Borne sur la torsion dans les variétés abéliennes de type C.M.

Nicolas Ratazzi

Abstract : Let A be an abelian variety of dimension $g \geq 1$ defined over a number field K. We study the size of the torsion group $A(F)_{\text{tors}}$ where F/K is a finite extension and more precisely we study the possible exponent γ in the inequality $\text{Card}(A(F)_{\text{tors}}) \ll [F : K]^{\gamma}$ when F is any extension of K. In the C.M. case we give an exact formula for the best possible exponent in terms of the characters of the Mumford-Tate group—a torus in this case—and discuss briefly the general case.

Finally we give applications of this result in direction of a conjecture of Rémond generalising the Manin-Mumford conjecture.

Keywords : C.M. Abelian varieties, bound of torsion points.
2000 Mathematics Subject Classification : 11G10, 11G15, 14K15, 11F80.

1 Introduction et résultats

Soit A/K une variété abélienne de dimension g sur un corps de nombres K. On note

$$\gamma(A) = \inf \{x > 0 \ / \exists C > 0, \quad \forall F/K \text{ finie}, \quad |A(F)_{\text{tors}}| \leq C[F : K]^x\} .$$

Dans le cas général, la meilleure estimation de ce nombre est due à Masser [5] et [6].

Théorème 1.1 (Masser) *On a $\gamma(A) \leq g$.*

Dans le cas des courbes elliptiques de type C.M., le résultat de Masser est optimal. On peut se demander ce qu'il en est en dimension supérieure. Dans le cas des variétés abéliennes simples de type C.M., Ribet a donné une minoration de $\gamma(A)$. Précisément, en notant $\omega(n)$ le nombre de facteurs premiers de l'entier n, Ribet [14] montre que

Adresse électronique : ratazzi@math.jussieu.fr, janvier 2005

Théorème 1.2 (Ribet) *Si A/K est une variété abélienne de type C.M., alors, il existe deux constantes strictement positives C_1 et C_2 ne dépendant que de A et K telles que : pour tout entier $n \geq 1$,*

$$C_1^{\omega(n)} \leq \frac{[K(A[n]) : K]}{n^d} \leq C_2^{\omega(n)},$$

où d est la dimension de groupe de Mumford-Tate de A.

Comme corollaire du théorème 1.2, on obtient immédiatement

Corollaire 1.1 *Si A/K est une variété abélienne simple de type C.M., on a*

$$\gamma(A) \geq \frac{2g}{d}$$

où d est la dimension du groupe de Mumford-Tate de A.

En fait nous montrons plus généralement que cette minoration reste valable pour toute variété abélienne. On montre ceci au paragraphe 3.

Théorème 1.3 *Soit A/K une variété abélienne quelconque de dimension g. On a*

$$\gamma(A) \geq \frac{2g}{d}$$

où d est la dimension du groupe de Mumford-Tate de A.

La proposition 3.1 du paragraphe 3 montre qu'il est facile d'obtenir un encadrement de $\gamma(A)$ en fonction de facteurs plus simples. Elle montre notamment qu'il est assez naturel de se restreindre au cas où la variété abélienne est sans facteur carré (*cf.* la définition 1.1) ce que nous ferons dans la suite. Nous obtenons dans le présent article une valeur exacte pour $\gamma(A)$ dans le cas où A/K est une variété abélienne de type C.M., sans facteur carré.

Définition 1.1. On dit qu'une variété abélienne A/K est *sans facteur carré* si elle est isogène sur $\overline{K}$ à un produit $\prod_{i=1}^{d} A_i$ avec les A_i simples et deux à deux non-isogènes.

Pour énoncer notre résultat nous avons besoin de quelques notations supplémentaires. Si A/K est de type C.M., on note T son groupe de Mumford-Tate. Dans le cas C.M. c'est un tore algébrique. On note $X^*(T)$ le groupe des caractères de ce tore (*cf.* le paragraphe suivant pour des définitions précises de ces objets). On note $I = \{\chi_1, \ldots, \chi_{2g}\}$ l'ensemble des caractères diagonalisant (sur $\overline{\mathbb{Q}}$) l'action de T sur l'espace vectoriel $V = H_1(A(\mathbb{C}), \mathbb{Q})$ de dimension $2g$. Soit W un sous-espace vectoriel sur $\mathbb{Q}$ de $X^*(T) \otimes \mathbb{Q}$. On pose

$$n(W) = \mathrm{Card}\left(\{\chi \in I \ / \ \ \chi \in W\}\right), \quad \text{et} \quad d(W) = \dim W.$$

Définition 1.2. On définit un invariant $\alpha(A)$ comme suit :

$$\alpha(A) = \sup\left\{\frac{n(W)}{d(W)} \ / \ W \text{ sous-}\mathbb{Q}\text{-espace vectoriel non nul de } X^*(T)\otimes\mathbb{Q}\right\}.$$

Remarque 1.1. Le nombre $\alpha(A)$ ne dépend en fait que du $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $X^*(T)$. En particulier, étant donné un tore $T/\mathbb{Q}$, ce nombre est calculable explicitement.

Avec ces notations, suivant une stratégie suggérée par Serre, notre résultat principal est le suivant :

Théorème 1.4 *Soit A/K une variété abélienne sans facteur carré, de type C.M., de dimension g. On a l'égalité*

$$\gamma(A) = \alpha(A).$$

Remarque 1.2. Notons quelque chose qui n'est pas évident *a priori* : l'exposant $\gamma(A)$ est un nombre rationnel.

Par ailleurs, nous calculons une majoration de $\alpha(A)$ en fonction de g et, dans certains cas particuliers nous pouvons même calculer sa valeur exacte en fonction de g et $d = \dim T$.

Théorème 1.5 *Soit A/K une variété abélienne sans facteur carré, de type C.M., de dimension g. On a*

$$\alpha(A) \leq \frac{2g}{2+\log_2(g)},$$

où l'on a noté $\log_2$ le logarithme en base 2.

En regroupant ensembles nos théorèmes 1.4 et 1.5, nous obtenons :

Corollaire 1.2 *Soit A/K une variété abélienne de type C.M. de dimension $g \geq 1$, sans facteur carré. On a,*

$$\gamma(A) \leq \frac{2g}{2+\log_2(g)},$$

où l'on a noté $\log_2$ le logarithme en base 2.

Remarque 1.3. On sait (cf. par exemple [3] theorem 1.0.) que pour tout g de la forme 2^n, avec $n \geq 2$, il existe une variété abélienne C.M. simple telle que la dimension de son groupe de Mumford-Tate soit précisément $2 + \log_2(g)$. En utilisant le théorème 1.3, ceci prouve que la borne du corollaire précédent sur $\gamma(A)$ est optimale en général.

On voit ainsi que dès lors que la dimension de la variété abélienne est strictement supérieure à 1, ceci raffine le résultat de Masser (dans le cas de type C.M.) :

Corollaire 1.3 *Soit A/K une variété abélienne sans facteur carré, de type C.M. et de dimension $g \geq 2$. Alors,*

$$\gamma(A) < g.$$

Passons maintenant aux cas particuliers dans lesquels on peut calculer explicitement la constante $\alpha(A)$ et donc $\gamma(A)$. On introduit pour cela une définition :

Définition 1.3. On dit qu'une variété abélienne A de type C.M., de dimension g est de type *non-dégénéré* si la dimension du groupe de Mumford-Tate T de A est $g+1$.

Remarque 1.4. Soit A une variété abélienne de type C.M. de dimension g. Notons d la dimension du groupe de Mumford-Tate de A. On a

$$2 + \log_2(g) \leq d \leq g + 1,$$

la minoration de d étant due à Ribet [14].

Remarque 1.5. On sait par un théorème de Yanai [21] que si A est une variété abélienne simple de type C.M. et de dimension un entier g premier, alors A est de type non dégénéré.

Proposition 1.1 *Soit A/K une variété abélienne simple, de type C.M., de dimension g. Si le type de A est non-dégénéré ou si g est inférieur ou égal à 7, alors*

$$\alpha(A) = \frac{2g}{d}$$

où d est la dimension du groupe de Mumford-Tate de A.

Remarque 1.6. Il suffit en fait dans la proposition précédente de montrer la majoration de $\alpha(A)$. L'égalité découle alors de notre théorème 1.4 et du corollaire 1.1.

Enfin il y a également un dernier cas où l'on sait calculer la valeur de $\gamma(A)$: si A est une courbe elliptique sans multiplication complexe. Dans ce cas on connait le groupe de Mumford-Tate de A, c'est le groupe algébrique GL_2 sur $\mathbb{Q}$.

Proposition 1.2 *Si E/K est une courbe elliptique sans multiplication complexe, alors*

$$\gamma(E) = \frac{1}{2}.$$

Remarque 1.7. Dans ce dernier cas on a $\frac{2g}{d} = \frac{1}{2}$ et on trouve encore l'égalité $\gamma(A) = \frac{2g}{d}$.

