf{Z}\gamma_\ell$ est un $\mathbf{Z}$-module de type fini muni d'un système générateur $(\gamma_1, \ldots, \gamma_\ell)$, on note, pour M réel positif,

$$\Gamma(M) = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell;\ (h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell,\ 0 \leqslant h_j \leqslant M,\ 1 \leqslant j \leqslant \ell\},$$

et

$$\Gamma_\pm(M) = \{h_1\gamma_1 + \ldots + h_\ell\gamma_\ell;\ (h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell,\ |h_j| \leqslant M,\ 1 \leqslant j \leqslant \ell\}.$$

Par exemple on notera

$$\mathbf{Z}^\ell_\pm(M) = \{(h_1, \ldots, h_\ell) \in \mathbf{Z}^\ell;\ |h_j| \leqslant M,\ 1 \leqslant j \leqslant \ell\}.$$

Enfin on choisit une norme sur $T_G(\mathbf{C})$.

THÉORÈME 1.4. *On suppose que G est défini sur $\bar{\mathbf{Q}} \cap K$. On suppose aussi que pour tout $\varepsilon > 0$, il existe $M_0 > 0$ tel que pour tout $M \geqslant M_0$, pour tout sous-groupe algébrique H de G défini par des équations de degré $\leqslant M$, pour tout $y \in Y_\pm(M)$ vérifiant $\exp_G Y \notin H(\mathbf{C})$, et pour tout $u \in T_G(\mathbf{C})$ vérifiant $\exp_G u \in H(\mathbf{C})$, on a*

$$|u - y| \geqslant \exp(-M^\varepsilon). \tag{1.5}$$

Alors

$$t + 1 \geqslant d\mu(Y)/(n\mu(Y) + d\varrho - \varkappa).$$

(d) *Principe de la démonstration.* L'outil essentiel de la démonstration est le critère d'indépendance algébrique obtenu récemment par Philippon [P4]. Nous l'utilisons sous la forme suivante : le coefficient $J(\theta_1, \ldots, \theta_t)$ introduit dans [WZ], et associé à un point $(\theta_1, \ldots, \theta_t)$ de $\mathbf{C}^t$, est majoré par $t+1$ (cf. § 2 ci-dessous).

Comme cela est expliqué dans [Br, MW2, P4, Wa4] (textes auxquels nous renvoyons pour une description des différentes méthodes d'indépendance algébrique, ainsi que pour des références bibliographiques), les seuls résultats que l'on connaissait jusqu'à un temps récent sur l'indépendance algébrique et les grands degrés de transcen-

dance concernaient la fonction exponentielle usuelle en une variable (Chudnovsky, Warkentin, Philippon-Reyssat, Endell, Brownawell, Nesterenko). La principale difficulté pour généraliser la méthode à d'autres groupes algébriques vient de ce que l'on ne connait pas de « lemme de petites valeurs » pour un sous-groupe $\Gamma=\mathbf{Z}\gamma_1+\ldots+\mathbf{Z}\gamma_\ell$ de $G(\mathbf{C})$.

Rappelons que, dans le jargon des spécialistes, un *lemme de zéros* (cf. [MW1]) est une minoration du degré des hypersurfaces de l'espace $\mathbf{P}_N$ (dans lequel est plongé G) qui contiennent $\Gamma(S)$, mais qui ne contiennent pas G. Un *lemme de petites valeurs* permettrait, pour une hypersurface Z de degré inférieur à cette borne, de trouver un point γ de $\Gamma(S)$ qui soit « loin » de Z.

Une telle estimation n'est connue que pour les polynômes exponentiels en une variable (Gel'fond, Mahler, Tijdeman; cf. [Br]). Elle intervient lorsqu'on utilise le critère d'indépendance algébrique de Chudnovsky-Reyssat : on doit construire une suite de polynômes de $\mathbf{Z}[X_1,\ldots,X_t]$ prenant en un point fixé $(\theta_1,\ldots,\theta_t)$ de $\mathbf{C}^t$ une valeur qui soit petite, mais pas trop petite; c'est la minoration de cette valeur qui est la source de nos problèmes.

Plusieurs méthodes ont été élaborées ces dernières années pour surmonter cette difficulté. Dans [MW2], Masser et Wüstholz utilisent une version effective du théorème des zéros de Hilbert qu'ils combinent avec un raffinement de leur lemme de zéros de [MW1] pour remplacer le lemme de petites valeurs dans le cas d'un produit de courbes elliptiques. Il leur faut aussi une description très précise des sous-groupes algébriques, et dans ce but ils apportent un raffinement quantitatif au théorème de Kolchin. Cela réduit sérieusement le champ d'application de la méthode. De plus, dans l'estimation finale, outre un terme en 2^t qui provient du Nullstellensatz (et dont on peut espérer qu'il puisse être remplacé par $t+1$), un terme parasite, linéaire en t, provient d'estimations techniques concernant les composantes primaires d'idéaux dans des anneaux de polynômes.

La première méthode ayant conduit, dans le présent contexte, à de bonnes estimations pour les grands degrés de transcendance dans la méthode de Schneider (c'est-à-dire à des minorations linéaires, alors que les précédentes étaient logarithmiques) est celle de Philippon [P2, P3]. Dans son critère d'indépendance algébrique, au lieu de considérer une suite de polynômes, il prend une suite d'idéaux. Comme dans les travaux de Masser et Wüstholz, l'outil essentiel est l'algèbre commutative, introduite dans ce sujet par Nesterenko. Les premiers critères de Philippon l'obligeaient à travailler avec des variétés abéliennes. Son critère récent [P4], plus général, lui permet de traiter aussi les groupes algébriques linéaires. Il a ainsi obtenu les meilleurs résultats

qu'on puisse espérer, dans l'état actuel de la théorie, sur l'indépendance algébrique des valeurs de la fonction exponentielle en une variable [P4].

Voici comment nous allons procéder pour ne pas utiliser de lemme de petites valeurs. Quand on regarde les démonstrations de grands degrés de transcendance pour la fonction exponentielle [Br], on constate que ce lemme sert de la manière suivante : si on perturbe un peu un système générateur de K sur $\mathbf{Q}$, et si $\tilde{\gamma}$ désigne le point obtenu à partir de γ (qui était « loin » de l'hypersurface Z) par cette déformation, alors $\tilde{\gamma}$ n'appartient pas à Z.

Ici, nous demanderons seulement que, pour toute petite perturbation du système générateur, il existe un point de $\tilde{\Gamma}(S)$, (dépendant de la perturbation), qui ne soit pas sur Z. Le coefficient $J(\theta_1, \ldots, \theta_t)$ de [P4] et [WZ] est précisément adapté à cette situation. Et on vérifie l'hypothèse que Z ne contient pas $\tilde{\Gamma}(S)$ en utilisant le lemme de zéros raffiné de [MW2]; mais c'est là qu'intervient l'hypothèse technique indésirable de nos énoncés.

Nous donnerons une série de corollaires des résultats sur les groupes algébriques. Nous ne chercherons pas des énoncés généraux, mais au contraire des exemples concrets, dans lesquels nous montrerons que l'hypothèse technique prend une forme naturelle. Pour un aperçu historique du sujet, nous renvoyons à [Wa4].

(e) Voici le *plan* de ce travail. Nous commençons par donner l'énoncé du critère d'indépendance algébrique de Philippon (§ 2), qui fait intervenir le coefficient J mentionné plus haut. Puis nous énonçons le théorème principal (§ 3) où nous supposons G défini sur $\bar{\mathbf{Q}}$. Nous construisons ensuite une fonction auxiliaire (§ 4). Pour utiliser la définition de J, nous sommes amené à faire subir des petites perturbations à $y_1, \ldots, y_m$ (§ 5). Nous complétons la démonstration du théorème principal au § 6, et celle du théorème 1.4 au § 7. Puis nous donnons une variante du théorème 1.4 (§ 8).

Nous généralisons ensuite le théorème principal au cas où G n'est plus défini sur $\bar{\mathbf{Q}}$ (§ 9). La démonstration (§ 11) utilise une déformation du groupe algébrique G dont la construction est exposée au § 10.

Dans la deuxième partie de ce texte, nous donnons des corollaires, en commençant par la fonction exponentielle usuelle (§ 12). Notons $\langle \cdot, \cdot \rangle$ le produit scalaire usuel dans $\mathbf{C}^n$:

$$\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle = u_1 v_1 + \ldots + u_n v_n.$$

Sous des hypothèses que nous allons expliciter, nous montrons que si

$$X = \mathbf{Z}x_1 + \ldots + \mathbf{Z}x_d \quad \text{et} \quad Y = \mathbf{Z}y_1 + \ldots + \mathbf{Z}y_m$$

sont des sous-groupes de $\mathbf{C}^n$ de rangs d et m respectivement, alors le degré de transcendance t du corps engendré sur $\mathbf{Q}$ par les nombres

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

vérifie

$$t+1 \geqslant md/n(m+d).$$

Quand $n=1$ on retrouve un résultat récent de Philippon [P4].

On prend ensuite (§ 13) une fonction elliptique $\wp$ d'invariant j algébrique. Quand $\wp$ n'a pas de multiplication complexe, sous les mêmes hypothèses que dans le cas exponentiel, le degré de transcendance t du corps engendré par les nombres $\wp\langle x, y\rangle$, pour $x \in X$, $y \in Y$ et $\langle x, y\rangle$ non pôle de $\wp$, vérifie

$$t+1 \geqslant md/n(m+2d).$$

On donne aussi des variantes de cet énoncé quand j est trancendant, ou quand $\wp$ admet des multiplications complexes. On considère également l'indépendance algébrique de nombres de la forme $\wp_i(v_j)$, quand $\wp_1, \ldots, \wp_d$ sont différentes fonctions elliptiques, et $v_1, \ldots, v_m$ des nombres complexes.

L'énoncé suivant (§ 14) porte sur des nombres de la forme

$$\sigma(v-u)\, e^{\zeta(u)v}/\sigma(v)\,\sigma(u),$$

quand $\wp(u)$ et $\wp(v)$ sont algébriques.

Enfin au § 15 on considère des fonctions abéliennes. On prend d'abord une variété abélienne A telle que $\mathrm{End}\, A = \mathbf{Z}$, de dimension $g \geqslant 1$, on note $f_1, \ldots, f_g$ des fonctions abéliennes, méromorphes sur $\mathbf{C}^g$, algébriquement indépendantes, associées à A, et on donne un résultat d'indépendance algébrique pour des nombres de la forme $f_i(uv)$, $(1 \leqslant i \leqslant g,\ u \in \mathbf{C}^g,\ v \in \mathbf{C})$. On donne aussi un énoncé pour un sous-groupe à n-paramètres d'une variété abélienne simple.

Pour terminer nous indiquons brièvement quelques résultats complémentaires et nous proposons plusieurs conjectures (§ 16).

§ 2. Le critère d'indépendance algébrique de Philippon

Etant donné un polynôme $P \in \mathbf{Z}[X_1, \ldots, X_t]$, $P \neq 0$, on note $d(P)$ le maximum de ses degrés partiels, $H(P)$ sa hauteur (maximum des valeurs absolues de ses coefficients), et

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

Soient $\theta_1, \ldots, \theta_t$ des nombres complexes. On désigne par $A(\theta_1, \ldots, \theta_t)$ l'ensemble des nombres $\eta > 1$ ayant la propriété suivants : il existe $T_0 > 0$ tel que pour tout $T > T_0$ et tout $(\tilde{\theta}_1, \ldots, \tilde{\theta}_t) \in \mathbf{C}^t$ vérifiant

$$\max_{1 \leqslant \tau \leqslant t} |\tilde{\theta}_\tau - \theta_\tau| < \exp(-2T^\eta), \tag{2.1}$$

il existe un polynôme $P \in \mathbf{Z}[X_1, \ldots, X_t]$ vérifiant $t(P) \leqslant T$ et

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

On note ensuite $J(\theta_1, \ldots, \theta_t)$ la borne supérieure cet ensemble $A(\theta_1, \ldots, \theta_t)$ s'il est non vide, avec $J(\theta_1, \ldots, \theta_t) = 1$ si $A(\theta_1, \ldots, \theta_t)$ est vide.

L'énoncé suivant, conjecturé dans [WZ], est une conséquence du critére de Philippon dans [P4] :

THÉORÈME 2.2 (Philippon). *Pour tout* $(\theta_1, \ldots, \theta_t) \in \mathbf{C}^t$, *on a*

$$J(\theta_1, \ldots, \theta_t) \leqslant t+1.$$

On peut aussi penser que $J(\theta_1, \ldots, \theta_t) = t+1$ pour presque tout $(\theta_1, \ldots, \theta_t) \in \mathbf{C}^t$, c'est-à-dire en dehors d'un ensemble de mesure nulle. D'un autre côté il existe des nombres complexes $\theta_1, \ldots, \theta_t$, algébriquement indépendants, tels que $J(\theta_1, \ldots, \theta_t) = 1$ (cf. [WZ] lemme 4.1). Ainsi une minoration de $J = J(\theta_1, \ldots, \theta_t)$ contient plus d'informations qu'une simple minoration du degré de transcendance. Néanmoins pour obtenir des énoncés effectifs d'approximation simultanée dans le cas algébrique ($\Gamma \subset G(\bar{\mathbf{Q}})$), la méthode indiquée au § 6 d de [Wa2] est plus efficace puisqu'elle ne nécessite aucune hypothèse parasite analogue à (1.5).

§ 3. Le théorème principal

Nous adoptons les notations du § 1, mais nous supposons ici que le groupe algébrique G est défini sur $K \cap \bar{\mathbf{Q}}$.

On dispose donc d'un sous-groupe $Y = \mathbf{Z}y_1 + \ldots + \mathbf{Z}y_m$ de type fini de $V \subset T_G(\mathbf{C})$, avec $\Gamma = \exp_G(Y) \subset G(K)$. Le rang sur $\mathbf{Z}$ de $Y \cap \Omega$ est $m - \ell$. On supposera que $y_{\ell+1}, \ldots, y_m$ appartiennent à $\Omega = \operatorname{Ker} \exp_G$.

THÉORÈME 3.1. *Soit* $(\theta_1, \ldots, \theta_t)$ *une base de transcendance de* K *sur* $\mathbf{Q}$, *et soit* $\mu > 0$. *Supposons*

$$J(\theta_1, \ldots, \theta_t) < (d\mu+\varkappa)/n(\mu+\varrho).$$

Alors il existe un réel $\varepsilon>0$, *deux entiers* ℓ_1 et d_1 *vérifiant*

$$0 \leqslant \ell_1 \leqslant \ell, \quad 1 \leqslant d_1 \leqslant d, \quad \ell_1/d_1 < \mu,$$

et il existe une infinité d'entiers $M>0$ *ayant la propriété suivante : il existe un sous-groupe algébrique* H *de* G, *de dimension* $\leqslant d-d_1$, *défini par des équations de degré* $\leqslant M$, *il existe des éléments* $h^{(1)}, \ldots, h^{(\ell-\ell_1)}$ *de* $\mathbf{Z}_{\pm}^{\ell}(M)$, *linéairement indépendants sur* $\mathbf{Z}$, *et enfin des éléments* $\tilde{y}_1, \ldots, \tilde{y}_\ell$ *de* $T_G(\mathbf{C})$, *avec*

$$\max_{1\leqslant j\leqslant \ell} |\tilde{y}_j - y_j| < \exp(-M^c),$$

tels que

$$\exp_G \sum_{j=1}^{\ell} h_j^{(s)} \tilde{y}_j \in H(\mathbf{C}) \quad \textit{pour } 1 \leqslant s \leqslant \ell-\ell_1.$$

Le paramètre μ n'est pas lié directement au coefficient $\mu(Y)=\mu(Y, V)$ du § 1, mais plutôt au coefficient $\mu(\Gamma, G)$ qui interviendra plus loin (§ 7). Dans le « cas général », on a

$$\mu(Y, V) = m/n \quad \text{et} \quad \mu(\Gamma, G) = \ell/d.$$

On peut noter que la conclusion du théorème 3.1 est banale si on choisit $\mu>\ell/d$: il suffit de prendre $\ell_1=\ell$, $d_1=d$, $H=0$. (Pour la même raison, la conclusion est banale, en prenant $\tilde{y}_j=y_j$, si on choisit $\mu>\mu(\Gamma, G)$).

§ 4. La fonction auxiliaire

Soit G un groupe algébrique commutatif connexe sur un sous-corps K de $\mathbf{C}$. On considère la compactification lisse $\bar{G}$ de G et un plongement projectif

$$f=(f_0, \ldots, f_N): \bar{G} \to \mathbf{P}_N$$

construits par Serre dans [S]. Notons

$$f \circ \exp_G = (F_0, \ldots, F_N): T_G(\mathbf{C}) \to \mathbf{P}_N(\mathbf{C}),$$

où $F_0, \ldots, F_N$ sont entières, d'ordre strict $\leqslant \varrho=\varrho(G)$, et ne s'annulent simultanément en aucun point de $T_G(\mathbf{C})$.

On considère un sous-espace vectoriel V de $T_G(\mathbf{C})$ de dimension n sur $\mathbf{C}$, on note $\Omega=\mathrm{Ker}\exp_G$, $\varkappa=\mathrm{rg}_{\mathbf{Z}}\,\Omega\cap V$, et on choisit $\mu>0$ et $\nu>0$ tels que

$$d\mu+\varkappa>n(\mu+\varrho) \quad \text{et} \quad \nu>\mu+\varrho.$$

On choisit aussi une distance sur $T_G(\mathbf{C})$.

Soit c_0 un entier positif suffisamment grand, et soit S_0 un entier beaucoup plus grand. Pour chaque réel $S\geqslant S_0$, on définit D, Δ, U par

$$D=c_0^{-1}S^{\mu}, \quad \Delta=c_0^{-1}S^{\mu+\varrho}, \quad U^{n+1}=c_0^{-d-2}S^{\mu+\varrho+d\mu+\varkappa}.$$

On désigne par $\mathscr{E}(S)$ l'ensemble des $z\in T_G(\mathbf{C})$ vérifiant

$$|z|\leqslant c_0 S \quad \text{et} \quad \mathrm{dist}(z,V)\leqslant\exp(-(2-3c_0^{-1})S^{\nu}).$$

PROPOSITION 4.1. *Il existe un polynôme homogène $P\in\mathbf{Z}[X_0,\ldots,X_N]$, non partout nul sur $G(\mathbf{C})$, de degré $\leqslant D$ et de hauteur $\leqslant e^{\Delta}$, tel que la fonction entière $E=P(F_0,\ldots,F_N)$ vérifie*

$$\sup_{z\in\mathscr{E}(S)}|E(z)|\leqslant e^{-U}+\exp(-(2-4c_0^{-1})S^{\nu}).$$

Démonstration. La proposition 2.1 de [Wa2] permet de construire P de telle sorte que

$$|E(v)|\leqslant e^{-U}$$

pour tout $v\in V$ vérifiant $|v|\leqslant(c_0+1)S$. Ensuite, pour $z\in\mathscr{E}(S)$, on choisit $v\in V$ tel que

$$|z-v|\leqslant\exp(-(2-3c_0^{-1})S^{\nu}).$$

Comme $|z|\leqslant c_0 S$, on a $|v|\leqslant(c_0+1)S$, donc $|E(v)|\leqslant e^{-U}$. Mais

$$|E(z)-E(v)|\leqslant|z-v|\exp(c_0^3\Delta),$$

d'où la proposition.

