*Ann. Scient. Éc. Norm. Sup.,*
4e série, t. 40, 2007, p. 951 à 983.

# BORNE SUR LA TORSION DANS LES VARIÉTÉS ABÉLIENNES DE TYPE CM

PAR NICOLAS RATAZZI

RÉSUMÉ. – Soit $A$ une variété abélienne de dimension $g \geqslant 1$ définie sur un corps de nombres $K$. On étudie la taille du groupe de torsion $A(F)_{\mathrm{tors}}$ où $F/K$ est une extension finie, et on étudie plus précisément le meilleur exposant possible $\gamma$ dans l'inégalité $\mathrm{Card}(A(F)_{\mathrm{tors}}) \ll [F : K]^{\gamma}$ quand $F$ parcourt les extensions finies de $K$. Dans le cas CM, nous donnons une formule exacte pour l'exposant $\gamma$ en fonction des caractères du groupe de Mumford–Tate—un tore dans ce cas—et nous donnons une brève discussion dans le cas général.

Enfin nous donnons une application du résultat principal en direction d'une généralisation de la conjecture de Manin–Mumford.



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

Finally we give an application of the main result in direction of a generalisation of the Manin–Mumford conjecture.



## 1. Introduction et résultats

Soient $K$ un corps de nombres et $A/K$ une variété abélienne sur $K$ de dimension $g \geqslant 1$. Le classique théorème de Mordell–Weil assure que le groupe $A(K)$ des points $K$-rationnels de $A$ est de type fini. Un problème naturel qui se pose alors est de comprendre le sous-groupe de torsion $A(K)_{\mathrm{tors}}$. Dans le cas où $A$ est une courbe elliptique (définie) sur $\mathbb{Q}$, Mazur [9] a classifié les groupes de torsion possibles. Ceci étant, ce problème semble tout à fait hors de portée dans le cas général et un sous-problème plus raisonnable consiste à essayer de comprendre le cardinal de $A(K)_{\mathrm{tors}}$ lorsque $A$ et $K$ varient. Il y a essentiellement deux approches possibles pour ce problème : soit l'on fixe le corps de nombres $K$ et l'on s'intéresse à la variation du cardinal lorsque $A$ décrit les variétés abéliennes sur $K$ de dimension $g$ fixée. Dans cette direction, citons le célèbre résultat de Merel [10] : si $E$ est une courbe elliptique sur un corps de nombres $K$, le cardinal de $E(K)_{\mathrm{tors}}$ est borné par une constante ne dépendant que du degré de $K$ sur $\mathbb{Q}$. Parent [16] a rendu effectif le résultat de Merel, obtenant une borne doublement exponentielle en le degré $[K : \mathbb{Q}]$. En dimension supérieure essentiellement rien n'est connu concernant ce problème connu sous le nom de conjecture de borne uniforme. La seconde approche possible concernant le cardinal de $A(K)_{\mathrm{tors}}$ consiste à fixer une variété abélienne $A$ définie sur un corps


0012-9593/06/© 2007 Publié par Elsevier Masson SAS.

de nombres $K_0$ et à faire varier $K$ parmi les extensions finies de $K_0$, l'objectif étant cette fois-ci d'obtenir une borne par une constante $C(A/K_0, [K : K_0])$ avec une dépendance explicite (la meilleure possible) en le degré $[K : K_0]$ (ou, ce qui revient au même, en le degré $[K : \mathbb{Q}]$). Concernant ce second problème, Masser [7] et [8] a montré dans le cas général que la dépendance est polynomiale en $[K : \mathbb{Q}]$. La question naturelle qui se pose est alors de savoir quel est le plus petit exposant $\gamma(A)$ possible dans cette borne polynomiale. Nous donnons dans cet article une réponse à cette question dans le cas des variétés abéliennes CM. De plus, indépendamment de son intérêt propre, l'obtention d'une borne meilleure que celle de Masser a des conséquences concrètes concernant des problèmes de géométrie diophantienne (cf. théorème 1.21 ci-dessous).

Soit $A/K$ une variété abélienne de dimension $g \geqslant 1$ sur un corps de nombres $K$. On utilise la notation $\ll$ pour dire à une constante près ne dépendant que de $A/K$ et on pose

$$\gamma(A) = \inf\bigl\{x > 0 \mid \forall F/K \text{ finie}, \bigl|A(F)_{\mathrm{tors}}\bigr| \ll [F : K]^x\bigr\}.$$

Dans le cas général, la meilleure estimation de ce nombre est due à Masser [7] et [8].

THÉORÈME 1.1 (Masser). – *On a $\gamma(A) \leqslant g$.*

Dans le cas des courbes elliptiques de type CM, le résultat de Masser est optimal. On peut se demander ce qu'il en est en dimension supérieure. Pour cela nous avons besoin de rappeler la notion de groupe de Mumford–Tate d'une variété abélienne $A/K$ sur un corps de nombres.

Fixons désormais un plongement $K \subset \mathbb{C}$ et notons $\overline{K}$ une clôture algébrique de $K$ dans $\mathbb{C}$. Soit $A/K$ une variété abélienne. On note $V = H^1(A(\mathbb{C}), \mathbb{Q})$ le premier groupe de cohomologie singulière de la variété analytique complexe $A(\mathbb{C})$. C'est un $\mathbb{Q}$-espace vectoriel de dimension $2g$. Il est naturellement muni d'une structure de Hodge de type $\{(1,0),(0,1)\}$, c'est-à-dire d'une décomposition sur $\mathbb{C}$ de $V_{\mathbb{C}} := V \otimes_{\mathbb{Q}} \mathbb{C}$ donnée par $V_{\mathbb{C}} = V^{1,0} \oplus V^{0,1}$ telle que $V^{0,1} = \overline{V^{1,0}}$ où $\overline{\cdot}$ désigne la conjugaison complexe. On note $\mu : \mathbb{G}_{m,\mathbb{C}} \to \mathrm{GL}_{V_{\mathbb{C}}}$ le cocaractère tel que pour tout $z \in \mathbb{C}^\times$, $\mu(z)$ agisse par multiplication par $z$ sur $V^{1,0}$ et agit trivialement sur $V^{0,1}$. On définit le groupe de Mumford–Tate en suivant [17].

DÉFINITION 1.2. – Le *groupe de Mumford–Tate* $\mathrm{MT}(A)/\mathbb{Q}$ de $A$ est le plus petit $\mathbb{Q}$-sous-groupe algébrique $G$ de $\mathrm{GL}_V$ (vu comme $\mathbb{Q}$-schéma en groupes) tel que, après extension des scalaires à $\mathbb{C}$, le cocaractère $\mu$ se factorise à travers $G_{\mathbb{C}} := G \times_{\mathbb{Q}} \mathbb{C}$.

Nous faisons au paragraphe 2 des rappels concernant le groupe de Mumford–Tate, dans le cas général et plus spécifiquement dans le cas CM.

Dans le cas des variétés abéliennes simples de type CM, Ribet a donné une minoration de $\gamma(A)$. Précisément, en notant $\omega(n)$ le nombre de facteurs premiers de l'entier $n$ et $A[n]$ l'ensemble des points de $A(\overline{K})$ d'ordre divisant $n$, Ribet [25] montre que

THÉORÈME 1.3 (Ribet). – *Si $A/K$ est une variété abélienne de type CM, alors il existe deux constantes strictement positives $C_1$ et $C_2$ ne dépendant que de $A$ et $K$ telles que : pour tout entier $n \geqslant 1$,*

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

*où $d = \dim \mathrm{MT}(A)$. De plus si $A$ est géométriquement simple, on a $d \geqslant 2 + \log_2 g$.*

Comme corollaire du théorème 1.3, on obtient immédiatement, dans le cas où $A/K$ est une variété abélienne de type CM, l'inégalité

$$\gamma(A) \geqslant \frac{2 \dim A}{\dim \mathrm{MT}(A)}. \tag{1}$$

Nous montrons plus généralement que cette minoration reste valable pour toute variété abélienne sur un corps de nombres. C'est l'objet du théorème suivant, prouvé au paragraphe 3.

THÉORÈME 1.4. – *Soit $A/K$ une variété abélienne quelconque de dimension $g$. On a*

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

*où $d$ est la dimension du groupe de Mumford–Tate de $A$.*

DÉFINITION 1.5. – 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.

Rappelons la notion de groupe des caractères d'un tore algébrique sur un corps $k$ (i.e. d'un groupe algébrique $G/k$ isomorphe sur $\overline{k}$ au groupe multiplicatif $\mathbb{G}_{m,\overline{k}}^{\dim G}$).

DÉFINITION 1.6. – Soit $\mathcal{T}/k$ un tore algébrique sur un corps $k$. On note $\overline{k}$ la clôture séparable de $k$. On appelle *groupe des caractères de $\mathcal{T}$* et on note $X^*(\mathcal{T})$ le groupe

$$X^*(\mathcal{T}) = \mathrm{Hom}_{\overline{k}}(\mathcal{T}_{\overline{k}}, \mathbb{G}_{m,\overline{k}}).$$

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

$$X_*(\mathcal{T}) = \mathrm{Hom}_{\overline{k}}(\mathbb{G}_{m,\overline{k}}, \mathcal{T}_{\overline{k}}).$$

Dans les deux cas précédents et dans la suite, $\mathrm{Hom}_{\overline{k}}$ désigne le groupe des homomorphismes entre groupes algébriques sur $\overline{k}$. On note $X^*(\mathcal{T}) \otimes \mathbb{Q}$ le $\mathbb{Q}$-espace vectoriel déduit de $X^*(\mathcal{T})$.

Nous pouvons maintenant en venir au résultat principal de cet article : l'obtention d'une valeur exacte pour $\gamma(A)$ dans le cas où $A/K$ est une variété abélienne de type CM, sans facteur carré. De fait, le cas où $A$ est géométriquement simple est déjà suffisant dans les applications (cf. par exemple le théorème 1.21 ci-dessous) et la proposition 3.1 du paragraphe 3 montre qu'il est facile d'obtenir un encadrement de $\gamma(A)$ en fonction des facteurs $\gamma(A_i)$ correspondant aux facteurs géométriquement simples $A_i$ de $A$. Néanmoins la preuve étant valable sans complication supplémentaire dans le cas (légèrement) plus général des variétés abéliennes de type CM sans facteur carré, nous énonçons notre résultat dans ce cadre.

Si $A/K$ est de type CM sans facteur carré, on note $\mathcal{T}$ son groupe de Mumford–Tate : c'est un tore algébrique sur $\mathbb{Q}$ (cf. le sous-paragraphe 2.2). On note

$$I = \{\chi_1, \ldots, \chi_{2g}\}$$

l'ensemble des caractères diagonalisant (sur $\overline{\mathbb{Q}}$) l'action de $\mathcal{T}$ sur l'espace vectoriel $V_{\overline{\mathbb{Q}}}$ de dimension $2g$ donné par $V = H^1(A(\mathbb{C}), \mathbb{Q})$. L'hypothèse *sans facteur carré* est faite pour assurer que les $\chi_i$ sont deux à deux distincts.

DÉFINITION 1.7. – Soit $A/K$ de type CM sans facteur carré. Soit $W$ un sous-espace vectoriel sur $\mathbb{Q}$ de $X^*(\mathcal{T}) \otimes \mathbb{Q}$. On pose

$$n(W) = |I \cap W| = \mathrm{Card}\big(\{i \in \{1, \ldots, 2g\} \mid \chi_i \in W\}\big).$$

DÉFINITION 1.8. – On définit un invariant $\alpha(A)$ comme suit :

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

*Remarque* 1.9. – On voit sur la définition que le nombre $\alpha(A)$ ne dépend que des caractères $\chi_1, \ldots, \chi_{2g}$. En particulier, étant donnée une variété abélienne de type CM, i.e. étant donné un type CM, le nombre $\alpha(A)$ est calculable explicitement et algorithmiquement. De fait il est clair que si l'on note $W_S = \mathrm{Vect}(S)$ pour tout sous-ensemble $S$ de $I$, alors

$$\alpha(A) = \max \frac{n(W_S)}{\dim W_S}$$

le max portant sur la collection finie des sous-ensembles $S$ de $I$. Ceci se calcule en déterminant les relations entre les différents caractères $\chi \in I$.

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

THÉORÈME 1.10. – *Soit $A/K$ une variété abélienne sans facteur carré, de type CM. On a*

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

*Remarque* 1.11. – Notons quelque chose qui n'était pas évident *a priori* sur la définition de $\gamma(A)$ : dans le cas de type CM sans facteur carré, l'exposant $\gamma(A)$ est un nombre rationnel (puisqu'il est clair sur la définition que $\alpha(A)$ l'est, avec un numérateur compris entre 2 et $2g$ et un dénominateur compris entre 1 et $\dim \mathcal{T}$).

Par ailleurs ce résultat est d'autant plus intéressant qu'il est possible de calculer une bonne majoration de $\alpha(A)$ en fonction de $g$ voire dans certains cas particuliers de calculer sa valeur exacte en fonction de $g$ et $d = \dim \mathcal{T}$.

THÉORÈME 1.12. – *Soit $A/K$ une variété abélienne sans facteur carré, de type CM, de dimension $g \geqslant 1$. On a*

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

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

En conséquence de nos théorèmes 1.10 et 1.12, nous obtenons :

COROLLAIRE 1.13. – *Soit $A/K$ une variété abélienne de type CM de dimension $g \geqslant 1$, sans facteur carré. On a*

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

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

*Remarque* 1.14. – On sait (cf. par exemple [4] theorem 1.0) que pour tout $g$ de la forme $2^n$, avec $n \geqslant 2$, il existe une variété abélienne CM simple telle que la dimension de son groupe de Mumford–Tate soit précisément $2 + \log_2(g)$. En utilisant le théorème 1.4, 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 CM) :

COROLLAIRE 1.15. – *Soit $A/K$ une variété abélienne sans facteur carré, de type CM et de dimension $g \geqslant 2$. 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 1.16. – On dit qu'une variété abélienne $A$ de type CM, de dimension $g$, est de type *non dégénéré* si la dimension du groupe de Mumford–Tate $\mathcal{T}$ de $A$ est $g+1$.

*Remarque* 1.17. – Soit $A$ une variété abélienne quelconque de dimension $g$, de groupe de Mumford–Tate de dimension $d$. On sait que $d \leqslant g+1$. Par ailleurs si $A$ est géométriquement simple de type CM, alors Ribet [25] a montré que

$$2 + \log_2(g) \leqslant d.$$

De plus un autre résultat de Ribet (cf. [26] Theorem 2) dit que si $A$ est une variété abélienne géométriquement simple de type CM et de dimension un entier $g$ premier, alors $A$ est de type non dégénéré.

PROPOSITION 1.18. – *Soit $A/K$ une variété abélienne géométriquement simple, de type CM, 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 $A$.*

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 connaît le groupe de Mumford–Tate de $A$, c'est le groupe algébrique $\mathrm{GL}_2$ sur $\mathbb{Q}$.