Au vu des deux propositions 1.1 et 1.2 précédentes et au vu de notre théorème 1.3, on est tenté de poser la question suivante :

Question : si A/K est une variété abélienne sans facteur carré, de dimension $g \geq 1$, a-t-on

$$\gamma(A) = \frac{2g}{d},$$

où d est la dimension du groupe de Mumford-Tate de A ?

La réponse à cette question est probablement non, mais déjà dans le cas des variétés abéliennes de type C.M., il serait intéressant d'avoir un contre-exemple.

Pour conclure cette introduction nous donnons un exemple d'application des théorèmes 1.4 et 1.5 concernant une conjecture de Rémond [13] généralisant la conjecture de Manin-Mumford. Nous avons pour cela besoin de quelques notations :

Définition 1.4. Soit X/K une courbe incluse dans une variété abélienne A/K. On dit que X *est transverse* si X n'est contenue dans aucun translaté de sous-variété abélienne de A.

Soient A/K une variété abélienne sur un corps de nombres, X une courbe transverse de A et r un entier. Suivant Bombieri, Masser et Zannier [1] dans le cas de $\mathbb{G}_m^n$ et Rémond [13] dans le cas des variétés abéliennes, on s'intéresse au problème suivant : on considère l'ensemble

$$A^{[r]} := \bigcup_{\operatorname{codim} G \geq r} G(\overline{K})$$

où l'union porte sur les sous-groupes algébriques fermés de A de codimension au moins r. À quelle condition sur r peut-on garantir que l'ensemble $X(\overline{K}) \cap A^{[r]}$ est fini ? C'est essentiellement à ce problème qu'est consacré l'article de Rémond. Notons que dans le cas le plus faible possible, si $r = \dim A$, on retrouve déjà la conjecture de Manin-Mumford. Si A est une puissance d'une courbe elliptique, on peut voir que $X(\overline{K}) \cap A^{[1]}$ est infini, donc on doit nécessairement prendre $r \geq 2$.

Conjecture 1.1 (Rémond) [13] *Soient A/K une variété abélienne sur un corps de nombres K et X une courbe transverse dans A. L'ensemble $X(\overline{K}) \cap A^{[2]}$ est fini.*

Dans le cas des variétés abéliennes de type C.M. il obtient un résultat inconditionnel mais sensiblement plus faible. On se donne A une variété abélienne de type C.M., isogène au produit $\prod_{i=1}^m A_i^{n_i}$ où les A_i sont des variétés abéliennes simples de dimension respective g_i, deux à deux non-isogènes.

Théorème 1.6 (Rémond) [13] *Soient A/K une variété abélienne de type C.M. et X une courbe transverse dans A, alors $X(\overline{K}) \cap A^{[2+\sum_{i=1}^m g_i]}$ est fini.*

Comme nous l'expliquons dans [12], en utilisant notre corollaire 1.2 concernant la borne sur les points de torsion pour les variétés abéliennes de type C.M., ainsi qu'un résultat de minoration de hauteur faisant l'objet de l'article séparé [12], nous améliorons ceci et obtenons un résulat optimal dans le cas d'une puissance d'une variété abélienne simple de type C.M. :

Théorème 1.7 ([12]) *Soit A/K une variété abélienne C.M., isogène à une puissance d'une variété abélienne simple. Soit X une courbe transverse dans A. L'ensemble*

$$X(\overline{K}) \cap A^{[2]}$$

est fini.

Ceci généralise le résultat de Viada [20], valable pour une puissance d'une courbe elliptique C.M., au cas d'une puissance d'une variété abélienne C.M. simple de dimension quelconque. On peut même donner un résultat un peu plus général en fonction de exposants $\gamma(A_i)$ correspondant aux différents facteurs simples de A : voir la remarque 1.5. de [12].

Plan de l'article : on commence tout d'abord par rappeler ce qu'est le groupe de Mumford-Tate d'une variété abélienne de type C.M. Nous donnons au paragraphe 3 suivant une preuve de la minoration de $\gamma(A)$ annoncée dans le théorème 1.3. Ensuite nous donnons au paragraphe 4 une preuve du théorème 1.5. Les paragraphes 5 et 6 sont consacrés à la preuve du résultat principal : l'inégalité $\gamma(A) \leq \alpha(A)$ dans le théorème 1.4. On commence pour cela par se ramener au cas l-adique. Ensuite, étant donné un sous-groupe H de $A[l^\infty]$, on veut majorer son cardinal par une puissance convenable de $[K(H) : K]$. Pour se faire on décompose essentiellement H en une somme directe de sous-groupes H_i plus simples. Ceci permet de majorer le cardinal de H en fonction de la somme des cardinaux des H_i. On donne ensuite une minoration de $[K(H) : K]$ par récurrence sur le nombre de H_i intervenant. On utilise pour cela le fait que les points à valeurs dans $\mathbb{Z}/l^n\mathbb{Z}$ d'un tore $T/\mathbb{Q}$ sont essentiellement de l'ordre de $l^{n \dim T}$. Dans le paragraphe 7 on particularise la construction faite auparavant au cas d'un groupe H inclus dans $A[l]$ pour obtenir l'inégalité $\gamma(A) \geq \alpha(A)$. Enfin on s'intéresse aux cas particuliers correspondant aux propositions 1.1 et 1.2 dans le dernier paragraphe.

Remerciements : Je tiens ici à exprimer ma sincère gratitude envers Jean-Pierre Serre. La preuve du théorème 1.4 est en effet basée sur une stratégie de preuve qu'il a eu la gentillesse de m'expliquer.

2 Le groupe de Mumford-Tate

2.1 Caractères et cocaractères

On commence avant tout par rappeler la notion de groupe des caractères d'un tore.

Définition 2.1. Soit T/k un tore algébrique sur un corps k. On note $\overline{k}$ la cloture séparable de k. On appelle *groupe des caractères de T* et on note $X^*(T)$ le groupe

$$X^*(T) = \mathrm{Hom}_{\overline{k}-\text{gr-alg}}\left(T_{\overline{k}}, \mathbb{G}_{m,\overline{k}}\right).$$

On définit de même le *groupe des cocaractères de T* et on note $X_*(T)$ le groupe

$$X_*(T) = \mathrm{Hom}_{\overline{k}-\text{gr-alg}}\left(\mathbb{G}_{m,\overline{k}}, T_{\overline{k}}\right).$$

On sait que le groupe des endomorphismes de $\mathbb{G}_m$ est isomorphe à $\mathbb{Z}$. Ceci nous donne un accouplement parfait

$$\langle \cdot, \cdot \rangle : X^*(T) \times X_*(T) \to \mathbb{Z}.$$

On note $X^*(T) \otimes \mathbb{Q}$ le $\mathbb{Q}$-espace vectoriel déduit de $X^*(T)$.

2.2 Groupe de Mumford-Tate

Soit A/K un variété abélienne de type C.M. On note $V = H_1(A(\mathbb{C}), \mathbb{Q})$ le premier groupe d'homologie de la variété analytique complexe $A(\mathbb{C})$ à coefficients dans $\mathbb{Q}$. On définit le groupe de Mumford-Tate en suivant [8] et [7].

On introduit pour cela le tore $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_{m,\mathbb{C}})$, restriction des scalaires à la Weil de $\mathbb{C}$ à $\mathbb{R}$ du groupe multiplicatif. C'est un $\mathbb{R}$-tore algébrique de dimension 2. Son groupe des caractères, $X^*(\mathbb{S})$ est engendré par deux éléments : z et z' tels que les applications induites sur les points $\mathbb{C}^* = \mathbb{S}(\mathbb{R}) \subset \mathbb{S}(\mathbb{C}) \to \mathbb{G}_{m,\mathbb{C}}(\mathbb{C}) = \mathbb{C}^*$ soient respectivement l'identité et la conjugaison complexe. L'élément non-trivial de $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ échange les caractères z et z'. On note μ l'unique cocaractère de $S_{\mathbb{C}}$ tel que $z' \circ \mu$ est trivial et $z \circ \mu = \mathrm{Id}$. On note de même μ' le cocaractère "conjugué". Avec le tore $\mathbb{S}$ arrive naturellement (par les propriétés fonctorielles de la restriction des scalaires à la Weil) un $\mathbb{R}$-homomorphisme

$$w : \mathbb{G}_{m,\mathbb{R}} \to \mathbb{S},$$

appelé *morphisme de poids*. Dire que V est munie d'une $\mathbb{Q}$-structure de Hodge de poids 1 équivaut à dire qu'il existe un $\mathbb{R}$-homomorphisme $h : \mathbb{S} \to \mathrm{GL}_{V_{\mathbb{R}}}$ tel que

$$h \circ w : \mathbb{G}_{m,\mathbb{R}} \to \mathrm{GL}_{V_{\mathbb{R}}}$$

est défini sur $\mathbb{Q}$ (autrement dit provient d'un $\mathbb{Q}$-homomorphisme : $\mathbb{G}_{m,\mathbb{Q}} \to \mathrm{GL}_V$), et est donné sur les points par $x \mapsto x\mathrm{Id}$.

