Rev. Mat. Iberoam. **33** (2017), no. 4, 1173–1195
DOI 10.4171/RMI/967
© European Mathematical Society

Variétés abéliennes et ordres maximaux

Gaël Rémond

Abstract. We prove that an abelian variety whose endomorphism ring is a maximal order can be written as a direct product of simple factors with the same property, in which furthermore two isogenous factors have isomorphic nth powers for some n. Conversely every such product has a maximal order as endomorphism ring. We deduce from this some properties for arbitrary abelian varieties, in particular for almost complements of abelian subvarieties.

1. Introduction

Nous nous proposons ci-dessous de décrire aussi précisément que possible la structure des variétés abéliennes dont l'anneau des endomorphismes est un ordre maximal et d'en tirer quelques conséquences pour les variétés abéliennes quelconques.

Nous fixons un corps K et considérons des variétés abéliennes définies sur K. Nous ne faisons pas d'extensions de corps, c'est-à-dire que tous les morphismes, endomorphismes, isomorphismes, isogénies ou sous-variétés abéliennes seront toujours définis sur K. En particulier, si A et B désignent des variétés abéliennes (sur K), nous notons $\mathrm{Hom}(A,B)$ le groupe des (K-)morphismes de A vers B et $\mathrm{End}\,A$ l'anneau des (K-)endomorphismes de A. Ce dernier est un ordre, c'est-à-dire un anneau $\mathcal{O}$ qui est un $\mathbb{Z}$-module libre de rang fini. Un tel ordre est dit maximal s'il est maximal pour l'inclusion parmi les ordres sous-anneaux de l'algèbre $\mathcal{O}\otimes\mathbb{Q}$. Lorsqu'une $\mathbb{Q}$-algèbre $\mathfrak{A}$ (de dimension finie) est fixée, la locution *ordre de* $\mathfrak{A}$ désigne un ordre $\mathcal{O}$ sous-anneau de $\mathfrak{A}$ tel que $\mathcal{O}\otimes\mathbb{Q}=\mathfrak{A}$.

Nous montrons tout d'abord comment nous ramener au cas d'un ordre maximal.

Théorème 1.1. *Soient A une variété abélienne et N un entier non nul tel que $N^{-1}\,\mathrm{End}\,A$ contient un ordre maximal $\mathcal{O}$ de $(\mathrm{End}\,A)\otimes\mathbb{Q}$. Alors il existe une variété abélienne A' et deux isogénies $\varphi\colon A\to A'$ et $\psi\colon A'\to A$ de sorte que $\psi\circ\varphi=[N]$ et $\mathrm{End}\,A'\simeq\mathcal{O}$.*

Classification mathématique (2010) : Primaire 11G10; Secondaires 14K05, 16H10.
Mots-clefs : Variété abélienne, endomorphisme, ordre, ordre maximal.

Nous rappelons qu'un entier N comme ci-dessus existe toujours, par exemple puisque $\mathrm{End}\, A$ est contenu dans un ordre maximal $\mathcal{O}$ par le théorème 10.4 de [8] (on peut alors choisir $N = [\mathcal{O} : \mathrm{End}\, A]$).

Ce résultat permet de traduire les énoncés de structure sur A' en des versions (plus faibles) valables sur A. Par exemple, nous établirons le fait suivant.

Théorème 1.2. *Si* $\mathrm{End}\, A$ *est maximal alors toute sous-variété abélienne* B *est un facteur direct de* A *et son anneau d'endomorphismes* $\mathrm{End}\, B$ *est maximal.*

Dire que B est un facteur direct de A signifie bien entendu qu'il existe une seconde sous-variété abélienne B' de A telle que $B + B' = A$ et $B \cap B' = 0$.

Corollaire 1.3. *Soient* A *une variété abélienne et* N *un entier non nul tel que* $N^{-1}\,\mathrm{End}\, A$ *contient un ordre maximal de* $(\mathrm{End}\, A) \otimes \mathbb{Q}$. *Alors pour toute sous-variété abélienne* B *de* A *il existe une sous-variété abélienne* B' *de* A *telle que* $B + B' = A$ *et* $B \cap B' \subset \mathrm{Ker}[N]$. *De plus* $N^{-1}\,\mathrm{End}\, B$ *contient un ordre maximal de* $(\mathrm{End}\, B) \otimes \mathbb{Q}$.

Ce corollaire est une variante d'un résultat de Bertrand (voir [1] ainsi que le théorème 1.3 et la proposition 5.2 de [3]). Comme nous ne supposons pas K de caractéristique nulle, la formule $B \cap B' \subset \mathrm{Ker}[N]$ se comprend au sens schématique ($B \times_A B' \hookrightarrow A$ se factorise à travers $\mathrm{Ker}[N] \hookrightarrow A$).

Voici encore un énoncé que nous démontrerons par réduction au cas d'un ordre maximal.

Proposition 1.4. *Soient* A *une variété abélienne et* $b \geq 0$ *un entier. Il n'y a, à isomorphismes près, qu'un nombre fini de variétés abéliennes* B *de dimension* $\leq b$ *telles qu'il existe un entier* $n \geq 0$ *et une injection* $B \hookrightarrow A^n$.

En particulier, ceci contient le fait que les sous-variétés abéliennes de A ne parcourent qu'un nombre fini de classes d'isomorphie (voir [5]).

Revenons maintenant à la structure d'une variété abélienne A telle que $\mathrm{End}\, A$ est maximal. Une application itérée du théorème 1.2 entraîne que A est un produit de variétés abéliennes simples. Nous souhaitons à présent caractériser les produits ainsi obtenus. Une condition nécessaire est que chaque facteur ait un anneau d'endomorphismes maximal mais nous verrons qu'elle n'est pas suffisante (voir exemple 1.8). Pour énoncer notre critère, nous introduisons la définition suivante. Nous disons que deux variétés abéliennes (sur K comme toujours) sont *similaires* s'il existe un entier $n \geq 1$ et un isomorphisme $A^n \simeq B^n$ (sur K). Remarquons que la proposition 1.4 entraîne qu'il n'y a, à isomorphismes près, qu'un nombre fini de variétés abéliennes similaires à une variété abélienne donnée. L'observation suivante fait le lien avec notre problème.

Proposition 1.5. *Si* $\mathrm{End}\, A$ *est maximal, deux sous-variétés abéliennes de* A *isogènes sont similaires.*

Ceci fournit une nouvelle restriction sur les produits évoqués ci-dessus et elle s'avère cette fois suffisante.

Théorème 1.6. *L'ordre* $\operatorname{End} A$ *est maximal si et seulement si* A *est isomorphe à un produit* $\prod_{i=1}^{t} A_i$ *où, pour* $1 \leq i, j \leq t$,

(1) A_i *est une variété abélienne simple et* $\operatorname{End} A_i$ *est maximal ;*

(2) *si* A_i *et* A_j *sont isogènes alors elles sont similaires.*

En particulier, lorsque $\operatorname{End} A$ est maximal, la variété abélienne A est similaire à un produit de la forme $\prod_{i=1}^{s} A_i^{n_i}$ où les A_i sont simples et deux à deux non isogènes. En revanche, elle n'est pas en général isomorphe à un tel produit (voir exemple 1.9).

Nous décrivons à présent les sous-variétés à isomorphismes près.

Proposition 1.7. *Soient* A_0 *une variété abélienne simple telle que* $\operatorname{End} A_0$ *est maximal,* $n \geq 2$ *un entier et* A *une variété abélienne similaire à* A_0^n. *Pour tout entier* $0 \leq m \leq n-1$ *et tout choix* $A_1, \ldots, A_m$ *de variétés abéliennes similaires à* A_0, *il existe une sous-variété abélienne de* A *isomorphe à* $A_1 \times \cdots \times A_m$. *Réciproquement, toute sous-variété abélienne de* A *différente de* A *est isomorphe à un tel produit. En particulier, il existe une sous-variété abélienne de* A *isomorphe à* A_0^{n-1} *et donc il existe* A_n *similaire à* A_0 *telle que* A *est isomorphe à* $A_0^{n-1} \times A_n$.

La détermination des sous-variétés abéliennes d'une variété abélienne A avec $\operatorname{End} A$ maximal s'en déduit, en regroupant dans le produit du théorème 1.6 les facteurs similaires. Comme la dernière assertion de la proposition l'illustre, il n'y a pas d'unicité possible dans la décomposition en produit. Nous aurions aussi pu énoncer que toute sous-variété abélienne non nulle de A est isomorphe à un produit de la forme $A_0^{m-1} \times A_m$ pour A_m similaire à A_0 (et $1 \leq m \leq n$). Même dans cette écriture, A_m n'est pas en général uniquement déterminée à isomorphisme près (voir exemple 1.10).

La proposition 1.7 entraîne aussi facilement que si $\operatorname{End} A$ est maximal alors une variété abélienne B est similaire à A si et seulement si elle est isogène à A et isomorphe à une sous-variété abélienne de A^2. Dans ce cas, $\operatorname{End} B$ est également maximal.

Après ces résultats généraux, nous présentons trois exemples pour les illustrer.

Exemple 1.8. *Soit* E *une courbe elliptique sur* K *telle que* $\operatorname{End} E = \mathbb{Z}$ *et possédant un sous-groupe* G *d'ordre* 2 *rationnel sur* K. *Posons* $E' = E/G$. *Alors les trois variétés abéliennes* E^2, E'^2 *et* $E \times E'$ *sont deux à deux non isomorphes. Toute courbe elliptique tracée sur* $E \times E'$ *est isomorphe à* E *ou à* E'. *L'anneau* $\operatorname{End}(E \times E')$ *n'est pas un ordre maximal.*

Ici E et E' sont isogènes mais non similaires. La condition (2) du théorème 1.6 n'est donc pas remplie pour $E \times E'$.

Exemple 1.9. *Soit* E *une courbe elliptique sur* K *telle que* $\operatorname{End} E = \mathbb{Z}[i\sqrt{5}]$. *Notons* G *l'unique sous-groupe de* E *d'ordre* 2 *stable sous* $\operatorname{End} E$ *et* $E' = E/G$ (*définie sur* K). *Alors* $E^2 \simeq E'^2$ *mais* $E \times E'$ *n'est pas isomorphe à* E^2. *Toute courbe elliptique tracée sur* $E \times E'$ *est isomorphe à* E *ou à* E'. *L'anneau* $\operatorname{End}(E \times E')$ *est un ordre maximal.*

Ici le théorème 1.6 s'applique mais $E \times E'$ n'est isomorphe à aucun carré de courbe elliptique.

Exemple 1.10. *Il existe deux variétés abéliennes simples A et A' sur $K = \overline{\mathbb{Q}}$ non isomorphes avec* $\operatorname{End} A$ *et* $\operatorname{End} A'$ *maximaux de sorte que $A^2 \simeq A'^2 \simeq A \times A'$ et toute sous-variété abélienne de $A \times A'$ est isomorphe à 0, A^2, A ou A'.*

Ici pour $m \geq 2$ toute variété abélienne similaire à A^m lui est isomorphe mais c'est faux pour $m = 1$ où il existe une (unique) variété A' similaire mais non isomorphe à A.

Les démonstrations de ces énoncés reposent principalement sur la structure des modules de type fini sur les ordres maximaux dans les $\mathbb{Q}$-algèbres semi-simples de dimension finie.

La partie 3 constitue le cœur du texte : nous y démontrons nos théorèmes principaux 1.2 et 1.6 ainsi que les propositions 1.5 et 1.7. Avant cela, nous avons regroupé dans la partie suivante quelques énoncés auxiliaires ainsi que la démonstration du théorème 1.1. L'étude des exemples occupe quant à elle la partie 4 tandis que les autres énoncés de cette introduction sont établis dans la partie 5.

Enfin, les trois dernières parties sont plus indépendantes : nous montrons tout d'abord comment le théorème 1.1 permet d'améliorer légèrement des théorèmes d'isogénies de [3] sur les corps de nombres (théorème 6.1) ; ensuite, nous examinons la question de savoir si un ordre donné peut être l'anneau des endomorphismes d'une variété abélienne. En particulier nous donnons une réponse complète sur un corps algébriquement clos de caractéristique nulle (ce type de résultats est utile pour l'exemple 1.10 ci-dessus).

2. Préliminaires

Soient $\mathcal{O}$ un anneau, M un $\mathcal{O}$-module à droite et $M' \subset M$ un sous-module. Nous disons que le sous-module M' est saturé dans M lorsque le $\mathcal{O}$-module M/M' est sans torsion, divisible lorsque le $\mathbb{Z}$-module M/M' est sans torsion. Lorsque $\mathcal{O}$ est un ordre héréditaire dans une $\mathbb{Q}$-algèbre semi-simple de dimension finie, on sait (par le corollaire 10.7 de [8]) que tout $\mathcal{O}$-module qui est libre de rang fini comme $\mathbb{Z}$-module est projectif. Ceci entraîne que si M est un $\mathcal{O}$-module à droite de type fini alors tout sous-$\mathcal{O}$-module M' divisible admet un supplémentaire dans M (le quotient M/M' étant sans torsion sur $\mathbb{Z}$ donc libre comme $\mathbb{Z}$-module donc projectif comme $\mathcal{O}$-module).

