Classe d'isogénie de variétés abéliennes pleinement de type GSp

Nicolas Ratazzi *

Abstract : Faltings in 1983 proved the following result for two abelian varieties A, B defined over a number field K : a necessary and sufficient condition for A and B to be K-isogenous is that the local factors of the L-series of A and B are equal for a density one subset of primes of K (of good reduction for A and B) ; for each such prime this implies that the reductions of A and B have the same number of points over the residue field. The aim of this work is showing that for a certain class of abelian varieties 'having the same number of points' may be replaced by 'the number of points have the same prime divisors' and still gives a sufficient condition for A and B to be K-isogenous. The result is proven for abelian varieties faithfully of type GSp (a class containing the abelian varieties with endomorphism ring $\mathbb{Z}$ and of dimension 2 or odd). The proof is based on ideas of Serre [10] and Frey-Jarden [3] and follows closely Hall-Perucca [5] who proved the result for elliptic curves.

1 Introduction

En 1983, Faltings a prouvé le résultat suivant pour deux variétés abéliennes A et B définies sur un corps de nombres : une condition nécessaire et suffisante pour que A et B soient K-isogènes est qu'il existe un ensemble S de densité un de premiers $\mathfrak{p}$ de K (de bonne réduction pour A et B) tels que les facteurs locaux des séries L de A et B soit égaux. Ce résultat a été récemment amélioré dans [5] pour les courbes elliptiques de la façon suivante : plutôt que demander que les réductions $A_\mathfrak{p}$ et $B_\mathfrak{p}$ aient le même nombre de points sur le corps résiduel $k_\mathfrak{p}$ (condition équivalente à l'égalité des facteurs locaux des séries L dans le cas de dimension 1), il suffit (pour des courbes elliptiques) de demander que le nombre de points de $A(k_\mathfrak{p})$ et de $B(k_\mathfrak{p})$ aient le même ensemble de diviseurs premiers. De plus il suffit de savoir ceci non pour tous les nombres premiers mais seulement pour une famille infinie. Dans cet article nous améliorons le résultat de Faltings de la même façon pour les variétés abéliennes pleinement de type GSp (au sens de la définition 1.1 ci-dessous), famille contenant les variétés abéliennes ayant un anneau d'endomorphismes $\mathbb{Z}$ et de dimension 2 ou impaire. Nous suivons pour cela la stratégie de Hall-Perucca [5], elle même basée sur des travaux antérieurs de Serre [10] et de Frey-Jarden [3].

1.1 Variétés abéliennes pleinement de type GSp

Soit A une variété abélienne de dimension $g \geq 1$ définie sur un corps de nombres K. Considérant l'action du groupe de Galois $\mathrm{Gal}(\bar{K}/K)$ sur les points de ℓ^∞-torsion, pour ℓ premier, on associe naturellement à A/K, la représentation ℓ-adique

$$\rho_{\ell^\infty,A} : G_K := \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}(\mathrm{T}_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$$

avec $\mathrm{T}_\ell(A) = \varprojlim A[\ell^n]$ le module de Tate ℓ-adique de A et on note également son image

*Université Paris-Sud XI, Bâtiment 425, 91405 Orsay Cedex, FRANCE, nicolas.ratazzi@math.u-psud.fr

$$\rho_{\ell^\infty,A}(G_K) := G_{\ell^\infty,A}.$$

Nous noterons également $\rho_{\ell,A}$ et $G_{\ell,A}$ (voire ρ_ℓ et G_ℓ s'il n'y a pas d'ambiguité) les objets déduits modulo ℓ. On supposera pour simplifier que A est munie d'une polarisation principale. Dans ce cas $\rho_{\ell^\infty,A}$ est à valeurs dans $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ (dans le cas général, une polarisation e sur A étant choisie, munissant les $T_\ell(A)$ d'une forme alternée e_ℓ, la représentation est à valeurs dans $\mathrm{GSp}_{2g}(T_\ell(A), e_\ell)$).

Un problème naturel est de savoir quand l'image $G_{\ell^\infty,A}$ est d'indice fini dans (voire égale à) $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$, pour tout premier ℓ assez grand (dépendant de A/K).

Définition 1.1 *Soit A/K une variété abélienne principalement polarisée de dimension $g \geq 1$. Nous dirons que A est pleinement de type* GSp *si A est telle que*

$$\textit{pour tout premier } \ell \textit{ assez grand}, \quad \rho_{\ell,A}(G_K) = \mathrm{GSp}_{2g}(\mathbb{F}_\ell).$$

On sait par exemple après Serre [10] que toute courbe elliptique sans CM, ie à anneau d'endomorphismes (sur $\bar{K}$) $\mathrm{End}_{\bar{K}}(A) = \mathbb{Z}$, est pleinement de type GSp (il s'agit même dans ce cas d'une condition équivalente à être sans CM sur $\bar{K}$). En dimension quelconque, une condition nécessaire est d'avoir $\mathrm{End}_{\bar{K}} A = \mathbb{Z}$; cette condition n'est pas en général suffisante, mais on sait qu'elle l'est (cf. théorème 1.2 ci-dessous) si g n'appartient pas à l'ensemble exceptionnel Σ défini comme suit :

$$\Sigma = \left\{ g \geq 1 \mid \exists k \geq 3, \text{ impair}, \ \exists a \geq 1, \ 2g = (2a)^k \text{ ou } 2g = \binom{2k}{k} \right\}. \tag{1}$$

Dans notre contexte le résultat important est un théorème de Serre ([12] Théorème 3 et [13] Théorème 3) complété par Pink ([8] Theorem 5.14) et dans une autre direction par Hall ([4] Theorem 1).

Théorème 1.2 (Serre, Pink, Hall) *Si A/K est une variété abélienne de dimension g n'appartenant pas à Σ, définie sur un corps de nombres, telle que $\mathrm{End}_{\bar{K}}(A) = \mathbb{Z}$, alors A est pleinement de type* GSp*. Si g est quelconque mais l'on suppose que le groupe de Mumford-Tate $\mathrm{MT}(A) = \mathrm{GSp}$ et que le modèle de Néron de A sur l'anneau des entiers $\mathcal{O}_K$ possède une fibre semistable avec dimension torique égale à un, la même conclusion vaut.*

1.2 Résultat principal

Le théorème 1.2 précédent donne une vaste classe de variétés abéliennes pleinement de type GSp. Nous pouvons maintenant énoncer notre résultat principal.

