Applications de la théorie de Kummer à des problèmes de transcendance.

WALDSCHMIDT, M.

pp. 1 - 14

Séminaire de Théorie des Nombres
Année 1978-1979 - exposé n° 22

27 avril 1979

APPLICATIONS DE LA THÉORIE DE KUMMER A DES PROBLÈMES DE TRANSCENDANCE

par

Michel WALDSCHMIDT

-:-:-:-

§.1. - Aperçu historique

Les méthodes transcendantes classiques font intervenir une fonction auxiliaire F, qui est entière ou méromorphe dans $\mathbb{C}$ et non identique à zéro. Un des problèmes qu'il faut résoudre consiste à trouver un point où F ne s'annule pas. De nombreuses techniques ont été développées pour majorer le nombre de zéros de F dans un disque, et en particulier on était souvent amené à montrer qu'un certain déterminant ne s'annulait pas. John Coates a introduit un nouvel argument : il montre que F ne s'annule pas en un point $\frac{1}{\ell}$ pour ℓ premier assez grand, et pour cela il introduit des considérations provenant de la théorie de Kummer.

Le premier exemple qu'il donne [1] concerne une fonction $F(z) = P(\wp(u\,z), \alpha^z)$, où $P \in \mathbb{Z}[X,Y]$, $\wp$ est une fonction elliptique de Weierstrass sans multiplication complexe d'invariants g_2, g_3 algébriques, et $\wp(u)$ et α sont algébriques. Pour avoir $F(\frac{1}{\ell}) \neq 0$, il suffit de minorer le degré du nombre algébrique $\wp(\frac{u}{\ell})$, et pour cela J. Coates utilise un théorème de J. Tate sur le degré du corps des points de division (un énoncé plus général est le théorème de Bashmakov que nous verrons plus loin). Cela lui permet de donner une minoration d'une forme linéaire $\beta_1 u + \beta_2 \log \alpha$, quand les nombres β_1, β_2, α, $\wp(u)$, g_2 et g_3 sont algébriques avec $\alpha \neq 0$ et $\log \alpha \neq 0$ (Th. Schneider avait montré que cette forme linéaire ne s'annule pas quand β_1, β_2 ne sont pas tous les deux nuls).

Le deuxième exemple [2] est celui d'une fonction auxiliaire $P(\wp(\omega_1 z), \wp(\omega_2 z), e^{2i\pi z})$, où ω_1, ω_2 sont deux périodes linéairement indépendantes de $\wp$. Il utilise maintenant un énoncé de Serre sur le degré du corps des points de torsion et en déduit l'indépendance linéaire sur le corps $\bar{\mathbb{Q}}$ des nombres algébriques de 1, ω_1, ω_2, $2i\pi$, quand $\wp$ n'a pas de multiplication complexe. (Cette étude a été poursuivie depuis, notamment par D.W. Masser ; cf. [7], chap. 6.)

La théorie de Kummer usuelle (pour le groupe multiplicatif) est ensuite apparue dans un travail commun de Baker et Stark sur les formes linéaires de logarithmes, puis dans l'article de Baker "Sharpening III" sur le même sujet (voir à ce propos le chapitre 1 de [7]).

En 1972, dans un manuscrit non publié (cité dans [4]), J. Coates avait montré comment le théorème de Baker sur les formes linéaires de logarithmes usuels

$$\beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n, \quad (\alpha_j, \beta_j \text{ algébriques})$$

pourrait être étendu aux formes linéaires de logarithmes elliptiques

$$\beta_1 u_1 + \ldots + \beta_n u_n, \quad (\wp(u_j), \beta_j, g_2, g_3 \text{ algébriques})$$

dans le cas de multiplication complexe, à condition de disposer d'un théorème convenable sur le degré du corps des points de division. Cette propriété du corps de division avait en fait été démontrée par Bashmakov en 1970, et a été étendue aux variétés abéliennes de type C. M. par K. Ribet [3] en 1975. Coates et Lang [4] ont montré comment ces énoncés Kummeriens permettaient de simplifier et de raffiner des résultats antérieurs de D.W. Masser.