§ 5. Petites perturbations

Nous nous plaçons de nouveau dans la situation des paragraphes 1 et 3. De plus nous désignons par $y_{\ell+1},\ldots,y_{\ell+\varkappa}$ des éléments $\mathbf{Z}$-linéairement indépendants de $\Omega\cap V$, ce qui est cohérent avec les notations précédentes.

Supposons $d\mu+\varkappa>n(\mu+\varrho)$, choisissons un nombre réel η vérifiant

$$1<\eta<(d\mu+\mu+\varrho+\varkappa)/(n+1)(\mu+\varrho),$$

et posons

$$\nu=\eta(\mu+\varrho).$$

On suppose (ce n'est pas restrictif) que le corps K est de type fini sur $\mathbf{Q}$. On écrit $K=\mathbf{Q}(\theta_1,\ldots,\theta_t,\theta_{t+1})$, où θ_{t+1} est entier sur l'anneau $A=\mathbf{Z}[\theta_1,\ldots,\theta_t]$. Soit $B\in A[X]$ le polynôme minimal (unitaire) de θ_{t+1} sur A.

Soit encore $c_0>0$ suffisamment grand. Pour utiliser la définition de J (§ 2), on choisit T_0 beaucoup plus grand que c_0. Soit $T>T_0$, et soit $(\tilde\theta_1,\ldots,\tilde\theta_t)\in\mathbf{C}^t$ vérifiant (2.1). Le semi-résultant de Chudnovsky (cf. par exemple [Br, WZ]) montre qu'il existe une racine $\tilde\theta_{t+1}$ de $B(\tilde\theta_1,\ldots,\tilde\theta_t,X)$, à distance minimale de θ_{t+1}, que cette racine est simple, et qu'elle vérifie

$$|\tilde\theta_{t+1}-\theta_{t+1}|<\exp(-(2-c_0^{-1})T^\eta).$$

Fixons un indice j, $1\leqslant j\leqslant\ell+\varkappa$. On écrit que $\gamma_j=\exp_G y_j$ appartient à $G(K)$: il existe des polynômes homogènes $\varphi_0,\ldots,\varphi_N$ (dépendant de j, mais pas de c_0) dans $\mathbf{Z}[X_1,\ldots,X_{t+1}]$ tels que

$$(\varphi_\nu(\theta_1,\ldots,\theta_{t+1}),\quad 0\leqslant\nu\leqslant N)$$

soit un système de coordonnées projectives de γ_j dans $\mathbf{P}_N(K)$. On considère le point $\tilde\gamma_j$ de $\mathbf{P}_N(\mathbf{C})$, de coordonnées projectives

$$(\varphi_\nu(\tilde\theta_1,\ldots,\tilde\theta_{t+1}),\quad 0\leqslant\nu\leqslant N).$$

Pour c_0 suffisamment grand, $\tilde\gamma_j$ est bien défini et appartient à $G(\mathbf{C})$. En effet, dans l'anneau factoriel $R=(K\cap\bar{\mathbf{Q}})[\theta_1,\ldots,\theta_t,X]$, on décompose B en facteurs irréductibles; il existe un et un seul facteur, disons B_1, qui s'annule au point $\theta=(\theta_1,\ldots,\theta_{t+1})$. Donc pour c_0 suffisamment grand il s'annule aussi en $\tilde\theta=(\tilde\theta_1,\ldots,\tilde\theta_{t+1})$. Maintenant si $Q\in R$ vérifie $Q(\theta)=0$, alors B_1 divise Q, donc $Q(\tilde\theta)=0$. Nous appliquons cette remarque aux éléments de l'idéal de G.

Notons que si $\gamma_j\in G(K\cap\bar{\mathbf{Q}})$, alors $\tilde\gamma_j=\gamma_j$; en effet, si, disons, $\varphi_0(\theta)\neq0$ et $\varphi_0(\tilde\theta)\neq0$ (pour c_0 suffisamment grand), alors il existe $\alpha_\nu\in K\cap\bar{\mathbf{Q}}$ tel que $\varphi_\nu(\theta)=\alpha_\nu\varphi_0(\theta)$. Mais B_1 divise $\varphi_\nu-\alpha_\nu\varphi_0$ dans l'anneau R, donc $\varphi_\nu(\tilde\theta)=\alpha_\nu\varphi_0(\tilde\theta)$, et $\tilde\gamma_j=(1,\alpha_1,\ldots,\alpha_N)=\gamma_j$.

L'exponentielle de G étant un difféomorphisme local, on peut choisir $\tilde y_j\in T_G(\mathbf{C})$ tel

que $\exp_G \tilde{y}_j = \tilde{\gamma}_j$ et

$$|\tilde{y}_j - y_j| < \exp(-(2-2c_0^{-1})T^{\eta}).$$

Comme $\gamma_{\ell+1} = \ldots = \gamma_{\ell+\varkappa} = 0$, on a aussi $\tilde{\gamma}_{\ell+1} = \ldots = \tilde{\gamma}_{\ell+\varkappa} = 0$, et $\tilde{y}_{\ell+k} = y_{\ell+k}$, $(1 \leqslant k \leqslant \varkappa)$. Notons

$$\tilde{Y} = \mathbf{Z}\tilde{\gamma}_1 + \ldots + \mathbf{Z}\tilde{\gamma}_{\ell+\varkappa} \quad \text{et} \quad \tilde{\Gamma} = \mathbf{Z}\tilde{\gamma}_1 + \ldots + \mathbf{Z}\tilde{\gamma}_{\ell}.$$

On définit $S > 0$ par

$$S^{\nu} = T^{\eta},$$

et on suppose que T_0 a été choisi suffisamment grand pour que l'on ait, avec les notations du § 4, $S \geqslant S_0$.

Enfin on désigne par $\omega(\tilde{\Gamma}(S), G)$ le plus petit des degrés des hypersurfaces de $\mathbf{P}_N$ qui contiennent $\tilde{\Gamma}(S)$ mais qui ne contiennent pas G.

LEMME 5.1. *On suppose que pour tout $T > T_0$ et tout $(\tilde{\theta}_1, \ldots, \tilde{\theta}_t) \in \mathbf{C}^t$ vérifiant* (2.1), *on a*

$$\omega(\tilde{\Gamma}(S), G) > c_0^{-1} S^{\mu}. \tag{5.2}$$

Alors $J(\theta_1, \ldots, \theta_t) \geqslant \eta$.

Démonstration. Fixons $T > T_0$ et $(\tilde{\theta}_1, \ldots, \tilde{\theta}_t) \in \mathbf{C}^t$ vérifiant (2.1). Il s'agit de construire un polynôme $Q \in \mathbf{Z}[X_1, \ldots, X_t]$ vérifiant $t(Q) \leqslant T$ et

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

La proposition 4.1 fournit un polynôme homogène $P \in \mathbf{Z}[X_0, \ldots, X_N]$ de degré majoré par $D = c_0^{-1} S^{\mu}$, non partout nul sur G. L'hypothèse (5.2) montre qu'il existe $\tilde{\gamma} \in \tilde{\Gamma}(S)$ tel que $P(\tilde{\gamma})$ ne soit pas nul. On écrit

$$\tilde{\gamma} = \sum_{j=1}^{\ell} h_j \tilde{\gamma}_j, \quad \text{avec } (h_1, \ldots, h_{\ell}) \in \mathbf{Z}^{\ell}(S),$$

et on pose

$$\tilde{y} = \sum_{j=1}^{\ell} h_j \tilde{y}_j.$$

Alors $\tilde{y} \in \mathscr{E}(S)$, donc

$$|E(\tilde{y})| < \exp(-(2-5c_0^{-1})S^{\nu}).$$

Soit i un entier, $0 \leqslant i \leqslant N$, tel que $|F_i(\tilde{y})|$ soit maximal. Pour simplifier les notations on va supposer $i=0$. La construction de $F_0, \ldots, F_N$ (cf. [S]) et les propriétés des fonctions thêta permettent facilement de vérifier

$$|F_0(\tilde{y})| > \exp(-c_0 S^{\varrho}).$$

Soit D° le degré exact de P. En divisant $E(\tilde{y})$ par $F_0(\tilde{y})^{D^{\circ}}$, on trouve

$$0 < |P(1, F_1/F_0, \ldots, F_N/F_0)(\tilde{y})| < \exp(-(2-6c_0^{-1})S^{\nu}).$$

On utilise maintenant le lemme 7 de Bertrand dans [Be1] : le point $\tilde{y}$ admet des coordonnées projectives $(u_0, \ldots, u_N)$ qui sont des polynômes, à coefficients entiers dans un corps de nombres $K_0 \subset K \cap \bar{\mathbf{Q}}$, en les $F_i(\tilde{y}_j)$, $(0 \leqslant i \leqslant N,\ 1 \leqslant j \leqslant \ell)$, de degrés $\leqslant c_0^{1/2} S^{\varrho}$, dont les coefficients ont une hauteur logarithmique absolue $\leqslant c_0^{1/2} S^{\varrho}$. Comme $F_0(\tilde{y}) \neq 0$, on a $u_0 \neq 0$, et

$$0 < |P(1, u_1/u_0, \ldots, u_N/u_0)| < \exp(-(2-6c_0^{-1})S^{\nu}).$$

On majore trivialement $|u_0|$ par $\exp(c_0 S^{\varrho})$, et on trouve

$$0 < |P(u_0, u_1, \ldots, u_N)| < \exp(-(2-7c_0^{-1})S^{\nu}).$$

Enfin $P(u_0, \ldots, u_N)$ est une fraction rationnelle en $\tilde{\theta}_1, \ldots, \tilde{\theta}_{t+1}$ à coefficients dans K_0. On multiplie par un dénominateur (que l'on majore trivialement) : on obtient un polynôme en $\tilde{\theta}_1, \ldots, \tilde{\theta}_{t+1}$ à coefficients entiers dans K_0, dont on prend la norme sur $\mathbf{Q}$ pour obtenir un polynôme à coefficients dans $\mathbf{Z}$ en $\tilde{\theta}_1, \ldots, \tilde{\theta}_{t+1}$. On prend enfin le semi-résultant de ce dernier polynôme avec $B(\tilde{\theta}_1, \ldots, \tilde{\theta}_t, X)$, ce qui donne le polynôme Q cherché.

On raffine maintenant le lemme 5.1 en utilisant l'astuce de Landau-Philippon : l'inégalité finale sur J peut être rendue homogène de poids 1 en d, $\varkappa$, n et de poids 0 en J, μ, ϱ.

LEMME 5.3. *Supposons $J < (d\mu+\varkappa)/n(\mu+\varrho)$. Choisissons η vérifiant*

$$J < \eta < (d\mu+\varkappa)/n(\mu+\varrho),$$

et posons $\nu = \eta(\mu+\varrho)$. Alors il existe un ensemble infini non borné de réels $S>0$ ayant la propriété suivante : il existe $(\tilde{\theta}_1, \ldots, \tilde{\theta}_t) \in \mathbf{C}^t$ avec

$$\max_{1\leqslant\tau\leqslant t}|\tilde{\theta}_\tau-\theta_\tau|<\exp(-2S^\nu), \tag{5.4}$$

tel que, si on définit $\tilde{\theta}_{t+1}$, $\tilde{\gamma}_1,\dots,\tilde{\gamma}_\ell$ *comme précédemment, on ait*

$$\omega(\tilde{\Gamma}(S),G)<c_0^{-1}S^\mu.$$

Démonstration. Soit k un entier $\geqslant 1$ tel que

$$\eta<(k(d\mu+\varkappa)+\mu+\varrho)/(kn+1)(\mu+\varrho).$$

On applique le lemme 5.1 à Y^k, V^k, G^k, en remarquant que

$$\omega(\tilde{\Gamma}^k(S),G^k)=\omega(\tilde{\Gamma}(S),G).$$

§ 6. Fin de la démonstration du théorème principal

Sous les hypothèses du théorème 3.1, le lemme 5.3 donne l'existence de $\tilde{y}_1,\dots,\tilde{y}_\ell$ tels que

$$\omega(\tilde{\Gamma}(S),G)<c_0^{-1}S^\mu.$$

Le lemme de zéros de Masser-Wüstholz, sous la forme raffinée donnée dans [MW2] Chapitre I, montre qu'il existe un sous-groupe algébrique H de G, $H\neq G$, dont on notera d_1 la codimension dans G, $1\leqslant d_1\leqslant d$, défini par des équations de degré $\leqslant S^\mu$, et qu'il existe des éléments $h^{(1)},\dots,h^{(\ell-\ell_1)}$ de $\mathbf{Z}_\pm(S^{\mu d_1/(\ell_1+1)})$, linéairement indépendants sur $\mathbf{Z}$, avec

$$0\leqslant\ell_1\leqslant\ell \quad\text{et}\quad \ell_1/d_1<\mu,$$

tels que

$$\sum_{j=1}^{\ell}h_j^{(s)}\tilde{\gamma}_j\in H(\mathbf{C}) \quad\text{pour } 1\leqslant s\leqslant\ell-\ell_1.$$

On prend alors pour M la partie entière de $S^{d\mu}$, et on choisit $\varepsilon=\nu/d\mu=\eta(\mu+\varrho)/d\mu$.

§ 7. Démonstration du théorème 1.4

Rappelons la définition de l'exposant $\mu(\Gamma,G)$ du lemme de zéros de Masser-Wüstholz [MW1] :

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

où H décrit les sous-groupes algébriques de G, $H \neq G$.

On va démontrer que, sous les hypothèses du théorème 1.4, si $(\theta_1, \ldots, \theta_t)$ est une base de transcendance de K sur $\mathbf{Q}$, on a

$$J(\theta_1, \ldots, \theta_t) \geqslant d\mu(Y)/(n\mu(Y) + d\varrho - \varkappa). \tag{7.1}$$

Le théorème 1.4 résulte de cette inégalité, grâce au théorème 2.2.

Notons $J = J(\theta_1, \ldots, \theta_t)$. On peut évidemment supposer $d > nJ$. Montrons d'abord, sous l'hypothèse (1.5) :

$$J \geqslant (d\mu(\Gamma, G) + \varkappa)/n(\mu(\Gamma, G) + \varrho). \tag{7.2}$$

En effet, si $\mu > 0$ est tel que $J < (d\mu + \varkappa)/n(\mu + \varrho)$, le théorème 3.1, combiné avec l'hypothèse (1.5), implique

$$\sum_{j=1}^{\ell} h_j^{(s)} \gamma_j \in H(\mathbf{C}) \quad \text{pour } 1 \leqslant s \leqslant \ell - \ell_1,$$

donc

$$\mu(\Gamma, G) \leqslant \ell_1/d_1 < \mu,$$

ce qui démontre (7.2).

On en déduit :

$$\textit{si } \mu(\Gamma, G) = \ell/d, \textit{ alors } J \geqslant d(\ell + \varkappa)/n(\ell + d\varrho). \tag{7.3}$$

Comme $\mu(Y) \leqslant (\ell + \varkappa)/n$ et $\varkappa \leqslant n\varrho < d\varrho$, l'inégalité (7.1) est démontrée dans le cas où $\mu(\Gamma, G) = \ell/d$.

De (7.2), grâce à l'inégalité $m \leqslant \ell + \varkappa$, on déduit aussi :

$$\textit{si } \mu(\Gamma, G) = \ell/d, \textit{ alors } J \geqslant dm/n(\ell + d\varrho). \tag{7.4}$$

Supposons maintenant $\mu(\Gamma, G) < \ell/d$. On écrit la définition de $\mu(\Gamma, G)$:

$$\mu(\Gamma, G) = \ell_1/d_1, \quad d_1 = \dim G/H, \quad \ell_1 = \mathrm{rg}_{\mathbf{Z}} \Gamma/\Gamma \cap H,$$

avec

$$1 \leqslant d_1 \leqslant d, \quad 0 \leqslant \ell_1 \leqslant \ell, \quad \ell_1/d_1 < \ell/d.$$

On en déduit $\ell_1 < \ell$, puis $d_1 < d$. Notons

$$V_1 = V \cap T_H(\mathbf{C}), \quad n_1 = \dim_{\mathbf{C}} V/V_1.$$

Comme $\exp_G V$ est dense dans $G(\mathbf{C})$, V n'est pas contenu dans $T_H(\mathbf{C})$, et on a $1 \leqslant n_1 \leqslant n$. Enfin on pose

$$Y_1 = Y/Y \cap V_1, \quad m_1 = \mathrm{rg}_{\mathbf{Z}} Y_1.$$

Ainsi

$$\mu(Y, V) \leqslant m_1/n_1.$$

L'isomorphisme $T_G/T_H \simeq T_{G/H}$ permet de considérer V/V_1 comme un sous-espace vectoriel de $T_{G/H}(\mathbf{C})$, et le sous-groupe Y_1 de V/V_1 vérifie l'hypothèse analogue à (1.5). Comme

$$\ell_1/d_1 = \mu(\Gamma, G) \leqslant \mu(\Gamma/\Gamma \cap H, G/H) \leqslant \ell_1/d_1,$$

on peut appliquer (7.4) à $Y_1 \subset V/V_1$:

$$J \geqslant d_1 m_1/n_1(\ell_1 + d_1 \varrho_1),$$

avec $\varrho_1 = \varrho(G/H) \leqslant \varrho$. Donc

$$\mu(Y, V) \leqslant m_1/n_1 \leqslant J\left(\frac{\ell_1}{d_1} + \varrho\right).$$

On utilise maintenant (7.2) avec $\mu(\Gamma, G) = \ell_1/d_1$:

$$\ell_1/d_1 \leqslant (Jn\varrho - \varkappa)/(d - nJ),$$

d'où

$$\mu(Y, V) \leqslant J(d\varrho - \varkappa)/(d - nJ),$$

ce qui est l'inégalité (7.1) annoncée.

Remarque. Ces arguments permettent de simplifier considérablement la démonstration du § 4 de [Wa2].

§ 8. Une variante du théorème 1.4

Soit G un groupe algébrique commutatif connexe sur $\mathbf{C}$. Quand V est un sous-espace vectorial de $T_G(\mathbf{C})$ sur $\mathbf{C}$, on définit (cf. [Wa2] § 3) :

$$\mu(V) = \mu(V, G) = \min_H \{\dim H/\dim T_H \cap V\},$$

quand H décrit les sous-groupes algébriques de G tels que $T_H \cap V \neq 0$.

Du théorème 1.4 on déduit évidemment, quand $\mu(Y)+\varrho\mu(V)\neq 0$:

$$t+1 \geqslant \mu(Y)\mu(V)/(\mu(Y)+\varrho\mu(V)).$$

COROLLAIRE 8.1. *Sous les hypothèses du théorème* 1.4, *on a*

$$t+1 \geqslant m\mu(V)/(m+\varrho n\mu(V)).$$

Démonstration. On va montrer, plus précisément, que si $(\theta_1, \ldots, \theta_t)$ est une base de transcendance de K sur $\mathbf{Q}$, et si $J=J(\theta_1, \ldots, \theta_t)$, on a

$$(m-n\varrho J)\mu(V) \leqslant mJ. \tag{8.2}$$

On peut donc supposer $m>n\varrho J$. D'après (7.1), on a

$$(d-nJ)\mu(Y) \leqslant J(d\varrho-\varkappa).$$

On distingue deux cas.