Théorème 1.3 *Soit K un corps de nombres et soient $A_1, A_2/K$ deux variétés abéliennes pleinement de type* GSp*. Considérons S un sous-ensemble de places finies v de K, de corps résiduel $\mathbb{F}_v$, de bonne réduction pour A_1 et A_2, de densité analytique* 1 *et supposons également donné un sous-ensemble Λ infini de l'ensemble des nombres premiers. Alors A_1 est K-isogène à A_2 si et seulement si*

$$\forall v \in S, \ \forall \ell \in \Lambda \quad (\ell \mid \mathrm{Card}(A_1(\mathbb{F}_v)) \iff \ell \mid \mathrm{Card}(A_2(\mathbb{F}_v))).$$

Notons que l'on sait après Faltings [2] que la classe d'isogénie d'une variété abélienne A/K est donnée par sa fonction ζ qui donne en particulier les valeurs $\mathrm{Card}(A(\mathbb{F}_v))$. Le théorème 1.3 (dont la preuve utilise néanmoins [2]) prouve qu'une donnée sensiblement plus faible est en fait suffisante (au moins pour les variétés abéliennes pleinement de type GSp).

S'il est clair qu'un tel résultat doit se borner à des variétés abéliennes sans facteur carré (ie A isogène à un produit $\prod A_i$ les A_i deux à deux non isogènes), il doit être possible, en utilisant les résultats connus sur les images de Galois (cf. notamment [10] et [6]) d'étendre d'une aute manière ce résultat en traitant le cas des produits de courbes elliptiques sans facteur carré. Nous comptons revenir sur ce problème dans un article ultérieur. Notons par ailleurs que ce résultat

n'est certainement pas vrai en général, même pour une variété abélienne simple quelconque, le cardinal de $A(\mathbb{F}_v)$ avec v variable ne caractérisant pas en général la classe d'isogénie de la variété abélienne.

Structure de la preuve : Nous commençons par des rappels sur les groupes symplectiques utilisés dans les parties suivantes. Les paragraphes 3 et 4 sont consacrés à la preuve proprement dite du théorème 1.3. Pour cela nous suivons de près en l'adaptant en dimension supérieure l'argument de Hall-Perucca [5] et les idées de Serre [10] et Frey-Jarden [3]. La structure de la preuve de l'implication *si* (l'autre implication étant facile) du théorème 1.3 est en trois étapes :

1. Montrer, pour ℓ variant dans un sous-ensemble infini Λ_1 de Λ, que $K(A_1[\ell]) = K(A_2[\ell])$, puis en déduire que A_1 et A_2 sont $\bar{K}$-isogènes.
2. Montrer qu'il existe un caractère quadratique $\varepsilon : G_K \to \{\pm 1\}$ tel que pour tout ℓ variant dans un sous-ensemble infini Λ_2 de Λ_1 les représentations ρ_{ℓ,A_1} et $\varepsilon \otimes \rho_{\ell,A_2}$ sont isomorphes.
3. Montrer que pour tout ℓ variant dans un sous-ensemble infini Λ_3 de Λ_2, la représentation ρ_{ℓ,A_1} est en fait isomorphe à ρ_{ℓ,A_2}, puis conclure que A_1 et A_2 sont K-isogènes.

Pour l'étape 1 nous avons besoin de prouver un résultat d'un intérêt indépendant : le théorème d'isogénies horizontales 3.1 (suivant la terminologie de [3]) pour la classe de variétés abéliennes considérées. Ce théorème nous assure que deux variétés abéliennes pleinement de type GSp sont isogènes sur $\bar{K}$ dès qu'elles vérifient une condition du type $[K(A_1[\ell], A_2[\ell]) : K(A_1[\ell])] \leq c$ pour une certaine constante $c > 0$ et pour une infinité de premiers ℓ. Ce résultat peut se voir comme un corollaire du théorème 1.6 de [7] prouvant la conjecture de Mumford-Tate forte pour le produit $A_1 \times A_2$ de telles variétés abéliennes. Il remplace dans notre preuve l'usage fait par [5] du Theorem A de [3]. Par ailleurs nous aurons besoin d'un raffinement de ce résultat et nous donnons donc une preuve alternative, dans l'esprit de [3] et [10], notamment en prouvant le lemme 3.3.

La proposition 3.4 donne essentiellement une preuve de l'étape 2. Il s'agit d'une adaptation en dimension supérieure du paragraphe 6.2 de [10], en utilisant les résultats de Raynaud [9] en lieu et place du paragraphe 1 de [10].

L'étape 3 se prouve comme dans [5] et utilise notamment le théorème de Faltings (proposition 3.5 rappelée plus loin).

Remerciements : Je remercie Pascal Autissier, Chris Hall et Marc Hindry pour les commentaires qu'ils m'ont fait sur une version préliminaire de ce texte.

2 Rappels sur les groupes symplectiques

Étant donné un entier $g \geq 1$, on rappelle la définition du *groupe (algébrique) symplectique* :

$$\mathrm{GSp}_{2g} := \left\{ M \in \mathrm{GL}_{2g} \mid \exists \lambda(M) \in \mathbb{G}_m,\ {}^tM \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} M = \lambda(M) \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix} \right\}.$$

C'est un groupe algébrique sur $\mathbb{Z}$. On introduit $\lambda : \mathrm{GSp}_{2g} \to \mathbb{G}_m$, l'homomorphisme qui associe à M son multiplicateur $\lambda(M)$. Par définition, le *groupe spécial symplectique* Sp_{2g} est le noyau du morphisme λ et un corps F étant donné, les groupes *projectifs symplectiques* $\mathrm{PGSp}_{2g}(F)$ et $\mathrm{PSp}_{2g}(F)$ sont les quotients respectifs de $\mathrm{GSp}_{2g}(F)$ et de $\mathrm{Sp}_{2g}(F)$ par les matrices scalaires appartenant respectivement à $\mathrm{GSp}_{2g}(F)$ et à $\mathrm{Sp}_{2g}(F)$.

Remarque 2.1 *Notons le lien suivant entre l'application multiplicateur et le déterminant :*

$$\forall M \in \mathrm{GSp}_{2g}, \quad \det M = \lambda(M)^g.$$

Rappelons également le lien bien connu entre caractère cyclotomique, représentation ℓ-adique et multiplicateur :

Lemme 2.2 *En notant ρ_ℓ la représentation ℓ-adique modulo ℓ associée à une variété abélienne principalement polarisée, la composée $\lambda \circ \rho_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathbb{F}_\ell^\times$ n'est autre que le caractère cyclotomique χ_{cycl}.*

Lemme 2.3 *Soient g_1, g_2 deux entiers strictement positifs et soit ℓ un nombre premier impair. On se donne également un sous-groupe $Z_i \subset \{\pm I_{2g_i}\} \subset \mathrm{Sp}_{2g_i}(\mathbb{F}_\ell)$ pour $i \in \{1,2\}$. On a alors*

$$\left|\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)/Z_1\right| = \left|\mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)/Z_2\right| \Rightarrow g_1 = g_2.$$

Démonstration : Le cardinal d'un ℓ-Sylow est $\ell^{g_i^2}$. □

Nous rappelons ici un lemme tiré de [7] (cf. lemmes 2.13 et 2.15 ainsi que les preuves), rassemblant quelques résultats classiques sur les groupes symplectiques, leurs sous-groupes distingués et leurs automorphismes (voir notamment Dieudonné [1] Chap. IV paragraphes 3 et 6).