Ces arguments sur le degré des points de division ont été utilisés par D. Bertrand [5, 6] dans ses travaux sur les nombres transcendants p-adiques. Il y utilise aussi un énoncé de K. Ribet [5] (appendice) sur le corps $K(\wp(\frac{u}{\ell}), \alpha^{1/\ell})$ pour donner un analogue p-adique du résultat de Coates [1] sur $\beta_1 u + \beta_2 \log \alpha$ mentionné plus haut. Il développe dans [6] une remarque de Cassels qui rend effectif le théorème de Bashmakov-Ribet (voir aussi [8]). Les meilleures minorations actuellement connues pour les formes linéaires de logarithmes elliptiques sont dues à M. Anderson [7] chap. 7, pour la dépendance en la hauteur des coefficients β_j, et à H. Groscot [12] qui a précisé non seulement la dépendance en les hauteurs des $\wp(u_j)$, mais aussi en celles de g_2, g_3, pour l'appliquer à l'étude des points entiers sur une courbe elliptique. G. V. Chudnovsky annonce aussi plusieurs résultats dans cette direction.

Les travaux récents concernent la théorie de Kummer sur des groupes algébriques commutatifs connexes : produit d'une courbe elliptique par le groupe multiplicatif [9], extension non triviale d'une courbe elliptique par le groupe multiplicatif [10], et plus généralement extension d'une variété abélienne par un produit de groupes multiplicatifs [11]. Ces groupes algébriques sont importants pour l'étude des intégrales abéliennes (travaux de M. Laurent sur la transcendance des périodes d'intégrales elliptiques de troisième espèce notamment).

§.2. - Le groupe multiplicatif

Dans toute la suite K désigne un corps de nombres, et n un entier positif (non nécessairement premier).

a) Torsion

Soit ζ une racine primitive n-ième de l'unité. Notons $K_n = K(\zeta)$ l'extension cyclotomique correspondante. Alors K_n est une extension galoisienne de K ; soit $\sigma \in \mathrm{Gal}(K_n/K)$; il existe un entier $a \in \mathbb{Z}$ tel que $\sigma(\zeta) = \zeta^a$. Cet entier est bien déterminé modulo n, et sa classe dans $\mathbb{Z}/n\mathbb{Z}$ est inversible. On obtient

ainsi un homomorphisme injectif

$$\mathrm{Gal}(K_n/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^* .$$

Comme le sous-groupe de torsion de K^* est fini, il existe un entier M tel que si n est un entier positif premier à M on ait :

$$\mathrm{Gal}(K_n/K) \simeq (\mathbb{Z}/n\mathbb{Z})^* .$$

b) Division

Soient $a \in K^*$, n un entier positif, μ_n le groupe des racines n-ièmes de l'unité, $K_n = K(\mu_n)$, et θ un nombre algébrique sur K tel que $\theta^n = a$. La théorie classique de Kummer a pour point de départ l'homomorphisme injectif

$$\begin{aligned} \mathrm{Gal}(K_n(\theta)/K_n) &\hookrightarrow \mu_n \\ \sigma &\longmapsto \frac{\sigma\theta}{\theta} . \end{aligned}$$

De manière plus générale, si $a_1, \ldots, a_r$ sont des éléments de K^*, on a un homomorphisme injectif du groupe de Galois H de $K_n(a_1^{1/n}, \ldots, a_r^{1/n})$ sur K_n dans μ_n^r, qui envoie $\sigma \in H$ sur $(\zeta_1, \ldots, \zeta_r)$, où $\zeta_j = (\sigma(a_j^{1/n}))/(a_j^{1/n})$, où $a_j^{1/n}$ désigne une racine n-ième quelconque (choisie une fois pour toutes) de a_j. Il est clair que si cet homomorphisme est surjectif, alors $a_1, \ldots, a_r$ sont multiplicativement indépendants. Nous étudions la réciproque.

PROPOSITION 1. - Soient $a_1, \ldots, a_r$ des éléments multiplicativement indépendants de K^*. Il existe un entier M tel que si n est un entier positif premier à M, l'homomorphisme

$$\begin{aligned} H = \mathrm{Gal}(K_n(a_1^{1/n}, \ldots, a_r^{1/n})/K_n) &\hookrightarrow \mu_n^r \\ \sigma &\longmapsto (\zeta_1, \ldots, \zeta_r) \end{aligned}$$

soit un isomorphisme.

