HOMOTHÉTIES EXPLICITES DES REPRÉSENTATIONS ℓ-ADIQUES

par

Aurélien Galateau & César Martínez

Résumé. — Cet article présente et précise les principaux résultats connus sur la taille du sous-groupe des homothéties des représentations ℓ-adiques associées à la torsion d'une variété abélienne. De telles estimations permettent notamment de donner des bornes uniformes explicites dans le cadre du problème de Manin-Mumford.

1. Introduction

La question de la distribution des points de torsion d'une courbe algébrique plongée dans sa jacobienne est posée par Lang en 1965 ([**15**]). Inspiré par des travaux de Manin et par ses discussions avec Mumford, il formule une conjecture qui sera démontrée une vingtaine d'années plus tard.

Théorème 1.1 **(Raynaud).** — *Si C est une courbe algébrique de genre au moins deux, définie sur un corps de nombres et plongée dans sa jacobienne, elle contient un nombre fini de points de torsion.*

À la lumière des travaux d'Ihara, Serre et Tate sur l'analogue torique de ce problème, Lang montre que certaines propriétés galoisiennes des points de torsion pourraient permettre de résoudre la question posée par Manin et Mumford.

Soit A une variété abélienne de dimension $g \geq 1$ définie sur un corps de nombres K dont on fixe une clôture algébrique $\bar{K}$. Si ℓ est dans l'ensemble $\mathcal{P}$ des nombres premiers, l'action du groupe de Galois $G_K := \mathrm{Gal}(\bar{K}/K)$ sur le module de Tate T_ℓ de A (dont on fixe une base sur $\mathbb{Z}_\ell$) définit une représentation :

$$\rho_\ell : G_K \to \mathrm{GL}_{\mathbb{Z}_\ell}(T_\ell) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell),$$

dont l'image sera désormais notée G_ℓ. L'hypothèse faite par Lang est devenue la conjecture suivante, toujours ouverte aujourd'hui.

Conjecture 1.2 **(Lang).** — *Si ℓ est assez grand, le groupe G_ℓ contient le sous-groupe des homothéties $\mathbb{Z}_\ell^\times$ de $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.*

De nombreux résultats sont connus en direction de cette conjecture. Bogomolov a d'abord démontré, en utilisant la théorie de Hodge-Tate, que les représentations ℓ-adiques contiennent les homothéties à un indice fini près (voir [**2**]).

Théorème 1.3 **(Bogomolov).** — *Le groupe G_ℓ contient un sous-groupe ouvert du groupe $\mathbb{Z}_\ell^\times$ des homothéties de $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$.*

Si on considère le « groupe de monodromie » H_ℓ, c'est-à-dire l'enveloppe algébrique de G_ℓ dans GL_{2g} sur $\mathbb{Q}_\ell$, les travaux de Bogomolov montrent en fait que G_ℓ est un sous-groupe ouvert – pour la topologie ℓ-adique – de $H_\ell(\mathbb{Q}_\ell)$. Serre, avec des arguments plus sophistiqués, a ensuite donné une version uniforme du résultat de Bogomolov.

Théorème 1.4 **(Serre).** — *Il existe un entier $c(A) > 0$ tel que :*

$$\forall \ell \in \mathcal{P},\ (\mathbb{Z}_\ell^\times)^{c(A)} \subset G_\ell.$$

Ce résultat, annoncé dans ses cours au Collège de France ([**29**], 136), a ensuite été exposé en détail par Wintenberger ([**33**]).

Le théorème de Serre se révèle être suffisant pour mener à bien la stratégie imaginée par Lang dans le problème de Manin-Mumford. Suivant cette voie, Hindry a généralisé le théorème de Raynaud aux sous-variétés des variétés semi-abéliennes ([**14**]).

En combinant une variante de cette approche développée par Beukers et Smyth ([**1**]) avec de nouveaux arguments d'interpolation, nous avons obtenu dans [**11**] des bornes uniformes permettant de quantifier la torsion dans les sous-variétés des variétés abéliennes. Pour rendre ces estimations totalement explicites, il faudrait pouvoir estimer la « constante de Serre », c'est-à-dire l'exposant apparaissant dans le Théorème 1.4. Nous nous proposons ici de rassembler et de préciser les résultats connus sur cette question.

Plan de l'article. — Nous revisitons d'abord les travaux de Serre et Wintenberger, qui montrent que pour un nombre premier ℓ suffisamment grand, le groupe G_ℓ contient un sous-groupe « assez grand » du groupe dérivé $H_\ell(\mathbb{Q}_\ell)'$. Il est alors possible de borner simplement l'exposant du groupe d'homothéties en fonction de g. Toute la difficulté ici est d'estimer la taille des nombres premiers pour lesquels ce phénomène a lieu, et ceci a été partiellement réalisé par Zywina ([**35**]).

Nous reprenons ensuite des résultats classiques de cohomologie galoisienne sur les corps locaux démontrés par Tate dans [**32**], que nous précisons en estimant les sauts de ramification d'une extension procyclique. La détermination de certains groupes de cohomologie permet d'exploiter la décomposition de Hodge-Tate des représentations abéliennes ℓ-adiques pour montrer leur algébricité locale.

Le cas des grands premiers étant essentiellement compris, il suffit alors de donner une version explicite du théorème de Bogomolov. Ce problème se décompose en deux parties. La première consiste à contrôler l'écart entre G_ℓ et $H_\ell(\mathbb{Q}_\ell)'$, ce qui semble actuellement hors d'atteinte. La seconde revient à estimer la taille des homothéties dans une représentation abélienne qui a la propriété d'être de Hodge-Tate. Nous le faisons ici en reprenant l'exposé donné par Serre dans [**27**], III A.

Nous revenons enfin sur le problème de Manin-Mumford et nous explicitons les résultats uniformes déjà connus dans deux cas particuliers importants : les puissances de courbes elliptiques et les variétés abéliennes CM. De telles bornes, lorsqu'elles sont calculables, permettent de déterminer effectivement le lieu de torsion recherché.

Nous tenons à remercier la Deutsche Forschungsgemeinschaft et le programme SFB 1085 : *Higher Invariants – Interactions between Arithmetic Geometry and Global Analysis* pour leur soutien pendant la conception et la rédaction de cet article.

2. Constante de Serre pour les grands premiers

Serre a d'abord exposé la preuve du Théorème 4 dans son cours au Collège de France de 1985-1986. Les grandes lignes de la démonstration apparaissent dans sa correspondance de l'époque (en particulier la lettre à Bertrand [**29**], 134). Elles ont été reprises par Wintenberger dans [**33**], où il est aussi prouvé que la conjecture de Mumford-Tate entraîne la conjecture de Lang.

2.1. Extension des scalaires. — Un certain nombre de simplifications apparaissent à condition de se placer sur une extension finie de K, dont le degré peut être borné explicitement en fonction de g. C'est ce qu'on fera dans la suite de cet article.

On commencera par choisir K assez grand pour que A ait réduction semi-stable en tout idéal premier de l'anneau des entiers $\mathcal{O}_K$. Il suffit pour cela de remplacer K par $K(A[12])$, qui est une extension de K de degré $\leq 12^{4g^2}$ ([**13**], Exposé IX, Proposition 4.7). On peut ensuite se demander si les représentations ρ_ℓ sont indépendantes dans le sens suivant.

Définition 2.1. — *Les $(\rho_\ell)_{\ell\in\mathcal{P}}$ sont indépendantes si le morphisme produit :*

$$\rho := (\rho_\ell)_{\ell\in\mathcal{P}} : G_K \longrightarrow \prod_\ell G_\ell$$

est surjectif.

Dans ce cas, on a : $\rho(G_K) = \prod_\ell G_\ell$ et il est possible de recoller les résultats obtenus sur chaque représentation ℓ-adique.

Proposition 2.2. — *Les ρ_ℓ sont indépendantes.*

Démonstration. — Voir [**30**], Théorème 1. Une version moins précise de ce résultat figure dans la Lettre de Serre à Ribet, [**29**], 138. □

Une autre propriété intéressante apparaît avec l'extension qu'on a fixée : les groupes de monodromie sont simultanément connexes.

Lemme 2.3. — *Pour tout $\ell \in \mathcal{P}$, H_ℓ est connexe.*

Démonstration. — Voir la lettre de Serre à Ribet [**29**], 133. Le plus petit corps de définition rendant connexes tous les H_ℓ est inclus dans $K(A[\ell^\infty])$, pour tout premier ℓ. Son degré est borné par :

$$\prod_{k=1}^{2g}(2^k-1)(3^k-1) \leq 36^{g^2},$$

et on voit que l'extension choisie pour assurer la semi-stabilité partout convient également ici. □

2.2. Groupes dérivés. — On considère maintenant l'enveloppe algébrique $\mathcal{H}_\ell$ de G_ℓ dans le groupe algébrique GL_{2g} sur $\mathbb{Z}_\ell$, dont la fibre générique est H_ℓ. Son groupe dérivé au sens des schémas en groupes réductifs ([**9**], Exposé XXII, 6.2) sera noté $\mathcal{S}_\ell$. Le principal résultat en direction du Théorème 1.4 est le suivant ([**33**], Théorème 2).

