SÉMINAIRE N. BOURBAKI

PIERRE DELIGNE

Preuve des conjectures de Tate et de Shafarevitch

Séminaire N. Bourbaki, 1983-1984, exp. n° 616, p. 25-41.

<http://www.numdam.org/item?id=SB_1983-1984__26__25_0>

Séminaire BOURBAKI
36e année, 1983/84, n° 616 Novembre 1983

PREUVE DES CONJECTURES DE TATE ET DE SHAFAREVITCH
[d'après G. Faltings]

par Pierre DELIGNE

Dans cet exposé, nous expliquons comment G. Faltings prouve la conjecture de Tate (2.7) et celle de Shafarevitch (3.3, 3.4). Nous traitons en détail des propriétés de la "hauteur" d'une variété abélienne, introduite par G. Faltings. C'est la partie la plus technique, et la plus longue, de la preuve. Le lecteur qui, après avoir lu les définitions 1.1, 1.2, est prêt à admettre 1.3, peut passer directement aux paragraphes 2 et 3.

Notations et terminologie

Certains termes seront employés dans un sens restreint :
Corps := corps commutatif.
Corps de nombres := extension finie de $\mathbb{Q}$.
Schéma := schéma noethérien séparé.
Schéma en groupes sur S : toujours de type fini sur S . En général, plat sur S et commutatif.

Pour k un corps, on notera $\overline{k}$ une clôture algébrique de k . Pour A une variété abélienne sur k et ℓ un nombre premier, premier à la caractéristique, on note $T_\ell(A)$ le module de Tate de A : $T_\ell(A) := \lim \text{proj } A_{\ell^n}(\overline{k})$. Il est muni d'une action du groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ et d'une structure de module sur l'anneau $\mathrm{End}(A)$ des k-endomorphismes de A . On pose $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

1. HAUTEURS

1.1. Soient k un corps de nombres et L un espace vectoriel de rang un sur k muni pour chaque place v de k d'une valeur absolue v-adique : $\|\lambda \ell\|_v = \|\lambda\|_v \|\ell\|_v$ pour $\lambda \in k$, $\ell \in L$. On suppose que pour $\ell \in L^* := L - \{0\}$, on a $\|\ell\|_v = 1$ sauf en un nombre fini de places. D'après la formule du produit $\prod \|\lambda\|_v = 1$ pour $\lambda \in k^*$, le produit $\prod_v \|\ell\|_v$ est indépendant du choix de $\ell \in L^*$. On appelle *degré* de $\mathcal{L}$ le logarithme de son inverse :

$$\deg \mathcal{L} := -\log \prod_v \|\ell\|_v .$$

Soit $\mathcal{O}$ l'anneau des entiers de k. Pour v une place de k, on note par v en indice une complétion en v. Une *$\mathcal{O}$-forme* $L_{\mathcal{O}}$ de L, i.e. un $\mathcal{O}$-module projectif de rang un tel que $L_{\mathcal{O}} \otimes_{\mathcal{O}} k \xrightarrow{\sim} L$, fournit pour chaque place finie v de k une valeur absolue v-adique sur L ; transporter à L_v la valeur absolue de k_v par un isomorphisme de k_v-vectoriels $k_v \xrightarrow{\sim} L_v$ qui envoie $\mathcal{O}_v$ sur $L_{\mathcal{O}v}$. Pour $\ell \in L^*$, on a $\|\ell\|_v = 1$ pour presque tout v. Si $\ell \in L_{\mathcal{O}}$,

$$\#(L_{\mathcal{O}}/\mathcal{O}.\ell) = \prod_{v \text{ fini}} \|\ell\|_v^{-1} .$$

Donnons-nous de plus, pour chaque plongement complexe $\iota : k \hookrightarrow \mathbb{C}$, une structure hermitienne (:= une forme hermitienne définie > 0) $< >_\iota$ sur l'espace vectoriel complexe $L_\iota := L \otimes_{k,\iota} \mathbb{C}$. Deux plongements complexes conjugués fournissent des espaces vectoriels L_ι complexes conjugués, et on suppose que pour $\ell \in L_\iota$ on a $\langle \ell, \ell \rangle_\iota = \langle \bar{\ell}, \bar{\ell} \rangle_{\bar{\iota}}$. Si, pour v archimédienne induite par un plongement complexe ι, on pose

$$\|\ell\|_v = \langle \ell, \ell \rangle_\iota^{1/2} \qquad \text{pour } v \text{ réelle,}$$

et

$$\|\ell\|_v = \langle \ell, \ell \rangle_\iota \qquad \text{pour } v \text{ complexe,}$$

on obtient un système de valeurs absolues du type voulu, et $\deg L$ est défini.

Exemple.— Pour $k = \mathbb{Q}$, on a $\mathcal{O} = \mathbb{Z}$ et si e est l'un des deux générateurs $\pm e$ de $L_{\mathbb{Z}}$,

$$\deg L = -\frac{1}{2} \log \langle e, e \rangle .$$

1.2. Soit A une variété abélienne sur un corps k. On note $\omega(A)$ l'espace vectoriel de rang un suivant sur k : si A est de dimension g,

$$\omega(A) := \bigwedge^g ((\mathrm{Lie}\ A)^\vee) .$$

Si k est un corps de nombres, on dispose pour chaque place v de k d'une valeur absolue v-adique naturelle sur $\omega(A)$:

(a) Soient $\mathcal{O}$ l'anneau des entiers de k et $A_{\mathcal{O}}$ le modèle de Néron de A sur $\mathrm{Spec}(\mathcal{O})$. Le $\mathcal{O}$-module projectif de rang un

$$\omega(A)_{\mathcal{O}} := \bigwedge^g ((\mathrm{Lie}\ A_{\mathcal{O}})^\vee)$$

est une $\mathcal{O}$-forme de $\omega(A)$. Il fournit les valeurs absolues cherchées pour les places finies.

(b) Soient $\iota : k \hookrightarrow \mathbb{C}$ un plongement complexe et ιA la variété abélienne sur $\mathbb{C}$ déduite de A par extension des scalaires. L'espace vectoriel complexe $\omega(A)_\iota := \omega(A) \otimes_{k,\iota} \mathbb{C}$ est l'espace des g-formes différentielles holomorphes sur ιA. On le munit de la structure hermitienne pour laquelle

$$\langle \alpha, \alpha \rangle = \frac{1}{(2\pi)^g} \int_{\iota A} |\alpha \wedge \bar{\alpha}| .$$

Ceci fournit les $\| \ \|_v$, pour v archimédien. Faltings utilise $\frac{1}{2^g}|\alpha \wedge \bar{\alpha}|$; peu

importe.

En terme de ces valeurs absolues, on définit la *hauteur* $h(A)$ de A comme étant

$$h(A) := \frac{1}{[k:\mathbb{Q}]} \deg \omega(A) .$$

Exemple.— Pour $k = \mathbb{Q}$, si α est l'un des deux générateurs $\pm\alpha$ de $\omega(A)_{\mathbb{Z}}$ (une *différentielle de Néron*), on a

$$h(A) = -\frac{1}{2} \log\left(\frac{1}{(2\pi)^g} \int_{A(\mathbb{C})} |\alpha \wedge \bar{\alpha}|\right) .$$

Généralisation.— Pour $a : G \to S$ un schéma en groupes plat purement de dimension relative g sur une base S, de section neutre e, on note $\omega(G)$ le faisceau inversible sur S dont le faisceau dualisant relatif est l'image inverse : $Ra^!\mathcal{O}_S = a^*\omega(G)[g]$, $\omega(G) = e^*H^{-g}Ra^!\mathcal{O}_S$. Pour G lisse sur S, on retrouve

$$\omega(G) = \bigwedge^g ((\mathrm{Lie}\ G)^\vee) .$$

Pour k un corps de nombres d'anneau d'entiers $\mathcal{O}$ et $S = \mathrm{Spec}(\mathcal{O})$, si la fibre générale de G est propre sur k, i.e. extension d'un groupe fini par une variété abélienne, l'intégration sur $G(\mathbb{C})$ fournit encore, pour chaque plongement complexe $\iota : k \hookrightarrow \mathbb{C}$, une structure hermitienne sur $\omega(G) \otimes_{k,\iota} \mathbb{C}$. Le degré $\deg \omega(G)$ est donc défini. Le cas G quasi-fini sera utilisé au § 2.