Il est important pour les applications de préciser le nombre M. Pour cela notons Γ le sous-groupe de K^* engendré par $a_1, \dots, a_r$, et Γ' le groupe de division de Γ dans K^* :

$$\Gamma' = \{ a \in K^* \ ; \text{ il existe } m \in \mathbb{Z},\ m \neq 0 \text{, tel que } a^m \in \Gamma \} .$$

Alors Γ est d'indice fini dans Γ', et on peut choisir

$$M = 2(\Gamma' : \Gamma) .$$

Indiquons la démonstration de ce dernier point dans le cas particulier où $K_n = K$. Remarquons d'abord que $\Gamma^n = \Gamma \cap K^{*n}$. En effet, soit $\gamma \in \Gamma \cap K^{*n}$; comme $\gamma \in K^{*n}$, il existe $\beta \in K^*$ tel que $\gamma = \beta^n$. Alors $\beta \in \Gamma'$, donc $\beta^h \in \Gamma$ pour $h = (\Gamma' : \Gamma)$. Comme $(n, h) = 1$, on en déduit $\beta \in \Gamma$, donc $\gamma \in \Gamma^n$. Par conséquent :

$$\Gamma / \Gamma^n = \Gamma / (\Gamma \cap K^{*n}) \simeq \Gamma K^{*n} / K^{*n} .$$

L'application bilinéaire

$$\begin{aligned} H \times \Gamma K^{*n} &\longrightarrow \mu_n \\ (\sigma, a) &\longmapsto \frac{\sigma a^{1/n}}{a^{1/n}} \end{aligned}$$

a un noyau à gauche trivial et un noyau à droite K^{*n}.

Un théorème de dualité des groupes abéliens (cf. par exemple S. Lang, Algebra, chap. I, §.11, th. 10) montre que l'ordre de H est égal à l'indice de K^{*n} dans ΓK^{*n}. Mais $(\Gamma K^{*n} : K^{*n}) = (\Gamma : \Gamma^n) = n^r$ donc l'homomorphisme injectif $H \hookrightarrow \mu_n^r$ est aussi surjectif.

Quand on ne suppose pas $\mu_n \subset K$, tout le problème est de démontrer $\Gamma \cap K_n^{*n} = \Gamma^n$ (cf. [8] chap. V, §.4, th. 4.1).

Pour utiliser la proposition 1, il reste donc à majorer le plus grand facteur premier de $(\Gamma' : \Gamma)$. En fait c'est l'exposant du groupe Γ'/Γ que nous allons majorer, en développant une remarque de Cassels. Définissons d'abord une hauteur sur K : soit $\{v\}$ l'ensemble des valeurs absolues de K normalisées de telle manière que

$$\prod_v |\alpha|_v^{n_v} = 1 \qquad \text{pour } \alpha \in K^* ,$$

n_v étant le degré local en v. Pour $\alpha \in K^*$ on pose

$$H_K(\alpha) = \prod_v \max\{1, |\alpha|_v^{n_v}\} .$$

Nous utiliserons les propriétés suivantes [8] :

$$H_K(\alpha_1 \dots \alpha_\ell) \leq H_K(\alpha_1) \dots H_K(\alpha_\ell)$$

$$H_K(\alpha^m) = H_K(\alpha)^m \qquad \text{pour } m \in \mathbb{Z}, m \neq 0 .$$

De plus si $\alpha \in K^*$ n'est pas une racine de l'unité, on a

$$H_K(\alpha) \geq C_o > 1$$

où C_o ne dépend que de $[K:\mathbb{Q}]$ (les meilleures estimations connues de C_o sont dues à E. Dobrowolski ; cf. l'exposé de C. L. Stewart le 20 septembre 1978, sur le problème de Lehmer).

PROPOSITION 2. - Soient K un corps de nombres, $\alpha_1, \dots, \alpha_r$ des éléments multiplicativement indépendants de K^*, Γ le sous-groupe de K^* engendré par $\alpha_1, \dots, \alpha_r$ et par les racines de l'unité de K, et Γ' le groupe de division de Γ dans K :

$$\Gamma' = \{\alpha \in K^* \ ; \text{ il existe } m \in \mathbb{Z}, m \neq 0, \text{ tel que } \alpha^m \in \Gamma\} .$$

Alors l'exposant N de Γ'/Γ vérifie

$$\varphi(N) \leq C_1 (h_1 + \dots + h_r)^r ,$$

où φ est l'indicatrice d'Euler, $h_j = \log H_K(\alpha_j)$, $(1 \leq j \leq r)$, et C_1 est une constante facilement calculable ne dépendant que du degré $[K:\mathbb{Q}]$.