Théorème 2.4 **(Wintenberger).** — *Il existe un entier ℓ_0 tel que pour tout premier $\ell \geq \ell_0$:*

$$\mathcal{S}_\ell(\mathbb{Z}_\ell)' \subset G_\ell.$$

Ce résultat repose en grande partie sur une étude de la représentation modulo ℓ donnée par l'action de G_K sur la ℓ-torsion. Dans sa lettre à Bertrand ([**29**], 134), Serre explique qu'on pourrait trouver une borne effective à condition d'obtenir une version précise d'un théorème de Faltings affirmant la semi-simplicité de cette représentation. Wintenberger ([**33**], Remarque 2.2) fait un inventaire des obstacles à l'effectivité.

Dans un travail récent, Zywina utilise la version donnée par Masser et Wüstholz du théorème de Faltings pour estimer partiellement l'entier ℓ_0. Par des travaux de Serre, le rang r de H_ℓ est indépendant de ℓ et il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ tel que le tore de Frobénius $T_\mathfrak{p}$, c'est-à-dire le groupe multiplicatif engendré par les racines du polynôme caractéristique du Frobénius en $\mathfrak{p}$, soit de rang r ([**29**], 133 ou [**35**], 2.5). On fixe un tel idéal $\mathfrak{p}$ de norme minimale, et on note $h_F(A)$ la hauteur de Faltings de A.

Théorème 2.5 **(Zywina).** — *Il existe des réels positifs α et β dépendant de g tels qu'on puisse choisir :*

$$\ell_0 = \alpha \cdot \max\{[K:\mathbb{Q}], h_F(A), N(\mathfrak{p})\}^\beta.$$

Remarque. Zywina montre qu'il est possible de faire disparaître la dépendance en l'idéal $\mathfrak{p}$ si on admet l'Hypothèse de Riemann généralisée. En utilisant le théorème de Minkowksi et la comparaison entre régulateur et hauteur de Faltings ([**23**], Theorem 1.1), la borne devient alors :

$$\ell_0 = \alpha \cdot \max\{\log \Delta_K, h_F(A)\}^\beta,$$

où Δ_K est le discriminant absolu du corps K ([**35**], Theorem 1.4).

2.3. Version effective du théorème de Faltings. — Il est possible d'aller un peu plus loin en utilisant les travaux de Gaudron et Rémond sur les degrés d'isogénies. On introduit la notation suivante :

$$\kappa(A) := \left((14g)^{64g^2}[K:\mathbb{Q}]\max\left\{1, h_F(A), \log[K:\mathbb{Q}]\right\}^2\right)^{2^{10}g^3},$$

qui apparaît de façon répétée dans [**12**].

Proposition 2.6. — *Si $\ell \geq \kappa(A)^3$, le groupe $G(\ell)$ est semi-simple de commutant $\mathbb{F}_\ell \otimes \mathrm{End}(A)$.*

Démonstration. — Si B est une variété abélienne définie sur K, on note $d(B)$ la valeur absolue du discriminant de $\mathrm{End}_K(B)$ et $b(B)$ le plus petit entier b tel que pour toute variété abélienne B' définie sur K et K-isogène à B, il existe une isogénie de B' vers B de degré au plus b. L'existence d'un tel entier est une conséquence des travaux de Faltings (voir aussi le Lemme 5.1 de [**19**]).

On reprend les principaux résultats de [**19**]. Le Lemma 2.3 associé au Lemma 3.1 montre que $G(\ell)$ est semi-simple dès que $\ell \geq d(A)b(A)$. En combinant le Lemma 4.1 et la formule (2.2), on voit que son commutant est $\mathbb{F}_\ell \otimes \mathrm{End}(A)$ si :

$$\ell \geq \sqrt{d(A)}b(A^2).$$

Par le Théorème 1.4 de [**12**], on a : $b(A) \leq \kappa(A)$. Si B est K-isogène à A^2, on peut écrire B comme produit de deux sous-variétés abéliennes K-isogènes à A (en considérant les images dans B de chacun des facteurs de A^2). On a donc :

$$b(A^2) \leq \kappa(A)^2.$$

Majorons maintenant le discriminant. Suivant [**12**], on note $\Lambda(\mathrm{End}(A))$ le dernier minimum du réseau $\mathrm{End}(A)$ dans l'espace euclidien $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{R}$ pour la métrique de Rosati. Si r est le rang de $\mathrm{End}(A)$ sur $\mathbb{Z}$, l'inégalité d'Hadamard entraîne :

$$|d(\mathrm{End}(A)| = \left(\frac{r}{2g}\right)^r \mathrm{vol}(\mathrm{End}(A))^2 \leq \Lambda(\mathrm{End}(A))^{4g}.$$

Si A_i est un facteur simple de A, on a :

$$\Lambda(\mathrm{End}(A_i)) \leq (9g)^g P^{\nu(A_i)} \leq (9g)^g P^{2g^2} \leq \kappa(A)^{\frac{1}{4g}},$$

par le Corollaire 2.10, le Lemme 9.2 et le Lemme 9.4 de [**12**] (voir le début de la partie 8 pour la définition et la majoration de ν). On a également :

$$\Lambda(\mathrm{End}(A)) \leq \max_i \Lambda(\mathrm{End}(A_i)),$$

et on en déduit : $|d(\mathrm{End}(A))| \leq \kappa(A)$. Pour :

$$\ell \geq \kappa(A)^3 \geq \max\{\sqrt{d(A)}b(A^2), d(A)b(A)\},$$

les deux conditions demandées sur G_ℓ sont donc réalisées. □

On peut alors estimer en partie l'exposant qui apparaît dans le Théorème 2.5.

Corollaire 2.7. — *Il existe des réels positifs α, β dépendant de g tels qu'on puisse choisir :*

$$\ell_0 = \alpha \cdot N(\mathfrak{p})^{\beta} \cdot \max\{[K:\mathbb{Q}], h_F(A)\}^{2^{14}g^3}.$$

Démonstration. — En suivant la preuve du Théorème 2.5, on voit que la seule contrainte sur l'exposant γ de $\max\{[K:\mathbb{Q}], h_F(A)\}$ est liée à l'utilisation du théorème de Faltings. D'après la Proposition 2.6, il suffit de prendre $\ell \geq \kappa(A)^3$, ce qui donne $\gamma = 2^{14}g^3$. □

Remarques. Les majorations de $d(A)$ et de $b(A)$ dans la démonstration de la Proposition 2.6 ne dépendent que de la classe d'isogénies de A (voir [**12**], §8 et Théorème 1.4). Comme le polynôme caractéristique du Frobénius en $\mathfrak{p}$ est invariant par isogénie, la borne du corollaire ne dépend que de la classe de K-isogénies de A. On en déduit que la constante de Serre est invariante par K-isogénies.

On peut théoriquement déterminer α et β en fonction de g. Cela demanderait de rendre effectifs de nombreux résultats profonds de théorie des groupes et de théorie des représentations (dont des théorèmes de Jordan et de Nori), puis de reprendre en détail la preuve du Théorème 2.5.

2.4. Homothéties pour les grands premiers. — Lorsque ℓ est assez grand, on peut donner une borne assez simple pour la constante de Serre (l'exposant du Théorème 1.4).