(a) Si $\mu(Y)=m/n$, alors on a

$$(d-nJ)m \leqslant nJ(d\varrho-\varkappa),$$

donc

$$\mu(V) \leqslant d/n \leqslant J(m-\varkappa)/(m-n\varrho J),$$

ce qui démontre (8.2) dans ce cas.

(b) Supposons $\mu(Y)<m/n$. On utilise le lemme 3.2 de [Wa2] : il existe un suos-espace vectoriel V' de V, de dimension $n'<n$, tel que si on pose $Y'=Y\cap V'$ et $m'=\mathrm{rg}_{\mathbf{Z}} Y'$, on ait $\mu(Y', V')=m'/n'>m/n$. Alors on a $\varrho J<m/n<m'/n'$. On utilise le cas (a) pour $Y'\subset V'$:

$$\mu(V') \leqslant Jm'/(m'-n'\varrho J) < Jm/(m-n\varrho J).$$

Mais $V\subset V'$, donc $\mu(V')\geqslant\mu(V)$, et (8.2) en résulte.

§ 9. Groupes algébriques définis sur une extension transcendante

La méthode que nous avons présentée permet de travailler avec un groupe algébrique G défini sur K. Voici ce que deviennent les petites perturbations (§ 5) quand on ne suppose plus que G est défini sur $\bar{\mathbf{Q}}$.

On choisit encore $c_0>0$ suffisamment grand, puis T_0 beaucoup plus grand. Soit $T>T_0$, et soit $(\tilde\theta_1,\dots,\tilde\theta_t)\in\mathbf{C}^t$ vérifiant (2.1). On construit $\tilde\theta_{t+1}$ comme au § 5.

Le groupe algébrique G est défini sur le corps $K=\mathbf{Q}(\theta_1,\dots,\theta_{t+1})$. Pour $\max_{1\leqslant\tau\leqslant t+1}|\tilde\theta_\tau-\theta_\tau|$ suffisamment petit (ce qui est assuré par le choix de c_0 suffisamment grand), on peut déformer G en un groupe algébrique $\tilde G$ défini sur le corps $\tilde K=\mathbf{Q}(\tilde\theta_1,\dots,\tilde\theta_{t+1})$. Il suffit, par exemple, d'écrire dans les espace projectifs correspondants des équations de $\tilde G$, de $\tilde G-G$, et du graphe de $\tilde G\times G\to\tilde G$, et d'y substituer $(\tilde\theta_1,\dots,\tilde\theta_{t+1})$ à $(\theta_1,\dots,\theta_{t+1})$. Alors les points $\tilde\gamma_1,\dots,\tilde\gamma_\ell$ de $\mathbf{P}_N(\mathbf{C})$ construits comme au § 5 appartiennent à $\tilde G(\tilde K)$.

Nous explicitons cette construction au § 10, et nous démontrons au § 11 le résultat suivant :

THÉORÈME 9.1. *Soit $\mu>0$. Supposons*

$$J(\theta_1,\dots,\theta_t)<(d\mu+\varkappa)/n(\mu+\varrho).$$

Choisissons η vérifiant

$$J(\theta_1,\dots,\theta_t)<\eta<(d\mu+\varkappa)/n(\mu+\varrho),$$

et posons $v=\eta(\mu+\varrho)$. Alors il existe un ensemble infini non borné de réels $S>0$ ayant la propriété suivante : il existe $(\tilde\theta_1,\dots,\tilde\theta_t)\in\mathbf{C}^t$ vérifiant (5.4) *tels que, si on définit $\tilde\theta_{t+1}$, $\tilde\gamma_1,\dots,\tilde\gamma_\ell$ comme précédemment, on ait*

$$\omega(\tilde\Gamma(S),\tilde G)<c_0^{-1}S^\mu.$$

En utilisant de nouveau le chapitre I de [MW2], on en déduit, comme au § 6, qu'il existe un sous-groupe algébrique H_1 de $\tilde G$, de dimension $\leqslant d-d_1$, défini par des équations de degré $\leqslant S^\mu$, et il existe aussi des éléments $h^{(1)},\dots,h^{(\ell-\ell_1)}$ de $\mathbf{Z}^\ell_\pm(S^{d\mu})$, linéairement indépendants sur $\mathbf{Z}$, avec

$$0\leqslant\ell_1\leqslant\ell,\quad 1\leqslant d_1\leqslant d,\quad \ell_1/d_1<\mu,$$

tels que

$$\sum_{j=1}^{\ell}h_j^{(s)}\tilde\gamma_j\in H_1(\mathbf{C})\quad\text{pour } 1\leqslant s\leqslant\ell-\ell_1.$$

La difficulté vient ensuite, quand il s'agit d'en déduire un énoncé dans le style des théorèmes 1.4 et 8.1. En effet, il peut exister des sous-groupes algébriques H_1 de $\tilde G$ qui ne sont pas de la forme $\tilde H$, c'est-à-dire qui ne proviennent pas par déformation d'un

sous-groupe algébrique H de G. Cela arrive, par exemple, quand G est une puissance d'une courbe elliptique E d'invariant modulaire $j=j(E)$ transcendant : on peut approcher j par des nombres $\tilde{j}=j(\tilde{E})$, où $\tilde{E}$ est une courbe elliptique ayant des multiplications complexes. Il semble inévitable d'introduire à ce moment une hypothèse supplémentaire; par exemple, dans le cas $G=E^d$, en notant $\tau=\omega_2/\omega_1$ le quotient de deux périodes fondamentales de E (de sorte que $j=j(\tau)$), on suppose :

(9.2) *Pour tout $\varepsilon>0$, il existe $H_0>0$ tel que pour tout $H>H_0$ et pour tout nombre imaginaire quadratique β de hauteur $\leqslant H$, on ait*

$$|\tau-\beta|>\exp(-H^{\varepsilon}).$$

Bien entendu, on espère que les inégalités (1.2) et (1.3) sont encore vraies sans aucune hypothèse technique de la forme (1.5) ou (9.2).

§ 10. Déformation d'un groupe algébrique

Soit G un groupe algébrique commutatif défini sur une extension K de $\mathbf{Q}$ de type fini. On remplace K par un sous-corps $\tilde{K}$ de $\mathbf{C}$ (obtenu en perturbant un système générateur de K sur $\mathbf{Q}$) et on construit un groupe algébrique commutatif $\tilde{G}$ défini sur $\tilde{K}$.

Comme cette section est indépendante de celles qui précèdent nous rappelons les notations. Soit K un sous-corps de $\mathbf{C}$ de type fini sur $\mathbf{Q}$. On choisit une base de trancendance $(\theta_1,\ldots,\theta_t)$ de K sur $\mathbf{Q}$, et un élément θ_{t+1} de K tel que $K=\mathbf{Q}(\theta_1,\ldots,\theta_{t+1})$. Nous allons construire un ouvert de Zariski Ω de $\mathbf{A}_t$; pour chaque $(\tilde{\theta}_1,\ldots,\tilde{\theta}_t)$ dans $\Omega(\mathbf{C})$, nous considérerons l'un quelconque des homomorphismes, que nous noterons $u\to\tilde{u}$, de $\mathbf{Q}[\theta_1,\ldots,\theta_{t+1}]$ dans $\mathbf{C}$, qui envoie θ_i sur $\tilde{\theta}_i$ $(1\leqslant i\leqslant t)$.

Soit $P\in\mathbf{P}_N(K)$. S'il existe un système de coordonnées projectives $(u_0,\ldots,u_N)$ de P avec $u_\nu\in\mathbf{Q}[\theta_1,\ldots,\theta_{t+1}]$, $(0\leqslant\nu\leqslant N)$, tel que $\tilde{u}_0,\ldots,\tilde{u}_N$ ne soient pas tous nuls, alors on désigne par $\tilde{P}$ le point de $\mathbf{P}_N(\tilde{K})$ de coordonnées projectives $(\tilde{u}_0,\ldots,\tilde{u}_N)$. L'ensemble des P vérifiant cette hypothèse sera noté $\mathscr{A}$ (points admissibles).

Soit G un groupe algébrique commutatif de dimension d, défini sur K, plongé comme sous-variété quasi-projective définie sur K dans P_N. Nous allons démontrer l'existence de Ω tel que l'énoncé suivant soit valide.

PROPOSITION 10.1. *Il existe un groupe algébrique commutatif $\tilde{G}$ défini sur $\tilde{K}$ et plongé dans $\mathbf{P}_N$, de dimension d, tel que*

(a) *l'ensemble H des $P\in G(K)\cap\mathscr{A}$ vérifiant $\tilde{P}\in\tilde{G}(\tilde{K})$ soit un sous-groupe de $G(K)$,*

(b) *l'application $P\mapsto\tilde{P}$ définisse un homomorphisme de H dans $\tilde{G}(\tilde{K})$.*

Si on fixe un ensemble fini $\{P_1, \ldots, P_\ell\}$ de points de $G(K)$, alors on peut choisir Ω de telle sorte que $P_j \in H$ pour $1 \leqslant j \leqslant \ell$, et alors $\mathbf{Z}P_1 + \ldots + \mathbf{Z}P_\ell \subseteq H$.

La construction qui suit ne fera intervenir qu'un nombre fini de sous-ensembles algébriques de $\mathbf{P}_N$ ou de $\mathbf{P}_N \times \mathbf{P}_N$, donc un nombre fini d'idéaux, tous définis sur K. Pour chacun de ces idéaux, nous disposerons d'un ou de plusieurs systèmes générateurs, mais nous ne travaillerons qu'avec un nombre fini de polynômes à coefficients dans K, et l'ouvert Ω en dépendra. Cela restera sous-entendu dans la suite.

Quand A est un polynôme à coefficients dans K, nous noterons $\tilde{A}$ le polynôme à coefficients dans $\tilde{K}$ obtenu en substituant $(\tilde{\theta}_1, \ldots, \tilde{\theta}_{t+1})$ à $(\theta_1, \ldots, \theta_{t+1})$. Quand $\mathscr{I}$ est un idéal homogène de $\mathbf{C}[X_0, \ldots, X_N]$ défini sur K, ayant un système générateur $A_1, \ldots, A_h$ à coefficients dans K, $\tilde{\mathscr{I}}$ désignera l'idéal de $\mathbf{C}[X_0, \ldots, X_N]$, défini sur $\tilde{K}$, engendré par $\tilde{A}_1, \ldots, \tilde{A}_h$. Si $F = Z(\mathscr{I})$ est le fermé de $\mathbf{P}_N$ associé à $\mathscr{I}$, nous noterons $\tilde{F} = Z(\tilde{\mathscr{I}})$. Si U est le complémentaire de F dans $\mathbf{P}_N$, $\tilde{U}$ désignera le complémentaire de $\tilde{F}$. Enfin, pour F fermé et U ouvert dans $\mathbf{P}_N$, et pour $V = F \cap U$, on peut définir $\tilde{V} = \tilde{F} \cap \tilde{U}$, et on vérifie que l'on a $(V_1 \cap V_2)^{\sim} = \tilde{V}_1 \cap \tilde{V}_2$; de plus, si $V_1 \subseteq V_2$, alors $\tilde{V}_1 \subseteq \tilde{V}_2$.

On effectue la même construction pour les polynômes bi-homogènes de $K[X_0, \ldots, X_N, Y_0, \ldots, Y_N]$, et les sous-variétés quasi-projectives de $\mathbf{P}_N \times \mathbf{P}_N$ définies sur K. Par exemple, si V_1 et V_2 sont deux sous-variétés quasi-projectives de $\mathbf{P}_N$ définies sur K, alors $(V_1 \times V_2)^{\sim} = \tilde{V}_1 \times \tilde{V}_2$.

Soient V_1 et V_2 deux sous-variétés quasi-projectives de $\mathbf{P}_N$ définies sur K, et $\varphi: V_1 \to V_2$ un morphisme défini sur K. On écrit un recouvrement de V_1 par une famille finie d'ouverts U_i, avec pour chaque i, $N+1$ polynômes homogènes $(A_0^{(i)}, \ldots, A_N^{(i)})$ de $K[X_0, \ldots, X_N]$, donnant φ sur U_i. Alors $(\tilde{U}_i)$ est un recouvrement ouvert de $\tilde{V}_1$, et les polynômes $(\tilde{A}_0^{(i)}, \ldots, \tilde{A}_N^{(i)})$ définissent un morphisme $\tilde{\varphi}: \tilde{V}_1 \to \tilde{V}_2$. On procède de même quand V_1 est une sous-variété quasi-projective de $\mathbf{P}_N \times \mathbf{P}_N$ définie sur K.

Notons alors 0 l'élément neutre de $G(K)$. On choisit Ω de telle sorte que $0 \in \mathscr{A}$ et que $\tilde{0} \in \tilde{G}(\tilde{K})$. La loi de G est définie par un morphisme ψ de $G \times G$ dans G qui envoie (x, y) sur $x - y$. Alors le morphisme $\tilde{\psi}: \tilde{G} \times \tilde{G} \to \tilde{G}$ munit $\tilde{G}$ d'une structure de groupe algébrique commutatif défini sur $\tilde{K}$.

On peut noter que si ψ se prolonge en un morphisme de $G \times \tilde{G}$ dans $\tilde{G}$ (cf. [S]), alors $\tilde{\psi}$ se prolonge en un morphisme de $\tilde{G} \times \tilde{\tilde{G}}$ dans $\tilde{\tilde{G}}$ (où $\tilde{\tilde{G}}$ est l'adhérence de Zariski de G dans $\mathbf{P}_N$, et $\tilde{\tilde{G}} = \tilde{\tilde{G}}$ celle de $\tilde{G}$). De même, si G est une variété abélienne, alors $\tilde{G}$ est une variété abélienne. Evidemment, si G est une variété linéaire, alors $\tilde{G}$ est une variété linéaire isomorphe à G sur $\mathbf{C}$ (si $G_1 \simeq G_2$, alors $\tilde{G}_1 \simeq \tilde{G}_2$).

Démonstration de la proposition 10.1. Soient P et Q dans H. Comme $\tilde{G}(\tilde{K})$ est un

groupe qui contient $\tilde{P}$ et $\tilde{Q}$, il contient aussi $\tilde{P}-\tilde{Q}$. Grâce à $\tilde{\psi}$, on écrit des coordonnées projectives de $\tilde{P}-\tilde{Q}$, et on en déduit $P-Q\in\mathscr{A}$ et $\tilde{P}-\tilde{Q}=(P-Q)^{\sim}$.

Il reste à vérifier $\dim\tilde{G}=\dim G$. En spécialisant des relations de dépendance algébrique entre des fonctions sur G, on trouve immédiatement $\dim\tilde{G}\leqslant\dim G$. D'autre part la méthode de Hermann (cf. [MW2] proposition du § 4.3) permet de vérifier que si des polynômes homogènes $A_1,\ldots,A_d$ de $K[X_0,\ldots,X_N]$ sont C-linéairement indépendants dans $\mathbf{C}[X_0,\ldots,X_N]/\mathscr{I}$, où $\mathscr{I}$ est un idéal homogène défini sur K, alors $\tilde{A}_1,\ldots,\tilde{A}_d$ sont C-linéairement indépendants dans $\mathbf{C}[X_0,\ldots,X_N]/\tilde{\mathscr{I}}$. En écrivant que $\dim G$ est la dimension de l'anneau local de G en 0, on en déduit $\dim\tilde{G}=\dim G$.

M. J. Brown m'a fait remarquer que cette égalité $\dim\tilde{G}=\dim G$ peut aussi s'obtenir en considérant le morphisme

$$\operatorname{Proj}\mathbf{Q}[\theta_1,\ldots,\theta_{t+1},X_0,\ldots,X_N]/\mathscr{I}\to\operatorname{Spec}\mathbf{Q}[\theta_1,\ldots,\theta_{t+1}],$$

où $\mathscr{I}$ engendre l'idéal de $\tilde{G}$ dans $\mathbf{C}[X_0,\ldots,X_N]$. La dimension des fibres est constante sur un ouvert de Zariski.

Ceci termine la démonstration de la proposition 10.1. Une autre démonstration, reposant sur les arguments de EGA 4, est présentée par J. Fresnel en appendice.

§ 11. Démonstration du théorème 9.1

La démonstration du théorème 9.1 est une variante de celle du lemme 5.1. Nous indiquons seulement les points principaux pour préciser le passage de G à $\tilde{G}$. La plus grande partie de la démonstration va s'effectuer sur G, ce qui évite d'avoir à considérer l'espace tangent de $\tilde{G}$.

Grâce à l'astuce de Landau-Philippon (cf. lemme 5.3), on peut supposer

$$\eta<(d\mu+\mu+\varrho+\varkappa)/(n+1)(\mu+\varrho).$$

On utilise la construction du § 10; comme S est suffisamment grand, on a $(\tilde{\theta}_1,\ldots,\tilde{\theta}_t)\in\Omega$, et $\Gamma\subseteq H$. Supposons que l'on ait

$$\omega(\tilde{\Gamma}(S),\tilde{G})\geqslant c_0^{-1}S^{\mu}. \tag{11.1}$$

Si on numérote les coordonnées de $\mathbf{P}_N$ de telle sorte que les fonctions $X_1/X_0,\ldots,X_d/X_0$ soient algébriquement indépendantes sur G, alors ces fonctions sont aussi algébriquement indépendantes sur $\tilde{G}$, et le polynôme P de la proposition 4.1 peut être construit de telle sorte qu'il ne soit pas partout nul sur $\tilde{G}(\mathbf{C})$.

On déduit de (11.1) qu'il existe $\gamma \in \Gamma(S)$ tel que $P(\tilde{\gamma}) \neq 0$. En reprenant les arguments des § 4 et § 5, ainsi que ceux du lemme 7 de [Be1], on trouve des coordonnées $(v_0, \ldots, v_N)$ de γ dans $\mathbf{P}_N$ telles que

$$|P(v_0, \ldots, v_N)| < \exp(-(2-7c_0^{-1})S^{\nu}),$$

où, pour $0 \leqslant j \leqslant N$, v_j est un élément de $\mathbf{Z}[\theta_1, \ldots, \theta_{t+1}]$ de degré et de hauteur logarithmique $\leqslant c_0^{1/2} S^{\varrho}$. Alors $(\tilde{v}_0, \ldots, \tilde{v}_N)$ est un système de coordonnées projectives de $\tilde{\gamma}$, et on a

$$0 < |P(\tilde{v}_0, \ldots, \tilde{v}_N)| < \exp(-(2-8c_0^{-1})S^{\nu}).$$

La contradiction s'obtient, comme précédemment, en utilisant le critère 2.2 de Philippon.

Complément : les coefficients $J_k(\theta_1, \ldots, \theta_t)$. Voici une méthode plus facile pour traiter le cas où G n'est pas défini sur $\bar{\mathbf{Q}}$; mais elle donne des résultats moins profonds.