Remarque.— Un schéma en groupes commutatifs plat sur une base S est dit *semi-abélien* si ses fibres sont des extensions de variétés abéliennes par des tores. On dit que A est à *réduction semi-stable* si son modèle de Néron connexe $A^\circ_{\mathcal{O}}$ (de fibres les composantes neutres du modèle de Néron) est semi-abélien. Il revient au même d'exiger que A soit la fibre générale d'*un* schéma semi-abélien sur $\mathrm{Spec}(\mathcal{O})$; ce dernier est unique. Si A est à réduction semi-stable, la formation de $A^\circ_{\mathcal{O}}$ et donc celle de $\omega(A)_{\mathcal{O}} = \omega(A^\circ_{\mathcal{O}})$ commute à une extension des scalaires $k \hookrightarrow k'$, et le facteur $1/[k:\mathbb{Q}]$ dans la définition de $h(A)$ assure que $h(A)$ est invariant par extension des scalaires. Si une variété abélienne A sur k acquiert une réduction semi-stable sur une extension k' de k, on définit la *hauteur géométrique* de A par

$$h_{\mathrm{geom}}(A) := h(A_{k'}) .$$

Du fait que $(A_{\mathcal{O}})_{\mathcal{O}'}$ s'envoie dans $(A_{k'})_{\mathcal{O}'}$, on déduit que $h(A) \geq h_{\mathrm{geom}}(A)$, avec égalité si et seulement si la réduction est semi-stable.

Rappelons qu'une *polarisation* de A est une classe d'équivalence algébrique (définie sur k) de faisceaux inversibles amples sur A. Son *degré* est l'entier $c_1(\mathcal{L})^g/g! = \chi(\mathcal{L})$. Une *polarisation principale* est une polarisation de degré 1.

PROPOSITION 1.3.— *Quels que soient le corps de nombres k, les entiers g et n, et h, il n'y a qu'un nombre fini de classes d'isomorphie de variétés abéliennes polarisées (A,Θ) sur k, de dimension g, de degré de polarisation n et de hauteur $h(A) \leq h$.*

Exemple 1.4 Le cas $k = \mathbb{Q}$, $g = 1$.– Soient E une courbe elliptique sur $\mathbb{Q}$ et ω une différentielle de Néron. La courbe E admet une équation

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

à coefficients entiers, telle que, notant $F(x,y)$ le premier membre, la forme ω soit la forme $dx/F_y = - dy/F_x$. Soit $\Lambda \subset \mathbb{C}$ le réseau tel que (E,ω) soit isomorphe, sur $\mathbb{C}$, à $(\mathbb{C}/\Lambda,dz)$. Soient (ω_1,ω_2) une base positive de Λ , $\tau = \omega_2/\omega_1$ $(\mathrm{Im}(\tau) > 0)$ et $q = \exp(2\pi i\tau)$. On a sur $\mathbb{C}$

$$(E,\omega) \simeq (\mathbb{C}/\Lambda,dz) \simeq \left(\mathbb{C}^*/q^{\mathbb{Z}}, \frac{\omega_1}{2\pi i}\frac{du}{u}\right) .$$

Les nombres

$$c_4 = \left(\frac{\omega_1}{2\pi i}\right)^{-4}(1 + 240\,\Sigma\sigma_3(n)q^n)$$
$$c_6 = -\left(\frac{\omega_1}{2\pi i}\right)^{-6}(1 - 504\,\Sigma\sigma_5(n)q^n)$$

et $\Delta = (c_4^3 - c_6^2)/1728$ sont indépendants du choix de la base (ω_1,ω_2) de Λ . Ce sont des polynômes à coefficients entiers en les a_i (voir par exemple le formulaire de Tate, mis au goût du jour par P. Deligne, dans Anvers IV (Springer Lecture Notes 476)). Ce sont donc des entiers. La courbe E admet l'équation de Weierstrass

$$Y^2 = 4X^3 - \frac{c_4}{12}X - \frac{c_6}{216} .$$

Posons $H(E) = \exp h(E)$ et $H^*(E) = \sup(|c_4|^{1/4},|c_6|^{1/6})$. Pour montrer qu'il n'y a qu'un nombre fini de courbes elliptiques sur $\mathbb{Q}$ à $h(E)$ donné, il suffit de borner $H^*(E)$ en terme de $H(E)$.

Prenons une base (ω_1,ω_2) de Λ avec $|\omega_1|$ minimal. On a alors $\mathrm{Im}(\tau) \geq \sqrt{3}/2$ et

$$H(E) = \left(\frac{1}{\pi}|\omega_1|.|\omega_1\ \mathrm{Im}(\tau)|\right)^{-1/2} = \frac{1}{|\omega_1|}.|\mathrm{Im}(\tau)/\pi|^{-1/2}$$
$$H^*(E) \leq C_0.H(E).\mathrm{Im}(\tau)^{1/2} .$$

Pour $\mathrm{Im}(\tau) > a$ avec $a > 0$, la relation $j = c_4^3/\Delta = q^{-1} + 744 + \ldots$ entre τ et l'invariant modulaire j fournit que $\mathrm{Im}(\tau) \sim \sup(1,\log|j|)/2\pi$. Parce que Δ est entier, on a aussi $|j| \leqslant H^*(E)^{12}$, d'où

$$H^*(E) \leq C_1.H(E).\sup(1,\log H^*(E))^{1/2}$$

et donc

$$H^*(E) \leq C_2.H(E).\sup(1,\log H(E))^{1/2} .$$

Remarque 1.5.– Pour τ dans le demi-plan de Poincaré, soient $y = \mathrm{Im}(\tau)$, $q = \exp(2\pi i\tau)$, $\Lambda(\tau)$ le réseau $\mathbb{Z} \oplus \mathbb{Z}.\tau$, $E(\tau)$ la courbe elliptique $\mathbb{C}/\Lambda(\tau)$, munie de la forme différentielle dz , α la forme différentielle $\alpha = \Delta(E(\tau),dz)^{1/12}.dz$ (peu importe le choix de la racine douzième) et

$$V_0(\tau) = \frac{1}{2\pi}\int_{E(\tau)} |\alpha \wedge \bar{\alpha}| = 4\pi y.|q^{1/12}\textstyle\prod(1 - q^n)^2|^2 .$$

Cette fonction de τ est invariante par $SL(2,\mathbb{Z})$, donc provient d'une fonction $V(j)$ de l'invariant modulaire j . Pour E une courbe elliptique sur k , d'invariant modulaire $j \in k$, posons $H(E) = \exp([k:\mathbb{Q}]h(E))$ (resp.

$H_{geom}(E) = \exp([k:\mathbb{Q}]h_{geom}(E))$. On a

$$H_{geom}(E) = \prod_{\iota:k\hookrightarrow\mathbb{C}} V(\iota j)^{-1/2} \cdot \prod_{v \text{ fini}} \sup(1, \|j\|_v)^{1/12} .$$

La différentielle logarithmique $\partial_\tau \log V(\tau)$ est, à un facteur près, la série d'Eisenstein non holomorphe E_2 ; D. Masser a montré qu'elle ne s'annule que pour $j = 0$ ou $j = 1728$ (Springer, Lecture Notes 437, lemme 3.2). On en déduit que le maximum de $V(j)$ est atteint en $j = 0$ et que le minimum de $h_{geom}(E)$ est atteint par les courbes elliptiques d'invariant modulaire 0 . Ceci fournit le minimum de $h(E)$.

Pour E une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}$ du corps quadratique imaginaire de discriminant $-D$, la formule de Chowla-Selberg (J. Crelle 227(1967), 86-110) donne la valeur de $h_{geom}(E)$: si ε est le caractère de Dirichlet quadratique de conducteur D , on a

$$(\exp h_{geom}(E))^{-2} = \frac{1}{\sqrt{D}} \cdot \Big[\prod_{0<a<D} \Gamma(a/D)^{\varepsilon(a)} \Big]^{w/2h}$$

($w = \#\mathcal{O}^*$, h = nombre de classes). Le cas particulier $D = 3$ fournit la valeur minimum de $h(E)$:

$$h_{min} = -\frac{1}{2}\left\{\log \frac{1}{\sqrt{3}} (\Gamma(1/3)/\Gamma(2/3))^3\right\} = -0.749 .$$

Nous prouverons tout d'abord le lemme suivant, qui suffirait pour les applications.