Proposition 2.8. — *On suppose que $\ell \geq \max\{\ell_0, \Delta_K + 1\}$. Alors il existe $c \,|\, (2g)!$ tel que :*

$$(\mathbb{Z}_\ell^\times)^c \subset G_\ell.$$

Démonstration. — On reprend les arguments donnés dans [**33**], 2.3. Par une remarque de Deligne (voir [**28**], 2, 3), on sait déjà que le groupe des homothéties $\mathbb{Z}_\ell^\times$ est inclus dans $H_\ell(\mathbb{Q}_\ell)$. Les travaux de Tate aux places de bonne réduction, étendus par Raynaud aux places quelconques ([**2**], 2), montrent que la restriction de ρ_ℓ à tout groupe de décomposition en une place divisant ℓ est de Hodge-Tate. Par [**2**], 1 (preuve du Corollaire), c'est encore vrai pour la représentation abélienne :

$$\rho_\ell^{\mathrm{ab}} : G_K \longrightarrow H_\ell(\mathbb{Q}_\ell)/H_\ell(\mathbb{Q}_\ell)'.$$

Comme A admet réduction semi-stable partout et K est non ramifié au-dessus de ℓ, on peut appliquer le Corollaire 2.4 de [**34**] à ρ_ℓ^{ab}, et on en déduit que : $\mathbb{Z}_\ell^\times \subset \rho_\ell^{\mathrm{ab}}(G_K)$. Par le Théorème 2.4, si c est un annulateur du quotient $\mathcal{S}_\ell(\mathbb{Z}_\ell)/\mathcal{S}_\ell(\mathbb{Z}_\ell)'$, on a :

$$(\mathbb{Z}_\ell^\times)^c \subset G_\ell.$$

Si on note π_ℓ le morphisme de projection associé au revêtement universel de $\mathcal{S}_\ell$, on a : $\mathcal{S}_\ell(\mathbb{Z}_\ell)' = \operatorname{Im}\pi_\ell(\mathbb{Z}_\ell)$ ([**33**], 1.2). Il suffit alors de trouver un entier c qui annule le groupe fondamental de $\operatorname{Ker}\pi_\ell(\overline{\mathbb{Q}}_\ell)$, qui est un sous-groupe semi-simple de $\mathrm{GL}_{2g}(\mathbb{C})$. Comme ses facteurs simples sont de rang borné par $2g-1$, ils ont au plus $2g-1$ poids minuscules et leur groupe fondamental est annulé par un entier inférieur ou égal à $2g$. On peut donc prendre pour c le plus petit commun multiple des entiers $\leq 2g$, qui vérifie la condition annoncée. □

Remarques. On remarque que la constante c donnée par la preuve vérifie :

$$\log(c) = \sum_{p\in\mathcal{P}} \left\lfloor \frac{\log(2g)}{\log p} \right\rfloor \log p \leq \pi(2g)\log(2g) \leq 3g,$$

où $\pi(2g)$, le nombre de premiers inférieurs ou égaux à $2g$, est majoré suivant [**25**], (3.7). On a donc : $c \leq e^{3g}$.

Par le Corollaire 2.7.5 de [**34**], si $g \leq 4$ ou si la conjecture de Mumford-Tate est vraie pour A, on peut prendre $c = 1$ dans la proposition précédente. La conjecture de Lang est donc une conséquence de la conjecture de Mumford-Tate.

En faisant la même hypothèse sur ℓ, il est en fait possible de majorer le quotient $[\mathcal{H}_\ell(\mathbb{Z}_\ell) : G_\ell]$, qui est fini par le théorème de Bogomolov. Par [**35**], Theorem 1.2 (b), on peut trouver une borne qui dépend uniquement de g.

3. Cohomologie galoisienne sur les corps locaux

On étudie dans cette partie des groupes de cohomologie galoisienne introduits par Tate dans [**32**], §3, dont on précise certains résultats en estimant les sauts de ramification d'une extension procyclique. L'étude de ces groupes de cohomologie nous servira dans la partie suivante pour transcrire la structure de Hodge-Tate d'une variété abélienne en une propriété d'algébricité de sa représentation abélienne ℓ-adique.

À l'exception du dernier paragraphe, on se place dans un cadre un peu plus général qui permet d'englober le cas des corps de fonctions en caractéristique positive. On fixe un nombre premier ℓ et un corps local K_v, complet pour une valuation v, dont le corps résiduel est parfait de caractéristique ℓ, et dont l'indice de ramification est noté e. Soit $\bar{K_v}$ la clôture algébrique de K_v. La complétion de $\bar{K_v}$ pour la valeur absolue associée à v est notée C. C'est un corps algébriquement clos.

3.1. Préliminaires sur une extension procyclique totalement ramifiée. — On fixe désormais une extension galoisienne K_∞ de K_v totalement ramifiée telle que :

$$\mathscr{C} := \mathrm{Gal}(K_\infty/K_v) \simeq \mathbb{Z}_\ell,$$

et on se donne un générateur σ de $\mathscr{C}$. On peut obtenir une telle extension en considérant un sous-corps bien choisi du corps engendré sur K_v par les racines ℓ^n-ièmes de l'unité, où n varie dans $\mathbb{N}$.

Si n est un entier naturel, on note K_n le sous-corps de K_∞ correspondant au sous-groupe $\mathscr{C}(n) := \ell^n\mathbb{Z}_\ell$ de $\mathscr{C}$. On a :

$$G(n) := \mathrm{Gal}(K_n/K_v) \simeq \mathscr{C}/\mathscr{C}(n).$$

Pour $\nu \geq -1$, le groupe de ramification en notation supérieure $G(n)^\nu$ est donné par (voir [**26**], IV, §3, Proposition 14, et la remarque qui suit la preuve de cette proposition pour passer aux extensions profinies) :

$$G(n)^\nu = \mathscr{C}^\nu\mathscr{C}(n)/\mathscr{C}(n).$$

Soit $(\nu_i)_{i\geq -1}$ la suite définie par : $\mathscr{C}^\nu = \mathscr{C}(i)$, pour $\nu_i < \nu \leq \nu_{i+1}$. On a $\nu_0 = -1$ et les $(\nu_i)_{i\geq 0}$ sont des entiers positifs par le théorème de Hasse-Arf (voir [**26**], V,

§7, Théorème 1, pour le cas des extensions finies auquel on se ramène immédiatement). Pour une extension procyclique, on peut en dire un peu plus sur ces « sauts de ramification ».

Lemme 3.1. — *Il existe un entier κ tel que pour tout $i \geq \kappa + 1$:*

$$\nu_{i+1} - \nu_i = e,$$

et

$$\max\{\nu_{\kappa+1}, \ell^\kappa + 1\} \leq \frac{e\ell}{\ell - 1}.$$

Démonstration. — Soit κ le plus grand entier i pour lequel :

$$\nu_i < \frac{e}{\ell - 1}.$$

Ce nombre est bien défini, car les $(\nu_i)_{i\geq 0}$ sont une suite strictement croissante d'entiers et $\nu_0 = -1$. On applique maintenant [**18**], Example page 280 (qui précise le Theorem 6) à K_n/K_v en prenant $n > \kappa + 1$. On voit d'abord que pour $\kappa + 1 \leq i \leq n$:

$$\nu_{i+1} - \nu_i = e\,;$$

puis que :

$$\nu_{\kappa+1} \leq \tfrac{e\ell}{\ell-1} \quad \text{ou} \quad \nu_{\kappa+1} = \min\{\ell\nu_\kappa, \nu_\kappa + e\} = \ell\nu_\kappa,$$

ce qui donne dans chaque cas la majoration annoncée pour $\nu_{\kappa+1}$. De plus, pour tout $1 \leq i \leq n$,

$$\nu_{i+1} \geq \min\{\ell\nu_i, \nu_i + e\}.$$

Pour $i < \kappa$, ceci impose que $\nu_{i+1} \geq \ell\nu_i$, donc

$$\ell^{\kappa-1} \leq \nu_\kappa < \frac{e}{\ell - 1}.$$

Ceci valant pour tout $n > \kappa + 1$, le lemme est entièrement démontré. □

Remarque. Les travaux de Maus ([**20**]) et Miki ([**21**]) montrent que les conditions utilisées ici caractérisent la suite des sauts de ramification d'une extension cyclique de corps locaux, et que les estimations du lemme sont essentiellement optimales.

La différente relative d'une extension M/L sera notée $\mathfrak{d}_{M/L}$. On peut estimer précisément les valuations de la différente sur la tour d'extensions $(K_n)_{n\in\mathbb{N}}$.

Lemme 3.2. — *On a :*

$$v(\mathfrak{d}_{K_n/K_v}) = en + c_1 + \ell^{-n}c_2,$$

où $|c_1| \leq 6e^2$ *et* $|c_2| \leq 2\left(\frac{\ell e}{\ell-1}\right)^2 - 1 \leq 8e^2$.