Lemme 2.4 *Soit $g \geq 1$ et soit $\mathbb{F}$ un corps ; on exclut les cas $g = 1$, $\mathbb{F} = \mathbb{F}_2$, $\mathbb{F}_3$ ou $\mathbb{F}_4$ et $g = 2$, $\mathbb{F} = \mathbb{F}_2$.*

1. *Le seul sous-groupe distingué non trivial de $\mathrm{Sp}_{2g}(\mathbb{F})$ est son centre $\{\pm I_{2g}\}$.*
2. *Les $\mathbb{F}$-automorphismes de $\mathrm{PGSp}_{2g}(\mathbb{F})$ sont tous intérieurs et l'action par conjugaison se fait via un élément de $\mathrm{Sp}_{2g}(\mathbb{F})$.*

3 Isogénies horizontales

Nous voulons ici prouver le théorème 3.1 ci-dessous d'isogénies horizontales (dans la terminologie de [3]). Nous donnons d'abord une preuve directe utilisant le théorème 1.6 de [7] prouvant la conjecture de Mumford-Tate forte pour un produit de variétés abéliennes pleinement de type GSp. Puis nous donnons, dans la suite de ce paragraphe une preuve alternative, (notée preuve (B) ci-après) utilisant directement les idées du paragraphe 6 de Serre [10]. La raison est que les divers énoncés qui interviennent dans cette preuve (B), notamment la proposition 3.4 qui suit, sont également nécessaires pour la preuve du théorème principal 1.3.

Notations Dans la suite, Λ désignera un ensemble infini de nombres premiers, K un corps de nombres et A_1 et A_2 des variétés abéliennes pleinement de type GSp, de dimensions respectives g_1, g_2, définies sur K. La notation ℓ indiquera toujours un nombre premier.
Nous noterons

$$N_\ell := K\left(A_1[\ell], A_2[\ell]\right) \quad \text{et} \quad M_\ell := K\left(A_1[\ell]\right) \cap K\left(A_2[\ell]\right).$$

Nous utiliserons également la notation $\gg$ pour signifier "supérieur à, à une constante multiplicative près indépendante de ℓ". De même pour la notation $\ll$; la notation $\gg\ll$ signifiant la conjonction de $\gg$ et de $\ll$.
Étant donnée A/K une variété abélienne, rappelons comme introduit au paragraphe 1.1 que nous notons $\rho_{\ell^\infty,A}$ la représentation ℓ-adique associée à l'action de Galois sur le module de Tate $T_\ell(A)$ et $\rho_{\ell,A}$ sa réduction modulo ℓ (agissant sur $A[\ell]$).
Étant donnés deux entiers n_1, n_2 et deux représentations ℓ-adiques, $\rho_1 : G_K \to \mathrm{GL}_{n_1}(\mathbb{F}_\ell)$ et $\rho_2 : G_K \to \mathrm{GL}_{n_2}(\mathbb{F}_\ell)$, nous écrirons $\rho_1 \sim \rho_2$ si ρ_1 et ρ_2 sont isomorphes, c'est à dire si $n := n_1 = n_2$ et s'il existe $u \in \mathrm{GL}_n(\mathbb{F}_\ell)$ tel que $u^{-1}\rho_1 u = \rho_2$.
Introduisons la projection canonique $\pi_{\ell,1} : \mathrm{GSp}_{2g_1}(\mathbb{F}_\ell) \to \mathrm{PGSp}_{2g_1}(\mathbb{F}_\ell)$ de noyau $\mathbb{F}_\ell^\times$. Notons $\overline{\rho}_{A_1,\ell}$ la composée de $\rho_{A_1,\ell}$ par $\pi_{\ell,1}$ et de même pour A_2, $\rho_{A_2,\ell}$ et $\overline{\rho}_{A_2,\ell}$. Notons enfin $L_{A_1,\ell}$ le corps fixé par $\ker(\overline{\rho}_{A_1,\ell})$ et de même pour $L_{A_2,\ell}$ correspondant à $\overline{\rho}_{A_2,\ell}$.

Théorème 3.1 *Soient $A_1, A_2/K$ deux variétés abéliennes pleinement de type* GSp*, sur un corps de nombres K. Soit $c > 0$ telle qu'il existe un ensemble infini Λ de nombres premiers, vérifiant*

$$\forall \ell \in \Lambda, \quad \left[K\left(A_1[\ell], A_2[\ell]\right) : K\left(A_1[\ell]\right)\right] \leq c.$$

Alors A_1 est $\bar{K}$-isogène à A_2.

Remarque 3.2 *Dans le cas de dimension* 1*, ceci est un résultat de Frey-Jarden [3] basé sur les travaux de Serre [10]. En fait le résultat de [3] est plus général car il vaut pour des courbes elliptiques quelconques sur un corps K de type fini sur son sous-corps premier.*

Notons que l'on ne suppose pas a priori que A_1 et A_2 sont de même dimension : c'est une conséquence automatique.

Démonstration : Rappelons l'énoncé prouvé dans [7] théorème 1.6 et remarque 1.7 que nous voulons utiliser : si A_1 et A_2 sont pleinement de type GSp de dimensions respectives g_1 et g_2 et non isogènes sur $\bar{K}$, alors pour tout ℓ suffisamment grand (dépendant de A_1 et A_2), on a

$$\rho_{\ell,A_1\times A_2}\left(\mathrm{Gal}(K(A_1\times A_2[\ell^\infty])/K(\mu_{\ell^\infty}))\right) = \mathrm{Sp}_{2g_1}(\mathbb{Z}_\ell)\times \mathrm{Sp}_{2g_2}(\mathbb{Z}_\ell).$$

Supposons donc par l'absurde que A_1 et A_2 ne sont pas $\bar{K}$-isogènes. Dans ce cas, pour tout ℓ assez grand, on a

$$\mathrm{Card}\left(\rho_{\ell,A_1\times A_2}(G_K)\right) \gg\ll \ell^{\dim(\mathrm{Sp}_{2g_1})+\dim(\mathrm{Sp}_{2g_2})+1} = \ell^{2g_1^2+g_1+2g_2^2+g_2+1},$$

et de même, A_1 étant pleinement de type GSp,

$$\mathrm{Card}\left(\rho_{\ell,A_1}(G_K)\right) \gg\ll \ell^{2g_1^2+g_1+1}.$$

En particulier, on en déduit que

$$\forall \ell\in\Lambda,\quad c \geq [K\left(A_1[\ell],A_2[\ell]\right):K\left(A_1[\ell]\right)] \gg\ll \ell^{2g_2^2+g_2}.$$

Le dernier terme tendant vers l'infini avec ℓ ceci est contradictoire, donc A_1 et A_2 ne peuvent être $\bar{K}$-isogènes. □

Passons maintenant à la preuve alternative (B) et aux lemmes intermédiaires que nous ré-utiliserons dans le paragraphe 4.

