TORSION DES VARIÉTÉS ABÉLIENNES CM

ÉRIC GAUDRON ET GAËL RÉMOND

Abstract. In this note, we improve on a result of Silverberg giving an upper bound for the order of a rational torsion point on a CM abelian variety over a number field in terms of the degree of the field and the dimension of the variety. The proof uses the main theorem of complex multiplication and class field theory.

1. Résultats

Dans cet article, nous majorons l'ordre d'un point de torsion d'une variété abélienne CM en fonction de la dimension de la variété abélienne et du degré d'un corps de définition de la variété et du point. Les résultats obtenus améliorent ceux démontrés par Silverberg en 1988 [S1].

Lorsque A est une variété abélienne sur un corps K, on dit que A est complètement CM ou CCM si A est CM au sens usuel ($\mathrm{End}(A_{\overline{K}})\otimes_{\mathbb{Z}}\mathbb{Q}$ contient une $\mathbb{Q}$-algèbre commutative de dimension $2\dim A$) et si $\mathrm{End}(A)=\mathrm{End}(A_{\overline{K}})$. Nous désignons par φ la fonction indicatrice d'Euler.

Théorème 1. *Soit A une variété abélienne de dimension g sur un corps de nombres K. On note N l'exposant du groupe des points de torsion $A(K)_{\mathrm{tors}}$ et μ le nombre de racines de l'unité dans le centre de* $\mathrm{End}(A)$. *Alors :*

(1) *si A est CCM, $\varphi(N)$ divise $\mu[K:\mathbb{Q}]/2$;*
(2) *si A est CM, $\varphi(N)\leq c(g)6^g g![K:\mathbb{Q}]$ où*

$$c(2)=c(5)=4/3,\quad c(4)=5,\quad c(6)=7/6$$

et $c(g)=1$ sinon.

À titre de comparaison, sous les hypothèses de (1), le résultat de Silverberg (voir [S1, corollaire 2]) donne

$$\varphi(N)\leq 2^{(g-1)\nu(N)+1}\mu[K:\mathbb{Q}]$$

où $\nu(N)$ est le nombre de diviseurs premiers de N. Dans le cadre de (2), la majoration annoncée (voir [S1, corollaire 6]) s'écrit

$$\varphi(N)\leq 2^{(g-1)\nu(N)+1}12^g g![K:\mathbb{Q}]$$

mais la déduction de cette formule à partir de la première semble comporter une faute (voir ci-dessous, après la démonstration du théorème 1). Ici nous employons une variante de l'argument de Silverberg pour établir (1) tandis que pour passer de (1) à (2) nous invoquons les résultats de [Ré].

Notons que, dans le cas particulier $g=1$, le théorème 1 correspond aux bornes données par Silverberg dans un autre texte (voir [S2, corollaire 6.1]). Notre résultat apparaît donc comme une généralisation de ce raffinement en dimension supérieure.

Par définition de l'exposant, le groupe $A(K)_{\mathrm{tors}}$ est inclus dans l'ensemble des points de N-torsion de A, de cardinal N^{2g}. Ainsi le théorème fournit une borne pour $\mathrm{Card}\,A(K)_{\mathrm{tors}}$ qui améliore la version explicite de la conjecture de torsion uniforme dans le cas CM que l'on peut déduire du travail de Silverberg. Dans le résultat suivant, nous présentons une majoration un peu plus fine de ce cardinal lorsque A est isotypique, c'est-à-dire isogène à une puissance d'une variété abélienne simple.

Théorème 2. *Soit A une variété abélienne de dimension g sur un corps de nombres K. On note X le plus grand entier tel que $\varphi(X)\leq[K:\mathbb{Q}]$. Si A est isotypique et CCM alors* $\mathrm{Card}\,A(K)_{\mathrm{tors}}\leq X^{2g}$.

MSC 2010 : 11G10 (11G15, 14G05, 14K22).
Mots-clefs : Variété abélienne CM, point de torsion, théorème fondamental de la multiplication complexe, corps de classes.
Date: 11 juillet 2017.