Reprenons une base de transcendance $(\theta_1, \ldots, \theta_t)$ de K sur $\bar{\mathbf{Q}}$. Soit k un entier, $0 \leqslant k \leqslant t$. On désigne par $A_k(\theta_1, \ldots, \theta_t)$ l'ensemble des nombres $\eta > 1$ ayant la propriété suivante : il existe $T_0 > 0$ tel que pour tout $T \geqslant T_0$ et tout $(\tilde{\theta}_{k+1}, \ldots, \tilde{\theta}_t) \in \mathbf{C}^{t-k}$ vérifiant

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

il existe un polynôme $P \in \mathbf{Z}[X_1, \ldots, X_t]$ satisfaisant $t(P) \leqslant T$ et

$$0 < |P(\theta_1, \ldots, \theta_k, \tilde{\theta}_{k+1}, \ldots, \tilde{\theta}_t)| < \exp(-T^{\eta}).$$

On note ensuite $J_k(\theta_1, \ldots, \theta_t)$ la borne supérieure de cet ensemble s'il est non vide, avec $J_k(\theta_1, \ldots, \theta_t) = 1$ s'il est vide.

Ainsi $J_0(\theta_1, \ldots, \theta_t) = J(\theta_1, \ldots, \theta_t)$ (cf. § 2). Comme

$$A_k(\theta_1, \ldots, \theta_t) \subseteq A_{k+1}(\theta_1, \ldots, \theta_t), \quad (0 \leqslant k < t),$$

on a $J_k(\theta_1, \ldots, \theta_t) \leqslant J_{k+1}(\theta_1, \ldots, \theta_t)$. Du théorème de [WZ] on déduit :

$$J_1(\theta_1, \ldots, \theta_t) \leqslant 2^t.$$

Il peut arriver que $J_2(\theta_1, \ldots, \theta_t)$ soit infini. Mais, si K a un type de transcendance $\leqslant \tau$ (cf. [Br]), alors $J_t(\theta_1, \ldots, \theta_t) \leqslant \tau$.

Dans la situation décrite au § 1, il est facile d'établir, sans aucune hypothèse technique :

$$\text{si } d\mu(Y) > n\mu(Y)+d\varrho-\varkappa, \text{ alors } J_t(\theta_1, \ldots, \theta_t) > d\mu(Y)/(n\mu(Y)+d\varrho-\varkappa). \quad (11.2)$$

D'autre part, sous l'hypothèse (1.5), la méthode des § 4 à 7 permet d'obtenir

(11.3) *Supposons le groupe algébrique G défini sur un sous-corps K' de K; notons t' le degré de transcendance de K' sur* **Q**, *et choisissons une base de transcendance* $(\theta_1, \ldots, \theta_t)$ *de K sur* **Q** *de telle sorte que* $(\theta_1, \ldots, \theta_{t'})$ *soit une base de transcendance de K' sur* **Q**. *Alors*

$$J_{t'}(\theta_1, \ldots, \theta_t) \geqslant d\mu(Y)/(n\mu(Y)+d\varrho-\varkappa).$$

En particulier si $t' \leqslant 1$ on trouve

$$2^t \geqslant d\mu(Y)/(n\mu(Y)+d\varrho-\varkappa).$$

§ 12. Indépendance algébrique de valeurs de la fonction exponentielle

(a) *Exponentielles en plusieurs variables.* Soient $X=\mathbf{Z}x_1+\ldots+\mathbf{Z}x_d$ et $Y=\mathbf{Z}y_1+\ldots+\mathbf{Z}y_m$ deux sous-groupes de $\mathbf{C}^n$ vérifiant l'hypothèse suivante :

(12.1) Pour tout $\varepsilon>0$, il existe $H_0>0$ tel que pour tout $H>H_0$, tout $(\lambda_1, \ldots, \lambda_d) \in \mathbf{Z}^d_{\pm}(H)$ et tout $(h_1, \ldots, h_m) \in \mathbf{Z}^m_{\pm}(H)$ vérifiant

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

on ait

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

On note $\mu(X) = \mu(X, \mathbf{C}^n)$ et $\mu(Y)=\mu(Y, \mathbf{C}^n)$.

COROLLAIRE 12.2. *Soit t le degré de transcendance sur* **Q** *du corps engendré par les dm nombres*

$$\exp\langle x_i, y_j\rangle, \quad (1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant m).$$

Alors

$$t+1 \geqslant d\mu(Y)/(n\mu(Y)+d) \quad \text{et} \quad t+1 \geqslant m\mu(X)/(n\mu(X)+m).$$

On peut mettre la conclusion sous la forme symétrique (mais en fait équivalente) :

$$t+1 \geqslant \mu(X)\mu(Y)/(\mu(X)+\mu(Y)) \quad \text{si } \mu(X)+\mu(Y) \neq 0. \quad (12.3)$$

Ce résultat améliore le théorème 1.2 de [Wa3] où $t+1$ était remplacé par 2^t. On peut donc aussi remplacer 2^{t+1} par $2(t+1)$ dans le corollaire 1.3 de [Wa3]. L'amélioration provient uniquement du critère de Philippon [P4] qui a remplacé 2^t par $t+1$ dans le critère utilisé dans [Wa3].

D'autre part, pour $n=1$, on a $\mu(X)=\mathrm{rg}_{\mathbf{Z}} X$ et $\mu(Y)=\mathrm{rg}_{\mathbf{Z}} Y$, et on retrouve un énoncé de Philippon dans [P4].

(b) *A propos de la conjecture de Gel'fond-Schneider.* On peut déduire aussi du théorème 3.1 le résultat suivant, dû à Philippon [P4] :

COROLLAIRE 12.4. *Soient α et β deux nombres algébriques, avec $\alpha\neq 0$; on choisit une détermination non nulle $\log\alpha$ du logarithme de α. Soit d le degré de β sur $\mathbf{Q}$. Si k est un entier tel que $d\geqslant 2k$, alors parmi les $d-1$ nombres*

$$\alpha^{\beta}, \ldots, \alpha^{\beta^{d-1}},$$

il y en a au moins k algébriquement indépendants.

(c) *Démonstrations.* Pour démontrer le corollaire 12.2, on se ramène au cas particulier $\mu(X)=d/n$ et $\mu(Y)=m/n$, grâce au lemme suivant (cf. [Wa3], début du § 4) :

LEMME 12.5. *Soient X et Y deux sous-groupes de type fini de $\mathbf{C}^n$, de rangs d et m respectivement. Il existe un entier positif $n'\leqslant n$ et deux sous-groupes X' et Y' de $\mathbf{C}^{n'}$, de rangs d' et m' respectivement, tels que*

$$\mu(X', \mathbf{C}^{n'}) = d'/n' \geqslant d/n, \quad \mu(Y', \mathbf{C}^{n'}) = m'/n' \geqslant \mu(Y, \mathbf{C}^n),$$

et

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

Ce lemme 12.5 montre aussi que l'inégalité (12.3) est équivalente à chacune des inégalités de la conclusion du corollaire 12.2.

L'hypothèse (12.1) permet ensuite d'utiliser le théorème 3.1, grâce à la description des sous-groupes algébriques de $\mathbf{G}_m^d$ à l'aide de déterminants de Vandermonde.

Comme le même type d'arguments interviendra dans le cas elliptique, nous omettons les détails.

Le corollaire 12.4 se déduit de même soit du théorème 1.4, soit du théorème 3.1, en utilisant le groupe algébrique $\mathbf{G}_a\times\mathbf{G}_m^d$, et en remarquant que l'inégalité $t+1\geqslant d(d+1)/(2d+1)$ implique $t+1>d/2\geqslant k$, donc $t\geqslant k$.

D'autre part, au lieu d'utiliser le théorème 1.4, on peut aussi utiliser le théorème 8.1. En effet, si, pour $G=\mathbf{G}_m^d$, on identifie $T_G(\mathbf{C})$ à $\mathbf{C}^d$ par $\exp_G(z_1,\ldots,z_d)=(e^{z_1},\ldots,e^{z_d})$, alors quand V est un sous-espace vectoriel de $\mathbf{C}^d$ de dimension n sur $\mathbf{C}$, avec une base $x^{(1)},\ldots,x^{(n)}$, où $x^{(\nu)}=(x_{1\nu},\ldots,x_{d\nu})$, $(1\leqslant\nu\leqslant n)$, on a $\mu(V,\mathbf{G}_m^d)=\mu(X,\mathbf{C}^n)$, où $X=\mathbf{Z}x_1+\ldots+\mathbf{Z}x_d$, et $x_i=(x_{i1},\ldots,x_{in})$, $1\leqslant i\leqslant d$.

§ 13. Indépendance algébrique de valeurs de fonctions elliptiques

(a) *Généralisation d'un résultat de Masser et Wüstholz.* Pour commencer on prend une seule fonction elliptique $\wp$ de Weierstrass, d'invariants g_2, g_3. Soient $X=\mathbf{Z}x_1+\ldots+\mathbf{Z}x_d$ et $Y=\mathbf{Z}y_1+\ldots+\mathbf{Z}y_m$ deux sous-groupes de $\mathbf{C}^n$, de rangs d et m respectivement, vérifiant l'hypothèse (12.1). On désigne par t le degré de transcendance sur $\mathbf{Q}$ du corps obtenu en adjoignant à $\mathbf{Q}(g_2,g_3)$ les valeurs de $\wp$ aux points $\langle x_i,y_j\rangle$ $(1\leqslant i\leqslant d,\ 1\leqslant j\leqslant m)$ qui ne sont pas pôles de $\wp$. Enfin on note $\mathcal{O}$ l'anneau des endomorphismes de la courbe elliptique E associée à $\wp$, et $j(E)$ son invariant modulaire.

COROLLAIRE 13.1. *Si $\mathcal{O}=\mathbf{Z}$ et si $j(E)$ est algébrique, alors*

$$t+1\geqslant d\mu(Y)/(n\mu(Y)+2d) \quad \textit{et} \quad t+1\geqslant m\mu(X)/(m+2n\mu(X)).$$

Donc

$$t+1\geqslant \mu(X)\mu(Y)/(2\mu(X)+\mu(Y)) \quad \text{si } \mu(X)+\mu(Y)\neq 0.$$

Dans le cas $n=1$, la conclusion s'écrit

$$t+1\geqslant md/(m+2d),$$

alors que le résultat principal de [MW2] donnait seulement

$$2^{t+2}(t+8)\geqslant md/(m+2d).$$

Pour reprendre l'exemple de [MW2] p. 408, on en déduit que si $\wp$ a des invariants g_2, g_3 algébriques et n'a pas de multiplication complexe, pour N et k entiers vérifiant $N\geqslant(3+2\sqrt{2})k$, au moins k des N nombres

$$\wp(e),\wp(e^2),\ldots,\wp(e^N)$$

sont définis et algébriquement indépendants sur $\mathbf{Q}$. Comme dans [MW2], on peut remplacer e par π ou par tout nombre transcendant vérifiant la condition assez faible (mesure de transcendance) indiquée p. 408 de [MW2].

Le théorème 7.1 de [Wa3] montre que, si $j(E)$ est transcendant, on a

$$2^t \geqslant \mu(X)\mu(Y)/(2\mu(X)+\mu(Y)) \quad \text{si } \mu(X)+\mu(Y) \neq 0. \tag{13.2}$$

On peut améliorer cette inégalité en ajoutant une petite hypothèse.

COROLLAIRE 13.3. *Si $j(E)$ est transcendant, et si le quotient $\tau=\omega_2/\omega_1$ de deux périodes fondamentales de $\wp$ vérifie l'hypothèse* (9.2), *alors*

$$t+1 \geqslant d\mu(Y)/(n\mu(Y)+2d) \quad et \quad t+1 \geqslant m\mu(X)/(m+2n\mu(X)).$$

Enfin l'énoncé 13.1 admet une variante quand $\mathcal{O} \neq \mathbf{Z}$, c'est-à-dire quand E admet des multiplications complexes. On remplace le $\mathbf{Z}$-module $X=\mathbf{Z}x_1+\ldots+\mathbf{Z}x_d$ par un $\mathcal{O}$-module $X=\mathcal{O}x_1+\ldots+\mathcal{O}x_d$, et on remplace l'exposant de Dirichlet $\mu(X)$ par le nombre

$$\min_W \{(\mathrm{rg}_{\mathcal{O}} X/X\cap W)/\dim_{\mathbf{C}} \mathbf{C}^n/W\},$$

où W décrit les sous-espaces vectoriels de $\mathbf{C}^n$ sur $\mathbf{C}$, avec $W \neq \mathbf{C}^n$, et $\mathrm{rg}_{\mathcal{O}} X/X\cap W$ est le rang du $\mathcal{O}$-module quotient $X/X\cap W$. On modifie l'hypothèse (12.1) de façon évidente.

Par exemple, quand $\wp$ est une fonction de Weierstrass associée à une courbe elliptique ayant des endomorphismes non triviaux, avec g_2 et g_3 algébriques, pour N et k entiers vérifiant $N \geqslant 4k$, parmi les N nombres

$$\wp(e), \ldots, \wp(e^N),$$

au moins k sont définis et algébriquement indépendants.

(b) *Analogue elliptique de la conjecture de Gel'fond-Schneider.* Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, $\mathcal{O}$ l'anneau des endomorphismes de la courbe elliptique E associée à $\wp$, K le corps des fractions de $\mathcal{O}$ (c'est le corps des endomorphismes de E), et β un nombre algébrique de degré d sur K.

Le théorème 3.1 permet de donner une nouvelle démonstration du résultat suivant, dû encore une fois à Philippon [P2, P4] :

COROLLAIRE 13.4. *Soit u un nombre complexe tel que $\wp$ soit définie aux points u, $\beta u, \ldots, \beta^{d-1}u$. Soit k un entier positif. On suppose*

$$\begin{cases} d \geqslant 3k & si\ \mathcal{O}=\mathbf{Z} \\ d \geqslant 2k & si\ \mathcal{O} \neq \mathbf{Z}. \end{cases}$$

Alors parmi les d nombres

$$\wp(u), \wp(\beta u), \ldots, \wp(\beta^{d-1}u),$$

il y en a au moins k algébriquement indépendants.

On obtient aussi :

COROLLAIRE 13.5. *Soient $u_1, \ldots, u_h$ des nombres complexes linéairement indépendants sur $K(\beta)$, et vérifiant la mesure d'indépendance linéaire suivante : pour tout $\varepsilon>0$, il existe $H_0>0$ tel que, pour tout $H>H_0$ et pour tout élément non nul $a \in \mathcal{O}^{dh}$, dont les composantes a_{ij} $(0\leqslant i\leqslant d-1,\ 1\leqslant j\leqslant h)$ ont toutes une hauteur majorée par H, on a*

$$\left|\sum_{i=0}^{d-1}\sum_{j=1}^{h} a_{ij}\beta^i u_j\right| > \exp(-H^{\varepsilon}).$$

Soit k un entier tel que

$$\begin{cases} hd > (h+2)k & \text{si } \mathcal{O} = \mathbf{Z} \\ hd > (h+1)k & \text{si } \mathcal{O} \neq \mathbf{Z}. \end{cases}$$

Alors, parmi les dh nombres

$$\wp(\beta^i u_j), \quad (0\leqslant i\leqslant d-1,\ 1\leqslant j\leqslant h),$$

il y en a au moins k qui sont définis et algébriquement indépendants.

(c) *Indépendance des valeurs de plusieurs fonctions elliptiques.* Soient $\Omega_1, \ldots, \Omega_d$ des réseaux de $\mathbf{C}$ tels que les courbes elliptiques $E_i=\mathbf{C}/\Omega_i$, $(1\leqslant i\leqslant d)$ soient définies sur $\bar{\mathbf{Q}}$ et deux-à-deux non isogènes. On désigne par $\wp_i$ la fonction elliptique de Weierstrass associée à Ω_i. Soient $v_1, \ldots, v_m$ des nombres complexes linéairement indépendants sur $\mathbf{Q}$, vérifiant l'hypothèse suivante :

(13.6) Pour tout $\varepsilon>0$, il existe $M_0>0$ tel que, pour tout $\omega \in \Omega_1 \cup \ldots \cup \Omega_d$ et tout $(h_1, \ldots, h_m) \in \mathbf{Z}^m_{\pm}(M)$ avec $M\geqslant M_0$, si le nombre

$$\xi = \omega - \sum_{j=1}^{m} h_j v_j$$

n'est pas nul, alors

$$|\xi| > \exp(-M^{\varepsilon}).$$

COROLLAIRE 13.7. *Si t désigne le degré de transcendance du corps obtenu en adjoignant à* $\mathbf{Q}$ *les nombres* $\wp_i(v_j)$, *pour les* i, j *avec*

$$1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant m, \quad et \quad v_j \notin \Omega_i,$$

alors

$$t+1 \geqslant md/(m+2d). \tag{13.8}$$

Si, au lieu de l'hypothèse (13.6), on demande seulement une mesure d'indépendance linéaire de $v_1, \ldots, v_m$ (ce qui revient à faire $\omega=0$ dans (13.6)), on trouve

$$t+1 \geqslant (m-2)\,d/(m-2+2d). \tag{13.9}$$

Mais, si $m \geqslant 4d^2$, l'inégalité (13.9) implique (13.8).

(d) *Démonstrations.*

Démonstration du corollaire 13.1. Grâce au lemme 12.5, il n'y a pas de restriction à supposer $\mu(X)=d/n$ et $\mu(Y)=m/n$. Il s'agit alors de démontrer, sous l'hypothèse (12.1),

$$t+1 \geqslant md/n(m+2d).$$

On va d'abord se ramener au cas où les invariants g_2, g_3 sont algébriques. Posons $\Delta=g_2^3-27g_3^2$, et choisissons $c \in \mathbf{C}$ tel que $c^{12}=1/\Delta$. La fonction $\tilde{\wp}(z)=c^2\wp(cz)$ est une fonction elliptique de Weierstrass, d'invariants $\tilde{g}_2=c^4g_2$ et $\tilde{g}_3=c^6g_3$ algébriques. Posons

$$\tilde{x}_i = c^{-1}x_i,\ \tilde{y}_j = y_j, \quad (1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant m).$$

On considère le corps K engendré sur $\mathbf{Q}(g_2, g_3)$ par les valeurs de $\wp$ aux points $\langle x_i, y_j \rangle$, et le corps $\tilde{K}$ engendré sur $\mathbf{Q}(\tilde{g}_2, \tilde{g}_3)$ par les valeurs de $\tilde{\wp}$ aux points $\langle \tilde{x}_i, \tilde{y}_j \rangle$. Alors K et $\tilde{K}$ ont le même degré de transcendance sur $\mathbf{Q}$.