Lemme 1.6.– *Soit* m *un entier divisible par deux nombres premiers* ≥ 3 . *Il n'y a qu'un nombre fini de classes d'isomorphie de variétés abéliennes principalement polarisées* (A,Θ) *sur* k , *de dimension* g , *munie d'une structure de niveau* m : $\varepsilon : (\mathbb{Z}/(m))^{2g} \xrightarrow{\sim} A_m$ *et de hauteur* $h(A) \leq h$.

Parce que $m \geq 3$, les triples (A,Θ,ε) n'ont pas d'automorphisme non trivial. Les classes d'isomorphie, sur k , de ces triples, s'identifient aux k-points d'un espace de modules M convenable. On prouvera 1.6 en comparant $h(A)$ à la hauteur, en un sens plus classique, du point de M correspondant à (A,Θ,ε) . L'hypothèse sur m assure que A a réduction semi-stable, de sorte que la hauteur est invariante par extension des scalaires.

1.7. Soit X une variété projective sur $\mathbb{Q}$. Un faisceau inversible $\mathcal{L}$ sur X définit une classe mod. $O(1)$ de fonctions hauteur $h_{\mathcal{L}}$ sur $X(\overline{\mathbb{Q}})$. On peut construire une telle fonction comme suit :

(a) On choisit une variété projective $X_{\mathbb{Z}}$ sur $\mathrm{Spec}(\mathbb{Z})$, et un faisceau inversible $\mathcal{L}_{\mathbb{Z}}$ sur $X_{\mathbb{Z}}$, tels que $(X,\mathcal{L})$ se déduise de $(X_{\mathbb{Z}},\mathcal{L}_{\mathbb{Z}})$ par extension des scalaires de $\mathbb{Z}$ à $\mathbb{Q}$.

(b) On choisit une structure hermitienne sur $\mathcal{L}$, i.e. sur le fibré en droites $\mathcal{L}_{\mathbb{C}}$ sur $X(\mathbb{C})$ déduit de $\mathcal{L}$. Pour simplifier, on la suppose invariante par la conjugaison complexe de $(X(\mathbb{C}),\mathcal{L}_{\mathbb{C}})$.

Soient alors k un corps de nombres, d'anneau des entiers $\mathcal{O}$, et $x \in X(k)$.

Parce que $X_{\mathbb{Z}}$ est propre sur $\mathrm{Spec}(\mathbb{Z})$, x se prolonge en $x_{\mathcal{O}} \in X_{\mathbb{Z}}(\mathcal{O}) = \mathrm{Hom}(\mathrm{Spec}(\mathcal{O}), X_{\mathbb{Z}})$. Soit $\mathcal{L}_x$ la fibre de $\mathcal{L}$ en x ; c'est un k-espace vectoriel de rang 1. Le choix (a) fournit la $\mathcal{O}$-forme $x^*_{\mathcal{O}}\mathcal{L}_{\mathbb{Z}}$ de $\mathcal{L}_x$. Le choix (b) fournit, pour chaque plongement complexe ι de k, une forme hermitienne sur $\mathcal{L}_x \otimes_{k,\iota} \mathbb{C}$. On prend

$$h_{\mathcal{L}}(x) = \frac{1}{[k:\mathbb{Q}]} \deg \mathcal{L}_x .$$

Le facteur $1/[k:\mathbb{Q}]$ dans la définition assure que pour $k \subset k'$, la fonction $h_{\mathcal{L}}$ sur $X(k)$ est la restriction à $X(k)$ de la fonction $h_{\mathcal{L}}$ sur $X(k')$; par passage à la limite, on obtient $h_{\mathcal{L}}$ sur $X(\overline{\mathbb{Q}})$.

Une version savante du fait qu'il n'y a qu'un nombre fini d'entiers n avec $|n| \leq h$ est :

Rappel 1.8.— *Si* $\mathcal{L}$ *est ample, il n'y a qu'un nombre fini de* $x \in X(k)$ *avec* $h_{\mathcal{L}}(x) \leq h$.

Soit U un ouvert de X, de complément Y. On appellera *distance logarithmique* à Y une fonction $\rho > 0$ sur $U(\mathbb{C})$ qui près de Y a le comportement asymptotique $\rho \asymp -\log \Sigma |f_i|^2$, pour Y localement défini par des équations $f_i = 0$. Cette classe de fonctions sur $U(\mathbb{C})$ ne dépend que de la structure de variété algébrique complexe de $U(\mathbb{C})$, non de la compactification $X(\mathbb{C})$ de $U(\mathbb{C})$.

Soit, sur U, s une structure hermitienne sur le fibré en droites $\mathcal{L}$, supposée invariante par conjugaison complexe. La construction ci-dessus de $h_{\mathcal{L}}$ permet encore d'attacher à $(\mathcal{L},s)$ une classe mod. $O(1)$ de fonctions *hauteur* $h_{\mathcal{L},s}$ sur $U(\overline{\mathbb{Q}})$. On dit que s est à *singularités logarithmiques* le long de Y si pour ρ une distance logarithmique à Y et pour s_o une structure hermitienne sur $\mathcal{L}$, on a pour r assez grand

$$\sup(s/s_o, s_o/s) \leq O(\rho^{-r}) .$$

PROPOSITION 1.9.— *Si* $\mathcal{L}$ *est ample et que* s *est à singularités logarithmiques le long de* $Y = X - U$, *pour tout corps de nombres* k *il n'y a qu'un nombre fini de* $x \in U(k)$ *avec* $h_{\mathcal{L},s}(x) \leq h$.

Preuve.— Fixons un plongement projectif $X \hookrightarrow \mathbb{P}$ et soit D une hypersurface de $\mathbb{P}$ contenant Y. Soient $r > 0$ et $s(D,r)$ une structure hermitienne sur $\mathcal{L}_{\mathbb{C}}|(X-D)(\mathbb{C})$ avec le long de D le comportement asymptotique $s(D,r) \asymp s_o.|f|^{-2r}$, pour s_o une structure hermitienne sur $\mathcal{L}$ et f une équation locale de D. On a $s \leqslant s(D,r)$ donc, à $O(1)$ près, $h_{\mathcal{L},s} \geq h_{\mathcal{L},s(D,r)}$ sur $(X-D)(\overline{\mathbb{Q}})$. Par ailleurs, encore à $O(1)$ près,

$$h_{\mathcal{L},s(D,1/n)} \geq \frac{1}{n} h_{\mathcal{L}^{\otimes n}(-D)} .$$

Pour n assez grand, $\mathcal{L}^{\otimes n}(-D)$ est ample et, d'après 1.8, il n'y a qu'un nombre fini de $x \in (U-D)(k)$ avec $h_{\mathcal{L}^{\otimes n}(-D)}$ borné. On conclut en écrivant Y comme intersection de diviseurs D.

1.10. Preuve de 1.6.– Sur l'espace de modules M, on dispose du schéma abélien universel $A[M]$ et du faisceau inversible $\omega := \omega(A[M])$. Ce dernier est muni de la structure hermitienne s suivante : la fibre ω_x de ω en $x \in M(\mathbb{C})$ est $\omega(A_x)$, pour A_x la fibre de $A[M]$ en x, et pour $\alpha \in \omega_x$, $\langle \alpha,\alpha \rangle_s = \frac{1}{(2\pi)^g} \int_{A_x} |\alpha \wedge \bar{\alpha}|$.

Description analytique de (M,ω,s).– Soit V un espace vectoriel réel de dimension $2g$ muni d'une forme symplectique ψ. L'*espace de Siegel* S correspondant est l'espace des structures de Hodge réelles de type $\{(-1,0),(0,-1)\}$ sur V polarisées par ψ (sous-espaces isotropes maximaux $F^o \subset V_{\mathbb{C}} := V \otimes_{\mathbb{R}} \mathbb{C}$, tels que $F^o \oplus \bar{F}^o \xrightarrow{\sim} V_{\mathbb{C}}$ et que $i\psi(x,\bar{x}) > 0$ pour $x \in F^o$, $x \neq 0$). Le groupe $Sp(V)$ agit sur S. Le choix d'une base symplectique $(e_i,f_i)_{1 \leq i \leq d}$ de V identifie S à l'espace des matrices symétriques Z_{ij} avec $Im(Z_{ij})$ défini > 0 : imposer $f_i - \sum_j Z_{ij} e_j \in F^o$.

