Décompte de polarisations de degré donné

María Carrizosa

1er septembre 2020

Résumé

Nous calculons une borne pour le nombre de classes de polarisations de degré donné pour une variété abélienne A définie sur un corps quelconque. Cette borne dépend de la dimension de la variété, du rang du $\mathbb{Z}$-module libre $\mathrm{End}(A)$ des endomorphismes de A et du discriminant de $\mathrm{End}(A)$. Nous utilisons des idées classiques de la théorie des groupes algébriques et plus précisément un résultat de Borel et Harish-Chandra dans l'étude des sous-groupes artihmétiques des groupes réductifs.

Abstract

An abelian variety can be endowed with a polarization of fixed degree in only a finite number of essentially different ways. We give a bound for this number using classical ideas from the theory of algebraic groups, and more precisely a theorem of Borel and Harish-Chandra concerning arithmetic subgroups of reductive groups.

1 Introduction

Si l'on dispose d'une polarisation $\phi_{\mathcal{L}}$ de degré d sur une variété abélienne A, on peut produire de nouvelles polarisations de degré d en faisant agir le groupe d'automorphismes de la variété sur la polarisation par

$$\phi_{\mathcal{L}} \cdot g = \phi_{g^*\mathcal{L}},$$

où $g \in \mathrm{Aut}(A)$. Il est donc naturel de regarder les classes de polarisations de degré donné modulo cette action. Narasimhan et Nori ont montré dans [13] qu'il n'y a qu'un nombre fini de classes. Leur preuve cependant ne permet pas de calculer ou borner ce nombre puisqu'elle utilise entre autres un argument de compacité qui n'est pas effectif.

Des bornes ont été calculées par plusieurs auteurs (Hayashida, Nishi, Lange, Rotger,...) pour le nombre de classes de polarisations principales (de degré 1) pour des variétés abéliennes particulières : pour un produit de 2 courbes elliptiques ([8], [9]), pour une variété abélienne simple de dimension un entier impair sans facteur carré ([15], [10]), ou pour une puissance d'une courbe elliptique non CM ([11]). À titre d'exemple le résultat de [10] est le suivant : le nombre de classes de polarisations principales d'une variété abélienne complexe simple A telle que $\mathrm{End}(A) \otimes \mathbb{Q} = K$ soit un corps totalement réel et telle que $\dim(A) = [K : \mathbb{Q}]$ est inférieur ou égal à h^+/h où h (resp. h^+) est le nombre de classes (resp. nombre de classes restreint) de K. Si $\mathrm{End}(A)$ est un ordre maximal dans K et l'ensemble de polarisations principales n'est pas vide, on a égalité.

On sait aussi qu'on ne peut pas espérer obtenir une borne qui ne dépend que de la dimension de la variété abélienne et du degré des polarisations : on pourra voir [15] où on construit pour g un entier pair quelconque une variété abélienne simple de dimension g dont le nombre de classes de polarisations principales est arbitrairement grand.

Nous calculons une borne pour le nombre de classes de polarisations de degré donné pour une variété abélienne A définie sur un corps quelconque. Cette borne dépend de la dimension de la variété, du rang et du discriminant du $\mathbb{Z}$-module libre $\mathrm{End}(A)$ des endomorphismes de A, et d'une polarisation fixée. Plus précisément on montre

Théorème 1.1. *Soient A une variété abélienne sur un corps K et d un entier naturel non nul. Soient $\mathcal{L}_0$ une polarisation sur A et $h_0 = h^0(A, \mathcal{L}_0)$ la racine de son degré. On note P l'ensemble de classes de polarisations sur A de degré d pour l'action naturelle de $\mathrm{Aut}\, A$. Alors*

$$\mathrm{Card}(P) \leq (n^6 D h_0^g d)^{2n^6}$$

où $g = \dim A$, $n = \mathrm{rg}(\mathrm{End}(A))$ et D est le discriminant de $\mathrm{End}(A)$.

On remarque que l'on peut donner une borne qui ne dépend que des paramètres g, D et d. En effet, on sait que $n \leq 4g^2$ (on a même $n \leq 2g^2$ si K est de caractéristique 0). Quant à h_0, dès que l'ensemble P est non vide, on peut considérer $\mathcal{L}_0 \in P$ et dans ce cas $h_0^2 = d$.

D'autre part, à partir de la borne du théorème ci-dessus et des résultats établis par É. Gaudron et G. Rémond dans [7] on peut donner une variante de ce résultat lorsque K est un corps de nombres. En effet, dans [7] (théo. 1.9) les auteurs prouvent les résultats suivants :

Théorème 1.2. *(G-R) Soit A une variété abélienne définie sur un corps de nombres K. On pose $g = \dim A$, $h_F(A)$ la hauteur de Faltings de A, D le discriminant de $\mathrm{End}(A)$ et $\Xi(A) = \Big((7g)^{8g^2}[K:\mathbb{Q}]\max(1, \log[K:\mathbb{Q}], h_F(A)\Big)^{2g^2}$. Alors*

1. *Il existe une polarisation $\mathcal{L}_0$ sur A telle que $h^0(A, \mathcal{L}_0) \leq \frac{1}{g!}\,\Xi(A)^{3/2}$.*
2. *On a la majoration $D \leq g^n\,\Xi(A)^g$.*

On en déduit :

Théorème 1.3. *Soient A une variété abélienne de dimension g sur un corps de nombres K et d un entier naturel non nul. Soit P l'ensemble de classes de polarisations sur A de degré d pour l'action naturelle de $\mathrm{Aut}\, A$. Alors*

$$\mathrm{Card}(P) \leq \big((7g)^9[K:\mathbb{Q}]\max(1, \log[K:\mathbb{Q}], h_F(A))\big)^{640g^{17}} d^{32g^8}.$$

La preuve du théorème 1.1 repose sur l'idée initiale de Narasimhan et Nori et sur la théorie développée par Borel et Harish-Chandra dans l'étude des représentations des sous-groupes arithmétiques des groupes réductifs ([1],[2]).

Le début de la preuve est assez classique. Pour étudier l'ensemble des polarisations (classes amples dans le groupe de Néron-Severi $\mathrm{NS}(A)$) on le plonge dans l'algèbre semi-simple $\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}A \otimes \mathbb{Q}$ à l'aide d'une polarisation préalablement choisie $\phi_{\mathcal{L}_0}$ de degré d_0 grâce à l'application

$$\begin{array}{rcl} \iota : \mathrm{NS}(A) & \hookrightarrow & \mathrm{End}_{\mathbb{Q}}(A) \\ \mathcal{L} & \longmapsto & \phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}}. \end{array}$$

L'algèbre $\mathrm{End}_{\mathbb{Q}}(A)$ est munie de l'involution de Rosati $\dagger$ associée à $\mathcal{L}_0$ par

$$f^\dagger = \phi_{\mathcal{L}_0}^{-1} \circ \hat{f} \circ \phi_{\mathcal{L}_0}.$$

De plus l'action de $\mathrm{Aut}(A)$ sur $\mathrm{NS}(A)$ est compatible avec l'action naturelle (à droite) de $\mathrm{Aut}(A)$ sur $\mathrm{End}_{\mathbb{Q}}(A)$ donnée par

$$f \cdot g = g^\dagger f g$$

pour $g \in \mathrm{Aut}(A)$ et $f \in \mathrm{End}_{\mathbb{Q}}(A)$. L'ensemble P des classes de polarisations de degré d s'injecte donc dans

$$\{f \in \mathrm{End}_{\mathbb{Q}}(A) \mid f \text{ déf. positif, } \deg f = \frac{d}{d_0}\}/\mathrm{Aut}A.$$

En suivant Narasimhan et Nori, on fait agir sur $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{R}$ le groupe des $\mathbb{R}$-points d'un groupe réductif

$$G = \{f \in \mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{R} \mid N(f) = \pm 1\}$$

(où $N(\cdot)$ désigne la norme intrinsèque) dont $\mathrm{Aut}(A)$ est un sous-groupe arithmétique. Dans un premier temps (paragraphe 3.2), nous montrons que notre ensemble donne naissance à un nombre fini d'orbites pour cette action et nous distinguons un élément particulier r dans chaque orbite, dont nous contrôlons la taille. On obtient ainsi un sous-ensemble fini $\mathcal{R}$ de $\mathrm{End}_{\mathbb{Q}}(A) \otimes \mathbb{R}$ dont les éléments sont contrôlés et une injection

$$P \hookrightarrow \bigcup_{r \in \mathcal{R}} \left(\iota(\mathrm{NS}(A)) \cap (r \cdot G)\right)/\mathrm{Aut}A.$$

Le plus gros de la preuve consiste à étudier $(\iota(\mathrm{NS}(A)) \cap (r \cdot G))/\mathrm{Aut}A$, montrer la finitude et donner une borne pour son cardinal.

Dans un premier temps, nous trouvons une représentation ρ de G dans $\mathrm{GL}_n(\mathbb{R})$ telle que $\rho(\mathrm{Aut}(A)) = \rho(G) \cap \mathrm{GL}_n(\mathbb{Z})$ et un espace vectoriel approprié W muni d'une action de $\mathrm{GL}_n(\mathbb{R})$. Pour chaque $r \in \mathcal{R} \cup \{0\}$ on définit un élément $w_r \in W$ et un réseau Ω de W tels que

$$(\iota(\mathrm{NS}(A)) \cap (r \cdot G))/\mathrm{Aut}A \hookrightarrow (\Omega \cap w_r \cdot \rho(G))/\rho(\mathrm{Aut}(A)).$$

L'intérêt de translater le problème dans ce cadre est de pouvoir travailler sur le groupe $\mathrm{GL}_n(\mathbb{R})$ et d'utiliser la théorie développée par Borel et Harish-Chandra. On utilisera notamment les ensembles de Siegel qui sont des ensembles fondamentaux pour l'action de $\mathrm{GL}_n(\mathbb{Z})$ sur $\mathrm{GL}_n(\mathbb{R})$; on choisira un tel ensemble $\mathfrak{S}$ vérifiant $\mathrm{GL}_n(\mathbb{R}) = \mathfrak{S}\mathrm{GL}_n(\mathbb{Z})$ et dont la décomposition d'Iwasawa est contrôlée par certains paramètres. Ceci nous permettra de trouver une injection

$$(\Omega \cap w_r \cdot \rho(G))/\rho(\mathrm{Aut}(A)) \hookrightarrow (\Omega \cap v_0 \cdot \mathfrak{S}) \times (\Omega \cap v_r \cdot \mathfrak{S})$$

où v_0 et v_r sont à peu de choses près les éléments w_0 et w_r qu'on a légèrement modifiés pour que leurs groupes d'isotropie soient stables par conjuguaison (hypothèse technique nécéssaire dans certaines preuves).

Pour conclure il ne restera plus qu'à borner la norme des élements de $\Omega \cap v_r \cdot \mathfrak{S}$ (pour $r \in \mathcal{R} \cup \{0\}$) et par la suite le cardinal de ces ensembles. Nous faisons ceci en suivant l'exposé de Borel dans [1] mais en remplaçant l'argument de compacité par le théorème 2.1. Ce dernier, étant indépendant du reste de l'article, est démontré dans la première partie de ce travail. Ce théorème montre que dans une $\mathbb{R}$-algèbre semi-simple de dimension n munie d'une involution positive $(\mathfrak{A}, \dagger)$, le plus gros ellipsoïde contenu dans $\{x \in \mathfrak{A},\, |N(x)| \leq 1\}$ est $\{x \in \mathfrak{A},\, \mathrm{Tr}(xx^\dagger) \leq n\}$ où N et Tr désignent la norme et la trace intrinsèques.