Démonstration. — Suivant la Proposition 5 de [**32**], on voit que $|G(n)^\nu| = \ell^{n-i}$ si $\nu_i < \nu \leq \nu_{i+1}$ $(0 \leq i \leq n)$. De plus :

$$\begin{aligned} v(\mathfrak{d}_{K_n/K_v}) &= \int_{-1}^{\infty} \left(1 - \frac{1}{|G(n)^\nu|}\right) d\nu \\ &= \sum_{i=0}^{n} (1-\ell^{i-n})(\nu_{i+1} - \nu_i) \\ &= \sum_{i=0}^{\kappa} (1-\ell^{i-n})(\nu_{i+1} - \nu_i) + e \sum_{i=\kappa+1}^{n} (1-\ell^{i-n}) \\ &= en - e\kappa + \nu_{\kappa+1} + 1 - e\frac{\ell - \ell^{\kappa+1-n}}{\ell - 1} - \sum_{i=0}^{\kappa} \ell^{i-n}(\nu_{i+1} - \nu_i) \\ &= en + c_1 + \ell^{-n} c_2, \end{aligned}$$

où

$$c_1 = -e\kappa + \nu_{\kappa+1} + 1 - \frac{e\ell}{\ell - 1},$$

et

$$c_2 = \frac{e\ell^{\kappa+1}}{\ell - 1} - \sum_{i=0}^{\kappa} \ell^i (\nu_{i+1} - \nu_i).$$

On a :

$$|c_1| \leq 1 + \frac{2e\ell}{\ell - 1} + e^2 \leq 6e^2,$$

et

$$|c_2| \leq \left(\frac{e\ell}{\ell - 1}\right)^2 + \ell^\kappa(1 + \nu_{\kappa+1}) \leq 2\left(\frac{\ell}{\ell - 1}\right)^2 e^2 - 1 \leq 8e^2,$$

ce qui conclut la preuve. □

Corollaire 3.3. — *On a :*

$$v(\mathfrak{d}_{K_{n+1}/K_n}) = e + \ell^{-n} c_3,$$

où $|c_3| \leq \frac{2e^2\ell}{\ell-1} - 1 + \frac{1}{\ell} \leq 4e^2$.

Démonstration. — Par transitivité de la différente ([**26**], III §4, Proposition 8), on obtient :

$$v(\mathfrak{d}_{K_{n+1}/K_n}) = e + \ell^{-n} c_2 \frac{1-\ell}{\ell}.$$

Posons :

$$c_3 := c_2 \frac{1-\ell}{\ell}.$$

La majoration de c_2 dans le Lemme 3.2 donne :

$$|c_3| \leq 2e^2 \frac{\ell}{\ell - 1} - \frac{\ell - 1}{\ell} \leq 4e^2,$$

et le corollaire est prouvé. □

On peut maintenant évaluer la variation de la valeur absolue $|\cdot|$ associée à v par application de la trace de K_{n+1} à K_n, notée $\mathrm{Tr}_{K_{n+1}/K_n}$.

Corollaire 3.4. — *Pour $x \in K_{n+1}$, on a :*

$$|\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq \ell^{-e+\ell^{-n}c_4}|x|,$$

où $|c_4| \leq 2e^2\frac{\ell}{\ell-1} + \frac{1}{\ell} \leq 5e^2$.

Démonstration. — Soit $\mathfrak{m}_n$ l'idéal maximal de l'anneau des entiers R_n de K_n. Par K_v-linéarité de la trace, on peut supposer que $x \in R_{n+1}$ quitte à le multiplier par une puissance de ℓ suffisamment grande. On pose $\mathfrak{d}_{K_{n+1}/K_n} = \mathfrak{m}_{n+1}^d$. Par **[26]**, V §3, Lemme 4 :

$$\mathrm{Tr}_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}_n^j,$$

avec $j = \left[\frac{i+d}{\ell}\right]$. Comme K_n est totalement ramifiée sur K de degré ℓ^n, on en déduit :

$$\begin{aligned} v(\mathrm{Tr}_{K_{n+1}/K_n}(x)) &= \ell^{-n}\left[\ell^n(v(x) + v(\mathfrak{d}_{K_{n+1}/K_n}))\right] \\ &= e + \ell^{-n}[\ell^n v(x) + c_3] \\ &> e + v(x) + \ell^{-n}(c_3 - 1). \end{aligned}$$

Le corollaire s'en déduit en passant à la valeur absolue et en posant $c_4 = c_3 - 1$. □

Remarque. Le Lemme 3 de **[26]**, V §3 donne une expression assez simple pour d, mais qui nécessite de connaître le saut de ramification dans K_{n+1}/K_n.

On définit une fonction K_v-linéaire t sur K_∞ par :

$$t(x) := \ell^{-n}\mathrm{Tr}_{K_n/K_v}(x),$$

si $x \in K_n$. Cette formule ne dépend pas du choix de K_n contenant x, par les propriétés élémentaires de la trace et car $[K_n/K_v] = \ell^n$. Rappelons qu'on a aussi fixé un générateur σ du groupe $\mathscr{C}$. Si $x \in K_{n+1}$, par **[32]**, Lemma 2 (et la remarque à la fin de la preuve du lemme) :

$$\left|x - \ell^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x)\right| \leq \ell^e\left|\sigma^{\ell^n}(x) - x\right| = \ell^e\left|\sigma(x) - x\right|, \tag{1}$$

la dernière inégalité résultant de la formule du binôme (quitte à supposer x entier par linéarité).

Ceci va nous permettre de démontrer l'inégalité suivante.

Proposition 3.5. — *Pour tout $x \in K_\infty$:*

$$|x - t(x)| \leq \ell^{c_5}|x - \sigma(x)|,$$

où $|c_5| \leq \frac{2\ell}{(\ell-1)^2}e^2 + e + \frac{1}{\ell(\ell-1)} \leq 6e^2$.

Démonstration. — Prouvons par récurrence sur $n \geq 1$ que pour $x \in K_n$:

$$|x - t(x)| \leq \ell^{u_n}|x - \sigma(x)|,$$

avec $u_1 = e$ et si $n \geq 2$:

$$u_n = e + |c_4|\sum_{k=1}^{n-1}\ell^{-k}.$$

Pour $n = 1$, c'est une conséquence immédiate de (1). Supposons le résultat montré au rang $n \geq 1$ et prenons $x \in K_{n+1}$. On applique l'hypothèse de récurrence à $y = \mathrm{Tr}_{K_{n+1}/K_n}(x)$:

$$\begin{aligned} |y - t(y)| &\leq \ell^{u_n}|y - \sigma(y)| \\ &\leq \ell^{u_n}|\mathrm{Tr}_{K_{n+1}/K_n}(x - \sigma(x)| \\ &\leq \ell^{u_n - e + \ell^{-n}c_4}|x - \sigma(x)|. \end{aligned}$$

Par les propriétés de la trace et en appliquant (1), on en déduit que :

$$\begin{aligned} |x - t(x)| &= |x - \ell^{-1}y + \ell^{-1}y - \ell^{-1}t(y)| \\ &\leq \max\{|x - \ell^{-1}y|, |\ell^{-1}y - \ell^{-1}t(y)|\} \\ &\leq \max\{\ell^e, \ell^{u_n + \ell^{-n}c_4}\}|x - \sigma(x)| \\ &\leq \ell^{u_{n+1}}|x - \sigma(x)|. \end{aligned}$$

Comme pour tout n :

$$u_n \leq e + \frac{|c_4|}{(\ell - 1} \leq \frac{2\ell}{(\ell-1)^2}e^2 + e + \frac{1}{\ell(\ell-1)} \leq 6e^2,$$

la proposition suit. □

Remarque. Si on remplace le corps de base K_v par K_n, où $n \geq 1$, la preuve peut être adaptée *mutatis mutandis* et on obtient exactement la même inégalité.

3.2. Condition d'annulation de groupes de cohomologie. — Si A est un K_v-espace vectoriel normé muni d'une action continue de $\mathscr{C}$, on peut définir les groupes de cohomologie $H^i(\mathscr{C}, A)$, où $i \geq 0$, pour les cochaînes continues. Le groupe $H^0(\mathscr{C}, A)$ est constitué des éléments de A fixés par $\mathscr{C}$; le groupe $H^1(\mathscr{C}, A)$ est constitué des *cocyles* continus χ de $\mathscr{C}$ dans A qui sont des *cobords*, c'est-à-dire tels qu'il existe $a \in A$ vérifiant :

$$\forall \tau \in \mathscr{C} : \quad \chi(\tau) = \tau \cdot a - a.$$

On renvoie à [**26**], VII §3 pour plus de détails.

On considère maintenant la complétion X de K_∞ pour la valeur absolue associée à v. C'est un K_v-espace de Banach sur lequel $\mathscr{C}$ agit continûment. Dans ce cas, la structure des deux premiers groupes de cohomologie est clarifiée par les travaux de Tate ([**32**], Proposition 8).

Lemme 3.6. — *On a $H^0(\mathscr{C}, X) = K_v$, et $H^1(\mathscr{C}, X)$ est un K_v-espace vectoriel de dimension* 1.