Fixons un réseau entier $V_{\mathbb{Z}}$, engendré par une base symplectique $(e_i,f_i)_{1 \leq i \leq d}$, et $\varepsilon_o : (\mathbb{Z}/(m))^{2d} \xrightarrow{\sim} V_{\mathbb{Z}}/mV_{\mathbb{Z}}$. Le quotient de S par le groupe de congruence de niveau m, $\Gamma := Aut(V_{\mathbb{Z}},\psi,\varepsilon_o)$, s'identifie alors à une composante connexe de $M(\mathbb{C})$; la variété abélienne correspondant à $F^o \in S$ est $A_x := F^o \backslash V_{\mathbb{C}}/V_{\mathbb{Z}}$, sa polarisation est déduite de ψ et sa structure de niveau m de ε_o. Variant ε_o, on obtient toutes les composantes connexes.

Sur S, les $\bigwedge^g ((V_{\mathbb{C}}/F^o)^\vee)$ sont les fibres d'un fibré en droites $Sp(V)$-équivariant ω. Sur S, nous trivialiserons ω par sa base e déduite de la base $e_1,\ldots,e_g$ de $V_{\mathbb{C}}/F^o$. La métrique hermitienne s sur ω pour laquelle $\langle e,e \rangle = \pi^{-g} \det Im(Z)$ est $Sp(V)$-invariante, et cette invariance la caractérise à un facteur près. Par passage au quotient par Γ, ω et s sur S fournissent ω et s sur $M(\mathbb{C})$.

Pour $g > 1$, les $H^o(M,\omega^{\otimes n})$ sont de dimension finie et la *compactification de Baily-Borel* $M(\mathbb{C})^-$ de $M(\mathbb{C})$ est, pour n assez grand, l'adhérence de $M(\mathbb{C})$ dans le plongement projectif défini par les sections globales de $\omega^{\otimes n}$. Cette description montre que $M(\mathbb{C})^-$ provient d'une compactification M^- de M (définie sur $\mathbb{Q}$) et fournit un prolongement de ω à M^- (utiliser aussi A. Borel, J. diff. géom. 6(1972),543-560).

La proposition 1.9 ramène 1.6 aux propositions 1.11 et 1.12 suivantes.

PROPOSITION 1.11.– *La structure hermitienne s de ω est à singularités logarithmiques le long de $M^- - M$.*

Sur un domaine de Siegel, la base e de ω est $\asymp$ aux images inverses sur S des sections locales inversibles de ω sur M^- ; on le vérifie à l'aide des séries d'Eisenstein ; les images inverses de fonctions "distance logarithmique à $M^- - M$" sont $\asymp$ aux fonctions $\ell(Im\ Z)$, pour ℓ une forme linéaire $\ell(Y) = Tr(FY)$, avec F symétrique défini > 0 ; on peut le vérifier en utilisant, plutôt que la compactification de Baily-Borel M^- de M, les compactifications toroïdales de [1]. La proposition en résulte.

A (ω,s) correspond une classe mod. $0(1)$ de fonctions hauteur $h_{\omega,s}$ sur $M(\overline{\mathbb{Q}})$. Identifions un triple (A,Θ,ε) comme en 1.6 au point correspondant de $M(k) \subset M(\overline{\mathbb{Q}})$.

PROPOSITION 1.12.– *A un* $0(1)$ *(uniforme en* k *) près, on a*

$$h(A) = h_{\omega,s}(A,\Theta,\varepsilon) .$$

Si on disposait, sur $\mathbb{Z}$, d'une bonne théorie des compactifications des espaces de modules de variétés abéliennes, on pourrait donner de 1.6 la preuve suivante. On dispose de $M_{\mathbb{Z}}$ sur $\mathrm{Spec}(\mathbb{Z})$ et, sur $M_{\mathbb{Z}}$, d'un schéma abélien "universel" $A[M_{\mathbb{Z}}]$ prolongeant le schéma abélien universel $A[M]$ sur M .

On espère que :

(a) Chaque compactification toroïdale du type introduit dans [1] de $M(\mathbb{C})$, si définie sur $\mathbb{Q}$, a un analogue sur $\mathrm{Spec}(\mathbb{Z})$. Choisissons-en une, $M(\mathbb{C})^{\sim}$ et soit $M^{\sim}_{\mathbb{Z}}$ la compactification correspondante de $M_{\mathbb{Z}}$.

(b) Le schéma abélien universel sur $M_{\mathbb{Z}}$ se prolonge en un schéma semi-abélien $A[M^{\sim}_{\mathbb{Z}}]$ sur $M^{\sim}_{\mathbb{Z}}$.

(c) Sur $\mathbb{Q}$, la compactification $M^{\sim}$ de M domine M^{-} : on dispose de $u : M^{\sim} \longrightarrow M^{-}$. Le prolongement $u^*\omega$ de ω à $M^{\sim}$ est $\omega(A[M^{\sim}])$.

De (a) (b) résulte que si (A,Θ,ε) sur k correspond au point $x \in M(k)$, se prolongeant en $x_0 : \mathrm{Spec}(\mathcal{O}) \longrightarrow M$, le modèle de Néron connexe $A^0_{\mathcal{O}}$ de A est $x_{\mathcal{O}}^*A[M^{\sim}_{\mathbb{Z}}]$. La fonction hauteur $h(A)$ correspond donc à la fonction hauteur $h_{\omega,s}$ sur $M(\overline{\mathbb{Q}})$, relative au faisceau inversible $\omega := \omega(A[M_{\mathbb{Z}}])$ sur $M^{\sim} \supset M$, à s , et à la structure entière $(M^{\sim}_{\mathbb{Z}},\omega(A[M^{\sim}_{\mathbb{Z}}]))$. A des $0(1)$ près, les hauteurs $h_{\omega,s}$ sont indépendantes des structures entières, et 1.12 résulte de ce que ω sur $M^{\sim}$ est l'image inverse de ω sur M^{-} .

On ne dispose malheureusement pas de (a) (b) (c) et, pour prouver 1.12, nous nous raccrocherons à la théorie des compactifications des espaces de modules de courbes.

Lemme 1.13.– *Pour* X *un schéma en courbes semi-stables sur* S , $\mathrm{Pic}^0(X/S)$ *est un schéma semi-abélien sur* S .

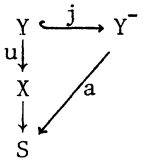
Lemme 1.14.– *Soient* A *un schéma semi-abélien sur un schéma normal* S . *Toute décomposition* $A = A' \times A''$ *sur un ouvert dense de* S *se prolonge à* S *entier, avec des facteurs semi-abéliens.*

Lemme 1.15.– *Soient* A *un schéma semi-abélien sur un schéma* S *et, sur un ouvert dense* U *de* S , *soit* H *un sous-schéma en groupes fini et plat de* A . *Après un changement de base propre surjectif* $S' \to S$, H' *se prolonge en un sous-schéma en groupes plat sur* S *tout entier, fermé dans* A , *et* A/H' *est semi-abélien.*

Dans ces lemmes, pour éviter des questions délicates et sans intérêt de représentabilité, il y a intérêt à travailler partout avec des espaces algébriques.

PROPOSITION 1.16 (O. Gabber).— *Soient* X *irréductible, de type fini sur* S , *et* A *un schéma abélien sur* X . *Il existe un diagramme commutatif*

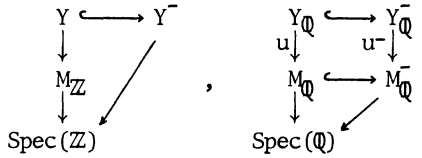
(1.16.1)



avec u *propre surjectif et* a *propre, tel que* u*A *se prolonge en un schéma semi-abélien sur* Y^- .

Preuve (esquisse).— Utilisant que la fibre générique de A/X est quotient d'une jacobienne, le théorème de complète réductibilité de Poincaré et la propreté du champ modulaire des courbes stables, on trouve Y , Y^- , un ouvert dense V de Y , un schéma abélien A' sur V et une courbe stable C sur Y^- , tels que sur V , $A \times_V A'$ soit quotient de $\mathrm{Pic}^0_Y(C)$ par un schéma en groupes fini et plat. On conclut en appliquant les lemmes 1.13 à 1.15.