PROPOSITION 1.19. – *Si $E/K$ est une courbe elliptique sans multiplication complexe, alors*

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

Remarquons que dans ce dernier cas on a $\frac{2g}{d} = \frac{1}{2}$ et on trouve encore l'égalité $\gamma(A) = \frac{2g}{d}$. Ainsi au vu des deux propositions 1.18 et 1.19 précédentes et au vu de notre théorème 1.4, on est tenté de poser la question suivante :

*Question* 1. – Si $A/K$ est une variété abélienne géométriquement simple et $n \geqslant 1$, a-t-on

$$\gamma(A^n) = \frac{2n \dim A}{\dim \mathrm{MT}(A)} \ ?$$

En plus des résultats précédents, cet énoncé se ramène aisément au cas où $n = 1$ : on vérifie dans le lemme 2.1 et le corollaire 3.2 que

$$\forall n \geqslant 1 \quad \gamma(A^n) = n\gamma(A) \quad \text{et} \quad \mathrm{MT}(A^n) \simeq \mathrm{MT}(A).$$

Ceci étant, un travail en cours indique que la question ne peut pas se généraliser telle que au cas d'une variété abélienne quelconque, le bon énoncé dans le cas général semblant plutôt être le suivant :

*Question* 2. – Si $A/K$ est une variété abélienne isogène au produit $\prod_{i=1}^{r} A_i^{n_i}$ où les $A_i$ sont géométriquement simples et deux à deux non isogènes sur $\overline{\mathbb{Q}}$, a-t-on

$$\gamma(A) = \max_{\emptyset \neq I \subset \{1,\dots,r\}} \frac{2 \dim \prod_{i\in I} A_i^{n_i}}{\dim \mathrm{MT}(\prod_{i\in I} A_i)} ?$$

Si $A$ est de la forme $A_1^n$ on retombe sur la première question. Notons que déjà dans le cas des variétés abéliennes de type CM, il serait très intéressant de savoir répondre à ces questions : affirmativement ou en donnant un contre-exemple. Un autre test intéressant serait le cas d'un produit $E_1^{n_1} \times E_2^{n_2}$ avec $E_1, E_2$ deux courbes elliptiques quelconques et $n_1, n_2$ deux entiers.

Pour conclure cette introduction, nous donnons un exemple d'application des théorèmes 1.10 et 1.12 concernant une récente conjecture généralisant les conjectures de Manin–Mumford et de Mordell–Lang :

Soient $A/\overline{\mathbb{Q}}$ une variété abélienne (définie) sur $\overline{\mathbb{Q}}$, $X/\overline{\mathbb{Q}}$ une courbe irréductible de $A$ et $r$ un entier positif ou nul. Suivant Bombieri, Masser et Zannier [1] dans le cas de $\mathbb{G}_m^n$ et Rémond [23] dans le cas des variétés abéliennes, on s'intéresse au problème suivant : on considère l'ensemble

$$A^{[r]} := \bigcup_{\operatorname{codim} G \geqslant r} G(\overline{\mathbb{Q}})$$

où l'union porte sur les sous-groupes algébriques non nécessairement connexes de $A$ de codimension au moins $r$. À quelles conditions sur $r$ et sur $X$ peut-on garantir que l'ensemble $X(\overline{\mathbb{Q}}) \cap A^{[r]}$ 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 retombe sur un problème du type Manin–Mumford (théorème de Raynaud [21]). Si $A$ est une puissance d'une courbe elliptique, on peut voir que $X(\overline{\mathbb{Q}}) \cap A^{[1]}$ est infini, donc on doit nécessairement prendre $r \geqslant 2$. De manière indépendante, Zilber ([40] Conjecture 2) pour les variétés semi-abéliennes et Pink ([18] Conjecture 1.3) pour les variétés de Shimura mixtes, ont formulé une conjecture qui, dans le cas des courbes incluses dans une variété abélienne sur $\overline{\mathbb{Q}}$ se spécialise en la suivante :

CONJECTURE 1.1 (Zilber–Pink, cas particulier). – *Soient $A/\overline{\mathbb{Q}}$ une variété abélienne et $X/\overline{\mathbb{Q}}$ une courbe dans $A$ irréductible. Si $X$ n'est pas contenue dans un sous-groupe algébrique strict de $A$, alors l'ensemble $X(\overline{\mathbb{Q}}) \cap A^{[2]}$ est fini.*

Rémond [23] a montré que la conjecture précédente est vraie si une très bonne minoration (conjecturale) des points d'ordre infini de $A$ est vraie : il s'agit d'une conjecture de David généralisant le problème de Lehmer. Par ailleurs, dans le cas des variétés abéliennes de type CM, Rémond [23] obtient un résultat inconditionnel, mais sensiblement plus faible que la conjecture 1.1 : soit $A$ une variété abélienne de type CM, 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 1.20 (Rémond [23]). – *Soient $A/\overline{\mathbb{Q}}$ une variété abélienne de type CM et $X/\overline{\mathbb{Q}}$ une courbe dans $A$ qui n'est pas incluse dans un translaté de sous-variété abélienne stricte de $A$ ; alors $X(\overline{\mathbb{Q}}) \cap A^{[2+\sum_{i=1}^{m} g_i]}$ est fini.*

Comme nous l'expliquons dans [22], en suivant la stratégie de Rémond (et Bombieri–Masser–Zannier), en utilisant notre corollaire 1.13 ci-dessus concernant la borne sur les points de torsion

pour les variétés abéliennes de type CM, ainsi qu'un résultat de minoration de hauteur faisant l'objet de l'article séparé [22], nous améliorons ce théorème et obtenons un résultat optimal dans le cas d'une puissance d'une variété abélienne simple de type CM :

THÉORÈME 1.21 ([22]). – *La conjecture* 1.1 *est vraie si $A$ est une puissance d'une variété abélienne de type CM, simple de dimension quelconque.*

Ceci généralise au cas d'une puissance d'une variété abélienne de type CM simple de dimension quelconque le résultat de Viada [38] et Rémond–Viada ([24] théorème 1.7), valable pour une puissance d'une courbe elliptique à multiplication complexe. On peut même donner un résultat un peu plus général en fonction des exposants $\gamma(A_i)$ correspondant aux différents facteurs simples de $A$ : voir pour cela la remarque 1.5 de l'article [22].

PLAN DE L'ARTICLE. Nous faisons au paragraphe 2 les rappels nécessaires concernant le groupe de Mumford–Tate $\mathrm{MT}(A)$, dans le cas général et plus spécifiquement dans le cas CM. Nous donnons également le lien entre la représentation naturelle $\rho\colon \mathrm{MT}(A) \to \mathrm{GL}_V$ et les représentations $\ell$-adiques correspondant à l'action de $\mathrm{Gal}(\overline{K}/K)$ sur les points de torsion d'ordre une puissance de $\ell$ lorsque $\ell$ décrit l'ensemble des nombres premiers. Nous donnons au paragraphe 3 une preuve de la minoration de $\gamma(A)$ annoncée dans le théorème 1.4. Ensuite nous donnons au paragraphe 4 une preuve du théorème 1.12. Les paragraphes 5, 6 et 7 sont consacrés à la preuve du résultat principal. Nous prouvons tout d'abord au paragraphe 5 l'inégalité $\gamma(A) \geqslant \alpha(A)$ : la preuve est plus simple et contient déjà une grande partie des idées utilisées dans la preuve de la seconde inégalité. Nous discutons plus avant de la stratégie concernant la seconde inégalité à la fin du paragraphe 5. Enfin on s'intéresse aux cas particuliers correspondant aux propositions 1.18 et 1.19 dans le dernier paragraphe.

## 2. Rappels sur le groupe de Mumford–Tate et sur les tores algébriques

### 2.1. Groupe et conjecture de Mumford–Tate

Concernant les groupes de Mumford–Tate $\mathrm{MT}(A)$ la définition a été rappelée dans l'introduction.

LEMME 2.1. – *Soit $A/K$ une variété abélienne sur un corps de nombres $K$ plongé dans $\mathbb{C}$. Soit $n \geqslant 1$ un entier. On a*

$$\mathrm{MT}(A^n) \simeq \mathrm{MT}(A).$$

*Démonstration.* – On commence par remarquer que $H^1(A^n(\mathbb{C}), \mathbb{Q}) \simeq H^1(A(\mathbb{C}), \mathbb{Q})^{\oplus n}$. Posons $V = H^1(A(\mathbb{C}), \mathbb{Q})$. Vu la définition du groupe de Mumford–Tate, on voit que l'on obtient le résultat en plongeant diagonalement $\mathrm{GL}_V$ dans $\mathrm{GL}_{V^{\oplus n}}$. □

Rappelons maintenant la célèbre conjecture de Mumford–Tate. Notons $A/K$ une variété abélienne quelconque de dimension $g \geqslant 1$, définie sur un corps de nombres $K$ que l'on suppose plongé dans $\mathbb{C}$. Notons également $\mathrm{MT}(A)$ le groupe de Mumford–Tate correspondant.

DÉFINITION 2.2. – Notons $T_\ell(A)$ le module de Tate et $V_\ell := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Soient $\ell$ un premier et $\rho_\ell\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(A)) \subset \mathrm{GL}(V_\ell)$ la représentation $\ell$-adique associée à l'action de Galois sur les points de $\ell^\infty$-torsion de $A$. On définit $\overline{G_\ell}$ comme étant l'adhérence de Zariski de l'image $G_\ell$ de $\rho_\ell$ dans le groupe algébrique $\mathrm{GL}_{V_\ell} \simeq \mathrm{GL}_{2g,\mathbb{Q}_\ell}$. C'est un groupe algébrique sur $\mathbb{Q}_l$ dont on notera $\overline{G_\ell}^0$ la composante neutre (composante connexe de l'identité).

Les théorèmes de comparaison entre cohomologie étale et cohomologie classique (cf. [33] XI) d'une part, et la comparaison entre le premier groupe de cohomologie étale et le module de Tate (cf. [11] 15.1(a)), d'autre part, donnent pour tout premier $\ell$ l'isomorphisme canonique :

$$V_\ell = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \simeq V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Nous fixons une fois pour toutes dans la suite un tel isomorphisme. Ceci permet de comparer $\mathrm{MT}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell$ et $\overline{G_\ell}^0$ :

CONJECTURE 2.1 (Mumford–Tate). – *Pour tout $\ell$ premier, on a $\overline{G_\ell}^0 = \mathrm{MT}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell$.*

DÉFINITION 2.3. – Notons $\rho : \mathrm{MT}(A) \hookrightarrow \mathrm{GL}_V$ la représentation naturelle du groupe de Mumford–Tate.

Un certain nombre de cas particuliers, ainsi que de résultats en direction de la conjecture précédente sont connus. Nous renvoyons à la référence [17] pour une discussion détaillée de ces résultats. Disons simplement ici que cette conjecture est un théorème pour les variétés abéliennes de type CM (travaux de Shimura–Taniyama [34]) ainsi que pour les courbes elliptiques sans multiplication complexe (Serre [27]). De manière générale on sait par les travaux de Borovoĭ [3], Deligne [5] Exp I, 2.9, 2.11, et Pjateckiĭ-Šapiro [19] qu'une inclusion est toujours vraie :

THÉORÈME 2.4. – *Pour tout $\ell$ premier, $\overline{G_\ell}^0 \subset \mathrm{MT}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell$.*

Par ailleurs, on a le résultat suivant, dû à Shimura–Taniyama [34] dans le cas de type CM et dû à Serre [30] 2.2.3 (cf. également [29]), dans le cas général.

THÉORÈME 2.5. – *L'application*

$$\varepsilon : \mathrm{Gal}(\overline{K}/K) \to \overline{G_\ell}(\mathbb{Q}_\ell) \to \overline{G_\ell}(\mathbb{Q}_\ell)/\overline{G_\ell}^0(\mathbb{Q}_\ell)$$

*est continue surjective, de noyau indépendant de $\ell$ pour tout premier $\ell$.*

Ainsi, le noyau de $\varepsilon$ est un sous-groupe d'indice fini de $\mathrm{Gal}(\overline{K}/K)$ donc il existe une extension finie $K'/K$ telle que $\mathrm{Gal}(\overline{K'}/K') \subset \ker \varepsilon$. Dit autrement, les deux théorèmes précédents donnent le lien entre la représentation $\rho$ et les représentations $\ell$-adiques $\rho_\ell$ pour tout premier $\ell$ : quitte à remplacer au départ $K$ par une extension $K'$ finie ne dépendant que de $A$ (ce que nous ferons dans la suite), on a pour tout premier $\ell$ la factorisation

$$\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{MT}(A)(\mathbb{Q}_\ell) \xrightarrow{\rho} \mathrm{GL}_V(\mathbb{Q}_\ell) \simeq \mathrm{GL}(V_\ell).$$

Enfin dans deux cas particuliers déjà mentionnés précédemment, on peut encore préciser les choses :

THÉORÈME 2.6 (Serre). – *Soit $A/K$ une variété abélienne de type CM ou une courbe elliptique sans multiplication complexe. Pour tout $\ell$ premier on a*

$$G_\ell = \mathrm{Im}(\rho_\ell) \subset \mathrm{MT}(A)(\mathbb{Z}_\ell),$$

*cette inclusion étant de conoyau fini, borné indépendamment de $\ell$.*

*Démonstration.* – Dans le cas des variétés abéliennes de type CM, cela découle du théorème 1 p. II-26 de [31]. Dans le cas des courbes elliptiques sans multiplication complexe, il s'agit du théorème 3 p. 299 de [27]. □

### 2.2. Groupe de Mumford–Tate des variétés abéliennes de type CM

Intéressons-nous maintenant plus particulièrement au cas des variétés abéliennes de type CM. Nous suivons pour cela la référence [14] pp. 108–110. Commençons par le cas d'une variété géométriquement simple de type CM de dimension $g$. Soit $E$ le corps CM de la variété abélienne $A$. Rappelons que l'on a noté dans l'introduction $V = H^1(A(\mathbb{C}), \mathbb{Q})$ le premier groupe de cohomologie singulière de la variété analytique complexe $A(\mathbb{C})$. C'est un $\mathbb{Q}$-espace vectoriel de dimension $2g$. Il est naturellement muni d'une structure de Hodge de type $\{(1,0),(0,1)\}$, c'est-à-dire d'une décomposition sur $\mathbb{C}$ de $V_{\mathbb{C}} := V \otimes_{\mathbb{Q}} \mathbb{C}$ donnée par $V_{\mathbb{C}} = V^{1,0} \oplus V^{0,1}$ telle que $V^{0,1} = \overline{V^{1,0}}$ où $\overline{\cdot}$ désigne la conjugaison complexe. Mieux, suivant [14] équation (3) p. 108 on a la décomposition

$$V^{1,0} = \bigoplus_{\sigma \in \Phi} V^{1,0}_{\sigma}$$

où $\Phi$ est un type CM, *i.e.* un ensemble de plongements $\sigma : E \hookrightarrow \mathbb{C}$ tel que

$$\Phi \cup \overline{\Phi} = \mathrm{Hom}(E, \mathbb{C}) \quad \text{et} \quad \Phi \cap \overline{\Phi} = \emptyset.$$

Notons $T_E = \mathrm{Res}_{E/\mathbb{Q}} \mathbb{G}_{m,E}$ le tore correspondant au corps CM $E$. Si $\sigma$ est l'un des plongements de $E$ dans $\overline{\mathbb{Q}}$, alors $\sigma$ s'étend en un morphisme $E \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ et définit donc un caractère $[\sigma] \in X^*(T_E)$. Une base du groupe des caractères $X^*(T_E)$ est donnée par la famille $\{[\sigma] \mid \sigma : E \hookrightarrow \mathbb{C}\}$. Par définition $\mathrm{MT}(A)$ est le plus petit sous-groupe algébrique sur $\mathbb{Q}$ de $\mathrm{GL}_V$ contenant l'image de

$$\mu = \sum_{i=1}^{g} e_i,$$

les $e_i \in X_*(T_E)$ étant les cocaractères duaux des $[\sigma_i] \in X^*(T_E)$ avec $\{\sigma_1, \ldots, \sigma_g\} = \Phi$. En effet, $\mu$ n'est rien d'autre que l'homomorphisme défini par la même notation dans l'introduction et donné sur les complexes par : $\mu_{\mathbb{C}} : \mathbb{G}_{m,\mathbb{C}} \to \mathrm{GL}_{V_{\mathbb{C}}}$ tel que, pour tout $z \in \mathbb{C}^\times$, $\mu(z)$ agisse par multiplication par $z$ sur $V^{1,0}$ et agisse trivialement sur $V^{0,1}$. Le groupe $\mathrm{MT}(A)$ est inclus dans $T_E$, c'est donc un sous-tore algébrique : on le note désormais $\mathcal{T}$ pour simplifier les notations. De plus par définition $\mu$ est un cocaractère de $\mathcal{T}$. On note $\mu'$ son cocaractère conjugué (donné par $\mu' = \sum_{i=g+1}^{2g} e_i$). Le groupe des caractères $X^*(\mathcal{T})$ de $\mathcal{T}$ est un quotient de $X^*(T_E)$. On note $\chi_1, \ldots, \chi_{2g}$ les images dans $X^*(\mathcal{T})$ des caractères $[\sigma_1], \ldots, [\sigma_{2g}]$ de $X^*(T_E)$.