Remerciements Je remercie vivement Gaël Rémond pour les nombreuses discussions que nous avons eu sur ce travail, pour ses encouragements et ses conseils. Je remercie également le soutien du projet ANR Gardio 14-CE25-0015.

2 Un gros ellipsoïde

Soit $(\mathfrak{A}, \dagger)$ une $\mathbb{R}$-algèbre semi-simple de dimension n munie d'une involution positive. Notons $\mathrm{Tr}_{\mathfrak{A}/\mathbb{R}}(\cdot)$ la trace intrinsèque (définie par la représentation régulière à gauche). On montre facilement que l'application qui à $x \in \mathfrak{A}$ associe $q_\dagger(x) = \mathrm{Tr}_{\mathfrak{A}/\mathbb{R}}(x^\dagger x)$ est une forme quadratique sur $\mathfrak{A}$; dire que $\dagger$ est positive signifie que $q_\dagger$ est définie positive, ainsi

$$\{x \in \mathfrak{A},\, q_\dagger(x) \leq n\}$$

est un ellipsoïde. On remarque aussi que cet ellipsoïde est contenu dans $\{x \in \mathfrak{A},\, |N_{\mathfrak{A}/\mathbb{R}}(x)| \leq 1\}$ où $N_{\mathfrak{A}/\mathbb{R}}$ désigne la norme intrinsèque dans $\mathfrak{A}$. Le théorème suivant montre que l'ellipsoïde ci-dessus est maximal (en volume) parmi les ellipsoïdes contenus dans $\{x \in \mathfrak{A},\, |N_{\mathfrak{A}/\mathbb{R}}(x)| \leq 1\}$.

Théorème 2.1. *Soit $(\mathfrak{A}, \dagger)$ une $\mathbb{R}$-algèbre semi-simple de dimension n munie d'une involution positive. Soit q une forme quadratique définie positive sur $\mathfrak{A}$ et supposons*

$$\mathrm{vol}\{x \in \mathfrak{A},\, q(x) \leq 1\} \geq \mathrm{vol}\{x \in \mathfrak{A},\, q_\dagger(x) \leq n\} \tag{1}$$

où le volume est une mesure de Haar quelconque sur $\mathfrak{A}$. Alors il existe $y \in \mathfrak{A}$ tel que $q(y) \leq 1$ et $|N_{\mathfrak{A}/\mathbb{R}}(y)| \geq 1$.

La preuve de ce résultat s'attache principalement au cas de l'algèbre simple $\mathfrak{A} = M_m(\mathbb{H})$ des matrices à coefficients dans le corps des quaternions de Hamilton, dont on déduira le cas simple réel et complexe et ensuite le cas d'une algèbre semi-simple quelconque. On commence par fixer quelques notations. Si $\mathfrak{A}$ est de la forme $M_m(\mathbb{K})$ où $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$, on pose $n_\mathfrak{A} = \dim_\mathbb{R} \mathfrak{A} = [\mathbb{K} : \mathbb{R}]m^2$, $\beta_\mathfrak{A} = (n_\mathfrak{A}/m)^{1/2}$, $\varrho_\mathfrak{A} = (n_\mathfrak{A}/m)^{n_\mathfrak{A}}$, $\mathcal{U}_\mathbb{K} \subset \mathbb{K}$ le sous-ensemble donné selon le cas par $\mathcal{U}_\mathbb{R} = \{1\}, \mathcal{U}_\mathbb{C} = \{1, i\}$ et $\mathcal{U}_\mathbb{H} = \{1, i, j, k\}$. On choisit la base $\mathcal{B}_\mathfrak{A}$ de $\mathfrak{A}$ donnée selon le cas par : $\mathcal{B} = \{E_{11}, E_{21}, \ldots, E_{mm}\}$ si $\mathbb{K} = \mathbb{R}$, $\mathcal{B}_\mathfrak{A} = \{E_{11}, iE_{11}, E_{21}, \ldots, iE_{mm}\}$ si $\mathbb{K} = \mathbb{C}$ et $\mathcal{B}_\mathfrak{A} = \{E_{11}, iE_{11}, jE_{11}, kE_{11}, \ldots, kE_{mm}\}$ si $\mathbb{K} = \mathbb{H}$. Lorsque aucune confusion n'est possible on la notera simplement $\mathcal{B}$.

On munit $\mathfrak{A}$ de l'involution naturelle $M^\dagger = {}^t\bar{M}$.

On donne ci-dessous un tableau récapitulatif des différents objets et quantités intervenant dans la preuve qui suit.

$\mathfrak{A} = M_m(\mathbb{K})$	$\mathbb{K} = \mathbb{R}$	$\mathbb{K} = \mathbb{C}$	$\mathbb{K} = \mathbb{H}$
$\dim \mathfrak{A}$	m^2	$2m^2$	$4m^2$
involution $\dagger$	$X^\dagger = {}^tX$	$X^\dagger = {}^t\bar{X}$	$X^\dagger = {}^t\bar{X}$ (conjugaison quaternionique)
$Q = \mathrm{Mat}_{\mathcal{B}}(q_\dagger)$ où $q_\dagger(X) = \mathrm{Tr}_{\mathfrak{A}/\mathbb{R}}(XX^\dagger)$ $\det Q = \varrho_{\mathfrak{A}}$	$Q = mI_{m^2}$ m^{m^2}	$Q = 2mI_{2m^2}$ $(2m)^{2m^2}$	$Q = 4mI_{4m^2}$ $(4m)^{4m^2}$
$N_{\mathfrak{A}/\mathbb{R}}(X)$	$(\det X)^m$	$\lvert\det X\rvert^{2m}$	$(\det \Psi_X)^{2m}$
$\mathrm{Tr}_{\mathfrak{A}/\mathbb{R}}(X)$	$m\mathrm{Tr}X$	$2m\mathrm{Tr}A$ où $X = A + iB$, $A, B \in M_m(\mathbb{R})$	$4m\mathrm{Tr}A_1$ où $X = A_1 + A_2 i + A_3 j + A_4 k$, $A_1, A_2, A_3, A_4 \in M_m(\mathbb{R})$

Dans ce tableau, pour $X \in M_m(\mathbb{H})$ on a noté Ψ_X la matrice dans $M_{2m}(\mathbb{C})$ définie par

$$\Psi_X = \begin{pmatrix} A & -\bar{B} \\ B & \bar{A} \end{pmatrix}$$

où $X = A + Bj$ avec $A, B \in M_m(\mathbb{C})$. Il est bien connu que la norme réduite de la $\mathbb{R}$-algèbre $\mathfrak{A} = M_m(\mathbb{H})$ est $N(X) = \det(\Psi_X)$ et que pour tout X, $\det \Psi_X$ est un réel positif ([16], prop. 4.2). En comparant $N_{\mathfrak{A}/\mathbb{R}}(\lambda I_m)$ et $N(\lambda I_m)$ pour $\lambda \in \mathbb{R}$ on en déduit

$$N_{\mathfrak{A}/\mathbb{R}}(X) = (\det \Psi_X)^{2m}.$$

Le plus gros de la preuve repose sur la proposition suivante :

Proposition 2.2. *Soient $R \in \mathfrak{A} = M_m(\mathbb{K})$ et $T \in M_{n_\mathfrak{A}}(\mathbb{R})$ une matrice triangulaire supérieure dont les coefficients diagonaux sont strictement positifs. Alors il existe une permutation $\sigma \in S_m$, $\lambda \in \mathcal{U}_\mathbb{K}$ et $\epsilon_1, \ldots, \epsilon_m \in \{\pm 1\}$ tels que pour $M \in M_m(\mathbb{K})$ définie par $(M)_\mathcal{B} = T(Y)_\mathcal{B}$ avec $Y = \lambda\beta_\mathfrak{A}(\epsilon_{\sigma(1)}E_{1,\sigma(1)} + \ldots + \epsilon_{\sigma(m)}E_{m,\sigma(m)})$ où les E_{ij} sont les matrices élémentaires, on ait*

$$|N_{\mathfrak{A}/\mathbb{R}}(M + R)|^2 \geq (\det T)^2 \varrho_\mathfrak{A}.$$

Démonstration. Démontrons la proposition dans le cas $\mathfrak{A} = M_m(\mathbb{H})$. Notons les coefficients diagonaux de T

$$\left(d_{1,1}^{(1)}, \ldots, d_{1,1}^{(4)}, d_{2,1}^{(1)}, \ldots, d_{m,1}^{(4)}, d_{1,2}^{(1)}, \ldots, d_{1,m}^{(1)}, \ldots, d_{m,m}^{(4)}\right).$$

Avec cette notation, $d_{ij}^{(\kappa)} = t_{l,l}$ où $l = 4m(j-1) + 4(i-1) + \kappa$.

Soient $\sigma \in S_m$ une permutation, $\lambda \in \mathcal{U}_{\mathbb{H}}$ et des variables $\epsilon_1, \ldots, \epsilon_m$. On pose comme dans l'énoncé

$$Y = Y(\lambda, \epsilon, \sigma) = \beta_{\mathbb{H}}\lambda(\epsilon_{\sigma(1)}E_{1,\sigma(1)} + \epsilon_{\sigma(2)}E_{2,\sigma(2)} + \ldots + \epsilon_{\sigma(m)}E_{m,\sigma(m)}),$$

et $X = X(\lambda, \epsilon, \sigma) \in \mathfrak{A}$ tel que $(X)_{\mathcal{B}} = T(Y)_{\mathcal{B}}$. Notons $i_t = \sigma(t)$ pour $t = 1, \ldots, m$. Notre premier but est de comprendre le coefficient qui accompagne le monôme $\epsilon_1^2 \cdots \epsilon_m^2$ lorsque l'on développe $\det \Psi_{X+R}$. On notera ce coefficient $C = C_{\lambda,\sigma}$. En écrivant $X + R$ et Ψ_{X+R} on remarque les faits suivants (qui découlent facilement du choix de Y et de $\mathcal{B}$ et du fait que T soit triangulaire supérieure) :

(a) Chaque coefficient de Ψ_{X+R} est un polynôme de degré au plus 1 en $\epsilon_1, \ldots, \epsilon_m$.

(b) Pour tout $t = 1, \ldots, m$, ϵ_t n'apparaît pas dans les coefficients des colonnes $t+1, \ldots, m$ ni dans les colonnes $m+t+1, \ldots, 2m$ de Ψ_{X+R}.

(c) dans la i_t-ième et $m+i_t$-ième colonne de Ψ_{X+R}, la variable ϵ_{i_t} n'apparaît pas dans les lignes $t+1, \ldots, m$ ni dans les lignes $m+t+1, \ldots, 2m$.