1.17. Preuve de 1.12.— Appliquons 1.16 aux composantes irréductibles de $M_{\mathbb{Z}} \longrightarrow \mathrm{Spec}(\mathbb{Z})$. On peut supposer, et on suppose, que dans le diagramme (1.16.1) obtenu, Y^- est normal, que Y est dense dans Y^- et que $Y^-_{\mathbb{Q}}$ domine la compactification $M^-_{\mathbb{Q}}$ de $M_{\mathbb{Q}}$.



Vu l'invariance de la hauteur h(A) par extension des scalaires, la méthode de démonstration esquissée après 1.12 s'applique, pour autant qu'on puisse montrer que $u^{-*}(\omega)$ est le ω du schéma semi-abélien $A[Y^-_{\mathbb{Q}}]$ sur $Y^-_{\mathbb{Q}}$ qui prolonge $u^*A[M_{\mathbb{Q}}]$. Il suffit de le vérifier après extension des scalaires à $\mathbb{C}$.

Notons que pour $\mathcal{L}$ un fibré en droites sur un ouvert dense Y d'une variété normale Y^- , (a) une extension de Y à Y^- est uniquement déterminée par ses images inverses sur des courbes lisses $v : C \longrightarrow Y^-$, avec $v^{-1}(Y)$ dense - cette image inverse étant vue comme extension à C de l'image inverse de $\mathcal{L}$ sur $v^{-1}(Y)$; (b) pour s une structure hermitienne sur $\mathcal{L}$, $\mathcal{L}$ admet au plus une extension à Y^- relativement à laquelle s soit à singularités logarithmiques le long de $Y^- - Y$. Cumulant ces remarques et invoquant 1.11, on se ramène à vérifier le

Lemme 1.18.— *Soient* C *une courbe algébrique lisse sur* $\mathbb{C}$ *et* A *un schéma semi-abélien sur* C , *abélien sur le complément* U = C - S *d'un ensemble fini de points. La métrique hermitienne sur* $\omega(A)|U$ *donnée, en* $y \in U$, *par* $\langle \alpha, \alpha \rangle = \int_{A_y} |\alpha \wedge \bar{\alpha}|$, *est à singularités logarithmiques le long de* S .

Soient $s \in S$ et identifions un petit voisinage de s (évitant $S - \{s\}$) au

disque unité D, par une coordonnée locale z centrée en s. Considérons l'image inverse A_D de A sur D. Soient L le fibré vectoriel $\mathrm{Lie}(A_D)$ et Λ le noyau de l'exponentielle $\mathrm{Lie}(A_D) \to A_D$. Ce noyau est fermé dans L, étalé sur D et, sauf au-dessus de 0, un fibré en réseaux. Soit $\Lambda^0 \subset \Lambda$ la réunion (disjointe) des sections passant par les points de la fibre de Λ en 0. Si on choisit une base de L, $\Lambda_z \subset L_z \sim \mathbb{C}^g$ apparaît comme un réseau variable dans $\mathbb{C}^g$ $(z \neq 0)$; le sous-réseau Λ^0_z se prolonge en $z = 0$, et $\Lambda_z - \Lambda^0_z$ tend vers l'infini (puisque Λ est fermé). Parce que A est un modèle de Néron connexe, les sections de A_D sur D^* appartenant à un sous-groupe d'indice fini du groupe de toutes les sections de torsion se prolongent à D. Ceci impose : Λ^0_z = invariants de la monodromie locale dans Λ_z. Parce que la fibre de A_D en 0 est semi-stable, L_0 est engendré par Λ^0_0. On a

(*) L est l'unique fibré vectoriel prolongeant $L|D^*$, de sections locales les combinaisons linéaires à coefficients holomorphes de sections locales de Λ^0.

On sait (voir par exemple P. Griffiths, Periods of integrals on algebraic manifolds III, Publ. Math. IHES 38, aux p. 175-177) que, en dehors de $z = 0$, A_D admet une description analytique du type suivant : pour une base convenable $\underline{e}$ de L sur D^*, on a $A_z = \mathbb{C}^g/\Lambda(z)$, le réseau variable $\Lambda(z)$ vérifiant : il contient $\mathbb{Z}^g$; si $\Lambda^0(z)$ est le sous-réseau fixe par la monodromie locale, $\Lambda^0(z)$ tend vers une limite pour $z \to 0$ (limite dans l'espace des sous-$\mathbb{Z}$-modules discrets de rang $r = \mathrm{rg}\,\Lambda^0(z)$ de $\mathbb{C}^g$) ; $\Lambda(z) - \Lambda^0(z)$ tend vers l'infini. Les formules asymptotiques de *loc. cit.* montrent de plus que le volume de $\mathbb{C}^g/\Lambda(z)$ croît en $|\log|z||^{2g-r}$. D'après (*), la base $\underline{e}$ de $L|D^*$ se prolonge en une base de L sur D ; 1.18 en résulte.

1.19. La preuve donnée de 1.6 s'applique aussi bien pour Θ une polarisation de degré fixe n, plutôt que de degré 1. La description analytique de l'espace de modules correspondant $M = M_{g,n,m}$ est un peu plus compliquée. Le groupe $G := \mathrm{GL}(2g, \mathbb{Z}/(m))$ agit sur M (changement de structure de niveau) et M/G est l'espace grossier de modules $M_{g,n}$ des variétés abéliennes polarisées (A,Θ), de dimension g et de degré de polarisation n. Le fibré ω sur M, avec sa structure hermitienne, est G-équivariant. Sa puissance tensorielle $(\#G)$-ième se descend donc à M/G. Soit h une fonction hauteur correspondante sur $M_{g,n} = M/G$, divisée par $\#G$. On déduit de l'analogue de 1.12 pour les variétés abéliennes munies d'une polarisation de degré n (plutôt que principale) le

Lemme 1.20.— *Pour* (A,Θ) *sur* k *correspondant à un point* a *de* $M_{g,n}(k) \subset M_{g,n}(\overline{\mathbb{Q}})$, *on a*

$$h_{\mathrm{geom}}(A) = h(a) + O(1) .$$

La preuve de 1.9 montre que, comme c'est le cas pour les hauteurs usuelles, $h(a)$ est borné inférieurement sur $M_{g,n}(\overline{\mathbb{Q}})$:

Lemme 1.21.– *Quels que soient* g *et* n , *il existe* $C_{g,n}$ *tel que pour toute variété abélienne* A *sur un corps de nombres, admettant une polarisation de degré* n , *on ait*

$$h(A) \geq h_{geom}(A) \geq C_{g,n} .$$

Remarque 1.22.– On peut montrer que pour A une variété abélienne à réduction semi-stable sur un corps de nombres k , de duale A^* , on a $h(A) = h(A^*)$. Sur un corps quelconque, pour A une variété abélienne sur k , $A^4 \times A^{*4}$ admet toujours une polarisation principale (Zarhin). Puisque $h(A \times B) = h(A) + h(B)$, il en résulte que dans 1.21 on peut prendre $C_{g,n}$ indépendant de n (remplacer $C_{g,n}$ par $\frac{1}{8} C_{8g,1}$).

Lemme 1.23.– *Le corps* k , g , n *et* h *étant fixés, il existe un ensemble fini* S *de places de* k *tel que toute variété abélienne polarisée* (A,Θ) *de dimension* g *et de degré de polarisation* n *sur* k , *avec* $h(A) \leq h$, *ait réduction semi-stable en dehors de* S .

Soit (A,Θ) . Sur une extension k' de k qu'on peut prendre de degré $\leq |GL(2g,\mathbb{Z}/(15))|$, $A' := A_{k'}$ a réduction semi-stable. Le morphisme $A_0 \otimes O' \longrightarrow A'_0$, a une différentielle non inversible en réduction en chaque place de k' au-dessus d'une place de k où A a réduction non semi-stable. Si la caractéristique résiduelle est p , chacune de ces places contribue un terme au moins égal à $\log p/[k':\mathbb{Q}]$ à $h(A) - h(A')$. On a donc $\log p/[k':\mathbb{Q}] \leq h(A) - C_{g,n}$ et ceci borne p .

1.24 Preuve de 1.3.– On déduit de 1.20 que les (A,Θ) ne forment, sur la clôture algébrique de k , qu'un nombre fini de classes d'isomorphie. Pour chacune de ces classes, le lieu de mauvaise réduction est borné par la réunion de S (1.23) et du lieu de mauvaise réduction potentielle (fixe), et A admet une structure de niveau $m = 15$ sur une extension k' de k de degré et ramification bornés. Il n'y a qu'un nombre fini de tels corps k' (Hermite), et qu'un nombre fini de façon de descendre de k' à k .