On suppose donc g_2 et g_3 algébriques. On va utiliser le théorème 3.1, en prenant $G=E^d$. Grâce à la fonction $\wp$, on identifie $T_E(\mathbf{C})$ à $\mathbf{C}$, et $T_G(\mathbf{C})$ à $\mathbf{C}^d$. On prend $V=\mathscr{L}(\mathbf{C}^n)$, où $\mathscr{L}: \mathbf{C}^n \to \mathbf{C}^d$ est définie par

$$\mathscr{L}(z) = (\langle x_1, z \rangle, \ldots, \langle x_d, z \rangle) \quad (z \in \mathbf{C}^n).$$

Comme on peut supposer $\mu(X)>2$, on a $V \cap \operatorname{Ker} \exp_G = 0$. Prenons dans le théorème 3.1 : $\mu=m/d$, $\varkappa=0$, $\varrho=2$, $\ell=m$. Supposons $t+1<md/n(m+2d)$. On obtient alors un sous-groupe algébrique H de G, de dimension $\leqslant d-r$, défini par des équations de degré $\leqslant M$, et des éléments $h^{(1)}, \ldots, h^{(k)}$ de $\mathbf{Z}^m_{\pm}(M)$, linéairement indépendants sur $\mathbf{Z}$, avec

$$0 \leqslant k \leqslant m, \quad 1 \leqslant r \leqslant d, \quad (m-k)/r < m/d,$$

et enfin des nombres complexes z_{ij}, $(1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant m)$, vérifiant

$$|z_{ij} - \langle x_i, y_j \rangle| < \exp(-M^c),$$

tels que, si on pose

$$\tilde{y}_j = (z_{1j}, \ldots, z_{dj}) \in \mathbf{C}^d, \quad (1 \leqslant j \leqslant m),$$

on ait

$$\exp_G\left(\sum_{j=1}^{m} h_j^{(\varkappa)} \tilde{y}_j\right) \in H(\mathbf{C}), \quad (1 \leqslant \varkappa \leqslant k).$$

La condition

$$(m-k)/r < m/d$$

s'écrit $mr+kd>md$, et elle implique $k \neq 0$. On utilise maintenant le théorème de Kolchin sous la forme précisée donnée dans [MW2] Théorème III. Posons $N=3^d-1$. Pour $1 \leqslant i \leqslant d$, soit π_i la i-ème projection de E^d sur E. Il existe alors des éléments $\lambda^{(1)}, \ldots, \lambda^{(r)}$ de $\mathbf{Z}^d$, linéairement indépendants sur $\mathbf{Z}$, avec

$$\max_{1 \leqslant i \leqslant d} |\lambda_i^{(\varrho)}| \leqslant 2^{5N} M^{2r/(r+1-\varrho)}, \quad (1 \leqslant \varrho \leqslant r),$$

tels que, pour tout $h \in H$, on ait

$$\sum_{i=1}^{d} \lambda_i^{(\varrho)} \pi_i(h) = 0, \quad (1 \leqslant \varrho \leqslant r).$$

On écrit cela dans l'espace tangent : si $z=(z_1, \ldots, z_d) \in \mathbf{C}^d$ est tel que $\exp_G z \in H(\mathbf{C})$, alors

$$\sum_{i=1}^{d} \lambda_i^{(\varrho)} z_i \in \Omega, \quad (1 \leqslant \varrho \leqslant r),$$

où Ω est le réseau des périodes de $\wp$. Pour obtenir une contradiction, il ne reste plus qu'à démontrer le lemme suivant, qui précise un résultat de Philippon [P1] :

LEMME 13.10. *Soient* $X=\mathbf{Z}x_1+\ldots+\mathbf{Z}x_d$ *et* $Y=\mathbf{Z}y_1+\ldots+\mathbf{Z}y_m$ *deux sous-groupes de* $\mathbf{C}^n$ *vérifiant l'hypothèse* (12.1). *On suppose*

$$\mu(X) = d/n, \quad \mu(Y) = m/n, \quad \text{et} \quad md \geqslant 2n(m+d).$$

Soient $\varepsilon_0>0$ *et* $\varepsilon>0$. *Il existe* $S_0>0$ *ayant la propriété suivante : soit* $\Omega=\mathbf{Z}\omega_1+\mathbf{Z}\omega_2$ *un réseau de* $\mathbf{C}$ *vérifiant*

$$\min\{|\omega|;\ \omega\in\Omega,\ \omega\neq 0\}>\varepsilon_0;$$

soit $S>S_0$; *soient* z_{ij} $(1\leqslant i\leqslant d,\ 1\leqslant j\leqslant m)$ *des nombres complexes vérifiant*

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

soient $\lambda^{(1)},\dots,\lambda^{(r)}$ *des éléments* $\mathbf{Z}$*-linéairement indépendants de* $\mathbf{Z}^d_{\pm}(S)$, *et* $h^{(1)},\dots,h^{(k)}$ *des éléments* $\mathbf{Z}$*-linéairement indépendants de* $\mathbf{Z}^m_{\pm}(S)$, *avec*

$$1\leqslant r\leqslant d,\quad 1\leqslant k\leqslant m,\quad mr+kd>md.$$

Alors l'un au moins des rk *nombres*

$$\sum_{i=1}^{d}\sum_{j=1}^{m}\lambda_i^{(\varrho)}h_j^{(\varkappa)}z_{ij}\quad(1\leqslant\varrho\leqslant r,\ 1\leqslant\varkappa\leqslant k)$$

n'appartient pas à Ω.

Démonstration du lemme 13.10. On reprend les arguments de Philippon dans [P1]. On pose

$$x'_\varrho=\sum_{i=1}^{d}\lambda_i^{(\varrho)}x_i\quad\text{et}\quad y'_\varkappa=\sum_{j=1}^{m}h_j^{(\varkappa)}y_j\quad(1\leqslant\varrho\leqslant r,\ 1\leqslant\varkappa\leqslant k),$$

et

$$X'=\mathbf{Z}x'_1+\dots+\mathbf{Z}x'_r,\quad Y'=\mathbf{Z}y'_1+\dots+\mathbf{Z}y'_k.$$

Ainsi $\mathrm{rg}_{\mathbf{Z}}X'=r$, $\mathrm{rg}_{\mathbf{Z}}Y'=k$. Notons W le $\mathbf{C}$-espace vectoriel engendré par X', V celui engendré par Y', $\pi:\mathbf{C}^n\to W$ la projection orthogonale de $\mathbf{C}^n$ sur W, de noyau $W^{\perp}$, et $W_1=\pi(V)$. On pose aussi

$$\nu=\dim_{\mathbf{C}}V,\quad\omega=\dim_{\mathbf{C}}W,\quad\eta=\dim_{\mathbf{C}}W_1,\quad\text{et}\quad\lambda=\mathrm{rg}_{\mathbf{Z}}\pi(Y').$$

Comme $W_1=V/V\cap W^{\perp}$, on a $\dim_{\mathbf{C}}V\cap W^{\perp}=\nu-\eta$. D'autre part $\pi(Y')=Y'/Y'\cap W^{\perp}$, donc $\mathrm{rg}_{\mathbf{Z}}Y'\cap W^{\perp}=k-\lambda$. Alors

$$\begin{aligned}\mu(Y)&\leqslant(\mathrm{rg}_{\mathbf{Z}}Y/Y\cap V\cap W^{\perp})/\dim_{\mathbf{C}}\mathbf{C}^n/V\cap W^{\perp}\\&\leqslant(m-k+\lambda)/(n-\nu+\eta).\end{aligned}$$

On va supposer que les nombres

$$\omega_{\varrho\varkappa} = \sum_{i=1}^{d} \sum_{j=1}^{m} \lambda_i^{(\varrho)} h_j^{(\varkappa)} z_{ij} \quad (1 \leqslant \varrho \leqslant r,\ 1 \leqslant \varkappa \leqslant k)$$

appartiennent tous à Ω, et on en déduira $\lambda \leqslant 2\eta$. Alors, comme $\mu(Y)=m/n$, on trouve

$$(\nu-\eta)/n \geqslant (k-2\eta)/m.$$

Symétriquement, en posant $\eta'=\dim_{\mathbf{C}} \pi'(W)$ où $\pi' : \mathbf{C}^n \to V$ est la projection orthogonale sur V :

$$(\omega-\eta')/n \geqslant (r-2\eta')/d.$$

Mais, comme l'a remarqué Philippon [P1], on a $\eta'=\eta$ et $\omega+\nu-\eta \leqslant n$. D'où

$$1-\frac{\eta}{n} \geqslant \frac{k}{m}+\frac{r}{d}-2\eta\left(\frac{1}{m}+\frac{1}{d}\right).$$

Puisque $(1/m)+(1/d) \leqslant 1/2n$, on trouve $(k/m)+(r/d) \leqslant 1$, ce qui fournit la contradiction attendue.

Il reste à vérifier $\lambda \leqslant 2\eta$, sachant que $\omega_{\varrho\varkappa} \in \Omega$, $(1 \leqslant \varrho \leqslant r,\ 1 \leqslant \varkappa \leqslant k)$. Supposons $\lambda > 2\eta$. Par le principe des tiroirs de Dirichlet, on peut trouver des entiers rationnels $a_1, \ldots, a_k$, vérifiant

$$\max_{1 \leqslant \varkappa \leqslant k} |a_\varkappa| \leqslant S^{2\eta+1},$$

tels que, si on pose

$$y'' = a_1 y_1' + \ldots + a_k y_k' \quad \text{et} \quad w = \pi(y''),$$

on ait

$$0 < |w| < S^{-1-1/3\eta}.$$

Pour $1 \leqslant \varrho \leqslant r$, on a d'une part

$$|\langle w, x_\varrho' \rangle| < S^{-1/4\eta},$$

et d'autre part

$$\left| \langle y'', x_\varrho' \rangle - \sum_{\varkappa=1}^{k} a_\varkappa \omega_{\varrho\varkappa} \right| \leqslant \exp(-S^\varepsilon/2).$$

Mais $w-y'' \in \operatorname{Ker}\pi = W^{\perp}$, et $x'_{\varrho} \in W$, donc $\langle w, x'_{\varrho}\rangle = \langle y'', x'_{\varrho}\rangle$. On en déduit d'abord

$$\left|\sum_{\varkappa=1}^{k} a_{\varkappa}\omega_{\varrho\varkappa}\right| \leqslant 2S^{-1/4\eta},$$

donc, pour $S>(2/\varepsilon_0)^{4\eta}$,

$$\sum_{\varkappa=1}^{k} a_{\varkappa}\omega_{\varrho\varkappa} = 0,$$

et ensuite

$$|\langle y'', x'_{\varrho}\rangle| \leqslant \exp(-S^{\varepsilon}/2).$$

Mais

$$\langle y'', x'_{\varrho}\rangle = \left\langle \sum_{j=1}^{m}\sum_{\varkappa=1}^{k} a_{\varkappa} h_j^{(\varkappa)} y_j, \sum_{i=1}^{d} \lambda_i^{(\varrho)} x_i \right\rangle,$$

et l'hypothèse (12.1) assure

$$\langle y'', x'\rangle = 0 \quad \text{pour } 1 \leqslant \varrho \leqslant r.$$

Ainsi $y'' \in W^{\perp}$, mais cela contredit la condition $w \neq 0$.

Ceci termine la démonstration du lemme 13.10, donc aussi celle du corollaire 13.1.

Montrons que si N et k sont des entiers positifs vérifiant $N \geqslant (3+2\sqrt{2})k$, alors parmi les nombres $\wp(e^n)$, $(1 \leqslant n \leqslant N)$, il y en a au moins k qui sont définis et algébriquement indépendants.

Pour cela, on choisit $x_i = e^i$, $(1 \leqslant i \leqslant d)$, et $y_j = e^{j-1}$, $(1 \leqslant j \leqslant m)$, où m et d sont les entiers définis par

$$N(\sqrt{2}-1) < d < N(\sqrt{2}-1)+1, \quad N(2-\sqrt{2}) < m < N(2-\sqrt{2})+1.$$

Ainsi $m+d<N+2$, donc $m+d-1 \leqslant N$, et $(2/m)+(1/d)<(3+2\sqrt{2})/N \leqslant 1/k$. Le degré de transcendance t du corps obtenu en adjoignant à $\mathbf{Q}$ les valeurs de $\wp$ aux points de la forme e^n, $(1 \leqslant n \leqslant m+d-1)$ qui ne sont pas pôles de $\wp$ vérifie $t+1 \geqslant md/(m+2d) > k$, donc $t \geqslant k$.

Avant de démontrer le corollaire 13.3, remarquons que l'inégalité (13.2) résulte de l'énoncé (11.3) (avec $t'=1$: on se ramène à $\mathbf{Q}(g_2, g_3) = \mathbf{Q}(j)$) grâce au lemme 13.10, exactement comme dans la démonstration du corollaire 13.1.

Démonstration du corollaire 13.3. En voici le principe : on reprend la démonstration du corollaire 13.1, mais au lieu d'utiliser le théorème 3.1, on utilise le théorème 9.1

avec $\theta_1=j(E)$. On aura donc un groupe algébrique $\tilde{G}=\tilde{E}^d$, où $\tilde{E}$ est une courbe elliptique ayant un invariant modulaire $\tilde{\theta}_1=j(\tilde{E})$ proche de θ_1, et il faudra montrer, à l'aide de l'hypothèse (9.2), que les seuls sous-groupes algébriques qui interviennent (i.e. ceux qui sont définis par des équations de degré $\leqslant S^{\mu}$) sont de la forme $\tilde{H}$, où H est un sous-groupe algébrique de $G=E^d$. Ce dernier point proviendra de la version effective du théorème de Kolchin pour E^d (cf. [MW2] p. 426), et d'un lemme que nous allons donner maintenant. Pour ce lemme, on note Im la partie imaginaire d'un nombre complexe, et, pour α nombre algébrique, $H(\alpha)$ désigne sa hauteur usuelle (maximum des valeurs absolues des coefficients du polynôme minimal de α sur $\mathbf{Z}$).

LEMME 13.11. *Soit $\tau\in\mathbf{C}$ vérifiant $\operatorname{Im}\tau>0$. Posons $c_1=\frac{1}{2}\operatorname{Im}\tau$. Soit β un nombre imaginaire quadratique vérifiant $|\beta-\tau|\leqslant c_1$. On désigne par a_0 le coefficient directeur du polynôme minimal de β sur $\mathbf{Z}$. Alors pour tout $\lambda\in\mathbf{Z}+\mathbf{Z}a_0\beta$ vérifiant $\lambda\notin\mathbf{Z}$, on a*

$$|\lambda|\geqslant c_2 H(\beta) \quad \text{où } c_2=c_1/(|\tau|+c_1+1)^2.$$

Démonstration du lemme 13.11. Soit $a_0X^2+a_1X+a_2$ le polynôme minimal de β sur $\mathbf{Z}$. On a

$$H(\beta)=\max(a_0,|a_1|,|a_2|)\leqslant a_0\max(1,|\beta+\bar{\beta}|,|\beta|^2)$$
$$\leqslant a_0(1+|\beta|)^2\leqslant a_0(|\tau|+c_1+1)^2.$$

D'autre part $|\operatorname{Im}\beta-\operatorname{Im}\tau|\leqslant|\beta-\tau|\leqslant c_1$, donc $\operatorname{Im}\beta\geqslant c_1$ et

$$a_0c_1\leqslant a_0\operatorname{Im}\beta\leqslant\operatorname{Im}\lambda\leqslant|\lambda|.$$

d'où le lemme.

Revenons à la démonstration du corollaire 13.3. On se ramène, comme précédemment, au cas où $\mathbf{Q}(g_2,g_3)=\mathbf{Q}(j)$, $\mu(X)=d/n$, et $\mu(Y)=m/n$. On suppose $t+1<md/n(m+2d)$, et on utilise le théorème 9.1, avec $\mu=m/d$, $\theta_1=j$. On trouve donc une infinité non bornée de réels $S>0$ telle que les propriétés suivantes soient vérifiées; on désignera par S l'un de ces réels, suffisamment grand, tandis que c_3, c_4, c_5 ne dépendront pas de S.

On dispose d'abord d'une approximation $\tilde{\theta}_1$ de θ_1 :

$$|\tilde{\theta}_1-\theta_1|<\exp(-2S^{\nu}).$$

Soit $\tilde{\tau}\in\mathbf{C}$ vérifiant $j(\tilde{\tau})=\tilde{\theta}_1$ et

$$|\tilde{\tau}-\tau|<\exp(-c_3S^{\nu}).$$

On pose $\tilde{\omega}_1=\omega_1$, $\tilde{\omega}_2=\tilde{\tau}\omega_1$, $\tilde{\Omega}=\mathbf{Z}\tilde{\omega}_1+\mathbf{Z}\tilde{\omega}_2$, et on désigne par $\tilde{\wp}$ la fonction elliptique de Weierstrass associée à $\tilde{\Omega}$, et par $\tilde{E}$ la courbe elliptique correspondante, plongée dans $\mathbf{P}_2(\mathbf{C})$ par $(1, \tilde{\wp}, \tilde{\wp}')$. Enfin $\tilde{G}=\tilde{E}^d$.

On dispose ensuite d'un sous-groupe algébrique H_1 de $\tilde{G}$, de dimension $\leqslant d-r$, défini (dans un espace projectif où on a plongé $\mathbf{P}_2^d(\mathbf{C})$) par des équations de degré $\leqslant S^\mu$, et enfin on dispose, toujours d'après le § 9, d'éléments $h^{(1)}, \ldots, h^{(k)}$ de $\mathbf{Z}_{\pm}^m(S^{d\mu})$, linéairement indépendants sur $\mathbf{Z}$, avec

$$1 \leqslant k \leqslant m, \quad 1 \leqslant r \leqslant d, \quad mr+kd > md,$$

tels que

$$\sum_{j=1}^{m} h_j^{(\varkappa)} \tilde{\gamma}_j \in H_1, \quad (1 \leqslant \varkappa \leqslant k).$$

Le point $\tilde{\gamma}_j$ de $\tilde{E}^d$ correspond, via $\tilde{\wp}$, à un point $(z_{1j}, \ldots, z_{dj})$ de $\mathbf{C}^d$, avec

$$\max_{i,j} |z_{ij} - \langle x_i, y_j \rangle| < \exp(-c_4 S^\nu).$$

Soit $\tilde{\mathcal{O}}$ l'anneau des endomorphismes de $\tilde{E}$; on a $\tilde{\mathcal{O}}=\mathbf{Z}$ si $\tilde{\tau}$ n'est pas imaginaire quadratique, et $\tilde{\mathcal{O}}=\mathbf{Z}+\mathbf{Z}a_0\tilde{\tau}$, où a_0 est le coefficient directeur du polynôme minimal de $\tilde{\tau}$, si $\tilde{\tau}$ est imaginaire quadratique.

D'après la version effective du théorème de Kolchin donnée dans [MW2] Chap. III, on peut trouver des éléments $\lambda^{(1)}, \ldots, \lambda^{(r)}$ de $\tilde{\mathcal{O}}^d$, linéairement indépendants sur $\tilde{\mathcal{O}}$, dont les composantes $\lambda_i^{(\varrho)} \in \tilde{\mathcal{O}}$ $(1 \leqslant i \leqslant d)$, $1 \leqslant \varrho \leqslant r)$ vérifient

$$|\lambda_i^{(\varrho)}| \leqslant S^{c_5},$$

tels que

$$\sum_{i=1}^{d} \sum_{j=1}^{m} \lambda_i^{(\varrho)} h_j^{(\varkappa)} z_{ij} \in \tilde{\Omega} \quad (1 \leqslant \varrho \leqslant r, \ 1 \leqslant \varkappa \leqslant k).$$

Montrons que pour $1 \leqslant i \leqslant d$ et $1 \leqslant \varrho \leqslant r$, on a $\lambda_i^{(\varrho)} \in \mathbf{Z}$. Supposons donc $\tilde{\tau}$ imaginaire quadratique. On utilise l'hypothèse (9.2) avec $\beta=\tilde{\tau}$, $0<\varepsilon<\nu/c_5$, $H=(c_3 S^\nu)^{1/\varepsilon}$. On trouve donc $H(\beta)>H$, et tout élément λ de $\tilde{\mathcal{O}}$ vérifiant $|\lambda| \leqslant S^{c_5}$, est alors dans $\mathbf{Z}$, d'après le lemme 13.11.