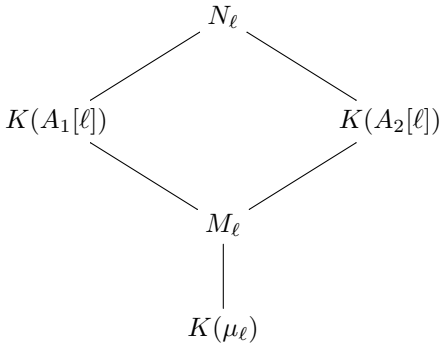
Lemme 3.3 *On suppose ici qu'il existe $c>0$ et un ensemble Λ infini tel que pour tout $\ell\in\Lambda$, on a*

$$[N_\ell : K\left(A_1[\ell]\right)] \leq c.$$

Alors, $g_1=g_2$ et pour tout $\ell\in\Lambda$ assez grand, on a

$$\textit{soit}\ \ K(A_1[\ell])=K(A_2[\ell]),\ \ \textit{soit pour tout } i\in\{1,2\},\ \textit{on a}\ \ [N_\ell:K\left(A_i[\ell]\right)]=2=[K\left(A_i[\ell]\right):M_\ell].$$

Démonstration : La preuve est une adaptation formelle de la remarque 2.4 de [3]. Soit $\ell\in\Lambda$, $\ell\geq 5$. Considérons la tour d'extensions suivante



et notons H_ℓ (respectivement H'_ℓ) le groupe correspondant à l'extension $K(A_1[\ell])/M_\ell$ (respectivement $K(A_2[\ell])/M_\ell$). L'extension $M_\ell/K(\mu_\ell)$ est galoisienne donc si ℓ est assez grand, les variétés abéliennes A_1 et A_2 étant pleinement de type GSp, les groupes H_ℓ et H'_ℓ sont des sous-groupes distingués de $\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)$, respectivement $\mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)$. Par le lemme 2.4 on en déduit que ces groupes sont soit $\{I_{2g_i}\}$, soit $\{\pm I_{2g_i}\}$ (pour $i\in\{1,2\}$), ou bien le groupe spécial symplectique tout entier. Nous allons distinguer les différents cas possibles.

1. Si $\mathrm{H}_\ell = \{I_{2g_1}\}$, alors l'extension $K(A_1[\ell])$ est incluse dans $K(A_2[\ell])$ et donc $N_\ell = K(A_2[\ell])$. Dès lors, soit $\mathrm{H}'_\ell = \{I_{2g_2}\}$ et donc $K(A_1[\ell]) = K(A_2[\ell])$; soit $\mathrm{H}'_\ell = \{\pm I_{2g_2}\}$ et on obtient l'égalité de cardinaux suivante : $2 \times |\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)| = |\mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)|$ donc $g_1 = g_2$ par le lemme 2.3 et l'égalité précédente est alors impossible. Enfin, si $\mathrm{H}'_\ell = \mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)$, alors $K(A_1[\ell]) = M_\ell = K(\mu_\ell)$ ce qui est impossible. Donc

$$\mathrm{H}_\ell = \{I_{2g_1}\} \Rightarrow \mathrm{H}'_\ell = \{I_{2g_2}\}.$$

2. Si $\mathrm{H}_\ell = \{\pm I_{2g_1}\}$, on voit par le même argument de cardinalité que précédemment que $\mathrm{H}'_\ell = \{I_{2g_2}\}$ est impossible. De même, si $\mathrm{H}'_\ell = \mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)$, alors $M_\ell = K(\mu_\ell)$ et donc $\mathrm{H}_\ell = \mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)$ ce qui est absurde. Donc

$$\mathrm{H}_\ell = \{\pm I_{2g_1}\} \Rightarrow \mathrm{H}'_\ell = \{\pm I_{2g_2}\}.$$

3. Si $\mathrm{H}_\ell = \mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)$, alors $M_\ell = K(\mu_\ell)$ donc on a $\mathrm{H}'_\ell = \mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)$. Or les extensions $K(A_1[\ell])$ et $K(A_2[\ell])$ sont linéairement disjointes au dessus de M_ℓ donc $|\mathrm{H}'_\ell| = [N_\ell : K(A_1[\ell])] \leq c$, ce qui est impossible si ℓ est suffisamment grand.

Dans les deux premiers cas précédents, les seuls pouvant se produire, notons que l'on aboutit à une égalité de la forme

$$\left|\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)/\mathrm{H}_\ell\right| = \left|\mathrm{Sp}_{2g_2}(\mathbb{F}_\ell)/\mathrm{H}'_\ell\right|$$

et le lemme 2.3 implique $g_1 = g_2$. □

Proposition 3.4 *Soit $\ell \geq 5$ un nombre premier tel que $G_{\ell,A_i} = \mathrm{GSp}_{2g_i}(\mathbb{F}_\ell)$ pour $i \in \{1,2\}$. On suppose de plus que $g_1 = g_2$ et que $[N_\ell : K(A_1[\ell])] \leq 2$. Alors il existe un caractère quadratique*

$$\varepsilon_\ell : G_K \to \{\pm 1\} \text{ tel que } \rho_{\ell,A_1} \sim \varepsilon_\ell \otimes \rho_{\ell,A_2}.$$

Si de plus $\ell \geq 4g+1$, alors ce caractère ε_ℓ est non ramifié en toute place ultramétrique non ramifiée sur $\mathbb{Q}$ en laquelle A_1 et A_2 ont bonne réduction. En particulier, lorsque ℓ varie, le noyau $\ker(\varepsilon_\ell)$ varie dans un ensemble fini.