Ce qui précède s'applique de même dans le cas d'une variété abélienne sans facteur carré de type CM, à condition de remplacer le corps CM $E$ par le produit de corps CM $\prod_i E_i$ et en remplaçant le tore $T_E$ par le tore $\prod_i T_{E_i}$. On suppose désormais que $A$ est de type CM sans facteur carré.

DÉFINITION 2.7. – Étant donné un tore $T$ sur un corps $k$ de clôture séparable $\overline{k}$, notons $\langle\ ,\ \rangle$ l'accouplement donné par

$$X^*(T) \times X_*(T) \to \mathbb{Z}, \quad (x, y) \mapsto \langle x, y \rangle := \deg(x \circ y).$$

PROPOSITION 2.8. – *En étendant les scalaires à $\overline{\mathbb{Q}}$, les images de $\sigma\mu$, $\sigma$ décrivant $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, engendrent $\mathcal{T}_{\overline{\mathbb{Q}}}$. Par ailleurs, pour tout entier $i$ compris entre $1$ et $2g$ on a*

$$\langle \chi_i, \mu + \mu' \rangle = 1 \quad \textit{et} \quad \langle \chi_i, \mu \rangle \in \{0, 1\}.$$

*Démonstration.* – Par construction du groupe de Mumford–Tate (cf. par exemple [17] Fact 5.9) on sait que les images de $\sigma\mu$, $\sigma$ décrivant $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, engendrent $\mathcal{T}_{\overline{\mathbb{Q}}}$, ceci étant précisément la première assertion de la proposition. La seconde découle directement des définitions et de la discussion précédant l'énoncé de la proposition. □

### 2.3. Tores algébriques

Nous rappelons ici quelques résultats et notations sur les tores algébriques.

PROPOSITION 2.9. – *Soient $k$ un corps de clôture séparable $\overline{k}$ et $T_1$, $T_2$ deux tores algébriques (définis) sur $k$. Alors, $T_1$ et $T_2$ sont isogènes sur $k$ 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 $\mathrm{Gal}(\overline{k}/k)$-modules.*

*Démonstration.* – C'est la proposition 1.3.2 de [15]. □

NOTATIONS. – Soient $T$ 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

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

PROPOSITION 2.10. – *Avec les notations précédentes, on a*

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

*De plus, on a*

$$(X_1^\perp)^\perp = X_1, \quad \textit{et} \quad (T_1^\perp)^\perp = T_1.$$

*Démonstration.* – C'est la proposition 1.1.1 de [15]. □

Le résultat suivant est dû à Ribet. Nous introduisons pour cela une nouvelle notation :

NOTATION. – Soient $\ell$ un nombre premier, $\mathbb{K}$ une extension finie de $\mathbb{Q}$, contenue dans $\mathbb{Q}_\ell$, $X/\mathbb{K}$ un tore algébrique et $\mathcal{X}$ un modèle sur $\mathcal{O}_\mathbb{K}$. Si $n$ est un entier strictement positif, on note

$$X(\mathbb{Z}/\ell^n\mathbb{Z}) := \mathcal{X}(\mathbb{Z}_\ell)/\mathcal{X}(1+\ell^n\mathbb{Z}_\ell).$$

THÉORÈME 2.11 (Ribet). – *Soient $\ell$ un nombre premier, $\mathbb{K}$ une extension finie de $\mathbb{Q}$, contenue dans $\mathbb{Q}_\ell$, $X/\mathbb{K}$ un tore algébrique de dimension $\nu$ et $n$ un entier strictement positif. Il existe deux constantes $C$ et $C'$ strictement positives, ne dépendant que de $X/\mathbb{K}$ telles que*

$$C'\ell^{n\nu} \geqslant X(\mathbb{Z}/\ell^n\mathbb{Z}) \geqslant C\ell^{n\nu}.$$

*Démonstration.* – Il s'agit du théorème (2.5) de Ribet [25]. Précisément, Ribet montre cet énoncé avec $\mathbb{K}=\mathbb{Q}$ mais sa preuve vaut dans le cas énoncé ci-dessus. □

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

### 3.1. Un encadrement de $\gamma(A)$

On donne ici un encadrement élémentaire de l'exposant $\gamma$ pour un produit de variétés abéliennes.

PROPOSITION 3.1. – *Soient $r \geqslant 2$ un entier et $A_1, \ldots, A_r$ des variétés abéliennes sur un corps de nombres $K$. Soient $n_1, \ldots, n_r \geqslant 1$ des entiers. On a*

$$\max_{\emptyset \neq S \subset \{1,\ldots,r\}} \Big(\min_{i\in S} n_i\Big)\gamma\Big(\prod_{j\in S} A_j\Big) \leqslant \gamma\Big(\prod_{i=1}^{r} A_i^{n_i}\Big) \leqslant \sum_{i=1}^{r} n_i\gamma(A_i).$$

*Démonstration.* – Cela découle immédiatement de ce que si $F/K$ est une extension finie et $P = (P_1, \ldots, P_m)$ est un point de $A_1 \times \cdots \times A_m(F)$, alors $P$ est de torsion si et seulement si tous les $P_i$ le sont. Explicitons par exemple la preuve de l'inégalité de gauche : soit $S$ un sous-ensemble non vide de $\{1, \ldots, r\}$. On a

$$\begin{aligned}\Big|\Big(\prod_{j\in S} A_j\Big)(F)_{\mathrm{tors}}\Big|^{\min_{i\in S} n_i} &= \Big|\Big(\prod_{j\in S} A_j^{\min_{i\in S} n_i}\Big)(F)_{\mathrm{tors}}\Big| \\ &\leqslant \Big|\Big(\prod_{i=1}^{r} A_i^{n_i}\Big)(F)_{\mathrm{tors}}\Big|.\end{aligned}$$

On en déduit

$$\gamma\Big(\prod_{j\in S} A_j\Big) \leqslant \frac{1}{\min_{i\in S} n_i}\gamma\Big(\prod_{i=1}^{r} A_i^{n_i}\Big).$$

Ceci prouve la première inégalité. La seconde se démontre de la même façon. □

COROLLAIRE 3.2. – *Soient $A/K$ une variété abélienne sur un corps de nombres $K$ et $n \geqslant 1$ un entier. On a*

$$\gamma(A^n) = n\gamma(A).$$

*De plus si $A$ est isogène (sur $\overline{K}$) au produit $\prod_{i=1}^{r} A_i^{n_i}$ les $A_i$ étant deux à deux non isogènes, on a*

$$\max\left\{\max_{1\leqslant i\leqslant r} n_i\gamma(A_i), \Big(\min_{1\leqslant i\leqslant r} n_i\Big)\gamma\Big(\prod_{i=1}^{r} A_i\Big)\right\} \leqslant \gamma(A) \leqslant \sum_{i=1}^{r} n_i\gamma(A_i).$$

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 toutefois que l'encadrement donné dans le corollaire 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 CM deux à deux non isogènes définies sur un corps de nombres $K$ et où $n_0$ et $n_1$ sont deux entiers strictement positifs tels que $n_0 \geqslant 2(n_1 + 1)$. En admettant les résultats de l'introduction (précisément le corollaire 1.13), l'encadrement précédent donne dans ces deux cas

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

### 3.2. Minoration de $\gamma(A)$

Comme annoncé, on étend ici l'inégalité (1) de l'introduction au cas d'une variété abélienne quelconque.

PROPOSITION 3.3. – *Soit $A/K$ une variété abélienne quelconque avec $K$ un corps de nombres plongé dans $\mathbb{C}$. On a*

$$\gamma(A) \geqslant \frac{2\dim A}{\dim \mathrm{MT}(A)}$$

*où $\mathrm{MT}(A)$ est le groupe de Mumford–Tate de $A$.*

*Démonstration.* – On se donne un premier $\ell$, un entier strictement positif $n$ tels que $(\ell, n) \neq (2, 1)$ et le groupe $H = A[\ell^n]$. On veut montrer que

$$\ell^{2gn} = |H| \geqslant c(A/K)\big[K(H) : K\big]^{\frac{2g}{d}}$$

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

$$\forall n \in \mathbb{N}, \quad V_n := \big\{x \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \mid x = \mathrm{Id} \bmod \ell^n\big\}, \quad \text{et} \quad G_n = G_\ell \cap V_n.$$

On vérifie immédiatement que pour tout entier $n$ positif, $G_n/G_{n+1}$ et $V_n/V_{n+1}$ sont des $\mathbb{F}_\ell$-espaces vectoriels, où l'on a noté $\mathbb{F}_\ell$ le corps à $\ell$ éléments. Par ailleurs, on a les inclusions de groupes (c'est pour que la première inclusion soit vraie que l'on a fait l'hypothèse sur le couple $(\ell, n)$) :

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

la première inclusion étant définie par l'élévation à la puissance $\ell$ et la seconde étant induite par l'application $x \mapsto x$. De plus, $V_n/V_{n+1}$ s'injecte dans l'espace tangent de $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ en l'identité. Notons

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

La suite $(d_n)_{n\in\mathbb{N}}$ est croissante et stationnaire à partir d'un certain rang $n_0$. On note $d_\infty$ sa limite. Le groupe $G_{n_0}$ est limite profinie des groupes $G_{n_0}/G_{n_0+k}$. Dans ces conditions on peut montrer que le groupe $G_{n_0}$ est homéomorphe à $\mathbb{Z}_\ell^{d_\infty}$. En particulier on en déduit que

$$d_\infty \leqslant \dim \overline{G_\ell} \leqslant \dim \mathrm{MT}(A)$$

la dernière inégalité résultant du théorème 2.4. On a ainsi :

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

On conclut en élevant ceci à la puissance $\frac{2g}{d}$. □

## 4. Majoration de l'exposant $\alpha(A)$ : le théorème 1.12

Soient $K$ un corps de nombres et $A/K$ une variété abélienne de type CM, sans facteur carré et de dimension $g$. Nous utiliserons dans la suite les notations du paragraphe 2.2. Notamment on note $\chi_1, \ldots, \chi_{2g}$ les caractères de $\mathcal{T}$ diagonalisant l'action de $\mathcal{T}$ sur $V_{\overline{\mathbb{Q}}}$. L'hypothèse faite sur $A$, à savoir qu'elle est sans facteur carré, entraîne en particulier que les caractères $\chi_i$ sont deux

à deux distincts. Suivant une idée de Ribet et Lenstra (cf. [25] p. 87), on peut en fait montrer mieux. Les caractères $\chi_i$ sont dans $X^*(\mathcal{T})$ qui est un $\mathbb{Z}$-module libre de rang fini. Étant donné un nombre premier $\ell$, nous dirons que *deux caractères coïncident modulo* $\ell$ s'ils coïncident dans le quotient $X^*(\mathcal{T})/\ell X^*(\mathcal{T})$.

LEMME 4.1. – *Les caractères $\chi_i$ sont deux à deux distincts modulo* 2.

*Démonstration.* – Soient $i$ et $j$ deux entiers tels que $\chi_i = \chi_j \bmod 2$. Montrons que $\chi_i = \chi_j$. Par la proposition 2.8 on sait que, en étendant les scalaires à $\overline{\mathbb{Q}}$, les images de $\sigma\mu$, $\sigma$ décrivant $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, engendrent $\mathcal{T}_{\overline{\mathbb{Q}}}$. Ainsi pour montrer que deux caractères coïncident, il suffit de montrer que

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

Or $\langle \chi_i - \chi_j, \sigma^{-1}\mu \rangle = \langle \chi_i^\sigma - \chi_j^\sigma, \mu \rangle$. De plus pour tout $\sigma$ et pour tout $\chi \in I$, $\chi^\sigma \in I$. D'autre part si deux caractères $s, t$ coïncident modulo 2, alors $s^\sigma = t^\sigma \bmod 2$. Il suffit donc de montrer que si $\chi_i = \chi_j \bmod 2$ alors $\langle \chi_i - \chi_j, \mu \rangle = 0$. Or par la proposition 2.8 on sait que $\langle \chi_i, \mu \rangle \in \{0, 1\}$, et de même pour $j$. On en déduit donc que $\langle \chi_i - \chi_j, \mu \rangle \in \{-1, 0, 1\}$. On conclut en remarquant qu'un nombre dans cet ensemble vaut zéro modulo 2 si et seulement s'il est nul. □

*Remarque* 4.2. – La même preuve montre plus généralement que les $\chi_i$ sont deux à deux distincts modulo $\ell$ pour tout nombre premier $\ell$.

COROLLAIRE 4.3. – *Soit $W$ un sous-$\mathbb{Q}$-espace vectoriel non nul de $X^*(\mathcal{T}) \otimes \mathbb{Q}$. En utilisant la notation $n(W) = |I \cap W|$ on a*

$$n(W) \leqslant 2^{\dim W - 1}.$$

*Démonstration.* – Quitte à renuméroter, soient $\chi_1, \ldots, \chi_{n(W)}$ les $n(W)$ éléments de $I$ dans $W$. Ils engendrent dans $X^*(\mathcal{T})$ un $\mathbb{Z}$-module libre $X$ de rang inférieur à $\dim W$. En réduisant modulo 2, on voit que $X/2X$ est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel de dimension majorée par $\dim W$ et qui contient les $\bar{\chi}_1, \ldots, \bar{\chi}_{n(W)}$, où $\bar{\chi}$ désigne le caractère $\chi$ modulo 2. Par le lemme 4.1 précédent les $\bar{\chi}_i$ sont deux à deux distincts. Par ailleurs, la proposition 2.8 indique que si $\chi \in I$ alors $\langle \chi, \mu + \mu' \rangle = 1$. Donc pour tout entier $i$ compris entre 1 et $n(W)$, les $\chi_i$ sont contenus dans l'hyperplan affine $H_1 = \{\chi \mid \langle \chi, \mu + \mu' \rangle = 1\}$ de $W$. En réduisant modulo 2, on conclut par cardinalité. □

COROLLAIRE 4.4. – *On a*

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

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

*Démonstration.* – Soit $W$ un sous-$\mathbb{Q}$-espace vectoriel non nul de $X^*(\mathcal{T}) \otimes \mathbb{Q}$. Il s'agit de montrer que $\frac{n(W)}{\dim W} \leqslant \frac{2g}{2+\log_2 g}$. On découpe la preuve en deux morceaux :

1. Si $\dim W \leqslant 2 + \log_2 g$, 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 1.10 : l'inégalité $\alpha(A) \leqslant \gamma(A)$

Avant de prouver l'inégalité qui nous intéresse le plus, à savoir une majoration de l'exposant $\gamma(A)$, nous commençons par montrer dans ce paragraphe que la borne donnée par $\alpha(A)$ est

nécessairement optimale : on a $\alpha(A) \leqslant \gamma(A)$. La preuve de ceci correspond à un cas particulier plus simple de la preuve de l'inégalité réciproque. Certaines idées intervenant sous forme moins technique, il nous semble instructif de détailler ici les choses, en espérant rendre ainsi plus accessible la preuve de la seconde inégalité.

Rappelons brièvement les notations que nous utiliserons ici et dans la suite : $A/K$ est une variété abélienne de dimension $g$, de type CM, sans facteur carré sur un corps de nombres $K$. Son groupe de Mumford–Tate est noté $\mathcal{T}$ : c'est un tore algébrique sur $\mathbb{Q}$. Pour tout premier $\ell$ nous notons $V_\ell = T_\ell(A) \otimes \mathbb{Q}_\ell$ le module de Tate : c'est un $\mathbb{Q}_\ell$-espace vectoriel de dimension $2g$. Enfin nous notons, comme dans la définition 2.2, $G_\ell$ l'image dans $\mathrm{Aut}(T_\ell(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ de la représentation $\ell$-adique $\rho_\ell$.