Définition 2.2. Le *groupe de Mumford-Tate* $T/\mathbb{Q}$ de A est le plus petit $\mathbb{Q}$-sous-groupe algébrique G de GL_V (vu comme $\mathbb{Q}$-schéma en groupes) tel que, après extension des scalaires à $\mathbb{R}$, le groupe $G_{\mathbb{R}}$ contient l'image de h.

Remarque 2.8. Dans le cas d'une variété abélienne de type C.M., le groupe de Mumford-Tate est bien un tore algébrique sur $\mathbb{Q}$.

Lemme 2.1 *On note $\chi_1, \ldots, \chi_{2g}$ les caractères de T diagonalisant l'action de T sur V sur $\overline{\mathbb{Q}}$. Il existe deux cocaractères $y, y' \in X_*(T_{\mathbb{C}})$ tels que*

$$\forall 1 \leq i \leq 2g, \quad \langle \chi_i, y + y' \rangle = 1 \quad \text{et} \quad \langle \chi_i, y \rangle \in \{0, 1\}.$$

Démonstration : Il suffit de prendre $y = h \circ \mu$ et $y' = h \circ \mu'$ (cf. par exemple [9] p. 110). □

3 Un encadrement et une minoration de $\gamma(A)$

3.1 Un encadrement de $\gamma(A)$

On donne ici un encadrement élémentaire de $\gamma(A)$ en fonction des $\gamma(A_i)$ où les A_i sont les différents facteurs simples de A.

Proposition 3.1 *Soient $A = \prod_{i=1}^{n} A_i^{n_i}$ une variété abélienne telle que les A_i sont deux à deux non-isogènes. On a*

$$\max\left\{\max_{1\leq i\leq n} n_i\gamma(A_i), (\min_{1\leq i\leq n} n_i)\gamma\left(\prod_{i=1}^{n} A_i/K\right)\right\} \leq \gamma(A) \leq \sum_{i=1}^{n} n_i\gamma(A_i).$$

Démonstration : Cela découle immédiatement de ce que si F/K est une extension finie et $P = (P_1, \ldots, P_n)$ un point de $A^n(F)$, alors P est de torsion si et seulement si tous les P_i le sont. □

Ceci montre que pour avoir un encadrement de $\gamma(A)$ dans le cas général, il suffit de savoir calculer $\gamma(A)$ pour les variétés abéliennes A/K sans facteur carré. Notons par ailleurs que s'il parait difficile *a priori* de réellement améliorer l'encadrement donné dans la proposition, celui-ci peut tout de même être très large. Ceci se voit par exemple en considérant les deux variétés abéliennes $A_1 = E_1 \times E_0^{n_0}$ et $A_2 = \prod_{i=1}^{n_1} E_i \times E_0^{n_0}$ où les E_i sont des courbes elliptiques C.M. deux à deux non-isogènes définies sur un corps de nombres K et où n_0 et n_1 sont deux entiers strictement positifs. L'encadrement de la proposition donne dans ces deux cas

$$n_0 \leq \gamma(A_1) \leq n_0 + 1 \text{ et } n_0 \leq \gamma(A_2) \leq n_0 + n_1.$$

3.2 Minoration de $\gamma(A)$

Soit A/K une variété abélienne quelconque de dimension g. Soient l un nombre premier et G_l l'image de la représentation l-adique de $\mathrm{Gal}(\overline{K}/K)$ dans $\mathrm{GL}_{2g}(\mathbb{Z}_l) \simeq \mathrm{GL}(T_l(A))$. On note $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$ et $\overline{G_l}$ l'adhérence de Zariski de G_l dans le $\mathbb{Q}_l$-schéma en groupes $\mathrm{GL}_{V_l(A)}$. Enfin on note d la dimension de $\overline{G_l}$.

Proposition 3.2 *Avec les notations précédentes, on a*

$$\gamma(A) \geq \frac{2g}{d_M}$$

où d_M est la dimension du groupe de Mumford-Tate de A.

Démonstration : On se donne un premier l, un entier strictement positif n et le groupe $H = A[l^n]$. On veut montrer que

$$l^{2gn} = |H| \geq c(A/K)[K(H) : K]^{\frac{2g}{d_M}}$$

où $c(A/K)$ est une constante ne dépendant que de A/K. Pour cela on introduit les voisinages de l'identité suivants de $\mathrm{GL}_{2g}(\mathbb{Z}_l)$:

$$\forall n \in \mathbb{N}, \quad V_n := \{x \in \mathrm{GL}_{2g}(\mathbb{Z}_l) \ / \ x = \mathrm{Id} \bmod l^n\}, \quad \text{et} \quad G_n = G \cap V_n.$$

On vérifie immédiatement que pour tout entier n positif, G_n/G_{n+1} et V_n/V_{n+1} sont des $\mathbb{F}_l$-espaces vectoriels, où on a noté $\mathbb{F}_l$ le corps à l éléments. Par ailleurs, pour tout n positif, on a les inclusions de groupes

$$G_n/G_{n+1} \hookrightarrow G_{n+1}/G_{n+2}, \quad \text{et} \quad G_n/G_{n+1} \hookrightarrow V_n/V_{n+1},$$

la première inclusion étant définie par la multiplication par l^n et la seconde étant l'identité. De plus, pour tout entier n, V_n/V_{n+1} s'injecte dans l'espace tangent de $\mathrm{GL}_{2g}(\mathbb{F}_l)$ en l'identité. Notons

$$d_n = \dim_{\mathbb{F}_l} G_n/G_{n+1}.$$

La suite $(d_n)_{n\in\mathbb{N}}$ est croissante et stationnaire à partir d'un certain rang n_0. On note d_∞ sa limite. le groupe G_{n_0} est limite profinie des groupes $G_{n_0}/G_{n_0+k} \simeq (\mathbb{Z}/l^k\mathbb{Z})^{d_\infty}$. Ainsi le groupe G_{n_0} est isomorphe à $\mathbb{Z}_l^{d^\infty}$. En particulier on en déduit que

$$d_\infty \leq d.$$

On a ainsi :

$$[K(H) : K] = |G/G_n| \leq \prod_{k=0}^{n-1} |G_i/G_{i+1}| \leq l^{nd_\infty} \leq l^{nd}.$$

En élevant ceci à l'exposant $\frac{2g}{d_M}$, on peut conclure sous réserve que d soit effectivement inférieur à d_M. Or on sait par [2] et [11] que pour tout premier l, le groupe de Mumford-Tate $MT(A) \times \mathbb{Q}_l$ contient le groupe $\overline{G_l}$ (quitte à monter au préalable sur une extension K'/K finie ne dépendant que de A). Ceci permet de conclure. □

4 Majoration de l'exposant $\alpha(A)$: le théorème 1.5

Soient K un corps de nombres et A/K une variété abélienne de type C.M., sans facteur carré et de dimension g. On note $\chi_1, \ldots, \chi_{2g}$ les caractères de T diagonalisant l'action de T sur V sur $\overline{\mathbb{Q}}$. L'hypothèse faite sur A, à savoir qu'elle est sans facteur carré, entraîne en particulier que les caractères χ_i sont deux à deux distincts. Suivant une idée de Ribet et Lenstra (*cf.* [14] p.87), on peut en fait montrer mieux :

Lemme 4.1 *Les caractères χ_i sont deux à deux distincts modulo* 2.

Démonstration : Soient i et j deux entiers tels que $\chi_i = \chi_j \mod 2$. Montrons que $\chi_i = \chi_j$. Par construction du groupe de Mumford-Tate (cf. par exemple [16] p.180) on sait que en

étendant les scalaires à $\mathbb{C}$, les images de σy, σ décrivant $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, engendrent $T_{\mathbb{C}}$. Ainsi pour montrer que deux caractères coincident, il suffit de montrer que

$$\forall \sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}), \quad \langle \chi_i - \chi_j, \sigma y \rangle = 0.$$

Par le lemme 2.1 on sait que $\langle \chi_i, y \rangle \in \{0, 1\}$, et de même pour j. On en déduit donc que $\langle \chi_i - \chi_j, y \rangle \in \{-1, 0, 1\}$ On conclut en remarquant qu'un nombre dans cet ensemble vaut zéro modulo 2 si et seulement il est nul. Par ailleurs, si $\chi \in I = \{\chi_1, \ldots, \chi_{2g}\}$, alors $\sigma(\chi) \in I$ pour tout σ. Ceci conclut. □

Remarque 4.9. La même preuve montre plus généralement que les χ_i sont deux à deux distincts modulo l pour tout nombre premier l.