Démonstration (cf. [8], chap. IV, §.5, th. 5.1) - Soit $\alpha \in \Gamma'$ et soit m le plus petit entier positif tel que $\alpha^m \in \Gamma$:

$$\alpha^m = \alpha_1^{m_1} \dots \alpha_r^{m_r} \zeta ,$$

où ζ est une racine de l'unité. Il s'agit de majorer m.

Grâce au principe des tiroirs, il existe un nombre q premier à m tel que pour $1 \leq j \leq r$ on ait :

$$\| q m_j / m \| \leq C_2 \, \varphi(m)^{-1/r}, \quad (C_2 \text{ constante absolue})$$

(la double barre est la distance à l'entier le plus proche). On obtient ainsi des entiers $s_1, \ldots, s_r$, tels que

$$|q m_j - m s_j| \leq C_2 \, m \, \varphi(m)^{-1/r}, \quad (1 \leq j \leq r) .$$

Comme m a été choisi minimal, les nombres $m, m_1, \ldots, m_r$ sont premiers entre eux dans leur ensemble, donc les entiers $n_j = q m_j - m s_j$, $(1 \leq j \leq r)$ ne sont pas tous nuls. Le nombre $\beta \in K^*$ défini par

$$\alpha_1^{n_1} \ldots \alpha_r^{n_r} \cdot \zeta' = \beta^m$$

(ζ' racine de l'unité) n'est donc pas une racine de l'unité. Grâce aux propriétés de H_K on en déduit

$$C_o^m \leq (H_K(\alpha_1) \ldots H_K(\alpha_r))^{|n|}$$

avec

$$|n| = \max_{1 \leq j \leq r} |n_j| \leq C_2 \, m \, \varphi(m)^{-\frac{1}{r}},$$

d'où

$$\varphi(m) \leq C_1 (h_1 + \ldots + h_r)^r .$$

En étant plus soigneux, on peut démontrer le résultat plus précis suivant qui permet, pour les minorations de formes linéaires, de se ramener au cas où les logarithmes sont $\mathbb{Q}$-linéairement indépendants.

PROPOSITION 3.- Soient K un corps de nombres de degré D sur $\mathbb{Q}$, $\ell_1, \ldots, \ell_m$ des nombres complexes $\mathbb{Q}$-linéairement dépendants tels que $\alpha_j = e^{\ell_j} \in K$, $(1 \leq j \leq m)$. Alors il existe des entiers rationnels $b_1, \ldots, b_m$, non tous nuls, tels que :

$$b_1 \ell_1 + \ldots + b_m \ell_m = 0$$

avec :

$$|b_k| \leq (9(m-1) D^2)^{m-1} \, V_1 \ldots V_m / V_k, \quad (1 \leq k \leq m),$$

où

$$V_j = \max \{ \log H_K(\alpha_j), |\ell_j| \}, \qquad (1 \leq j \leq m) .$$

En appliquant ce résultat au cas $m=2$, $\ell_1 = \log \alpha$, $\ell_2 = \ell_1/m$, on en déduit le corollaire suivant :

COROLLAIRE 4. - Soient K un corps de nombres de degré D, α un élément non nul de K, $\log \alpha$ une détermination non nulle du logarithme de α. Soit n un entier positif tel que le nombre

$$\alpha^{\frac{1}{n}} = \exp(\tfrac{1}{n} \log \alpha)$$

appartienne à K. Alors

$$n \leq 9\, D^2 \max \{\log H_K(\alpha), |\log \alpha|\} .$$

Plus précisément, si α est une racine de l'unité on a :

$$n \leq \frac{1}{2\pi}\, \varphi_{-1}(D)\ |\log \alpha|$$

où

$$\varphi_{-1}(D) = \max \{N \geq 1,\ \varphi(N) \leq D\} ,$$

(donc $\varphi_{-1}(D) \leq 2D^2$ et $\varphi_{-1}(D) \leq 4D \log\log(6D)$) ; si α est une unité mais pas une racine de l'unité on a