Démonstration : Pour la première partie de l'énoncé, il s'agit d'une adaptation en dimension supérieure du lemma 2.5 de [3], lui même basé sur la preuve du lemme 8 de [10]. Pour la seconde partie de l'énoncé, concernant le caractère quadratique ε_ℓ, il s'agit également de reprendre l'argument de la preuve du lemme 8 de [10] en utilisant le corollaire 3.4.4. de [9] en lieu et place des corollaires 11 et 12 de [10]. Nous utiliserons ici librement les notations du début du paragraphe. Nous noterons $g = g_1 = g_2$. Pour $i \in \{1,2\}$, le corps $L_{A_i,\ell}$ est le sous-corps de $K(A_i[\ell])$ fixé par le centre de $\mathrm{Gal}(K(A_i[\ell])/K)$. Nous allons montrer que

$$L_{A_1,\ell} = L_{A_2,\ell}. \tag{2}$$

Admettons (2) un instant et voyons comment conclure à l'existence du caractère quadratique ε_ℓ : par la théorie de Galois on obtient $\ker(\overline{\rho}_{A_1,\ell}) = \ker(\overline{\rho}_{A_2,\ell})$. Ainsi, à composition à gauche par un automorphisme de $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ près, $\overline{\rho}_{A_1,\ell}$ et $\overline{\rho}_{A_2,\ell}$ coïncident. Or $\ell \geq 5$, donc d'après le lemme 2.4 les automorphismes de $\mathrm{PGSp}_{2g}(\mathbb{F}_\ell)$ sont intérieurs et l'action par conjuguaison se fait via un élément de $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. Autrement dit,

$$\exists y \in \mathrm{Sp}_{2g}(\mathbb{F}_\ell)\ \forall x \in G_K,\quad \pi_\ell\left(\rho_{A_1,\ell}(x)\right) = \pi_\ell\left(y^{-1}\rho_{A_2,\ell}(x)y\right).$$

Ainsi il existe un morphisme $\varepsilon_\ell : G_K \to \mathbb{F}_\ell^\times$ tel que

$$\forall x \in G_K,\quad \rho_{A_1,\ell}(x) = \varepsilon_\ell(x)\left(y^{-1}\rho_{A_2,\ell}(x)y\right).$$

En composant par le morphisme multiplicateur et en appliquant le lemme 2.2 on en déduit que

$$\forall x \in G_K,\quad \varepsilon_\ell(x)^2 = 1.$$

Reste à prouver l'assertion (2) pour conclure la première partie de la proposition. C'est ce que nous allons nous attacher à faire ci-dessous.

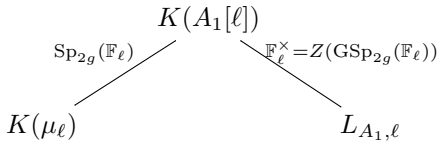
Commençons par remarquer que si $K(A_1[\ell]) = K(A_2[\ell])$, il n'y a rien à montrer. En utilisant les hypothèses et le lemme 3.3, on sait donc que

$$[K(A_1[\ell]) : M_\ell] = [K(A_2[\ell]) : M_\ell] = 2. \tag{3}$$

Notamment, la représentation ρ_{ℓ,A_1} envoie M_ℓ sur l'unique sous-groupe $\{\pm I_{2g}\}$ distingué d'ordre 2 de $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.

Fait 1 : Le corps $K(\mu_\ell) \cap L_{A_1,\ell}$ est l'unique sous-extension quadratique de $K(\mu_\ell)/K$.

Pour ℓ assez grand, l'extension $K(\mu_\ell)/K$ est cyclique de groupe de Galois $\mathbb{F}_\ell^\times$. Elle possède donc une et une seule sous-extension quadratique correspondant à l'unique sous-groupe d'indice 2 de $\mathbb{F}_\ell^\times$. On a le diagramme



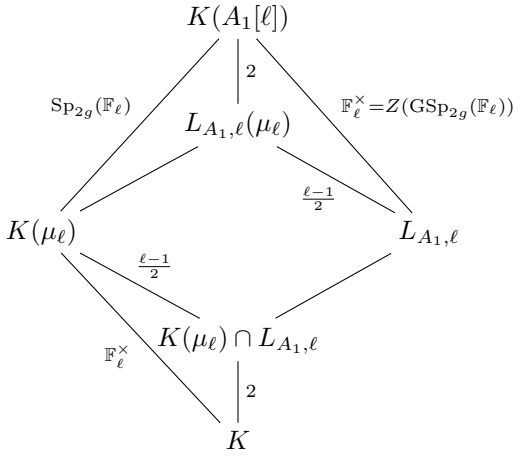
d'extensions de corps. Or le groupe engendré par $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ et $\mathbb{F}_\ell^\times$ (correspondant via la théorie de Galois à l'extension $K(\mu_\ell) \cap L_{A_1,\ell}$) n'est autre que le sous-groupe

$$\{xM \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) \mid x \in \mathbb{F}_\ell^\times,\ M \in \mathrm{Sp}_{2g}(\mathbb{F}_\ell)\}.$$

Ce sous-groupe est d'indice 2 dans $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$. En effet, il est clair sur la définition du multiplicateur λ que $\lambda(xI_{2g}) = x^2$ pour tout scalaire non nul x. Dès lors on conclut en considérant la décomposition $M^2 = \lambda(M)\left(\frac{1}{\lambda(M)}M^2\right)$ ainsi que le fait que les carrés de $\mathbb{F}_\ell^\times$ forment un sous-groupe d'indice deux dans $\mathbb{F}_\ell^\times$ pour ℓ impair. □

Fait 2 : On a l'égalité $M_\ell = L_{A_1,\ell} \cdot K(\mu_\ell)$.

Par construction, $L_{A_1,\ell}$ est le sous-corps de $K(A_1[\ell])$ des invariants par $\mathbb{F}_\ell^\times = Z(\mathrm{GSp}_{2g}(\mathbb{F}_\ell))$. Or on a montré juste avant le fait 1 que M_ℓ est le sous-corps de $K(A_1[\ell])$ des invariants par $\{\pm I_{2g}\} = Z(\mathrm{Sp}_{2g}(\mathbb{F}_\ell))$. On en déduit que $L_{A_1,\ell}$ est inclus dans M_ℓ. L'extension $K(A_1[\ell])/M_\ell$ est de degré deux et on voit en considérant le diagramme d'extensions suivant



que l'extension $K(A_1[\ell])/L_{A_1,\ell}(\mu_\ell)$ est également de degré 2. Ceci conclut la preuve du fait 2. □

L'équation (3) étant symétrique en A_1 et A_2, on en déduit symétriquement que le corps $L_{A_2,\ell}$ vérifie également les faits 1 et 2. Le groupe de Galois $\mathrm{Gal}(M_\ell/K(\mu_\ell)) = \mathrm{PSp}_{2g}(\mathbb{F}_\ell)$ étant simple

non abélien, ceci détermine le corps $L_{A_i,\ell}$ de manière unique et conclut la preuve de la première partie de la proposition.