Ainsi on a $\lambda^{(\varrho)} \in \mathbf{Z}^d$ pour $1 \leqslant \varrho \leqslant r$. Le lemme 13.10, appliqué à $\tilde{\Omega}$, donne finalement la contradiction attendue.

Démonstration du corollaire 13.4. On travaille avec le groupe algébrique $G=\mathbf{G}_a\times E^d$, de dimension $d+1$. On identifie $T_G(\mathbf{C})$ à $\mathbf{C}\times\mathbf{C}^d$, et on considère le sous-espace vectoriel V de $T_G(\mathbf{C})$ engendré par $v=(1;1,\beta,\beta^2,\ldots,\beta^{d-1})$. Soit $\mathcal{O}=\mathrm{End}\,E$. On prend

$$Y=(\mathcal{O}+\mathcal{O}\beta+\mathcal{O}\beta^2+\ldots+\mathcal{O}\beta^{d-1})\,uv.$$

Ainsi le rang m de Y sur $\mathbf{Z}$ est d si $\mathcal{O}=\mathbf{Z}$, et $2d$ si $\mathcal{O}\neq\mathbf{Z}$. Soit t le degré de transcendance sur $\mathbf{Q}$ du corps

$$\mathbf{Q}(\wp(u),\wp(\beta u),\ldots,\wp(\beta^{d-1}u)).$$

Si on avait $t<k$, alors on aurait $t+1\leqslant k<m(d+1)/(m+2d+2)$, et le théorème 3.1, combiné avec l'inégalité de Liouville dans $\mathbf{Q}(\beta)$, à la version effective du théorème de Kolchin [MW2] Chapitre 3, et au lemme 13.10 (dans le cas plus facile $n=1$) apporterait la contradiction attendue.

La démonstration du corollaire 13.5 est analogue et nous l'omettrons.

Démonstration du corollaire 13.7. On utilise le théorème 1.4 pour $G=E_1\times\ldots\times E_d$. On identifie $T_G(\mathbf{C})$ à $\mathbf{C}^d$ via $\wp_1,\ldots,\wp_d$, et on considère le sous-groupe à un paramètre $\exp_G\circ\mathscr{L}$ de $G(\mathbf{C})$, où $\mathscr{L}(z)=(z,\ldots,z)$. On note $y_j=\mathscr{L}(v_j)\in\mathbf{C}^d$, $(1\leqslant j\leqslant m)$.

Soit H un sous-groupe algébrique de G. L'hypothèse que $E_1,\ldots,E_d$ sont deux-à-deux non isogènes implique $H=H_1\times\ldots\times H_d$, où H_i est un sous-groupe algébrique de E_i, $(1\leqslant i\leqslant d)$ Si H est défini par des équations de degré $\leqslant S$, et si i est un indice tel que $H_i\neq E_i$, alors H_i est un sous-groupe fini de E_i, d'ordre $\leqslant S^{c_1}$ où c_1 ne dépend pas de S (cela résulte, par exemple, de [MW2] Théorème III). L'hypothèse (13.6) montre que si un point $y\in Y_{\pm}(S^{c_2})$ n'appartient pas à $\exp_G^{-1}(H)$, alors sa distance à ce sous-ensemble fermé de $T_G(\mathbf{C})$ est au moins $\exp(-S^{\varepsilon})$. C'est précisément l'hypothèse du théorème 1.4. D'où

$$t+1\geqslant md/(m+2d-\varkappa)\geqslant md/(m+2d)$$

où $\varkappa=\mathrm{rg}_{\mathbf{Z}}\,\mathscr{L}(\mathbf{C})\cap\mathrm{Ker}\exp_G$. Ceci démontre le corollaire 13.7.

Si on remplace l'hypothèse (13.6) par une mesure d'indépendance linéaire de $v_1,\ldots,v_m$, on utilise le théorème 3.1 avec $\mu=(\ell-2)/d$, où ℓ est le rang sur $\mathbf{Z}$ de $\Gamma=\mathbf{Z}\gamma_1+\ldots+\mathbf{Z}\gamma_m$, et $\gamma_j=\exp_G y_j$ $(1\leqslant j\leqslant m)$. Si $t+1<(m-2)\,d/(\ell+2d-2)$, alors $t+1<(d\mu+\varkappa)/(\mu+2)$, et on trouve un indice i, $1\leqslant i\leqslant d$, et k relations de la forme

$$\sum_{j=1}^{m}h_j^{(\varkappa)}\tilde{\gamma}_j\in\Omega_i\quad(1\leqslant\varkappa\leqslant k),$$

avec $h^{(1)}, \ldots, h^{(k)} \in \mathbf{Z}_{\pm}^{\ell}(M)$ linéairement indépendants sur $\mathbf{Z}$, et $k=\ell-\ell_1 \geqslant 3$. Comme $\mathrm{rg}_{\mathbf{Z}}\, \Omega_i = 2$, on en déduit par combinaison linéaire une relation

$$\sum_{j=1}^{m} h_j \tilde{y}_j = 0,$$

avec $(h_1, \ldots, h_m) \in \mathbf{Z}_{\pm}^{m}(M^c)$, où c ne dépend pas de M, ce qui conduit à une contradiction avec l'hypothèse sur la mesure d'indépendance linéaire de $y_1, \ldots, y_m$.

Si $m \geqslant 4d^2$, alors $(m-2)\,d/(m+2d-2) > (md-1)/(m+2d)$, donc la condition $t+1 \geqslant (m-2)\,d/(m+2d-2)$ implique $t+1 \geqslant md/(m+2d)$.

§ 14. Fonctions zêta et sigma : extension d'une courbe elliptique par un tore

Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, $\Omega = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ le réseau des périodes de $\wp$, σ et ζ les fonctions sigma et zêta de Weierstrass associées à Ω. On désigne par $\mathcal{O}$ l'anneau des endomorphismes de $E = \mathbf{C}/\Omega$.

On considère des nombres complexes $u_1, \ldots, u_h$ $\mathcal{O}$-linéairement indépendants modulo Ω, et des nombres complexes $v_1, \ldots, v_m$ linéairement indépendants sur $\mathbf{Z}$. On suppose qu'aucun de ces $h+m$ nombres n'est pôle de $\wp$, et que les nombres $\wp(u_i)$ et $\wp(v_j)$, $(1 \leqslant i \leqslant h,\ 1 \leqslant j \leqslant m)$ sont tous algébriques.

L'hypothèse technique s'écrit de la manière suivante : pour tout $\varepsilon > 0$ il existe $H_0 > 0$ tel que pour tout $H > H_0$, tout $(h_1, \ldots, h_m) \in \mathbf{Z}_{\pm}^{m}(H)$ et tout $\omega \in \Omega$, si le nombre

$$\xi = \omega - \sum_{j=1}^{m} h_j v_j$$

n'est pas nul, alors

$$|\xi| \geqslant \exp(-H^{\varepsilon}).$$

Cette hypothèse est toujours vérifiée dans le cas $\mathcal{O} \neq \mathbf{Z}$, grâce à un théorème de D. W. Masser [M] Chapitre 7, Théorème V. Elle l'est vraisemblablement aussi dans le cas $\mathcal{O} = \mathbf{Z}$: il s'agit d'un analogue quantitatif d'un théorème de Bertrand-Masser, que les travaux de Wüstholz sur la méthode de Baker devraient donner (cf. [Wü]).

COROLLAIRE 14.1. *Si k est un entier tel que*

$$m(h+1) > k(m+2h+2),$$

alors parmi les mh nombres

$$\sigma(v_j-u_i)\,e^{v_j\zeta(u_i)}/\sigma(v_j)\,\sigma(u_i),\quad (1\leqslant i\leqslant h,\ 1\leqslant j\leqslant m)$$

il y en a au moins k qui sont algébriquement indépendants.

Pour $k=2$ et $k=3$, Reyssat [R] a obtenu des énoncés d'indépendance algébrique assez précis pour des nombres liés à ceux du corollaire 14.1.

Démonstration du corollaire 14.1. Au point de E^h paramétré par $(u_1,\dots,u_h)$ via $\wp$ est associé un groupe algébrique G, extension de E par $\mathbf{G}_m^h$, dont l'exponentielle est paramétrée à l'aide de fonctions de $h+1$ variables $(t_1,\dots,t_h;z)\in\mathbf{C}^h\times\mathbf{C}$:

$$\sigma(z-u_i)\,e^{t_i+z\zeta(u_i)}/\sigma(z)\,\sigma(u_i),\quad (1\leqslant i\leqslant h)$$

et $\wp(z)$. On considère ici le sous-groupe à un paramètre $\exp_G\circ\mathscr{L}$ de $G(\mathbf{C})$, où $\mathscr{L}\colon\mathbf{C}\to\mathbf{C}^h\times\mathbf{C}$ est donnée par

$$\mathscr{L}(z)=(0,\dots,0;z).$$

L'hypothèse $\wp(u_i)\in\bar{\mathbf{Q}}$, $(1\leqslant i\leqslant h)$ assure d'abord que G est défini sur $\bar{\mathbf{Q}}$, ensuite que $u_1,\dots,u_h$ sont linéairement indépendants sur $\bar{\mathbf{Q}}$ (théorème de Masser si $\mathcal{O}\neq\mathbf{Z}$, et de Bertrand-Masser si $\mathcal{O}=\mathbf{Z}$; cf. [M, Be2]). Si H est un sous-groupe algébrique propre de G, alors sa projection $\pi(H)$ sur E est finie (cf. [Be2] § 2). De plus, si H est défini par des équations de degré $\leqslant M$, alors $\pi(H)$ est d'ordre au plus M^c.

Posons $y_j=\mathscr{L}(v_j)$, $(1\leqslant j\leqslant m)$, et $Y=\mathbf{Z}y_1+\dots+\mathbf{Z}y_m$. Soit $(h_1,\dots,h_m)\in\mathbf{Z}_{\pm}^m(M)$; posons $y=h_1y_1+\dots+h_my_m$; soit $u\in T_G(\mathbf{C})$ tel que $\exp_G u\in H(\mathbf{C})$; supposons

$$|u-y|<\exp(-M^{\varepsilon}).$$

Alors la dernière coordonnée de u dans $\mathbf{C}^h\times\mathbf{C}$ est de la forme ω/s, avec $\omega\in\Omega$, et $s\in\mathbf{Z}$, $0<s\leqslant M^c$. Pour $v=s(h_1v_1+\dots+h_mv_m)$, on a

$$|v-\omega|<\exp(-M^{\varepsilon}/2),$$

et par hypothèse cela implique $v=\omega$, donc $\exp_G y\in H(\mathbf{C})$. On peut ainsi appliquer le théorème 1.4, et le corollaire 14.1 en découle.

§ 15. Variétés abéliennes

Plusieurs résultats d'indépendance algébrique, concernant les sous-groupes à plusieurs paramètres de variétés abéliennes, ont déjà été obtenus par Philippon [P2]. Nous allons en donner quelques autres.

20—868283 *Acta Mathematica* 156. Imprimé le 15 mai 1986

(a) *Sous-groupes à un paramètre de A^h avec* $\mathrm{End}\,A=\mathbf{Z}$. Reprenons l'exemple de [MW2] p. 411. Soit A une variété abélienne définie sur un corps de nombres, de dimension $g\geqslant 1$, dont l'anneau des endomorphismes est trivial. On dispose alors de fonctions abéliennes $f_1,\ldots,f_g$, méromorphes sur $\mathbf{C}^g$, algébriquement indépendantes, admettant pour périodes un réseau Ω de $\mathbf{C}^g$, avec $A\simeq\mathbf{C}^g/\Omega$. Soient $u_1,\ldots,u_h$ des éléments $\mathbf{Q}$-linéairement indépendants de $\mathbf{C}^g$, et soient $v_1,\ldots,v_m$ des nombres complexes $\mathbf{Q}$-linéairement indépendants.

Voici l'hypothèse technique :

(15.1) Pour tout $\varepsilon>0$, il existe $H_0>0$ tel que pour tout $H>H_0$ et tout $(\lambda_1,\ldots,\lambda_h,h_1,\ldots,h_m)$ dans $\mathbf{Z}_{\pm}^{h+m}(H)$ vérifiant

$$\xi=\left(\sum_{i=1}^{h}\lambda_i u_i\right)\left(\sum_{j=1}^{m}h_j v_j\right)\notin\Omega,$$

on a

$$\mathrm{dist}(\xi,\Omega)>\exp(-H^{\varepsilon}),$$

une fois choisie une distance dans $\mathbf{C}^g$.

COROLLAIRE 15.2. *Soit k un entier positif tel que*

$$gmh>k(m+2gh). \tag{15.3}$$

Alors k au moins des gmh nombres

$$f_\nu(u_i v_j),\quad (1\leqslant\nu\leqslant g,\ 1\leqslant i\leqslant h,\ 1\leqslant j\leqslant m)$$

sont définis et algébriquement indépendants sur $\mathbf{Q}$.

De la même manière qu'au § 13(c), on peut affaiblir l'hypothèse (15.1) en demandant seulement un mesure d'indépendance linéaire des u_i et aussi des v_j, quitte à imposer une condition (15.3) légérement plus forte.

(b) *Sous-groupes à n-paramètres d'une variété abélienne simple.* Dans l'énoncé (15.2) précédent, quand $h=1$, on peut remplacer l'hypothèse $\mathrm{End}\,A=\mathbf{Z}$ par la condition (plus faible) que A est simple. Donnons l'énoncé pour les sous-groupes à plusieurs paramètres.

On considère donc une variété abélienne simple A de dimension g définie sur le corps $\bar{\mathbf{Q}}$ des nombres algébriques, un sous-espace vectoriel V de $T_A(\mathbf{C})$ de dimension n

sur $\mathbf{C}$, et des éléments $\mathbf{Q}$-linéairement indépendants $y_1, \ldots, y_m$ de V. On note $\Omega = \operatorname{Ker} \exp_A$, et $Y = \mathbf{Z}y_1 + \ldots + \mathbf{Z}y_m$. Soit K un sous-corps de $\mathbf{C}$, de degré de transcendance t sur $\mathbf{Q}$, tel que $\exp_A y_j \in A(K)$ pour $1 \leqslant j \leqslant m$.

On suppose que pour tout $\varepsilon > 0$ il existe $H_0 > 0$ tel que pour tout $H > H_0$, pour tout $(h_1, \ldots, h_m) \in \mathbf{Z}^m_{\pm}(H)$ et tout $\omega \in \Omega$, la condition

$$|h_1 y_1 + \ldots + h_m y_m - \omega| < \exp(-H^{\varepsilon})$$

implique

$$h_1 y_1 + \ldots + h_m y_m = \omega.$$

COROLLAIRE 15.4. *On a*

$$t + 1 \geqslant mg/n(m+2g).$$

(c) *Démonstrations.*

Démonstration du corollaire 15.2. On utilise le théorème 1.4 pour $G = A^h$, avec $d = gh$. On prend pour V le sous-espace de dimension 1 de $T_G(\mathbf{C}) \simeq \mathbf{C}^{gh}$ engendré par le point $(u_1, \ldots, u_g)$. Pour vérifier l'hypothèse (1.5), on utilise la description des sous-groupes algébriques de G donnée dans [MW2] p. 426.

Démonstration du corollaire 15.4. On va utiliser le théorème 8.1 avec $G = A$, $d = g$. Comme A est simple, on a évidemment $\mu(V) = g/n$. Il reste à vérifier l'hypothèse (1.5).

Dans cette hypothèse, on a un sous-groupe algébrique H de A, défini par des équations de degré $\leqslant M$, et un élément y de $Y_{\pm}(M)$ tel que $\exp_A y \notin H(\mathbf{C})$. Donc $H \neq A$, et par conséquent H est fini, avec au plus M^c éléments, où c ne dépend pas de M. Alors l'élément u de $T_G(\mathbf{C})$ qui vérifie $\exp_A u \in H(\mathbf{C})$ est de la forme ω/s, avec $\omega \in \Omega$ et $s \in \mathbf{Z}$, $1 \leqslant s \leqslant M^c$, et l'hypothèse du corollaire 15.4 donne la minoration voulue de $|u - y|$.

Si on demandait seulement une mesure d'indépendance linéaire pour $y_1, \ldots, y_m$, on trouverait, à l'aide du théorème 3.1

$$t + 1 \geqslant (m - 2n)\, g/n(m - 2n + 2g),$$

ce qui, pour $m \geqslant 4ng^2$, redonne le même résultat.

§ 16. Compléments

(a) *Raffinements.* On peut apporter quelques améliorations aux résultats précédents. Ainsi, en écrivant, comme dans [Wa2], le groupe algébrique G sous la forme

$\mathbf{G}_a^{d_0}\times G_1\times G_2$ où G_1 est linéaire, on peut remplacer partout $d\varrho$ par d_1+2d_2, avec $d_1=\dim G_1$ et $d_2=\dim G_2$, à condition de disposer d'un lemme de zéros « multihomogène » sous une forme précise analogue à celle donnée dans [MW2] pour le cas homogène. De même on obtient des inégalités plus précises quand on ajoute des hypothèses de nature arithmétique sur le sous-groupe Y, par exemple $Y\subset T_G(K)$, ou sur le sous-espace vectoriel V, par exemple $V\subset T_G(K)$, en utilisant des lemmes de zéros avec multiplicité.

On peut aussi améliorer les résultats dans le cas $\varkappa>0$ (i.e. $\Omega\cap V\neq 0$) en utilisant mieux les périodes; par exemple, pour $n=\varkappa=1$, on peut montrer d'une part

$$si\ 2d\ell>3(\ell+d_1+2d_2-1),\ alors\ t>1,$$

et d'autre part, sous l'hypothèse (1.5),

$$J(\theta_1,\dots,\theta_t)\geqslant 2d\ell/(\ell+d_1+2d_2-1)-1$$

Enfin il n'y a pas de difficulté à démontrer des versions p-adiques de ces différents résultats, grâce à [Be1].

(b) *Conjectures*. Nous ne cherchons pas ici à formuler les meilleures conjectures possibles, mais seulement à donner quelques énoncés qui pourraient être accessible dans un futur assez proche, compte tenu des méthodes actuellement connues.

On considère un groupe algébrique commutatif connexe G de dimension d, défini sur un sous-corps K de $\mathbf{C}$ de degré de transcendance t sur $\mathbf{Q}$. On écrit G comme extension d'une variété abélienne A de dimension $g\geqslant 0$ par un groupe linéaire L. Sans perte de généralité on peut supposer L déployé sur K: $L=L_u\times L_m$, où $L_u=\mathbf{G}_a^{d_a}$ est un groupe unipotent de dimension $d_a\geqslant 0$, et $L_m=\mathbf{G}_m^{d_m}$ est un groupe de type multiplicatif de dimension $d_m\geqslant 0$. Ainsi $d=d_a+d_m+g$.