Puisque $\det \Psi_{X+R}$ est une somme dont chaque terme est un produit de coefficients (multiplié par $\pm$ 1) de la matrice Ψ_{X+R} où chaque coefficient appartient à une colonne et une ligne différente de la matrice, on en déduit que pour avoir un terme avec $\epsilon_1^2 \cdots \epsilon_m^2$ en facteur il faut pour chaque t choisir dans les colonnes i_t et $m + i_t$ un élément des lignes $1, \ldots, t$ ou $m+1, \ldots, m+t$. Notons $(\Psi_{X+R}) = (p_{ij})_{i,j}$. Si on commence par la colonne i_1 il n'y a que 2 choix possibles : le coefficient p_{1,i_1} ou p_{m+1,i_1}. Mais du coup ce choix force le choix dans la colonne $i_1 + m$. On a donc pour l'instant les 2 produits suivants possibles : $p_{1,i_1}p_{m+1,m+i_1}$ ou $-p_{m+1,i_1}p_{1,m+i_1}$. On remarque de plus que ces éléments se réécrivent $|p_{1,i_1}|^2$ et $|p_{m+1,i_1}|^2$. On choisit ensuite dans la colonne i_2. Puisque on ne peut plus choisir un élément dans les lignes 1 ni $m+1$ il n'y a que deux choix possibles p_{2,i_2} ou p_{m+2,i_2} et, comme avant, ceci définit le choix dans la colonne $m + i_2$. Le produit de ces coefficients dans les deux cas donne comme avant $|p_{2,i_2}|^2$ ou $|p_{m+2,i_2}|^2$ et on a donc 4 produits différents possibles. On continue ce procédé et on obtient 2^m produits possibles où en développant on peut obtenir le terme recherché. On déduit de ce qui précède que C est le coefficient de $\epsilon_1^2 \cdots \epsilon_m^2$ dans

$$\prod_{t=1}^{m} |p_{t,\sigma(t)}|^2 + |p_{m+t,\sigma(t)}|^2.$$

Plus précisément,

$$C = \prod_{t=1}^{m} |\zeta_{t,\sigma(t)}|^2 + |\zeta_{m+t,\sigma(t)}|^2$$

où $\zeta_{i,j} \in \mathbb{C}$ est le coefficient de ϵ_j dans $p_{i,j}$. Voyons maintenant que pour chaque t on a $|\zeta_{t,\sigma(t)}|^2 + |\zeta_{m+t,\sigma(t)}|^2 \geq (\beta_{\mathfrak{A}} d_{t,\sigma(t)}^{(\kappa)})^2$. On remarque d'abord que parmi $\zeta_{t,\sigma(t)}$ et $\zeta_{m+t,\sigma(t)}$ un des deux est de la forme

$$a(\epsilon_{\sigma(t)}, \ldots, \epsilon_m) + i\epsilon_{\sigma(t)}\beta_{\mathfrak{A}} d_{t,\sigma(t)}^{(\kappa)} \quad \text{ou} \quad \epsilon_{\sigma(t)}\beta_{\mathfrak{A}} d_{t,\sigma(t)}^{(\kappa)}$$

où a est un polynôme de degré 1 à coefficients réels dans les variables indiquées et $d_{t,i_t}^{(\kappa)}$ correspond à un coefficient diagonal de la matrice T avec $\kappa = 1, 2, 3$ ou

4 selon si $\lambda = 1, i, j$ ou k respectivement. Puisque pour tout nombre complexe $\alpha+i\beta$ on a $|\alpha+i\beta|^2 \geq \max\{\alpha^2, \beta^2\}$ on peut donc minorer $|\zeta_{t,\sigma(t)}|^2$ ou $|\zeta_{m+t,\sigma(t)}|^2$ par $(\beta_{\mathfrak{A}} d_{t,\sigma(t)}^{(\kappa)})^2$ (et l'autre terme par 0) et on a

$$C \geq (\beta_{\mathfrak{A}} d_{1,i_1}^{(\kappa)})^2 \cdots (\beta_{\mathfrak{A}} d_{m,i_m}^{(\kappa)})^2 \geq \beta_{\mathfrak{A}}^{2m} (d_{1,i_1}^{(\kappa)})^2 \cdots (d_{m,i_m}^{(\kappa)})^2, \tag{2}$$

d'où

$$\beta_{\mathfrak{A}}^{n_{\mathfrak{A}}} ((d_{1,i_1}^{(\kappa)})^2 \cdots (d_{m,i_m}^{(\kappa)})^2)^{2m} \leq C^{2m}.$$

D'autre part, si $\tau \in S_m$ est un cycle d'ordre m on vérifie facilement que

$$\det T = \prod_{l=1}^{m} \prod_{\kappa=1}^{4} \prod_{i=1}^{m} d_{i,\tau^l(i)}^{(\kappa)}. \tag{3}$$

On choisit maintenant σ parmi les τ^l et $\lambda \in \mathcal{U}_{\mathbb{H}}$ (ou ce qui est équivalent on choisit l et κ) de façon que

$$\left(\prod_{i=1}^{m} d_{i,\sigma(i)}^{(\kappa)} \right)^{4m} \geq \det T. \tag{4}$$

En combinant cette inégalité et la minoration (2) on a

$$C_{\lambda,\sigma}^{2m} \geq \det T (4m)^{2m^2}. \tag{5}$$

Il nous reste à voir que nous pouvons choisir $\epsilon = (\epsilon_1, \ldots, \epsilon_m) \in \{\pm 1\}^m$ tels que si $M = X(\lambda, \epsilon, \sigma)$ alors $\det \Psi_{M+R} \geq C_{\lambda,\sigma}$. Il s'agit du résultat général suivant :

Lemme 2.3. *Soient $m \geq 0$ et $P \in \mathbb{R}[X_1, \ldots, X_m]$. On suppose $\deg_{(X_1,\ldots,X_i)} P \leq 2i$ pour tout $1 \leq i \leq m$ et que P prend des valeurs positives sur $\mathbb{R}^m$. Alors il existe $\epsilon \in \{-1, 1\}^m$ tel que $P(\epsilon) \geq$ coefficient de $X_1^2 \cdots X_m^2 \geq 0$.*

Démonstration. Nous procédons par récurrence sur m. Si $m = 0$, P est constant et on a trivialement le résultat voulu. Soit $m \geq 1$ et supposons le résultat vrai pour tout polynôme en k variables $k < m$ vérifiant les hypothèses du lemme. Soit $P \in \mathbb{R}[X_1, \ldots, X_m]$ comme dans l'énoncé. On écrit P sous la forme

$$P = R + X_1 S + X_1^2 Q$$

où $Q, R, S \in \mathbb{R}[X_2, \ldots, X_m]$ et notons a le coefficient de $X_2^2 \cdots X_m^2$ dans Q. On déduit de la condition sur le degré de P que pour tout i, $2 \leq i \leq m$ on a $\deg_{(X_2,\ldots,X_i)} Q \leq 2(i-1)$. D'un autre côté, si $(y_2, \ldots, y_m) \in \mathbb{R}^{m-1}$, le polynôme de degré 2 :

$$X \mapsto R(y_2, \ldots, y_m) + XS(y_2, \ldots, y_m) + X^2 Q(y_2, \ldots, y_m)$$

est à valeurs positives. Cela implique que le coefficient constant $R(y_2, \ldots, y_m)$ et le coefficient dominant $Q(y_2, \ldots, y_m)$ sont positifs. On en déduit que le polynôme Q est à valeurs positives sur $\mathbb{R}^{m-1}$ et par hypothèse de récurrence, il existe $\epsilon_2, \ldots, \epsilon_m \in \{-1, 1\}$ tels que $Q(\epsilon_2, \ldots, \epsilon_m) \geq a \geq 0$. Enfin il suffit de choisir ϵ_1 du signe de $S(\epsilon_2, \ldots, \epsilon_m)$ et on a bien $P(\epsilon_1, \ldots, \epsilon_m) \geq a$. Nous concluons en remarquant que a est aussi le coefficient de $X_1^2 \cdots X_m^2$ de P. $\square$

On applique ce résultat à $P : \epsilon \mapsto \det \Psi_{X(\lambda,\epsilon,\sigma)+R}$. Comme expliqué plus haut, pour chaque $i = 1, \ldots, m$, ϵ_i n'apparaît pas dans les coefficients des colonnes $i+1, \ldots, m$ ni dans les colonnes $m+i+1, \ldots, 2m$ de $\Psi_{X(\lambda,\epsilon,\sigma)+R}$. En calculant le déterminant on vérifie facilement que la condition sur le degré est vérifiée. Une fois ϵ fixé avec la propriété voulue, λ et σ comme dans (5) on a pour $M = X(\lambda, \epsilon, \sigma)$

$$\det \Psi_{M+R}^{2m} \geq C_{\lambda,\sigma}^{2m} \geq \det T (4m)^{2m^2}$$

et donc

$$|N_{\mathfrak{A}/\mathbb{R}}(M+R)|^2 \geq (\det T)^2 (4m)^{4m^2}$$

ce qu'on voulait démontrer.

Voyons maintenant que la proposition est vraie pour $\mathfrak{A} = M_m(\mathbb{R})$. Nous disposons de $T = (t_{ij})_{1 \leq i,j \leq m^2} \in M_{m^2}(\mathbb{R})$ et $R \in M_m(\mathbb{R})$. Soient $\sigma \in S_m$ une permutation, $\lambda = 1$ et des variables $\epsilon_1, \ldots, \epsilon_m$. On pose comme dans l'énoncé

$$Y = Y(\lambda, \epsilon, \sigma) = \beta_{\mathfrak{A}}(\epsilon_{\sigma(1)} E_{1,\sigma(1)} + \epsilon_{\sigma(2)} E_{2,\sigma(2)} + \ldots + \epsilon_{\sigma(m)} E_{m,\sigma(m)}).$$

On construit une matrice $\tilde{T} \in M_{4m^2}(\mathbb{R})$ de façon que si X est la matrice telle que $(X)_{\mathcal{B}_{\mathfrak{A}}} = T(Y)_{\mathcal{B}_{\mathfrak{A}}}$ on a $(X)_{\mathcal{B}_{M_m(\mathbb{H})}} = \tilde{T}(Y)_{\mathcal{B}_{M_m(\mathbb{H})}}$. Les coefficients de la matrice $\tilde{T}$ sont donnés par

$$u_{ij} = \begin{cases} 0 & \text{si } i \neq j \text{ et } i, j \equiv 0, 2, 3 \pmod 4 \\ 1 & \text{si } i = j \text{ et } i, j \equiv 0, 2, 3 \pmod 4 \\ t_{k+1,l+1} & \text{si } i = 4k+1 \text{ et } j = 4l+1 \end{cases} .$$

On applique le raisonnement fait dans le cas de l'algèbre $M_m(\mathbb{H})$ à la matrice $\tilde{T}$ ainsi définie. On a donc, comme avant, l'équivalent de l'inégalité (2)

$$C \geq \beta_{\mathfrak{A}}^{2m} (d_{1,i_1}^{(1)})^2 \cdots (d_{m,i_m}^{(1)})^2$$

pour tout $\sigma \in S_m$. De plus (3) se réécrit

$$\det \tilde{T} = \prod_{l=1}^{m} \prod_{\kappa=1}^{4} \prod_{i=1}^{m} d_{i,\tau^l(i)}^{(\kappa)} = \prod_{l=1}^{m} \prod_{i=1}^{m} d_{i,\tau^l(i)}^{(1)} = \det T,$$

et pour un choix approprié de $\sigma = \tau^l$ l'inégalité (4) devient

$$\left(\prod_{i=1}^{m} d_{i,\sigma(i)}^{(1)} \right)^m \geq \det \tilde{T} = \det T.$$

Ainsi, la minoration (5) est affinée en

$$C_{1,\sigma}^m \geq (\det T)^2 m^{m^2}.$$

Finalement, on choisit comme avant $\epsilon \in \{-1, 1\}^m$ de façon que, pour $M = X(1, \epsilon, \sigma)$, on ait $\det \psi_{M+R} \geq C_{1,\sigma}$. On a donc

$$|N_{\mathfrak{A}/\mathbb{R}}(M+R)|^2 = (\det(M+R))^{2m} = (\det \Psi_{M+R})^m \geq C_{1,\epsilon,\sigma}^m \geq (\det T)^2 m^{m^2}$$

et donc
$$|N_{\mathfrak{A}/\mathbb{R}}(X+R)|^2 \geq (\det T)^2 m^{m^2},$$
ce qu'il fallait démontrer.