Montrons qu'on peut améliorer 1.3 en omettant Θ .

Rappel 1.25.– *Soit* E *un ordre d'une algèbre semi-simple* S *sur* $\mathbb{Q}$.

(i) E^* , *agissant sur l'ensemble des idempotents de* E *par automorphismes intérieurs, n'a qu'un nombre fini d'orbites.*

(ii) *Pour* S *une algèbre à involution,* E^* , *agissant sur l'ensemble des éléments hermitiens* $(h = h^*)$ *de* E *de norme donnée (par* xhx^* *), n'a qu'un nombre fini d'orbites.*

Appliquant 1.25 à l'anneau des endomorphismes d'une variété abélienne A sur k , on obtient

Rappel 1.26.– (i) *Les variétés abéliennes facteur direct de* A *ne forment qu'un nombre fini de classes d'isomorphie.*

(ii) *Les polarisations de degré* n , Θ , *de* A *ne fournissent qu'un nombre fini de classes d'isomorphie de variétés abéliennes polarisées* (A,Θ) .

De 1.26 (i), on déduit de 1.3 par l'argument 1.22 de passage à $A^4 \times A^{*4}$, la

Variante 1.27.– *Pour* k, g *et* h *fixés, il n'y a qu'un nombre fini de classes d'isomorphie de variétés abéliennes* A *sur* k *de dimension* g *et de hauteur* $h(A) \leq h$.

Noter que, par 1.26 (ii), cette variante renforce 1.3.

2. ISOGÉNIES

Dans ce paragraphe, nous étudions la variation de la hauteur h(A) par isogénie, pour A à réduction semi-stable, et en déduisons la conjecture de Tate.

2.1. Pour toute suite exacte $0 \to A' \to A \to A'' \to 0$ de schémas en groupes commutatifs plats sur une base S, on dispose d'un isomorphisme naturel

$$\omega(A) \simeq \omega(A') \otimes \omega(A'') .$$

Pour k un corps de nombres d'anneau d'entiers $\mathcal{O}$, $S = \mathrm{Spec}(\mathcal{O})$ et A (donc A', A'') de fibre générale propre sur k, cet isomorphisme est compatible aux structures hermitiennes des deux membres. Ceci traduit que

$$\int_{A(\mathbb{C})} = \int_{A''(\mathbb{C})} \int_{A'(\mathbb{C})} .$$

On a donc

$$\deg \omega(A) = \deg \omega(A') + \deg \omega(A'') .$$

Soit $u : A \to B$ une isogénie entre variétés abéliennes sur k, de noyau H, et soit $H_{\mathcal{O}}$ l'adhérence schématique de H dans le modèle de Néron connexe $A^0_{\mathcal{O}}$ de A. On suppose A à réduction semi-stable. La suite

$$0 \to H_{\mathcal{O}} \to A^0_{\mathcal{O}} \to B^0_{\mathcal{O}} \to 0$$

est alors exacte. Elle fournit

$$h(B) = h(A) - \frac{1}{[k:\mathbb{Q}]} \deg \omega(H^*_{\mathcal{O}}) . \tag{2.1.1}$$

2.2. Calculons $\omega(H)$ pour H un schéma en groupes commutatifs plat quasi-fini sur $S = \mathrm{Spec}(\mathcal{O})$. Sur k, H est étale, Lie H = 0 et $\omega(H) \otimes_{\mathcal{O}} k$ est canoniquement isomorphe à k. Via cet isomorphisme, la $\mathcal{O}$-structure $\omega(H)$ de $\omega(H) \otimes_{\mathcal{O}} k$ coïncide avec celle $\mathcal{O}$ de k sur l'ouvert de S où H est étale, mais pas ailleurs, et les structures hermitiennes diffèrent.

(a) La structure hermitienne de $\omega(H) \otimes_{\mathcal{O}} \mathbb{C} \simeq C$ est #H fois la structure standard.

(b) Supposons tout d'abord H fini sur S, d'algèbre affine $\mathcal{O}(H)$. Cette algèbre est d'intersection complète. Soit $\mathcal{D}^{-1}$ sa différente inverse : le plus grand sous-$\mathcal{O}(H)$-module de $\mathcal{O}(H) \otimes_{\mathcal{O}} k$ sur lequel la trace $\mathrm{Tr}_{H/S}$ soit à valeurs dans $\mathcal{O}$. La trace l'identifie au $\mathcal{O}$-dual de $\mathcal{O}(H)$. On a $\mathcal{O}(H) \subset \mathcal{D}^{-1}$. Parce que H est un groupe, il existe un $\mathcal{O}$-module $\mathcal{D}_0^{-1}$: $\mathcal{O} \subset \mathcal{D}_0^{-1} \subset k$, tel que $\mathcal{D}^{-1} = \mathcal{D}_0^{-1} \otimes_{\mathcal{O}} \mathcal{O}(H)$. On a

$$\omega(H) = \mathcal{D}_0^{-1} .$$

(c) Dans le cas général, on définit $\mathcal{D}_0^{-1}$ en se localisant pour la topologie étale sur S : localement, H est extension d'un schéma en groupe étale H'' par H' fini, et $\mathcal{D}_0^{-1}$ pour $H := \mathcal{D}_0^{-1}$ pour H' . On a encore $\omega(H) = \mathcal{D}_0^{-1}$. En particulier, l'isomorphisme $\omega(H) \otimes_{\mathcal{O}} k = k$ se prolonge en $\mathcal{O} \hookrightarrow \omega(H)$.

La définition du degré donne

$$\deg \omega(H) = \log\Big[(\#H)^{-[k:\mathbb{Q}]/2} . \#(\omega(H)/\mathcal{O}) \Big] . \tag{2.2.1}$$

Il résulte de [3] prop. 9 de l'appendice que $\omega(H)/\mathcal{O}$ est annulé par $\#H$, d'où la borne

$$\#\omega(H)/\mathcal{O} \mid \#H^{[k:\mathbb{Q}]} . \tag{2.2.2}$$

Nous aurons à faire usage de la condition suivante, automatique pour H fermé dans A semi-abélien sur S .

(2.2.3) Pour toute place finie v de k , soit H_v le schéma en groupes sur $S_v := \mathrm{Spec}(\mathcal{O}_v)$ déduit de H . Il est extension d'un sous-groupe ouvert H_v'' d'un groupe $H_v'^-$ fini étale sur S_v par un groupe H_v' fini sur S_v .

Soit ℓ un nombre premier et supposons H annulé par ℓ . Soit $\bar{k}$ une clôture algébrique de k . Le groupe de Galois $\mathrm{Gal}(\bar{k}/k)$ agit sur $H(\bar{k})$, qui est un vectoriel de rang fini r sur $\mathbb{F}_\ell$. Soient $\chi[H] : \mathrm{Gal}(\bar{k},k) \to \mathbb{F}_\ell^*$ le déterminant de cette représentation et $\chi_0[H]$ son composé avec le transfert $\mathrm{Gal}(\bar{k}/\mathbb{Q})^{ab} \to \mathrm{Gal}(\bar{k}/k)^{ab}$. Si ε est la signature de la représentation de permutation de $\mathrm{Gal}(\bar{k}/\mathbb{Q})$ sur $\mathrm{Gal}(\bar{k}/\mathbb{Q})/\mathrm{Gal}(\bar{k}/k)$, on a

$$\chi_0[H] = \det\Big(\mathrm{Ind}_{\mathrm{Gal}(\bar{k}/k)}^{\mathrm{Gal}(\bar{k}/\mathbb{Q})} (H(\bar{k}) - \mathbb{F}_\ell^r) \Big) = \det \mathrm{Ind}\, H(\bar{k}) . \varepsilon^r .$$

L'hypothèse (2.2.3) assure que $\chi_0[H] : \mathrm{Gal}(\bar{k}/\mathbb{Q}) \to \mathbb{F}_\ell^*$ n'est ramifié qu'en ℓ , donc est une puissance du caractère τ donnant l'action de $\mathrm{Gal}(\bar{k}/\mathbb{Q})$ sur les racines ℓ-ièmes de 1 .