Lemme 4.2 *Soient W un sous-$\mathbb{Q}$-espace vectoriel non nul de $X^*(T) \otimes \mathbb{Q}$ et $\chi_1, \ldots, \chi_n$ les caractères (appartenant à la famille $\chi_1, \ldots, \chi_{2g}$ précédemment définie) contenus dans W. Alors pour tout entier i compris entre 1 et n, les $\chi_i \mod 2$ sont contenus dans l'hyperplan affine $H_1 = \{\chi \mod 2 \ / \ \langle \chi, y + y' \rangle = 1\}$ de W.*

Démonstration : Ceci découle de la propriété $\langle \cdot, y + y' \rangle = 1$ du lemme 2.1. □

Corollaire 4.1 *Avec les notations précédentes, on a : $n \leq 2^{\dim W - 1}$.*

Corollaire 4.2 *On a*

$$\alpha(A) \leq \frac{2g}{2 + \log_2 g}$$

où $\log_2$ désigne le logarithme en base 2.

Démonstration : Soit W un sous-$\mathbb{Q}$-espace vectoriel de $X^*(T) \otimes \mathbb{Q}$. On découpe la preuve en deux morceaux :

1. Si $\dim W \leq 2 + \log_2 g$, alors la croissance de la fonction $x \mapsto \frac{2^{x-1}}{x}$ permet de conclure.
2. Sinon on majore naïvement $n(W)$ par $2g$ ce qui permet encore de conclure. □

5 Le théorème 1.4 : réduction au cas l-adique

On va pour l'instant simplement montrer l'inégalité

$$\gamma(A) \leq \alpha(A). \tag{1}$$

On montrera l'inégalité contraire au paragraphe 7.

Quitte à augmenter K, on peut supposer (et on le fait) que tous les endomorphismes de A sont définis sur K et que A/K a bonne réduction en toute place (ceci car une variété abélienne de type C.M. a potentiellement bonne réduction). On peut également remplacer K par son corps de classe de Hilbert.

Lemme 5.1 *Il existe une constante $C(A/K)$ ne dépendant que de A et de K telle que : pour toute extension finie L/K, en notant n_L l'ordre du groupe $A(L)_{\text{tors}}$, on a la majoration*

$$\omega(n_L) \leq C(A/K)\frac{\log[L:K]}{\log\log[L:K]}.$$

Démonstration : Soit L/K une extension finie. On note N le plus grand ordre des éléments du groupe $A(L)_{\text{tors}}$ et on note n_L l'ordre de ce groupe. Ce groupe est un sous-groupe de $A[N]$. Ainsi le nombre de facteurs premiers $\omega(n_L)$ est égal à $\omega(N)$. Or on sait que pour tout entier x assez grand,

$$\omega(x) \leq \frac{4\log x}{\log\log x}.$$

Par le théorème 1.1 de Masser (ou dans notre cas C.M. par un résultat de Silverberg [19]), on a,avec une constante C_1 ne dépendant que de A et K,

$$n_L \leq C_1(A/K)[L:K]^{2g+1}.$$

La fonction $x \mapsto \frac{4\log x}{\log\log x}$ étant croissante pour x assez grand, on en déduit le lemme. □

Ceci va nous permettre de nous ramener comme dans Ribet [14] au cas l-adique :

Lemme 5.2 *Pour démontrer l'inégalité (1), il suffit de montrer que : il existe une constante strictement positive $C(A/K)$ ne dépendant que de A/K telle que pour tout nombre premier l et tout sous-groupe fini H de $A[l^\infty]$, stable par Galois, on a*

$$\text{Card}\,(H) \leq C(A/K)[K(H):K]^{\alpha(A)}. \tag{2}$$

Démonstration : Soit L/K une extension finie. Pour tout entier $M \geq 1$, on note $A(L)[M]$ la partie de M-torsion de $A(\overline{K})$ qui est rationnelle sur le corps L. On note $d_L(M) = [K(A(L)[M]) : K]$. Par la théorie de Serre-Tate [17], on sait que l'extension $K(A(L)[M])/K$ ne peut être ramifiée qu'en des places au-dessus de premiers divisant M. Ainsi, si m et M sont premiers entre eux, alors $K(A(L)[m]) \cap K(A(L)[M]) \subset K'$ où K' est le corps de classes de Hilbert de K. En remplaçant K par son corps de classe de Hilbert on obtient ainsi : la fonction

$$M \mapsto d_L(M)$$

est multiplicative au sens arithmétique. Le lemme 5.1 précédent permet de conclure. □

Dans le paragraphe 6 suivant, nous donnons une preuve de l'inégalité (2).

6 Le théorème 1.4 : cas de la l^∞-torsion

6.1 Préliminaires

Soient l un nombre premier et H un sous-groupe fini de $A[l^\infty]$, stable par Galois. Le tore T opère fidèlement sur V. On note comme précédemment $I = \{\chi_1, \ldots, \chi_{2g}\}$ les caractères

diagonalisant l'action de T sur V sur $\overline{\mathbb{Q}}$. Sur $\mathbb{Q}$, on peut décomposer la représentation correspondant à l'action de T en une somme de représentations irréductibles $\rho_1,\ldots,\rho_m$. On note V_{ρ_i} (ou V_i pour soulager les notations) la sous-représentation associée à ρ_i. Chacune des ρ_i se décompose sur $\overline{\mathbb{Q}}$ en $\begin{pmatrix} \chi_i & & \\ & \ddots & \\ & & \chi_i^{\sigma_{t_i}(i)} \end{pmatrix}$ où si $\chi \in I$, on note $\chi^{\sigma_k(\chi)}$ ses différents conjugués et où on note $\sigma_1(\chi),\ldots,\sigma_{t_\chi}(\chi)$ les différents plongements de $\mathbb{Q}(\chi)$ dans $\mathbb{C}$. On note ρ_χ le morceau irréductible de la représentation ρ dans lesquel apparaît χ quand on étend les scalaires à $\overline{\mathbb{Q}}$. Les caractères χ étant deux à deux distincts, les sous-représentations V_ρ sont uniquement déterminées. On note alors

$$T_{\rho_\chi} = \left(V_{\rho_\chi} \otimes \mathbb{Q}_l\right) \cap T_l(A).$$

Soit n le plus petit entier positif tel que $H \subset A[l^n]$. On note alors (abusivement pour la première égalité mais commodément)

$$H_{\rho_\chi} = \bigoplus_{i=1}^{t_\chi} H_{\chi^{\sigma_i\chi}} := \left(T_{\rho_\chi} \bmod l^n\right) \cap H = \left\{P \in H \ / \ \forall t \in T(\mathbb{Z}_l) \quad \rho_\chi(t)P = \rho(t)P\right\},$$

où $\rho_\chi(t)$ agit comme $\rho(t)$ sur V_χ et comme 0 sur $V_{\chi'}$ avec $\chi \neq \chi'$.

Lemme 6.1 *Les différents H_{ρ_χ} correspondants aux différents morceaux irréductibles ρ_χ de ρ sont en somme directe. De plus, chaque H_{ρ_χ} est en tant que groupe de la forme*

$$H_{\rho_\chi} \simeq \prod_{i=1}^{s_\chi} \mathbb{Z}/l^{n_i}\mathbb{Z},$$

où s_χ est un entier inférieur à t_χ. Par ailleurs, la somme $\bigoplus_{\chi\in I} H_\chi$ est un sous-groupe de H d'indice fini, l'indice étant de cardinal borné indépendamment de l.

Démonstration : On note $V_1,\ldots,V_m$ les sous-représentations de V sur $\mathbb{Q}$. On se donne des $\mathbb{Z}$-bases $\mathcal{B}_1,\ldots,\mathcal{B}_m$ de chaque sous-réseau $V_i \cap \mathbb{Z}^{2g}$ de $V \cap \mathbb{Z}^{2g}$. On obtient ainsi une $\mathbb{Z}$-base $\mathcal{B}$ d'un sous-réseau de $V \cap \mathbb{Z}^{2g}$ qui est une $\mathbb{Q}$-base de V. Ceci nous donne : les $V_i \cap \mathbb{Z}^{2g}$ sont en somme directe et l'indice de cette somme dans $\mathbb{Z}^{2g}$ est le nombre entier $\Delta = |\det(\mathcal{B})|$. En tensorisant par $\mathbb{Z}_l$, on en déduit que la somme des T_{ρ_χ} est directe et que l'indice de cette somme dans $T_l(A)$ est majoré par Δ. En réduisant modulo l^n et en intersectant avec H on voit que la somme des H_{ρ_χ} est directe. De plus, si l^n ne divise pas Δ on voit également que l'indice de la somme des $T_{\rho_\chi} \bmod l^n$ dans $A[l^n]$ est fini, majoré indépendamment de l et n par Δ. Si l^n divise Δ (entier fixe), cet indice est évidemment aussi borné indépendamment de l et n. Soit maintenant $x \in H$. En particulier, x est dans $A[l^n]$ donc par ce qui précède, il existe un entier $c > 0$ indépendant de l et n tel que $cx = \sum x_{\rho_\chi}$ chaque x_{ρ_χ} étant dans $T_{\rho_\chi} \bmod l^n$. On a

$$\prod_{\rho_{\chi'} \neq \rho_\chi} (\rho(t) - \rho_{\chi'}(t))cx = \prod_{\rho_{\chi'} \neq \rho_\chi} (\rho_\chi(t) - \rho_{\chi'}(t))x_{\rho_\chi} = \rho_\chi(t)^b x_{\rho_\chi}$$

où b est le nombre de facteurs du produit. En multipliant cette égalité par $\rho_\chi(t)^{-b}$, on constate que x_{ρ_χ} est bien un élément de H. Ceci prouve que la décomposition de cx en $\sum x_{\rho_\chi}$ vaut dans H ce qui prouve que H est, à indice fini près borné indépendamment de l et n, la somme directe des H_{ρ_χ}.