Le cas $\mathfrak{A} = M_m(\mathbb{C})$ est similaire. Nous avons $T = (t_{ij})_{1\leq i,j\leq 2m^2} \in M_{2m^2}(\mathbb{R})$ et $R \in M_m(\mathbb{C})$. Soient $\sigma \in S_m$ une permutation, $\lambda \in \mathcal{U}_{\mathbb{C}}$ et des variables $\epsilon_1, \ldots, \epsilon_m$. On pose comme dans l'énoncé

$$Y = Y(\lambda, \epsilon, \sigma) = \beta_{\mathbb{C}}\lambda(\epsilon_{\sigma(1)}E_{1,\sigma(1)} + \epsilon_{\sigma(2)}E_{2,\sigma(2)} + \ldots + \epsilon_{\sigma(m)}E_{m,\sigma(m)}).$$

On construit une matrice triangulaire supérieure $\tilde{T} \in M_{2m^2}(\mathbb{R})$ dont les coefficients sont donnés par :

$$u_{ij} = \begin{cases} 0 & \text{si } i \equiv 0,3 \pmod 4,\ j \neq i \\ 1 & \text{si } i \equiv 0,3 \pmod 4,\ j = i \\ 0 & \text{si } i \equiv 1,2 \pmod 4,\ j \equiv 0,3 \pmod 4 \\ t_{2k+b,2l+b} & \text{si } i = 4k+b,\ j = 4l+b \text{ et } b \in \{1,2\} \end{cases}.$$

On en déduit l'équivalent de (3) :

$$\det \tilde{T} = \prod_{l=1}^{m}\prod_{\kappa=1}^{4}\prod_{i=1}^{m} d^{(\kappa)}_{i,\tau^l(i)} = \prod_{l=1}^{m}\prod_{\kappa=1}^{2}\prod_{i=1}^{m} d^{(\kappa)}_{i,\tau^l(i)} = \det T,$$

et pour un choix approprié de $\sigma = \tau^l$ et κ l'équivalent de (4) et (5)

$$C^m_{\kappa,\sigma} \geq \left(\prod_{i=1}^{m} d^{(\kappa)}_{i,\sigma(i)}\right)^{2m} (2m)^{m^2} \geq \det \tilde{T}(2m)^{m^2} = \det T(2m)^{m^2}.$$

Pour conclure, on choisit ϵ tel que pour $M = X(\lambda,\epsilon,\sigma)$ on ait $\det \psi_{M+R} \geq C_{\kappa,\sigma}$ et on a

$$|N_{\mathfrak{A}/\mathbb{R}}(M+R)|^2 = |\det(M+R)|^{4m} = (\det \Psi_{M+R})^{2m} \geq C^{2m}_{\kappa,\sigma} \geq (\det T)^2(2m)^{2m^2},$$

ce qu'il fallait démontrer.

□

Démonstration. (du theorème 2.1)

On remarque dans un premier temps que si $\mathcal{B}$ est une base quelconque de $\mathfrak{A}$, la condition (1) se réécrit

$$(\det_{\mathcal{B}} q)^{-1} \geq n^n \det(Q)^{-1} \tag{6}$$

où Q est la matrice dans la base $\mathcal{B}$ de la forme quadratique $x \mapsto \mathrm{Tr}_{\mathfrak{A}/\mathbb{R}}(x^\dagger x)$. Nous allons montrer qu'il existe $x \in \mathfrak{A}$ tel que

$$\det(Q)(\det_{\mathcal{B}} q)^{-1} \leq |N_{\mathfrak{A}/\mathbb{R}}(x)|^2 \quad \text{et} \quad q(x) = n. \tag{7}$$

Ceci répond au problème puisque $y = n^{-1/2}x$ vérifie $q(y) = 1$ et $|N_{\mathfrak{A}/\mathbb{R}}(y)| = n^{-n/2}|N_{\mathfrak{A}/\mathbb{R}}(x)| \geq 1$.

On identifie $(\mathfrak{A}, \dagger)$ au produit

$$\prod_{t=1}^{l} M_{a_t}(\mathbb{K}_t)$$

muni de l'involution produit des involutions usuelles, où $a_t \geq 1$ et $\mathbb{K}_t \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$. On pose $\mathfrak{A}_t = M_{a_t}(\mathbb{K}_t)$, puis pour alléger les notations, $n_t = n_{\mathfrak{A}_t}, \beta_t = \beta_{\mathfrak{A}_t}, \rho_t = \rho_{\mathfrak{A}_t}$ et $\mathcal{B}_t = \mathcal{B}_{\mathfrak{A}_t}$. Soit $\mathcal{B}$ la base de $\mathfrak{A}$ obtenue à partir des bases $\mathcal{B}_t$. On note $A = \mathrm{Mat}_{\mathcal{B}}(q)$. Puisque A est symétrique définie positive, il existe une matrice U triangulaire supérieure (décomposition de Cholesky) telle que $A = {}^tUU$. On peut donc écrire pour tout $x \in \mathfrak{A}$,

$$q(x) = {}^t(x)_{\mathcal{B}} A (x)_{\mathcal{B}} = \|U(x)_{\mathcal{B}}\|_2^2.$$

La matrice U^{-1} est aussi triangulaire supérieure et on notera $T_1, \ldots, T_l$ ses blocs diagonaux avec $T_t \in M_{n_t}(\mathbb{R})$.

Dans ce contexte les conditions dans (7) se résument à trouver x tel que

$$(\det U^{-1})^2 \prod_{t=1}^{l} \rho_t \leq |N_{\mathfrak{A}/\mathbb{R}}(x)|^2 \tag{8}$$

et

$$\|U(x)_{\mathcal{B}}\|_2^2 = n = \sum_{t=1}^{l} n_t = \sum_{t=1}^{l} a_t^2 [\mathbb{K}_t : \mathbb{R}].$$

On considère des permutations $\sigma_1, \ldots, \sigma_l$, des scalaires $\lambda_1, \ldots, \lambda_l$ et pour chaque $t \in \{1, \ldots, l\}$, des réels $\epsilon_s^{(t)} \in \{\pm 1\}$ où $1 \leq s \leq a_t$. On définit des matrices $Y_1, \ldots, Y_l$ en les variables ci-dessus par : $Y_t = \lambda_t \beta_t (\epsilon_{\sigma_t(1)}^{(t)} E_{1,\sigma_t(1)} + \cdots + \epsilon_{\sigma_t(t)}^{(t)} E_{t,\sigma_t(t)})$. On note aussi $X_1, \ldots, X_l$ des matrices telles que pour chaque t, $X_t \in M_{a_t}(\mathbb{K}_t)$ et $(X_t)_{\mathcal{B}_t} = T_t (Y_t)_{\mathcal{B}_t}$. On peut ainsi définir des matrices $R_1, \ldots, R_l$ de façon que si $Y = (Y_1, \ldots, Y_l)$ et $U^{-1}(Y)_{\mathcal{B}} = (X)_{\mathcal{B}}$ alors on ait

$$X = (X_1 + R_1, \ldots, X_l + R_l).$$

De plus, les matrices X_t ne contiennent que les variables $\epsilon_1^{(t)}, \ldots, \epsilon_{a_t}^{(t)}$ et chaque matrice R_t ne contient pas les variables $\epsilon_j^{(i)}$ pour $i \leq t$.

Il reste à choisir pour chaque t une permutation σ_t, les réels $\epsilon_1^{(t)}, \ldots, \epsilon_{a_t}^{(t)} \in \{\pm 1\}$ et les scalaires λ_t pour que l'élément X satisfasse les conditions (8) ci-dessus.

On applique d'abord la proposition 2.2 à la matrice $R = R_l = 0$ et à $T = T_l$ ce qui nous permet de choisir $\epsilon_1^{(l)}, \ldots, \epsilon_{a_l}^{(l)}$, λ_l et $\sigma^{(l)}$ tels que

$$|N_{\mathfrak{A}_l/\mathbb{R}}(X_l)|^2 \geq (\det T_l)^2 \rho_l.$$

Notons cette matrice M_l. Par récurrence, supposons qu'on a fixé les uplets de variables $\epsilon^{(t)}$, les permutations σ_t et les scalaires λ_t pour $t = i+1, \ldots, l$ et donc on a construit les matrices M_t et R_t pour $t = i+1, \ldots, l$ de façon que $M_t \in \mathfrak{A}_t$, et

$$|N_{\mathfrak{A}_t/\mathbb{R}}(M_t + R_t)|^2 \geq (\det T_t)^2 \rho_t.$$

On applique à nouveau la proposition 2.2 aux matrices $R = R_i$ et $T = T_i$. On trouve donc un uplet $\epsilon^{(i)}$, une permutation σ_i et un scalaire λ_i tels que $M_i = X_i(\lambda_i, \epsilon^{(i)}, \sigma_i)$ vérifie

$$|N_{\mathfrak{A}_i/\mathbb{R}}(M_i + R_i)|^2 \geq (\det T_i)^2 \rho_i.$$

On pose donc $x = (M_1 + R_1, \ldots, M_l)$ et $(x)_{\mathcal{B}} = U^{-1}(y)_{\mathcal{B}}$. On a comme prévu

$$\|U(x)_{\mathcal{B}}\|_2^2 = \|(y)_{\mathcal{B}}\|_2^2 = \sum a_i^2 [\mathbb{K}_i : \mathbb{R}]$$

et

$$\begin{aligned} |N_{\mathfrak{A}/\mathbb{R}}(x)|^2 = \prod_{t=1}^{l} |N(M_t + R_t)|^2 &\geq \prod_{t=1}^{l} |(\det(T_t))|^2 \rho_t \\ &\geq \det(U^{-1})^2 \prod_{t=1}^{l} \rho_t. \end{aligned}$$

□

3 Intersection d'orbites et de réseaux

3.1 Données

Soient A une variété abélienne sur un corps quelconque, $\mathcal{L}_0$ un faisceau inversible ample sur A et $\phi_{\mathcal{L}_0}$ la polarisation associée. On note $h_0 = h^0(A, \mathcal{L}_0)$ et $d_0 = \deg \phi_{\mathcal{L}_0} = h_0^2$ qu'on appelera le degré de la polarisation. On notera aussi $\dagger$ l'involution de Rosati associée à $\mathcal{L}_0$, $q_\dagger : \mathrm{End} A \otimes \mathbb{R} \to \mathbb{R}$ la forme quadratique définie positive définie par $q_\dagger(\varphi) = |\varphi|^2 = \mathrm{Tr}(\varphi\varphi^\dagger)$ où Tr est la trace intrinsèque (définie par la représentation régulière à gauche) dans $\mathrm{End} A \otimes \mathbb{R}$. On remarque que dans la littérature une autre métrique de Rosati est souvent utilisée, définie à l'aide d'une autre trace qui dépend de l'action des endomorphismes sur A (voir [6], p. 2063–5).