Soit $W$ un sous-espace vectoriel non nul de $X^*(\mathcal{T}) \otimes \mathbb{Q}$ réalisant le sup $\alpha(A)$. Soit $\ell$ un nombre premier totalement décomposé dans le produit de corps CM correspondant à $A$, de sorte que l'action de $\mathcal{T}$ sur $V_\ell$ est décomposée : les caractères $\chi_1, \ldots, \chi_{2g}$ diagonalisant l'action sont rationnels sur $\mathbb{Q}_\ell$. Quitte à renuméroter et à extraire une base, on a :

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

les $\chi_1, \ldots, \chi_{\dim W}$ formant une base de $W$. L'espace vectoriel $W$ étant fixé dans la suite nous noterons également

$$H = \left\{ Q \in A[\ell] \;\middle|\; Q = \sum_{i \in I_W} m_i P_i,\ m_i \in \mathbb{F}_\ell \right\},$$

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

Posons $L = K(H)$. On a par définition de $H$ :

$$\big|A(L)_{\mathrm{tors}}\big| \geqslant |H| = \ell^{n(W)}.$$

Nous voulons montrer que $\ell^{n(W)} \gg [L : K]^{\alpha(A)} = [L : K]^{\frac{n(W)}{\dim W}}$, où $\gg$ signifie « supérieur à, à une constante multplicative près indépendante de $\ell$ ». En simplifiant par $n(W)$ nous voulons donc montrer que $[L : K] \ll \ell^{\dim W}$. Nous allons en fait montrer mieux : nous allons voir que

$$\ell^{\dim W} \gg\!\ll [L : K].$$

Posons

$$G_H = \big\{ t \in \mathcal{T}(\mathbb{Z}_\ell) \mid \forall i \in I_W\ \chi_i(t) = 1 \bmod \ell \big\}.$$

On a

$$\begin{aligned} G_H \cap G_\ell &= \big\{ t \in G_\ell \mid \forall i \in I_W\ \chi_i(t) = 1 \bmod \ell \big\} \\ &= \big\{ \sigma \in G_\ell \mid \forall i \in I_W\ \sigma(P_i) = P_i \big\} \\ &= t\{ \sigma \in G_\ell \mid \sigma_{|H} = \mathrm{Id} \}. \end{aligned}$$

Notamment ceci montre que

$$[L : K] = \left| \frac{G_\ell}{G_\ell \cap G_H} \right|.$$

Or le théorème 2.6 dit que l'inclusion $G_\ell \hookrightarrow \mathcal{T}(\mathbb{Z}_\ell)$ est de conoyau de cardinal majoré par une constante $C_1$ indépendante de $\ell$. On en déduit que l'inclusion de $G_\ell/G_\ell \cap G_H$ dans $\mathcal{T}(\mathbb{Z}_\ell)/G_H$ est également de conoyau majoré indépendamment de $\ell$. Notamment

$$[L:K] \gg\ll \left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_H}\right|.$$

On voudrait maintenant conclure en appliquant le théorème 2.11 de Ribet. Pour cela il nous reste à interpréter le quotient $|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_H}|$ comme le cardinal de $T_1(\mathbb{Z}/\ell\mathbb{Z})$ où $T_1$ est un tore algébrique à déterminer. Si $T_1$ est de dimension $\dim W$ on aura alors le résultat attendu :

$$[L:K] \gg\ll \ell^{\dim T_1} = \ell^{\dim W}.$$

Notons $X^*$ le sous-$\mathbb{Z}$-module de $X^*(\mathcal{T})$ engendré par les $\chi_i$ pour $i \in I_W$ et posons

$$T^{(1)} = X^{*\perp} = \bigcap_{\chi \in X^*} \ker \chi \quad \text{et} \quad T_1 = \mathcal{T}/T^{(1)}.$$

On a une isogénie $\mathcal{T} \sim T^{(1)} \times T_1$. Ces groupes algébriques sont définis sur $\mathbb{Q}_\ell$ par construction, mais étant définis par les caractères $\chi_i$, ils sont également définis sur une extension finie de $\mathbb{Q}$. Autrement dit, ils sont définis sur une extension finie $\mathbb{K}$ de $\mathbb{Q}$, contenue dans $\mathbb{Q}_\ell$. Donc l'isogénie est une isogénie sur $\mathbb{K}$. De plus cette extension $\mathbb{K}/\mathbb{Q}$ est une sous-extension de $\mathbb{Q}(I)$, corps de définition des $\chi \in I$. Il n'y a donc qu'un nombre fini de telles extensions $\mathbb{K}$ lorsque $\ell$ varie (parmi les premiers totalement décomposés comme indiqué au début du paragraphe).

De plus $X^*(T_1) = X^*(\mathcal{T}/X^{*\perp}) \simeq X^*$ et $T_1$ est de dimension $\dim W$. Par construction de $T^{(1)}$, on a :

$$\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_H}\right| \gg\ll \left|\frac{T_1(\mathbb{Z}_\ell)}{\{t \in T_1(\mathbb{Z}_\ell) \mid \forall \chi \in X^*\ \chi(t) = 1 \bmod \ell\}}\right|.$$

Suivant les notations de Ribet on a donc

$$\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_H}\right| \gg\ll \left|\frac{T_1(\mathbb{Z}_\ell)}{T_1(1+\ell\mathbb{Z}_\ell)}\right| \gg\ll \ell^{\dim T_1} = \ell^{\dim W}.$$

Suivant la même idée nous allons dans la suite prouver l'inégalité $\gamma(A) \leqslant \alpha(A)$. On commence pour cela par montrer qu'il suffit de savoir montrer l'inégalité $\mathrm{Card}\,(H) \ll [K(H):K]^{\alpha(A)}$ pour tout sous-groupe fini $H$ de $A[\ell^\infty]$, stable par $\mathrm{Gal}(\overline{K}/K)$ et pour tout premier $\ell$ : c'est la réduction au cas $\ell$-adique. Ensuite la preuve suit ce qui vient d'être fait précédemment : on commence par découper le groupe $H$ selon les morceaux irréductibles de la représentation du groupe de Mumford–Tate dans $\mathrm{GL}(\mathbb{Q}_\ell)$. Il reste ensuite une dernière étape consistant à recomposer astucieusement ces morceaux de sorte à pouvoir estimer le degré de l'extension des morceaux recomposés en fonction de la taille des morceaux. Là encore le degré des extensions qui interviendront s'interprétera comme le cardinal des points d'ordre une puissance de $\ell$ d'un tore algébrique, fabriqué par le même principe que ci-dessus. Dans la dernière étape, il y a deux complications qui se présentent par rapport au cas traité ci-dessus. D'une part le groupe $H$ n'est plus de type $(\ell,\dots,\ell)$ : les morceaux intervenant vont donc avoir des poids distincts ce qui complique la partie combinatoire ; d'autre part les caractères n'ont aucune raison d'être définis dans $\mathbb{Q}_\ell$, il faudra donc les grouper par paquets. Afin de rendre plus lisible la preuve nous traiterons pour cette dernière étape tout d'abord le cas où les caractères sont définis sur $\mathbb{Q}_\ell$ (i.e.

$\mathcal{T}_\ell$ décomposé sur $\mathbb{Q}_\ell$) : il s'agit du paragaphe 7.2. Le cas général avec groupement par paquets n'induit essentiellement pas de difficulté supplémentaire autre que de notation. La preuve est faite au paragraphe 7.3.

## 6. Le théorème 1.10 : réduction au cas $\ell$-adique

Nous allons maintenant montrer la seconde inégalité

$$\gamma(A) \leqslant \alpha(A). \tag{2}$$

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 d'après Serre–Tate [32] une variété abélienne de type CM a potentiellement bonne réduction en toute place). Ceci va nous permettre de nous ramener comme dans Ribet [25] au cas $\ell$-adique. Nous rappelons avant cela un résultat classique concernant les variétés abéliennes de type CM :

LEMME 6.1. – *Soit $A/K$ une variété abélienne de type CM sur un corps de nombres $K$. Quitte à remplacer $K$ par une extension finie $K'$ ne dépendant que de $A$, on a : pour tout ensemble $S$ de points de torsion de $A(\overline{K})$, l'extension $K(S)/K$ est abélienne.*

*Démonstration.* – Il suffit de montrer que $A_{\mathrm{tors}}$ engendre une extension abélienne sur $K$. Pour vérifier ceci il suffit de traiter le cas d'une variété abélienne simple de type CM et de montrer que, pour tout entier $n \geqslant 1$ et tout premier $\ell \geqslant 2$, l'extension $K(A[\ell^n])/K$ est abélienne (on prend ensuite le compositum). Ceci revient à voir que l'image $G_\ell$ de $\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(A)) \subset \mathrm{Aut}(V_\ell)$ est commutative. Or ceci est vrai : c'est le corollaire 2 p. 502 de [32]. □

PROPOSITION 6.2. – *Pour démontrer l'inégalité* (2)*, 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 $\ell$ et tout sous-groupe fini $H$ de $A[\ell^\infty]$, stable par $\mathrm{Gal}(\overline{K}/K)$, on ait*

$$\mathrm{Card}(H) \leqslant C(A/K)\big[K(H) : K\big]^{\alpha(A)}. \tag{3}$$

*Démonstration.* – Soit $L/K$ une extension finie. Posons

$$L' = K\big(A(L)_{\mathrm{tors}}\big), \quad H = A(L')_{\mathrm{tors}} \quad \text{et pour tout premier } \ell,\ H_\ell = A(L')_{\mathrm{tors}}[\ell^\infty].$$

Vérifions tout d'abord que $H_\ell$ est stable par $\mathrm{Gal}(\overline{K}/K)$ : si $\sigma \in \mathrm{Gal}(\overline{K}/K)$ et $x \in H_\ell$, alors $\sigma(x) \in A[\ell^\infty]$. Par ailleurs $A$ étant de type CM, les extensions engendrées par des points de torsion sont galoisiennes sur $K$ d'après le lemme 6.1 (quitte à avoir au départ remplacé, ce que l'on suppose ici, $K$ par une extension finie $K'$ ne dépendant que de $A$). Or $K(H_\ell) \subset L'$, donc $\sigma(x) \in A(L') \cap A[\ell^\infty] = H_\ell$. On peut donc appliquer l'hypothèse de l'énoncé aux groupes $H_\ell$ pour tout premier $\ell$ :

$$|H_\ell| \ll \big[K(H_\ell) : K\big]^{\alpha(A)}.$$

En notant $\omega(n)$ le nombre de nombres premiers divisant $n$, il vient

$$\big|A(L)_{\mathrm{tors}}\big| = \big|A(L')_{\mathrm{tors}}\big| = |H| = \prod_\ell |H_\ell| \leqslant C(A/K)^{\omega(|A(L')_{\mathrm{tors}}|)} \prod_\ell \big[K(H_\ell) : K\big]^{\alpha(A)}. \tag{4}$$

En effet, sur la définition de $L'$ on voit immédiatement que $A(L)_{\mathrm{tors}} = A(L')_{\mathrm{tors}}$. Par ailleurs, une estimation classique de $\omega(n)$ est la suivante (cf. par exemple [37] p. 85 § 5.3) : $\omega(n) \ll \frac{\log n}{\log\log n}$. L'inégalité (4) peut donc se réécrire

$$\big|A(L)_{\mathrm{tors}}\big|^{1-\frac{C_1(A/K)}{\log\log|A(L)_{\mathrm{tors}}|}} \leqslant \prod_{\ell} \big[K(H_\ell) : K\big]^{\alpha(A)}.$$

Or $H_\ell = A(L')[\ell^\infty]$. Si pour tout entier $M \geqslant 1$, si on note $A(L')[M]$ la partie de $M$-torsion de $A(\overline{K})$ rationnelle sur le corps $L'$, et $d_{L'}(M) = [K(A(L')[M]) : K]$, alors par la théorie de Serre–Tate [32], 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 $K$ (rappelons, cf. par exemple [36] p. 118 Example 3.3, que par définition le corps de classes de Hilbert de $K$ est la plus grande extension abélienne de $K$ partout non ramifiée). En remplaçant $K$ par son corps de classes de Hilbert on obtient ainsi : la fonction

$$M \mapsto d_{L'}(M)$$

est multiplicative au sens arithmétique. On en déduit

$$\big|A(L)_{\mathrm{tors}}\big|^{1-\frac{C_1(A/K)}{\log\log|A(L)_{\mathrm{tors}}|}} \leqslant \big[K(H) : K\big]^{\alpha(A)} \leqslant [L' : K]^{\alpha(A)} \leqslant [L : K]^{\alpha(A)}.$$

Ceci conclut. □

Dans le paragraphe 7 suivant, nous donnons une preuve de l'inégalité (3).

## 7. Le théorème 1.10 : cas de la $\ell^\infty$-torsion

### 7.1. Un résultat préliminaire

Le résultat principal de cette section est la proposition 7.4.

#### 7.1.1. Préliminaires

LEMME 7.1. – *Soient $\mathbb{K}$ un corps, $G/\mathbb{K}$ un groupe algébrique, $V$ un $\mathbb{K}$-espace vectoriel non nul de dimension finie et $\rho : G \to \mathrm{GL}_V$ une représentation telle que $\rho : G(\mathbb{K}) \to \mathrm{GL}(V)$ soit irréductible. Soit $\mathcal{G}$ un sous-groupe abstrait de $G(\mathbb{K})$, Zariski dense dans $G$. Alors la représentation*

$$\rho_{|\mathcal{G}} : \mathcal{G} \to \mathrm{GL}(V)$$

*est irréductible.*

*Démonstration.* – Soit $W \neq \{0\}$ un sous-$\mathbb{K}$-espace vectoriel de $V$ stable par $\rho_{|\mathcal{G}}$. Notons $G_W$ le stabilisateur de $W$ dans $G$ (i.e. le foncteur défini par $G_W(R) := \{g \in G(R) \mid \rho(g)(W \otimes_{\mathbb{K}} R) = W \otimes_{\mathbb{K}} R\}$) : c'est un sous-groupe algébrique de $G/\mathbb{K}$. Par hypothèse, $\mathcal{G} \subset G_W(\mathbb{K})$, donc par densité de $\mathcal{G}$ dans $G$, on en déduit que $G_W = G$. Ainsi $W$ est stable par la représentation $\rho : G(\mathbb{K}) \to \mathrm{GL}(V)$, donc par irréductibilité de cette dernière, $W = V$. □

Reprenons les notations des paragraphes précédents. Soit $\ell$ un nombre premier. Le tore $\mathcal{T}/\mathbb{Q}$ opère fidèlement sur $V$ par la représentation $\rho$. On note comme précédemment $I = \{\chi_1, \ldots, \chi_{2g}\}$ les poids du tore, i.e. les caractères diagonalisant l'action de $\mathcal{T}$ sur $V_{\overline{\mathbb{Q}}}$.

Si $\chi \in I$ nous noterons $\sigma_1(\chi) = \mathrm{Id}, \ldots, \sigma_{t_\chi}(\chi)$ les différents plongements de $\mathbb{Q}_\ell(\chi)$, corps de définition de $\chi$ sur $\mathbb{Q}_\ell$, dans $\overline{\mathbb{Q}_\ell}$. Sur $\mathbb{Q}_\ell$, on peut décomposer la représentation

$$\mathcal{T}(\mathbb{Q}_\ell) \xrightarrow{\rho_{\mathbb{Q}_\ell}} \mathrm{GL}(V_\ell)$$

en une somme de représentations irréductibles, chacune se décomposant à nouveau sur $\overline{\mathbb{Q}}_\ell$ en

$$\begin{pmatrix} \chi & & \\ & \ddots & \\ & & \chi^{\sigma_{t_\chi}(\chi)} \end{pmatrix}$$

où $\chi$ ainsi que ses conjugués sont des éléments de $I$. Par le lemme 7.1 précédent (appliqué avec $\mathbb{K} = \mathbb{Q}_\ell$, $G = \mathcal{T}$ et $\mathcal{G} = G_\ell$), cette décomposition en irréductibles correspond également à la décomposition en irréductibles de la représentation restreinte

$$\rho_{|\ell} : G_\ell \subset \mathcal{T}(\mathbb{Q}_\ell) \xrightarrow{\rho_{\mathbb{Q}_\ell}} \mathrm{GL}(V_\ell)$$

correspondant à la représentation $\ell$-adique $\rho_\ell$.