Soit V un sous-espace vectoriel de $T_G(\mathbf{C})$ de dimension n sur $\mathbf{C}$, et soit Y un sous-groupe de type fini de V, tel que $\exp_G Y\subset G(K)$. On suppose que $\exp_G V$ est dense dans $G(\mathbf{C})$. On note $\mu(Y)=\mu(Y, V)$.

CONJECTURE 16.1. *Si* $d\mu(Y)>n\mu(Y)+d_m+2g$, *alors*

$$t+1>d\mu(Y)/(n\mu(Y)+d_m+2g).$$

On peut espérer un peu mieux dans le cas où le sous-groupe à n paramètres $\exp_G|_V$: $V\to G(\mathbf{C})$ admet des périodes. Pour cela notons $\varkappa=\mathrm{rg}_{\mathbf{Z}} V\cap\mathrm{Ker}\exp_G$.

CONJECTURE 16.2. *Si* $n=1$ *on a*

$$t\left(1-\frac{\varkappa}{2}\right)+1 \geqslant d\mu(Y)/(n\mu(Y)+d_m+2g-\varkappa).$$

La quantité d_m+2g, qui remplace l'expression dQ des théorèmes ci-dessus (ou d_1+2d_2 dans le (a)) est égale au rang de $\Omega=\mathrm{Ker}\exp_G$, et

$$d_m+2g-\varkappa = \mathrm{rg}_{\mathbf{Z}}\,\Omega/\Omega\cap V.$$

Les deux conjectures précédentes correspondent à la méthode de Schneider. En voici deux autres liées à la méthode de Gel'fond-Baker. On désigne par W le plus petit sous-C-espace vectoriel de $T_G(\mathbf{C})$, défini sur K, et contenant Y. Soit n' la dimension de W, $n\leqslant n'\leqslant d$. On note toujours $\mu(Y)=\mu(Y, V)$.

CONJECTURE 16.3. *Si* $d>n'$ *et* $\mu(Y)>0$, *alors*

$$t>(d-n')\mu(Y)/(n\mu(Y)+d_m+2g).$$

Le fait que les conditions $d>n'$ et $\mu(Y)>0$ impliquent $t>0$ a été démontré par Wüstholz [Wü].

CONJECTURE 16.4. *Si* $n=1$ *on a*

$$t\left(1-\frac{\varkappa}{2}\right)\geqslant(d-n')\mu(Y)/(n\mu(Y)+d_m+2g-\varkappa).$$

On peut espérer des inégalités plus fines en ajoutant des hypothèses, par exemple :

— G défini sur $\bar{\mathbf{Q}}$,

— pour un sous-groupe algébrique H de G (par exemple $H=L$), en notant $\pi: G\to G/H$ la surjection naturelle, on a $\pi\circ\exp_G(Y)\subset(G/H)_{\mathrm{tors}}$;

ou encore, en supposant G défini sur $\bar{\mathbf{Q}}$,

— pour un sous-groupe algébrique H de G, défini sur $\bar{\mathbf{Q}}$, on a $\pi\circ\exp_G Y\subset G/H(\bar{\mathbf{Q}})$,

— pour un sous-groupe Y' de Y, on a $\exp_G Y'\subset G(\bar{\mathbf{Q}})$,

— enfin on peut aussi faire intervenir la dimension du plus petit sous-espace vectoriel de $T_G(\mathbf{C})$ sur $\mathbf{C}$, défini sur $\bar{\mathbf{Q}}$ et contenant Y.

References

[Be1] BERTRAND, D., Problèmes locaux. Appendice 1 de [Wa1].

[Be2] — Endomorphismes de groupes algébriques : applications arithmétiques. *Approxima-*

tions diophantiennes et nombres transcendants, Luminy 1982. Birkhäuser, Progress in Math., 31 (1983), 1–45.

[Br] BROWNAWELL, W. D., On the development of Gel'fond's method. *Proc. Number Theory, Carbondale* 1979, Lecture Notes in Math., 751 (1979), 16–44. Springer Verlag.

[M] MASSER, D. W., *Elliptic functions and transcendence*. Lecture Notes in Math., 437 (1975). Springer Verlag.

[MW1] MASSER, D. W. & WÜSTHOLZ, G., Zero estimates on group varieties I. *Invent. Math.*, 64 (1981), 489–516.

[MW2] — Fields of large trancendence degree generated by values of elliptic functions. *Invent. Math.*, 72 (1983), 407–464.

[P1] PHILIPPON, P., Sur la répartition relative de sous-groupes de type fini de $\mathbf{C}^d$. *Problèmes Diophantiens* 1981/1982. Publ. Math. Univ. P. et M. Curie, 49 (1982).

[P2] — Sous-groupes à n-paramètres et indépendance algébrique. *Approximations diophantiennes et nombres transcendants, Luminy* 1982. Birkhäuser, Progress in Math., 31 (1983), 221–234.

[P3] — *Pour une théorie de l'indépendance algébrique*. Thèse Sc. Math., Orsay, 1983.

[P4] — Critères d'indépendance algébrique. *Publ. Math. I.H.E.S.* À paraître.

[R] REYSSAT, E., Propriétés d'indépendance algébrique de nombres liés aux fonctions de Weierstrass. *Acta Arith.*, 41 (1982), 291–310.

[S] SERRE, J.-P., Quelques propriétés des groupes algébriques commutatifs. Appendice 2 de [Wa1].

[Wa1] WALDSCHMIDT, M., *Nombres transcendants et groupes algébriques*. Soc. Math. France, Astérisque, 69–70 (1979).

[Wa2] — Sous-groupes analytiques de groupes algébriques. *Ann. of Math.*, 117 (1983), 627–657.

[Wa3] — Indépendance algébrique et exponentielles en plusieurs variables. *Number theory, Noordwijkerbout* 1983. Lecture Notes in Math., 1068 (1984), 268–279. Springer Verlag.

[Wa4] — Algebraic independence of transcendental numbers : Gel'fond's method and its developments. *Perspective in Math., Anniversary of Oberwolfach* 1984. Birkhäuser Verlag, 551–571.

[WZ] WALDSCHMIDT, M. & ZHU Y. C., Une généralisation en plusieurs variables d'un critère de transcendance de Gel'fond. *C.R. Acad. Sci. Paris, Sér. I*, 297 (1983), 229–232.

[Wü] WÜSTHOLZ, G., Some remarks on a conjecture of Waldschmidt. *Approximations diophantiennes et nombres transcendants, Luminy* 1982. Birkhäuser, Progress in Math., 31 (1983), 329–336.

Appendice : Déformation d'un groupe algébrique

par

J. FRESNEL

Université de Bordeaux I
Talence, France

Soient un groupe R un sous-anneau de $\mathbf{C}$ de type fini sur $\mathbf{Z}$, $K=\mathrm{Fr}R$ le corps des fractions de R, G un groupe algébrique sur K qui est commutatif, ouvert d'un fermé de $\mathbf{P}_K^N$, $\varphi: R\to\mathbf{C}$ un homomorphisme et $\tilde{K}=\mathrm{Fr}(\varphi(R))$. On souhaite construire un groupe algébrique commutatif $\tilde{G}$ sur $\tilde{K}$, de même dimension que G, qui soit ouvert d'un fermé de $\mathbf{P}_{\tilde{K}}^N$ et qui possède les propriétés supplémentaires suivantes.

Il existe un sous-groupe H du groupe $G(K)$ (le groupe des points rationnels de G sur K) tel que tout point de H puisse s'écrire sous la forme $(u_0, u_1, \ldots, u_N)$ dans $\mathbf{P}_K^N(K)$ avec $u_i\in R$ et l'un des $\varphi(u_i)$ n'est pas nul; de plus $(\varphi(u_0), \ldots, \varphi(u_N))\in\tilde{G}(\tilde{K})\subset\mathbf{P}_{\tilde{K}}^N(\tilde{K})$ et l'application $(u_0, u_1, \ldots, u_N)\mapsto(\varphi(u_0), \ldots, \varphi(u_N))$ est un homomorphisme. On souhaite en plus que cette propriété soit valable pour une famille « suffisamment grosse » d'homomorphismes φ.

En fait ce problème n'est autre chose que la construction d'une famille de déformations du groupe G, indexée sur un ouvert Zariski dense de $\mathrm{Sp}R$; le groupe G étant indexé par le point générique de $\mathrm{Sp}R$. L'existence d'une famille de déformations, ou encore l'existence d'un schéma en groupes sur un ouvert dense de Zariski de $\mathrm{Sp}R$ dont la fibre générique est G est bien connue (EGA, Chapitre IV); il suffit donc d'utiliser ces résultats, de les interpréter et de les adapter au « problème de la transcendance ».

1. Définition de la déformation

(On peut consulter Hartshorne p. 89, EGA Chapitres I, 2.5 p. 103, 3.6 p. 117, 3.7.3 p. 119.) Soient $\varphi: \mathfrak{X}\to S$ un morphisme entre deux schémas, $s\in S$, $k(s)\overset{\text{déf}}{=}\mathcal{O}_{S,s}/\mathfrak{M}_s$ le corps résiduel de s et $\mathrm{Sp}\,k(s)\to S$ le morphisme canonique. La *fibre du morphisme* φ au point s est le schéma $\mathfrak{X}_s\overset{\text{déf}}{=}\mathfrak{X}\times_S\mathrm{Sp}\,k(s)$; c'est donc un schéma sur le corps $k(s)$. L'espace $\mathfrak{X}_s$ est canoniquement homéomorphe à $\varphi^{-1}(s)$, muni de la topologie induite par $\mathfrak{X}$.

Considérons le cas où $S=\mathrm{Sp}R$ avec R noethérien intègre. Soient $\eta\in S$ le point générique de S et X une variété algébrique sur $K=\mathrm{Fr}R=k(\eta)$. On appelle *famille de*

déformations de X tout schéma $\varphi: \mathfrak{X} \to S$ tel que $\mathfrak{X}_\eta \simeq X$; les autres fibres $\mathfrak{X}_s$, $s \in S$ s'appellent les *déformations* de X.

2. Existence de la déformation

Ce qui suit n'est autre chose qu'un ensemble de résultats qui se trouvent dans EGA, Chapitre IV.

THÉORÈME 1 (EGA, Chapitre IV). *Soient R un anneau noethérien intègre, $K = \mathrm{Fr}(R)$, $G \xrightarrow{\alpha} G_1 \xrightarrow{\beta} \mathbf{P}^N_K$ trois variétés algébriques réduites, $\mathbf{P}^N_K = \mathrm{Proj}\, K[X_0, \ldots, X_N]$ est l'espace projectif de dimension N, α est une immersion ouverte dominante, β est une immersion fermée; en plus G est un groupe algébrique commutatif, connexe, régulier. Alors il existe $f \in R - \{0\}$, $\mathfrak{G}$, $\mathfrak{G}_1$ des schémas plats sur $S_f \overset{\text{déf}}{=} \mathrm{Sp}\, R[1/f]$, et des morphismes $a: \mathfrak{G} \to \mathfrak{G}_1$, $b: \mathfrak{G}_1 \to \mathbf{P}^N_{R[1/f]} = \mathrm{Proj}\, R[1/f]\,[X_0, \ldots, X_N]$ avec les propriétés suivantes.*

(1) *$\mathfrak{G}$ est un schéma en groupes commutatifs, a est une immersion ouverte dominante, b est une immersion fermée; en particulier $\mathfrak{G}_s$ est un groupe algébrique commutatif sur $k(s)$ pour tout $s \in S_f$.*

(2) *Soit η le point générique de S_f, alors $\mathfrak{G}_\eta \simeq G$, $\mathfrak{G}_{1\eta} \simeq G_1$, $a_\eta = \alpha$, $b_\eta = \beta$.*

(3) *Pour tout $s \in S_f$, $a_s: \mathfrak{G}_s \to \mathfrak{G}_{1s}$ est une immersion ouverte dominante, $b_s: \mathfrak{G}_{1s} \to \mathbf{P}^N_{k(s)}$ est une immersion fermée.*

(4) *Pour tout $s \in S_f$, le groupe algébrique $\mathfrak{G}_s$ est géométriquement régulier.*

(5) *Pour tout $s \in S_s$, chaque composante connexe de $\mathfrak{G}_s$ a même dimension que $\mathfrak{G}_\eta \simeq G$.*

(6) *Le nombre géométrique de composantes connexes de $\mathfrak{G}_s$ est le nombre géométrique de composantes connexes de $\mathfrak{G}_\eta \simeq G$, pour tout $s \in S_f$.*

(7) *Si $\mathbf{P}^N_{R[1/f]} = \mathrm{Proj}\, R[1/f]\,[X_0, \ldots, X_N]$, alors il existe i, $0 \leqslant i \leqslant N$, tel que $D_+(X_i) \cap \mathfrak{G}_s$ soit dense dans $\mathfrak{G}_s$ pour tout $s \in S_f$ ($\mathfrak{G}_s$ est identifie à $\varphi^{-1}(s) \subset \mathfrak{G}$ selon* **1**).

Démonstration. On feuillette EGA, Chapitre IV.

L'existence de $\mathfrak{G}$, $\mathfrak{G}_1$, a, b avec $\mathfrak{G}_\eta = G$, $\mathfrak{G}_{1\eta} = G_1$, $a_\eta = \alpha$, $b_\eta = \beta$ est le théorème 8.8.2, Chapitre IV, p. 28. La platitude de $\mathfrak{G}$, $\mathfrak{G}_1$ est le théorème 6.9.1, Chapitre IV, p. 153. Que $\mathfrak{G}$ soit un schéma en groupes commutatifs est le Scholie 8.8.3 p. 33–34. Le théorème 8.10.5, Chapitre IV, p. 37 montre que a est une immersion ouverte dominante et b une immersion fermée. Par le corollaire 9.9.5, Chapitre IV, p. 94 on a $\mathfrak{G}_s$

(géométriquement) régulier. Le corollaire 9.5.6, Chapitre IV p. 69 montre 5), et la proposition 9.7.8, Chapitre IV, p. 82 montre 6).

Comme $\mathfrak{G}_\eta \simeq G$ est connexe, on peut supposer (quitte à changer les indices) que $D_+(X_0) \cap \mathfrak{G}_\eta \neq \emptyset$, donc que $D_+(X_0) \cap \mathfrak{G}_\eta$ est dense dans $\mathfrak{G}_\eta$; il suit de la proposition 9.5.3, Chapitre IV, p. 67 que $D_+(X_0) \cap \mathfrak{G}_s$ est dense dans $\mathfrak{G}_s$.

Remarque. Si on change f en $f_1 = fh$, avec $h \in R - \{0\}$, les schémas $\mathfrak{G} \times_{S_f} S_{f_1}$, $\mathfrak{G}_1 \times_{S_f} S_{f_1}$, et les morphismes qui s'en déduisent satisfont le théorème 1 (en remplaçant f par f_1). Le schéma $\mathfrak{G}$ est « unique »; i.e. si $\mathfrak{G}$ et $\mathfrak{G}'$ conviennent, il existe S' ouvert non vide de $\operatorname{Sp} R$ avec $\mathfrak{G} \times S' \simeq \mathfrak{G}' \times S'$.

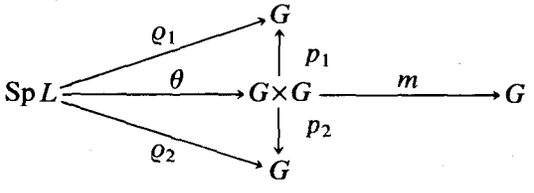
Remarque. Si G est une variété abélienne (resp. affine), on peut choisir $\mathfrak{G}$ abélien (resp. affine) et les $\mathfrak{G}_s$ seront abéliens (resp. affines).

Si $G_1 \to G_2 \to G_3$ est une suite exacte de groupes algébriques alors il existe une suite exacte de schémas en groupes $\mathfrak{G}_1 \to \mathfrak{G}_2 \to \mathfrak{G}_3$ et l'on a aussi les suites exactes $\mathfrak{G}_{1s} \to \mathfrak{G}_{2s} \to \mathfrak{G}_{3s}$.

3. Le groupe des « points rationnels »

3.1. *Le groupe des points rationnels d'un groupe algébrique.* Soient G un groupe algébrique sur un corps L, $G(L)$ le sous-ensemble des points de G rationnels sur L; comme les points de $G \times G$ rationnels sur L s'identifient canoniquement à $G(L) \times G(L)$, il suit que la structure de groupe algébrique G induit sur l'ensemble $G(L)$ une structure de groupe (au sens ordinaire).

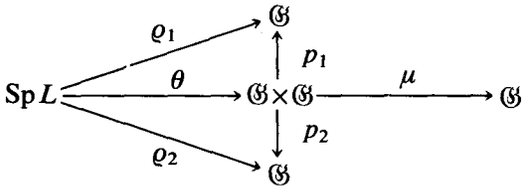
On peut interpréter un point rationnel comme la donnée d'un morphisme $\varrho : \operatorname{Sp} L = \{\xi\} \to G$ par $\varrho \to \varrho(\xi) \in G(L)$. Soient ϱ_1, ϱ_2 deux tels morphismes, p_1, p_2 les projections canoniques de $G \times G$ sur G, θ l'unique morphisme tel que $p_i \circ \theta = \varrho_i$, et m la multiplication :



Alors on vérifie immédiatement que $m \circ \theta(\xi) = m(\varrho_1(\xi), \varrho_2(\xi))$. Ainsi donc le groupe $G(L)$ est aussi l'ensemble des morphismes $\varrho : \operatorname{Sp} L \to G$ muni de l'opération $\varrho_1 * \varrho_2 =$

$m \circ \theta$. C'est cette interprétation qui permet de définir les « points rationnels » d'un schéma en groupes.

3.2. *Le groupe des « points rationnels » d'un schéma en groupes.* Soient R un anneau noethérien intègre, $\varphi: \mathfrak{G} \to S = \operatorname{Sp} R$ un schéma en groupes de type fini sur S. Soit $\mathfrak{G}(R)$ l'ensemble des morphismes $\varrho: \operatorname{Sp} R \to \mathfrak{G}$; en particulier le morphisme « élément neutre » $e: \operatorname{Sp} R \to \mathfrak{G}$ est élément de $\mathfrak{G}(R)$. Montrons que la structure de schéma en groupes induit sur $\mathfrak{G}(R)$ une structure de groupe (au sens ordinaire). Si θ est l'unique morphisme de $\operatorname{Sp} L$ dans $\mathfrak{G} \times \mathfrak{G}$ tel que $p_i \circ \theta = \varrho_i$, on définit $\varrho_1 * \varrho_2 \overset{\text{déf}}{=} \mu \circ \theta$ où μ est le morphisme multiplication :



Il est facile de vérifier que $(\mathfrak{G}(R), *)$ est un groupe (au sens ordinaire), e est l'élément neutre, et $i \circ \varrho$ est l'inverse de ϱ si $i: \mathfrak{G} \to \mathfrak{G}$ est le morphisme « inversion ».