Commençons par une remarque simple sur les modules d'endomorphismes entre variétés abéliennes.

Lemme 2.1. *Soient A et C deux variétés abéliennes et B une sous-variété abélienne de C. Le sous-*$\operatorname{End} A$*-module à droite* $\operatorname{Hom}(A, B)$ *de* $\operatorname{Hom}(A, C)$ *est divisible.*

Démonstration. Soient $\varphi \in \operatorname{Hom}(A, C)$ et $m \geq 1$ tel que $m\varphi \in \operatorname{Hom}(A, B)$. Comme $(m\varphi)(A) \subset B$, nous avons $\varphi(A) \subset [m]^{-1}B = B + \operatorname{Ker}[m]$. La variété abélienne A étant intègre, φ se factorise à travers la composante neutre de $B + (\operatorname{Ker}[m])_{\text{réd}}$ égale à B. Ainsi $\varphi \in \operatorname{Hom}(A, B)$. □

Alternativement, on peut établir l'exactitude de la suite

$$0 \longrightarrow \mathrm{Hom}(A,B) \longrightarrow \mathrm{Hom}(A,C) \longrightarrow \mathrm{Hom}(A,C/B)$$

et la divisibilité découle du fait que le $\mathbb{Z}$-module $\mathrm{Hom}(A,C/B)$ est sans torsion (il est même libre). En général, $\mathrm{Hom}(A,B)$ n'est pas saturé comme $\mathrm{End}\,A$-module à droite. Toutefois, c'est le cas si A est simple car alors saturation et divisibilité coïncident puisque si $\varphi \in \mathrm{End}\,A \setminus \{0\}$ il existe $m \in \mathbb{Z} \setminus \{0\}$ et $\psi \in \mathrm{End}\,A$ tels que $m = \varphi \circ \psi$.

Nous nous intéressons ensuite au lien entre B et $\mathrm{Hom}(A,B)$. Le résultat suivant donne un critère pour que la correspondance soit bijective et peut être vu comme une généralisation du lemme 5.1 de [3] (à l'exception de la formule sur la dimension).

Lemme 2.2. *Soient A et C deux variétés abéliennes. L'application de l'ensemble des sous-variétés B de C vers l'ensemble des sous-*$\mathrm{End}\,A$*-modules à droite divisibles de* $\mathrm{Hom}(A,C)$ *qui à B associe* $\mathrm{Hom}(A,B)$ *est surjective. De plus elle est injective si et seulement s'il existe un entier $n \geq 1$ et une surjection $A^n \to C$.*

Démonstration. Commençons par la surjectivité. Soit $M \subset \mathrm{Hom}(A,C)$ un sous-$\mathrm{End}\,A$-module à droite divisible. Notons $\varphi_1,\ldots,\varphi_r$ une famille génératrice de M, $\varphi = (\varphi_1,\ldots,\varphi_r)\colon A^r \to C$ et $B = \varphi(A^r)$. Si $\psi \in M$ il existe $\omega_1,\ldots,\omega_r \in \mathrm{End}\,A$ avec $\psi = \sum_{i=1}^r \varphi_i \circ \omega_i = \varphi \circ \omega$ pour $\omega = (\omega_1,\ldots,\omega_r)\colon A \to A^r$ d'où $\psi \in \mathrm{Hom}(A,B)$. Réciproquement si $\psi \in \mathrm{Hom}(A,B)$ notons $\chi = (\varphi,-\psi)\colon A^{r+1} \to C$. Comme $\mathrm{Im}\psi \subset \mathrm{Im}\varphi$, le noyau $\mathrm{Ker}\,\chi$ (qui s'identifie au produit fibré de φ et ψ) se projette surjectivement sur le dernier facteur de A^{r+1}. Par suite, il existe un morphisme $A \to \mathrm{Ker}\,\chi$ de sorte que la composée avec cette projection soit $[m]$ pour un entier $m \geq 1$. En écrivant $(\omega,[m])\colon A \to A^{r+1}$ le morphisme obtenu, nous avons $\chi \circ (\omega,[m]) = 0$ soit $m\psi = \sum_{i=1}^r \varphi_i \circ \omega_i \in M$. Par divisibilité $\psi \in M$ et nous concluons bien $M = \mathrm{Hom}(A,B)$.

Supposons maintenant que notre application soit injective. Choisissons une famille $B_1,\ldots,B_n$ de sous-variétés abéliennes simples de C telles que $B_1 + \cdots + B_n = C$. Par hypothèse, $\mathrm{Hom}(A,B_i) \neq \mathrm{Hom}(A,0) = 0$ donc il existe $\varphi_i\colon A \to B_i$ non nul. Par suite φ_i est surjectif (simplicité) et il en va donc de même pour $\varphi = (\varphi_1,\ldots,\varphi_n)\colon A^n \to C$. Réciproquement, supposons avoir une telle surjection $A^n \to C$ et deux sous-variétés abéliennes B et B' de C telles que $B' \not\subset B$. Nous pouvons choisir une sous-variété abélienne simple D de B' telle que $B \cap D$ soit un sous-schéma fermé fini donc contenu dans un $\mathrm{Ker}[m]$ pour $m \geq 1$. Comme D est un quotient de C, l'hypothèse entraîne qu'il existe un morphisme non nul $\psi\colon A \to D$. Alors $\psi \in \mathrm{Hom}(A,B')$ mais si nous avions aussi $\psi \in \mathrm{Hom}(A,B)$ alors ψ induirait un morphisme de A dans $B \cap D$ puis dans $\mathrm{Ker}[m]$. Ceci fournit $m\psi = 0$ en contradiction avec $\psi \neq 0$ donc $\mathrm{Hom}(A,B) \neq \mathrm{Hom}(A,B')$ et nous concluons que l'application de l'énoncé est injective dans ce cas. □

Nous terminons cette partie par une démonstration du théorème 1.1. Il résulte de l'énoncé légèrement plus précis suivant.

Proposition 2.3. *Soient A une variété abélienne, $N \geq 1$ un entier, $\mathcal{O}$ un ordre maximal de $(\operatorname{End} A) \otimes \mathbb{Q}$ et $d = \operatorname{rg}_{\mathbb{Z}} \operatorname{End} A = \operatorname{rg}_{\mathbb{Z}} \mathcal{O}$. Si $\mathcal{O} \subset N^{-1} \operatorname{End} A$ alors il existe une sous-variété abélienne A' de A^d et deux isogénies $\varphi\colon A \to A'$ et $\psi\colon A' \to A$ de sorte que $\psi \circ \varphi = [N]$ et $\operatorname{End} A' \simeq \mathcal{O}$.*

Démonstration. Notons $e_1 = 1, e_2, \dots, e_d$ une $\mathbb{Z}$-base de l'ordre $\mathcal{O}$. Par hypothèse $Ne_i\alpha \in \operatorname{End} A$ pour tous $1 \leq i \leq d$ et $\alpha \in \mathcal{O}$ donc nous pouvons définir $\chi_\alpha = (Ne_1\alpha, \dots, Ne_d\alpha)\colon A \to A^d$. Notons $A' = \chi_1(A)$, $\varphi\colon A \to A'$ la restriction de χ_1 et $\psi\colon A' \to A$ la restriction de la première projection. Nous avons bien $\psi \circ \varphi = [N]$ et φ et ψ sont des isogénies. Écrivons $e_i\alpha = \sum_{j=1}^d a_{ij}e_j$ pour $1 \leq i \leq d$ et $a_{ij} \in \mathbb{Z}$ ($\alpha \in \mathcal{O}$ étant fixé). La matrice $N_\alpha = (a_{ij})_{i,j}$ fournit un morphisme $\omega_\alpha\colon A^d \to A^d$ tel que $\omega_\alpha \circ \chi_1 = \chi_\alpha$. Par ailleurs, nous avons $N\chi_\alpha = \chi_1 \circ (N\alpha)$ où $N\alpha \in \operatorname{End} A$ donc $N\chi_\alpha \in \operatorname{Hom}(A, A')$. Par divisibilité de $\operatorname{Hom}(A, A')$ dans $\operatorname{Hom}(A, A^d)$ (lemme 2.1), nous avons $\chi_\alpha \in \operatorname{Hom}(A, A')$ donc nous pouvons en déduire que ω_α induit un endomorphisme ω'_α de A'. De cette façon, l'application $\mathcal{O} \to M_d(\mathbb{Z}) \to \operatorname{End}(A^d)$ déduite de la représentation régulière à droite induit un morphisme d'anneaux $\mathcal{O} \to \operatorname{End} A'$, $\alpha \mapsto \omega'_\alpha$. Il est injectif car $\psi \circ \omega'_\alpha \circ \varphi = N\alpha$ par construction pour tout $\alpha \in \mathcal{O}$. Par isogénie, $\operatorname{rg}_{\mathbb{Z}} \operatorname{End} A' = d = \operatorname{rg}_{\mathbb{Z}} \mathcal{O}$ donc la maximalité de $\mathcal{O}$ entraîne $\mathcal{O} \simeq \operatorname{End} A'$. □

3. Ordres maximaux

Soit $\mathfrak{A}$ une $\mathbb{Q}$-algèbre semi-simple de dimension finie.

Proposition 3.1. *Soient $\mathcal{I}$ un idéal à droite de $\mathfrak{A}$ et $\mathcal{O}$ un ordre maximal de $\mathfrak{A}$. Il existe $\pi \in \mathcal{O}$ tel que $\pi^2 = \pi$ et $\mathcal{I} \cap \mathcal{O} = \pi\mathcal{O}$. De plus $\pi\mathcal{O}\pi$ est un ordre maximal de l'algèbre $\pi\mathfrak{A}\pi$.*

Démonstration. Par semi-simplicité, $\mathfrak{A}$ est isomorphe à un produit d'anneaux de matrices $\prod_{i=1}^s M_{n_i}(D_i)$ sur des corps (gauches) D_i (voir les théorèmes 7.1 et 7.4 de [8]). Si nous identifions $\mathfrak{A}$ à ce produit, la i-ème projection $p_i(\mathcal{O})$ de $\mathcal{O}$ est un ordre de $M_{n_i}(D_i)$. La maximalité de $\mathcal{O}$ et l'inclusion $\mathcal{O} \subset \prod_{i=1}^s p_i(\mathcal{O})$ entraînent que $\mathcal{O} = \prod_{i=1}^s p_i(\mathcal{O})$ et que $p_i(\mathcal{O})$ est maximal. Choisissons maintenant un ordre maximal Δ_i de D_i. D'après le théorème 21.6 de [8], il existe un Δ_i-module à droite $N_i \subset D_i^{n_i}$ tel que $p_i(\mathcal{O}) = \operatorname{End}_{\Delta_i} N_i \subset \operatorname{End}_{D_i} D_i^{n_i} = M_{n_i}(D_i)$.

Par ailleurs, il existe des sous-espaces vectoriels à droite $V_i \subset D_i^{n_i}$ tels que $\mathcal{I} = \prod_{i=1}^s V_i^{n_i}$ où $V_i^{n_i} \subset M_{n_i}(D_i)$ désigne ici les matrices dont les colonnes appartiennent à V_i. Ainsi $\mathcal{I} \cap \mathcal{O}$ s'écrit comme le produit des idéaux $\{\varphi \in \operatorname{End}_{\Delta_i} N_i \mid \varphi(N_i) \subset V_i\}$. Maintenant Δ_i est maximal donc héréditaire (voir le théorème 21.4 de [8]) et $N_i \cap V_i$ est un sous-module saturé de N_i donc il admet un supplémentaire M_i soit $N_i = (N_i \cap V_i) \oplus M_i$. Notons alors $\pi_i \in \operatorname{End}_{\Delta_i} N_i$ le projecteur sur le premier facteur de cette décomposition puis $\pi = (\pi_1, \dots, \pi_s)$. Nous avons $\{\varphi \in \operatorname{End}_{\Delta_i} N_i \mid \varphi(N_i) \subset V_i\} = \pi_i \cdot \operatorname{End}_{\Delta_i} N_i$ car $\pi_i(N_i) = N_i \cap V_i \subset V_i$ et $\varphi(N_i) \subset V_i$ entraîne $\varphi = \pi_i \circ \varphi$. L'égalité $\mathcal{I} \cap \mathcal{O} = \pi\mathcal{O}$ s'en déduit. Enfin $\pi\mathcal{O}\pi = \prod_{i=1}^s \pi_i \cdot \operatorname{End}_{\Delta_i} N_i \cdot \pi_i$ s'identifie à $\prod_{i=1}^s \operatorname{End}_{\Delta_i} N_i \cap V_i \subset \prod_{i=1}^s \operatorname{End}_{D_i} V_i \simeq \prod_{i=1}^s \pi_i \cdot M_{n_i}(D_i) \cdot \pi_i = \pi\mathfrak{A}\pi$ et $\operatorname{End}_{\Delta_i} N_i \cap V_i$ est un ordre maximal (voir le théorème 21.6 de [8]). □

Ce résultat admet une traduction directe dans le monde des variétés abéliennes.