Dans la pratique, on peut ensuite combiner ces énoncés avec des estimations pour l'indicatrice d'Euler comme par exemple : $n \leq \max(2, \varphi(n)^3)$, $n \leq \max(6, \varphi(n)^2)$, $n \leq \max(42, \varphi(n)^{3/2})$ ou bien encore $n \leq 3\varphi(n)\max(1, \log\varphi(n))$, valides pour tout entier $n \geq 1$. Ces bornes se déduisent de la majoration

$$\forall\, n \geq 3, \quad \frac{n}{\varphi(n)} < e^{\gamma}\log\log n + \frac{2,51}{\log\log n}$$

(γ est la constante d'Euler, voir [RS, (3.42)]) et de vérifications numériques pour les petites valeurs de n. Cette formule permet aussi de montrer que, dans l'énoncé du théorème 2, nous avons $X \leq 10[K:\mathbb{Q}]|\log\log[K:\mathbb{Q}]|$ (car $[K:\mathbb{Q}]$ est pair).

Mettons à présent en perspective nos énoncés avec d'autres résultats, postérieurs à ceux de Silverberg. Tout d'abord, Clark et Xarles ont établi une borne de la forme

$$\operatorname{Card} A(K)_{\mathrm{tors}} \leq B(g, [K:\mathbb{Q}])$$

valable pour toute variété abélienne CM (et, en fait, sous une hypothèse de réduction bien plus faible, voir le corollaire 1.2 de [CX]) où la fonction explicite B vérifie en particulier

$$6^{g[K:\mathbb{Q}]} < B(g, [K:\mathbb{Q}]) \leq \left(6 + \frac{29}{[K:\mathbb{Q}]}\right)^{g[K:\mathbb{Q}]}.$$

Dans le cas où A est isotypique et complètement CM, la majoration du théorème 2 est toujours meilleure que $B(g, [K:\mathbb{Q}])$ car nous avons facilement $X \leq \sqrt{6}^{[K:\mathbb{Q}]}$. D'un autre côté, ce même théorème nous donne

$$\operatorname{Card} A(K)_{\mathrm{tors}} \leq (10[K:\mathbb{Q}]\log\log[K:\mathbb{Q}])^{2g}$$

tandis que le résultat elliptique de Clark et Pollack montre que si A est de la forme E^g alors

$$\operatorname{Card} A(K)_{\mathrm{tors}} \leq \left|c[K:\mathbb{Q}]\log\log[K:\mathbb{Q}]\right|^g$$

pour un réel $c > 0$ (calculable) et ceci est optimal à la valeur de c près (voir [CP]). Bien entendu, dans le cas CM général, les bornes déduites du théorème 1 sont de moins bonne qualité en g à cause de la présence de $g!$; la dépendance en $[K:\mathbb{Q}]$ reste en revanche polynomiale (contrairement à $B(g, [K:\mathbb{Q}])$).

Pour les démonstrations de nos théorèmes, le point de départ est, comme dans l'article [S1] de Silverberg, le théorème fondamental de la multiplication complexe couplé à la théorie du corps de classes. Ces ingrédients sont au cœur de l'énoncé technique de la deuxième partie.

2. Proposition clef

Si R est un anneau, on désigne par $Z(R) = \{r \in R\,;\ \forall\, s \in R,\ rs = sr\}$ son centre et par $R^{\times}$ son groupe des unités.

Proposition. *Soient A une variété abélienne sur un corps de nombres K et N l'exposant du groupe $A(K)_{\mathrm{tors}}$. Si A est CCM alors il existe un sous-groupe fini G de $Z(\operatorname{End} A)^{\times}$ et un morphisme $\alpha\colon G \to (\mathbb{Z}/N\mathbb{Z})^{\times}$ tels que*

$$\varphi(N) \mid \frac{1}{2}[K:\mathbb{Q}]\operatorname{Card}\alpha(G)$$

et, en notant $\pi\colon \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ la surjection canonique, pour tout couple $(\zeta, a) \in G \times \mathbb{Z}$ avec $\alpha(\zeta) = \pi(a)$ on a $(\zeta - a)A(K)_{\mathrm{tors}} = \{0\}$.

Démonstration.