Soit χ un caractère continu de $\mathscr{C}$ à valeurs dans K_v^*. On note $X(\chi)$ le $\mathscr{C}$-module X pour l'action « tordue » :

$$\forall x \in X, \tau \in \mathscr{C} : \quad \tau \cdot x := \chi(\tau)\tau(x).$$

Lorsque l'image du caractère χ n'est pas trop petite dans un sens qu'on va désormais préciser, l'action qu'il induit annule les groupes de cohomologie. Soit :

$$c_6 := 2 + \left[\frac{1}{e\ell(\ell-1)} + \frac{2\ell e}{(\ell-1)^2} + \frac{\log(2e)}{\log \ell} \right] \leq 7e.$$

Proposition 3.7. — *Si $\chi^{\ell^{c_6}} \neq 1$, on a $H^0(\mathscr{C}, X(\chi)) = 0$ et $H^1(\mathscr{C}, X(\chi)) = 0$.*

Démonstration. — On reprend les résultats de la Proposition 7 de [**32**] en les précisant. La fonction K_v-linéaire t définie sur K_∞ se prolonge à X par continuité. Si on note X_0 son noyau, l'espace X est la somme directe de X_0 et de K_v. D'autre part, l'opérateur $\sigma - \mathrm{Id}$ admet un inverse K_v-linéaire et continu ρ sur X_0 tel que :

$$\forall y \in X_0 : \ |\rho(y)| \leq \ell^{c_5} |y|.$$

Soit $\lambda := \chi(\sigma)^{-1}$. On vérifie immédiatement que le groupe $H^0(\mathscr{C}, X(\chi))$ est le noyau de $\sigma' := \sigma - \lambda \mathrm{Id}$ sur X, et que $H^1(\mathscr{C}, X(\chi))$ est un sous-groupe du conoyau de σ'. Il suffit donc de démontrer que σ' est bijectif sur X. Comme $\lambda \neq 1$, la bijectivité de σ' sur K_v est immédiate et il suffit donc d'étudier σ' sur X_0.

Par continuité de χ, on observe que :

$$|\lambda^{-\ell^n} - 1| \longrightarrow 0,$$

donc $|\lambda^{-1} - 1| < 1$, et $|\lambda - 1| < 1$. Pour $i \geq 0$, soit $w_i := v\big(\lambda^{\ell^i} - 1\big)$. On a donc $w_0 \geq 1$. Par la formule du binôme et les propriétés usuelles des coefficients binomiaux, on obtient :

$$\forall i \geq 0 : \ w_{i+1} \geq \min\{e + w_i, \ell w_i\},$$

et on a une égalité dès que $e + w_i \neq \ell w_i$. Soit κ le plus petit entier $i \geq 0$ pour lequel $w_i > e/(\ell - 1)$. Cet entier existe car la suite des entiers $(w_i)_i$ est strictement croissante. Remarquons que $\ell^\kappa \leq \ell e/(\ell - 1)$, ce qui donne :

$$\kappa \leq \left[\frac{\log(2e)}{\log \ell} \right].$$

On en déduit que $c_6 > \kappa$. Il vient :

$$\begin{aligned} w_{c_6} &\geq \ell^\kappa + (c_6 - \kappa)e \\ &\geq \frac{e}{\ell - 1} + (c_6 - \kappa)e \\ &\geq \frac{e}{\ell - 1} + e + \frac{1}{\ell(\ell-1)} + \frac{2\ell e^2}{(\ell-1)^2} \\ &> |c_5|. \end{aligned}$$

Par hypothèse, $\lambda^{\ell^{c_6}} \neq 1$. Si $y \in X_0$, on a donc :

$$\big|(\lambda^{\ell^{c_6}} - 1)\rho(y)\big| \leq \ell^{c_5 - w_{c_6}} |y| < |y|.$$

Si on prend K_{c_6} comme corps de base au lieu de K_v, ces résultats restent vrais par la remarque suivant la preuve de la Proposition 3.5. Par linéarité de ρ, on obtient :

$$\rho(\sigma^{\ell^{c_6}} - \lambda^{\ell^{c_6}}) = 1 - (\lambda^{\ell^{c_6}} - 1)\rho,$$

qui est donc inversible. On en déduit que $\sigma^{\ell^{c_6}} - \lambda^{\ell^{c_6}}$ est inversible sur X_0. Mais comme $\sigma^{\ell^{c_6}} - \lambda^{\ell^{c_6}} = \sigma'\tau$, pour un certain $\tau \in K_v[\sigma]$, l'application σ' est également bijective. □

Remarques. Si on suppose que $\ell \geq 4e^2$, on voit d'abord que $e/(\ell-1) < 1$, donc $\kappa = 0$. Mais on a également :

$$|c_5| \leq e + \frac{1}{\ell^2 - \ell} + \frac{1}{(\ell-1)^2} < 1 + e.$$

Comme $w_1 \geq 1 + e$, on peut alors choisir $c_6 = 1$.

Si K_v est de caractéristique ℓ, on note que la borne obtenue dépend de l'indice de ramification, et pas des racines de l'unité contenues dans K_v^* (liées à son corps des constantes), qui apparaissent naturellement dans l'étude de l'image de χ.

3.3. Logarithme des caractères admissibles. — Les calculs qu'on vient d'effectuer sur une extension procyclique totalement ramifiée ont des conséquences importantes pour la théorie des modules de Hodge-Tate. On suppose dans ce paragraphe que K_v est de caractéristique nulle. On note $\mathscr{G} := \mathrm{Gal}(\bar{K}_v/K_v)$, $\mathscr{I}$ son sous-groupe d'inertie, et on fixe un caractère continu $\chi : \mathscr{G} \to K_v^*$.

Définition 3.8. — *Le caractère χ est dit admissible (noté $\chi \sim 1$) s'il existe $x \in C^*$ tel que :*

$$\forall \sigma \in \mathscr{G} : \ \sigma(x) = \chi(\sigma)x.$$

On peut alors définir une relation d'équivalence entre deux caractères χ, χ' :

$$\chi \sim \chi' \text{ si et seulement si } \chi'\chi^{-1} \sim 1.$$

Soit $H^1(\mathscr{G}, C^*)$ le premier groupe de cohomologie de $\mathscr{G}$ à valeurs dans C^* (les cochaînes étant supposées continues). Un caractère continu de $\mathscr{G}$ dans C^* définit un élément de $H^1(\mathscr{G}, C^*)$ qui est nul si et seulement si le caractère est admissible.

Le caractère χ permet aussi de définir une action « tordue » :

$$\forall x \in C, \sigma \in \mathscr{G} : \sigma \cdot x = \chi(\sigma)\sigma(x).$$

On note $C(\chi)$ le $\mathscr{G}$-module ainsi obtenu. Si χ est admissible, le $\mathscr{G}$-module $C(\chi)$ est isomorphe à C, l'isomorphisme étant la multiplication par l'élément de C^* intervenant dans la définition d'un caractère admissible.

On se donne un sous-corps E de K_v^* contenant $\mathbb{Q}_\ell$ et tel que $[E : \mathbb{Q}_\ell] < \infty$. On suppose que tous les conjugués de E sur $\mathbb{Q}_\ell$ sont dans K_v, et on note Γ_E l'ensemble des $\mathbb{Q}_\ell$-plongements de E dans K_v. Le logarithme ℓ-adique sur le groupe U_E des unités de E, noté log (voir [**27**], III, A2), permet d'interpréter certaines conditions d'admissibilité apparaissant naturellement en théorie de Hodge-Tate.

Proposition 3.9. — *On suppose que χ est à valeurs dans E^*, et que pour $\tau \in \Gamma_E$, on a $\tau \circ \chi \sim 1$. Alors :*

$$\log \chi(\mathscr{I}) = 0.$$

Démonstration. — On reprend les arguments donnés dans la preuve de [**27**], III, A3, Proposition 3. Le sous-groupe $\log\chi(\mathscr{I})$ de E est compact, isomorphe à $\mathbb{Z}_\ell^n$ pour un certain entier n. Supposons par l'absurde que $n \geq 1$.

En considérant un projecteur bien choisi, on voit qu'il existe une application $\mathbb{Q}_\ell$-linéaire : $f : E \to K_v$ telle que $f\big(\log\chi(\mathscr{I}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell\big)$ soit de dimension 1. Par indépendance des caractères, l'ensemble Γ_E est une base de $\mathrm{Hom}_{\mathbb{Q}_\ell}(E, K_v)$, ce qui donne une décomposition :

$$f = \sum_{\tau\in\Gamma_E} k_\tau \tau,$$

où les k_τ sont dans K_v. Le logarithme étant défini sur $\mathbb{Q}_\ell$, on a :

$$f \circ \log\chi = \sum_{\tau\in\Gamma_E} k_\tau \log\tau \circ \chi.$$

Les hypothèses et la Proposition 3 de [**27**], III, A2 impliquent que l'image de $f\circ\log\chi$ dans $H^1(\mathscr{G}, C)$ est nulle. Par les propriétés du logarithme ([**29**], III, A2), quitte à multiplier f par une puissance convenable de ℓ, il existe un morphisme continu

$$F : U_E \to U_{K_v}$$

tel que $f\circ\log = \log\circ F$. En utilisant une nouvelle fois la Proposition 3 de [**27**], III, A2, on voit que $F\circ\chi \sim 1$. De plus, $\log F\circ\chi(\mathscr{I}) \simeq \mathbb{Z}_\ell$, et $F\circ\chi(\mathscr{I}) \simeq \mathbb{Z}_\ell \times H$, pour un certain groupe H fini.