Démonstration du théorème 1.2. Soit $\mathcal{J} = \{\varphi \in \operatorname{End} A \mid \varphi(A) \subset B\}$, idéal à droite de $\mathcal{O} = \operatorname{End} A$. La propriété de divisibilité du lemme 2.1 s'écrit ici $\mathcal{J} = (\mathcal{J} \otimes \mathbb{Q}) \cap \mathcal{O}$ et $\mathcal{J} \otimes \mathbb{Q}$ est un idéal à droite de l'algèbre semi-simple $\mathcal{O} \otimes \mathbb{Q}$. Par la proposition 3.1, il existe $\pi \in \mathcal{O}$ tel que $\pi^2 = \pi$ et $\mathcal{J} = \pi\mathcal{O}$. De $\pi \in \mathcal{J}$ nous tirons $\pi(A) \subset B$ et, comme il existe un morphisme surjectif $\varphi\colon A \to B$, nous avons $\pi(A) = B$ (car $\varphi \in \mathcal{J}$ donne $\varphi = \pi \circ \varphi$). Notons $B' = \operatorname{Ker} \pi = (\mathrm{id} - \pi)(A)$ sous-variété abélienne de A. L'égalité $\pi^2 = \pi$ entraîne usuellement $A = B + B'$ et $B \cap B' = 0$. Enfin $\pi\mathcal{O}\pi$ s'identifie à $\operatorname{End} B$ (facteur de $\operatorname{End}(B \times B')$). □

Notons dès à présent que le théorème 1.2 suffit à montrer une implication dans le théorème 1.6.

Lemme 3.2. *Si les conditions* (1) *et* (2) *du théorème 1.6 sont remplies alors l'ordre* $\operatorname{End}(\prod_{i=1}^t A_i)$ *est maximal.*

Démonstration. Si les A_i sont ordonnées de telle sorte que, pour un entier s avec $1 \leq s \leq t-1$, aucune des $A_1, \ldots, A_s$ ne soit isogène à l'une des $A_{s+1}, \ldots, A_t$ alors $\operatorname{End}(\prod_{i=1}^t A_i) \simeq \operatorname{End}(\prod_{i=1}^s A_i) \times \operatorname{End}(\prod_{i=s+1}^t A_i)$. Cette remarque permet ici de supposer toutes les A_i isogènes donc similaires. En particulier, $A_i^{n_i} \simeq A_1^{n_i}$ montre que A_i est isomorphe à une sous-variété abélienne de $A_1^{n_i}$ pour un certain entier $n_i \geq 1$. Ainsi $\prod_{i=1}^t A_i$ est isomorphe à une sous-variété abélienne de A_1^n où $n = n_1 + \cdots + n_t$. La maximalité de $\operatorname{End}(\prod_{i=1}^t A_i)$ découle donc par le théorème 1.2 de celle de $\operatorname{End} A_1^n \simeq M_n(\operatorname{End} A_1)$ (voir le théorème 8.7 de [8]). □

Ceci dit, le théorème 1.6 découlera directement de la première assertion de la proposition suivante.

Proposition 3.3. *Soient A et B deux variétés abéliennes simples isogènes telles que* $\operatorname{End}(A \times B)$ *est maximal. Alors A et B sont similaires et toute variété abélienne similaire à A est isomorphe à une sous-variété abélienne de $A \times B$.*

Nous démontrons ceci en plusieurs étapes.

Lemme 3.4. *Sous les hypothèses de la proposition 3.3, il existe un entier $n \geq 1$ tel que B est isomorphe à une sous-variété abélienne de A^n.*

Démonstration. Choisissons une isogénie $\varphi\colon A \to B$. Notons $\mathcal{O} = \operatorname{End} A$, $\mathcal{I} = \varphi^{-1} \circ \operatorname{Hom}(A, B)$, $\mathcal{J} = \operatorname{Hom}(B, A) \circ \varphi$ et $\mathcal{O}' = \varphi^{-1} \circ \operatorname{End}(B) \circ \varphi$. Ce sont tous des sous-groupes de $\mathcal{O} \otimes \mathbb{Q}$. De plus $\mathcal{O}$ et $\mathcal{O}'$ sont des ordres maximaux, $\mathcal{I}$ est un $\mathcal{O}$-module à droite, $\mathcal{J}$ un $\mathcal{O}$-module à gauche. Ce sont même des idéaux fractionnaires. De plus le sous-anneau $\mathcal{O} \oplus \mathcal{I} \oplus \mathcal{J} \oplus \mathcal{O}' \subset (\mathcal{O} \otimes \mathbb{Q})^4 \simeq M_2(\mathcal{O} \otimes \mathbb{Q})$ s'identifie à $\operatorname{End}(A \times B)$. Comme $\mathcal{J}\mathcal{I} \subset \mathcal{O}$ nous avons $\mathcal{J} \subset \mathcal{I}^{-1}$. En outre $\mathcal{O} \oplus \mathcal{I} \oplus \mathcal{I}^{-1} \oplus \mathcal{O}'$ est aussi un ordre ($\mathcal{I}^{-1}\mathcal{I} = \mathcal{O}$, $\mathcal{I}\mathcal{I}^{-1} = \mathcal{O}'$: comme $\mathcal{I}$ est aussi un $\mathcal{O}'$-module à gauche, son ordre à gauche $\mathcal{O}_g(\mathcal{I})$ contient $\mathcal{O}'$ d'où $\mathcal{O}' = \mathcal{O}_g(\mathcal{I}) = \mathcal{I}\mathcal{I}^{-1}$, voir le théorème 22.7 de [8]). Par maximalité, nous avons $\mathcal{J} = \mathcal{I}^{-1}$ donc en particulier $\mathcal{I}\mathcal{J} = \mathcal{O}'$. En d'autres termes, l'application $\operatorname{Hom}(A, B) \otimes \operatorname{Hom}(B, A) \to \operatorname{End} B$ donnée par la composition

est surjective. Ainsi nous pouvons écrire $\mathrm{id}_B = \sum_{i=1}^n f_i \circ g_i$ pour un $n \geq 1$, des $f_i \colon A \to B$ et $g_i \colon B \to A$. Ces derniers forment des applications $f \colon A^n \to B$ et $g \colon B \to A^n$ telles que $f \circ g = \mathrm{id}_B$. En particulier, g est injective d'où le résultat souhaité. □

À ce stade, toutes les variétés abéliennes apparaissant dans la proposition 3.3 sont des sous-variétés abéliennes d'une puissance de A : c'est le cas pour B par ce lemme donc pour $A \times B$ ainsi que pour toute variété abélienne similaire à A par définition même. Nous allons donc nous concentrer sur les sous-variétés abéliennes de A^n et les caractériser en termes de modules sur l'ordre maximal $\mathcal{O} = \mathrm{End}\, A$. En particulier, nous fixons un tel A simple pour les trois lemmes suivants. Commençons par rappeler que si M, N et P sont trois modules à droite de type fini et sans torsion sur $\mathcal{O}$ alors (voir le paragraphe 35 de [8] et en particulier le corollaire 35.13)

$$M \oplus P \simeq N \oplus P \Longrightarrow M \oplus \mathcal{O} \simeq N \oplus \mathcal{O}$$

et, si de plus M est de rang au moins 2, alors

$$M \oplus P \simeq N \oplus P \Longrightarrow M \simeq N.$$

La maximalité de $\mathcal{O}$ permet d'ajouter la précision suivante à la bijection du lemme 2.2 (avec $C = A^n$).

Lemme 3.5. *Si B et B' sont deux sous-variétés abéliennes de A^n telles que les $\mathcal{O}$-modules à droite $\mathrm{Hom}(A, B)$ et $\mathrm{Hom}(A, B')$ sont isomorphes alors $B \simeq B'$.*

Démonstration. Quitte à augmenter n, nous pouvons supposer que le rang de $\mathrm{Hom}(A, B)$ (égal à $\dim B / \dim A$) est au plus $n - 2$. Nous choisissons des supplémentaires C de B et C' de B' (dans A^n). Nous avons donc $\mathrm{Hom}(A, B) \oplus \mathrm{Hom}(A, C) = \mathrm{Hom}(A, A^n) = \mathrm{Hom}(A, B') \oplus \mathrm{Hom}(A, C')$. La conjonction de l'hypothèse $\mathrm{Hom}(A, B) \simeq \mathrm{Hom}(A, B')$ et de $\mathrm{rg}\,\mathrm{Hom}(A, C) \geq 2$ nous permet d'affirmer $\mathrm{Hom}(A, C) \simeq \mathrm{Hom}(A, C')$. Par suite, il existe un automorphisme φ de $\mathcal{O}^n \simeq \mathrm{Hom}(A, A^n)$ tel que $\varphi(\mathrm{Hom}(A, B)) = \mathrm{Hom}(A, B')$. Un tel φ s'identifie à un élément ψ de $\mathrm{End}\, A^n \simeq M_n(\mathcal{O})$. On vérifie $\varphi(\mathrm{Hom}(A, B)) = \mathrm{Hom}(A, \psi(B))$ donc, par le lemme 2.2, $\psi(B) = B'$. Ainsi l'automorphisme ψ de A^n induit un isomorphisme $B \to B'$. □

Par exemple, cet énoncé permet de traduire la propriété de modules donnée de la façon suivante : si B, B' et B'' sont trois sous-variétés abéliennes de A^n telles que $B \times B'' \simeq B' \times B''$ alors $B \times A \simeq B' \times A$ et si de plus $\dim B > \dim A$ alors $B \simeq B'$. L'exemple 1.10 que nous démontrerons plus loin illustre que l'on n'a pas toujours $B \simeq B'$ lorsque $\dim B = \dim A$.

Nous en déduisons aussi, par le théorème de Jordan–Zassenhaus (théorème 26.4 de [8]), que les sous-variétés abéliennes de A^n appartiennent à un nombre fini de classes d'isomorphie.

Nous pouvons maintenant conclure la démonstration de la proposition 3.3 en deux lemmes.

Lemme 3.6. *Si B est une sous-variété abélienne de A^n et si $\dim B = \dim A$ alors A et B sont similaires.*

Démonstration. Le module projectif $\mathrm{Hom}(A,B)$ est de rang 1 donc isomorphe à un idéal à droite $\mathcal{I}_B$ de $\mathcal{O}$. Les classes des idéaux à droite de $\mathcal{O}$ modulo la relation d'équivalence $\mathcal{I}\sim\mathcal{I}' \iff \mathcal{O}\oplus\mathcal{I}\simeq\mathcal{O}\oplus\mathcal{I}'$ forment un groupe dans lequel la somme $\mathcal{I}''$ de $\mathcal{I}$ et $\mathcal{I}'$ est caractérisée par $\mathcal{I}\oplus\mathcal{I}'\simeq\mathcal{O}\oplus\mathcal{I}''$ (voir le théorème 35.5 de [8]). De plus ce groupe est fini par le théorème de Jordan-Zassenhaus donc il existe un entier $m\geq 1$ tel que $\mathcal{I}_B^{\oplus m}\simeq\mathcal{O}^{\oplus m}$ soit $\mathrm{Hom}(A,B^m)\simeq\mathrm{Hom}(A,A^m)$ donc (lemme 3.5) $B^m\simeq A^m$. □

Lemme 3.7. *Si B et C sont similaires à A alors C est isomorphe à une sous-variété abélienne de $A\times B$.*

Démonstration. Par le lemme 3.5, il s'agit de montrer que si $\mathcal{I}$ et $\mathcal{I}'$ sont deux idéaux à droite de $\mathcal{O}$ alors $\mathcal{I}'$ est isomorphe à un sous-module saturé de $\mathcal{O}\oplus\mathcal{I}$. Si nous notons $[\cdot]$ la classe d'un idéal modulo la relation d'équivalence décrite dans la démonstration précédente, nous pouvons introduire un idéal à droite $\mathcal{J}$ tel que $[\mathcal{J}]=[\mathcal{I}]-[\mathcal{I}']$. Par définition de la loi de groupe, cela signifie $\mathcal{I}'\oplus\mathcal{J}\simeq\mathcal{O}\oplus\mathcal{I}$ d'où le résultat. □

La proposition 3.3 résulte donc directement des lemmes 3.4, 3.5 et 3.7. Comme nous l'avons vu plus haut, elle entraîne le théorème 1.6. Voyons maintenant comment nous en déduisons aussi les propositions 1.5 et 1.7.