Par ailleurs, en tant que groupe, H_{ρ_χ} est de la forme

$$H_{\rho_\chi} \simeq \prod_{i=1}^{s_\chi} \mathbb{Z}/l^{n_i}\mathbb{Z}$$

et on voit (par exemple en réduisant modulo l et en tensorisant par $\overline{\mathbb{F}}_l$) que s_χ est inférieur à t_χ. Ceci conclut la preuve. □

Notation : avec les notations du lemme précédent, on note

$$n_\chi = \sup_{1\leq i\leq s_\chi} n_i.$$

6.2 Les objets combinatoires

Les caractères $\chi_1, \ldots, \chi_{2g}$ sont définis sur $\overline{\mathbb{Q}}$. Précisément, chaque χ_i est défini sur une extension $\mathbb{Q}(\chi_i)/\mathbb{Q}$ de degré t_i.

Définition 6.1. On dit que le caractère $\chi \in I$ *intervient dans* H si le sous-groupe H_{ρ_χ} de H correspondant à la représentation ρ_χ est non-trivial.

On pose $W_H = \mathrm{Vect}_{\mathbb{Q}}(\chi_1, \ldots, \chi_n)$ l'espace vectoriel engendré par tous les caractères intervenant dans H. À chaque caractère χ_i est associé un entier n_i comme dans le lemme 6.1. On note

$$I = \{\chi_1, \ldots, \chi_n\}, \quad n^{(1)} = \sup_{\chi\in I} n_\chi, \quad W_1 = \mathrm{Vect}_{\mathbb{Q}}\left((\chi^{(1)})^{\sigma_1(1)}, \ldots, (\chi^{(1)})^{\sigma_{t_1}(1)}\right),$$

où $\chi^{(1)}$ est un caractère appartenant à I associé à $n^{(1)}$ et où $\sigma_1(1), \ldots, \sigma_{t_1}(1)$ sont les différents plongements de $\mathbb{Q}(\chi^{(1)})$ dans $\mathbb{C}$. De plus on note

$$I_1 = \{\chi \in I \ / \ \chi \in W_1\}, \quad w_1 = \dim W_1, \quad b_1 = \mathrm{Card}\,(I_1), \quad H_1 = \bigoplus_{\chi\in I_1} H_\chi,$$

et on extrait de I_1 une base $\left\{(\chi^{(1)})^{\sigma_1(1)}, \ldots, (\chi^{(1)})^{\sigma_{w_1}(1)}\right\}$ de W_1.

Remarque 6.10. Notons que si $\chi \in I_1$, alors pour tout plongement σ, on a $\chi^\sigma \in I_1$, l'espace W_1 étant par construction stable par l'action de Galois.

On définit alors par récurrence (jusqu'à ce que $W_i = W_H$) pour tout entier $i \geq 2$

$$n^{(i)} = \sup_{\chi\in I\setminus I_{i-1}} n_\chi, \quad W_i = \mathrm{Vect}_{\mathbb{Q}}\left(W_{i-1}, (\chi^{(i)})^{\sigma_1(i)}, \ldots, (\chi^{(i)})^{\sigma_{t_i}(i)}\right), \quad I_i = \{\chi \in I \ / \ \chi \in W_i\},$$

où $\chi^{(i)}$ est un caractère appartenant à $I \backslash I_{i-1}$, associé à l'entier $n^{(i)}$ et où $\sigma_1(i), \ldots, \sigma_{t_i}(i)$ sont les différents plongements de $\mathbb{Q}(\chi^{(i)})$ dans $\mathbb{C}$. Par ailleurs, on note

$$\forall i \geq 2, \quad w_i = \dim W_i - \dim W_{i-1}, \quad b_i = \mathrm{Card} I_i - \mathrm{Card} I_{i-1}, \quad H_i = \bigoplus_{\chi \in I_i} H_\chi,$$

et on complète, avec des éléments de I_i, la base de W_{i-1} (construite par la récurrence) en une base de W_i. On note r le premier entier i tel que $W_i = W_H$.

Finalement quitte à réordonner les termes, et pour soulager les notations, on suppose que

$$\forall r \geq i \geq 1, \quad \sigma_1(i) = \mathrm{Id}, \quad \chi_i = \chi^{(i)}, \quad \text{et donc} \quad n_i = n^{(i)}.$$

Lemme 6.2 *La famille* $\{\chi_1, \ldots, (\chi_1)^{\sigma_{w_1}(1)}, \ldots, \chi_r, \ldots, (\chi_r)^{\sigma_{w_r}(r)}\}$ *est une base de* W_H*. De plus, pour tout* i *compris entre* 1 *et* r*, le cardinal de* H_i *est majoré par* $l^{\sum_{k=1}^{i} b_k n_k}$ *et* $\sum_{k=1}^{i} b_k$ *est le nombre de caractères (intervenant dans* H*) appartenant à* W_i*.*

Démonstration : Ceci découle immédiatement de la construction de tous les objets et du lemme 6.1. □

6.3 Degré du corps de rationalité

Nous voulons maintenant minorer le degré de l'extension $K(H)/K$. Nous voulons prouver la proposition suivante.

Proposition 6.1 *Il existe une constante strictement positive* C_2*, indépendante de* l *telle que*

$$C_2 l^{\sum_{i=1}^{r} w_i n_i} \leq [K(H) : K].$$

On va faire une preuve de cette proposition par récurrence sur r. On commence par rappeler certains résultats et notations dont nous avons besoin. Les deux premières propositions sont des résultats sur les tores algébriques dus à Ono.

Proposition 6.2 *Soient* T_1 *et* T_2 *deux tores algébriques sur* $\mathbb{Q}$*. Alors, il sont isogènes si et seulement si les* $\mathbb{Q}$*-espaces vectoriels de caractères* $X^*(T_1) \otimes \mathbb{Q}$ *et* $X^*(T_2) \otimes \mathbb{Q}$ *sont isomorphes en tant que* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-modules.*

Démonstration : C'est la proposition 1.3.2. de [10]. □

Notations Soit T un tore et $X^*(T)$ son groupe de caractères. On se donne un sous-tore T_1 de T et un sous-$\mathbb{Z}$-module libre X_1 de $X^*(T)$. On note alors

$$X_1^{\perp} = \bigcap_{\chi \in X_1} \ker \chi, \quad \text{et} \quad T_1^{\perp} = \{\chi \in X(T) \ / \ T_1 \subset \ker \chi\}.$$

Proposition 6.3 *Avec les notations précédentes, on a*

$$X^*(T/T_1) \simeq T_1^{\perp}, \quad \text{et } X^*(T_1) \simeq X^*(T)/T_1^{\perp}.$$

De plus, on a les isomorphismes

$$(X_1^{\perp})^{\perp} \simeq X_1, \quad \text{et} \quad (T_1^{\perp})^{\perp} \simeq T_1.$$

Démonstration : C'est la proposition 1.1.1. de [10]. □

On a ensuite un résultat de Ribet. On introduit pour cela une nouvelle notation :

Notation Si $X/\mathbb{Q}$ est un tore algébrique, si l est un nombre premier et si n est un entier strictement positif, on note

$$X\left(\mathbb{Z}/l^n\mathbb{Z}\right) := X(\mathbb{Z}_l)/X(1+l^n\mathbb{Z}_l).$$

Avec cette notation, le théorème (2.5) de Ribet [14] est le suivant :

Théorème 6.1 (Ribet) *Soient $X/\mathbb{Q}$ un tore algébrique de dimension ν, l un nombre premier et n un entier strictement positif. Il existe deux constantes C et C' strictement positives, ne dépendant que de X (et indépendantes de l et n) telles que*

$$C' l^{n\nu} \geq X\left(\mathbb{Z}/l^n\mathbb{Z}\right) \geq C l^{n\nu}.$$

Par ailleurs, on note G_l le groupe de Galois de l'extension $K(A[l^\infty])/K$ et G_i le groupe de Galois de l'extension $K(A[l^\infty])/K(H_i)$.