Étant donné un caractère $\chi \in I$, nous noterons $\rho_\chi$ (et $V_\chi$ le $\mathbb{Q}_\ell$-espace vectoriel correspondant) la sous-représentation irréductible de $\rho_{\mathbb{Q}_\ell}$ (ou de manière équivalente $\rho_{|\ell}$) dans laquelle apparaît $\chi$ quand on étend les scalaires à $\overline{\mathbb{Q}}_\ell$. Le nombre $t_\chi$ est la dimension de $V_\chi$ sur $\mathbb{Q}_\ell$. Les caractères $\chi$ étant deux à deux distincts, les sous-représentations $V_\chi$ sont uniquement déterminées. On note alors

$$T_\chi = V_\chi \cap T_\ell(A).$$

Si $x \in V_\chi$, on a : $\forall t \in \mathcal{T}(\mathbb{Q}_\ell)$, $\rho(t)x = \rho_\chi(t)x$. De plus la représentation $\rho_{|\ell}$ (définie sur $G_\ell = \mathrm{Im}(\rho_\ell)$) est en fait à valeur dans $\mathrm{Aut}(T_\ell(A))$. En particulier, pour tout $t \in G_\ell$, $\rho(t)$ laisse stable $T_\ell(A)$ et donc $\rho_\chi(t)$ laisse stable $T_\chi$.

On a la décomposition $V_\ell = \bigoplus V_\chi$, donc en posant $T = \bigoplus T_\chi$ on obtient un réseau de $V_\ell$ qui est un sous-réseau de $T_\ell(A)$ . En prolongeant (pour $t \in \mathcal{T}(\mathbb{Q}_\ell)$) $\rho_\chi(t)$ à $V_\ell$ par $\rho_\chi(t)x = 0$ si $x$ est dans $V_{\chi'}$ pour $\chi'$ non conjugué à $\chi$, on a

$$\forall t \in G_\ell,\ \forall x \in T, \quad \rho_\chi(t)x \in T_\chi \subset T.$$

LEMME 7.2. – *L'inclusion $T \subset T_\ell(A)$ est de conoyau d'indice borné indépendamment de $\ell$.*

*Démonstration.* – Rappelons tout d'abord que le module $T_\ell(A)$ provient de $\mathbb{Z}$ : en effet on a $T_\ell(A) = \mathrm{H}_1(A(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ (cf. [11] 15.1 (a)). Les $2g$ caractères $\chi$ sont tous définis sur une extension finie $\mathbb{Q}(I)$ de $\mathbb{Q}$. Donc la décomposition de $\rho_{\mathbb{Q}_\ell}$ (et donc de $\rho_{|\ell}$) en irréductibles selon les $\rho_\chi$ est en fait déjà valable sur une sous-extension $L$ de $\mathbb{Q}(I)$, contenue dans $\mathbb{Q}_\ell$ ; les $V_\chi$ provenant de la décomposition en irréductibles de $V_L = V \otimes_{\mathbb{Q}} L$ par extension des scalaires à $\mathbb{Q}_\ell$. Il n'y a qu'un nombre fini de sous-$\mathbb{Q}$-extensions contenues dans $\mathbb{Q}(I)$. Pour $\ell$ variable, les décompositions de $\rho_{|\ell}$ en irréductibles proviennent donc d'un nombre fini de décompositions. Ceci montre en particulier que pour $\ell$ assez grand $T = T_\ell(A)$. □

Nous noterons dans la suite $\ell_0$ un premier tel que si $\ell \geqslant \ell_0$, alors $T_\ell(A) = T$ et nous noterons $n_0$ un entier tel que, pour tout premier $\ell$, on ait $\ell^{n_0} T_\ell(A) \subset T$.

Faisons quelques remarques sur $T$ et les $T_\chi$ (les points 1 et 2 découlant de ce que $T = \bigoplus T_\chi$) :

1. Soit $m \geqslant 1$. On a $T_\chi/T_\chi \cap \ell^m T = T_\chi/\ell^m T_\chi$.
2. Soit $m \geqslant 1$. On a $T/\ell^m T = \bigoplus T_\chi/\ell^m T_\chi$.
3. Soit $n \geqslant m \geqslant 1$. On a un isomorphisme

$$\ell^m T_\chi/\ell^n T_\chi \simeq T_\chi/\ell^{n-m} T_\chi,$$

donné par $x \mapsto \ell^{-m} x \mod \ell^{n-m}$.
4. Enfin on a de même, pour $n \geqslant m \geqslant 1$ :

$$(T_\chi/\ell^n T_\chi)[\ell^m] = \ell^{n-m} T_\chi/\ell^n T_\chi \subset T_\chi/\ell^m T_\chi,$$

la dernière inclusion étant due au point 3 ; et de même pour $T$ et pour $T_\ell(A)$.

**7.1.2. La proposition**

Soit $H$ un sous-groupe fini non trivial de $A[\ell^\infty]$ stable par Galois (donc par $\rho_{|\ell}$) et d'exposant $\ell^n$. Nous allons décomposer $H$ selon les sous-représentations $\rho_\chi$. Par définition $n \geqslant 1$ est le plus petit entier tel que $H \subset A[\ell^n]$. Si $m \geqslant 1$, notons

$$j_m : T_\ell(A)/\ell^m T_\ell(A) \to T/\ell^m T, \quad x \mapsto \begin{cases} \ell^{n_0} x & \text{si } \ell < \ell_0, \\ x & \text{si } \ell \geqslant \ell_0. \end{cases}$$

Notons que si $\ell \geqslant \ell_0$, l'application $j_m$ n'est autre que l'identité sur $A[\ell^m]$. Un premier $\ell$ quelconque étant fixé, nous allons travailler avec $j_n(H)$ plutôt qu'avec $H$. Les remarques précédentes entraînent que $j_n(H) \simeq j_m(H)$ pour $m \geqslant n$. On renote $H'$ ce groupe. Il est stable par $\rho_{|\ell}$ et $|H'| \gg\ll |H|$, $\gg\ll$ signifiant comparable à des constantes indépendantes de $\ell$ et $n$ près.

Notons pour tout entier $m \geqslant 1$, $\pi_m : T \to T/\ell^m T$ la projection canonique. On définit

$$\widehat{H'} := \pi_n^{-1}(H'), \quad \widehat{H_{\rho_\chi}} := \widehat{H'} \cap V_\chi, \quad \text{et} \quad H_{\rho_\chi} := \pi_n(\widehat{H_{\rho_\chi}}).$$

Les $H_{\rho_\chi}$ sont inclus dans $H'$ et leur somme est directe. De plus, par définition on a bien le découpage voulu :

$$H_{\rho_\chi} = \{x \in H' \mid \forall t \in G_\ell,\ \rho(t)x = \rho_\chi(t)x\}.$$

DÉFINITION 7.3. – Nous noterons dans la suite $n_\chi$ l'entier tel que $\ell^{n_\chi}$ soit l'exposant de $H_{\rho_\chi}$ pour tout $\chi \in I$.

PROPOSITION 7.4. – *Le $\mathbb{Z}_\ell$-module $\widehat{H'}$ est, à un indice fini borné indépendamment de $\ell$ près, la somme directe des $\widehat{H_{\rho_\chi}}$ correspondant aux différentes sous-représentations irréductibles $\rho_\chi$ de $\rho_{|\ell}$. Il en est de même pour l'inclusion $\bigoplus H_{\rho_\chi} \subset H'$. De plus, il existe $\ell_1$ premier et $n_1 \in \mathbb{N}^*$ (indépendants de $H$) tels que chaque $H_{\rho_\chi}$ soit en tant que groupe, de la forme suivante* :

$$\text{si } \ell \geqslant \ell_1 \quad \text{alors } H_{\rho_\chi} \simeq (\mathbb{Z}/\ell^{n_\chi}\mathbb{Z})^{t_\chi}, \tag{5}$$

*et,*

$$\text{si } \ell < \ell_1 \text{ et, si } n_\chi \geqslant n_1, \quad \text{alors } H_{\rho_\chi} \simeq \prod_{i=1}^{t_\chi} \mathbb{Z}/\ell^{n_\chi - r_i}\mathbb{Z} \tag{6}$$

*où pour tout $i$, $0 \leqslant r_i < n_1$.*

Avant d'aborder la preuve proprement dite, nous commençons par trois lemmes. Les deux premiers seront utilisés pour prouver la première assertion concernant la décomposition en somme directe ; le dernier nous servira à prouver l'affirmation concernant le cardinal des $H_{\rho_\chi}$ pour les petits $\ell$.

On sait par le théorème 2.6 qu'il existe une constante $c \in \mathbb{N}^*$ telle que

$$\forall \ell \text{ premier}, \quad \left|\mathcal{T}(\mathbb{Z}_\ell)/G_\ell\right| \text{ divise } c.$$

LEMME 7.5. – *Il existe $t \in \mathcal{T}(\mathbb{Q})$ tel que* $\operatorname{disc}\rho(t^c) \neq 0$.

*Démonstration.* – Notons $\Delta$ la sous-variété de $\mathcal{T}/\mathbb{Q}$ définie par $\operatorname{disc}\rho = 0$. C'est une sous-variété stricte de $\mathcal{T}$ (par exemple en passant sur $\overline{\mathbb{Q}}$, on voit que $\Delta_{\overline{\mathbb{Q}}}$ est une réunion finie d'hypersurfaces, car les caractères $\chi$ sont deux à deux distincts). Par ailleurs, l'ensemble $\mathcal{T}(\mathbb{Q})$ est Zariski-dense dans $\mathcal{T}$, donc il en est de même pour l'ensemble $\{t^c \in \mathcal{T}(\mathbb{Q}) \mid t \in \mathcal{T}(\mathbb{Q})\}$. On peut donc trouver un $t$ comme annoncé. □

Nous fixons dans la suite $t_0$ un élément de $\mathcal{T}(\mathbb{Q})$ fourni par le lemme 7.5.

*Remarque* 7.6. – Notons que $t_0$ étant défini sur $\mathbb{Q}$, il existe un premier $\ell_2$ tel que

$$\forall \ell \geqslant \ell_2 \text{ premier}, \quad t_0 \in \mathcal{T}(\mathbb{Z}_\ell).$$

En particulier, pour tout premier $\ell \geqslant \ell_2$ on a $t_0^c \in G_\ell$.

LEMME 7.7. – *Le premier $\ell$ étant fixé, il existe $t_\ell \in G_\ell$ tel que* $\operatorname{disc}\rho(t_\ell) \neq 0$.

*Démonstration.* – C'est la même que précédemment en travaillant sur $\mathbb{Q}_\ell$ plutôt que sur $\mathbb{Q}$ et en utilisant la densité de $G_\ell$ dans $\mathcal{T} \times_{\mathbb{Q}} \mathbb{Q}_\ell$. □

LEMME 7.8. – *Soient $\ell$ un nombre premier, $X$ un $\mathbb{Q}_\ell$-espace vectoriel de dimension finie $d \geqslant 1$, $G$ un groupe (abstrait) abélien et $\sigma : G \to \mathrm{GL}(X)$ une représentation linéaire irréductible. Soit enfin $R$ un réseau de $X$ (i.e. un sous-$\mathbb{Z}_\ell$-module de $X$ tel que $X = R \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$) stable par $\sigma$. Il existe $c_1 > 0$ (dépendant de $\ell$) tel que $\forall n \in \mathbb{N}^*$, $\forall x \in R/\ell^n R$ d'ordre $\ell^n$, on ait :*

$$|R/\ell^n R| = \ell^{nd} \geqslant \operatorname{Card}\big(\langle G \cdot x\rangle\big) \geqslant c_1 \ell^{nd},$$

*où $< G \cdot x >$ est le sous-groupe de $R/\ell^n R$ engendré par les $\sigma(g)(x)$ pour $g \in G$.*

*Démonstration.* – Pour tout entier $n \geqslant 1$, notons $\pi_n : R \to R/\ell^n R$ la réduction modulo $\ell^n$. Supposons par l'absurde le résultat faux : il existe une suite $(x_k) \in R/\ell^{n_k} R$ d'éléments d'ordre $\ell^{n_k}$ telle que

$$\frac{\ell^{n_k d}}{|\langle G \cdot x_k\rangle|} \underset{k \to +\infty}{\longrightarrow} +\infty. \tag{7}$$

Pour tout entier $k$, notons $S_k := \pi_{n_k}^{-1}(\langle G \cdot x_{n_k}\rangle)$. La suite $(S_k)$ est une suite de sous-$\mathbb{Z}_\ell$-modules de $R$ stables par $\sigma$. Écrivons la décomposition de $S_k$ selon les diviseurs élémentaires :

$$S_k = \bigoplus_{i=1}^{d} \ell^{n_i(k)} e_i(k) \mathbb{Z}_\ell$$

avec $n_1(k) \leqslant \cdots \leqslant n_d(k)$ et, pour tout $i$, $\ell \nmid e_i(k)$ (si pour un $k_0$ l'un des $e_i(k_0) = 0$, alors $S_{k_0} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ est un sous-espace vectoriel strict non nul de $X$, stable par $\sigma$, ce qui est impossible par

irréductibilité : on suppose donc que tous les $e_i(k)$ sont non nuls). S'agissant d'entiers positifs, quitte à extraire une sous-suite, on peut supposer (et on le fait) que les suites $(n_i(k))_{k\geqslant 1}$ sont croissantes pour tout $i$. De plus, comme $x_{n_k}$ est d'ordre $\ell^{n_k}$ dans $R/\ell^{n_k}R$, on voit que $n_1(k)=0$ pour tout $k$. On a

$$\big|\langle G\cdot x\rangle\big| = \mathrm{Card}\big(\pi_{n_k}(S_k)\big) = \prod_{i=1}^{j(k)} \ell^{n_k-n_i(k)}$$

où $1\leqslant j(k)\leqslant d$ est le plus petit entier tel que $n_{j(k)+1}(k)\geqslant n_k$ (et où l'on pose $n_{d+1}(k)=+\infty$ pour tout $k$).
Si la suite $(n_d(k))_{k\geqslant 1}$ ne tendait pas vers $+\infty$, alors elle serait bornée (et donc il en serait de même des suites $(n_i(k))\leqslant(n_d(k))$) :

$$\exists m_0\geqslant 1\ \forall k\geqslant 1,\ \forall 1\leqslant i\leqslant d,\quad n_i(k)\leqslant m_0.$$

Ainsi, si $k$ est assez grand on aurait $n_k>m_0\geqslant n_d(k)$. Notamment, pour $k$ assez grand on aurait $j(k)=d$ et,

$$\big|\langle G\cdot x\rangle\big| = \ell^{n_k d-\sum_{i=1}^{d} n_i(k)} \geqslant \ell^{dn_k-dm_0}.$$

Ceci contredit (7), donc la suite $(n_d(k))$ tend vers $+\infty$. Par ailleurs, les suites $(n_i(k))$ sont stationnaires ou tendent vers $+\infty$ (et $(n_1)$ est stationnaire et $(n_d)$ tend vers $+\infty$). Notons $a\in\{1,\dots,d-1\}$ le plus petit entier tel que la suite $(n_{a+1})\to+\infty$. Comme $(n_1)\leqslant\cdots\leqslant(n_d)$, on a donc : pour $1\leqslant i\leqslant a$, la suite $(n_i)$ est stationnaire de limite notée $n_i$, et, pour $i\geqslant a+1$, $(n_i)\to+\infty$.
Pour tout entier $k\geqslant 1$, notons $\mathcal{B}_k=\{e_1(k),\dots,e_d(k)\}$. La suite $(\mathcal{B}_k)$ est une suite de bases de $R$. Par compacité on en extrait une sous-suite convergente de limite $\mathcal{B}:=\{e_1,\dots,e_d\}$. Posons

$$S=\bigoplus_{i=1}^{a}\ell^{n_i}e_i\mathbb{Z}_\ell.$$

Si $S$ est stable par $\sigma$, alors, comme $S\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$ est non nul et de dimension majorée par $a$ avec $1\leqslant a<d$, on pourra conclure par l'absurde grâce à l'irréductibilité de $\sigma$. Reste à voir que $S$ est stable par $\sigma$. Pour cela, il suffit de voir que, pour tout entier $n\geqslant 1$, la projection $\pi_n(S)$ est stable. Soit donc $n\geqslant 1$. Nous allons montrer que, pour $k$ assez grand,

$$\pi_n(S)=\pi_n(S_k).$$

Ceci permettra de conclure car $S_k$ est stable par $\sigma$.