Démonstration de la proposition 1.7. Puisque $\mathrm{End}\,A$ est maximal (A étant isomorphe à une sous-variété abélienne de A_0^{nm} pour un $m\geq 1$) nous avons $A\simeq\prod_{i=1}^n A_i'$ pour des A_i' similaires à A_0 par le théorème 1.6. Par la proposition 3.3, A_1 est isomorphe à une sous-variété abélienne de $A_1'\times A_2'$ donc de A. Nous pouvons donc changer les A_i' pour avoir $A_1'\simeq A_1$. Il suffit alors d'itérer ce procédé : si $2\leq m\leq n-1$ alors A_2 s'injecte dans $A_2'\times A_3'$ donc peut remplacer A_2' et ainsi de suite. Pour la réciproque, si $B\subset A$, on écrit $A\simeq B\times C$, on décompose B et C en produits de variétés abéliennes simples, toutes similaires par la proposition 3.3. Elles sont donc similaires à A_0 et B est bien de la forme annoncée. □

Le cas où les deux sous-variétés abéliennes de la proposition 1.5 sont simples est contenu dans la proposition 3.3. Le cas général s'en déduit par décomposition en produits.

4. Exemples

Nous démontrons ici les trois exemples cités dans l'introduction.

Démonstration de l'exemple 1.8. Notons $\varphi\colon E\to E'$ le quotient. Toute isogénie $E\to E'$ est un multiple de φ cyclique donc $\mathrm{Hom}(E,E')=\mathbb{Z}\varphi$. De la même façon, $\mathrm{Hom}(E',E)=\mathbb{Z}\widehat{\varphi}$ pour l'isogénie $\widehat{\varphi}\colon E'\to E$ qui vérifie $\widehat{\varphi}\circ\varphi=[2]$. Par conséquent, l'image de l'application $\mathrm{Hom}(E',E)\otimes\mathrm{Hom}(E,E')\to\mathrm{End}\,E$ coïncide avec $2\cdot\mathrm{End}\,E$. Maintenant l'argument de la démonstration du lemme 3.4 montre que si $\mathrm{End}(E\times E')$ était maximal, cette application serait surjective. Ainsi $\mathrm{End}(E\times E')$ n'est pas

maximal et nous en déduisons que $E\times E'$ n'est isomorphe ni à E^2 ni à E'^2 (puisque $\operatorname{End} E^2 \simeq \operatorname{End} E'^2 \simeq M_2(\mathbb{Z})$). De plus, E et E' ne sont pas similaires (par le théorème 1.6) donc en particulier E^2 et E'^2 ne sont pas isomorphes. Soit finalement B une sous-variété abélienne de $E\times E'$ de dimension 1. Elle est certainement isogène à E donc peut s'écrire comme l'image d'une application $\psi\colon E\to E\times E'$. Celle-ci s'écrit $\psi=(a\mathrm{id}_E, b\varphi)$ où $a,b\in\mathbb{Z}$. Nous pouvons supposer, sans changer l'image, que a et b sont premiers entre eux. Alors $\operatorname{Ker}\psi=\operatorname{Ker}[a]\cap\operatorname{Ker} b\varphi=\operatorname{Ker}[a]\cap\operatorname{Ker}\varphi\subset\operatorname{Ker}\varphi$. Comme $\operatorname{Card}\operatorname{Ker}\varphi=2$, de deux choses l'une : soit $\operatorname{Ker}\psi=\{0\}$ et $B\simeq E$, soit $\operatorname{Ker}\psi=\operatorname{Ker}\varphi$ et $B\simeq E'$. □

Démonstration de l'exemple 1.9. L'isogénie $[1+i\sqrt{5}]$ est de degré 6 donc $\operatorname{Ker}[1+i\sqrt{5}]\cap\operatorname{Ker}[2]$ est un groupe de cardinal 2, défini sur K et stable sous $\operatorname{End} E$. C'est le seul car l'action de $[1+i\sqrt{5}]$ sur $\operatorname{Ker}[2]$ est nilpotente d'image ce groupe. Il s'agit donc de notre G. *Via* l'application $E\to E^2$ donnée par $x\mapsto(2x,(1+i\sqrt{5})x)$, de noyau G, la courbe E' est isomorphe à une sous-variété abélienne de E^2 donc similaire à E (lemme 3.6). Elle n'est pas isomorphe à E car il n'y a pas d'isogénie $E\to E$ de degré 2 donc on en déduit que $\operatorname{Hom}(E,E')$ est un $\operatorname{End} E$-module de rang 1 non libre (lemme 3.5). Un tel module est unique à isomorphisme près car le groupe de classes de $\mathbb{Z}[i\sqrt{5}]$ est de cardinal 2. Par suite, toute courbe elliptique contenue dans E^n donc en particulier dans $E\times E'\subset E^3$ est isomorphe à E ou à E'. Ainsi, en choisissant un supplémentaire de E' dans E^2 on a $E^2\simeq E'^2$ ou $E^2\simeq E\times E'$. Il nous reste seulement à montrer que ce dernier cas est exclu ou encore que $(\operatorname{End} E)^2$ et $\operatorname{End} E\oplus\operatorname{Hom}(E,E')$ sont des $\operatorname{End} E$-modules non isomorphes. Or leurs carrés extérieurs $\bigwedge^2(\cdot)$ diffèrent. □

Démonstration de l'exemple 1.10. Swan (voir [12]) a construit explicitement un ordre maximal $\mathcal{O}$ de rang 16 sur $\mathbb{Z}$ ayant, à isomorphisme près, un unique idéal I non principal qui vérifie de plus $\mathcal{O}\oplus I\simeq\mathcal{O}^2$. Comme dans cet exemple $\mathcal{O}\otimes\mathbb{Q}$ est une algèbre de quaternions totalement définie sur un corps de nombres totalement réel, il existe une variété abélienne A sur $\overline{\mathbb{Q}}$ de dimension 16 avec $\operatorname{End} A\simeq\mathcal{O}$ (voir théorème 7.3 et lemme 7.9). Si B est une sous-variété abélienne de A^2 alors $\operatorname{Hom}(A,B)$ est isomorphe à $\{0\}$, $\mathcal{O}$, I ou $\mathcal{O}^2$. Notons A' une sous-variété abélienne de A^2 avec $\operatorname{Hom}(A,A')\simeq I$. L'isomorphisme $\mathcal{O}\oplus I\simeq\mathcal{O}^2$ donne $A\times A'\simeq A^2$. Par ailleurs A'^2 est similaire à A^2 donc isomorphe à $A\times A''$ où A'' est similaire à A (proposition 1.7). Ainsi $A''\simeq A$ ou $A''\simeq A'$ mais dans les deux cas $A\times A''\simeq A^2$. □

Rappelons que la construction de Swan utilisée ci-dessus n'est possible que parce que $\mathcal{O}\otimes\mathbb{Q}$ ne vérifie pas la condition d'Eichler (voir la définition 34.3 de [8]) c'est-à-dire que $\mathcal{O}\otimes\mathbb{R}$ est isomorphe à une puissance des quaternions de Hamilton $\mathbb{H}$ (dans l'exemple $\mathcal{O}\otimes\mathbb{R}\simeq\mathbb{H}^4$). Dans tous les autres cas (cas (I), (II), (IV) de la classification d'Albert, voir la page 201 de [6] et la proposition 7.2 ci-après) ce phénomène ne se produit pas et, par exemple, la classe d'isomorphie de la variété abélienne A_n de la proposition 1.7 est uniquement déterminée par celle de A sous l'hypothèse que $(\operatorname{End} A_0)\otimes\mathbb{Q}$ vérifie la condition d'Eichler.

5. Ordres non maximaux

Voyons que les théorèmes 1.1 et 1.2 entraînent le corollaire 1.3.

Démonstration du corollaire 1.3. Nous appliquons à A le théorème 1.1 qui nous fournit A', φ et ψ puis le théorème 1.2 à la sous-variété abélienne $\varphi(B)$ de A'. Nous obtenons un supplémentaire C de $\varphi(B)$ dans A' et posons $B' = \psi(C)$. Alors l'isogénie φ envoie $B + B'$ sur $\varphi(B) + C = A'$ donc $B + B' = A$ et $B \cap B'$ sur $\varphi(B) \cap C = 0$ donc $B \cap B' \subset \operatorname{Ker}\varphi \subset \operatorname{Ker}[N]$. Par ailleurs, l'application $f \mapsto N^{-1}\psi_{|\varphi(B)} \circ f \circ \varphi_{|B}$ fournit un morphisme d'anneaux injectif $\operatorname{End}\varphi(B) \to (\operatorname{End} B)\otimes\mathbb{Q}$ dont l'image est bien un ordre maximal contenu dans $N^{-1}\operatorname{End} B$. □

Il nous reste un dernier énoncé de l'introduction à établir.

Démonstration de la proposition 1.4. Si A_0 est une variété abélienne simple telle que $\operatorname{End} A_0$ est maximal, nous avons vu plus haut comme conséquence du lemme 3.5 et du théorème de Jordan–Zassenhaus que, pour n donné, les sous-variétés abéliennes de A_0^n étaient en nombre fini à isomorphisme près. En particulier, avec $n = 2$, il n'y a qu'un nombre fini de variétés abéliennes similaires à A_0. Supposons maintenant que A est une variété abélienne telle que $\operatorname{End} A$ est maximal et $b \geq 1$ un entier. Il existe un isomorphisme $A \simeq \prod_{i=1}^{s} A_i$ où chaque A_i est simple et $\operatorname{End} A_i$ maximal. Soient $n \geq 1$ et B une sous-variété abélienne de A^n de dimension $\leq b$. Nous déduisons de la proposition 1.7 que B est isomorphe à un produit $\prod_{j=1}^{t} B_j$ où chaque B_j est similaire à l'un des A_i. Par suite, il n'y a qu'un nombre fini de choix pour chaque B_j et donc (avec disons $t \leq b$) pour B. Ceci démontre la proposition dans le cas où $\operatorname{End} A$ est maximal. Dans le cas général, nous utilisons le théorème 1.1 qui nous fournit A, φ et ψ. Si B est une sous-variété abélienne de A^n alors $B' = (\varphi^n)(B)$ est une sous-variété abélienne de A'^n et ψ^n induit une isogénie $B' \to B$ de noyau contenu dans $\operatorname{Ker}[N]$. Lorsque $\dim B = \dim B'$ est borné, il n'y a qu'un nombre fini de choix pour B' et pour chacun un nombre fini de sous-schémas en groupes contenus dans $\operatorname{Ker}[N] \subset B'$ qui donnent naissance à un nombre fini de quotients B. □

Voyons pour terminer cette partie que les lemmes 3.5 et 3.6 utilisés plus haut dans le cas maximal ne valent pas en général. Ceci ne pose pas de difficultés pour le lemme 3.6 car, pour toute variété abélienne A telle que $\operatorname{End} A$ n'est pas maximal, la proposition 2.3 fournit une variété abélienne A' sous-variété abélienne de A^d qui ne peut pas être similaire à A puisque sinon $\operatorname{End} A$ serait lui aussi maximal. Voyons maintenant un exemple pour le lemme 3.5.

