Astérisque

D. BERTRAND

Hauteurs et isogénies

Astérisque, tome 183 (1990), p. 107-125

<http://www.numdam.org/item?id=AST_1990__183__107_0>

Société Mathématique de France
Astérisque 183 (1990)

HAUTEURS ET ISOGÉNIES

par D. BERTRAND

Théorème (Masser-Wüstholz) : *soit* d *un entier* ≥ 1 . *Il existe un nombre réel* c(d) *effectivement calculable en fonction de* d *et une constante universelle effective* C *vérifiant la propriété suivante . Soient* E *une courbe elliptique définie sur un corps de nombres* k *de degré* d *sur* $\mathbf{Q}$, *et* γ *un majorant* ≥ 1 *des hauteurs logarithmiques des coefficients d'une équation de Weierstrass de* E *sur* k . *Pour toute courbe elliptique* E' *définie sur* k *et* k-*isogène à* E , *il existe une* k-*isogénie de* E' *vers* E *de degré majoré par* $c(d)\,\gamma^{C}$.

On trouvera une démonstration de cet énoncé dans [M-W2]. L'esquisse qu'en donne [Ma4] fournit 4 pour valeur de la constante C .

Nous donnons ici la preuve d'une version affaiblie de ce théorème: l'expression c(d) est remplacée par une fonction c(k) du corps k , effectivement calculable en termes de d et de la valeur absolue δ du *discriminant* de k sur $\mathbf{Q}$. Notre démarche suit celle de [Ma4], mais paraît, par certains aspects, mieux adaptée à d'éventuelles généralisations. Et on verra en fait (appendice A) qu'au prix d'une perte significative sur C , le théorème ci-dessus découle de la démonstration de sa version affaiblie : en d'autres termes, les données δ et γ sont intimement liées.

La démonstration comporte trois parties : la première, de nature essentiellement algébrique, consiste à décrire l'isogénie ϕ qui lie *a priori* E' à E dans un modèle de Weierstrass de E' dépendant de façon logarithmique de son degré N ; la dernière met en jeu la méthode de Baker qui, sous la forme rénovée que lui donnent les lemmes de zéros, fournit alors (modulo une réduction standard expliquée dans la deuxième partie) une isogénie de E' vers E de degré majoré par un monôme en Log N . Si on a pris soin de choisir ϕ de degré minimal , N

est alors bien borné !

Le théorème fournit une version effective d'un classique théorème d'irréductibilité dû à Serre ([Se], IV, 2.1). Nous renvoyons à [Ma4] pour ses applications les plus marquantes, et à l'appendice C du présent texte pour son lien avec [Ra].

§1 Préparatifs

On reprend les hypothèses du théorème, et on considère une k-isogénie ϕ d'une courbe elliptique E'/k vers E , dont on note N le degré. On désigne par C_1, C_2, ... des nombres réels > O effectivement calculables en fonction de d et de δ . Enfin, toutes les hauteurs sont logarithmiques.

Proposition 1: *il existe deux* k-*formes différentielles de 1ère espèce* ω (resp. ω')*sur* E (resp. E') *vérifiant les propriétés suivantes:*
i) $g_2(E,\omega)$ *et* $g_3(E,\omega)$ *sont des éléments de* k *de hauteurs majorées par* $C_1\gamma$;
ii) $\phi^*\omega = \beta\omega'$, *où* β *est un élément de* k *de hauteur* $\leq C_2$ LogN ;
iii) $g_2(E',\omega')$ *et* $g_3(E',\omega')$ *sont des éléments de* k *de hauteurs majorées par* $\gamma' = C_3(\gamma + \text{LogN})$.

Corollaire : *même énoncé avec* $\beta = 1$ (remplacer ω' par $\beta\omega'$).

Démonstration : Soient **E** , **E'** les modèles de Néron de E , E' sur l'anneau *O* des entiers de k . Pour clarifier les idées, je décris tout d'abord la démonstration dans le cas où *O* est principal. Les *O*- modules ω_E (image réciproque de $\Omega^1_{E/O}$ par la section nulle) et $\omega'_{E'}$ sont alors libres. J'en fixe des générateurs ω , ω' : ils ne sont définis qu'aux unités de k près, et c'est sur elles qu'on va jouer.

i) Sans perte de généralité, on peut supposer que l'équation de Weierstrass de E donnée par l'énoncé du théorème a des coefficients entiers (chasser les dénominateurs, qui sont majorés par $\exp(C_4\,\gamma)$).