On rappelle que $\mathrm{End}(A)$ est un réseau de $\mathrm{End}(A) \otimes \mathbb{R}$, on notera n son rang et $\lambda_1 \leq \cdots \leq \lambda_n$ ses minima successifs. Il est bien connu (voir par exemple [4], lemme 1, p. 204) qu'il existe une $\mathbb{Q}$-base $(\omega_1, \ldots, \omega_n)$ de $\mathrm{End}_{\mathbb{Q}}(A)$ d'éléments de $\mathrm{End}(A)$ telle que $|\omega_i| = \lambda_i$ pour tout i. Pour une telle base fixée on en déduit ([4], lemme 8, p. 135) l'existence d'une $\mathbb{Z}$-base $(\alpha_1, \ldots, \alpha_n)$ de façon que pour tout $i = 1, \ldots, n$,

$$|\alpha_i| \leq \max\{|\omega_i|, \frac{1}{2}(|\omega_1| + \ldots + |\omega_i|)\} \leq \max(1, \frac{i}{2})\lambda_i. \tag{9}$$

On notera D_i (respectivement G_i) la matrice de $M_n(\mathbb{Z})$ représentant dans la base $(\alpha_1, \ldots, \alpha_n)$ la multiplication à droite (resp. à gauche) $\beta \mapsto \beta\alpha_i$ (resp. $\beta \mapsto \alpha_i\beta$) pour tout $i = 1, \ldots, n$.

On notera $D := \mathrm{disc}(\mathrm{End}(A))$ le discriminant du $\mathbb{Z}$-module $\mathrm{End}(A)$ c'est-à-dire la valeur absolue du déterminant de la matrice de terme général $\mathrm{Tr}(\alpha_i\alpha_j)$; il s'agit aussi du carré du covolume de $\mathrm{End}(A)$ relatif à la mesure de Haar donnée sur $\mathrm{End}(A) \otimes \mathbb{R}$ par une base orthonormée. Cette quantité est entière et ne dépend pas du choix de la polarisation $\mathcal{L}_0$, mais on peut voir qu'il correspond aussi à $\det(\mathrm{Tr}(\alpha_i\alpha_j^\dagger))$ (voir par exemple [6], prop. 4.9).

Soit Q la matrice dans la base $(\alpha_1, \ldots, \alpha_n)$ de la forme quadratique $q_\dagger$. Puisque Q est symétrique définie positive, il existe une unique matrice $U \in M_n(\mathbb{R})$ symétrique définie positive telle que $U^2 = Q$. On remarque aussi que $\det(Q) = D$.

On utilisera à plusieurs reprises le résultat suivant :

Lemme 3.1. *L'image de* $\mathrm{End}(A)$ *dans* $\mathrm{End}_{\mathbb{Q}}(A)$ *par l'involution de Rosati est contenue dans* $\frac{1}{h_0}\mathrm{End}(A)$.

Démonstration. Il suffit de remarquer que $h^0(A, \mathcal{L}_0)\phi_{\mathcal{L}_0}^{-1} \in \mathrm{Hom}(\hat{A}, A)$ et de rappeler que pour tout $\alpha \in \mathrm{End}(A)$, $\alpha^\dagger = \phi_{\mathcal{L}_0}^{-1} \circ \widehat{\alpha} \circ \phi_{\mathcal{L}_0}$. □

Remarque 3.2. *On a de la même façon pour tout* $\alpha \neq 0 \in \mathrm{End}(A)$ $h_0\alpha\alpha^\dagger \in \mathrm{End}(A)$ *et donc en particulier* $Q \in \frac{1}{h_0}M_n(\mathbb{Z})$.

Dans toute la suite de ce travail on va supposer $n \geq 2$. En effet si $n = 1$, il y a une seule classe de polarisations de degré donné, donc les bornes annoncées dans les théorèmes 1.1 et 1.3 sont trivialement vraies.

Lemme 3.3. *Pour* $1 \leq i \leq n$, *on a* $|\alpha_i|^2 \leq \Sigma^2$ *où* $\Sigma^2 = \frac{1}{4}Dn^{n+2}h_0^{n-1}$.

Démonstration. On a choisi les α_i de façon que $|\alpha_1| \leq \max(1, \frac{1}{2})\lambda_1 = \lambda_1$. Puisque $h_0\alpha_i\alpha_i^\dagger \in \mathrm{End}(A)$, alors $h_0|\alpha_i|^2 \geq 1$. Pour $i = 1$ on obtient donc

$$\lambda_1 \geq \frac{1}{\sqrt{h_0}}.$$

On utilise le second théorème de Minkwoski sous la forme suivante (voir lemme 3.1 de [6]) :

$$\lambda_1^{n-1}\lambda_n \leq \sqrt{n}^n\sqrt{D}.$$

On a donc $|\alpha_i|^2 \leq \frac{n^2}{4}\lambda_i^2 \leq \frac{n^2}{4}\lambda_n^2 \leq \frac{n^2}{4}n^nDh_0^{n-1} \leq \Sigma^2$. □

3.2 Représentations et action de groupes

Commençons par rappeler un résultat important sur les endomorphismes des variétés abéliennes et le lien avec les composantes isotypiques de celles-ci. Pour plus de détails et les preuves des résultats cités ci-dessous voir [14], 3.2.

Pour toute variété abélienne A, il existe des sous-variétés abéliennes B_i isotypiques (isogènes à la puissance d'une variété abélienne simple) maximales, telles que la somme $B_1 \times \cdots \times B_s \to A$ soit une isogénie. De plus chaque endomorphisme de A laisse stables toutes les B_i et on obtient une application injective de conoyau fini

$$\mathrm{End}A \to \prod_{i=1}^{s}\mathrm{End}B_i.$$

On notera $n_i = \mathrm{rg}(\mathrm{End}B_i)$ et $g_i = \dim B_i$. En tensorisant avec $\mathbb{R}$ on a un isomorphisme

$$\mathrm{End}(A) \otimes \mathbb{R} \to \prod_{i=1}^{s}\mathrm{End}B_i \otimes \mathbb{R}.$$

On notera dorénavant $\mathfrak{A} = \mathrm{End}(A) \otimes \mathbb{R}$ et $\mathfrak{A}_i = \mathrm{End}B_i \otimes \mathbb{R}$. On remarque que, pour tout i, $\mathfrak{A}_i$ est une algèbre simple.

On peut donc associer à $f \in \mathfrak{A}$ un uplet $(f_1, \ldots, f_s)$ où $f_i \in \mathfrak{A}_i$. On a de plus

$$\deg\, f = \prod_{i=1}^{s}\deg\, f_i.$$

On peut aussi voir un s-uplet $(r_1, \ldots, r_s) \in \mathbb{R}^s$ comme un élément de $\prod_{i=1}^{s}\mathfrak{A}_i$ et il lui correspond donc un unique élément $r \in \mathfrak{A}$ par l'isomorphisme ci-dessus.

Définition 3.4. *On note ρ la représentation régulière à gauche*

$$\rho : \mathfrak{A} \hookrightarrow \mathrm{End}(\mathfrak{A}) \simeq M_n(\mathbb{R})$$

où la dernière identification se fait par le choix de la base $(\alpha_1, \dots, \alpha_n)$.

On vérifie aussi que

$$\det\, \rho(f) = \prod_{i=1}^{s} \det\, \rho_i(f_i)$$

où ρ_i est la représentation régulière à gauche $\rho_i : \mathfrak{A}_i \to M_{n_i}(\mathbb{R})$. De plus, on a (voir par exemple [6] p. 2063) la relation

$$(\deg\, f_i)^{n_i} = (\det\, \rho_i(f_i))^{2g_i} \tag{10}$$

pour tout $i = 1, \dots, s$.

Par la suite on notera

$$G = \{f \in \mathfrak{A} \mid N_{\mathfrak{A}/\mathbb{R}}(f) = \pm 1\}$$

où $N_{\mathfrak{A}/\mathbb{R}} = \det \circ \rho$ est la norme intrinsèque sur $\mathfrak{A}$ associée à la représentation régulière à gauche ci-dessus. On notera aussi

$$\Gamma = \mathrm{Aut}(A) \quad \text{ et } \quad H = \{f \in \mathfrak{A} \mid ff^\dagger = 1\}.$$

Le résultat suivant sera utilisé à plusieurs reprises :

Lemme 3.5. *Pour tout $f \in \mathfrak{A}$, l'adjoint pour le produit scalaire $\langle x, y\rangle = \mathrm{Tr}(xy^\dagger)$ sur $\mathfrak{A}$ de la multiplication à gauche par f est la multiplication à gauche par $f^\dagger$. On a donc pour tout $f \in \mathfrak{A}$,*

$$Q\rho(f^\dagger) = {}^t\rho(f)Q.$$

Démonstration. Soit $f \in \mathfrak{A}$. Pour tous $x, y \in \mathfrak{A}$ on a

$$\langle fx, y\rangle = \mathrm{Tr}(fxy^\dagger) = \mathrm{Tr}(xy^\dagger f) = \mathrm{Tr}(x(f^\dagger y)^\dagger) = \langle x, f^\dagger y\rangle.$$

En écrivant cette égalité matriciellement on obtient $Q\rho(f^\dagger) = {}^t\rho(f)Q$. □

Vérifions maintenant que Γ et H sont des sous-groupes de G.

Lemme 3.6. *Les groupes Γ et H sont des sous-groupes de G. De plus, G et H sont stables par l'involution de Rosati et $\rho(\Gamma) = \rho(G) \cap \mathrm{GL}_n(\mathbb{Z})$.*

Démonstration. La propriété essentielle sur laquelle reposent ces résultats est que si on associe à $f \in \mathfrak{A}$ l'élément $(f_1, \dots, f_s) \in \prod_{i=1}^s \mathfrak{A}_i$ alors $f^\dagger$ correspond au s-uplet $(f_1^\dagger, \dots, f_s^\dagger)$ pour les involutions de Rosati associées aux $\mathcal{L}_0|_{B_i}$.

Voyons d'abord que G est stable par l'action de $\dagger$. Soit $f \in G$, $f = (f_1, \dots, f_s)$. Puisque $\deg f_i^\dagger = \deg f_i$, en utilisant (10) on en déduit $\det \rho(f_i^\dagger) = \pm \det \rho(f_i)$ et en passant au produit $N_{\mathfrak{A}/\mathbb{R}}(f^\dagger) = \pm N_{\mathfrak{A}/\mathbb{R}}(f) = \pm 1$. On a donc $f^\dagger \in G$.

D'autre part, si $f \in H$, $\deg(f_i f_i^\dagger) = 1$ or $\deg(f_i f_i^\dagger) = (\deg f_i)^2$ et on en déduit $\deg f_i = \pm 1$. On a comme avant $\det \rho_i(f_i) = \pm 1$ et finalement $N_{\mathfrak{A}/\mathbb{R}}(f) = \prod_{i=1}^s \det \rho_i(f_i) = \pm 1$ d'où $f \in G$. Si $f, g \in H$ on a d'après les propriétés de l'involution de Rosati $(fg^{-1})(fg^{-1})^\dagger = fg^{-1}(g^\dagger)^{-1}f^\dagger = \mathrm{id}$. Ceci montre que H est un sous-groupe de G. D'autre part, les éléments de H sont inversibles, donc si $ff^\dagger = \mathrm{id}$ alors $f^\dagger = f^{-1}$ et donc $f^\dagger f = \mathrm{id}$ et H est stable par l'action de $\dagger$.