Exemple 5.1. *Il existe trois variétés abéliennes complexes A_0, A_1 et A_2 de dimension 3 telles que A_0 et A_1 sont deux sous-variétés abéliennes de A_2^3 non isomorphes bien que les* $\operatorname{End} A_2$*-modules à droite* $\operatorname{Hom}(A_2, A_0)$ *et* $\operatorname{Hom}(A_2, A_1)$ *soient isomorphes.*

Démonstration. Notons $D = \mathbb{Q}(\xi)$ où $\xi^3 = 4\xi - 1$. Il s'agit d'un corps de nombres totalement réel (car $27(1)^2 - 4(4)^3 < 0$) donc d'après le théorème 7.3 nous disposons

d'un $\mathbb{C}$-espace vectoriel V de dimension 3 contenant un $\mathbb{Q}$-espace vectoriel E de dimension 6 de sorte que $E\otimes_{\mathbb{Q}}\mathbb{R}=V$; $\{f\in\mathrm{End}_{\mathbb{C}}V\mid f(E)=E\}\simeq D$; pour tout réseau Ω de E, le tore complexe V/Ω est une variété abélienne. Dans ces conditions, E est un D-espace vectoriel de dimension 2 dont nous notons e_1,e_2 une base. Définissons maintenant des sous-$\mathbb{Z}$-modules de D par $M_0=\mathbb{Z}\oplus 4\mathbb{Z}\xi\oplus 8\mathbb{Z}\xi^2\supset M_1=2\mathbb{Z}\oplus 4\mathbb{Z}\xi\oplus 8\mathbb{Z}\xi^2\supset M_2=2\mathbb{Z}\oplus 4\mathbb{Z}\xi\oplus 16\mathbb{Z}\xi^2$. Remarquons que M_0 est l'anneau $\mathbb{Z}[4\xi,8\xi^2]$ dont M_1 et M_2 forment des idéaux. En outre, $\frac12 M_1=\mathbb{Z}[2\xi]$ est aussi un sous-anneau de D (contenant M_0). Posons finalement $\Omega_i=M_ie_1\oplus M_ie_2$ et $A_i=V/\Omega_i$ pour $0\leq i\leq 2$. Vérifions que ces trois variétés abéliennes remplissent les conditions de l'énoncé. Nous avons tout d'abord pour $0\leq i,j\leq 2$,

$$\mathrm{Hom}(A_i,A_j)=\{f\in\mathrm{End}_{\mathbb{C}}(V)\mid f(\Omega_i)\subset\Omega_j\}\simeq\{x\in D\mid xM_i\subset M_j\}.$$

Cet isomorphisme fait de $\mathrm{Hom}(A_i,A_j)$ un M_0-module. En particulier, c'est le cas de $\mathrm{End}\,A_i$ et $\mathrm{End}\,A_j$ et la construction montre que les trois structures de M_0-module sur $\mathrm{Hom}(A_i,A_j)$ induites par l'isomorphime ci-dessus et les structures de $\mathrm{End}\,A_i$-module à droite et de $\mathrm{End}\,A_j$-module à gauche coïncident (en d'autres termes, les compositions $\mathrm{Hom}(A_i,A_j)\times\mathrm{Hom}(A_j,A_k)\to\mathrm{Hom}(A_i,A_k)$ sont M_0-bilinéaires). Maintenant, des calculs fastidieux mais sans mystère permettent d'établir que $\{x\in D\mid xM_i\subset M_j\}$ vaut M_{j-i} si $i(2-j)=0$ et $\frac12 M_1$ dans tous les autres cas. Détaillons seulement un exemple : $\{x\in D\mid xM_2\subset M_0\}=\frac12 M_0\cap\frac{1}{4\xi}M_0\cap\frac{1}{16\xi^2}M_0$ où $\frac{1}{16\xi^2}M_0=\mathbb{Z}\frac{1}{16\xi^2}\oplus\mathbb{Z}\frac{1}{4\xi}\oplus\frac12\mathbb{Z}$ puis, comme $1/(4\xi)=1-\xi^2/4$ et $1/(16\xi^2)=1-\xi^2/4-\xi/16$, nous arrivons à $\frac{1}{16\xi^2}M_0=\frac12\mathbb{Z}\oplus\frac{1}{16}\mathbb{Z}\xi\oplus\frac14\mathbb{Z}\xi^2$; de façon analogue on calcule $\frac{1}{4\xi}M_0=\mathbb{Z}\oplus 2\mathbb{Z}\xi\oplus\frac14\mathbb{Z}\xi^2$ et cela conduit bien à $\{x\in D\mid xM_2\subset M_0\}=\frac12 M_1$.

De ces considérations, nous déduisons d'abord les isomorphismes d'anneaux $\mathrm{End}\,A_i\simeq M_0$ si $i=0,2$ et $\mathrm{End}\,A_1\simeq\frac12 M_1$. Ceci montre notamment que A_0 et A_1 ne peuvent pas être isomorphes. Ensuite l'isomorphisme de M_0-modules $\mathrm{Hom}(A_2,A_0)\simeq\frac12 M_1\simeq\mathrm{Hom}(A_2,A_1)$ fournit, par la remarque faite plus haut, l'isomorphisme de $\mathrm{End}\,A_2$-modules (à droite) cherché. Il nous reste à voir que pour $0\leq i\leq 2$ nous avons une injection $A_i\hookrightarrow A_2^3$. Nous cherchons donc un morphisme $f_i\colon V\to V^3$ tel que $f_i^{-1}(\Omega_2^3)=\Omega_i$ c'est-à-dire encore un élément $g_i\in D^3$ tel que $g_i^{-1}(M_2^3)=M_i$. Cette dernière condition s'écrit $\{x\in D\mid xg_i\in M_2^3\}=M_i$ ou encore $\{x\in D\mid xM_i'\subset M_2\}=M_i$ où M_i' est le $\mathbb{Z}$-module engendré par les coordonnées de g_i. D'après nos calculs, il suffit de faire en sorte que $M_i'=M_{2-i}$ pour avoir le résultat. □

6. Estimation explicite pour les corps de nombres

Plusieurs des énoncés que nous avons donnés améliorent des résultats de [3]. Nous avons déjà signalé que le lemme 2.1 généralisait partiellement le lemme 5.1 de [3] tandis que le corollaire 1.3 améliore la proposition 5.2 de [3]. Plus significativement, le théorème 1.1 remplace avantageusement la proposition 4.9 de [3] : sans l'hypothèse de caractéristique nulle, sans supposer que tous les $\overline{K}$-endomorphismes de A sont définis sur K et sans faire d'extension de corps K' (et, plus secondairement, l'hypothèse $\mathcal{O}\subset N^{-1}\,\mathrm{End}\,A$ est plus faible que $\mathrm{End}\,A\subset\mathcal{O}$

et $N = [\mathcal{O} : \operatorname{End} A]$). Ceci admet des conséquences dans certains des résultats principaux de [3] : il est parfois possible de travailler avec des extensions de corps de degré plus petit. Le premier exemple est la proposition 10.1 de [3] qui vaut avec $[k_1 : k] \leq 2$ (on peut utiliser $k_1 = k'$ dans la démonstration). L'autre énoncé améliorable est le théorème 1.2 sous l'hypothèse (3). Nous en donnons une nouvelle version, après avoir rappelé les notations.

Soit k un corps de nombres. Soit A une variété abélienne sur k de dimension $g \geq 1$. Notons $\alpha(g) = 2^{10} g^3$ et

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

où $h_F(A)$ est la hauteur de Faltings stable de A. Nous utilisons la notation $\varphi\colon A \rightleftharpoons A'$ pour un couple d'isogénies $\varphi_1\colon A \to A'$ et $\varphi_2\colon A' \to A$ et écrivons $\deg \varphi = \max(\deg \varphi_1, \deg \varphi_2)$. Contrairement au reste du présent texte, nous précisons les corps de définition des isogénies et employons la notation $\operatorname{End}_{k'} A$ pour désigner les endomorphismes de l'extension des scalaires $A_{k'}$ de A à k' (extension quelconque de k).

Théorème 6.1. *Pour toute extension k' de k, il existe des entiers naturels non nuls t et $n_1, \ldots, n_t$, des variétés abéliennes $A_1, \ldots, A_t$ sur k' et un couple d'isogénies définies sur k'*

$$\varphi\colon A_{k'} \rightleftharpoons \prod_{i=1}^{t} A_i^{n_i}$$

de sorte que, pour tous $1 \leq i, j \leq t$,

(1) *si $i \neq j$, A_i et A_j ne sont pas isogènes sur k',*

(2) *A_i est simple sur k',*

(3) *$\operatorname{End}_{k'} A_i$ est un ordre maximal,*

(4) *$\deg \varphi \leq \kappa(A)$.*

Démonstration. Elle suit exactement celle du théorème 1.2 de [3] en ne changeant que ce qui concerne l'extension de corps : dans la proposition 6.4 assertion (3′) nous pouvons prendre $G = \{0\}$ d'après le théorème 1.1 du présent texte. Ensuite, dans la partie 9 de [3], au lieu de choisir $K = k_1$, nous prenons $K = k' \cap k_1$. Les A_i sont des sous-variétés abéliennes de A_K simples sur K et non isogènes sur K. Elles le restent sur k' car $\operatorname{End}_{k'} A = \operatorname{End}_K A$ vu que tous les endomorphismes de A sont définis sur k_1. □

Si nous voulons un énoncé de la même forme que le théorème 1.2 de [3] nous choisissons pour k' une extension sur laquelle tous les endomorphismes de A sont définis : par isogénie, il en va de même pour $\prod_{i=1}^{t} A_i^{n_i}$ et donc nous pouvons remplacer k' par $\overline{k'}$ dans les assertions (1) et (2). Alors la borne sur le degré de l'extension est celle de Silverberg $[k' : k] \leq 2(9g)^{4g}$ (voir [11]) beaucoup plus petite que $\kappa(A)^g$ dans [3].

Remarquons aussi que le théorème 1.3 de [3] est maintenant une conséquence directe du théorème 6.1 ci-dessus.

7. Théorèmes d'existence, cas simple

Dans cette partie et la prochaine, nous considérons la question suivante : étant donné un corps K, un entier g et un ordre $\mathcal{O}$, existe-t-il une variété abélienne A sur K de dimension g telle que $\operatorname{End} A \simeq \mathcal{O}$? Nous nous limitons presque exclusivement au cas où K est algébriquement clos de caractéristique nulle. Dans ce cadre, le problème devient indépendant de K.

Proposition 7.1. *Soient $\mathcal{O}$ un ordre et g un entier naturel. Les assertions suivantes sont équivalentes.*

(1) *Il existe une variété abélienne A sur $\overline{\mathbb{Q}}$ de dimension g telle que* $\operatorname{End} A \simeq \mathcal{O}$.

(2) *Pour tout corps algébriquement clos de caractéristique nulle K, il existe une variété abélienne A sur K de dimension g telle que* $\operatorname{End} A \simeq \mathcal{O}$.

(3) *Il existe un corps algébriquement clos de caractéristique nulle K et une variété abélienne A sur K de dimension g telle que* $\operatorname{End} A \simeq \mathcal{O}$.

Démonstration. Nous avons (1) $\Longrightarrow$ (2) par extension des scalaires et (2) $\Longrightarrow$ (3) tautologiquement. Si (3) est vraie, nous pouvons supposer sans perte de généralité que K est la clôture algébrique d'un corps K' de type fini sur $\mathbb{Q}$ sur lequel A est définie. Notons k la clôture algébrique de $\mathbb{Q}$ dans K' (qui est un corps de nombres). Pour tout anneau R de corps des fractions K', le k-schéma $S = \operatorname{Spec} R$ est géométriquement intègre. Nous pouvons bien sûr choisir R de type fini sur k et intégralement clos. Ensuite, quitte à restreindre S, nous pouvons supposer que A/K' s'étend en un schéma abélien $\mathcal{A}/S$. Nous sommes alors en mesure d'appliquer le corollaire 1.5 de [7] qui fournit un point fermé s de S tel que $\operatorname{End} \mathcal{A}_{\overline{s}} \simeq \operatorname{End} A_K \simeq \mathcal{O}$. Ceci nous donne bien (1) car la fibre géométrique $\mathcal{A}_{\overline{s}}$ est une variété abélienne sur $\overline{\mathbb{Q}}$ (identifié à la clôture algébrique du corps résiduel de s, lui-même extension finie de k). □

Par le même argument, l'exemple de la partie 11 de [3] peut être donné sur $\overline{\mathbb{Q}}$. Ici, nous nous ramènerons toujours à $K = \mathbb{C}$ pour profiter de la théorie analytique.

Lorsque $\mathcal{O}$ est maximal, le théorème 1.1 montre qu'il suffit de trouver A' sur K de dimension g avec $(\operatorname{End} A') \otimes \mathbb{Q} \simeq \mathcal{O} \otimes \mathbb{Q}$. Nous commençons donc notre étude en cherchant quelles sont les $\mathbb{Q}$-algèbres de la forme $(\operatorname{End} A) \otimes \mathbb{Q}$. Dans le cas où A est de plus supposée simple (autrement dit $(\operatorname{End} A) \otimes \mathbb{Q}$ est un corps) le théorème 7.3 donne une réponse complète essentiellement due à Albert et Shimura (mais il ne semble pas que la description explicite des exceptions (6)–(8) se trouve dans la littérature, ce qui nous a conduit à détailler une preuve).

Une anti-involution positive sur une $\mathbb{Q}$-algèbre $\mathfrak{A}$ de dimension finie est une application $\mathbb{Q}$-linéaire $\iota\colon \mathfrak{A} \to \mathfrak{A}$ telle que $\iota(\iota(x)) = x$, $\iota(xy) = \iota(y)\iota(x)$ si $x, y \in \mathfrak{A}$ et $\operatorname{Tr}_{\mathfrak{A}/\mathbb{Q}}(x\iota(x)) > 0$ pour tout $x \in \mathfrak{A}\backslash\{0\}$. Rappelons la classification d'Albert donnée page 201 de [6] (où les isomorphismes sont des isomorphismes de $\mathbb{R}$-algèbres).

Proposition 7.2. *Soit D un corps de dimension finie sur $\mathbb{Q}$. Il existe une anti-involution positive sur D si et seulement si l'une des quatre assertions suivantes est vraie.*

(I) $D \otimes \mathbb{R} \simeq \mathbb{R}^e$ *pour* $e \in \mathbb{N} \setminus \{0\}$.

(II) $D \otimes \mathbb{R} \simeq M_2(\mathbb{R})^e$ *pour* $e \in \mathbb{N} \setminus \{0\}$.