Par stationnarité, il existe $k_0$ tel que $\forall k\geqslant k_0$, $n_i(k)=n_i$ pour tout $i\in\{1,\dots,a\}$. De plus il existe $k_0(n)\geqslant k_0$ tel que $\forall k\geqslant k_0(n)$, $n_d(k)\geqslant\cdots\geqslant n_{a+1}(k)>n$. Enfin, pour tout $i\in\{1,\dots,d\}$, la suite $(\pi_n(e_i(k)))_{k\geqslant 1}$ est une suite convergente d'éléments de l'ensemble fini $R/\ell^nR$. Elle est donc stationnaire. Donc il existe $k_1(n)\geqslant k_0(n)$ tel que $\forall k\geqslant k_1(n)$, $\pi_n(e_i(k))=\pi_n(e_i)$ pour tout $i$. De ceci, on déduit que si $k\geqslant k_1(n)$, on a $\pi_n(S)=\pi_n(S_k)$. Avec ce qui précède, ceci conclut. □

*Démonstration de la proposition 7.4.* – Commençons par prouver la première assertion. La seconde (concernant $\bigoplus H_{\rho_\chi}\subset H'$) s'en déduit immédiatement. Il restera ensuite encore à vérifier l'inégalité numérique sur le cardinal des $H_{\rho_\chi}$.

Considérons la représentation $\rho_{|\ell} : G_\ell \subset \mathcal{T}(\mathbb{Q}_\ell) \xrightarrow{\rho_{\mathbb{Q}_\ell}} \mathrm{GL}(V_\ell)$. Comme déjà expliqué, la décomposition en irréductibles de $\rho_{|\ell}$ est la même que celle de $\rho_{\mathbb{Q}_\ell}$ (il s'agit du lemme 7.1). Notons $V_\ell = \bigoplus_{i=1}^r V_{\ell,i}$ cette décomposition en irréductibles sur $\mathbb{Q}_\ell$ et notons $\mathrm{pr}_{\ell,i} : V_\ell \to V_{\ell,i}$ les projecteurs correspondants. Nous noterons également encore $\mathrm{pr}_{\ell,i}$ les endomorphismes de $V_\ell$ obtenus par composition avec l'inclusion $V_{\ell,i} \subset V_\ell$. Soit $x \in \widehat{H'}$. On a $x = \sum_{i=1}^r \mathrm{pr}_{\ell,i}(x)$ avec $\mathrm{pr}_{\ell,i}(x) \in V_{\ell,i}$. Par définition des $\widehat{H_{\rho_\chi}}$, il nous suffit donc juste de montrer que $\mathrm{pr}_{\ell,i}(x)$ appartient à $\widehat{H'}$ (au moins pourvu que $\ell$ soit assez grand, et, si $\ell$ est petit, que cette décomposition vaut quitte à multiplier au départ $x$ par une constante $M$). Le $\mathbb{Z}_\ell$-module $\widehat{H'}$ étant stable par $\rho_{|\ell}$, il suffit pour cela de montrer que $\mathrm{pr}_{\ell,i}$ est un polynôme, à coefficients dans $\mathbb{Z}_\ell$, en $\rho(t)$ pour $t \in G_\ell$ convenable.

On a déjà dit dans la preuve du lemme 7.2 que, $\rho_{\mathbb{Q}_\ell}$ provenant de $\rho : \mathcal{T} \to \mathrm{GL}_V$ par extension des scalaires à $\mathbb{Q}_\ell$, la décomposition en irréductibles de $\rho_{\mathbb{Q}_\ell}$ est déjà valable sur une extension finie $L/\mathbb{Q}$ incluse dans $\mathbb{Q}(I)$ ; les $V_\chi$ provenant de la décomposition en irréductibles de $V_L = V \otimes_{\mathbb{Q}} L$ par extension des scalaires à $\mathbb{Q}_\ell$. Il n'y a qu'un nombre fini de sous-$\mathbb{Q}$-extensions contenues dans $\mathbb{Q}(I)$ (et lorsque $\ell$ varie, les décompositions de $\rho_{|\ell}$ en irréductibles proviennent donc d'un nombre fini de décompositions). Notons $V_L = \bigoplus_{i=1}^r V_i$ la décomposition en irréductibles selon $\rho$, et, pour $i$ compris entre 1 et $r$, notons $\mathrm{pr}_i : V_L \to V_i$ les projecteurs correspondants. Nous noterons encore $\mathrm{pr}_i$ les endomorphismes de $V_L$ obtenus par composition avec l'inclusion $V_i \subset V_L$. Comme pour les $V_{\ell,i}$, les $\mathrm{pr}_{\ell,i}$ sont définis à partir des $\mathrm{pr}_i$ par extension des scalaires de $L$ à $\mathbb{Q}_\ell$.

*Fait.* – $\forall t \in \mathcal{T}(L),\ \mathrm{pr}_i \circ \rho(t) = \rho(t) \circ \mathrm{pr}_i$.

En effet, si $y \in V_L$, on a

$$\mathrm{pr}_i\big(\rho(t)y\big) = \mathrm{pr}_i\left(\rho(t)\sum_{j=1}^r y_j\right) = \mathrm{pr}_i\left(\sum_{j=1}^r \rho_j(t)y_j\right) = \rho_i(t)y_i = \rho_i(t)\,\mathrm{pr}_i(y) = \rho(t)\,\mathrm{pr}_i(y).$$

Rappelons un résultat d'algèbre linéaire : sur un corps $\mathbb{K}$ toute matrice appartenant au commutant d'une matrice donnée $N$ est un polynôme en $N$ à coefficients dans $\mathbb{K}$ si et seulement si les polynômes caractéristique et minimal de $N$ sont égaux. Dans notre situation, pour tout $t$, $\rho(t)$ est diagonalisable sur $\overline{\mathbb{Q}}$. Donc si pour un $t \in \mathcal{T}(L)$ on a $\mathrm{disc}\,\rho(t) \neq 0$ alors les $\mathrm{pr}_i$ sont des polynômes à coefficients dans $L$ en $\rho(t)$. Or le lemme 7.5 et la remarque 7.6 nous fournissent un premier $\ell_2$ et un $t_0 \in \mathcal{T}(\mathbb{Q})$ tels que

$$\text{si } \ell \geqslant \ell_2, \quad \text{alors } t_0^c \in G_\ell, \text{ et de plus on ait } \mathrm{disc}\big(\rho(t_0^c)\big) \neq 0.$$

Donc $\mathrm{pr}_i$ est un polynôme à coefficients dans $L$ en $\rho(t_0^c)$. Notamment il existe un premier $\ell_3 \geqslant \ell_2$ tel que : si $\ell \geqslant \ell_3$, alors $\mathrm{pr}_{\ell,i}$ est un polynôme à coefficients $\mathbb{Z}_\ell$ en $\rho(t_0^c)$ (le premier $\ell_3$ dépend a priori de $\mathrm{pr}_i$ donc du $\ell$ fixé au début de la section, mais comme il n'y a qu'un nombre fini de décompositions possibles lorsque $\ell$ varie, on peut en fait prendre pour $\ell_3$ une valeur indépendante de $\ell$). Comme $t_0^c \in G_\ell$ ceci conclut : si $\ell \geqslant \ell_3$, alors $\widehat{H'}$ est la somme directe des $\widehat{H_{\rho_\chi}}$. Si $\ell < \ell_3$, alors on applique le lemme 7.7 en lieu et place du lemme 7.5 (en travaillant directement sur $\mathbb{Q}_\ell$ plutôt que sur $L$) et on obtient que $\mathrm{pr}_{\ell,i}$ est un polynôme à coefficients dans $\mathbb{Q}_\ell$ en $\rho(t_\ell)$. Il existe donc une constante $M \in \mathbb{Z}$ telle que $M\,\mathrm{pr}_{\ell,i} \in \mathbb{Z}_\ell[\rho(t_\ell)]$ (là encore $M$ est a priori dépendante de $\ell$ mais comme $\ell < \ell_3$ on peut évidemment choisir $M$ indépendante de $\ell$). Donc $M\,\mathrm{pr}_{\ell,i}(x) \in \widehat{H}$ et donc $M\widehat{H} \subset \bigoplus \widehat{H_{\rho_\chi}}$. Ceci prouve donc la première assertion.

Déterminons maintenant la forme de $H_{\rho_\chi}$. En tant que groupe, $H_{\rho_\chi}$ est un produit de $\mathbb{Z}/\ell^m\mathbb{Z}$ comportant au plus $t_\chi$ facteurs et avec des $m \leqslant n_\chi$. L'assertion est donc une question de cardinalité.

Rappelons que si $\ell \geqslant \ell_0$, alors $T = T_\ell(A)$. Il existe $\ell_1 \geqslant \ell_0$ premier tel que pour tout premier $\ell \geqslant \ell_1$, la décomposition $\rho_{|\ell} \simeq \bigoplus_{i=1}^m \rho_i$ reste irréductible sur $\mathbb{F}_\ell$. En effet, soit $\rho_\chi$ l'une des sous-représentations irréductibles sur $\mathbb{Q}_\ell$ considérées. Elle se diagonalise sur $\overline{\mathbb{Q}}_\ell$ selon l'ensemble des caractères $E = \{\chi^\sigma \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)\}$. La représentation $\rho_\chi \mod \ell$ se diagonalise sur $\overline{\mathbb{F}}_\ell$ selon $\overline{E} = \{\chi^\sigma \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)\}$. Dire que $\rho_\chi \mod \ell$ reste irréductible sur $\mathbb{F}_\ell$ correspond donc à dire que $\overline{E}$ ne se décompose pas en plusieurs orbites sous l'action de $\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$. Comme $E$ forme une unique orbite on en déduit qu'il en est de même pour $\overline{E}$ pour tout $\ell$ suffisamment grand. Ceci va nous permettre de déterminer la forme de $H_{\rho_\chi}$.

Commençons par le cas des $\ell < \ell_1$ et fixons $\chi$. Le lemme 7.8 appliqué avec $G = G_\ell$, $X = V_\chi$ de dimension $t_\chi$, $R = T_\chi$ et $\sigma = \rho_\chi : G_\ell \to \mathrm{GL}(V_\chi)$ donne le résultat annoncé (en prenant un point $x \in H_{\rho_\chi}$ d'ordre maximal $\ell^{n_\chi}$).
Passons au cas $\ell \geqslant \ell_1$. En réduisant modulo $\ell H'$ on voit, par irréductibilité et cardinalité, que si $H_{\rho_\chi}$ n'est pas le groupe trivial $\{0\}$, alors sa réduction modulo $\ell$, que nous noterons ici plus simplement $H_1$, est isomorphe à $\prod_{i=1}^{t_\chi} \mathbb{Z}/\ell\mathbb{Z}$. Il reste à voir ce qu'il advient quand on passe de $H_1$ à $H_{\rho_\chi}$. Le groupe $H_{\rho_\chi}$ contient un élément d'ordre $\ell^{n_\chi}$. De plus $[\ell^{n_\chi - 1}]H_{\rho_\chi}$ est contenu dans $H_1$ et est stable par $\rho_{|\ell}$, donc par irréductibilité on voit que $[\ell^{n_\chi-1}] : H_{\rho_\chi} \to H_1$ est surjective. Ceci implique que $H_{\rho_\chi}$ est de la forme attendue $\prod_{i=1}^{t_\chi} \mathbb{Z}/\ell^{n_\chi}\mathbb{Z}$. □

NOTATIONS. – Rappelons que dans la suite on note $n_\chi$ l'entier tel que $\ell^{n_\chi}$ soit l'exposant de $H_{\rho_\chi}$. Par ailleurs, si $\ell < \ell_1$ et $n_\chi \geqslant n_1$, on notera $n_\chi^{\min} = \min n_\chi - r_i$ et pour unifier les notations on notera éventuellement $n_\chi^{\min} := n_\chi$ lorsque $\ell \geqslant \ell_1$.

Nous voulons dans la suite montrer une inégalité du type

$$|H| \ll \big[K(H) : K\big]^{\alpha(A)}.$$

Comme $|H| \gg\ll |H'|$ et comme $[K(H') : K] \leqslant [K(H) : K]$, on voit qu'il suffit de prouver la même assertion avec $H'$ plutôt que $H$. Précisément nous allons obtenir une majoration du cardinal de $\bigoplus H_{\rho_\chi}$ en fonction de $[K(\bigoplus H_{\rho_\chi}) : K] \leqslant [K(H') : K] \leqslant [K(H) : K]$. Ceci se traduira donc en la même borne, à constante multiplicative près, pour le cardinal de $H$.

### 7.2. Intermède : cas décomposé

Nous donnons ici la preuve pour les premiers $\ell$ tels que les caractères $\chi \in I$ soient définis sur $\mathbb{Q}_\ell$, i.e. tels que le tore $\mathcal{T}$ soit scindé sur $\mathbb{Q}_\ell$. Nous supposerons également $\ell \geqslant \ell_1$ où $\ell_1$ est la valeur introduite dans la proposition 7.4 précédente. Bien qu'inutile du strict point de vue logique la preuve dans cette situation particulière permet d'illustrer le raisonnement dans un cadre plus simple, notamment du point de vue des notations. Considérons donc un tel $\ell$. La représentation $\rho$ se décompose sur $\mathbb{Q}_\ell$ en $2g$ sous-représentations irréductibles de dimension 1 données par les caractères $\chi \in I$. Autrement dit on a $\rho_\chi = \chi$. Notamment *nous noterons* (*dans cette section uniquement*) $H_\chi$ *le groupe noté* $H_{\rho_\chi}$ *précédemment*. On a l'isomorphisme de groupes donné par la proposition 7.4

$$H_\chi \simeq \mathbb{Z}/\ell^{n_\chi}\mathbb{Z}.$$

DÉFINITION 7.9. – Nous dirons que le caractère $\chi \in I$ *intervient dans* $H$ si le sous-groupe $H_\chi$ de $H$ correspondant à $\chi$ est non trivial, i.e. si $n_\chi \neq 0$.