Soit v une place de k divisant ℓ . Sous l'hypothèse que l'indice de ramification absolu e en v soit $< (\ell - 1)$, M. Raynaud [3] théorème 4.1.1 relie la restriction de $\chi[H]$ au groupe d'inertie en v à la longueur de la v-composante de $\omega(H)/\mathcal{O}$. Il traite du cas d'un groupe fini sur S_v , mais l'hypothèse (2.2.3) permet de se ramener à ce cas. On déduit de son résultat que

PROPOSITION 2.3.— *Pour H annulé par ℓ et vérifiant (2.2.3), si pour toute place v de k divisant ℓ l'indice de ramification absolu est $< \ell - 1$, on a, posant $\#(\omega(H)/\mathcal{O}) = \ell^n$,*

$$\chi_0[H] = \tau^n .$$

Nous allons en déduire le

THÉORÈME 2.4.— *Soit A une variété abélienne sur k , à réduction semi-stable. Il existe un ensemble fini F de nombres premiers tels que, pour $u : A \to B$ une isogénie de degré premier aux $\ell' \in F$, on a*

$$h(A) = h(B) .$$

Nous prouverons qu'on peut prendre F ne dépendant que de la classe d'isogénie de A. Pour prouver cet énoncé plus fort, il suffit de traiter d'une isogénie de noyau H annulé par un nombre premier ℓ. Soient F_1 l'ensemble des ℓ' tels que, en une place de k divisant ℓ', l'indice de ramification absolu soit $\geq \ell' - 1$ et p un nombre premier tel qu'en chaque place divisant p, A ait bonne réduction. Notre F vérifiera $F \supset F_1 \cup \{p\}$.

Pour chaque place v de k divisant p, soient q_v le nombre d'éléments du corps résiduel, e_v l'indice de ramification absolu et P_v le polynôme caractéristique de l'automorphisme de Frobenius arithmétique φ_v agissant sur $T_\ell(A)$. C'est un polynôme unitaire à coefficients entiers indépendants de ℓ, ne dépendant que de la classe d'isogénie de A. Soient $\alpha_1^v \ldots \alpha_{2d}^v$ les racines complexes de P_v, avec leur multiplicité. D'après A. Weil, ce sont des nombres de valeur absolue $q_v^{1/2}$.

Soit R un anneau d'entiers de corps de nombres assez grand pour contenir les α_i^v $(v|p)$. Si $H(\overline{k})$ est de dimension r sur $\mathbb{F}_\ell$, il existe $R \to \mathbb{F}_{\ell a}$, de noyau λ, et, pour chaque $v|p$, une partie J_v à r éléments de $[1,2d]$ telle que le polynôme caractéristique de φ_v agissant sur $H(\overline{k})$ soit la réduction mod. λ du produit des $(T - \alpha_i^v)$, $i \in J_v$. On a alors

$$\chi_0[H](\varphi_p) \equiv \prod_{v|p}\Big(\prod_{i\in J_v} \alpha_i^v\Big)^{e_v}, \quad \text{mod. } \lambda .$$

Si $\#(\omega(H)/0) = \ell^n$, on en déduit par 2.3 que

$$\prod_{v|p}\Big(\prod_{i\in J_v} \alpha_i^v\Big)^{e_v} \equiv p^n, \quad \text{mod. } \lambda . \tag{2.4.1}$$

La valeur absolue complexe du premier membre est $p^{[k:\mathbb{Q}].r/2}$. La congruence ne peut donc être une égalité que si $n = [k:\mathbb{Q}].r/2$, auquel cas $\deg \omega(H) = 0$ (2.2.1). Si F_2 est l'ensemble des ℓ qui divisent l'un des nombres $N_{R/\mathbb{Z}}\Big(\prod_{v|p}\Big(\prod_{i\in J(v)} \alpha_i^v\Big)^{e_v} - p^b\Big)$, où, pour $1 \leq r \leq 2d$ convenable, les $J(v)$ sont des parties à r éléments de $[1,2d]$ et où $1 \leq b \leq [k:\mathbb{Q}].r$, $b \neq [k:\mathbb{Q}].r/2$, alors $F = F_1 \cup \{p\} \cup F_2$ convient : la congruence (2.4.1) implique égalité, $\deg \omega(H) = 0$, et on conclut par (2.1.1).

2.5. Fixons un nombre premier ℓ, soit $A_{\ell^\infty}(\overline{k})$ le groupe des points de torsion de $A(\overline{k})$ d'ordre une puissance de ℓ, et soit W un sous-groupe ℓ-divisible de $A_{\ell^\infty}(\overline{k})$, stable par $\mathrm{Gal}(\overline{k}/k)$. Il correspond à un sous-module stable $T_\ell(W) \subset T_\ell(A)$, avec $T_\ell(A)/T_\ell(W)$ sans ℓ-torsion. Pour chaque entier n, soit $B(n)$ le quotient A/W_{ℓ^n} de A.

THÉORÈME 2.6.— *Pour* n *assez grand,* $h(B(n))$ *est indépendant de* n.

La preuve est semblable à celle du théorème 2.4, la référence [3] 4.1.1 étant remplacée par [3] 4.2.1 qui affirme : si W est un groupe ℓ-divisible sur $S_v = \mathrm{Spec}(\mathcal{O}_v)$ (v place de k divisant ℓ), d'algèbre de Lie de dimension d, et si $\chi[W] : \mathrm{Gal}(\overline{k}_v/k_v) \to \mathbb{Z}_\ell^*$ est le déterminant de l'action de $\mathrm{Gal}(\overline{k}_v/k_v)$ sur $T_\ell(W)$, la restriction de $\chi[W]$ au groupe d'inertie $I_v \subset \mathrm{Gal}(\overline{k}_v/k_v)$ est τ^d,

pour τ le caractère donnant l'action de $\mathrm{Gal}(\overline{k}_v/k_v)$ sur les racines de l'unité d'ordre une puissance de ℓ . Par ailleurs, le $\mathcal{O}_v$-module $\omega(W_\ell)/\mathcal{O}$ est de longueur d.e$_v$.

Deux problèmes apparaissent.

(a) Soient $W(n)$ l'adhérence schématique de $W_{\ell n}$ dans $A^\circ_{\mathcal{O}}$, et $W(n)_v$ son image inverse sur S_v . Soit $W(n)^\circ_v$ le plus grand sous-schéma en groupes de $W(n)_v$ fini sur S_v . Alors

$$\bigcup W(n)^\circ_v(\overline{k}_v) \subset W$$

n'est peut-être pas un groupe ℓ-divisible.

(b) Même si c'est le cas, les $W(n)^\circ_v$ ne forment peut-être pas sur S_v un groupe ℓ-divisible : bien qu'exactes au point générique, les suites

$$0 \longrightarrow W(n)^\circ_v \longrightarrow W(n+m)^\circ_v \xrightarrow{\ell^n} W(m)^\circ_v \longrightarrow 0$$

pourraient ne pas être exactes.

Ces difficultés disparaissent pour A remplacé par $A/W_{\ell n}$, n assez grand (pour (b), cf. [4] prop. 12), et on en déduit le théorème.

Si A est principalement polarisée et que W est un sous-espace isotrope maximal, les $A/W_{\ell n}$ admettent encore une polarisation principale. Par 1.3 et 2.6, ces quotients se répartissent en un nombre fini de classes d'isomorphie. Comme expliqué dans l'exposé de Szpiro, on déduit de là la conjecture de Tate. L'information additionnelle fournie par le théorème 2.4 donne, par la même méthode, l'énoncé plus précis suivant

THÉORÈME 2.7.— *Soient* A *une variété abélienne sur un corps de nombres* k , *de clôture algébrique* $\overline{k}$. *Le groupe de Galois* $\mathrm{Gal}(\overline{k}/k)$ *agit sur* $T(A) := \prod_\ell T_\ell(A)$, *d'où* $\rho : \hat{\mathbb{Z}}[\mathrm{Gal}(\overline{k}/k)] \longrightarrow \mathrm{End}_{\hat{\mathbb{Z}}}(T(A))$. *La sous-algèbre* $\rho(\hat{\mathbb{Z}}[\mathrm{Gal}(\overline{k}/k)])$ *de* $\mathrm{End}_{\hat{\mathbb{Z}}}(T_\ell(A))$ *est d'indice fini dans le commutant de* $\mathrm{End}(A)$.