1. Considérons une isogénie (sur K) entre A et un produit $\prod_{i=1}^{t} A_i^{n_i}$ où les A_i sont des variétés abéliennes simples deux à deux non isogènes et les n_i des entiers naturels non nuls. Puisque A est CCM, chaque A_i est géométriquement simple et CCM ; en particulier $E_i = (\operatorname{End} A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ est un corps CM. Fixons un plongement de K dans $\mathbb{C}$ et notons A_i la variété abélienne complexe déduite de A_i *via* ce plongement. La structure complexe de A_i munit E_i d'un type CM Φ_i. Notons $(\widetilde{E}_i, \widetilde{\Phi}_i)$ le couple réflexe de (E_i, Φ_i) (voir [Sh, p. 62]) et $\eta_i\colon \widetilde{E}_i \to E_i$ la norme de type associée à $\widetilde{\Phi}_i$, c'est-à-dire, pour $x \in \widetilde{E}_i$, $\eta_i(x) = \prod_{\sigma\in\widetilde{\Phi}_i}\sigma(x)$ lorsque $\widetilde{\Phi}_i$ est vu comme partie de $\operatorname{Hom}(\widetilde{E}_i, \mathbb{C})$. Dans la suite, nous aurons seulement besoin de connaître l'action de η_i sur les éléments totalement réels. Lorsque F est un corps CM, nous notons systématiquement F^+ son sous-corps totalement réel maximal (donc $[F : F^+] = 2$). Les plongements de $\widetilde{\Phi}_i$ induisent l'ensemble des plongements

complexes de $\widetilde{E}_i^+$ et, en particulier, si $x \in \widetilde{E}_i^+$ l'élément $\eta_i(x)$ est la norme $N_{\widetilde{E}_i^+/\mathbb{Q}}(x)$ de x relative à l'extension $\widetilde{E}_i^+/\mathbb{Q}$. Désignons maintenant par $\widetilde{E}$ le compositum des $\widetilde{E}_i$, qui est encore un corps CM, et par η l'application $\widetilde{E} \to \prod_{i=1}^t E_i$ qui à $x \in \widetilde{E}$ associe le vecteur

$$\eta(x) = \left(\eta_i\left(N_{\widetilde{E}/\widetilde{E}_i}(x)\right)\right)_{1\le i\le t}.$$

Comme $\widetilde{E}^+ \cap \widetilde{E}_i = \widetilde{E}_i^+$, si $x \in \widetilde{E}^+$ nous avons $N_{\widetilde{E}/\widetilde{E}_i}(x) = N_{\widetilde{E}^+/\widetilde{E}_i^+}(x)$ et la restriction de η à $\widetilde{E}^+$ est simplement la norme $N_{\widetilde{E}^+/\mathbb{Q}}$ suivie de l'injection diagonale $\mathbb{Q} \hookrightarrow \prod_{i=1}^t E_i$. L'application η induit un morphisme de groupes $\widetilde{E}^\times \to \prod_{i=1}^t E_i^\times$ qui s'étend en un morphisme $\mathbb{A}_{\widetilde{E}}^\times \to \prod_{i=1}^t \mathbb{A}_{E_i}^\times$ sur les idèles que l'on notera encore η. Soit t_{A} l'espace tangent à l'origine de la variété abélienne complexe A induite par A et le plongement $K \hookrightarrow \mathbb{C}$ fixé. Un élément de $\mathrm{End}(\mathsf{A}) = \mathrm{End}\, A$ s'identifie à un endomorphisme de t_{A} qui stabilise le réseau des périodes Ω_{A} de A. Par le choix de l'isogénie initiale, le produit $\prod_{i=1}^t E_i$, vu comme centre du produit d'anneaux de matrices $\prod_{i=1}^t M_{n_i}(E_i) = \mathrm{End}(\prod_{i=1}^t A_i^{n_i}) \otimes_{\mathbb{Z}} \mathbb{Q}$, agit sur t_{A} et le centre de $\mathrm{End}\, A$ s'identifie alors aux éléments $q \in \prod_{i=1}^t E_i$ tels que $q\Omega_{\mathsf{A}} \subset \Omega_{\mathsf{A}}$. Comme dernières notations, nous écrirons encore Ω' le sous-groupe de t_{A} contenant Ω_{A} tel que $A(K)_{\mathrm{tors}} = \Omega'/\Omega_{\mathsf{A}}$ et, pour $c \in \mathbb{A}_{\widetilde{E}}^\times$, le nombre rationnel $N(c)$ sera la norme de l'idéal fractionnaire de $\widetilde{E}$ défini par la partie ultramétrique de c.