Voyons maintenant que Γ est un sous-groupe de G. Soit $f \in \mathrm{Aut}A$ et $(f_1, \ldots, f_s)$ comme ci-dessus. Alors chaque f_i appartient à $\mathrm{Aut}B_i$. On a donc $\deg f_i = 1$ et on procédant comme pour H on en déduit $f \in G$.

Pour la dernière assertion, on suppose $M \in \rho(G) \cap \mathrm{GL}_n(\mathbb{Z})$ et on pose $M = \rho(g)$ avec $g \in \mathfrak{A}$. Puisque $1 \in \mathrm{End}A$, on peut écrire $1 = \lambda_1\alpha_1 + \ldots + \lambda_n\alpha_n$ avec $\lambda_i \in \mathbb{Z}$, $\forall i = 1, \ldots, n$. On pose aussi $g = g \cdot 1 = \beta_1\alpha_1 + \ldots + \beta_n\alpha_n$. Ceci se traduit par $\begin{pmatrix}\beta_1 \\ \vdots \\ \beta_n\end{pmatrix} = M \begin{pmatrix}\lambda_1 \\ \vdots \\ \lambda_n\end{pmatrix}$ et puisque M est à coefficients entiers, alors les β_i sont entiers et $g \in \mathrm{End}A$. On fait de même pour g^{-1} et on déduit $g \in \mathrm{Aut}A$. Ceci montre l'inclusion $\rho(\Gamma) \supset \rho(G) \cap \mathrm{GL}_n(\mathbb{Z})$. Puisque $\Gamma \subset G$ l'autre inclusion est évidente et on a l'égalité voulue. $\square$

Soit $\mathrm{NS}(A)$ le groupe de Néron-Severi de A. Le groupe Γ agit sur $\mathrm{NS}(A)$ par $\mathcal{L} \mapsto u^*\mathcal{L}$ si $u \in \Gamma$. De plus si $\mathcal{L}$ est ample, $u^*\mathcal{L}$ est ample. On notera $(\mathrm{End}(A) \otimes \mathbb{R})^\dagger = \{f \in \mathrm{End}(A) \otimes \mathbb{R} \mid f^\dagger = f\}$. Il est bien connu (voir [12], Chap. 4, p. 208) que l'application de $\mathrm{NS}(A) \otimes \mathbb{Q}$ sur $(\mathrm{End}(A) \otimes \mathbb{Q})^\dagger$ définie par

$$\begin{gathered} \mathrm{NS}(A) \otimes \mathbb{Q} \overset{\iota}{\hookrightarrow} (\mathrm{End}(A) \otimes \mathbb{Q})^\dagger \\ \mathcal{L} \mapsto \phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}} \end{gathered}$$

est un isomorphisme d'espaces vectoriels et donc il en est de même pour l'application de $\mathrm{NS}(A) \otimes \mathbb{R}$ dans $(\mathrm{End}(A) \otimes \mathbb{R})^\dagger$. Si de plus $\mathcal{L}$ est ample, $\iota(\mathcal{L})$ est symétrique et défini positif. Notons $\mathrm{Amp}(A)$ l'ensemble des classes amples de $\mathrm{NS}(A)$. On remarque aussi, puisque $h_0\phi_{\mathcal{L}_0}^{-1} \in \mathrm{Hom}(\hat{A}, A)$ comme dans le lemme 3.1, que

$$\iota(\mathrm{NS}(A)) \subset \frac{1}{h_0}\mathrm{End}(A). \tag{11}$$

D'autre part G agit à droite sur $(\mathrm{End}(A) \otimes \mathbb{R})^\dagger$ par

$$f \cdot g = g^\dagger f g$$

où $g \in G$. Par restriction Γ agit sur $(\mathrm{End}(A) \otimes \mathbb{R})^\dagger$ et cette action est compatible avec l'action de Γ sur $\mathrm{NS}(A)$ puisque si $u \in \Gamma$ alors $\iota(u^*\mathcal{L}) = \phi_{\mathcal{L}_0}^{-1} \circ \hat{u} \circ \phi_{\mathcal{L}} \circ u = u^\dagger \circ \phi_{\mathcal{L}_0}^{-1} \circ \phi_{\mathcal{L}} \circ u = \iota(\mathcal{L}) \cdot u$.

Soit d un entier positif. Notre but est de majorer le nombre de classes de

$$\{\mathcal{L} \in \mathrm{Amp}(A),\ \deg(\phi_{\mathcal{L}}) = d\}/\Gamma$$

et donc, d'après la remarque ci-dessus, ceci revient à majorer le cardinal de l'ensemble

$$\mathrm{Pol}_d(A) = \{f \in \iota(\mathrm{Amp}(A)),\ \deg(f) = \frac{d}{d_0}\}/\Gamma. \tag{12}$$

Montrons d'abord que cet ensemble est recouvert par un nombre fini d'orbites sous l'action de G.

Proposition 3.7. *Il existe un sous-ensemble fini $\mathcal{R}$ de $(\mathbb{R}^*)^s$ et une injection*

$$\mathrm{Pol}_d(A) \hookrightarrow \bigcup_{r\in\mathcal{R}} \left(\iota(\mathrm{NS}(A)) \cap (r\cdot G)\right)/\Gamma.$$

De plus, pour tout $(r_1,\ldots,r_s)\in\mathcal{R}$ et pour tout $i=1,\ldots,s$, on a $r_i^2 \leq dd_0^{g-2}$ et $r_i \geq \frac{1}{h_0}$.

Démonstration. Soit $f\in\iota(\mathrm{Amp}(A))$ de degré $\frac{d}{d_0}$ et $(f_1,\ldots,f_s)$ le uplet associé dans $\prod_{i=1}^s \mathfrak{A}_i$. On montre dans un premier temps qu'il existe $g\in G$ et $r\in\mathfrak{A}$ tel que $f=rg^2$. En effet, on sait qu'il existe des isomorphismes de $\mathbb{R}$-algèbres (voir [12] théo. 6 p. 209–210) comme dans le diagramme commutatif suivant

$$\begin{array}{ccc}
\mathrm{End}(A)\otimes\mathbb{R} & \xrightarrow{\sim} & \prod M_{a_i}(\mathbb{R})\times\prod M_{b_i}(\mathbb{C})\times\prod M_{c_i}(\mathbb{H}) \\
\iota\uparrow & & \uparrow \\
\mathrm{NS}(A)\otimes\mathbb{R} & \xrightarrow{\sim} & \prod \mathcal{H}_{a_i}(\mathbb{R})\times\prod \mathcal{H}_{b_i}(\mathbb{C})\times\prod \mathcal{H}_{c_i}(\mathbb{H})
\end{array}$$

où $\mathcal{H}_a(\mathbb{R})$ désigne les matrices réelles symétriques, $\mathcal{H}_b(\mathbb{C})$ les matrices hermitiennes complexes et $\mathcal{H}_c(\mathbb{H})$ les matrices quaternioniques hermitiennes c'est-à-dire à coefficients dans le corps des quaternions de Hamilton, telles que ${}^t\bar{X}=X$ pour $X\mapsto\bar{X}$ l'involution usuelle de $\mathbb{H}$.

Dans ces trois algèbres il est vrai qu'une matrice définie positive admet une racine carrée définie positive (voir [5] pour le cas moins connu des matrices quaternioniques). On conclut qu'il existe $(h_1,\ldots,h_s)\in\prod_{i=1}^s\mathfrak{A}_i$ tels que pour tout $i=1,\ldots,s$ on ait $h_i^2=f_i$ et h_i défini positif et invariant par l'involution de Rosati.

On pose $r_i=(\det\,\rho(h_i))^{2/n_i}$ et $g_i=r_i^{-1/2}h_i$. On définit ensuite $g,r\in\mathfrak{A}$ tels que leurs images respectives dans $\prod_{i=1}^s\mathfrak{A}_i$ soient $(g_1,\ldots,g_s)$ et $(r_1,\ldots,r_s)$. Vérifions d'abord que $g\in G$. On calcule

$$\begin{aligned}
\det\,\rho(g) &= \prod_{i=1}^s \det\,\rho_i(g_i) \\
&= \prod_{i=1}^s \det\,\rho_i(r_i^{-1/2}h_i) \\
&= \prod_{i=1}^s r_i^{-n_i/2}\det\,\rho_i(h_i) \\
&= 1.
\end{aligned}$$

Puisque f est de la forme $\phi_{\mathcal{L}_0}^{-1}\circ\phi_{\mathcal{L}}$ alors $h_0 f\in\mathrm{End}A$ et $h_0 f_i\in\mathrm{End}B_i$. On a donc $d_0^{g_i}\deg f_i\in\mathbb{Z}$ (3.1). Par ailleurs, on sait que $\prod_{i=1}^s\deg f_i=\frac{d}{d_0}$, on a donc

$$dd_0^{g-1}=\prod_{i=1}^s d_0^{g_i}\deg f_i.$$

Puisque $d_0^{g_i}\deg f_i = d_0^{g_i}(\deg h_i)^2 = d_0^{g_i}r_i^{2g_i}$ est un entier qui divise dd_0^{g-1}, il est compris entre 1 et dd_0^{g-1}. On en déduit les inégalités $r_i\geq\frac{1}{h_0}$ et $r_i^2\leq dd_0^{g-2}$.

De plus, l'ensemble des r ainsi construits est fini car dd_0^{g-1} a un nombre fini de diviseurs.

Revenons maintenant à l'ensemble $\mathrm{Pol}_d(A)$. Le fait que f s'écrit $f = rg^2 = g^\dagger rg$ montre que dans chaque orbite de $\{\iota(\mathrm{Amp}(A)) \mid \deg f = \frac{d}{d_0}\}$ sous l'action de G il y a un élément r comme ci-dessus et que le nombre d'orbites est fini. Pour chaque orbite, on choisit un élément r et on note $\mathcal{R}$ l'ensemble de ces représentants. On identifiera $\mathcal{R}$ au sous-ensemble fini de $(\mathbb{R}^*)^s$ correspondant. On en déduit une injection

$$\mathrm{Pol}_d(A) \longrightarrow \bigcup_{r\in\mathcal{R}} \left(\iota(\mathrm{Amp}(A)) \cap (r \cdot G)\right)/\Gamma,$$

et en particulier, on peut remplacer $\iota(\mathrm{Amp}(A))$ par $\iota(\mathrm{NS}(A))$. □

3.3 Orbites et groupes d'isotropie

Définition 3.8. *Soient E un ensemble et G un groupe qui agit à droite sur E. Pour tout $x \in E$ le stabilisateur de x (ou sous-groupe d'isotropie) est*

$$\mathrm{Iso}(x) := \{g \in G \mid x \cdot g = x\}.$$

On reprend les notations de la partie 3.1. On construit un espace W et une représentation σ de façon que H et G correspondent aux groupes d'isotropie dans $\mathrm{GL}_n(\mathbb{R})$ de deux éléments bien choisis de W.