Soit $\mathscr{C}$ un quotient de $\mathscr{I}$ dont l'image est $\mathbb{Z}_\ell$. Il définit une extension K_∞/K_v totalement ramifiée de groupe de Galois $\mathscr{C}$ à laquelle on peut appliquer les résultats obtenus dans cette partie. Par le Lemme 3.6 et la Proposition 3.7 :

$$H^1(\mathscr{C}, X) \neq H^1(\mathscr{C}, X(F\circ\chi)).$$

La Proposition 10 de [**32**] donne alors :

$$H^1(\mathscr{G}, C) \neq H^1(\mathscr{G}, C(F\circ\chi)),$$

ce qui contredit l'admissibilité de $F\circ\chi$. □

4. Le cas des petits premiers : autour du théorème de Bogomolov

La question des homothéties étant à peu près clarifiée pour les grands premiers, il s'agit désormais de trouver un exposant indépendant de ℓ dans le Théorème 1.4. Dans la mesure où on dispose d'une borne pour l'entier ℓ_0 qui apparaît dans le Théorème 2.4, on peut se contenter, pour les premiers $\ell \leq \ell_0$, d'un exposant dépendant de A mais aussi de ℓ. La question est donc de donner une version explicite du Théorème 1.3, dont on va reprendre la preuve en détail.

4.1. Algèbre de Lie du groupe dérivé. — La première étape consiste à contrôler le groupe dérivé $H_\ell(\mathbb{Q}_\ell)'$, pour pouvoir ensuite utiliser les propriétés des représentations abéliennes. Pour y arriver, on s'appuie sur un résultat classique de la théorie des groupes algébriques en caractéristique nulle.

Proposition 4.1. — *Pour $\ell \in \mathcal{P}$, le groupe $G_\ell \cap \mathcal{S}_\ell(\mathbb{Z}_\ell)$ est d'indice fini dans $\mathcal{S}_\ell(\mathbb{Z}_\ell)$.*

Démonstration. — Soit $\mathfrak{g}_\ell$ l'algèbre de Lie de G_ℓ, $\mathfrak{h}_\ell$ celle de $H_\ell(\mathbb{Q}_\ell)$ et $\mathfrak{h}'_\ell$ celle de $H_\ell(\mathbb{Q}_\ell)'$. Par la Proposition 7.8 et le Corollaire 7.9 de [**3**], II, on a :

$$\mathfrak{h}'_\ell = [\mathfrak{h}_\ell, \mathfrak{h}_\ell] = [\mathfrak{g}_\ell, \mathfrak{g}_\ell] \subset \mathfrak{g}_\ell.$$

On en déduit que $G_\ell \cap H_\ell(\mathbb{Q}_\ell)' = G_\ell \cap S_\ell(\mathbb{Z}_\ell)$ est ouvert pour la topologie ℓ-adique dans $\mathcal{H}_\ell(\mathbb{Q}_\ell)' = \mathcal{S}_\ell(\mathbb{Q}_\ell)$, donc d'indice fini dans $\mathcal{S}_\ell(\mathbb{Z}_\ell)$. □

On note $s(A,\ell) := \big[\mathcal{S}_\ell(\mathbb{Z}_\ell) : G_\ell \cap \mathcal{S}_\ell(\mathbb{Z}_\ell)\big]$. Trouver une borne explicite pour $s(A,\ell)$ est un problème très difficile si l'on ne fait pas d'hypothèse sur A. La stratégie de Serre ne semble pas pouvoir s'adapter aisément pour majorer $s(A,\ell)$ lorsque ℓ est un premier quelconque.

Des résultats ont été obtenus en petite dimension, notamment basés sur l'étude de « l'algèbre de Lie entière » associée à G_ℓ (voir par exemple [**16**], qui donne une version explicite du théorème de l'image ouverte de Serre sur les courbes elliptiques).

4.2. Algébricité locale et structure de Hodge-Tate. — On souhaite maintenant étudier, pour ℓ quelconque, la représentation abélienne :

$$\rho_\ell^{\mathrm{ab}} : G_K \longrightarrow H_\ell(\mathbb{Q}_\ell)/H_\ell(\mathbb{Q}_\ell)'.$$

La première étape est de se ramener à une représentation linéaire.

Lemme 4.2. — *Il existe un entier $c(g) > 0$ et une représentation*

$$\sigma : H_\ell(\mathbb{Q}_\ell) \longrightarrow \mathrm{GL}_n(\mathbb{Q}_\ell),$$

telle que $n \leq c(g)$ et $\operatorname{Ker}\sigma = H_\ell(\mathbb{Q}_\ell)'$. De plus, la composée $\sigma \circ \rho_\ell$ est de Hodge-Tate.

Démonstration. — Il existe un nombre fini de sous-groupes semi-simples de $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$, à isomorphisme près et indépendamment de ℓ. En conséquence d'un théorème de Chevalley (voir [**8**], Proposition 3.1.c), si S est un tel groupe, il est caractérisé par ses invariants tensoriels, c'est-à-dire qu'il existe un entier $c(S) > 0$ tel que S est le sous-groupe de $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ fixant :

$$\Big\{x \in \bigoplus_{m \leq c(S)} (\mathbb{Q}_\ell^{2g})^{\otimes m}, \forall s \in S : s \cdot x = x\Big\}.$$

On prend $S := H_\ell(\mathbb{Q}_\ell)'$ et on considère le sous-espace vectoriel W de

$$\bigoplus_{m \leq c(S)} (\mathbb{Q}_\ell^{2g})^{\otimes m}$$

fixé par S. On a :

$$\dim(W) \leq \sum_{m=0}^{c(S)} (2g)^m \leq (2g)^{c(S)+1} \leq (2g)^{\max_S c(S)+1} := c(g).$$

La représentation σ donnée par l'action de $H_\ell(\mathbb{Q}_\ell)$ sur W est de degré borné par $c(g)$, et on a par construction :

$$\operatorname{Ker}\sigma = H_\ell(\mathbb{Q}_\ell)'.$$

De plus, on sait que ρ_ℓ est de Hodge-Tate et que cette propriété est préservée par tensorisation ([**2**], 1, preuve du Corollaire), donc la représentation $\sigma \circ \rho_\ell$ est encore de Hodge-Tate. □

On pose $\sigma_\ell^{\mathrm{ab}} := \sigma \circ \rho_\ell$. L'image T_ℓ de H_ℓ par σ est un groupe algébrique commutatif qui n'a pas de composante additive, car celle-ci donnerait lieu à une extension abélienne non-ramifiée infinie de K. C'est donc un tore.

Proposition 4.3. — *On pose* $m := n!(\ell^{n!}-1)\ell^{1+v_\ell(n!)}$. *Alors :*

$$T_\ell(\mathbb{Z}_\ell)^m \subset \sigma_\ell^{\mathrm{ab}}(G_K).$$

Démonstration. — On commence par fixer une place $v|\ell$ et on considère la représentation σ_v déduite de $\sigma_\ell^{\mathrm{ab}}$ par projection sur le groupe d'inertie I_v. D'après le théorème de Tate ([**27**], III, A7), la représentation σ_v, qui est semi-simple puisque T_ℓ est un tore, est localement algébrique. Cela signifie qu'elle provient d'un morphisme algébrique du tore T_v associé à K_v sur $\mathbb{Q}_\ell$ via la théorie du corps de classe local – modulo un sous-groupe fini de I_v.