2. La théorie du corps de classes associe au sous-groupe ouvert S de $\mathbb{A}_{\widetilde{E}}^\times$ défini par

$$S = \left\{ c \in \mathbb{A}_{\widetilde{E}}^\times ;\ \exists\, q \in \prod_{i=1}^t E_i^\times,\ q\overline{q}N(c) = 1,\ q\eta(c)\Omega_{\mathsf{A}} = \Omega_{\mathsf{A}} \text{ et } (q\eta(c)-1)\Omega' \subset \Omega_{\mathsf{A}} \right\}$$

une extension abélienne finie K_a de $\widetilde{E}$ de groupe de Galois isomorphe au groupe quotient $\mathbb{A}_{\widetilde{E}}^\times/S$ (voir [Ch, p. 135], on vérifie $\widetilde{E}^\times \subset S$ en choisissant $q = \eta(c)^{-1}$ lorsque $c \in \widetilde{E}^\times$). Une conséquence du théorème fondamental de la multiplication complexe de Shimura (voir [S1, p. 244], avec des notations un peu différentes) affirme que cette extension K_a est le corps de modules pour les données $(A, \mathcal{L}, \iota, a_1, \ldots, a_s)$ où $\mathcal{L}$ est une polarisation sur A, ι l'isomorphisme $\prod_{i=1}^t M_{n_i}(E_i) \to (\mathrm{End}\, A) \otimes_{\mathbb{Z}} \mathbb{Q}$ donné par l'isogénie fixée au départ et $a_1, \ldots, a_s$ des générateurs de $A(K)_{\mathrm{tors}}$. Ici, nous retenons seulement $K_a \subset K$ puisque K est un corps de définition pour tous ces objets (voir [Sh, Proposition 17.2]). Ainsi $\widetilde{E} \subset K$ et $\mathrm{Card}\, \mathbb{A}_{\widetilde{E}}^\times/S = [K_a : \widetilde{E}]$ divise $[K : \widetilde{E}]$. Soit $N_{\mathbb{Q}} \colon \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{Q}^\times$ l'application définie pour $\mathbb{Q}$ comme N pour $\widetilde{E}$. Si $c \in \mathbb{A}_{\widetilde{E}}^\times$ on a la relation $N(c) = N_{\mathbb{Q}}(N_{\widetilde{E}/\mathbb{Q}}(c))$ et donc, si $c \in \mathbb{A}_{\widetilde{E}^+}^\times$, on a $N(c) = N_{\mathbb{Q}}(N_{\widetilde{E}^+/\mathbb{Q}}(c))^2$. Lorsque $c \in \mathbb{A}_{\widetilde{E}^+}^\times$ les conditions apparaissant dans S ne dépendent que de $\eta(c) = N_{\widetilde{E}^+/\mathbb{Q}}(c)$ si bien que l'intersection $S \cap \mathbb{A}_{\widetilde{E}^+}^\times$ peut s'écrire $N_{\widetilde{E}^+/\mathbb{Q}}^{-1}(T)$ où $N_{\widetilde{E}^+/\mathbb{Q}} : \mathbb{A}_{\widetilde{E}^+}^\times \to \mathbb{A}_{\mathbb{Q}}^\times$ est l'application qui prolonge la norme de $\widetilde{E}^+/\mathbb{Q}$ aux idèles et

$$T = \left\{ c \in \mathbb{A}_{\mathbb{Q}}^\times ;\ \exists\, q \in \prod_{i=1}^t E_i^\times,\ q\overline{q}N_{\mathbb{Q}}(c)^2 = 1,\ qc\,\Omega_{\mathsf{A}} = \Omega_{\mathsf{A}} \text{ et } (qc-1)\Omega' \subset \Omega_{\mathsf{A}} \right\}.$$

Considérons la suite exacte

$$0 \longrightarrow \mathbb{A}_{\widetilde{E}^+}^\times/S \cap \mathbb{A}_{\widetilde{E}^+}^\times \xrightarrow{N_{\widetilde{E}^+/\mathbb{Q}}} \mathbb{A}_{\mathbb{Q}}^\times/T \longrightarrow \mathbb{A}_{\mathbb{Q}}^\times/T.N_{\widetilde{E}^+/\mathbb{Q}}(\mathbb{A}_{\widetilde{E}^+}^\times) \longrightarrow 0.$$