Passons maintenant à la preuve de la seconde partie de l'énoncé. Soit v une place ultramétrique du corps K telle que A_1 et A_2 ont bonne réduction en v et que v est non ramifiée sur $\mathbb{Q}$. Supposons que la caractéristique de v est ℓ (en effet ε_ℓ est non ramifié en v sinon par le theorem 1 de [14]) et notons $\bar{\mathbb{F}}_\ell$ une clôture algébrique de $\mathbb{F}_\ell$. Notons par ailleurs $\chi_1, \ldots, \chi_{2g}$ (respectivement $\chi'_1, \ldots, \chi'_{2g}$) les caractères du groupe d'inertie modérée en v à valeurs dans $\bar{\mathbb{F}}_\ell^\times$, intervenant dans le module galoisien $A_1[\ell] \otimes \bar{\mathbb{F}}_\ell$ (resp. $A_2[\ell] \otimes \bar{\mathbb{F}}_\ell$), cf. [10] paragraphe 1.13. et [9] corollaire 3.4.4. En notant ε_v la restriction de ε_ℓ au groupe d'inertie en v, on a pour tout i, (quitte à renuméroter les χ'_i)

$$\chi_i = \varepsilon_v \chi'_i.$$

Comme l'indice de ramification de v est 1, le corollaire 3.4.4. de [9] nous dit que les χ_i sont de la forme

$$\chi_i = \theta_{k_1}^{e(k_1)} \ldots \theta_{k_n}^{e(k_n)}$$

où pour tout r, $e(r) \in \{0, 1\}$ et où les θ_{k_i} sont les n caractères fondamentaux de niveau n (cf. [10] p.267 et [9] définition 1.1.1), l'entier n pouvant varier dans $1, \ldots, 2g$. Les invariants des χ_i et χ'_i dans $\mathbb{Q}/\mathbb{Z}$ (cf. [10] paragraphe 1.7) varient dans l'ensemble :

$$X = \left\{ e(k_1)\frac{\ell^{k_1}}{\ell^n - 1} + \cdots + e(k_n)\frac{\ell^{k_n}}{\ell^n - 1} \mid k_i \in \{0, \ldots, n-1\},\ n \in \{1, \ldots, 2g\} \right\}.$$

Enfin, l'invariant de ε_v, $\mathrm{Inv}(\varepsilon_v)$ vaut 0 ou $\frac{1}{2}$ car $\varepsilon_v^2 = 1$. Par ailleurs, $\mathrm{Inv}(\varepsilon_v)$ est de la forme $x - x'$ avec $x = \mathrm{Inv}(\chi_i)$ et $x' = \mathrm{Inv}(\chi'_i)$. En particulier on a $x, x' \in X$. Or si

$$x = e(k_1)\frac{\ell^{k_1}}{\ell^n - 1} + \cdots + e(k_n)\frac{\ell^{k_n}}{\ell^n - 1}, \text{ on a alors}$$

$$0 \leq x \leq \frac{n\ell^{n-1}}{\ell^n - 1} < \frac{2g}{\ell - 1}.$$

En particulier, $|x - x'| < \frac{2g}{\ell - 1}$ et comme $\ell \geq 4g + 1$, on voit que $|x - x'| < \frac{1}{2}$, donc nécessairement l'invariant de ε_v vaut 0 ce qui signifie que ε_v est non ramifié en v.

Pour la dernière assertion de la proposition, notons S l'ensemble des places de bonne réduction de A_1 et A_2. Nous venons de prouver que les caractères ε_ℓ se factorisent à travers le groupe de Galois G_S de la sous-extension maximale de $\bar{K}$ non ramifiée en dehors de S. Mais par le théorème classique de Hermite, il n'existe qu'un nombre fini d'extensions de degré au plus 2 de K, non ramifiées en dehors de S. Autrement dit les noyaux de ε_ℓ varient dans un ensemble fini quand ℓ est variable. □

Nous utiliserons ci-dessous la version suivante des résultats fondamentaux de Faltings [2].

Proposition 3.5 (Faltings) *Soient A et B deux variétés abéliennes sur un corps de nombres K.*

- *Si $\rho_{\ell^\infty,A}$ est isomorphe à $\rho_{\ell^\infty,B}$ alors A est K-isogène à B.*
- *Il existe $C_0 = C_0(A, K)$ telle que si pour un nombre premier $\ell \geq C_0$ les représentations modulo ℓ, $\rho_{\ell,A}$ et $\rho_{\ell,B}$ sont isomorphes, alors A est K-isogène à B.*

Démonstration : Dans l'article de Faltings [2], le premier énoncé est démontré dans le Korollar 2, page 361 ; le deuxième énoncé, pour les représentations modulo ℓ, peut se déduire des démonstrations comme cela est montré par Zarhin [15], Corollary 5.4.5. □

Preuve (B) du théorème 3.1 Soit Λ un ensemble infini de premiers comme dans l'énoncé et soit $\ell \in \Lambda$, $\ell \geq 4g + 1$. D'après le lemme de réduction 3.3, on voit que A_1 et A_2 ont même dimension

et que pour $i \in \{1,2\}$, on a $[N_\ell : K(A_i[\ell])] \in \{1,2\}$ (quitte à enlever un nombre fini de premiers de l'ensemble Λ). La proposition 3.4 entraîne alors qu'il existe un caractère quadratique

$$\varepsilon_\ell : G_K \to \{\pm 1\} \text{ tel que } \rho_{\ell,A_1} \sim \varepsilon_\ell \otimes \rho_{\ell,A_2},$$

et que de plus quand ℓ est variable, les ε_ℓ varient dans un ensemble fini. Quitte à remplacer Λ par une sous-partie infinie, on peut donc supposer que le caractère ε_ℓ est indépendant de ℓ : notons le ε. Sur l'extension K' de K correspondant au noyau de ε, on obtient donc que les représentations ρ_{ℓ,A_1} et ρ_{ℓ,A_2} sont isomorphes. Par la seconde partie de la proposition 3.5 ceci implique que A_1 et A_2 sont K'-isogènes, ce qui conclut la démonstration. □

4 Preuve du théorème 1.3

Nous conservons dans la suite les notations de la partie précédente (notamment A_1 et A_2 sont pleinement de type GSp), nous notons $G_{\ell,A_1\times A_2} \subset G_{\ell,A_1} \times G_{\ell,A_2}$ le groupe de Galois correspondant à $A_1 \times A_2$ et π_i la projection de $G_{\ell,A_1\times A_2}$ sur G_{ℓ,A_i} pour $i \in \{1,2\}$. Rappelons que comme indiqué dans le paragraphe 1.2 concernant la structure de la preuve (de la partie suffisante) du théorème principal 1.3, nous décomposons cette preuve en trois étapes. Dans la suite, on suppose donné un sous-ensemble S de places finies v de K, de corps résiduel $\mathbb{F}_v$, de bonne réduction pour A_1 et A_2, de densité analytique 1 et nous supposons également donné un sous-ensemble Λ infini de l'ensemble des nombres premiers tel que

$$\forall v \in S,\ \forall \ell \in \Lambda \quad (\ell \mid \mathrm{Card}(A_1(\mathbb{F}_v)) \iff \ell \mid \mathrm{Card}(A_2(\mathbb{F}_v)))\,. \tag{4}$$

Nous utiliserons le lemma 4.6 de [5] que nous rappelons ci-dessous.