$$n \leq \Phi(D)\ \log \max\{|\alpha|, |\alpha^{-1}|\} ,$$

où $\Phi(D)$, qui apparaît dans le problème de Lehmer, vérifie grâce à Dobrowolski

$$\Phi(D) \leq 6\, D^2 (\log D)^{-1} \qquad \text{pour } D \geq 2 ,$$

$$\Phi(D) \leq 600\ D (\frac{\log D}{\log\log D})^3 \quad \text{pour } D \geq 3 ,$$

et

$$\Phi(D) \leq (\frac{1}{2} + \varepsilon)\, D (\frac{\log D}{\log\log D})^3 \quad \text{pour } D \geq D_o(\varepsilon) .$$

Enfin si α n'est pas une unité on a :

$$n \leq \frac{1}{\log 2} \log |N_{K/\mathbb{Q}}(\alpha \text{ den } \alpha)| .$$

§.3. - Courbes elliptiques

Soient E une courbe elliptique définie sur un corps de nombres K, $\mathcal{O} = \mathrm{End}\, E$ son anneau d'endomorphismes, et $k = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$ son corps d'endomorphismes. Si E admet des multiplications complexes, c'est-à-dire si $k \neq \mathbb{Q}$, alors k est un corps quadratique imaginaire et on suppose $k \subset K$. Si P est un point complexe sur la courbe on note $K(P)$ le corps obtenu en adjoignant à K les coordonnées de P. On note $E(K)$ le groupe des points P qui sont K rationnels sur la courbe, c'est-à-dire tels que $K(P) = K$.

a) Torsion

Soient n un entier positif, E_n le noyau de l'endomorphisme de E multiplication par n, et $K(E_n) = K_n$ le corps obtenu en adjoignant à K les coordonnées des points de E_n. Alors l'extension K_n/K est galoisienne. Soit $\sigma \in \mathrm{Gal}(K_n/K)$, et soit $P \in E_n$; alors $\sigma P - P \in E_n$. On définit ainsi une opération de $\mathrm{Gal}(K_n/K)$ sur E_n, ce qui donne un homomorphisme injectif

$$\mathrm{Gal}(K_n/K) \hookrightarrow \mathrm{Aut}\, E_n .$$

Si on représente $E(\mathbb{C})$ comme un quotient $\mathbb{C}/\Omega$ où $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ est un réseau de $\mathbb{C}$, alors E_n est l'image du réseau

$$\frac{1}{n}\Omega = \mathbb{Z}\frac{\omega_1}{n} + \mathbb{Z}\frac{\omega_2}{n} ,$$

donc :

$$E_n \simeq \frac{\frac{1}{n}\Omega}{\Omega} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}} ,$$

et

$$\mathrm{Aut}\, E_n \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) .$$

Quand il y a multiplication complexe, la théorie du corps de classes (Hasse, Deuring) permet de préciser l'image de $\mathrm{Gal}(K_n/K)$: il existe un entier M tel que si n est un entier positif premier à M, alors

$$\mathrm{Gal}(K_n/K) \simeq (\mathcal{O}/n\mathcal{O})^* .$$

Supposons que n est un nombre premier ℓ qui ne se ramifie pas dans k ; soit $\psi(\ell) = [K_\ell : K]$. Alors

$$\psi(\ell) = \begin{cases} o(F_{\ell^2}^*) = \ell^2 - 1 & \text{si } \ell \text{ est premier dans } k \\ o(F^{*2}) = (\ell-1)^2 & \text{si } \ell \text{ est décomposé dans } k . \end{cases}$$

Supposons maintenant que E n'admet pas de multiplication complexe : $\mathcal{O} = \mathbb{Z}$. La structure de $\mathrm{Gal}(K_n/K)$ n a été déterminée qu'en 1972, par J.-P. Serre : il existe un entier M tel que si n est un entier positif premier à M, on ait :

$$\mathrm{Gal}(K_n/K) \simeq GL_2(\mathbb{Z}/n\mathbb{Z}) ,$$

autrement dit tel que l'homomorphisme précédent $\mathrm{Gal}(K_n/K) \hookrightarrow \mathrm{Aut}(E_n)$ soit un isomorphisme. Si n est un nombre premier ℓ ne divisant pas M, et si $\psi(\ell) = [K_\ell : K]$, on a alors :