(III) $D \otimes \mathbb{R} \simeq \mathbb{H}^e$ *pour* $e \in \mathbb{N} \setminus \{0\}$.

(IV) $D \otimes \mathbb{R} \simeq M_d(\mathbb{C})^e$ *pour* $d, e \in \mathbb{N} \setminus \{0\}$ *et l'isomorphisme peut être choisi de sorte que l'anti-involution canonique de* $M_d(\mathbb{C})^e$ (*transconjugaison*) *laisse* D *stable.*

Le cas (I) caractérise les corps de nombres totalement réels. Dans les cas (II) et (III), D est une algèbre de quaternions sur un corps totalement réel ; elle est dite totalement indéfinie en (II) et totalement définie en (III). Dans le dernier cas, le centre K de D vérifie $K \otimes \mathbb{R} \simeq \mathbb{C}^e$ et K est stable par la conjugaison sur $\mathbb{C}^e$: ces deux conditions équivalent à dire que K est un corps CM c'est-à-dire une extension quadratique totalement imaginaire d'un corps totalement réel. En particulier ($d = 1$), les corps CM font partie de la classification et ce sont avec (I) les seuls corps commutatifs qui y apparaissent.

Grâce aux résultats d'Albert et de Shimura, nous pouvons donner la caractérisation complète des corps $(\mathrm{End}\, A) \otimes \mathbb{Q}$ où A est une variété abélienne de dimension fixée g sur un corps algébriquement clos de caractéristique nulle.

Théorème 7.3. *Soient* $g \geq 1$ *un entier et* D *un corps de dimension finie sur* $\mathbb{Q}$. *Il existe une variété abélienne complexe* A *de dimension* g *telle que* $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq D$ *si et seulement si les conditions suivantes sont remplies.*

(1) D *admet une anti-involution positive.*

(2) $[D : \mathbb{Q}]$ *divise* $2g$.

(3) *Si* D *est un corps de nombres totalement réel,* $[D : \mathbb{Q}]$ *divise* g.

(4) *Si* D *est une algèbre de quaternions totalement définie sur un corps totalement réel,* $[D : \mathbb{Q}] \neq 2g$.

(5) *Si* D *est un corps quadratique imaginaire,* $g \neq 2$.

(6) *Si* D *est le compositum de deux corps quadratiques imaginaires,* $g \neq 2$.

(7) *Si* D *est une algèbre de quaternions sur un corps quadratique imaginaire,* $g \neq 4$.

(8) *Si* D *est un corps de nombres CM extension galoisienne de* $\mathbb{Q}$ *de groupe de Galois le groupe diédral* D_4, $g \neq 4$.

Lorsque D est fixé, une seule des conditions (3) à (8) doit être vérifiée. Notons aussi que (3) concerne le cas (I) de la classification d'Albert, (4) le cas (III), tandis que (5)–(8) concernent des cas particuliers de (IV) où $[D : \mathbb{Q}] \in \{2, 4, 8\}$. Aucune condition n'est vide : pour (8) un exemple de D est $\mathbb{Q}(\sqrt{7}, \sqrt{\sqrt{2} - 3})$, pour (7) on peut prendre $D = K \oplus Ki \oplus Kj \oplus Kk$ où $K = \mathbb{Q}(\sqrt{-7})$ et $i^2 = j^2 = k^2 = ijk = -1$.

Corollaire 7.4. *Si* D *est un corps de dimension finie sur* $\mathbb{Q}$ *admettant une anti-involution positive, il existe une variété abélienne* A *sur* $\overline{\mathbb{Q}}$ *telle que* $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq D$. *Si* D *n'est pas un corps quadratique imaginaire, on peut choisir* $\dim A = [D : \mathbb{Q}]$.

Nous démontrons le théorème à partir des résultats de [9]. Tout d'abord si A existe alors (1) résulte de l'existence de l'involution de Rosati (associée à une polarisation) tandis que (2) traduit le fait que $\Omega_A \otimes \mathbb{Q}$ est un D-espace vectoriel à gauche lorsque Ω_A est le réseau des périodes de A de rang $2g$. L'assertion (3) découle du corollaire page 191 de [6] puisque dans ce cas-là l'involution de Rosati est l'identité.

Maintenant l'objet principal de [9] (repris dans le chapitre 9 de [2]) consiste à décrire pour chaque couple (D, g) vérifiant (1), (2) et (3), toutes les variétés abéliennes A sur $\mathbb{C}$ de dimension g munies d'une injection $D \hookrightarrow (\mathrm{End}\, A) \otimes \mathbb{Q}$. Ces variétés sont réparties en familles, dépendant de données supplémentaires, selon le type (I) à (IV) de D dans la classification d'Albert. Dans chaque famille (paramétrée par ce que l'on appelle aujourd'hui une variété de Shimura) le théorème 5 de [9] (ou le théorème 9.9.1 de [2]) donne une condition suffisante pour qu'il existe une variété abélienne A pour laquelle l'injection ci-dessus est un isomorphisme.

Pour les types (I) et (II) la condition est vide donc notre théorème est établi dans ces deux cas. Pour la suite, notons $m = 2g/[D : \mathbb{Q}]$. Dans le cas (III), la condition suffisante donnée par Shimura dépend de la donnée d'une matrice $T \in M_m(D)$: précisément (cas (a) et (b) de son théorème 5) elle garantit l'existence de A avec $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq D$ lorsque $m \geq 3$ ou lorsque $m = 2$ et la norme réduite de T dans le centre de D n'est pas le carré d'un élément totalement positif (voir aussi 9.10(2) de [2]). Par ailleurs, Shimura montre aussi (remarque 6 page 180 de [9]) que pour tout D de type (III) il existe $T \in M_2(D)$ dont la norme réduite n'est pas le carré d'un élément totalement positif. Ainsi, si l'on oublie la donnée supplémentaire T, la condition suffisante sur D est $m \geq 2$ soit $[D : \mathbb{Q}] \neq 2g$. Ceci montre que dans notre théorème si (4) est vérifiée alors A existe. Pour conclure le type (III), il s'agit de voir que si $[D : \mathbb{Q}] = 2g$ alors $(\mathrm{End}\, A) \otimes \mathbb{Q}$ n'est pas isomorphe à D. Or ceci résulte de la proposition 15 de [9] qui affirme que si D s'injecte dans $(\mathrm{End}\, A) \otimes \mathbb{Q}$ alors A n'est pas simple (voir aussi 9.10(1) de [2]).

Venons-en au type (IV). Ici la donnée supplémentaire pertinente est fournie par des entiers naturels $r_1, \ldots, r_e$ et $s_1, \ldots, s_e$ tels que $r_\nu + s_\nu = md$ pour $1 \leq \nu \leq e$ où e et d sont, comme dans la proposition 7.2, caractérisés par $D \otimes \mathbb{R} \simeq M_d(\mathbb{C})^e$. Alors le théorème 5 de [9] (ou 9.9.1 de [2]) assure l'existence de A avec $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq D$ dans une famille associée à $(r_\nu, s_\nu)_\nu$ dans tous les cas sauf lorsque le produit $r_\nu s_\nu$ est identiquement égal à 0 ou 1. Si $md \geq 3$ nous pouvons choisir $r_\nu = 2$, $s_\nu = md - 2$ pour tout ν pour éviter le cas défavorable. De même si $md = 2$ et $e \geq 2$ alors tout choix avec $r_1 = s_1 = 1$, $r_2 = 2$ et $s_2 = 0$ convient. Notre théorème est donc établi sauf dans les trois cas $(m, d, e) = (2, 1, 1)$, $(m, d, e) = (1, 2, 1)$ et $(m, d) = (1, 1)$ que nous étudions séparément.

Si $(m, d, e) = (2, 1, 1)$ alors $D \otimes \mathbb{R} \simeq \mathbb{C}$ donc D est un corps quadratique imaginaire et $g = m[D : \mathbb{Q}]/2 = 2$. Cette situation correspond donc au cas exclu par (5) dans le théorème. De même $(m, d, e) = (1, 2, 1)$ se traduit par $D \otimes \mathbb{R} \simeq M_2(\mathbb{C})$, $g = 4$ et la première condition signifie que D est une algèbre de quaternions sur son centre Z qui, vérifiant $Z \otimes \mathbb{R} \simeq \mathbb{C}$ (centre de $M_2(\mathbb{C})$), est un corps quadratique imaginaire. Ainsi ce cas reflète la condition (7) du théorème. Nous devons donc montrer que si $(dm, e) = (2, 1)$ alors il n'existe pas de variété abélienne A de

dimension $g = 2d$ avec $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq D$. Ceci va résulter des propositions 14, 18 et 19 de [9]. En effet, si $D \hookrightarrow (\mathrm{End}\, A) \otimes \mathbb{Q}$ alors A appartient à une famille avec $r_1 s_1 = 0$ ou $r_1 s_1 = 1$. Dans le premier cas, la proposition 14 de [9] (voir 9.10(3) de [2]) montre que A n'est pas simple (isogène à un produit de $md^2 \geq 2$ copies d'une autre variété abélienne). Lorsque $r_1 = s_1 = 1$, nous concluons aussi que $(\mathrm{End}\, A) \otimes \mathbb{Q}$ n'est pas isomorphe à D : c'est la proposition 18 de [9] (ou 9.10(4) de [2]) si $m = 2$ et la proposition 19 de [9] (ou 9.10(5) de [2]) si $m = 1$.

Enfin il nous reste à traiter le cas $md = 1$. Ici $e = g$ et $D \otimes \mathbb{R} \simeq \mathbb{C}^g$ donc D est un corps CM. La question posée revient à se demander si, un corps CM D étant fixé, il existe une variété abélienne CM A telle que $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq D$. La notion de type CM va nous permettre de répondre à cette question après plusieurs préliminaires.

Soit K un corps CM de degré $2g$. Notons K_0 son sous-corps totalement réel de degré g. Si L est un sous-corps de K, alors de deux choses l'une : ou bien L est contenu dans K_0 ce qui est équivalent à dire que L est totalement réel, ou bien L est un corps CM (en effet, comme L engendre K au-dessus de K_0, il ne peut avoir de places réelles donc $L \otimes \mathbb{R} \simeq \mathbb{C}^h$ pour $h \mid g$ et L est stable par la conjugaison puisque qu'il s'écrit comme l'intersection de K et $L \otimes \mathbb{R}$ tous deux stables).

Un type CM de K (ou simplement un type) est une structure complexe sur $K \otimes \mathbb{R}$, autrement dit un morphisme de $\mathbb{R}$-algèbres $\mathbb{C} \to K \otimes \mathbb{R}$. On dit qu'un tel type provient d'un sous-corps L si ce morphisme se factorise à travers $L \otimes \mathbb{R} \subset K \otimes \mathbb{R}$ (le sous-corps L est nécessairement CM). Il est clair sur cette définition que si un type provient d'un sous-corps L il provient également de tout sous-corps L' de K contenant L. De même, deux types provenant de deux sous-corps CM coïncident si et seulement s'ils proviennent d'un même type de leur intersection (et donc ceci n'est possible que si cette intersection est elle-même un corps CM). Comme $K \otimes \mathbb{R} \simeq \mathbb{C}^g$, il y a exactement 2^g types de K.

Les types de K classifient les variétés abéliennes A sur $\mathbb{C}$ de dimension g munies d'une injection $\iota\colon K \hookrightarrow (\mathrm{End}\, A) \otimes \mathbb{Q}$ à isogénies près (voir les pages 210 à 214 de [6]). De plus une telle variété est simple (autrement dit ι est un isomorphisme) si et seulement si le type correspondant de K est primitif (cette propriété est énoncée pages 213–214 de [6] et démontrée au paragraphe 8.2 de [10]). Ceci nous donne le critère suivant.

Lemme 7.5. *Soit K un corps CM de degré $2g$. Il y a équivalence entre :*

(1) *Il existe une variété abélienne complexe A de dimension g pour laquelle*

$$(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq K.$$

(2) *Il existe un type primitif de K.*

Au vu des cas déjà établis ci-dessus, le théorème 7.3 est une conséquence de la caractérisation suivante.

Proposition 7.6. *Soit K un corps CM. Il y a équivalence entre :*

(1) *Aucun type de K n'est primitif.*

(2) *L'extension $K/\mathbb{Q}$ est galoisienne de groupe $(\mathbb{Z}/2\mathbb{Z})^2$ ou D_4.*

Pour obtenir exactement la formulation du théorème, il faut encore remarquer qu'un corps CM de degré 4 est galoisien de groupe $(\mathbb{Z}/2\mathbb{Z})^2$ si et seulement si c'est le compositum de deux corps quadratiques imaginaires.

Nous terminons donc la démonstration du théorème 7.3 en établissant cette proposition. Nous transitons par deux lemmes sur les extensions de corps (pour ceux-ci K n'est plus un corps CM).