Théorème 6.2 *Si A/K est une variété abélienne de type C.M., on a pour tout l premier,*

$$G_l \subset T(\mathbb{Z}_l),$$

cette inclusion étant de conoyau fini, borné indépendamment de l.

Démonstration : Il semble qu'on ne trouve pas de preuve de ce résultat dans la littérature. Toutefois ce résultat découle aisément des travaux de Shimura-Taniyama [18] reformulés par Serre-Tate [17] : on note $\mathcal{O} = \mathrm{End}(A)$ et $E = \mathcal{O} \otimes \mathbb{Q}$. De plus, si F est un produit $F_1 \times \ldots \times F_n$ d'extensions finies $F_i/\mathbb{Q}$, on note $T_F = \prod \mathrm{Res}_{F_i/\mathbb{Q}}$ le produit des restrictions des scalaires à la Weil des différentes extensions. Pour tout premier l on note G_l l'image de la représentation l-adique dans $\mathrm{Aut}(T_l(A))$. Comme c'est une représentation abélienne, on peut en fait la voir comme l'image de l'application

$$I_K \to (\mathcal{O} \otimes \mathbb{Z}_l)^*$$

où I_K est le groupe des idèles de K. De plus on peut en fait remplacer I_K par le produit $\prod_{v/l} U_v$ des groupes des unités des complétions v-adiques de K. Ainsi, on peut voir G_l comme l'image de l'application

$$\lambda_l : T_K(\mathbb{Z}_l) \to T_E(\mathbb{Z}_l),$$

où λ_l est l'application sur les $\mathbb{Z}_l$-points déduite d'une application $\lambda : T_K \to T_E$ entre $\mathbb{Q}$-tores algébriques. De plus sur $\mathbb{Q}_l$ le groupe de Mumford-Tate T est précisément l'adhérence de Zariski de G_l, donc $T(\mathbb{Z}_l) = (\mathrm{Im}\lambda)(\mathbb{Z}_l)$. Par ailleurs il suit de la preuve du théorème (2.4) de [14] que si $f : X_1 \to X_2$ est une application surjective entre tores sur $\mathbb{Q}$, alors le conoyau de $X_1(\mathbb{Z}_l)$ dans $X_2(\mathbb{Z}_l)$ est borné pour tout l et ce indépendamment de l. Ceci permet de conclure. □

Ainsi, au vu du résultat voulu, on peut supposer dans la suite (et on le fait) que $G_l = T_l(\mathbb{Z}_l)$. Ceci étant, on a par définition :

$$\forall 1 \leq i \leq r \quad G_i = \{t \in T(\mathbb{Z}_l) \ / \ \forall P \in H_i \ \ t.P = P\}.$$

Lemme 6.3 *On a l'inclusion*

$$G_i \subset \bigcap_{k=1}^{i} \left\{ t \in T(\mathbb{Z}_l) \ / \forall j \in [\![1, t_k]\!] \ \chi_k^{\sigma_j(k)}(t) = 1 \mod l^{n_k} \right\} =: G_i'.$$

Démonstration : Utilisant les notations du paragraphe précédent, on a

$$\begin{aligned} G_i &= \left\{ t \in T(\mathbb{Z}_l) \ / \ \forall \chi \in I_i, \ \ \forall P \in H_{\rho_\chi}, \ \ \rho_\chi(t)P = P \right\} \\ &\subset \left\{ t \in T(\mathbb{Z}_l) \ / \ \forall 1 \leq k \leq i, \quad \forall P_k \in H_{\rho_{\chi_k}}, \ \ \rho_{\chi_k}(t)P_k = P_k \right\} \\ &= \{ t \in T(\mathbb{Z}_l) \ / \ \forall 1 \leq k \leq i, \ \ \rho_{\chi_k}(t) = 1 \mod l^{n_k} \} \\ &= \bigcap_{k=1}^{i} \left\{ t \in T(\mathbb{Z}_l) \ / \ \forall j \in [\![1, t_k]\!], \ \ \chi_k^{\sigma_j(k)}(t) = 1 \mod l^{n_k} \right\}. \end{aligned}$$

La dernière égalité découle du fait que par constuction, ρ_{χ_k} est équivalente sur $\overline{\mathbb{Q}}$ à $\begin{pmatrix} \chi_k & & \\ & \ddots & \\ & & \chi_k^{\sigma_{t_k}(k)} \end{pmatrix}$. Ceci conclut. □

Remarque 6.11. On a $G_i \subset G_i' \subset G_l$, or on veut montrer que G_l/G_i est "grand". On peut donc, quitte à remplacer G_i par G_i' dans la suite, supposer que $G_i = G_i'$.

Notations Si X et Y sont deux tores algébriques sur $\mathbb{Q}$, on écrit $X \sim Y$ pour dire que X et Y sont isogènes par une isogénie de degré borné indépendamment de l. Si X est un groupe algébrique dont la composante connnexe de l'identité est un tore, on note X^0 cette composante connexe.

Pour tout entier i compris entre 1 et r, on définit les $\mathbb{Q}$-tores suivants :

$$T^{(i)} = \left(\bigcap_{j=1}^{i} \bigcap_{k=1}^{t_j} \ker \chi_j^{\sigma_k(j)} \right)^0.$$

En utilisant les notations de Ono rappelées au début du paragraphe, et en adoptant la convention $T^{(0)} = T$, on pose pour tout entier i compris entre 1 et r,

$$X_i = (T^{(i)})^{\perp} = \left\{ \chi \in X^*(T^{(i-1)}) \ / \ T^{(i)} \subset \ker \chi \right\}.$$

Pour tout $r \geq i \geq 1$ on peut alors trouver un $\mathbb{Q}$-tore T_i tel que

$$T^{(i-1)} \sim T^{(i)} \times T_i.$$

Lemme 6.4 *Pour tout i compris entre 1 et r et avec la convention $T^{(0)} = T$, on peut prendre pour tore T_i, le sous-tore de $T^{(i-1)}$ dont le groupe des caractères est $X^*(T_i) = X_i$. Il est de dimension w_i.*

Démonstration : En utilisant les notations de Ono, on a,

$$T^{(i-1)} \sim X_i^{\perp} \times T_i \iff X^*(T_i) \otimes \mathbb{Q} \simeq X^* \left(T^{(i-1)} / X_i^{\perp} \right) \otimes \mathbb{Q}.$$

Par la proposition 6.3, on a

$$X^* \left(T^{(i-1)} / X_i^{\perp} \right) \simeq (X_i^{\perp})^{\perp} \simeq X_i.$$

Ainsi, on en déduit

$$T^{(i-1)} \sim X_i^{\perp} \times T_i \iff X^*(T_i) \otimes \mathbb{Q} \simeq X_i \otimes \mathbb{Q}.$$

Par construction, X_i est engendré par les caractères $\chi_i^{\sigma_k(i)}$ pour k variant entre 1 et t_i. La dimension de T_i est donc $\dim W_i - \dim W_{i-1} = w_i$. □

On veut montrer par récurrence qu'il existe une constante C_2 strictement positive, indépendante de l, telle que

$$\forall 1 \leq i \leq r, \quad |G_l / G_i| \geq C_2 l^{\sum_{k=1}^{i} n_k w_k}.$$

On va pour cela utiliser le théorème 6.1 de Ribet. Vérifions tout d'abord la propriété au rang i=1 : par construction du tore algébrique T_1, on a

$$|T(\mathbb{Z}_l)/G_1| = |T_1(\mathbb{Z}_l)/T_1(\mathbb{Z}_l) \cap G_1|.$$

De plus les caractères $\chi_1^{\sigma_j(1)}$, avec $1 \leq j \leq t_1$, engendrent $X^*(T_1)$ qui est de dimension w_1 par le lemme 6.4. On a ainsi $T_1(\mathbb{Z}_l) \cap G_1 = T_1(1 + l^{n_1}\mathbb{Z}_l)$ et le théorème 6.1 permet de conclure : il existe une constante C_1' telle que

$$C_1' l^{w_1 n_1} \leq |T_1(\mathbb{Z}/l^{n_1}\mathbb{Z})|.$$

Passons maintenant au rang $i+1$: pour cela on supppose la propriété vraie au rang $i \geq 1$. On a par construction, $G_{i+1} \subset G_i \subset T(\mathbb{Z}_l)$. On a

$$|G_l/G_{i+1}| = |G_l/G_i| \times |G_i/G_{i+1}|\,.$$

Il suffit donc de savoir majorer convenablement chacun des deux termes du membre de droite de cette égalité. Le premier se majore précisément en utilisant l'hypothèse de récurrence. Il reste donc à majorer le second terme. On va pour cela réappliquer le théorème 6.1. On a l'inclusion

$$T^{(i)}(\mathbb{Z}_l)/\left(G_{i+1} \cap T^{(i)}(\mathbb{Z}_l)\right) \hookrightarrow G_i/G_{i+1}.$$