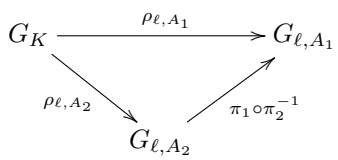
Lemme 4.1 ([5]) *Soit $\ell \in \Lambda$. Sous l'hypothèse (4) ci-dessus, on a*

$$\forall (x,y) \in G_{\ell,A_1\times A_2},\ \ \det(x - I_{2g_1}) = 0 \iff \det(y - I_{2g_2}) = 0.$$

4.1 Preuve de l'étape (1)

Lemme 4.2 *Soit $\ell \geq 5$ premier tel que $K(A_1[\ell]) \not\subset K(A_2[\ell])$. Le groupe $\pi_1(\ker(\pi_2))$ est distingué dans G_{ℓ,A_1} et contient l'élément non trivial $-I_{2g_1}$.*

Démonstration : La projection π_1 est surjective et $\ker(\pi_2)$ est distingué dans $G_{\ell,A_1\times A_2}$, ce qui entraîne la première partie de l'assertion. Si $u \in \pi_1(\ker(\pi_2))$, il existe $x \in G_K$ tel que $u = \rho_{\ell,A_1}(x)$ et $\rho_{\ell,A_2}(x) = I_{2g_2}$. De plus on sait par le lemme 2.2 que $\lambda \circ \rho_{\ell,A_1} = \lambda \circ \rho_{\ell,A_2}$, donc en particulier, $\lambda(u) = \lambda(I_{2g_2}) = 1$. Ceci prouve que $\pi_1(\ker(\pi_2))$ est inclus dans le groupe $\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)$. Montrons maintenant que $\pi_1(\ker(\pi_2))$ est non trivial. En effet, dire que $\pi_1(\ker(\pi_2)) = \{I_{2g_1}\}$ équivaut à dire que $\ker(\pi_2) \subset \ker(\pi_1)$ ce qui équivaut visiblement à dire que $\ker(\pi_2)$ est trivial. Dans ce cas le diagramme suivant est commutatif



et on en déduit que $\ker(\rho_{\ell,A_2}) \subset \ker(\rho_{\ell,A_1})$. Ceci entraîne que l'extension $K(A_1[\ell])$ est incluse dans $K(A_2[\ell])$ ce qui contredit l'hypothèse. Ainsi comme $\ell \geq 5$, le lemme 2.4 implique que le groupe $\pi_1(\ker(\pi_2))$ est $\{\pm I_{2g_1}\}$ ou $\mathrm{Sp}_{2g_1}(\mathbb{F}_\ell)$ et notamment $-I_{2g_1} \in \pi_1(\ker(\pi_2))$. □

Nous pouvons maintenant passer à la preuve de l'étape (1) proprement dite : supposons par l'absurde que pour tout $\ell \in \Lambda$ assez grand on a $K(A_1[\ell]) \neq K(A_2[\ell])$. On peut notamment supposer que $\ell \geq 5$ et quitte à intervertir A_1 et A_2, le lemme 4.2 nous assure que l'élément

$(-I_{2g_1}, I_{2g_2})$ est dans $G_{\ell,A_1\times A_2}$. Mais $\det(-I_{2g_1} - I_{2g_1}) \neq 0$ alors que $\det(I_{2g_2} - I_{2g_2}) = 0$. Ceci contredit le lemme 4.1 précédent et conclut la preuve de la première partie de l'étape (1). Pour une infinité de ℓ il est donc vrai que $K(A_1[\ell]) = K(A_2[\ell])$. Notre théorème 3.1 sur les isogénies horizontales permet de conclure que A_1 et A_2 sont $\bar{K}$-isogènes (en effet pour les ℓ concernés $[K(A_1[\ell], A_2[\ell]) : K(A_1[\ell])] = 1$). Notons que nous utilisons ici de manière sous-jacente les résultats de Faltings [2] (proposition 3.5 précédente). □

4.2 Preuve de l'étape (2)

Nous savons maintenant que les variétés abéliennes A_1 et A_2 sont isogènes sur $\bar{K}$. En particulier elles ont même dimension, notée g. De plus par l'étape (1) on sait qu'il existe un sous-ensemble infini Λ_1 de Λ tel que pour $\ell \in \Lambda_1$ on a $[K(A_1[\ell], A_2[\ell]) : K(A_1[\ell])] = 1$. Pour un tel premier $\ell \geq 5$ la proposition 3.4 affirme l'existence d'un caractère quadratique

$$\varepsilon_\ell : G_K \to \{\pm 1\} \text{ tel que } \rho_{\ell,A_1} \sim \varepsilon_\ell \otimes \rho_{\ell,A_2}.$$

De plus en choisissant $\ell \geq 4g + 1$, cette même proposition assure que les caractères ε_ℓ varient dans un ensemble fini (quand ℓ est variable dans Λ_1). Quitte à remplacer Λ_1 par une sous-partie infinie, on peut donc supposer que ε_ℓ est indépendant de ℓ. C'est précisément ce que l'on voulait montrer. □

4.3 Preuve de l'étape (3)

Montrons que ρ_{ℓ,A_1} est isomorphe à ρ_{ℓ,A_2} pour une infinité de ℓ. La conclusion résultera alors de Faltings (proposition 3.5). Pour ce faire nous utiliserons le résultat suivant sur la décomposition d'une place dans une extension de la forme $K(A[\ell])$.

Lemme 4.3 *Soient $p \neq q$ deux nombres premiers et soit A/K une variété abélienne sur un corps de nombres. Soit v une place finie de K au dessus de p, de corps résiduel $\mathbb{F}_v$, telle que A a bonne réduction en v. Le groupe $A(\mathbb{F}_v)$ contient $A[q] \simeq (\mathbb{Z}/q\mathbb{Z})^{2\dim A}$ si et seulement si v est totalement décomposée dans l'extension $K(A[q])/K$.*

Démonstration : Notons π_v l'endomorphisme de Frobenius sur la réduction $A_v/\mathbb{F}_v$ de A/K en une place de bonne réduction v. Notons que p étant premier à q, la réduction modulo v est injective sur les points de q-torsion et on identifie $A_v[q]$ et $A[q]$ via cette injection. Par construction on a

$$\ker(\pi_v - \mathrm{Id}) = A_v(\mathbb{F}_v).$$

Donc $A_v(\mathbb{F}_v)$ contient le groupe $A_v[q]$ si et seulement si $\pi_{v|A_v[q]} = \mathrm{Id}_{A_v[q]}$. Cette dernière assertion est équivalente à dire que le groupe de décomposition $D_q(v/p)$ est trivial dans $\mathrm{Gal}(K(A[q])/K)$ et ceci équivaut à dire que v est totalement décomposée dans l'extension $K(A[q])/K$. □