Si $c \in \mathbb{Q}^\times$ son inverse $q = c^{-1}$ satisfait les conditions qui définissent T donc $\mathbb{Q}^\times \subset T$. Ainsi le dernier terme de la suite exacte est un quotient de $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times N_{\widetilde{E}^+/\mathbb{Q}}(\mathbb{A}_{\widetilde{E}^+}^\times)$ qui, par la théorie du corps de classes, s'identifie au groupe de Galois de l'extension abélienne maximale M de $\mathbb{Q}$ contenue dans $\widetilde{E}^+$ (voir [Ch, Théorème 5.1]). Nous en déduisons que le cardinal de $\mathbb{A}_{\mathbb{Q}}^\times/T$ divise

$$\mathrm{Card}(\mathbb{A}_{\widetilde{E}}^\times/S)\,\mathrm{Card}(\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times N_{\widetilde{E}^+/\mathbb{Q}}(\mathbb{A}_{\widetilde{E}^+}^\times)) = [K_a : \widetilde{E}][M : \mathbb{Q}],$$

quantité qui, elle-même, divise $[K : \widetilde{E}][\widetilde{E}^+ : \mathbb{Q}] = [K : \mathbb{Q}]/2$.

3. Passons maintenant à la construction du groupe G et du morphisme α. Considérons le groupe

$$\mathcal{T} = \left\{ (q,c) \in \left(\prod_{i=1}^{t} E_i^\times \right) \times \mathbb{A}_\mathbb{Q}^\times \,;\; q\overline{q} = 1,\; q\frac{c}{N_\mathbb{Q}(c)}\Omega_\mathsf{A} = \Omega_\mathsf{A} \text{ et } \left(q\frac{c}{N_\mathbb{Q}(c)} - 1 \right) \Omega' \subset \Omega_\mathsf{A} \right\}.$$

L'image de $\mathcal{T}$ par la projection sur le facteur $\mathbb{A}_\mathbb{Q}^\times$ est égale à T comme on le voit en remplaçant q par $qN_\mathbb{Q}(c)^{-1}$ dans la définition de T. De plus, pour chaque nombre premier p, la p-composante de $c/N_\mathbb{Q}(c)$ est un inversible de $\mathbb{Z}_p$ et donc $\frac{c}{N_\mathbb{Q}(c)}\Omega_\mathsf{A} = \Omega_\mathsf{A}$, ce qui permet d'écrire

$$\mathcal{T} = \left\{ (q,c) \in \left(\prod_{i=1}^{t} E_i^\times \right) \times \mathbb{A}_\mathbb{Q}^\times \,;\; q\overline{q} = 1,\; q\Omega_\mathsf{A} = \Omega_\mathsf{A} \text{ et } \left(q\frac{c}{N_\mathbb{Q}(c)} - 1 \right) \Omega' \subset \Omega_\mathsf{A} \right\}.$$

Comme le $\mathbb{Z}$-module Ω_A est de rang fini, la condition $q\Omega_\mathsf{A} = \Omega_\mathsf{A}$ entraîne que les composantes $q_1, \dots, q_t$ de q sont des entiers algébriques. Si l'on a de plus la condition $q\overline{q} = 1$ alors la relation $q_i\overline{q_i} = 1$ force q_i à être une racine de l'unité car, les plongements $\sigma\colon E_i \hookrightarrow \mathbb{C}$ commutant avec la conjugaison complexe (E_i est un corps CM), on a $|\sigma(q_i)| = 1$ pour tout σ. Comme q_i appartient à un corps de nombres fixé, il n'y a qu'un nombre fini de possibilités. La projection

$$G = \left\{ q \in \prod_{i=1}^{t} E_i^\times \,;\; \exists\, c \in \mathbb{A}_\mathbb{Q}^\times,\; q\overline{q} = 1,\; q\Omega_\mathsf{A} = \Omega_\mathsf{A} \text{ et } \left(q\frac{c}{N_\mathbb{Q}(c)} - 1 \right) \Omega' \subset \Omega_\mathsf{A} \right\}$$

de $\mathcal{T}$ sur le produit des $E_i^\times$ est donc un groupe fini qui peut être vu comme un sous-groupe de $Z(\operatorname{End} A)^\times$. Notons $\mathcal{T}_1 = \mathcal{T} \cap (\{1\} \times \mathbb{A}_\mathbb{Q}^\times)$ le noyau de la projection $\mathcal{T} \to G$ et $T_1 \simeq \mathcal{T}_1$ son image dans T. Explicitement, nous avons