On pose $W = \mathrm{M}_n(\mathbb{R})^{n+1} \times \mathbb{R}^2$ et on considère l'action à droite de $\mathrm{GL}_n(\mathbb{R})$ sur W donnée par

$$(A_1, \ldots, A_n, B, a, b) \cdot M = (M^{-1}A_1M, \ldots, M^{-1}A_nM, {}^tMBM, (\det M)^2 a, \frac{b}{(\det M)^2}).$$

En utilisant cette action on considérera aussi une action de G sur W par

$$g \cdot w = w \cdot \rho(g).$$

Lemme 3.9. *On pose pour $r \in \mathcal{R} \cup \{0\}$,*

$$w_r = (D_1, \ldots, D_n, d_0 Q\rho(r), 1, 1).$$

Alors

(i) Pour $r \in \mathcal{R}$, $\mathrm{Iso}(r) = H$ (pour l'action de G sur $\mathrm{End}(A) \otimes \mathbb{R}$)

(ii) $\mathrm{Iso}(w_0) = \rho(G)$ (pour l'action de $\mathrm{GL}_n(\mathbb{R})$ sur W).

(iii) Pour $r \in \mathcal{R}$, $\mathrm{Iso}(w_r) = \rho(H)$ (pour l'action de $\mathrm{GL}_n(\mathbb{R})$ sur W).

Démonstration. Pour (i) il suffit de remarquer que r est dans le centre de $\mathrm{End}(A) \otimes \mathbb{R}$ et qu'il est inversible, d'où

$$\mathrm{Iso}(r) = \{f \in \mathrm{End}(A) \otimes \mathbb{R} \mid f^\dagger rf = r\} = \{f \in \mathrm{End}(A) \otimes \mathbb{R} \mid f^\dagger f = \mathrm{id}\} = H.$$

Démontrons (ii). On rappelle que $\rho : \mathfrak{A} \to M_n(\mathbb{R})$ est donnée par la représentation régulière à gauche et le choix de la base $(\alpha_1, \ldots, \alpha_n)$. Il est donc clair que $\rho(\mathfrak{A}) = \mathrm{Vect}(G_1, \ldots, G_n)$. Voyons maintenant que $\mathrm{Vect}(G_1, \ldots, G_n) = \{M \in M_n(\mathbb{R}),\ MD_i = D_iM,\ \forall i = 1, \ldots, n\}$. Pour simplifier la rédaction on va se placer dans l'espace $\mathcal{L}(\mathrm{End}(A)\otimes\mathbb{R})$ des endomorphismes linéaires de $\mathfrak{A}$. Notons d_i, g_i les endomorphismes correspondant aux D_i et G_i respectivement. D'une part, grâce à l'associativité de la multiplication on a pour tout $x \in \mathfrak{A}$

$$g_j d_i(x) = g_j(x\alpha_i) = \alpha_j x \alpha_i = d_i(\alpha_j x) = d_i(g_j(x))$$

et donc

$$\forall i, j \in \{1, \dots, n\}, \;\; G_j D_i = D_i G_j.$$

On a ainsi $\mathrm{Vect}(G_1, \dots, G_n) \subset \{M \in \mathrm{GL}_n(\mathbb{R}) \mid MD_i = D_i M, \forall i = 1, \dots, n\}$. D'autre part, notons $m \in \mathcal{L}(\mathfrak{A})$ tel que $md_i = d_i m$, $\forall i = 1, \dots, n$. Alors pour tout $x \in \mathfrak{A}$ on a $md_i(x) = d_i m(x)$. On applique ceci à $x = \mathrm{id}_{\mathfrak{A}}$ et on obtient

$$\begin{aligned} &md_i(\mathrm{id}_{\mathfrak{A}}) = m(\mathrm{id}_{\mathfrak{A}}\alpha_i) = m(\alpha_i) \text{ et} \\ &d_i m(\mathrm{id}_{\mathfrak{A}}) = m(\mathrm{id}_{\mathfrak{A}})\alpha_i. \end{aligned}$$

Puisque m est déterminé par l'image des éléments de la base $\alpha_1, \dots, \alpha_n$ on en déduit que m est la multiplication à gauche par $m(\mathrm{id}_{\mathfrak{A}})$. Pour conclure on vérifie facilement que

$$\mathrm{Iso}(w_0) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid \det(M) = \pm 1 \text{ et } MD_i = D_i M, \, \forall i = 1, \dots, n\}$$

et d'après la définition de G ceci correspond justement à $\rho(G)$.

Démontrons (iii). D'après le lemme 3.5 on a ${}^t\rho(a)Q = Q\rho(a^\dagger)$. On en déduit

$$\begin{aligned} \mathrm{Iso}(w_r) &= \rho(G) \cap \{M \in \mathrm{GL}_n(\mathbb{R}) \mid {}^tMQ\rho(r)M = Q\rho(r)\} \\ &= \{\rho(a) \mid {}^t\rho(a)Q\rho(r)\rho(a) = Q\rho(r), \, a \in G\} \\ &= \{\rho(a) \mid Q\rho(a^\dagger)\rho(r)\rho(a) = Q\rho(r), \, a \in G\} \\ &= \{\rho(a) \mid a^\dagger r a = r, \, a \in G\} \\ &= \rho(H). \end{aligned}$$

□

Plus tard on va devoir modifier légèrement les w_r pour que leurs groupes d'isotropie soient autoadjoints (préservés par conjugaison). On fera ceci en faisant agir sur w_r l'élément U (on rappelle que U est la matrice symétrique définie positive telle que $U^2 = Q$). Le lemme suivant regroupe ces informations.

Lemme 3.10. *Pour tout $r \in \mathcal{R} \cup \{0\}$ on a $\mathrm{Iso}(w_r \cdot U^{-1}) = U\mathrm{Iso}(w_r)U^{-1}$. De plus, ce groupe est stable par transposition.*

Démonstration. On a

$$\begin{aligned} M \in \mathrm{Iso}(w_r \cdot U^{-1}) &\Leftrightarrow w_r U^{-1} M = w_r U^{-1} \\ &\Leftrightarrow w_r U^{-1} M U = w_r \\ &\Leftrightarrow M \in U\mathrm{Iso}(w_r)U^{-1}. \end{aligned}$$

On considère maintenant $X \in U\mathrm{Iso}(w_r)U^{-1}$. Alors $X = U\rho(a)U^{-1}$ où $a \in G$ si $r = 0$ ou $a \in H$ si $r \neq 0$. On a donc ${}^tX = {}^tU^{-1}Q\rho(a^\dagger)Q^{-1}\,{}^tU$ (par le lemme 3.5), et alors

$${}^tX = U^{-1}U^2\rho(a^\dagger)U^{-2}U = U\rho(a^\dagger)U^{-1}.$$

Puisque G et H sont stables par $\dagger$ (lemme 3.6), on a finalement ${}^tX \in U\mathrm{Iso}(w_r)U^{-1}$.

□

3.4 Réseaux

On dispose de plusieurs réseaux dans les différents espaces vectoriels réels considérés. On liste ici quelques propriétés et on montre un résultat essentiel qui permet de se ramener à un calcul dans l'espace vectoriel W afin de contrôler $\mathrm{Pol}_d(A)$.

Notons $L = \frac{1}{h_0}\mathrm{End}A$ et $\Omega = M_n(\mathbb{Z})^{n+1} \times \mathbb{Z}^2$. On remarque que Ω est un réseau de W, $\iota(\mathrm{NS}(A))$ est un réseau de $(\mathrm{End}(A) \otimes \mathbb{R})^\dagger$ et on rappelle que $\iota(\mathrm{NS}(A)) \subset L$ (voir 3.2, (11)).

D'après la proposition 3.7, pour borner le cardinal de $\mathrm{Pol}_d(A)$ il suffit donc de montrer que pour tout $r \in \mathcal{R}$, $(L \cap r \cdot G)/\Gamma$ est fini et de trouver une borne. On montre qu'on peut se ramener à calculer des orbites dans W pour l'action définie plus haut :

Proposition 3.11. *Soit $r \in \mathcal{R}$. Alors on a une injection*

$$(L \cap r \cdot G)/\Gamma \longrightarrow (\Omega \cap w_r \cdot G)/\Gamma.$$

Démonstration. On considère $\mu : \mathfrak{A} \longrightarrow W$ définie par

$$\mu(x) = (D_1, \ldots, D_n, d_0 Q\rho(x), 1, 1).$$

On remarque d'abord que $\mu(L) \subset \Omega$. En effet, on a vu que $Q \in \frac{1}{h_0}M_n(\mathbb{Z})$ (remarque 3.2), et si $x = \frac{1}{h_0}\alpha$ avec $\alpha \in \mathrm{End}A$, alors $\rho(x) \in \frac{1}{h_0}M_n(\mathbb{Z})$ également. Voyons maintenant que pour tout $g \in G$, $\mu(x \cdot g) = \mu(x) \cdot g$.

$$\begin{aligned}\mu(x \cdot g) &= \mu(g^\dagger x g) \\ &= (D_1, \ldots, D_n, d_0 Q\rho(g^\dagger x g), 1, 1) \\ &= (D_1, \ldots, D_n, d_0 {}^t\rho(g) Q\rho(x)\rho(g), 1, 1) \\ &= (D_1, \ldots, D_n, d_0 Q\rho(x), 1, 1) \cdot \rho(g) \\ &= \mu(x) \cdot g.\end{aligned}$$

Puisque μ est injective (car Q inversible et ρ est fidèle) et $\mu(r) = w_r$, alors μ induit une bijection entre les orbites

$$r \cdot G \longrightarrow w_r \cdot G.$$

De plus, de façon évidente, l'action de Γ sur $L \cap r \cdot G$ est compatible avec μ. $\square$

Les propositions 3.11 et 3.7 montrent qu'il suffit de contrôler les orbites de $w_r \cdot G \cap \Omega$ sous l'action de Γ. Le reste de l'article sera dédié à cette tâche. Dans la partie 5 on introduira les ensembles de Siegel, mais nous pouvons dès à présent donner un aperçu du chemin à suivre.

Proposition 3.12. *Soit $\mathfrak{S}$ un sous-ensemble de* $\mathrm{GL}_n(\mathbb{R})$ *tel que* $\mathrm{GL}_n(\mathbb{R}) = \mathfrak{S}\mathrm{GL}_n(\mathbb{Z})$*, alors*

$$\mathrm{Pol}_d(A) \hookrightarrow (\Omega \cap w_0 \cdot U^{-1}\mathfrak{S}) \times \bigcup_{r \in \mathcal{R}} (\Omega \cap w_r \cdot U^{-1}\mathfrak{S}).$$

Démonstration. Les propositions 3.7 et 3.11 nous donnent une injection

$$\mathrm{Pol}_d(A) \hookrightarrow \bigcup_{r \in \mathcal{R}} \left(\iota(\mathrm{NS}(A)) \cap (r \cdot G)\right)/\Gamma \hookrightarrow \bigcup_{r \in \mathcal{R}} \left(\Omega \cap w_r \cdot G\right)/\Gamma.$$

Voyons maintenant qu'il existe un sous-ensemble C de $\mathrm{GL}_n(\mathbb{Z})$ et une injection $C \hookrightarrow \Omega \cap w_0 \cdot U^{-1}\mathfrak{S}$ tels que $\rho(G) \subset U^{-1}\mathfrak{S}C\rho(\Gamma)$. On regarde l'ensemble

$$C' = w_0 \cdot U^{-1}\mathfrak{S} \cap w_0 \cdot \mathrm{GL}_n(\mathbb{Z}),$$

et on choisit $C \subset \mathrm{GL}_n(\mathbb{Z})$ tel que $\forall y \in C' \exists! x \in C$ tel que $y = w_0 \cdot x^{-1}$. Puisque $w_0 \cdot \mathrm{GL}_n(\mathbb{Z}) \subset \Omega$ on a clairement une injection de C vers $w_0 \cdot U^{-1}\mathfrak{S} \cap \Omega$.