Lemme 4.4 *Soit A/K une variété abélienne pleinement de type* GSp *et L/K une extension finie. Si ℓ est suffisamment grand alors $L \cap K(A[\ell]) = K$.*

Démonstration : Il s'agit de la proposition 2.6 de [5] dans laquelle il faut appliquer le corollaire du théorème 3 de [12] en lieu et place du théorème 3 de [10]. □

Pour une variété abélienne A, notons $S_K(A)$ l'ensemble des places finies de K de bonne réduction pour A et notons

$$S_\ell^{td} := \{v \in S_K(A_1) \cap S_K(A_2) \mid v \text{ se décompose totalement dans } K(A_1[\ell])\}.$$

D'après le lemme 4.3 précédent, si $v \in S_\ell^{td}$ alors $A_1(\mathbb{F}_v)[\ell] = A_1[\ell]$. En particulier on voit que $\ell \mid \mathrm{Card}(A_1(\mathbb{F}_v))$. Pour $i \in \{1, 2\}$ et en notant v_ℓ la valuation ℓ-adique sur les entiers, introduisons

$$f_{\ell,A_i} : S_K(A_i) \to \{0, 1\}, \quad \text{définie par } \; v \mapsto \min\{1, v_\ell(\mathrm{Card}(A_i(\mathbb{F}_v)))\}.$$

Par construction $f_{\ell,A_i}(v) = 1$ si et seulement si $\ell \mid \mathrm{Card}(A_i(\mathbb{F}_v))$. Nous venons donc de prouver que si $v \in S_\ell^{td}$ alors $f_{\ell,A_1}(v) = 1$.

Montrons maintenant que nos hypothèses impliquent que $f_{\ell,A_2}(v) = 0$ pour v variant dans un sous-ensemble de densité strictement positive, ce qui contredira l'hypothèse (4). Précisément, on sait qu'il existe un caractère $\varepsilon : G_K \to \{\pm 1\}$ tel que $\rho_{\ell,A_1} \sim \varepsilon \otimes \rho_{\ell,A_2}$. Supposons que ε est non trivial, notons L/K l'extension quadratique correspondant au caractère ε et notons $\zeta_v := \varepsilon(\mathrm{Frob}_v) \in \{\pm 1\}$. Notons S'_ℓ le sous-ensemble de S_ℓ^{td} constitué des v telles que $\zeta_v = -1$. L'ensemble S'_ℓ a une densité non nulle d'après le lemme 4.4. Reste à vérifier que f_{ℓ,A_2} est nulle sur cet ensemble.

La place v est totalement décomposée dans $K(A_1[\ell])$ donc $\rho_{\ell,A_1}(\mathrm{Frob}_v) = \mathrm{Id}_{A_1[\ell]}$. De plus le Frobenius est un générateur topologique du groupe de Galois $G_{\mathbb{F}_v}$ et via l'accouplement de Weil on sait que le groupe μ_ℓ est inclus dans $A_1[\ell]$. Ceci nous permet d'en déduire que si $\sigma \in G_{\mathbb{F}_v}$ alors σ agit trivialement sur μ_ℓ. Notons par ailleurs

$$\pi_{A_i}(T) = \det\left(\mathrm{Id} - T\rho_{\ell,A_i}(\mathrm{Frob}_v)|V_\ell(A_i)\right) \quad \text{pour} \quad i \in \{1,2\}.$$

On voit que v totalement décomposée implique que

$$\pi_{A_1}(T) \equiv \det(\mathrm{Id} - T\mathrm{Id}) \equiv (1-T)^{2g} \mod \ell.$$

Rappelons que $\rho_{\ell,A_1}(\mathrm{Frob}_v)$ est, à conjugaison près, égal à $\varepsilon(\mathrm{Frob}_v)\rho_{\ell,A_2}(\mathrm{Frob}_v)$. Notamment, si de plus $v \in S'_\ell$ on a $\varepsilon(\mathrm{Frob}_v) = -1$ et donc

$$\pi_{A_2}(T) \equiv (1+T)^{2g} \mod \ell.$$

En particulier,

$$\mathrm{Card}(A_2(\mathbb{F}_v)) \equiv \pi_{A_2}(1) \equiv 2^{2g} \not\equiv 0 \mod \ell.$$

Ceci prouve que $f_{\ell,A_2}(v) = 0$ ce qui conclut. □

References

[1] Dieudonné, J. *La géométrie des groupes classiques.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1971.

[2] Faltings, G. *Finiteness Theorems for Abelian Varieties over Number Fields.* translated from the German original [*Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), 349–366.] in : Arithmetic Geometry, G. Cornell, J. H. Silverman (Eds.), New York etc. Springer (1986), 9–27.

[3] Frey, G. et Jarden, M. *Horizontal isogeny theorems.* Forum Math. 14 (2002), 931–952.

[4] Hall, C. *An open image theorem for a general class of abelian varieties.* Bull. Lond. Math. Soc. 43, No. 4 (2011), 703–711.

[5] Hall, C. et Perucca, A. *Radical characterizations of Elliptic curves.* Prépublication arXiv:1109.2440, publiée dans une version courte sous le titre *On the prime divisors of the numbers of points on an elliptic curve.* C. R. Acad. Sci. Paris, Ser. I 351 (2013), 1–3.

[6] Hindry, M. et Ratazzi, N. *Torsion dans un produit de courbes elliptiques.* J. Ramanujam Math. Soc. 25 (2010), 1–31.

[7] Hindry, M. et Ratazzi, N. *Points de torsion sur les variétés abéliennes de type GSp.* J. Institut Math. Jussieu 11, No. 1 (2012), 27–65.

[8] Pink, R. *ℓ-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture.* J. Reine Angew. Math. 495 (1998), 187–237.

[9] Raynaud, M. *Schémas en groupes de type* $(p, \ldots, p)$. Bull. SMF 102 (1974), 241–280.

[10] Serre, J-P. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. 15 (1972), 259–331.

[11] Serre, J-P. *Résumé des cours au Collège de France de 1984-1985, Œuvres. Collected papers. IV*, n° 135. 1985–1998. Springer-Verlag, Berlin, 2000.

[12] Serre, J-P. *Résumé des cours au Collège de France de 1985-1986, Œuvres. Collected papers. IV*, n° 136. 1985–1998. Springer-Verlag, Berlin, 2000.

[13] Serre, J-P. *Lettre à Marie-France Vignéras (10 février 1986), Œuvres. Collected papers. IV* n° 137. 1985–1998. Springer-Verlag, Berlin, 2000.

[14] Serre, J-P. et Tate, J. *Good reduction of abelian varieties.* Ann. of Math. 88 (1968), 492–517.

[15] Zarhin, Y.G. *A finiteness theorem for unpolarized Abelian varieties over number fields with prescribed places of bad reduction.* Invent. Math. 79 (1985), 309–321.