On pose $W_H = \mathrm{Vect}_{\mathbb{Q}}(\chi_1, \ldots, \chi_s)$ l'espace vectoriel engendré par tous les caractères intervenant dans $H$. À chaque tel caractère $\chi$ est associé l'entier $n_\chi \geqslant 1$. On note

$$n^{(1)} = \sup_{\chi \in I} n_\chi, \qquad W_1 = \mathrm{Vect}_{\mathbb{Q}}\big(\chi^{(1)}\big),$$

où $\chi^{(1)}$ est un caractère intervenant dans $H$ associé à $n^{(1)}$. De plus on note

$$I_1 = I \cap W_1, \qquad b_1 = \mathrm{Card}(I_1), \qquad H_1 = \bigoplus_{\chi \in I_1} H_\chi.$$

On définit alors par récurrence (jusqu'à un rang $r$ tel que $W_r = W_H$) pour tout entier $i \geqslant 2$

$$n^{(i)} = \sup_{\chi \in I \backslash I_{i-1}} n_\chi, \qquad W_i = \mathrm{Vect}_{\mathbb{Q}}\big(W_{i-1}, \chi^{(i)}\big), \qquad I_i = I \cap W_i,$$

où $\chi^{(i)}$ est un caractère appartenant à $I \backslash I_{i-1}$, associé à l'entier $n^{(i)}$. Par ailleurs, on note

$$\forall i \geqslant 2, \quad b_i = \mathrm{Card}\, I_i - \mathrm{Card}\, I_{i-1}, \quad H_i = \bigoplus_{\chi \in I_i} H_\chi.$$

On note $r$ le plus petit entier $i$ tel que $W_i = W_H$.

Par construction, les $W_i$ sont de dimension $i$ et la famille $\{\chi^{(1)}, \ldots, \chi^{(r)}\}$ est une base de $W_H$. De plus, pour tout $i$ compris entre 1 et $r$, le cardinal de $H_i$ est majoré par $\ell^{\sum_{k=1}^{i} b_k n^{(k)}}$. Notamment, par la proposition 7.4, on a

$$|H| \ll \ell^{\sum_{k=1}^{r} b_k n^{(k)}}. \tag{8}$$

Enfin pour tout $1 \leqslant i \leqslant r$, $\sum_{k=1}^{i} b_k$ est le nombre de caractères de $I$ appartenant à $W_i$. Il nous reste à estimer le degré de l'extension $K(H)/K$. Précisément nous voulons montrer que

$$\ell^{\sum_{i=1}^{r} n^{(i)}} \ll \big[K(H) : K\big]. \tag{9}$$

Admettons pour l'instant cette inégalité (9) et expliquons comment conclure dans ce cas. Les inégalités (8) et (9) impliquent :

$$|H| \ll \big[K(H) : K\big]^{\frac{\sum_{i=1}^{r} n^{(i)} b_i}{\sum_{i=1}^{r} n^{(i)}}}. \tag{10}$$

On utilise alors le lemme suivant :

LEMME 7.10. – *Soient $n_1 \geqslant \cdots \geqslant n_r$, $b_1, \ldots, b_r$ et $w_1, \ldots, w_r$ des entiers strictement positifs. On a*

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

*Démonstration.* – On pose $n_{r+1} = 0$ et on applique une transformation d'Abel à la somme $\sum n_i b_i$ :

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

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

On constate donc finalement que l'exposant maximal obtenu dans l'inégalité (10) est atteint quand les $n^{(i)}$ valent tous 0 ou 1, i.e. quand $H$ est en fait un sous-groupe de $A[\ell]$. De plus dans ce cas, un majorant de l'exposant maximal est

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

Ainsi, cet exposant est inférieur au nombre $\alpha(A)$ précédemment défini, ce qui conclut.

Il nous reste maintenant à prouver l'inégalité (9). On reprend pour cela ce qui avait été fait dans la section 5. Considérons pour cela la tour d'extensions

$$K \to \cdots \to K(H_1) \to \cdots \to K(H_r) \to K\big(A[\ell^\infty]\big).$$

Pour tout entier $i$ entre 1 et $r$, notons $\mathcal{G}_i := \{\sigma \in G_\ell \mid \sigma_{|H_i} = \mathrm{Id}\}$ le groupe de Galois correspondant à l'extension $K(H_i)$. On a

$$\begin{aligned}
\mathcal{G}_i &= \{\sigma \in G_\ell \mid \forall \chi \in I_i \ \forall P_\chi \in H_\chi \ \sigma P_\chi = P_\chi\} \\
&= \big\{\sigma \in G_\ell \mid \forall \chi \in I_i \ \chi(\sigma) = 1 \bmod \ell^{n_\chi}\big\} \\
&\subset \big\{\sigma \in G_\ell \mid \forall k \leqslant i \ \chi^{(k)}(\sigma) = 1 \bmod \ell^{n^{(k)}}\big\} \\
&= \big\{t \in \mathcal{T}(\mathbb{Z}_\ell) \mid \forall k \leqslant i \ \chi^{(k)}(t) = 1 \bmod \ell^{n^{(k)}}\big\} \cap G_\ell.
\end{aligned}$$

On pose $G_i := \{t \in \mathcal{T}(\mathbb{Z}_\ell) \mid \forall k \leqslant i \ \chi^{(k)}(t) = 1 \bmod \ell^{n^{(k)}}\}$ de sorte que $\mathcal{G}_i \subset G_i \cap G_\ell$. Ainsi

$$\big[K(H_i) : K\big] = \left|\frac{G_\ell}{\mathcal{G}_i}\right| \geqslant \left|\frac{G_\ell}{G_i \cap G_\ell}\right| \gg\ll \left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_i}\right|.$$

Comme précédemment nous allons maintenant interpréter ce dernier terme comme le cardinal des points d'un certain tore. On va montrer par récurrence sur $i \leqslant r$ que

$$\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_i}\right| \gg \ell^{\sum_{k=1}^{i} n^{(k)}}, \tag{11}$$

le cas $i = r$ étant la conclusion attendue. Commençons par le cas $i = 1$ : pour cela on pose $T^{(1)} = \ker \chi^{(1)}$ et $T_1 = \mathcal{T}/T^{(1)}$ . Le groupe des caractères de $T_1$ est engendré par $\chi_1$ et on a

$$\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_1}\right| \gg\ll \left|\frac{T_1(\mathbb{Z}_\ell)}{\{t \in T_1(\mathbb{Z}_\ell) \mid \chi^{(1)}(t) = 1 \bmod \ell^{n^{(1)}}\}}\right|$$
$$\gg\ll \ell^{n^{(1)}} \quad \text{par le théorème 2.11 de Ribet.}$$

Ceci prouve (11) quand $i = 1$.

Supposons maintenant l'inégalité vraie au rang $i$ et montrons-la au rang $i+1 \leqslant r$. On a

$$\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_{i+1}}\right| = \left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_i}\right| \times \left|\frac{G_i}{G_{i+1}}\right|.$$

En appliquant l'hypothèse de récurrence il suffit donc de montrer que $|\frac{G_i}{G_{i+1}}| \gg \ell^{n^{(i+1)}}$. On introduit pour cela

$$\forall i \geqslant 1 \quad T^{(i+1)} = \ker \chi^{(i+1)}{}_{|T^{(i)}} \quad \text{et} \quad T^{(i)} \sim T^{(i+1)} \times T_{i+1}$$

où là encore le groupe des caractères de $T_{i+1}$ est engendré par $\chi^{(i+1)}$. Comme on l'avait noté précédemment ces groupes algébriques sont définis sur $\mathbb{Q}_\ell$ par construction, mais étant définis par des caractères $\chi \in I$, ils sont également définis sur une extension finie de $\mathbb{Q}$. Autrement dit, ils sont définis sur une extension finie $\mathbb{K}$ de $\mathbb{Q}$, contenue dans $\mathbb{Q}_\ell$. Donc les différentes isogénies sont des isogénies sur $\mathbb{K}$. De plus cette extension $\mathbb{K}/\mathbb{Q}$ est une sous-extension de $\mathbb{Q}(I)$, corps de définition des $\chi \in I$. Il n'y a donc qu'un nombre fini de telles extensions $\mathbb{K}$ lorsque $\ell$ varie (parmi les premiers totalement décomposés).

Par construction de $T^{(i)}$, on a

$$\frac{T^{(i)}(\mathbb{Z}_\ell)}{T^{(i)}(\mathbb{Z}_\ell) \cap G_{i+1}} \hookrightarrow \frac{G_i}{G_{i+1}}.$$

On en déduit

$$\left|\frac{G_i}{G_{i+1}}\right| \geqslant \left|\frac{T^{(i)}(\mathbb{Z}_\ell)}{T^{(i)}(\mathbb{Z}_\ell) \cap G_{i+1}}\right| \gg \left|\frac{T_{i+1}(\mathbb{Z}_\ell)}{\{t \in T_{i+1}(\mathbb{Z}_\ell) \mid \chi^{(i+1)}(t) = 1 \bmod l^{n^{(i+1)}}\}}\right| \gg\ll \ell^{n^{(i+1)}}.$$

Ceci conclut la preuve dans le cas décomposé. Il nous reste maintenant à traiter le cas général : la preuve est exactement la même à ceci près que nous devons regrouper les caractères $\chi$ par paquets avec les $\chi^\sigma$, $\sigma$ décrivant les plongements de $\mathbb{Q}_\ell(\chi)$ dans $\overline{\mathbb{Q}_\ell}$. De même les tores à considérer seront cette fois définis par $\bigcap_\sigma \ker \chi^\sigma$ au lieu de $\ker \chi$. Nous aurons notamment besoin d'utiliser le lemme 7.10 avec des $w_i$ non nécessairement tous égaux à 1.

### 7.3. Cas général

#### 7.3.1. Les objets combinatoires

Les caractères $\chi_1, \ldots, \chi_{2g}$ sont définis sur $\overline{\mathbb{Q}}$ donc sur une extension $L/\mathbb{Q}$ finie.

DÉFINITION 7.11. – On dit que le caractère $\chi \in I$ *intervient dans* $H$ si :
1. soit $\ell \geqslant \ell_1$ et le sous-groupe $H_{\rho_\chi}$ de $H$ correspondant à la représentation $\rho_\chi$ est non trivial ;
2. soit $\ell < \ell_1$ et le sous-groupe $H_{\rho_\chi}$ de $H$ correspondant à la représentation $\rho_\chi$ est d'exposant $\ell^{n_\chi} \geqslant \ell^{n_1}$.

On pose $W_H = \mathrm{Vect}_{\mathbb{Q}}(\chi_1, \ldots, \chi_s)$ l'espace vectoriel engendré par tous les caractères intervenant dans $H$. Ici et dans la suite on suppose $H$ de cardinal suffisamment grand de sorte que $W_H \neq \{0\}$ (si $H$ est petit il n'y a rien à montrer). À chaque caractère $\chi$ intervenant dans $H$ est associé l'entier $n_\chi$. Comme au paragraphe 7.2 précédent, mais cette fois en regroupant les caractères conjugués, on note

$$n^{(1)} = \sup_{\chi \in I} n_\chi, \qquad W_1 = \mathrm{Vect}_{\mathbb{Q}}\big(\big(\chi^{(1)}\big)^{\sigma_1(1)}, \ldots, \big(\chi^{(1)}\big)^{\sigma_{t_1}(1)}\big),$$

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

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

où la somme porte sur les $\chi \in I_1$ modulo l'action de Galois. On extrait de l'ensemble $I_1$ une base $\{(\chi^{(1)})^{\sigma_1(1)},\dots,(\chi^{(1)})^{\sigma_{w_1}(1)}\}$ de $W_1$.

*Remarque* 7.12. – Notons que si $\chi \in I_1$, alors pour tout plongement $\sigma$, 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'au rang $r$ tel que $W_r = W_H$) pour tout entier $i \geqslant 2$

$$n^{(i)} = \sup_{\chi\in I\setminus I_{i-1}} n_\chi, \qquad W_i = \mathrm{Vect}_{\mathbb{Q}}\big(W_{i-1}, \big(\chi^{(i)}\big)^{\sigma_1(i)},\dots,\big(\chi^{(i)}\big)^{\sigma_{t_i}(i)}\big), \qquad I_i = I \cap W_i,$$

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

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

où la somme porte sur les $\chi \in I_i$ modulo l'action de Galois. 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 plus petit entier $i$ tel que $W_i = W_H$.
Finalement quitte à réordonner les termes, et pour soulager les notations, on suppose que

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

LEMME 7.13. – *La famille* $\{\chi_1,\dots,(\chi_1)^{\sigma_{w_1}(1)},\dots,\chi_r,\dots,(\chi_r)^{\sigma_{w_r}(r)}\}$ *est une base de* $W_H$. *De plus, pour tout* $i$ *compris entre* $1$ *et* $r$, *le cardinal de* $H_i$ *est majoré par* $\ell^{\sum_{k=1}^{i} b_k n_k}$ *et* $\sum_{k=1}^{i} b_k$ *est le nombre de caractères* (*éléments de* $I$) *appartenant à* $W_i$.

*Démonstration.* – Ceci découle de la construction des différents objets et de la proposition 7.4. □

### 7.3.2. Degré du corps de rationalité

Nous voulons maintenant minorer le degré de l'extension $K(H)/K$. Précisément nous voulons prouver l'inégalité suivante :

$$\ell^{\sum_{i=1}^{r} w_i n_i} \ll \big[K(H) : K\big]. \tag{12}$$

La conclusion suit alors exactement comme au paragraphe 7.2 de cette inégalité et du lemme 7.13 précédent. En effet, admettons pour l'instant l'inégalité (12). On a donc

$$\mathrm{Card}\, H \ll \ell^{\sum_{i=1}^{r} n_i b_i} \ll \big[K(H) : K\big]^{\frac{\sum_{i=1}^{r} n_i b_i}{\sum_{i=1}^{r} n_i w_i}}. \tag{13}$$

On utilise alors le lemme 7.10 comme on l'avait fait dans le cas décomposé, la seule différence étant que les $w_i$ ne sont plus nécessairement tous égaux à 1. On constate finalement que

l'exposant maximal obtenu dans l'inégalité (13) est atteint quand les $n_i$ valent tous 0 ou 1, i.e. quand $H$ est en fait un sous-groupe de $A[\ell]$. De plus dans ce cas, un majorant de l'exposant maximal est

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

Ainsi, cet exposant est inférieur au nombre $\alpha(A)$ précédemment défini, ce qui nous permet de conclure la partie $\ell$-adique et donc la preuve de l'inégalité $\gamma(A)\leqslant\alpha(A)$ du théorème 1.10.

Il nous reste finalement à prouver l'inégalité (12). Considérons pour cela la tour d'extensions

$$K\to\cdots\to K(H_1)\to\cdots\to K(H_r)\to K\big(A[\ell^\infty]\big).$$

Pour tout entier $i$ entre 1 et $r$, notons $\mathcal{G}_i:=\{\sigma\in G_\ell \mid \sigma_{|H_i}=\mathrm{Id}\}$ le groupe de Galois correspondant à l'extension $K(H_i)$.