$$T_1 = \left\{ c \in \mathbb{A}_\mathbb{Q}^\times \,;\; \left(\frac{c}{N_\mathbb{Q}(c)} - 1 \right) \Omega' \subset \Omega_\mathsf{A} \right\}$$

ou encore, grâce à l'égalité $\{n \in \mathbb{Z} \,;\; n\Omega' \subset \Omega_\mathsf{A}\} = N\mathbb{Z}$,

$$T_1 = \left\{ c \in \mathbb{A}_\mathbb{Q}^\times \,;\; \text{pour tout nombre premier } p \text{ divisant } N,\; \frac{c_p}{N_\mathbb{Q}(c)} \in 1 + N\mathbb{Z}_p \right\}$$

(c_p est la p-composante de c). Ainsi le quotient $\mathbb{A}_\mathbb{Q}^\times / T_1$ est un groupe isomorphe au produit $\prod_{p|N} \mathbb{Z}_p^\times / (1 + N\mathbb{Z}_p)$, lui-même isomorphe à $(\mathbb{Z}/N\mathbb{Z})^\times$. Nous pouvons donc former un diagramme commutatif à lignes exactes

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{T}_1 & \longrightarrow & \mathcal{T} & \longrightarrow & G & \longrightarrow & 0 \\
 & & | \wr & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T_1 & \longrightarrow & T & \longrightarrow & T/T_1 & \longrightarrow & 0 \\
 & & || & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T_1 & \longrightarrow & \mathbb{A}_\mathbb{Q}^\times & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^\times & \longrightarrow & 0.
\end{array}$$

Notons β le morphisme de groupes $G \to (\mathbb{Z}/N\mathbb{Z})^\times$ ainsi obtenu et définissons α par $\alpha(q) = \beta(q^{-1})$ si $q \in G$. Les flèches verticales sont surjectives entre les deux premières lignes, injectives entre la deuxième et la troisième. En particulier, $\beta(G) = \alpha(G) \simeq T/T_1$ et donc

$$\varphi(N) = \operatorname{Card} \mathbb{A}_\mathbb{Q}^\times / T_1 = \operatorname{Card} \alpha(G) \cdot \operatorname{Card} \mathbb{A}_\mathbb{Q}^\times / T.$$

Ceci donne la relation de divisibilité de l'énoncé puisque nous avons déjà vu que le cardinal de $\mathbb{A}_\mathbb{Q}^\times / T$ divisait $[K : \mathbb{Q}]/2$. De plus, si $(\zeta, a) \in G \times \mathbb{Z}$ satisfait $\alpha(\zeta) = \pi(a)$, choisissons $c \in \mathbb{A}_\mathbb{Q}^\times$ avec $c_p = 1$ si $p \nmid N$ et $c_p = a$ si $p \mid N$. Nous avons alors $N_\mathbb{Q}(c) = 1$ puisque a est premier à N et l'image de c dans $(\mathbb{Z}/N\mathbb{Z})^\times$ coïncide avec $\pi(a) = \beta(\zeta^{-1})$. Le diagramme montre $(\zeta^{-1}, c) \in \mathcal{T}$. Ceci entraîne $(\zeta^{-1}c - 1)\Omega' \subset \Omega_\mathsf{A}$ et donc $\zeta^{-1}a - 1$ s'annule sur $A(K)_{\text{tors}}$. Il en va de même de $a - \zeta$ en composant avec l'automorphisme ζ. □

Le point crucial de cette démonstration consiste à remplacer $\mathbb{A}_E^\times / S$ par $\mathbb{A}_{\widetilde{E}^+}^\times / S \cap \mathbb{A}_{\widetilde{E}^+}^\times$ alors que la preuve de Silverberg revient à le remplacer par $\mathbb{A}_\mathbb{Q}^\times / S \cap \mathbb{A}_\mathbb{Q}^\times$.