Ainsi, en terme de cardinaux on a

$$|G_i/G_{i+1}| \geq \left|T^{(i)}(\mathbb{Z}_l)/\left(G_{i+1} \cap T^{(i)}(\mathbb{Z}_l)\right)\right|.$$

La décomposition $T^{(i)} \sim T^{(i+1)} \times T_{i+1}$ et l'initialisation de la récurrence permettent alors de conclure : il existe une constante que l'on note encore C_1' telle que

$$|G_i/G_{i+1}| \geq C_1' l^{w_{i+1} n_{i+1}}.$$

ceci achève la preuve de la proposition 6.1 par récurrence. □

6.4 Conclusion

Proposition 6.4 *Avec les notations du paragraphe 6.2, il existe une constante strictement positive, C_1 telle que pour tout nombre premier l*

$$\mathrm{Card} H \leq C_1 l^{\sum_{i=1}^r n_i b_i}.$$

Démonstration : Il suffit d'appliquer les lemmes 6.1 et 6.2. □

En mettant ensemble les propositions 6.4 et 6.1, on obtient : il existe une constante strictement positive C_3 indépendante de l telle que

$$\mathrm{Card} H \leq C_3 [K(H) : K]^{\frac{\sum_{i=1}^r n_i b_i}{\sum_{i=1}^r n_i w_i}}. \tag{3}$$

On utilise alors le lemme suivant :

Lemme 6.5 *Soient $n_1 \geq \ldots \geq n_r$, $b_1, \ldots, b_r$ et $w_1, \ldots, w_r$ des entiers strictement positifs. On a*

$$\frac{\sum_{i=1}^r n_i b_i}{\sum_{i=1}^r n_i w_i} \leq \sup_{1 \leq k \leq r} \frac{\sum_{i=1}^k b_i}{\sum_{i=1}^k w_i}.$$

Démonstration : Les n_i sont ordonnés par ordre décroissant : $n_1 \geq n_2 \geq \ldots \geq n_r \geq 1$. On pose $n_{r+1} = 0$ et on applique une transformation d'Abel à la somme $\sum n_i b_i$:

$$\begin{aligned}\sum_{i=1}^{r+1} n_i b_i &= \left(\sum_{i=1}^{r+1} b_i\right) n_{r+1} + \sum_{i=1}^{r} \left(\sum_{k=1}^{i} b_k\right)(n_i - n_{i+1}) \\ &= \sum_{i=1}^{r} \left(\sum_{k=1}^{i} b_k\right)(n_i - n_{i+1}) \\ &\leq \left(\sup_{1\leq i\leq r} \frac{\sum_{k=1}^{i} b_k}{\sum_{k=1}^{i} w_k}\right) \sum_{i=1}^{r} \left(\sum_{k=1}^{i} w_k\right)(n_i - n_{i+1}) \\ &\leq \left(\sup_{1\leq i\leq r} \frac{\sum_{k=1}^{i} b_k}{\sum_{k=1}^{i} w_k}\right) \sum_{i=1}^{r} w_i n_i.\end{aligned}$$

On conclut en divisant par le nombre strictement positif $\sum_{i=1}^{r} w_i n_i$. □

Avec le choix des objets et le lemme 6.2, on constate finalement que l'exposant maximal obtenu dans l'inégalité (3) est obtenu quand les n_i valent tous 0 ou 1, *i.e.* quand H est en fait un sous-groupe de $A[l]$. De plus dans ce cas, un majorant de l'exposant maximal est

$$\sup_{1\leq i\leq r} \frac{\text{nombre de caractères dans } W_i}{\dim W_i}.$$

Ainsi, cet exposant est inferieur au nombre $\alpha(A)$ précédemment défini, ce qui nous permet de conclure la partie l-adique et donc la preuve de l'inégalité $\gamma(A) \leq \alpha(A)$ du théorème 1.4. □

7 Le théorème 1.4 : l'inégalité $\alpha(A) \leq \gamma(A)$

On veut montrer que l'exposant $\alpha(A)$ est effectivement atteint. On va pour cela utiliser la construction précédente. On commence par se donner un sous-espace vectoriel W de $X^*(T) \otimes \mathbb{Q}$ réalisant le sup $\alpha(A)$. On se donne un nombre premier l totalement décomposé dans le corps C.M., de sorte que l'action de T sur V_l est décomposée : les charactères $\chi_1, \ldots, \chi_{2g}$ diagonalisant l'action sont rationnels sur $\mathbb{Q}_l$. Quitte à renuméroter et à extraire une base, on a :

$$W = \mathrm{Vect}_{\mathbb{Q}}(\chi_1, \ldots, \chi_{d_W}),$$

les $\chi_1, \ldots, \chi_{d_W}$ formant une base de W qui est donc de dimension d_W. On note enfin

$$H_W = \left\{ Q \in A[l] \ / \ Q = \sum_{i\in I_W} m_i P_i,\ m_i \in \mathbb{F}_l \right\},$$

où $I_W = \{i \in [\![1, 2g]\!] \ / \ \chi_i \in W\}$ est de cardinal $n(W)$ et $\{P_1, \ldots, P_{2g}\}$ est la base du $\mathbb{F}_l$-espace vectoriel $A[l]$ de dimension $2g$, dans laquelle la représentation se diagonalise.

Lemme 7.1 *Le cardinal de H_W est $l^{n(W)}$.*

Démonstration : Découle de la définition de H_W. □

Il suffit maintenant pour conclure de montrer que le degré de l'extension $[K(H_W) : K]$ est essentiellement (*i.e.* à une constante multiplicative indépendante de l près) l^{d_W}. Pour cela on procède de la même façon qu'au paragraphe 6 précédent. Simplement dans le lemme 6.3 on a une égalité. De plus, il n'y a pas de récurrence à faire, mais juste le premier cran. En appliquant le théorème 6.1 de Ribet (minoration et majoration du cardinal des points des tores $T(\mathbb{Z}/l\mathbb{Z})$) on peut alors conclure de la même façon. On obtient finalement : il existe deux constantes strictement positives C_1 et C_2 ne dépendant que de A/K telles que

$$C_1[K(H_W) : K]^{\alpha(A)} \leq |H_W| = l^{n(W)} = l^{d_W \alpha(A)} \leq C_2[K(H_W) : K]^{\alpha(A)}.$$

Ceci conclut la preuve du théorème 1.4. □

8 Les cas particuliers

Nous allons traiter deux types de cas particuliers : certains cas particuliers de variétés abéliennes de type C.M. d'une part et le cas des courbes elliptiques sans multiplication complexe d'autre part.

8.1 Cas particuliers pour des variétés abéliennes de type C.M.

On rappelle en suivant Kubota [4], qu'une variété abélienne de type C.M. est de type non-dégénéré si $d = g + 1$, avec $g = \dim A$ et $d = \dim T$ où T est le groupe de Mumford-Tate de A.

Définition 8.1. Avec les notations précédentes en suivant Kubota [4], on dit qu'une variété abélienne de type C.M. est de *défaut* δ si

$$\delta = g + 1 - d.$$

Comme précédemment, on note $\chi_1, \ldots, \chi_{2g}$ les caractères diagonalisant l'action T sur V. Quitte à les renuméroter, on peut regrouper ces caractères par deux de sorte que

$$\chi_1 + \chi_{g+1} = \cdots = \chi_g + \chi_{2g} =: \chi_0.$$

Dans le cas non-dégénéré, ces relations sont les seules relations de dépendance linéaire. Par ailleurs, étant donné un sous-$\mathbb{Q}$-espace vectoriel W non-nul de $X^*(T) \otimes \mathbb{Q}$, on introduit deux notations

$$I_W = \{i \in \{1, \ldots, g\} \ / \ \chi_i \in W \text{ ou } \chi_{g+i} \in W\}, \quad \text{et} \quad m(W) = |I_W|.$$

Lemme 8.1 *Si A/K est de type non-dégénéré, alors*

$$\alpha(A) = \frac{2g}{d}.$$

Démonstration : On distingue deux cas :

1. Si $\chi_0 \notin W$ alors $n(W) = m(W)$ où l'on rappelle que $n(W)$ est le nombre de caractères, parmi les $\chi_1, \ldots, \chi_{2g}$, appartenant à W. De plus $d(W) = m(W)$, donc dans ce cas on a même $\frac{n(W)}{d(W)} \leq 1 \leq \frac{2g}{d}$.
2. Sinon $\chi_0 \in W$. Dans ce cas, on voit que $n(W) = 2m(W)$ et $d(W) = m(W) + 1$. En utilisant la croissance de la fonction $x \mapsto \frac{2x}{x+1}$, on a donc

$$\frac{n(W)}{d(W)} = \frac{2m(W)}{m(W)+1} \leq \frac{2g}{g+1} = \frac{2g}{d}.$$

Ceci conclut. □

De même qu'il est facile de traiter le cas des variétés abéliennes de type non-dégénéré, il est facile de traiter le cas des variétés abéliennes de défaut $\delta = 1$.