On va quantifier ce fait. Pour cela, on se donne un facteur simple V de $\mathbb{Q}_\ell^n$. Par le lemme de Schur, le commutant de $\sigma_v|_V$ est un corps E vérifiant :

$$[E:\mathbb{Q}_\ell] = \dim(V) \leq n,$$

et $\sigma_v|_V$ est donnée par un caractère χ_V à valeurs dans E^*. Soit K' le compositum de K_v et de la clôture galoisienne de E. La structure de Hodge-Tate de σ_v permet de définir un morphisme algébrique r_V défini sur le tore $T_{K'}$ associé à K' et à valeurs dans E^*. Il est donné par la formule ([**27**], III, A6, Proposition 6) :

$$r_V := \prod_{\tau \in \Gamma_E} \tau^{-1} \circ \chi_{\tau E}^{n_\tau},$$

où Γ_E est l'ensemble des $\mathbb{Q}_\ell$-morphismes $\tau : E \longrightarrow K'$, de poids n_τ dans la décomposition de Hodge-Tate, le caractère $\chi_{\tau E} : G_{K'}^{\mathrm{ab}} \longrightarrow \tau E^*$ se déduisant de l'inclusion $\tau E \subset K'$ par la théorie du corps de classe local sur τE ([**27**], III, A4). Le lien entre r_V et χ_V est alors donné par les relations ([**27**], III, A5, Theorem 2) :

$$\forall \tau \in \Gamma_E : \quad \tau \circ (r_V^{-1}\chi_V) \sim 1.$$

Par la Proposition 3.9, on en déduit :

$$\log\left(r_V^{-1}\chi_V\left(I_v^{[K':K_v]}\right)\right) = 0,$$

et

$$r_V^{-1}\chi_V\left(I_v^{[K':K_v]}\right) \subset \operatorname{Ker}\log.$$

Par le Lemma de [**27**], III, A2, si f_E est le degré résiduel de E et si la composante ℓ-primaire du sous-groupe de torsion de E^* est de la forme $(\mathbb{Z}/\ell\mathbb{Z})^{\alpha_E}$, on a :

$$\begin{aligned} |\operatorname{Ker}\log| &= (\ell^{f_E}-1)\ell^{\alpha_E} \\ &| \quad (\ell^{[E:\mathbb{Q}_\ell]}-1)\ell^{1+v_\ell([E:\mathbb{Q}_\ell])} \\ &| \quad (\ell^{n!}-1)\ell^{1+v_\ell(n!)}. \end{aligned}$$

On a ainsi : $r_V^m = \chi_V^m$ sur I_v. L'entier m ne dépendant pas du facteur simple V considéré, il existe donc un morphisme algébrique r_v défini sur le tore T_v tel que $r_v^m = \sigma_v^m$ sur I_v.

On peut finalement globaliser en considérant le produit des T_v, pour $v|\ell$: il existe un tore T, image de T_K par un certain morphisme algébrique r, tel que :

$$T(\mathbb{Z}_\ell)^m \subset \sigma_\ell^{\mathrm{ab}}(G_K) \subset T(\mathbb{Q}_\ell).$$

Mais comme H_ℓ est l'enveloppe algébrique de G_ℓ, on a $T_\ell = T$. □

Corollaire 4.4. — *Soit* $c := (\ell-1)\,\ell^{1+2v_\ell(c(g)!)}$. *Alors :*

$$(\mathbb{Z}_\ell^\times)^c \subset \rho_\ell^{\mathrm{ab}}(G_K).$$

Démonstration. — Par la remarque de Deligne ([**28**], 2, 3), on a :

$$\mathbb{Z}_\ell^\times \subset H_\ell(\mathbb{Z}_\ell).$$

Puisque σ induit une représentation fidèle de $H_\ell(\mathbb{Q}_\ell)/H_\ell(\mathbb{Q}_\ell)'$, la proposition précédente montre que l'indice c de $\mathbb{Z}_\ell^\times$ dans $\rho_\ell^{\mathrm{ab}}(G_K)$ est fini et divise m. On en déduit que c divise $(\ell-1)\ell^{v_\ell(m)}$, et comme :

$$v_\ell(m) \leq 1 + 2v_\ell(c(g)!),$$

le corollaire est démontré. □

Remarques. On observe que :

$$c \leq \big(\ell c(g)!\big)^2.$$

Comme on l'a déjà vu, si K est non ramifié au-dessus de ℓ, on peut appliquer le Corollaire 2.4 de [**34**] qui donne : $\mathbb{Z}_\ell^\times \subset \rho_\ell^{\mathrm{ab}}(G_K)$. Le résultat précédent ne sert donc que si ℓ divise Δ_K.

5. Homothéties et bornes uniformes pour la torsion

On revient pour finir sur le problème de Manin-Mumford et la recherche de bornes uniformes, aussi explicites que possible, pour la torsion dans les sous-variétés de A. Les cas les plus favorables sont ceux où la constante de Serre peut être le mieux explicitée. Ils se produisent par exemple lorsque A est une puissance de courbe elliptique ou une variété abélienne de type CM.

5.1. Constante de Serre dans des cas particuliers. — Commençons par regarder le cas où $A = E$ est une courbe elliptique. Il est alors possible d'expliciter entièrement la constante de Serre. Une borne précise pour les grands premiers, reposant sur des travaux de Momose ([**22**]), est donnée par le Théorème 39 de [**10**]. On note h_K le nombre de classes de K.

Théorème 5.1 **(Eckstein).** — *On suppose que E n'est pas de type CM. Si*

$$\ell \geq \max\left\{(48[K:\mathbb{Q}]h_K)^{3(48[K:\mathbb{Q}]h_K)^2}, \Delta_{K(E[3])}\right\},$$

on a : $\mathbb{Z}_\ell^\times \subset G_\ell$.

Pour un résultat sans restriction sur ℓ, on peut utiliser les estimations données par Lombardo dans le problème de l'image ouverte de Serre ([**16**], Theorem 1.1). On rappelle que la hauteur de Faltings de E est notée $h_F(E)$.

***Théorème 5.2* (Lombardo).** — *On suppose que E n'est pas de type CM. Alors $(\mathbb{Z}_\ell^\times)^c \subset G_\ell$, où*

$$c \leq e^{1{,}9\cdot 10^{10}} \big([K:\mathbb{Q}] \max\{1, h_F(E), \log[K:\mathbb{Q}]\}\big)^{12395}.$$

Remarque. Une étude fine de la représentation modulo ℓ est faite dans [**6**]. Dans le cas des surfaces abéliennes, une borne pour les grands premiers peut être dérivée de [**17**].

Les variétés abéliennes de type CM donnent lieu à des estimations particulièrement efficaces (voir [**10**], Théorème 6). Le problème porte alors essentiellement sur les représentations abéliennes et peut être attaqué grâce à la théorie du corps de classe dans le cas CM.

***Théorème 5.3* (Eckstein).** — *Si A est de type CM, on a :*

$$\forall \ell \in \mathcal{P} \ : \ (\mathbb{Z}_\ell^\times)^c \subset G_\ell,$$

où $c = [K:\mathbb{Q}] \cdot |\mathrm{GL}_{2g}(\mathbb{F}_3)|$.

La valeur de l'exposant est le plus souvent meilleure : si $\ell \nmid \Delta_K$, on peut prendre $c = |\mathrm{GL}_{2g}(\mathbb{F}_3)|$. Si, de plus, A admet bonne réduction en ℓ, on peut prendre $c = 1$.

5.2. Bornes uniformes dans le problème de Manin-Mumford. — Commençons par rappeler certains des résultats obtenus dans [**11**]. On fixe un plongement de A dans un espace projectif de dimension minimale $2g+1$ (suivant [**31**], 5.4, Theorem 9). Si V est une sous-variété de A, on note $\delta(V)$ le « degré de définition » de V, c'est-à-dire le plus petit d tel que V est l'intersection d'hypersurfaces de A de degré au plus d.

Par le théorème de Raynaud ([**24**]), on sait que V contient un nombre fini de translatés de sous-variétés abéliennes de A par des points de torsion. Le nombre $T(V)$ de tels translatés qui sont maximaux pour l'inclusion peut être borné uniformément en fonction de $\delta(V)$, de g et de la constante de Serre $c(A)$ ([**11**], Theorem 4.5 et la remarque qui suit la preuve).

Théorème 5.4. — *On a :*

$$T(V) \leq 16^{(c(A)+3)g^3} \delta(V)^g.$$

Si C est une courbe et A est sa jacobienne de dimension $g \geq 2$, le cardinal des points de torsion de C, noté $|C_{\mathrm{tors}}|$, vérifie ([**11**], Proposition 3.7 et la remarque qui suit la preuve) :

$$|C_{\mathrm{tors}}| \leq 4^{(2c(A)+2)g}.$$

Remarque. Il est probable qu'on obtienne de meilleurs résultats en séparant les petits premiers pour lesquels l'exposant d'homothétie est mal contrôlé, et les grands premiers

pour lesquels il est borné uniformément. Pour ce faire, on pourrait introduire une isogénie dont le noyau contient le sous-groupe de torsion fini pour lequel la borne uniforme n'est pas réalisée.