Outre la conjecture de Tate et la semi-simplicité de l'action de $\mathrm{Gal}(\overline{k}/k)$ sur $V_\ell(A)$, ce théorème affirme que pour presque tout ℓ , les combinaisons $\mathbb{Z}_\ell$-linéaires d'éléments de $\mathrm{Gal}(\overline{k}/k)$ remplissent le commutant de $\mathrm{End}(A)$ dans $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$.

COROLLAIRE 2.8.— *Sur un corps de nombres* k , *une classe d'isogénie de variétés abéliennes se compose d'un nombre fini de classes d'isomorphie.*

Soit A une variété abélienne sur k . La donnée d'une variété abélienne A' isogène à A équivaut à la donnée, pour tout ℓ , d'un réseau $T'_\ell \subset V_\ell(A)$ stable par $\mathrm{Gal}(\overline{k}/k)$, avec $T'_\ell = T_\ell(A)$ pour presque tout ℓ . Pour que A' soit isomorphe à A , il faut et il suffit qu'il existe $b \in \mathrm{End}(A) \otimes \mathbb{Q}$ tel que pour tout ℓ , $b.T_\ell(A) = T'_\ell$.

Pour chaque nombre premier ℓ , le fait que $\mathbb{Q}_\ell[\mathrm{Gal}(\overline{k}/k)]$ ait pour image dans $\mathrm{End}(V_\ell(A))$ le commutant de $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ implique que $(\mathrm{End}(A) \otimes \mathbb{Q}_\ell)^*$ n'a qu'un nombre fini d'orbites dans l'ensemble des réseaux $T'_\ell \subset V_\ell(A)$ stables sous Galois.

Pour les ℓ tels que $\mathrm{End}(A) \otimes \mathbb{Z}_\ell$ soit un ordre maximal dans l'algèbre semi-simple $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$, et que $\mathbb{Z}_\ell[\mathrm{Gal}(\overline{k}/k)]$ ait pour image dans $\mathrm{End}(T_\ell(A))$ le commutant de $\mathrm{End}(A)$, il n'y a même qu'une orbite.

Soit G le groupe algébrique sur $\mathbb{Q}$ groupe multiplicatif de la $\mathbb{Q}$-algèbre $\mathrm{End}(A) \otimes \mathbb{Q}$. C'est un groupe réductif. Le groupe adélique $G(\mathbb{A}^f)$ agit sur les systèmes de réseaux (T'_ℓ), et ce qui précède montre qu'il n'y a qu'un nombre fini d'orbites. Pour chacune, l'ensemble des classes d'isomorphie de variétés abéliennes correspondantes s'identifie à un ensemble de doubles classes $G(\mathbb{Q})\backslash G(\mathbb{A}^f)/K$, avec K sous-groupe compact ouvert de $G(\mathbb{A}^f)$. Un tel ensemble est fini, et le corollaire en résulte.

COROLLAIRE 2.9.— *Sur un corps de nombres* k, *les variétés abéliennes polarisées* (A,Θ), *de degré de polarisation* n *fixé, avec* A *isogène à une variété abélienne fixe* B, *ne forment qu'un nombre fini de classes d'isomorphie.*

Preuve.— Appliquer 1.26 (ii).

3. LA CONJECTURE DE SHAFAREVITCH

THÉORÈME 3.1.— *Soient* k *un corps de nombres,* $\overline{k}$ *une clôture algébrique de* k, S *un ensemble fini de places finies de* k, ℓ *un nombre premier et* d *un entier. Il existe un ensemble fini* T *de places finies de* k, *disjoint de* S, *tel qu'une représentation* ℓ*-adique semi-simple de dimension* d, $\rho : \mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{GL}(d,\mathbb{Q}_\ell)$, *non ramifiée en dehors de* S, *soit uniquement déterminée (à isomorphisme de représentations près) par les traces* $\mathrm{Tr}(\rho(\varphi_v))$, *pour* $v \in T$.

On sait (Hermite) qu'il n'existe qu'un nombre fini d'extensions galoisiennes k' de k, non ramifiées en dehors de S et de degré borné. D'après Čebotarev, il existe donc un ensemble fini T de places de k, disjoint de S, tel que les classes de conjugaison des Frobenius φ_v $(v \in T)$ remplissent tout $\mathrm{Gal}(k'/k)$, pour toute extension galoisienne k' de k, non ramifiée en dehors de S, de degré $\leq \ell^{2d^2}$. Prouvons que T convient.

Soient donc ρ_1, ρ_2 deux représentations ℓ-adiques du type dit, avec $\mathrm{Tr}\,\rho_1(\varphi_v) = \mathrm{Tr}\,\rho_2(\varphi_v)$ pour $v \in T$. Nous voulons montrer que ρ_1 et ρ_2 ont même caractère, donc, étant semi-simples, sont isomorphes. Soit M l'image de l'algèbre $\mathbb{Z}_\ell[\mathrm{Gal}(\overline{k}/k)]$ par

$$\rho_1 \times \rho_2 : \mathbb{Z}_\ell[\mathrm{Gal}(\overline{k}/k)] \longrightarrow M_d(\mathbb{Q}_\ell) \times M_d(\mathbb{Q}_\ell) .$$

Il s'agit de vérifier que, sur M, la forme linéaire $\delta(m_1,m_2) := \mathrm{Tr}(m_1) - \mathrm{Tr}(m_2)$ est identiquement nulle. L'algèbre M est un $\mathbb{Z}_\ell$-module de rang $\leq 2d^2$. L'image de $\mathrm{Gal}(\overline{k}/k)$ dans le quotient $(M/\ell M)^*$ a donc moins de ℓ^{2d^2} éléments et, par hypothèse, chaque élément de cette image est un $(\rho_1 \times \rho_2)(\varphi_v)$, $v \in T$. Par Nakayama, les $(\rho_1 \times \rho_2)(\varphi_v)$ $(v \in T)$ engendrent $\mathbb{Z}_\ell$-linéairement M. Sur eux, la forme linéaire δ s'annule par hypothèse, d'où $\delta = 0$ sur M.

Remarque.— Un énoncé plus faible que 3.1 avait été obtenu par J.-P. Serre, modulo une hypothèse de Riemann généralisée.

COROLLAIRE 3.2.— *Soient* k *un corps de nombres et* S *un ensemble fini de places de* k . *Il n'y a qu'un nombre fini de classes d'isogénie de variétés abéliennes de dimension* g *sur* k , *à bonne réduction en dehors de* S .

On fixe un nombre premier ℓ et on applique 3.1 à S ∪ {places divisant ℓ} , ℓ et d = 2g . Pour chaque variété abélienne A du type considéré, la représentation ℓ-adique $V_\ell(A) := T_\ell(A) \otimes \mathbb{Q}_\ell$ est semi-simple (par 2.7), et il n'y a qu'un nombre fini de possibilités pour la trace de φ_v ($v \in T$) : par A. Weil, elle est entière et bornée par $2g\sqrt{q_v}$. Il n'y a donc qu'un nombre fini de possibilités pour la classe d'isomorphie de $V_\ell(A)$, et on conclut par la conjecture de Tate.

De ce corollaire on déduit par 2.8 et 2.9 :

COROLLAIRE 3.3.— *Soient* k *un corps de nombres et* S *un ensemble fini de places de* k . *Il n'y a qu'un nombre fini de classes d'isomorphie de variétés abéliennes de dimension* g *sur* k , *à bonne réduction en dehors de* S .

COROLLAIRE 3.4.— *Soient* k *un corps de nombres et* S *un ensemble fini de places de* k . *Il n'y a qu'un nombre fini de classes d'isomorphie de variétés abéliennes polarisées* (A,Θ) *sur* k , *de dimension* g *et de degré de polarisation* n , *à bonne réduction en dehors de* S .

BIBLIOGRAPHIE

[1] A .ASH, D. MUMFORD, M. RAPOPORT and Y. TAI - *Smooth compactification of locally symmetric varieties*, Math. Sci. Press, Brookline, 1975.

[2] G. FALTINGS - *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inv. Math. 73(1983), 349-366.

[3] M. RAYNAUD - *Schémas en groupes de type* (p,...,p) , Bull. Soc. Math. France 102 (1974), 241-280.

[4] J. TATE - p-*divisible groups*, Proc. of a conf. on local fields (Driebergen 1966), 158-183, Springer-Verlag, New York, 1967.

Pierre DELIGNE

Institut des Hautes Études Scientifiques
F-91440 BURES sur YVETTE