3. Démonstrations des théorèmes

Démonstration du théorème 1. L'assertion (1) découle directement de la proposition puisque G est un sous-groupe des racines de l'unité du centre de $\mathrm{End}\, A$ et donc $\mathrm{Card}\, G$ divise μ. Pour la seconde assertion, considérons l'extension K_A/K de degré minimal telle que $\mathrm{End}\, A_{\overline{K}} = \mathrm{End}\, A_{K_A}$. Ainsi A_{K_A} est CCM et N divise l'exposant de $A_{K_A}(K_A)_{\mathrm{tors}}$ donc, par (1), $\varphi(N)$ divise $\mu[K_A : \mathbb{Q}]/2$. On conclut en utilisant le théorème 1.4 de [Ré] qui permet de majorer $\mu[K_A : K]$ par $2c(g)6^g g!$. □

Signalons que la majoration tirée de [Ré] et utilisée ci-dessus est optimale (à g fixé) même lorsqu'on la restreint aux variétés abéliennes CM. De son côté, l'argument employé par Silverberg fait apparaître une extension de corps de degré au plus $2^g g!$ mais il repose sur un énoncé (le lemme 6 de [S1]) qui est erroné comme le montre l'exemple suivant : soient E une courbe elliptique CM sur $\overline{\mathbb{Q}}$, $F = (\mathrm{End}\, E) \otimes \mathbb{Q}$, $g = [\mathbb{Q}(j(E)) : \mathbb{Q}]$ et $E_1 = E, \ldots, E_g$ les conjuguées de E. La variété abélienne $A = E_1 \times \cdots \times E_g$ sur $\overline{\mathbb{Q}}$ provient d'une variété abélienne sur $\mathbb{Q}$ (la restriction des scalaires de Weil de E dans l'extension $\mathbb{Q}(j(E))/\mathbb{Q}$). Notons ensuite θ l'injection naturelle de $F^g = \prod_{i=1}^g (\mathrm{End}\, E_i) \otimes \mathbb{Q}$ dans $(\mathrm{End}\, A) \otimes \mathbb{Q}$ (ici isomorphe à $M_g(F)$) c'est-à-dire que par exemple $\theta(1, 0, \ldots, 0)$ est le projecteur de $\mathrm{End}\, A$ d'image $E \times \{0\} \times \ldots \{0\}$. Le lemme 6 sus-cité affirme que le couple (A, θ) est défini sur F : si cela était vrai, nous aurions une variété abélienne sur F munie d'un endomorphisme dont l'extension à $\overline{\mathbb{Q}}$ serait le projecteur $\theta(1, 0, \ldots, 0)$ ci-dessus. L'image de cet endomorphisme serait donc une courbe elliptique sur F dont l'extension serait E. Par suite nous aurions $j(E) \in F$ et ceci est absurde dès que l'on choisit $g \geq 3$.

Démonstration du théorème 2. Comme dans la démonstration de la proposition, fixons un plongement $K \hookrightarrow \mathbb{C}$ et notons A la variété abélienne complexe obtenue à partir de A par extension des scalaires. Identifions $A(K)_{\mathrm{tors}}$ au quotient $\Omega'/\Omega_{\mathsf{A}}$ de $\mathrm{End}\, A$-modules. Comme A est isotypique, le centre de $(\mathrm{End}\, A) \otimes \mathbb{Q}$ est un corps (CM). Le groupe G de la proposition, composé de racines de l'unité de ce corps, est cyclique. Par suite, le sous-anneau $\mathcal{O} = \mathbb{Z}[G]$ engendré par G est l'anneau des entiers d'un sous-corps cyclotomique k de $(\mathrm{End}\, A) \otimes \mathbb{Q}$. Les modules Ω_{A} et Ω' sont deux $\mathcal{O}$-modules sans torsion. L'anneau $\mathcal{O}$ étant de Dedekind, on peut écrire dans une base adaptée de $\Omega_{\mathsf{A}} \otimes \mathbb{Q}$ sur k : $\Omega' = \bigoplus_{i=1}^m I_i'$ et $\Omega_{\mathsf{A}} = \bigoplus_{i=1}^m I_i$ où les $I_i \subset I_i'$ sont des idéaux fractionnaires de k et $m = \dim_k \Omega_{\mathsf{A}} \otimes \mathbb{Q} = 2g/[k : \mathbb{Q}] = 2g/\varphi(\mathrm{Card}\, G)$ (voir [Re, p. 49]). Par ailleurs, si $J = \{x\,;\ x\Omega' \subset \Omega_{\mathsf{A}}\}$ est l'idéal de $\mathcal{O}$ des éléments annulant la torsion alors $JI_i' \subset I_i$ donc

$$\mathrm{Card}\, A(K)_{\mathrm{tors}} = \mathrm{Card}\, \Omega'/\Omega_{\mathsf{A}} = \prod_{i=1}^m \mathrm{Card}\, I_i'/I_i \leq (\mathrm{Card}\, \mathcal{O}/J)^m\,.$$