Soit L/K une extension de corps finie et séparable. Nous appelons sous-corps maximal de L/K un élément maximal pour l'inclusion de l'ensemble des sous-corps stricts de L contenant K. Nous notons $m_{L/K}$ le nombre de sous-corps maximaux de L/K. La théorie de Galois permet de donner les majorations suivantes (entre autres).

Lemme 7.7. *Nous avons toujours $m_{L/K} \leq [L : K] - 1$. Si L/K n'est pas galoisienne et si n est le plus petit diviseur ≥ 3 de $[L : K]$, nous avons*

$$m_{L/K} \leq \frac{n[L : K]}{2(n-1)} - 1.$$

Démonstration. Notons N/K une clôture normale de L/K, $G = \mathrm{Gal}(N/K)$, $H = \mathrm{Gal}(N/L)$ et H' le normalisateur de H dans G. Les sous-corps maximaux de L/K sont en bijection avec les sous-groupes P de G contenant strictement H et minimaux pour cette propriété. Notons $\mathcal{P}$ leur ensemble et $\mathcal{P}_1 = \{P \in \mathcal{P} \mid P \subset H'\}$, $\mathcal{P}_2 = \mathcal{P} \setminus \mathcal{P}_1$. Par minimalité, si $P, P' \in \mathcal{P}$ et $P \neq P'$ nous avons $P \cap P' = H$; de même si $P \in \mathcal{P}_2$ alors $P \cap H' = H$. Ainsi

$$\bigcup_{P \in \mathcal{P}_1} P \setminus H \subset H' \setminus H \quad \text{et} \quad \bigcup_{P \in \mathcal{P}_2} P \setminus H \subset G \setminus H'$$

où les unions sont disjointes. Si $P \in \mathcal{P}$, $P \neq H$ donne $[P : H] \geq 2$ donc $\operatorname{Card} P \setminus H \geq \operatorname{Card} H$. Mieux, si $P \in \mathcal{P}_2$, $[P : H] = 2$ est exclu car sinon H serait distingué dans P d'où $P \subset H'$; par suite, comme $[P : H] \mid [G : H] = [L : K]$, nous avons $[P : H] \geq n$ et $\operatorname{Card} P \setminus H \geq (n-1) \operatorname{Card} H$. Il vient

$$\begin{aligned} m_{L/K} = \operatorname{Card} \mathcal{P} = \operatorname{Card} \mathcal{P}_1 + \operatorname{Card} \mathcal{P}_2 &\leq \frac{\operatorname{Card} H' \setminus H}{\operatorname{Card} H} + \frac{\operatorname{Card} G \setminus H'}{(n-1) \operatorname{Card} H} \\ &= \frac{n-2}{n-1} \cdot \frac{\operatorname{Card} H' \setminus H}{\operatorname{Card} H} + \frac{\operatorname{Card} G \setminus H}{(n-1) \operatorname{Card} H}. \end{aligned}$$

Ceci s'écrit encore

$$m_{L/K} \leq \frac{1}{n-1} \Big(1 + \frac{n-2}{[G : H']}\Big) [G : H] - 1.$$

Nous trouvons alors les formules de l'énoncé en utilisant $[G : H'] \geq 1$ en général et $[G : H'] \geq 2$ si L/K n'est pas galoisienne ($G \neq H'$ car H n'est pas distingué dans G). □

Remarquons que lorsque $[L : K]$ est impair le même argument donne $m_{L/K} \leq ([L : K] - 1)/(n-1)$ indépendamment du caractère galoisien ou non de l'extension. Nous utiliserons la conséquence suivante.

Lemme 7.8. *Si* 4 *ne divise par* $[L : K]$ *alors* $m_{L/K} \leq 2^{[L:K]/3}$. *Si* $[L : K]$ *est divisible par* 4 *alors* $m_{L/K} \leq 2^{[L:K]/4}$ *sauf si* L/K *est galoisienne et que son groupe de Galois est isomorphe à l'un des trois groupes* $(\mathbb{Z}/2\mathbb{Z})^2$, $(\mathbb{Z}/2\mathbb{Z})^3$ *ou* D_4.

Démonstration. Une vérification élémentaire montre que $a - 1 \leq 2^{a/3}$ pour tout entier naturel $a \notin \{4, 5, 6, 7, 8\}$. Par le lemme précédent, ceci suffit à montrer la première assertion si $[L : K] \notin \{5, 6, 7\}$. Lorsque $[L : K] = 5, 7$, le seul sous-corps strict de L contenant K est K donc $m_{L/K} = 1$. Si $[L : K] = 6$, le lemme précédent (avec $n = 3$) fournit $m_{L/K} \leq 7/2 \leq 2^{6/3}$ lorsque L/K n'est pas galoisienne ; si elle l'est soit $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/6\mathbb{Z}$ et $m_{L/K} = 2$, soit $\mathrm{Gal}(L/K) \simeq \mathfrak{S}_3$ et $m_{L/K} = 4$, en comptant les sous-groupes non triviaux minimaux. Nous procédons de même pour la seconde assertion. Nous avons $4a - 1 \leq 2^a$ pour tout entier $a \geq 4$ donc $m_{L/K} \leq [L : K] - 1$ suffit lorsque $[L : K] \notin \{4, 8, 12\}$. Dans ces trois cas, si L/K n'est pas galoisienne, la formule avec respectivement $n = 4$, $n = 4$ et $n = 3$ fournit $m_{L/K} \leq 5/3$, $m_{L/K} \leq 13/3$ et $m_{L/K} \leq 8$ qui entraînent bien $m_{L/K} \leq 2^{[L/K]/4}$ ($m_{L/K}$ étant entier). Il reste à examiner les douze groupes de cardinal 4, 8 ou 12 et à compter leurs sous-groupes minimaux (c'est-à-dire isomorphes à $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$). Par une étude de cas, on constate alors $m_{L/K} \leq 1$ en degré 4, $m_{L/K} \leq 3$ en degré 8 et $m_{L/K} \leq 8$ en degré 12 sauf pour les trois groupes de l'énoncé pour lesquels $m_{L/K}$ vaut respectivement 3, 7 et 5. □

Démonstration de la proposition 7.6. Comme $K/\mathbb{Q}$ admet un sous-corps maximal totalement réel K_0 unique, le nombre de sous-corps CM maximaux vaut $m_{K/\mathbb{Q}} - 1$. Notons d le degré maximal d'un sous-corps CM strict de K. Il y a donc au plus $(m_{K/\mathbb{Q}} - 1)2^{d/2} < m_{K/\mathbb{Q}}2^{d/2}$ types non primitifs de K. En particulier si $m_{K/\mathbb{Q}}2^{d/2} \leq 2^{[K:\mathbb{Q}]/2}$ alors il existe un type primitif sur K. Supposons $[K : \mathbb{Q}] \notin 4\mathbb{Z}$ alors $d \leq [K : \mathbb{Q}]/3$ (puisqu'un corps CM est de degré pair). Comme le lemme 7.8 nous donne $m_{K/\mathbb{Q}} \leq 2^{[K:\mathbb{Q}]/3}$ nous avons toujours $m_{K/\mathbb{Q}}2^{d/2} \leq 2^{[K:\mathbb{Q}]/2}$. Supposons maintenant que 4 divise $[K : \mathbb{Q}]$. L'estimation triviale $d \leq [K : \mathbb{Q}]/2$ montre que si $m_{K/\mathbb{Q}} \leq 2^{[K:\mathbb{Q}]/4}$ alors K admet un type primitif. Vu le lemme 7.8, il nous reste seulement à étudier les trois cas où $K/\mathbb{Q}$ est galoisienne de groupe $(\mathbb{Z}/2\mathbb{Z})^2$, $(\mathbb{Z}/2\mathbb{Z})^3$ ou D_4. Si $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$, le corps K admet $m_{K/\mathbb{Q}} - 1 = 2$ sous-corps CM de degré 2 ; chacun induit 2 types de K et les 4 types obtenus sont distincts puisque l'intersection des deux sous-corps CM est $\mathbb{Q}$. Ainsi aucun des 4 types de K n'est primitif. Lorsque $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$, nous avons 6 sous-corps CM de degré 4. Chacun est galoisien de groupe $(\mathbb{Z}/2\mathbb{Z})^2$ donc, par le cas précédent, n'admet pas de type primitif. Par suite, tous les types non primitifs de K proviennent de ses sous-corps CM de degré 2. Sur les 7 sous-corps quadratiques de K (en bijection avec les 7 sous-groupes d'indice 2 de $(\mathbb{Z}/2\mathbb{Z})^3$), trois sont totalement réel puisque $\mathrm{Gal}(K_0/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ donc 4 sont CM. On en déduit que K possède 8 types non primitifs et donc également 8 types primitifs. Finalement supposons $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_4$. Ici l'automorphisme de conjugaison $K \to K$ est l'unique élément non trivial du centre de D_4 donc $\mathrm{Gal}(K_0/\mathbb{Q}) \simeq D_4/Z(D_4) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Il y a donc trois sous-corps quadratiques réels et donc aucun sous-corps CM de degré 2 puisque D_4 n'a que 3 sous-groupes de cardinal 4. Par suite tous les types

provenant des sous-corps CM maximaux (de degré 4) sont distincts donc il y a $(m_{K/\mathbb{Q}} - 1) \cdot 4 = 16$ types non primitifs et donc aucun type primitif de K. □

Nous avons donc entièrement établi le théorème 7.3 qui donne une condition nécessaire et suffisante sur un couple (D, g) pour qu'il existe une variété abélienne A sur $\overline{\mathbb{Q}}$ de dimension g telle que $(\operatorname{End} A) \otimes \mathbb{Q} \simeq D$. Pour conclure le cas simple, il nous reste à nous demander si, un ordre $\mathcal{O}$ de D étant fixé, nous pouvons de plus obtenir $\operatorname{End} A \simeq \mathcal{O}$. Nous avons déjà dit plus haut que ceci est automatique grâce au théorème 1.1 lorsque $\mathcal{O}$ est maximal. En fait le résultat suivant prouve que c'est également le cas pour un ordre quelconque.

Lemme 7.9. *Soient K un corps algébriquement clos de caractéristique nulle et A une variété abélienne simple sur K. Pour tout ordre $\mathcal{O}$ de $(\operatorname{End} A) \otimes \mathbb{Q}$, il existe une variété abélienne A' sur K isogène à A telle que $\operatorname{End} A' \simeq \mathcal{O}$.*

Démonstration. On peut supposer que K est un sous-corps de $\mathbb{C}$. Alors l'extension des scalaires $A_{\mathbb{C}}$ est un tore complexe V/Ω_A et $E = \Omega_A \otimes \mathbb{Q}$ est un espace vectoriel (à gauche) sur le corps $D = (\operatorname{End} A) \otimes \mathbb{Q}$. Notons Λ l'image réciproque de $\mathcal{O}^n$ dans un isomorphisme $E \simeq D^n$. Alors $\{x \in D \mid x\Lambda \subset \Lambda\} = \mathcal{O}$ ce qui entraîne que $\mathcal{O}$ est isomorphe à l'anneau des endomorphismes du tore complexe $A' = V/\Lambda$. De plus A' est une variété abélienne définie sur K puisqu'elle est isogène à A (quotient par un groupe fini, défini sur le corps clos K). □

Cet énoncé ne s'étend pas en caractéristique non nulle : par exemple sur $\overline{\mathbb{F}_p}$ si A est une courbe elliptique supersingulière alors $\operatorname{End} A$ est toujours un ordre maximal (voir le théorème 4.2 de [13]).

8. Théorèmes d'existence, cas général

Nous poursuivons l'étude de la partie précédente sans hypothèse de simplicité. Comme plus haut, nous considérons d'abord les algèbres de la forme $(\operatorname{End} A) \otimes \mathbb{Q}$. Elles sont semi-simples et admettent une anti-involution positive. Leur classification se ramène immédiatement à celle d'Albert en vertu de l'énoncé suivant.

Proposition 8.1. *Soient $n_1, \dots, n_s$ des entiers naturels non nuls et $D_1, \dots, D_s$ des corps de dimension finie sur $\mathbb{Q}$. S'il existe une anti-involution positive sur l'algèbre $\prod_{i=1}^s M_{n_i}(D_i)$ alors il existe une anti-involution positive sur chaque D_i.*

Démonstration. Montrons d'abord que nous pouvons supposer $s = 1$ dans l'énoncé. Dans l'algèbre $\prod_{i=1}^s M_{n_i}(D_i)$ notons $\{e_1, \dots, e_s\}$ l'unique famille d'idempotents centraux non nuls tels que $e_1 + \cdots + e_s = 1$: il s'agit des s-uplets avec une seule composante non nulle égale à la matrice identité. L'involution ι préserve ces propriétés donc permute les e_i. De plus la positivité entraîne $e_i \iota(e_i) \neq 0$ ce qui force $\iota(e_i) = e_i$. Nous en déduisons que ι se décompose comme un produit d'involutions sur les s facteurs, qui sont encore positives. Il suffit donc de traiter le cas $s = 1$ et nous notons plutôt $n = n_1$, $D = D_1$.