Son discriminant est alors un élément de O de norme $\leq \exp(C_5\,\gamma)$, et il en est de même de $\Delta(E,\omega)$, qui le divise, et est bien entier en vertu des propriétés d'intégralité de la forme modulaire Δ (cf. [Ka], §1, dont je rappelle d'ailleurs le principe plus loin). Il existe donc (Dirichlet) une unité ε de k telle que $\Delta(E, \omega/\varepsilon) = \varepsilon^{12}\,\Delta(E, \omega)$ soit de hauteur $\leq C_6\gamma$. La forme différentielle ω/ε (que nous convenons de rebaptiser ω) répond alors à la question.

ii) Les isogénies s'étendant aux modèles de Néron (voir [Ra]), $\phi^*\omega$ est une section de $\omega_{E'}$, et il existe un élément β de O tel que $\phi^*\omega = \beta\omega'$. Le même raisonnement, appliqué à l'isogénie duale ϕ' de ϕ, fournit un élément β' de O tel que $\phi'^*\omega = \beta'\omega$. Mais alors, $\beta'\beta\omega = (\phi\phi')^*\omega = N\omega$, et l'entier rationnel $\mathrm{Norm}_{k/\mathbb{Q}}\beta$ divise N^d. Il existe donc une unité ε' de k telle que $\beta\varepsilon'$ soit de hauteur majorée par $C_7 \mathrm{Log} N$, et la forme différentielle ω'/ε' (que nous rebaptiserons ω') vérifie ii).

iii) Montrons tout d'abord que $g_2(E', \omega')$ et $g_3(E', \omega')$ sont essentiellement des entiers de k. Il suffira alors, pour borner leurs hauteurs, de majorer leurs différentes valeurs absolues archimédiennes.

Si v est une place finie de k première à 6, g_2 et g_3, qui sont des formes modulaires entières sur O_v (cf. [Ka1, §1), prennent des valeurs dans O_v dès que ω' engendre $\omega_{E'}$ localement en v. Idem aux places divisant 6, à des dénominateurs universellement bornés près. Les dénominateurs de $g_2(E', \omega')$ et $g_3(E', \omega')$ divisent donc un entier $C_8(k)$.

Passons aux places archimédiennes de k, que nous allons traiter suivant les techniques modulaires de [Ma1], §3 et [Ma3]. Soit v l'une d'elles. Désignons, pour tout réseau Λ de $\mathbf{C}$, par $\varpi(\Lambda)$ le minimum des valeurs absolues de ses éléments non nuls. Comme toute forme modulaire pour $SL_2(\mathbf{Z})$, soit f, de poids $w(f)$, est par définition bornée sur le domaine fondamental usuel, la fonction de réseaux $|f(\Lambda)|\,\varpi(\Lambda)^{w(f)}$

est bornée supérieurement. Les réseaux de périodes Λ_v , Λ'_v de ω et de ω' qui correspondent à v vérifiant $\beta^{-1}\Lambda'_v \subseteq \Lambda_v$, donc en particulier $\varpi(\Lambda'_v) \geq |\beta|_v \varpi(\Lambda_v)$, on en déduit :

$$\sup\{|g_2(\Lambda'_v)|_v^{1/2} , |g_3(\Lambda'_v)|_v^{1/3}\} \leq c\ |\beta|_v^{-2}\ \varpi(\Lambda_v)^{-2} ,$$

où c est une constante universelle, d'où, grâce à la majoration de la hauteur de β fournie par i) :

$$\text{Log}\ \sup\{|g_2(E',\omega')|_v^{1/2} , |g_3(E',\omega')|_v^{1/3}\} \leq C_9(\text{LogN} - \text{Log}\ \varpi(\Lambda_v)) .$$

Il reste à minorer $\varpi(\Lambda_v)$ en fonction de γ . Pour cela, complétons l'un des éléments ω_1 de Λ_v qui donne $\varpi(\Lambda_v)$ en une base directe $\{\omega_1, \omega_2=\tau\omega_1\}$ de ce réseau, de sorte que (Hermite) $\text{Im}\tau$ est $\geq \sqrt{3}/2$. La connaissance des zéros des fonctions $E_4(\tau)$ et $E_6(\tau)$ dans ce domaine entraîne que l'expression

$$\sup\{|g_2(\Lambda_v)|^{1/2} , |g_3(\Lambda_v)|^{1/3}\}\ \varpi(\Lambda_v)^2$$

est universellement minorée, et on déduit de l'inégalité de la taille la minoration : $\text{Log}\ \varpi(\Lambda_v) \geq - C_{10}\gamma$. Предложение доказано (pour O principal).

Pour passer au cas général, il suffit de noter que tout O-module de rang 1 sans torsion admet un sous-O- module libre d'indice majoré par la racine carrée de la valeur absolue du discriminant de k . Grâce aux relations $g_K(E, \lambda\omega) = \lambda^{-2K} g_K(E,\omega)$, les arguments précédents s'adaptent alors aisément en autorisant aux entiers de k qui y apparaissent d'avoir des dénominateurs divisant ces indices.

Remarque: **(i)** La démonstration (à la fois plus simple et plus précise !) que donne [Ma4] du corollaire à la Proposition 1 repose sur la formule suivante. Si Λ' est un sous-groupe d'indice N d'un réseau Λ , le réseau $N\Lambda$ est inclus dans Λ' , et l'on a (d'après Eisenstein) :

$$g_K(\Lambda') = g_K(N\Lambda) + \varepsilon_K \sum_x \wp^{(2K-2)}(x, N\Lambda) ,$$

où x parcourt un système de représentants de $\Lambda'/N\Lambda$, $\wp$ désigne la fonction de Weierstrass usuelle et ε_K est une expression simple. Les