LEMME 7.14. – *On a l'inclusion*

$$\mathcal{G}_i\subset G_\ell\cap\bigcap_{k=1}^{i}\big\{t\in\mathcal{T}(\mathbb{Z}_\ell)\mid\forall j\in[\![1,t_k]\!]\chi_k^{\sigma_j(k)}(t)=1 \bmod \ell^{n_k^{\min}}\big\}=:G_\ell\cap G_i.$$

*Démonstration.* – En utilisant les notations du paragraphe précédent, on a

$$\begin{aligned}\mathcal{G}_i&=\big\{t\in G_\ell\mid\forall\chi\in I_i,\ \forall P\in H_{\rho_\chi},\ \rho_\chi(t)P=P\big\}\\&\subset\big\{t\in G_\ell\mid\forall 1\leqslant k\leqslant i,\ \forall P_k\in H_{\rho_{\chi_k}},\ \rho_{\chi_k}(t)P_k=P_k\big\}\\&\subset\big\{t\in G_\ell\mid\forall 1\leqslant k\leqslant i,\ \rho_{\chi_k}(t)=1 \bmod \ell^{n_k^{\min}}\big\}\\&=G_\ell\cap\bigcap_{k=1}^{i}\big\{t\in\mathcal{T}(\mathbb{Z}_\ell)\mid\forall j\in[\![1,t_k]\!],\ \chi_k^{\sigma_j(k)}(t)=1 \bmod \ell^{n_k^{\min}}\big\}.\end{aligned}$$

La dernière égalité découle du fait que, par construction, la représentation $\rho_{\chi_k}$ est équivalente à

$$\begin{pmatrix}\chi_k & & \\ & \ddots & \\ & & \chi_k^{\sigma_{t_k}(k)}\end{pmatrix}$$

sur $\overline{\mathbb{Q}}_\ell$. Ceci conclut. □

Ainsi

$$\big[K(H_i):K\big]=\left|\frac{G_\ell}{\mathcal{G}_i}\right|\geqslant\left|\frac{G_\ell}{G_i\cap G_\ell}\right|\gg\ll\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_i}\right|.$$

Comme précédemment nous allons maintenant interpréter ce dernier terme comme le cardinal des points d'un certain tore. Précisément nous allons montrer par récurrence que

$$\forall 1\leqslant i\leqslant r,\quad\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_i}\right|\gg\ell^{\sum_{k=1}^{i}n_k^{\min}w_k}. \tag{14}$$

L'inégalité (12) en découle alors avec $i=r$ (en fait il reste encore à voir que l'on peut remplacer les entiers $n_i^{\min}$ par les $n_i$ ; mais ceci est immédiat, car on sait qu'il existe deux constantes

absolues $\ell_1$, $n_1$ telles que pour tout $\ell \geqslant \ell_1$, $n_i^{\min} = n_i$, et que, pour les $\ell < \ell_1$ en nombre fini restants, on ait $n_i^{\min} \geqslant n_i - n_1$).
Pour montrer l'inégalité (14) considérons pour tout entier $i$ compris entre 1 et $r$,

$$T^{(0)} := \mathcal{T}, \quad \text{et} \quad \forall i \geqslant 0\ T^{(i+1)} = \bigcap_{k=1}^{t_{i+1}} \ker\bigl(\chi_{i+1}^{\sigma_k(i+1)}\bigr)_{|T^{(i)}} \text{ et } T^{(i)} \sim T^{(i+1)} \times T_{i+1}.$$

où pour $i \geqslant 1$ le groupe des caractères de $T_i$ est $X_i = (T^{(i)})^{\perp} = \{\chi \in X^*(T^{(i-1)}) \mid T^{(i)} \subset \ker \chi\}$.

Ces tores sont définis sur $\mathbb{Q}_\ell$ par construction, mais étant définis par les caractères $\chi_i$, ils sont également définis sur une extension finie de $\mathbb{Q}$. Autrement dit, ces tores sont définis sur une extension finie $\mathbb{K}$ de $\mathbb{Q}$, contenue dans $\mathbb{Q}_\ell$. De plus cette extension est une sous-extension de $L$, corps de définition des $\chi \in I$. Il n'y a donc qu'un nombre fini de telles extensions $\mathbb{K}$ lorsque $\ell$ varie.

LEMME 7.15. – *Pour tout $i$ compris entre 1 et $r$ le tore $T_i$ est de dimension $w_i$.*

*Démonstration.* – Le groupe des caractères de $T_i$ est $X_i$ et par construction, $X_i \otimes \mathbb{Q}$ 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 $\dim W_i - \dim W_{i-1} = w_i$. □

Nous pouvons maintenant prouver l'inégalité (14) par récurrence sur $i \leqslant r$. Vérifions tout d'abord la propriété au rang $i = 1$ : par construction de $T_1$ et comme dans le cas décomposé, on a

$$\left|\frac{\mathcal{T}(\mathbb{Z}_\ell)}{G_1}\right| \gg\ll \left|\frac{T_1(\mathbb{Z}_\ell)}{T_1(1+\ell^{n_1^{\min}}\mathbb{Z}_\ell)}\right|.$$

Le théorème 2.11 permet de conclure :

$$\ell^{w_1 n_1^{\min}} \ll \bigl|T_1\bigl(\mathbb{Z}/\ell^{n_1^{\min}}\mathbb{Z}\bigr)\bigr|.$$

Le passage du rang $i$ au rang $i+1$ est exactement le même que dans le cas décomposé traité au paragraphe 7.2. Notons que les différentes constantes intervenant dans les inégalités $\gg$ dépendent du corps $\mathbb{K}$, mais on a vu que lorsque $\ell$ varie, seul un nombre fini de tels $\mathbb{K}$ interviennent, donc on peut bien choisir dans les $\gg$ des constantes multiplicatives indépendantes de $\ell$.

## 8. Les cas particuliers

Nous allons traiter deux types de cas particuliers : certains cas particuliers de variétés abéliennes de type CM 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 CM

On rappelle en suivant Kubota [6], qu'une variété abélienne de type CM est de type non dégénéré si $d = g + 1$, avec $g = \dim A$ et $d = \dim \mathcal{T}$ où $\mathcal{T}$ est le groupe de Mumford–Tate de $A$.

DÉFINITION 8.1. – Avec les notations précédentes en suivant Kubota [6], on dit qu'une variété abélienne de type CM est de *défaut* $\delta$ si

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

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

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

Ceci découle par exemple de [5] I Example 3.7 point (d) p. 47. De fait Deligne donne l'énoncé dual pour le groupe des cocaractères, mais la traduction est immédiate. Il faut également faire attention au fait que sa définition du groupe de Mumford–Tate est très légèrement différente de la nôtre, ce qui fait apparaître un cocaractère $e_0$ qui n'a pas lieu d'être avec nos conventions.

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 $X^*(\mathcal{T}) \otimes \mathbb{Q}$, on introduit deux notations

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

LEMME 8.2. – *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 $\dim W \geqslant m(W)$, donc dans ce cas on a même $\frac{n(W)}{\dim W} \leqslant 1 \leqslant \frac{2g}{d}$.
2. Sinon $\chi_0 \in W$. Dans ce cas, on voit que $n(W) = 2m(W)$ et $\dim W \geqslant m(W) + 1$. En utilisant la croissance de la fonction $x \mapsto \frac{2x}{x+1}$, on a donc

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

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 8.3. – *Si $A/K$ est de défaut* 1*, alors*

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

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

1. Si $\chi_0 \notin W$ alors $n(W) = m(W)$ et $\dim W \geqslant m(W) - 1$. Le quotient est donc inférieur à 2.

2. Sinon $\chi_0 \in W$. Dans ce cas $n(W) = 2m(W)$ et $\dim W \geqslant m(W)$. Là encore, le quotient est inférieur à 2, ce qui conclut. □

Nous pouvons maintenant passer à la preuve de la proposition 1.18 : notons tout d'abord qu'il suffit en fait de montrer la majoration de $\alpha(A)$. L'égalité découle alors de notre théorème 1.10 et de l'inégalité (1). Ceci étant, si la dimension $g$ est un nombre premier ou 1, alors le type est non dégénéré et donc le lemme 8.2 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 1.17 que la 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 8.2 et 8.3 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 $X^*(\mathcal{T}) \otimes \mathbb{Q}$. En prenant pour $W$ l'espace tout entier on constate que $\alpha(A) \geqslant \frac{2g}{d} \geqslant 2$. Par ailleurs, si $W$ est un sous-espace strict de $X^*(\mathcal{T}) \otimes \mathbb{Q}$, sa dimension est inférieure à 4. Le corollaire 4.3 du paragraphe 4 nous indique que $n(W) \leqslant 2^{4-1} = 8$. Ainsi on a $\frac{n(W)}{\dim W} \leqslant \frac{8}{4} = 2 \leqslant \frac{2g}{d}$. Ceci prouve bien que $\alpha(A) = \frac{2g}{d}$ et achève la preuve de la proposition 1.18. □

### 8.2. Cas d'une courbe elliptique sans multiplication complexe

Soit $E/K$ une courbe elliptique sans multiplication complexe. Comme précédemment, on peut, en utilisant l'indépendance algébrique des représentations $\ell$-adiques $\rho_\ell$ (cf. [27] théorème 3), se ramener au cas $\ell$-adique : on se donne un groupe fini $H$ inclus dans $E[\ell^\infty]$ pour un certain premier $\ell$. La courbe $E/K$ étant sans multiplication complexe, on sait par un résultat de Serre (théorème 3 et son corollaire 1 de [27] pp. 299–300) que pour presque tout premier $\ell$, on a

$$G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell).$$

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

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

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

$$G_H = \{\sigma \in G_\ell \mid \sigma_H = \mathrm{Id}_H\}.$$

On se donne une base de $T_\ell(E)$, $\{\hat{P}_1, \hat{P}_2\}$ telle que $P_i = \hat{P}_i \mod \ell^{n_i}$ pour $i \in \{1, 2\}$. On a ainsi l'identification

$$G_H = \left\{\sigma \in \mathrm{GL}_2(\mathbb{Z}_\ell) \mid \forall i \in \{1,2\}\ \sigma\hat{P}_i = \hat{P}_i \mod \ell^{n_i}\right\}.$$

On peut encore réécrire ceci sous la forme

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

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

$$C_1 \leqslant \frac{[G_\ell : G_H]}{\ell^{2(n_1+n_2)}} \leqslant C_2.$$

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

**Remerciements**

Je tiens ici à exprimer ma sincère gratitude envers Jean-Pierre Serre. La preuve du théorème 1.10 est en effet basée sur une stratégie qu'il a eu la gentillesse de m'expliquer. Je tiens également à remercier le rapporteur pour son travail qui a permis d'améliorer considérablement la rédaction de cet article. Enfin je tiens à remercier Marc Hindry pour l'aide précieuse qu'il m'a apportée : sans lui cet article n'aurait sans doute pas été achevé.

## RÉFÉRENCES

[1] BOMBIERI E., MASSER D., ZANNIER U., Intersecting a curve with algebraic subgroups of multiplicative groups, *Internat. Math. Res. Not.* **20** (1999) 1119–1140.
[2] BOMBIERI E., MASSER D., ZANNIER U., Intersecting curves and algebraic subgroups: conjectures and more results, *Trans. Amer. Math. Soc.* **358** (2006) 2247–2257.
[3] BOROVOĬ M.V., The action of the Galois group on the rational cohomology classes of type $(p, p)$ of abelian varieties, *Mat. Sb. (N.S.)* **94** (136) (1974) 649–652, 656.
[4] DODSON B., On the Mumford–Tate group of an abelian variety with complex multiplication, *J. Algebra* **111** (1) (1987) 49–73.
[5] DELIGNE P., MILNE J.S., OGUS A., SHIH K.-Y., Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Mathematics, vol. **900**, Springer-Verlag, Berlin, 1982.
[6] KUBOTA T., On the field extension by complex multiplication, *Trans. Amer. Math. Soc.* **118** (1965) 113–122.
[7] MASSER D., Lettre à Daniel Bertrand du 10 novembre 1986.
[8] MASSER D., Small values of the quadratic part of the Néron–Tate height, in: Progr. Math., vol. **12**, Birkhäuser, 1981, pp. 213–222.
[9] MAZUR B., Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44** (2) (1978) 129–162.
[10] MEREL L., Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.* **124** (1–3) (1996) 437–449.
[11] MILNE J.S., Abelian varieties, in: *Arithmetic Geometry*, Storrs, Conn., 1984, Springer, New York, 1984, pp. 103–150.
[12] MOONEN B., ZARHIN Y., Hodges classes on abelian varieties of low dimension, *Math. Ann.* **315** (4) (1999) 711–733.
[13] MUMFORD D., A note of Shimura's paper "Discontinuous groups and abelian varieties", *Math. Ann.* **181** (1969) 345–351.
[14] MURTY V.K., Hodge and Weil classes on abelian varieties, in: *The Arithmetic and Geometry of Algebraic Cycles*, Banff, AB, 1998, in: NATO Sci. Ser. C Math. Phys. Sci., vol. **548**, Kluwer Acad. Publ., Dordrecht, 1998, pp. 83–115.
[15] ONO T., Arithmetic of algebraic tori, *Ann. Math.* **74** (1) (1961) 101–139.
[16] PARENT P., Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, *J. reine angew. Math.* **506** (1999) 85–116.
[17] PINK R., $\ell$-Adic algebraic monodromy groups cocharacters, and the Mumford–Tate conjecture, *J. reine angew. Math.* **495** (1998) 187–237.
[18] PINK R., A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang. Prépublication de 2005 disponible à l'adresse http://www.math.ethz.ch/~pink/ftp/AOMMML.pdf.

[19] PJATECKIĬ-ŠAPIRO I.I., Interrelations between the Tate and Hodge hypotheses for abelian varieties, *Mat. Sb. (N.S.)* **85** (127) (1971) 610–620.
[20] POHLMANN H., Algebraic cycles on abelian varieties of complex multiplication type, *Ann. of Math.* **88** (2) (1968) 161–180.
[21] RAYNAUD M., Courbes sur une variété abélienne et points de torsion, *Invent. Math.* **71** (1983) 207–233.
[22] RATAZZI N., Intersection de courbes et de sous-groupes, et problèmes de minoration de hauteur dans les variétés abéliennes C.M. À paraître aux Annales de l'Institut Fourier.
[23] RÉMOND G., Intersection de sous-groupes et de sous-variétés I, *Math. Ann.* **333** (3) (2005) 525–548.
[24] RÉMOND G., VIADA E., Problème de Mordell–Lang modulo certaines sous-variétés abéliennes, *Int. Math. Res. Not.* **35** (2003) 1915–1931.
[25] RIBET K.A., Division fields of abelian varieties with complex multiplication, *Mém. Soc. Math. France* **2** (1980) 75–94.
[26] RIBET K.A., Hodge classes on certain types of abelian varieties, *Amer. J. Math.* **105** (1983) 523–538.
[27] SERRE J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259–331.
[28] SERRE J.-P., Représentations $\ell$-adiques, in : *Kyoto Int. Symposium on Algebraic Number Theory*, Japan Soc. for the Promotion of Science, 1977, pp. 177–193.
[29] SERRE J.-P., Lettre à Ken Ribet, Œuvres. Collected papers, vol. **IV**, Springer-Verlag, Berlin, 2000, 1985–1998.
[30] SERRE J.-P., Résumé des cours au Collège de France de 1984–1985, Œuvres. Collected papers, vol. **IV**, Springer-Verlag, Berlin, 2000, 1985–1998.
[31] SERRE J.-P., Abelian $\ell$-adic Representations and Elliptic Curves, revised reprint of the 1968 original, Research Notes in Mathematics, vol. **7**, AK Peters Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute.
[32] SERRE J.-P., TATE J., Good reduction of abelian varieties, *Ann. of Math.* **88** (1968) 492–517.
[33] Théorie des topos et cohomologie étale des schémas. Tome 3, Springer-Verlag, Berlin, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), dirigé par M. Artin, A. Grothendieck et J.L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat, Lecture Notes in Mathematics, vol. 305
[34] SHIMURA G., TANIYAMA Y., Complex Multiplication of Abelian Varieties and Its Applications to Number Theory, Publications of the Mathematical Society of Japan, vol. **6**, Mathematical Society of Japan, Tokyo, 1961.
[35] SILVERBERG A., Torsion points on abelian varieties of CM-type, *Compositio Math.* **68** (3) (1988) 241–249.
[36] SILVERMAN, J.H., Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol. **156**, 1999.
[37] TENENBAUM G., Introduction à la théorie analytique et probabiliste des nombres, seconde édition, Cours Spécialisés, vol. **1**, Société Mathématique de France, Paris, 1995.
[38] VIADA E., The intersection of a curve with algebraic subgroups in a product of elliptic curves, *Ann. Scuola Norm. Pisa Cl. Sci. Série (V)* **2** (2003) 47–75.
[39] YANAI H., On the rank of CM-type, *Nagoya Math. J.* **97** (1985) 169–172.
[40] ZILBER B., Exponential sums equations and the Schanuel conjecture, *J. London Math. Soc. (2)* **65** (1) (2002) 27–44.

(Manuscrit reçu le 8 février 2007 ;
accepté, après révision, le 4 octobre 2007.)

Nicolas RATAZZI
Université Paris Sud,
Département de mathématiques,
Bâtiment 425,
91405 Orsay Cedex, France
E-mail : nicolas.ratazzi@math.u-psud.fr