L'anti-involution $\iota\colon M_n(D) \to M_n(D)$ s'identifie à un morphisme d'anneaux $M_n(D) \to M_n(D)^{\mathrm{op}}$ que nous pouvons composer avec l'isomorphisme de transposition $M_n(D)^{\mathrm{op}} \to M_n(D^{\mathrm{op}})$. Nous appliquons alors le théorème d'isomorphisme de la page 206 de [4] qui montre qu'il existe un isomorphisme de corps $\sigma\colon D \to D^{\mathrm{op}}$ tel que l'isomorphisme $M_n(D) \to M_n(D^{\mathrm{op}})$ est la conjugaison par un isomorphisme $D^n \to (D^{\mathrm{op}})^n$ σ-semi-linéaire. Si nous reformulons ceci sans parler d'anneaux opposés, nous avons un anti-isomorphisme $D \to D$ (correspondant à σ) que nous notons $x \mapsto x^*$ et étendons à $M_n(D)$ par $(a_{ij})^* = (a_{ji}^*)$ ainsi qu'une matrice inversible $A \in M_n(D)$ telle que $\iota(M) = AM^*A^{-1}$ pour tout $M \in M_n(D)$.

Le centre Z de D est stable par $*$ et si $x \in Z$ nous avons $\iota(xI) = A(x^*I)A^{-1} = x^*I$ (où I est la matrice identité) ce qui entraîne en particulier $x^{**} = x$. Ainsi $x \mapsto x^{**}$ est un automorphisme de la Z-algèbre centrale simple D donc est intérieur (théorème de Skolem–Noether, donné comme corollaire page 222 de [4]) : il existe $b \in D^\times$ tel que $x^{**} = bxb^{-1}$ pour tout $x \in D$. Bien entendu, nous pouvons multiplier b par un élément de $Z^\times$ sans changer cette propriété. Pour une matrice M quelconque de $M_n(D)$ nous écrivons maintenant

$$M = \iota(\iota(M)) = A(AM^*A^{-1})^*A^{-1} = AA^{*-1}M^{**}A^*A^{-1} = AA^{*-1}bMb^{-1}A^*A^{-1}.$$

Nous en déduisons que $AA^{*-1}b$ est centrale donc de la forme αI, $\alpha \in Z^\times$. En remplaçant b par $b\alpha^{-1}$ nous supposons $AA^{*-1}b = I$ d'où $A^* = bA$.

Pour $x \in D$, nous posons à présent $M = A \cdot \mathrm{diag}(x, 0, \dots, 0)$. Nous avons $\iota(M) = A \cdot \mathrm{diag}(x^*, 0, \dots, 0)b$. Notons a le coefficient d'indice $(1,1)$ de A. La formule $A^* = bA$ donne en particulier $a^* = ba$. Un simple calcul matriciel montre que le seul coefficient diagonal éventuellement non nul de $M\iota(M)$ est $axax^*b$. L'hypothèse de positivité fournit donc $\mathrm{Tr}_{D/\mathbb{Q}}(axax^*b) > 0$ pour tout $x \neq 0$. En particulier a n'est pas nul donc nous pouvons poser, pour tout $y \in D$, $y^\dagger = ay^*a^{-1}$. Ceci nous définit un anti-isomorphisme et même, comme $y^{\dagger\dagger} = aa^{*-1}y^{**}a^*a^{-1} = aa^{*-1}byb^{-1}a^*a^{-1} = y$, une anti-involution. Enfin, si nous définissons x par $y = ax$, nous trouvons $yy^\dagger = axax^*b$ et nous en déduisons immédiatement que $\dagger$ est une anti-involution positive sur D. □

Ainsi, si nous disposons d'une algèbre semi-simple $\mathfrak{A}$ sur $\mathbb{Q}$ admettant une anti-involution positive, d'un corps K et d'un entier g, l'existence d'une variété abélienne A sur K de dimension g avec $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq \mathfrak{A}$ est équivalente, en écrivant $\mathfrak{A} \simeq \prod_{i=1}^s M_{n_i}(D_i)$, à l'existence d'entiers g_i tels que le problème pour (K, D_i, g_i) ait une solution pour $1 \leq i \leq s$ et $g = \sum_{i=1}^s n_i g_i$. En particulier nous avons une condition explicite lorsque K est algébriquement clos de caractéristique nulle avec le théorème 7.3. Citons une forme faible sans dimension.

Corollaire 8.2. *Si $\mathfrak{A}$ est une $\mathbb{Q}$-algèbre semi-simple de dimension finie admettant une anti-involution positive alors il existe une variété abélienne A sur $\overline{\mathbb{Q}}$ telle que* $(\mathrm{End}\, A) \otimes \mathbb{Q} \simeq \mathfrak{A}$.

Venons-en maintenant au problème plus précis où un ordre $\mathcal{O}$ de $\mathfrak{A}$ est fixé. Ici à nouveau (théorème 1.1) lorsque $\mathcal{O}$ est maximal il n'y a pas de contrainte supplémentaire. En revanche, la situation est différente pour un ordre non maximal

car le lemme 7.9 est faux sans l'hypothèse de simplicité. En effet, l'exemple suivant montre que, dans la classe d'isogénie du cube E^3 d'une courbe elliptique non CM, on ne peut pas obtenir tous les ordres de $\mathrm{End}(E^3)\otimes\mathbb{Q}\simeq M_3(\mathbb{Q})$ (alors que, répétons-le, on peut obtenir tous les ordres maximaux).

Exemple 8.3. *Soit p un nombre premier. Il n'existe pas de variété abélienne complexe de dimension 3 dont l'anneau des endomorphismes soit isomorphe au sous-anneau $\mathcal{O}$ de $M_3(\mathbb{Z})$ formé des matrices dont la réduction modulo p est triangulaire supérieure.*

Démonstration. Notons $(e_{ij})_{1\leq i,j\leq 3}$ la base canonique de $M_3(\mathbb{Z})$ où le seul coefficient non nul de la matrice e_{ij} est celui d'indice (i,j) égal à 1. Imaginons que A soit une variété abélienne complexe telle que $\mathrm{End}\,A\simeq\mathcal{O}$. Il existe A' isogène à A telle que $\mathrm{End}\,A'\simeq M_3(\mathbb{Z})$. Ceci force A' à être isomorphe au cube E^3 d'une courbe elliptique E avec $\mathrm{End}\,E=\mathbb{Z}$. Nous pouvons donc identifier Ω_A à un sous-réseau de Ω_E^3. Comme les projecteurs e_{11}, e_{22} et e_{33} appartiennent à $\mathcal{O}$, ce réseau doit s'écrire $\Lambda_1\oplus\Lambda_2\oplus\Lambda_3$ où $\Lambda_i\subset\Omega_E$. Avec $e_{12}\in\mathcal{O}$ et $e_{23}\in\mathcal{O}$, nous voyons $\Lambda_3\subset\Lambda_2\subset\Lambda_1$ tandis que $pe_{31}\in\mathcal{O}$ fournit $p\Lambda_1\subset\Lambda_3$. Comme $[\Lambda_1:p\Lambda_1]=p^2$ les trois inclusions obtenues ne peuvent pas être toutes strictes. Pourtant $\Lambda_1=\Lambda_2$ conduit à $e_{21}\in\mathcal{O}$, $\Lambda_2=\Lambda_3$ à $e_{32}\in\mathcal{O}$ et $p\Lambda_1=\Lambda_3$ à $p^{-1}e_{13}\in\mathcal{O}$ ce qui est à chaque fois faux. Notre hypothèse n'était donc pas correcte. □

Compte tenu de cet exemple, il semble difficile de donner un critère simple sur un couple $(\mathcal{O},g)$ pour qu'il existe $A/\mathbb{C}$ de dimension g avec $\mathrm{End}\,A\simeq\mathcal{O}$. Toutefois, avec un peu de liberté sur la dimension, nous pouvons démontrer le résultat d'existence général suivant pour un ordre quelconque.

Théorème 8.4. *Si $\mathcal{O}$ est un ordre tel que $\mathcal{O}\otimes\mathbb{Q}$ est une algèbre semi-simple admettant une anti-involution positive alors il existe une variété abélienne A sur $\overline{\mathbb{Q}}$ avec* $\mathrm{End}\,A\simeq\mathcal{O}$ *et* $\dim A\leq \mathrm{rg}_{\mathbb{Z}}\,\mathcal{O}$.

Démonstration. Nous choisissons un isomorphisme entre $\mathcal{O}\otimes\mathbb{Q}$ et un produit $\prod_{i=1}^s M_{n_i}(D_i)$ avec des corps D_i et des entiers $n_i\geq 1$. D'après la proposition 8.1, chaque D_i admet une anti-involution positive et donc d'après le théorème 7.3 il existe une variété abélienne complexe A_i avec $(\mathrm{End}\,A_i)\otimes\mathbb{Q}\simeq D_i$ ainsi que $\dim A_i=n_i[D_i:\mathbb{Q}]$ ou $\dim A_i=n_i[D_i:\mathbb{Q}]/2$ (le premier choix est toujours possible sauf si D_i est un corps quadratique imaginaire et $n_i=1$ auquel cas le second, $\dim A_i=1$, convient). La variété abélienne $A'=\prod_{i=1}^s A_i^{n_i}$ a pour dimension $\sum_{i=1}^s n_i\dim A_i\leq\sum_{i=1}^s n_i^2[D_i:\mathbb{Q}]=\mathrm{rg}_{\mathbb{Z}}\,\mathcal{O}$ et nous pouvons identifier $(\mathrm{End}\,A')\otimes\mathbb{Q}$ à $\mathcal{O}\otimes\mathbb{Q}$. Pour trouver A isogène à A' telle que $\mathrm{End}\,A\simeq\mathcal{O}$ il suffit de trouver un réseau Λ de $\Omega_A\otimes\mathbb{Q}$ tel que $\{x\in(\mathrm{End}\,A')\otimes\mathbb{Q}\mid x\Lambda\subset\Lambda\}=\mathcal{O}$. Par construction, $\Omega_{A_i}\otimes\mathbb{Q}$ s'écrit comme D_i-espace vectoriel (à gauche) sous la forme $V_i^{n_i}$ où $V_i\simeq D_i$ ou $V_i\simeq D_i^2$. Ceci montre que $\Omega_{A_i^{n_i}}\otimes\mathbb{Q}$ s'identifie à $M_{n_i}(D_i)$ ou $M_{n_i}(D_i)^2$ comme $\mathrm{End}(A_i^{n_i})\otimes\mathbb{Q}$-module à gauche. Ainsi si $I=\{i\mid 1\leq i\leq s,\ \dim A_i=n_i[D_i:\mathbb{Q}]\}$ et si p désigne la projection

$$\mathcal{O}\otimes\mathbb{Q}\simeq\prod_{i=1}^s M_{n_i}(D_i)\longrightarrow\prod_{i\in I}M_{n_i}(D_i)$$

alors $\Omega_{A'} \otimes \mathbb{Q}$ s'identifie à $\mathcal{O} \otimes \mathbb{Q} \oplus p(\mathcal{O} \otimes \mathbb{Q})$ comme $\mathcal{O} \otimes \mathbb{Q}$-module. Par suite le choix $\Lambda = \mathcal{O} \oplus p(\mathcal{O})$ convient. □

Références

[1] Bertrand, D.: Minimal heights and polarizations on abelian varieties. Prépublication Mathematical Sciences Research Institute 06220–87, 1987.

[2] Birkenhake, C. et Lange, H.: *Complex abelian varieties*. Grundlehren der Mathematischen Wissenschaften 302, Springer-Verlag, Berlin, 1992.

[3] Gaudron, É. et Rémond, G.: Polarisations et isogénies. *Duke Math. J.* **163** (2014), no. 11, 2057–2108.

[4] Jacobson, N.: *Basic algebra II*. Seconde édition. W. H. Freeman and Company, New York, 1989.

[5] Lenstra, H. W., Oort, F. et Zarhin, Yu. G.: Abelian subvarieties. *J. Algebra* **180** (1996), no. 2, 513–516.

[6] Mumford, D.: *Abelian varieties*. Oxford University Press, London, 1974.

[7] Noot, R.: Abelian varieties – Galois representation and properties of ordinary reduction. *Compositio Math.* **97** (1995), no. 1-2, 161–171.

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

[9] Shimura, G.: On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)* **78** (1963), 149–192.

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

[11] Silverberg, A.: Fields of definition for homomorphisms of abelian varieties. *J. Pure Appl. Algebra*. **77** (1992), no. 3, 253–262.

[12] Swan, R.: Projective modules over group rings and maximal orders. *Ann. of Math. (2)* **76** (1962), 55–61.

[13] Waterhouse, W.: Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.

Reçu le 17 julliet 2015.

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