La fin de la proposition nous assure $G \subset \mathbb{Z} + J$ donc $\mathcal{O} = \mathbb{Z} + J$ puis $\mathcal{O}/J \simeq \mathbb{Z}/\mathbb{Z} \cap J = \mathbb{Z}/N\mathbb{Z}$. Le cardinal des points de torsion est donc majoré par N^m et il reste à voir $N^{1/\varphi(\mathrm{Card}\, G)} \leq X$. Cela résulte du lemme élémentaire suivant avec $n = \mathrm{Card}\, \alpha(G)$ et $D = [K : \mathbb{Q}]/2$ (en notant que $\varphi(n)$ divise $\varphi(\mathrm{Card}\, G)$). □

Lemme. *Soit $D \geq 1$ un entier. Soit X le plus grand entier tel que $\varphi(X) \leq 2D$. Alors, pour tous entiers naturels non nuls n et N vérifiant $n \mid \varphi(N) \mid nD$ on a $N^{1/\varphi(n)} \leq X$.*

Démonstration. Nous utilisons ici $x \leq \varphi(x)^2$ pour tout $x \in \mathbb{N} \setminus \{0, 2, 6\}$. Nous avons

$$\varphi(6D) = 6D \prod_{p \mid 6D} \left(1 - \frac{1}{p}\right) \leq 6D \prod_{p \mid 6} \left(1 - \frac{1}{p}\right) = 2D$$

donc $X \geq 6D$. Si $\varphi(n) = 1$ alors $n \in \{1, 2\}$ donc $\varphi(N) \leq 2D$ d'où $N^{1/\varphi(n)} = N \leq X$. Si $\varphi(n) = 2$ alors $n \in \{3, 4, 6\}$ et $N \notin \{0, 2, 6\}$ donc $N \leq \varphi(N)^2 \leq (nD)^2 \leq (6D)^2 \leq X^2 = X^{\varphi(n)}$. Comme $\varphi(n) = 3$ est impossible, nous pouvons supposer $\varphi(n) \geq 4$. On a alors $n, N \notin \{0, 2, 6\}$ donc $N \leq \varphi(N)^2 \leq (nD)^2 \leq \varphi(n)^4 D^2 \leq 4^{\varphi(n)} D^{\varphi(n)} \leq (6D)^{\varphi(n)} \leq X^{\varphi(n)}$. □

Remerciements. Le premier auteur remercie la région Auvergne de son aide financière apportée à travers le projet Diophante. Les auteurs ont bénéficié du soutien du projet ANR Gardio 14-CE25-0015.

Références

[Ch] N. Childress. *Class field theory*. Universitext, Springer New York, 2009.

[CP] P. Clark et P. Pollack. The truth about torsion in the CM case. *C. R. Math. Acad. Sci. Paris* 353 (2015), 683–688.

[CX] P. Clark et X. Xarles. Local bounds for torsion points on abelian varieties. *Canad. J. Math.* 60 (2008), 532–555.

[Re] I. Reiner. *Maximal orders*, volume 28 de *London Mathematical Society Monographs. New Series*. The Clarendon Press Oxford University Press. 2003.

[Ré] G. Rémond. Degré de définition des endomorphismes d'une variété abélienne. Prépublication, mars 2017. `https://www-fourier.ujf-grenoble.fr/~remond`

[RS] J. Rosser et L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.* 6 (1962), 64–94.

[Sh] G. Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 de *Princeton Mathematical Series*, Princeton university press, 1998.

[S1] A. Silverberg. Torsion points on abelian varieties of CM-type. *Compos. Math.* 68 (1988), 241–249.

[S2] A. Silverberg. Points of finite order on abelian varieties. *Contemp. Math.* 133 (1992), 175–193.

Éric Gaudron
Université Clermont Auvergne
CNRS, LMBP
F-63000 Clermont-Ferrand
France
`Eric.Gaudron@uca.fr`

Gaël Rémond
Institut Fourier, UMR 5582
CS 40700
38058 Grenoble Cedex 9
France
`Gael.Remond@univ-grenoble-alpes.fr`