Cas des puissances de courbes elliptiques. On suppose ici que $A = E^g$, où E est une courbe elliptique non CM. Ce cas est particulièrement intéressant pour le problème de Manin-Mumford, dans la mesure où A admet beaucoup de sous-variétés de torsion. Si V est une sous-variété de E^g, le nombre de sous-variétés maximales est borné en utilisant le Théorème 5.2 :

$$T(V) \leq 16^{e^{2\cdot 10^{10}} g^3 \cdot \left([K:\mathbb{Q}] \max\{1, h_F(E), \log[K:\mathbb{Q}]\}\right)^{12395}} \delta(V)^g,$$

et si C est une courbe de E^g qui n'est pas la translatée d'une courbe elliptique par un point de torsion, on a :

$$|C_{\mathrm{tors}}| \leq 4^{e^{2\cdot 10^{10}} g \cdot \left([K:\mathbb{Q}] \max\{1, h_F(E), \log[K:\mathbb{Q}]\}\right)^{12395}}.$$

Cas des variétés abéliennes CM. On suppose que A est de type CM. Si V est une sous-variété de A, le nombre de sous-variétés maximales est borné en utilisant le Théorème 5.3 :

$$T(V) \leq 16^{[K:\mathbb{Q}] \cdot 3^{5g^2}} \delta(V)^g.$$

Si C est une courbe de A qui n'est pas la translatée d'une courbe elliptique par un point de torsion, on a :

$$|C_{\mathrm{tors}}| \leq 4^{[K:\mathbb{Q}] \cdot 3^{5g^2}}.$$

On pourra comparer avec les bornes classiques données par Coleman ([**5**]) et Buium ([**4**]).

5.3. L'effectivité dans le problème de Manin-Mumford. — Le principe central pour résoudre effectivement un problème diophantien consiste à trouver des bornes calculables pour la hauteur de Weil et le degré de ses solutions.

Concernant le problème de Manin-Mumford, c'est théoriquement possible. Expliquons le cas d'une courbe C plongée dans sa jacobienne J, de dimension g et définie sur K. La hauteur de Weil d'un point de torsion $x \in J(\bar{K})$ est bornée de façon totalement explicite. En effet, sa hauteur canonique est nulle et la différence entre les deux hauteurs est contrôlée par les travaux de Manin et Zarhin (voir par exemple [**7**], Proposition 3.9). On obtient :

$$h(x) = \left|h(x) - \hat{h}(x)\right| \leq 4^{g+1} h_F(A) + 3g \log(2).$$

D'autre part, on peut borner le nombre de points de torsion de C en fonction de g, $h_F(J)$ et Δ_K. Notons $\mathrm{Reg}(J)$ le régulateur de J, c'est-à-dire le produit des normes des idéaux premiers de mauvaise réduction de J. En combinant [**25**], (3.9) avec [**23**], Theorem 1.1 et le théorème de Minkowski, on peut trouver un premier $p \in \mathcal{P}$ qui ne divise pas $(2g+1) \cdot \Delta_K \cdot \mathrm{Reg}(J)$ et vérifiant :

$$p \leq (12g)^{25 g^{12 g^{4g}}} \max\left\{1, \log \Delta_K, h_F(J)\right\}^2.$$

Le théorème principal de [**4**] donne alors :

$$|C_{\mathrm{tors}}| \leq (12g)^{26g^{12g^{4g}}} \max\left\{1, \log \Delta_K, h_F(J)\right\}^{8g+4}.$$

On peut ensuite majorer le degré d'un point de torsion en remarquant que si $x \in C_{\mathrm{tors}}$, on a encore $x^\sigma \in C_{\mathrm{tors}}$ pour tout $\sigma \in G_K$. Il suit :

$$[\mathbb{Q}(x) : \mathbb{Q}] \leq [K : \mathbb{Q}] \cdot |C_{\mathrm{tors}}|.$$

Les coordonnées projectives des points de torsion recherchés sont alors les solutions d'un nombre fini d'équations algébriques à coefficients entiers, dont les coefficients sont explicitement bornés. Si on dispose de bornes calculables pour le nombre de translatés de torsion maximaux d'une sous-variété de A, on peut par le même procédé déterminer explicitement ces translatés.

Références

[1] F. Beukers & C. Smyth – « Cyclotomic points on curves », *Number Theory for the millenium, I* (2002), p. 67–85.

[2] F. Bogomolov – « Sur l'algébricité des représentations l-adiques », *C. R. Acad. Sci. Paris* **290** (1980), no. 15, p. 701–703.

[3] A. Borel – *Linear algebraic groups*, Grad. Texts in Math., Springer, 1969.

[4] A. Buium – « Geometry of p-jets », *Duke Math. J.* **82** (1996), p. 349–367.

[5] R. Coleman – « Torsion points on curves and p-adic abelian integrals », *Ann. of Math.* **121** (1985), p. 111–168.

[6] A. David – « Borne uniforme pour les homothéties dans l?image de Galois associée aux courbes elliptiques », *J. Number Theory* (2011), p. 2175–2191.

[7] S. David & P. Philippon – « Minoration des hauteurs normalisées des sous-variétés de variétés abéliennes II », *Comment. Math. Helv.* **77** (2002), p. 639–700.

[8] P. Deligne – *Hodge cycles on abelian varieties*, Lecture Notes in Math., vol. 900, Springer, 1982.

[9] M. Demazure & A. Grothendieck – *Structure des schémas en groupes réductifs, SGA 3, III*, Lecture Notes in Math., vol. 153, Springer, 1970.

[10] C. Eckstein – « Homothéties, à chercher dans l'action de Galois sur des points de torsion », *Thèse de Doctorat, Université de Strasbourg* (2005).

[11] A. Galateau & C. Martinez – « A bound for the torsion on subvarieties of abelian varieties », *Prépublication* (2017).

[12] É. Gaudron & G. Rémond – « Polarisations et isogénies », *Duke Math. J.* **163** (2014), no. 11, p. 2057–2108.

[13] A. Grothendieck – *Groupes de monodromie en géométrie algébrique, SGA 7, I*, Lecture Notes in Math., vol. 288, Springer, 1972.

[14] M. Hindry – « Autour d'une conjecture de Serge Lang », *Invent. Math.* **94** (1988), p. 575–603.

[15] S. Lang – « Division points on curves », *Ann. Mat. Pura Appl.* **70** (1965), no. 1.

[16] D. Lombardo – « Bounds for serre's open image theorem for elliptic curves over number fields », *Algebra Number Theory* **9-10** (2015), p. 2347–2395.

[17] ———, « Explicit surjectivity for galois representations attached to abelian surfaces », *J. Algebra* **460** (2016), p. 26–59.

[18] M. Marshall – « Ramification groups of abelian local field extensions », *Can. J. Math.* **23** (1971), no. 2.

[19] D. Masser & G. Wüstholz – « Refinements of the Tate conjecture for abelian varieties », *Abelian Varieties : Proceedings of the International Conference held in Egloffstein, Germany, October 3-8, 1993* (1995), p. 211–224.

[20] E. Maus – « On the jumps in the series of ramifications groups », *Mém. Soc. Math. Fr.* **25** (1971), p. 127–133.

[21] H. Miki – « On the ramification numbers of cyclic p-extensions over local fields », *J. Reine Angew. Math* **328** (1981), p. 99–115.

[22] F. Momose – « Isogenies of prime degree over number fields », *Compos. Math* **97** (1995), no. 3, p. 329–348.

[23] F. Pazuki – « Heights, ranks and regulators of abelian varieties », *Ramanujan Math. Soc. Lecture Note Series* **26** (2016).

[24] M. Raynaud – « Sous-variétés d'une variété abélienne et points de torsion », *Prog. Math.* **35** (1983), p. 327–352.

[25] G. Rosser & L. Schoenfeld – « Approximate formulas for some functions of prime numbers », *Illinois J. Math.* **6** (1962), no. 1, p. 64–94.

[26] J.-P. Serre – *Corps locaux*, Hermann, Paris, 1962.

[27] ———, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.

[28] ———, « Représentations ℓ-adiques », *Kyoto Symposium on Algebraic Number Theory* (1977), p. 177–193.

[29] ———, *Oeuvres, Collected papers, IV*, Springer-Verlag, Berlin, 1985-1998.

[30] ———, « Un critère d'indépendance pour une famille de représentations ℓ-adiques », *Comment. Math. Helv.* **88** (2013), p. 541–554.

[31] I. R. Shafarevich – *Basic algebraic geometry. 1*, second éd., Springer-Verlag, Berlin, 1994.

[32] J. Tate – « p-Divisible Groups », *Proceedings of a Conference on Local Fields* (1967), p. 158–183.

[33] J. Wintenberger – « Démonstration d'une conjecture de Lang dans des cas particuliers », *J. Reine Angew. Math.* **553** (2002), p. 1–16.

[34] ———, « Une extension de la théorie de la multiplication complexe », *J. Reine Angew. Math.* **552** (2002), p. 1–14.

[35] D. Zywina – « An effective open image theorem for abelian varieties », *Prépublication* (2019).

Aurélien Galateau, Université de Cergy-Pontoise • *E-mail :* aurelien.galateau@u-cergy.fr
César Martínez, Universität Regensburg • *E-mail :* cesar.martinez@ur.de