PROPOSITION 2. *Soient R un anneau noethérien intègre, $\mathfrak{G}$ un schéma en groupes plat, de type fini sur $S = \operatorname{Sp} R$. Soient $s \in S$, $\varrho \in \mathfrak{G}(R)$, i.e. $\varrho: \operatorname{Sp} R \to \mathfrak{G}$ un morphisme, $\varrho_s: \operatorname{Sp} k(s) \to \mathfrak{G}_s$ le morphisme induit, alors $\theta_s: \mathfrak{G}(R) \to \mathfrak{G}_s(k(s))$ défini par $\theta_s(\varrho) = \varrho_s$ est un homomorphisme. Soit η le point générique de S, alors $\theta_\eta: \mathfrak{G}(R) \to \mathfrak{G}_\eta(k(\eta))$ est injectif. Ainsi il existe un homomorphisme $\delta_s: \theta_\eta(\mathfrak{G}(R)) \to \mathfrak{G}_s(k(s))$ tel que $\delta_s(\varrho_\eta) = \varrho_s$ pour tout $\varrho \in \mathfrak{G}(R)$.*

3.3. *Les « points rationnels » de $\mathbf{P}_R^N$.* Soient $\varrho: \operatorname{Sp} R \to \mathbf{P}_R^N = \operatorname{Proj} R[X_0, \ldots, X_N]$ un morphisme, $K = \operatorname{Fr}(R)$, $\varrho_\eta: \operatorname{Sp} K \to \mathbf{P}_K^N$, on a $\varrho_\eta(\xi) \in \mathbf{P}_K^N(K)$. La proposition qui suit montre à quelle condition un point de $\mathbf{P}_K^N(K)$ définit un morphisme $\varrho: \operatorname{Sp} R \to \mathbf{P}_R^N$.

PROPOSITION 3. *Soient R un anneau noethérien intègre, $K = \operatorname{Fr}(R)$, $\mathbf{P}_R^N = \operatorname{Proj} R[X_0, \ldots, X_N]$, $x = (x_0, \ldots, x_N) \in \mathbf{P}_K^N(K)$, η le point générique de $S = \operatorname{Sp} R$. Alors les propriétés suivantes sont équivalentes.*

(i) *Il existe un morphisme $\varrho: \operatorname{Sp} R \to \mathbf{P}_R^N$ tel que $\varrho_\eta(\xi) = (x_0, \ldots, x_N)$, où $\{\xi\} = \operatorname{Sp} K$.*

(ii) *Pour tout $\mathfrak{p} \in \operatorname{Sp} R$ il existe $u_0(\mathfrak{p}), \ldots, u_N(\mathfrak{p})$ dans R avec $x = (u_0(\mathfrak{p}), \ldots, u_N(\mathfrak{p}))$, et l'un des $u_i(\mathfrak{p})$ n'appartient pas à $\mathfrak{p}$.*

(iii) *Pour $0 \leqslant i \leqslant N$, soit $\mathfrak{A}_i = \{d \in R \mid dx_j \in x_i R,\ 0 \leqslant j \leqslant N\}$. Alors $\sum_{i=0}^N \mathfrak{A}_i = R$.*

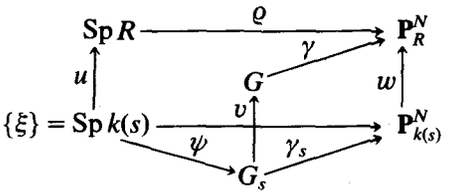
Si ces conditions sont réalisées, le morphisme ϱ est unique. Si $s \in \operatorname{Sp} R$, on a $x=(v_0(\mathfrak{p}_s), \ldots, v_N(\mathfrak{p}_s))$, $v_i(\mathfrak{p}_s) \in R$, et $v_{i_0}(\mathfrak{p}_s) \notin \mathfrak{p}_s$, et alors $\varrho_s(\xi')=(\overline{v_0(\mathfrak{p}_s)}, \ldots, \overline{v_N(\mathfrak{p}_s)})$, où $\{\xi'\}=\operatorname{Sp} k(s)$, et $\overline{v_i(\mathfrak{p}_s)}$ est l'image de $v_i(\mathfrak{p}_s)$ dans $k(s)$.

PROPOSITION 4. *Soient R un anneau noethérien intègre, $\mathfrak{G}$ et $\mathfrak{G}_1$ des schémas plats de type fini sur $S=\operatorname{Sp} R$, $\alpha: \mathfrak{G} \to \mathfrak{G}_1$ une immersion ouverte, $\beta: \mathfrak{G}_1 \to \mathbf{P}_R^N$ une immersion fermée, $\gamma=\beta \circ \alpha$, $\mathfrak{G}(R)$ (resp. $\mathbf{P}_R^N(R)$) l'ensemble des « points rationnels » de $\mathfrak{G}$ (resp. $\mathbf{P}_R^N$). Soit $\varrho \in \mathbf{P}_R^N(R)$; alors les propriétés suivantes sont équivalentes.*

(i) *Il existe $\varrho_2 \in \mathfrak{G}(R)$ tel que $\varrho_\eta=\gamma_\eta \circ \varrho_{2\eta}$ où η est le point générique de S, ϱ_η (resp. γ_η, $\varrho_{2\eta}$) est le morphisme induit par ϱ (resp. γ, ϱ_2).*

(ii) *Pour tout $s \in S$ il existe $\psi \in \mathfrak{G}_s(k(s))$ tel que $\gamma_s \circ \psi=\varrho_s$.*

Démonstration. (i) *implique* (ii) est immédiat, il suffit de prendre $\psi=\varrho_{2s}$. (ii) *implique* (i). On considère le diagramme commutatif, où u, v, w sont les projections canoniques :



On a $u(\xi)=s$, ainsi $\varrho \circ u(\xi)=\gamma \circ v \circ \psi(\xi)$, ce qui veut dire que $\varrho(s) \in \gamma(\mathfrak{G})$; ainsi $\varrho(\operatorname{Sp} R) \subset \gamma(\mathfrak{G})$. En particulier $\varrho(\operatorname{Sp} R) \subset \beta(\mathfrak{G}_1)$. Comme R est intègre il existe $\varrho_1: \operatorname{Sp} R \to \mathfrak{G}_1$ tel que $\beta \circ \varrho_1=\varrho$. Comme $\mathfrak{G}$ est ouvert dans $\mathfrak{G}_1$ et que $\varrho_1(\operatorname{Sp} R) \subset \mathfrak{G}$, il existe un morphisme $\varrho_2: \operatorname{Sp} R \to \mathfrak{G}$ tel que $\alpha \circ \varrho_2=\varrho_1$, ce qui montre $\gamma \circ \varrho_2=\varrho$.

Remarque. Conservons les hypothèses de la proposition 4 en identifiant $\mathfrak{G}_s$ à une partie de $\mathbf{P}_{k(s)}^N$ pour $s \in S$ (et donc $\mathfrak{G}_s(k(s))$ à une partie de $\mathbf{P}_{k(s)}^N(k(s))$), on peut traduire la proposition 4 en termes plus concrets.

Soit $x=(x_0, \ldots, x_N) \in \mathbf{P}_{k(\eta)}^N(k(\eta))=\mathbf{P}_K^N(K)$ qui provient d'un élément de $\mathbf{P}_R^N(R)$ (proposition 3). Alors on a équivalence entre (i) et (ii) :

(i) le point x provient d'un élément de $\mathfrak{G}(R)$,

(ii) pour tout premier $\mathfrak{p}$ (correspondant à $s \in S$) on a

$$(\overline{u_0(\mathfrak{p})}, \ldots, \overline{u_N(\mathfrak{p})}) \in \mathfrak{G}_s(k(s)) \subset \mathbf{P}_{k(s)}^N(k(s))$$

où $x=(u_0(\mathfrak{p}), \ldots, u_N(\mathfrak{p}))$ est une écriture de x satisfaisant (ii) de la proposition 3.

4. Application à « la transcendance »

PROPOSITION 5. *Soient R un sous-anneau de $\mathbf{C}$ de type fini sur $\mathbf{Z}$, $K=\mathrm{Fr}\,R\subset\mathbf{C}$, G un groupe algébrique commutatif connexe sur K de dimension d qui est ouvert dense d'un fermé G_1 de $\mathbf{P}^N_K=\mathrm{Proj}\,K[X_0,\dots,X_N]$. On peut supposer que $D_+(X_0)\cap G$ est dense dans G et que $(X_1/X_0)|_{G\cap D_+(X_0)},\dots,(X_d/X_0)|_{G\cap D_+(X_0)}$ sont algébriquement indépendantes sur K. Enfin soient $G(K)$ le groupe des points de G rationnels sur K, et $x_1,\dots,x_\ell\in G(K)$.*

Alors il existe $a\in R-\{0\}$ avec les propriétés suivantes.

(1) *Pour tout homomorphisme $\varphi: R\to\mathbf{C}$ tel que $\varphi(a)\neq 0$, il existe un groupe algébrique G_φ sur $k(\varphi)\overset{\text{déf}}{=}\mathrm{Fr}\,(\varphi(R))$ de dimension d. C'est un ouvert dense d'un fermé de $\mathbf{P}^N_{k(\varphi)}$, $D_+(X_0)\cap G_\varphi$ est dense dans G_φ et les fonctions $X_1/X_0,\dots,X_d/X_0$ restreintes à $G_\varphi\cap D_+(X_0)$ sont algébriquement indépendantes sur $k(\varphi)$. Si $\ker\varphi=0$ (i.e. $k(\varphi)\simeq K$), on a $G_\varphi\simeq G$.*

(2) *Soit H le sous-ensemble des points x de $G(K)\subset\mathbf{P}^N_K(K)$ possédant la propriété suivante : pour tout homomorphisme $\varphi: R\to\mathbf{C}$ avec $\varphi(a)\neq 0$, il existe $u_0(\varphi),\dots,u_N(\varphi)\in R$, $i_0=i_0(\varphi)$ avec $\varphi(u_{i_0}(\varphi))\neq 0$,*

$$x=(u_0(\varphi),\dots,u_N(\varphi))\quad(\textit{dans }\mathbf{P}^N_K(K)),\tag{*}$$

enfin l'élément $(\varphi(u_0(\varphi)),\dots,\varphi(u_N(\varphi))$ ne dépend pas de la représentation (*), on le note $\varepsilon_\varphi(x)$. Alors H est un sous-groupe de $G(K)$ qui contient $x_1,\dots,x_\ell$ et pour tout $\varphi: R\to\mathbf{C}$ avec $\varphi(a)\neq 0$ l'application $\varepsilon_\varphi: H\to G_\varphi(k(\varphi))$ est un homomorphisme de groupes.

Démonstration. Comme K est de caractéristique nulle, le groupe algébrique G est régulier (Mumford, p. 101), ainsi on est dans les conditions d'application du théorème 1. Il existe $f\in R-\{0\}$, $\mathfrak{G}$ un schéma en groupes plat sur $S_f=\mathrm{Sp}\,R[1/f]$ avec toutes les propriétés du théorème.

Le point $x_i\in G(K)$ définit un morphisme $\alpha_i: \mathrm{Sp}\,K=\{\xi\}\to G$ par $\alpha_i(\xi)=x_i\in G(K)\subset\mathbf{P}^N_K(K)$ (voir §3.1). Il existe $f_i\in R-\{0\}$ et un morphisme $\varrho_i: \mathrm{Sp}\,R[1/ff_i]\to\mathfrak{G}\times_{S_f}S_{ff_i}$ tel que $\varrho_{i\eta}=\alpha_i$, où $S_{ff_i}=\mathrm{Sp}\,R[1/ff_i]$ et η est le point générique de $S=\mathrm{Sp}\,R$ (EGA, Chapitre IV, Théorème 8.8.2, p. 28).

On sait que $D_+(X_0)\cap G_1$ est un ouvert affine et que la K-algèbre $\mathcal{O}_{G_1}(G_1\cap D_+(X_0))$ est engendrée par

$$(X_1/X_0)|_{G_1\cap D_+(X_0)},\dots,(X_N/X_0)|_{G_1\cap D_+(X_0)}.$$

On a $d=\dim G=\dim G_1$ et $D_+(X_0)\cap G_1$ dense dans G_1, donc $d=\dim D_+(X_0)\cap G_1$. Ainsi on peut supposer que

$$(X_1/X_0)|_{G_1\cap D_+(X_0)},\ldots,(X_d/X_0)|_{G_1\cap D_+(X_0)}$$

sont algébriquement libres sur K, et que $(X_i/X_0)|_{G_1\cap D_+(X_0)}$ est algébriquement lié à

$$(X_1/X_0)|_{G_1\cap D_+(X_0)},\ldots,(X_d/X_0)|_{G_1\cap D_+(X_0)}.$$

Ainsi il existe $f_0\in R-\{0\}$ tel que $(X_i/X_0)|_{G_1\cap D_+(X_0)}$ soit entier sur le sous-anneau de $\mathcal{O}_{G_1}(G_1\cap D_+(X_0))$ engendré par

$$(X_1/X_0)|_{G_1\cap D_+(X_0)},\ldots,(X_d/X_0)|_{G_1\cap D_+(X_0)}$$

sur $R[1/ff_0]$. Il suit de la platitude de $\mathfrak{G}_1$ sur $S_f=\mathrm{Sp}\,R[1/f]$ que $(X_i/X_0)|_{\mathfrak{G}_1\cap D_+(X_0)}$ est entier sur le sous-anneau de

$$\mathcal{O}_{\mathfrak{G}_1}(\mathfrak{G}_1\cap D_+(X_0))\otimes_{R[1/f]}R[1/ff_0]$$

engendré par

$$(X_1/X_0)|_{\mathfrak{G}_1\cap D_+(X_0)},\ldots,(X_d/X_0)|_{\mathfrak{G}_1\cap D_+(X_0)}\quad\text{et}\quad R[1/f]\otimes R[1/ff_0].$$

Soit $a=ff_0f_1\ldots f_\ell$; quitte à changer $\mathfrak{G}$ en $\mathfrak{G}\times_{S_f}S_a$ avec $S_a=\mathrm{Sp}\,R[1/a]$, on peut supposer que $\mathfrak{G}$ est un schéma en groupes plat sur S_a qui satisfait les propriétés du théorème 1. En plus il existe $\varrho_i\colon S_a\to\mathfrak{G}$ tel que $\varrho_{i\eta}(\xi)=x_i$ où $\{\xi\}=\mathrm{Sp}\,K$, η est le point générique de S_a. Ensuite $(X_i/X_0)|_{\mathfrak{G}_1\cap D_+(X_0)}$ est entier sur le sous-anneau de $\mathcal{O}_{\mathfrak{G}_1}(\mathfrak{G}_1\cap D_+(X_0))$ engendré par

$$(X_1/X_0)|_{\mathfrak{G}_1\cap D_+(X_0)},\ldots,(X_d/X_0)|_{\mathfrak{G}_1\cap D_+(X_0)}$$

et $R[1/a]$. Il suit facilement de cela que

$$(X_1/X_0)|_{\mathfrak{G}_s\cap D_+(X_0)},\ldots,(X_d/X_0)|_{\mathfrak{G}_s\cap D_+(X_0)}$$

sont algébriquement indépendants sur $k(s)$ et que $(X_i/X_0)|_{\mathfrak{G}_s\cap D_+(X_0)}$ est entier sur la sous-$k(s)$-algèbre de $\mathcal{O}_{\mathfrak{G}_s}(\mathfrak{G}_s\cap D_+(X_0))$ engendrée par

$$(X_1/X_0)|_{\mathfrak{G}_s\cap D_+(X_0)},\ldots,(X_d/X_0)|_{\mathfrak{G}_s\cap D_+(X_0)},$$

pour tout $s \in S_a$; il suffit d'utiliser le fait que $D_+(X_0) \cap \mathfrak{G}_s$ est dense dans $\mathfrak{G}_s$, que $\mathfrak{G}_s$ est dense dans $\mathfrak{G}_{1s}$ et que $d=\dim \mathfrak{G}_s=\dim \mathfrak{G}_{1s}$ (théorème 1).

Tout homomorphisme $\varphi: R \to \mathbf{C}$ définit l'idéal premier $\mathfrak{p}=\ker\varphi$ de R; comme le degré de transcendance de $\mathbf{C}$ sur $\mathbf{Q}$ est infini, tout idéal premier de R est le noyau d'un homomorphisme $\varphi: R \to \mathbf{C}$. Deux homomorphismes ϱ_1 et ϱ_2 peuvent avoir même noyau, mais dans ce cas $k(\varrho_1) \simeq k(\varrho_2)$. Enfin si $s=\ker\varphi$ on a $k(s)=k(\varphi)=\mathrm{Fr}(\varphi(R))$.

On pose alors $G_\varphi \overset{\text{déf}}{=} \mathfrak{G}_s$, en particulier $G_\varphi=\mathfrak{G}_\eta=G$ si $\ker\varphi=\{0\}$.

Ensuite la proposition 4 et la remarque qui la suit montrent que H n'est autre chose que l'image du groupe $\mathfrak{G}(R[1/a])$ dans $\mathfrak{G}_\eta(k(\eta))=G(K)$ et que $\varepsilon_\varphi=\delta_s$ si $s=\ker\varphi$ (proposition 2). Par ce qui précède on a $\varrho_1, \ldots, \varrho_\ell \in \mathfrak{G}(R[1/a])$, donc $x_1, \ldots, x_\ell \in H$.

Remarque. Si on le souhaite on peut décrire les homomorphismes $\varphi: R \to \mathbf{C}$ tels que $\varphi(a) \neq 0$. Supposons $R=\mathbf{Z}[\theta_1, \ldots, \theta_t][\theta_{t+1}]$ avec $\theta_1, \ldots, \theta_t$ algébriquement indépendants sur $\mathbf{Q}$, et θ_{t+1} algébrique sur $\mathbf{Q}(\theta_1, \ldots, \theta_t)$; alors θ_{t+1} satisfait une relation de la forme $u_0+u_1\theta_{t+1}+\ldots+u_m\theta_{t+1}^m=0$ avec $u_i \in \mathbf{Z}[\theta_1, \ldots, \theta_t]$ et $u_0 u_m \neq 0$. De même a satisfait une relation $v_0+v_1 a+\ldots+v_{m'} a^{m'}=0$ avec $v_i \in \mathbf{Z}[\theta_1, \ldots, \theta_t]$ et $v_0 v_{m'} \neq 0$. Soient $\tilde{\theta}_1, \ldots, \tilde{\theta}_t \in \mathbf{C}$ tels que $u_0 u_m v_0 v_{m'}(\tilde{\theta}_1, \ldots, \tilde{\theta}_t) \neq 0$, alors il existe un homomorphisme $\varphi: R \to \mathbf{C}$ tel que $\varphi(\theta_i)=\tilde{\theta}_i$ pour $1 \leqslant i \leqslant t$ et $\varphi(a) \neq 0$ (en général cet homomorphisme n'est pas unique).

Références

GROTHENDIECK, A. & DIEUDONNÉ, J., Eléments de Géométrie Algébrique, Chapitres I et IV. Publ. Math. IHES, 4 (1960); 24 (1965); 28 (1966).

HARTSHORNE, R., *Algebraic geometry*. Graduate Texts in Math. 52. Springer Verlag, 1977.

MUMFORD, D., *Abelian varieties*. Oxford Univ. Press, 1970.

Received February 16, 1984
Received in revised form March 18, 1985