Lemme 8.2 *Si A/K est de défaut* 1*, alors*

$$\alpha(A) = 2 = \frac{2g}{d}.$$

Démonstration : On commence par noter que si $W = X^*(T) \otimes \mathbb{Q}$, alors $\frac{n(W)}{d(W)} = \frac{2g}{g} = 2$. Soit maintenant W un sous-espace vectoriel non-nul strict de $X^*(T) \otimes \mathbb{Q}$. Comme dans le lemme précédent, on distingue deux cas.

1. Si $\chi_0 \notin W$ alors $n(W) = m(W)$ et $d(W) \geq m(W) - 1$. Le quotient est donc inférieur à 2.
2. Sinon $\chi_0 \in W$. Dans ce cas $n(W) = 2m(W)$ et $d(W) \geq m(W)$. Là encore, le quotient est inférieur à 2, ce qui conclut. □

Nous pouvons maintenant passer à la preuve de la proposition 1.1 : si la dimension g est un nombre premier, alors le type est non dégénéré et donc le lemme 8.1 permet de conclure. Il reste à traiter le cas des variétés abéliennes simples de dimension 4 ou 6.

1. Si $g = 4$, on sait par la remarque 1.2. que le dimension d du groupe de Mumford-Tate est comprise entre $2 + \log_2(4) = 4$ et $4 + 1 = 5$. Si $d = 5$ le type est non dégénéré et si $d = 4$ la variété est de défaut $\delta = 1$. Là encore les deux lemmes précédents permettent de conclure.
2. Si $g = 6$, l'encadrement précédent vaut toujours : d est compris entre $4 < 2 + \log_2(6)$ et $6 + 1 = 7$. Comme précédemment toujours, si $g = 7$ ou si $g = 6$, les lemmes 8.1 et 8.2 précédents permettent de conclure. Il reste le cas où $d = 5$. Dans ce cas, par définition $\alpha(A) = \sup \frac{n(W)}{\dim W}$ où le sup porte sur les sous-espaces vectoriels non-nuls de $X^*(T) \otimes \mathbb{Q}$. En prenant pour W l'espace tout entier on constate que $\alpha(A) \geq \frac{2g}{d} \geq 2$. Par ailleurs, si W est un sous-espace strict de $X^*(T) \otimes \mathbb{Q}$, sa dimension est inférieure à 4. Le corollaire 4.1 du paragraphe 4 nous indique que $n(W) \leq 2^{4-1} = 8$. Ainsi on a $\frac{n(W)}{\dim W} \leq \frac{8}{4} = 2 \leq \frac{2g}{d}$. Ceci prouve bien que $\alpha(A) = \frac{2g}{d}$ et achève la preuve de la proposition 1.1. □

8.2 Cas d'une courbe elliptique sans multiplication complexe

Soit E/K une courbe elliptique sans multiplication complexe. Comme précedemment, on peut se ramener au cas l-adique : on se donne un groupe H inclus dans $E[l^\infty]$ pour un certain premier l. La courbe E/K étant sans multiplication complexe, on sait par un résultat de Serre (théorème 3'. et son corollaire 1. de [15]) que pour presque tout premier l, on a

$$G_l = \mathrm{GL}_2(\mathbb{Z}_l).$$

Ainsi au vu de ce que l'on veut montrer et comme précédemment, on peut supposer que $G_l = \mathrm{GL}_2(\mathbb{Z}_l)$. Le groupe H est de la forme

$$H = \langle P_1 \rangle \oplus \langle P_2 \rangle \simeq \mathbb{Z}/l^{n_1}\mathbb{Z} \times \mathbb{Z}/l^{n_2}\mathbb{Z}.$$

Par ailleurs, le groupe de Galois associé, G_H, tel que $[G_l : G_H] = [K(H) : K]$ est défini par

$$G_H = \{\sigma \in G_l \ / \ \sigma_H = \mathrm{Id}_H\}.$$

On se donne une base de $T_l(E)$, $\{\widehat{P_1}, \widehat{P_2}\}$ telle que $P_i = \widehat{P}_i \mod l^{n_i}$ pour $i \in \{1, 2\}$. On a ainsi l'identification

$$G_H = \left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}_l) \ / \ \forall i \in \{1,2\} \ \ \sigma\widehat{P}_i = \widehat{P}_i \mod l^{n_i}\right\}.$$

On peut encore réécrire ceci sous la forme

$$G_H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_l) \ / \ a - 1 = c = 0 \mod l^{n_1} \ \text{ et } \ b = d - 1 = 0 \mod l^{n_2} \right\}.$$

Sur cette dernière écriture, on voit qu'il existe deux constantes absolues C_1 et C_2 strictement positives telles que

$$C_1 \leq \frac{[G_l : G_H]}{l^{2(n_1+n_2)}} \leq C_2.$$

Le groupe H étant précisément de cardinal $l^{n_1+n_2}$, ceci permet de conclure. □

Références

[1] E. Bombieri, D. Masser, and U. Zannier. Intersecting a Curve with Algebraic Subgroups of Multiplicative Groups. In *Internat. Math. Res. Notices*, volume 20, pages 1119–1139, 1999.

[2] M. V. Borovoĭ. The action of the Galois group on the rational cohomology classes of type (p, p) of abelian varieties. *Mat. Sb. (N.S.)*, 94(136) :649–652, 656, 1974.

[3] B. Dodson. On the Mumford-Tate group of an abelian variety with complex multiplication. *J. Algebra*, 111(1) :49–73, 1987.

[4] T. Kubota. On the field extension by complex multiplication. *Trans. Amer. Math. Soc.*, 118 :113–122, 1965.

[5] D. Masser. Lettre à Daniel Bertrand du 10 novembre 1986.

[6] D. Masser. Small values of the quadratic part of the Néron-Tate height. In *Progr. Math.*, volume 12, pages 213–222. Birkhäuser, 1981.

[7] B. Moonen and Y. Zahrin. Hodges classes on abelian varieties of low dimension. *Math. Ann.*, 315, n. 4 :711–733, 1999.

[8] D. Mumford. A note of Shimura's paper "Discontinuous groups and abelian varieties". *Math. Ann.*, 181 :345–351, 1969.

[9] V.K. Murty. Hodge and Weil classes on abelian varieties. In *The arithmetic and geometry of algebraic cycles (Banff, AB, 1998)*, volume 548 of *NATO Sci. Ser. C Math. Phys. Sci.*, pages 83–115. Kluwer Acad. Publ., Dordrecht, 2000.

[10] T. Ono. Arithmetic of algebraic tori. *Ann. Math.*, 74, n. 1 :101–139, 1961.

[11] I. I. Pjateckiĭ-Šapiro. Interrelations between the Tate and Hodge hypotheses for abelian varieties. *Mat. Sb. (N.S.)*, 85(127) :610–620, 1971.

[12] N. Ratazzi. Minoration de la hauteur sur les variétés abéliennes de type C.M. et applications. Prépublication de l'institut de Mathématiques de Jussieu, février 2005.

[13] G. Rémond. Intersection de sous-groupes et de sous-variétés I. Prépublication de l'Institut Fourier no. 626, octobre 2003.

[14] K. A. Ribet. Division fields of abelian varieties with complex multiplication. *Mémoires de la S.M.F*, 2 :75–94, 1980.

[15] J.-P.. Serre. Propriétés galoisiennes des points d'ordres fini des courbes elliptiques. *Inv. Math*, 15 :259–331, 1972.

[16] J.-P. Serre. Représentations l-adiques. In *Kyoto Int. Symposium on Algebraic Number Theory*, pages 177–193. Japan Soc. for the promotion of Science, 1977.

[17] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. Math.*, 88 :492–517, 1968.

[18] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.

[19] A. Silverberg. Torsion points on abelian varieties of CM-type. *Compositio Math.*, 68(3) :241–249, 1988.

[20] E. Viada. The intersection of a curve with algebraic subgroups in a product of elliptic curves. In *Ann. Scuola Norm. Pisa Cl. Sci.* Série *(V)*, volume 1, pages 47–75, 2002.

[21] H. Yanai. On the rank of CM-type. *Nagoya Math. J.*, 97 :169–172, 1985.

Adresse : Ratazzi Nicolas
Université Paris 6 Institut de Mathématiques
Projet Théorie des nombres

Case 247
4, place Jussieu
75252 Paris Cedex 05
FRANCE
email : ratazzi@math.jussieu.fr