$$\psi(\ell) = \ell(\ell-1)(\ell^2-1) .$$

C'est ce résultat qu'utilise J. Coates dans [2]. Une autre application du travail de J.-P. Serre a été donnée par P. Liardet dans sa thèse (Marseille, 1975). Pour énoncer le résultat de Liardet, notons G_n l'image de $\mathrm{Gal}(K_n/K)$ dans $\mathrm{Aut}(E_n)$, et Δ_n l'image de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $\mathrm{Aut}(E_n)$ (le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ agit de manière évidente sur E_n).

THÉORÈME 5 (P. Liardet). - Soit E une courbe elliptique définie sur un corps K de type fini sur $\mathbb{Q}$. Il existe un entier $C = C(E, K) \geq 1$ tel que pour tout entier $n \geq 1$ on ait :

$$(\Delta_n : G_n \cap \Delta_n) \leq C .$$

Il en déduit que si A est une variété abélienne isogène à une puissance d'une courbe elliptique, et si V est une courbe dans A dont l'intersection avec le sous-groupe de torsion de A est infinie, alors V est translatée d'un sous-groupe de A. Cet énoncé résout un cas particulier d'une conjecture de Lang.

b) Division

L'analogue elliptique de la proposition 1 est donné par le théorème de Bashmakov :

THÉORÈME 6 (Bashmakov). - Soit Γ un sous-groupe de $E(K)$ libre de rang r sur $\mathcal{O}$; il existe un entier M tel que si n est un entier positif premier à M, on ait :

$$\mathrm{Gal}(K_n(\tfrac{1}{n}\Gamma)/K_n) \simeq E_n^r$$

(on a noté $\frac{1}{n}\Gamma = \{P \in E(\mathbb{C}),\ nP \in \Gamma\}$).

On en déduit, sous les hypothèses du théorème,

$$[K_n(\tfrac{1}{n}\Gamma) : K_n] = n^{2r}.$$

Pour tout entier positif n on a un homomorphisme injectif du groupe de Galois dans E_n^r de la manière suivante : soit $P_1, \ldots, P_r$ une base de Γ sur $\mathcal{O}$; à $\sigma \in \mathrm{Gal}(K_n(\frac{1}{n}\Gamma)/K_n)$ on associe :

$$(\sigma Q_1 - Q_1, \ldots, \sigma Q_r - Q_r) \in E_n^r,$$

où, pour $1 \leq j \leq r$, Q_j est un point tel que $nQ_j = P_j$.

On montre alors (cf. [7] appendice du chap. 7, [8] chap. V, §. 5, ainsi que [3]) que cet homomorphisme est surjectif dès que les conditions suivantes sont simultanément réalisées : n est premier à $2(\Gamma' : \Gamma)$ où Γ' est le groupe de division de Γ dans $E(K)$:

$$\Gamma' = \{Q \in E(K) \ ;\ \text{il existe } m \in \mathbb{Z},\ m \neq 0 \text{ tel que } mQ \in \Gamma\},$$

et de plus :

a) si E n'a pas de multiplication complexe, on suppose

$$\mathrm{Gal}(K_n/K) \simeq GL_2(\mathbb{Z}/n\mathbb{Z})$$

b) dans le cas de multiplication complexe on suppose

$$\begin{cases} \mathrm{Gal}(K_n/K) \simeq (\mathcal{O}/n\mathcal{O})^* \\ \mathcal{O}/n\mathcal{O} = \dfrac{\mathbb{Z}}{n\mathbb{Z}}\,[(\mathcal{O}/n\mathcal{O})^*] \\ n \text{ premier au conducteur de } \mathcal{O} \text{ et au discriminant de } k. \end{cases}$$

Pour appliquer le théorème de Bashmakov il reste alors à majorer l'exposant de Γ'/Γ en utilisant la remarque de Cassels (analogue elliptique de la proposition 2 ; cf. [6], §.2.4, prop. 4, [8] chap. IV, §. 5, prop. 5.3, et [12]). On utilise pour cela la hauteur de Néron-Tate. L'analogue elliptique du problème de Lehmer a été étudié par M. Anderson dans le cas de multiplication complexe (cf. l'exposé de D.W. Masser aux Journées Arithmétiques de Luminy, Astérisque n° 61, p. 145-154).

§.4. - Groupes algébriques

Le théorème de Bashmakov a été étendu aux variétés abéliennes de type C.M. par K. Ribet en 1975 [3], aux produits d'une courbe elliptique par le groupe multiplicatif par D. Bertrand [9], aux extensions non triviales d'une courbe elliptique par le groupe multiplicatif par K. Ribet [10], et à une classe très vaste d'extensions de variétés abéliennes par un produit de groupes multiplicatifs (comprenant en particulier le cas où la variété abélienne est de type C.M.) par K. Ribet [11].

Soient V un groupe algébrique commutatif défini sur un corps de nombres K, n un entier positif, V_n le noyau de la multiplication par n, et $P_1, \ldots, P_r$ des points de V rationnels sur K ; on note $K_n = K(V_n)$; on a alors comme précédemment un homomorphisme injectif

$$\mathrm{Gal}(K_n(\tfrac{1}{n}P_1, \ldots, \tfrac{1}{n}P_r)/K_n) \hookrightarrow V_n^r$$

et le problème consiste à montrer que cet homomorphisme est surjectif dès que tous les facteurs premiers de n sont suffisamment grands. Il faut évidemment faire une hypothèse sur l'indépendance de $P_1, \ldots, P_r$. Cette hypothèse [11] fait intervenir la description de V comme extension d'une variété abélienne A par une variété linéaire qu'on suppose déployée (c'est-à-dire isomorphe à un produit $\mathbb{G}_m^s$ de groupes multiplicatifs). L'extension V de A par $\mathbb{G}_m^s$ définit s points $Q_1, \ldots, Q_s$ sur la variété $A^\vee$ duale de A. On considère alors un quotient maximal

W de V tel que $W \simeq A \times G_m^{s'}$ (avec $0 \leq s' \leq s$), et on considère les images de $P_1, \ldots, P_r$ par la surjection canonique $V \longrightarrow W$, et les images de $Q_1, \ldots, Q_r$ par l'injection $\hat{A} \longrightarrow W$ déduite d'une isogénie (sur K) entre A et sa variété abélienne duale $\hat{A}$. On peut ainsi faire agir $\mathrm{End}_K W$ sur les P_i et les Q_j. L'hypothèse est alors que toute relation

$$a_1 P_1 + \ldots + a_r P_r = b_1 Q_1 + \ldots + b_s Q_s$$

avec $a_1, \ldots, a_r, b_1, \ldots, b_s \in \mathrm{End}_K W$ implique $a_1 = \ldots = a_r = 0$.

-:-:-:-

REFERENCES

[1] John COATES, An application of the division theory of elliptic functions to diophantine approximation, Invent. Math., 11 (1970), 167-182.

[2] John COATES, Linear forms in the periods of the exponential and elliptic functions ; Invent. Math., 12 (1971), 290-299.

[3] Ken RIBET, Dividing rational points on abelian varieties of C. M. type, Compositio Math., 33 (1976), 69-74.

[4] John COATES and Serge LANG, Diophantine approximation on abelian varieties with complex multiplication, Invent. Math., 34 (1976), 129-133.

[5] Daniel BERTRAND, Sous-groupes à un paramètre p-adique de variétés de groupe, Invent. Math., 40 (1977), 171-193.

[6] Daniel BERTRAND, Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe, Compositio Math., 37 (1978), 21-50.

[7] Transcendence theory : advances and applications ; ed. Alan BAKER and David W. MASSER, Academic Press, 1977.

[8] Serge LANG, Elliptic curves diophantine analysis, Grund. der math. Wiss., 231, Springer-Verlag, 1978.

[9] Daniel BERTRAND, Kummer theory on the product of an elliptic curve by the multiplicative group, manuscrit, 1979.

[10] Ken RIBET, Kummer theory on extensions of an elliptic curve by the multiplicative group, manuscrit, 1979.

[11] Ken RIBET, Kummer theory on extensions of abelian varieties by tori, manuscrit, 1979.

[12] Herbert GROSCOT, Points entiers sur des courbes elliptiques, Thèse de troisième cycle (Paris VI), 1979.

(texte reçu le 11 mai 1979)

-:-:-:-

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