Si $g \in \rho(G)$ il existe donc $s \in \mathfrak{S}$ et $b \in \mathrm{GL}_n(\mathbb{Z})$ tels que $Ug = sb$. On a

$$\begin{aligned} w_0 &= w_0 \cdot g \\ &= w_0 \cdot U^{-1}sb \end{aligned}$$

et

$$w_0 \cdot b^{-1} = w_0 \cdot U^{-1}s$$

d'où il existe un unique $x \in C$ tel que

$$\begin{aligned} w_0 \cdot b^{-1} &= w_0 \cdot x^{-1} \quad \text{et} \\ w_0 &= w_0 \cdot x^{-1}b. \end{aligned}$$

De plus, $x^{-1}b \in \mathrm{GL}_n(\mathbb{Z}) \cap \rho(G) = \rho(\Gamma)$ et alors $g = U^{-1}sb \in U^{-1}\mathfrak{S}C\rho(\Gamma)$. On en déduit des injections successives

$$\begin{aligned} \mathrm{Pol}_d(A) &\hookrightarrow \bigcup_{r \in \mathcal{R}} \left(\Omega \cap w_r \cdot U^{-1}\mathfrak{S}C\rho(\Gamma)\right)/\Gamma \\ &\hookrightarrow C \times \bigcup_{r \in \mathcal{R}} \Omega \cap w_r \cdot U^{-1}\mathfrak{S} \\ &\hookrightarrow (\Omega \cap w_0 \cdot U^{-1}\mathfrak{S}) \times \bigcup_{r \in \mathcal{R}} \Omega \cap w_r \cdot U^{-1}\mathfrak{S}. \end{aligned}$$

□

Pour conclure on doit maintenant montrer que $\Omega \cap w_0 \cdot U^{-1}\mathfrak{S}$ et $\bigcup \Omega \cap w_r \cdot U^{-1}\mathfrak{S}$ sont finis et borner leur cardinal.

3.5 Normes

On notera $\|\cdot\|_W$ la norme produit sur $W = M_n(\mathbb{R})^{n+1} \times \mathbb{R}^2$ donnée par

$$\|(A_1, \ldots, A_{n+1}, a, b)\|_W = \sup\{\|A_1\|_F, \ldots, \|A_{n+1}\|_F, |a|, |b|\}$$

où $\|A\|_F = \sqrt{\mathrm{tr}(A^tA)}$ est la norme de Frobenius (ou norme de Hilbert-Schmidt). Rappelons quelques propriétés usuelles de cette norme.

Lemme 3.13. *1. Pour tous $M, N \in \mathrm{GL}_n(\mathbb{R})$, alors $\|MN\|_F \leq \|M\|_F\|N\|_F$.*

2. Pour tout $M \in \mathrm{GL}_n(\mathbb{R})$ et $x \in \mathbb{R}^n$, on a $\|Mx\|_2 \leq \|M\|_F\|x\|_2$.

3. Pour tout $M \in \mathrm{GL}_n(\mathbb{R})$, $\|M^{-1}\|_F \leq \|M\|_F^{n-1} \frac{1}{|\det M| n^{(n-2)/2}}$

Démonstration. Pour (1) et (2) voir par exemple [?], Chap.5.6. Pour l'inégalité (3) on remarque d'abord que $\|M^{-1}\|_F^2 = \mathrm{tr}((M^tM)^{-1}) = \mathrm{tr}(^tMM)^{-1}$. Puisque ^tMM est symétrique définie positive, ses valeurs propres sont toutes strictement positives. On les note $\lambda_1, \dots, \lambda_n$ et la trace de $(^tMM)^{-1}$ est $\frac{1}{\lambda_1} + \dots + \frac{1}{\lambda_n}$. Il suffit donc d'établir l'inégalité

$$\frac{1}{\lambda_1} + \dots + \frac{1}{\lambda_n} \leq \frac{(\lambda_1 + \dots + \lambda_n)^{n-1}}{\lambda_1 \cdots \lambda_n} \cdot \frac{1}{n^{n-2}} \tag{13}$$

pour tout $(\lambda_1, \dots, \lambda_n) \in (\mathbb{R}_+^*)^n$ qui s'obtient élémentairement (par exemple par extréma liés). Pour conclure il suffit de remarquer que $\lambda_1 \cdots \lambda_n = (\det M)^2$. □

On aura aussi besoin du résultat suivant :

Lemme 3.14. *Soient $\alpha, \beta \in \mathfrak{A}$ et $|\cdot|$ la norme induite par l'involution de Rosati sur $\mathfrak{A}$. Alors*

1. $|\alpha| = \|U\rho(\alpha)U^{-1}\|_F$.
2. $|\alpha\beta| \leq |\alpha||\beta|$.

Démonstration. Par définition de $|\cdot|$ on a $|\alpha|^2 = \mathrm{Tr}_{\mathfrak{A}/\mathbb{R}}(\alpha\alpha^\dagger) = \mathrm{tr}(\rho(\alpha)\rho(\alpha^\dagger)) = \mathrm{tr}(\rho(\alpha)Q^{-1t}\rho(\alpha)Q)$ d'après le lemme 3.5. On pose $X_\alpha = U\rho(\alpha)U^{-1}$. On a

$$\begin{aligned}
\mathrm{tr}(\rho(\alpha)Q^{-1t}\rho(\alpha)Q) &= \mathrm{tr}(\rho(\alpha)U^{-1}U^{-1t}\rho(\alpha)UU) \\
&= \mathrm{tr}(U\rho(\alpha)U^{-1t}U^{-1t}\rho(\alpha)^tU) \\
&= \mathrm{tr}(X_\alpha{}^tX_\alpha) = \|U\rho(\alpha)U^{-1}\|_F^2.
\end{aligned}$$

Ceci montre la première assertion. On en déduit la deuxième en utilisant (1) et le lemme 3.13 :

$$\begin{aligned}
|\alpha\beta| &= \|U\rho(\alpha\beta)U^{-1}\|_F \\
&\leq \|U\rho(\alpha)U^{-1}U\rho(\beta)U^{-1}\|_F \\
&\leq \|U\rho(\alpha)U^{-1}\|_F\|U\rho(\beta)U^{-1}\|_F \\
&\leq |\alpha||\beta|.
\end{aligned}$$

□

On peut à présent calculer des bornes pour les normes des différentes matrices introduites. On rappelle que $\Sigma = \frac{1}{2}D^{1/2}n^{\frac{n+2}{2}}h_0^{\frac{n-1}{2}}$. Alors

Lemme 3.15. *1. $\|Q\|_F \leq n\Sigma^2$ et $\|U\|_F \leq n^{1/2}\Sigma$.*

2. $\|U^{-1}\|_F \leq \Sigma^{n-1}n^{1/2}D^{-1/2}$.
3. *Pour tout $r \in \mathcal{R}$, $\|U\rho(r)U^{-1}\|_F^2 = |r|^2 \leq ndd_0^{g-2}$.*
4. $\|w_0 \cdot U^{-1}\|_W \leq \sup\left\{n^{1/2}\Sigma, D\right\}$.
5. *Pour tout $r \in \mathcal{R}$,*

$$\|w_r \cdot U^{-1}\|_W \leq \sup\left\{n^{1/2}\Sigma, (ndd_0^g)^{1/2}, D\right\}.$$

Démonstration. Pour (1) il suffit de rappeler que le terme général de Q est $\mathrm{Tr}(\alpha_i \alpha_j^\dagger)$ et que $|\alpha_i| \leq \Sigma$ (lemme 3.3). On écrit alors

$$\|Q\|_F \leq \|U\|_F^2 = \mathrm{tr}({}^tUU) = \mathrm{tr}(Q) = \sum_{i=1}^n |\alpha_i|^2 \leq n\Sigma^2.$$

Pour (2) on utilise l'estimation du lemme 3.13,

$$\begin{aligned}\|U^{-1}\|_F &\leq \frac{\|U\|_F^{n-1}}{|\det U|\sqrt{n^{n-2}}} \\ &\leq \frac{n^{(n-1)/2}\Sigma^{n-1}}{\sqrt{Dn^{n-2}}} \leq \Sigma^{n-1}D^{-1/2}n^{1/2}.\end{aligned}$$

Pour (3), la première égalité a été prouvée dans le lemme 3.14. Pour la deuxième, on remarque que $|r|^2 = \mathrm{tr}(\rho(r^2))$ car r est stable par l'involution de Rosati. De plus $\mathrm{tr}(\rho(r^2)) = \sum_{i=1}^s \mathrm{tr}(\rho_i(r_i^2)) = \sum_{i=1}^s n_i r_i^2$. En utilisant la proposition 3.7, on en déduit l'estimation

$$\begin{aligned}\|U\rho(r)U^{-1}\|_F^2 &\leq \sum_{i=1}^s n_i d d_0^{g-2} \\ &\leq n d d_0^{g-2}.\end{aligned}$$

Calculons maintenant $\|w_0 \cdot U^{-1}\|_F$. Par définition

$$\begin{aligned}\|w_0 \cdot U^{-1}\|_W &= \|(UD_1U^{-1}, \ldots, UD_nU^{-1}, 0, \det U^{-2}, \det U^2)\|_W \\ &\leq \sup_i\{\|UD_iU^{-1}\|_F, \det U^2, \det U^{-2}\}\end{aligned}$$

Pour calculer $\|UD_iU^{-1}\|_F$ on remarque que cette matrice représente la multiplication à droite par α_i dans la base $\mathcal{D}$ de $\mathfrak{A}$ dont les vecteurs ont pour coordonnées dans la base $(\alpha_1, \ldots, \alpha_n)$ les colonnes de la matrice U (*i.e.* U est la matrice de passage de la base $\mathcal{D}$ à la base $(\alpha_1, \ldots, \alpha_n)$). Puisque ${}^tU^{-1}QU^{-1} = I$ on en déduit que la base $\mathcal{D}$ est orthonormée pour la norme $|\cdot|$. Les coefficients de la k-ième colonne de UD_iU^{-1} sont les scalaires y_{jk} tels que si β_k désigne le k-ième vecteur de la base $\mathcal{D}$ alors $\beta_k\alpha_i = y_{1k}\beta_1 + \ldots + y_{nk}\beta_n$ on en déduit

$$y_{1k}^2 + \ldots + y_{nk}^2 = |\beta_k\alpha_i|^2 \leq |\alpha_i|^2$$

et en sommant sur tous les k on obtient

$$\|UD_iU^{-1}\|_F^2 = \sum_{k=1}^n y_{1k}^2 + \ldots + y_{nk}^2 \leq n|\alpha_i|^2 \leq n\Sigma^2$$

et donc

$$\|w_0 \cdot U^{-1}\|_W \leq \sup\left\{n^{1/2}\Sigma, D\right\}.$$

Similairement,

$$\begin{aligned}\|w_r \cdot U^{-1}\|_W &= \|(UD_1U^{-1}, \ldots, UD_nU^{-1}, d_0{}^tU^{-1}Q\rho(r)U^{-1}, \det U^{-2}, \det U^2)\|_W \\ &\leq \sup\{\|UD_iU^{-1}\|_F, d_0\|U\rho(r)U^{-1}\|_F, D\}\end{aligned}$$

et en utilisant les bornes déjà calculées on a

$$\|w_r \cdot U^{-1}\|_W \leq \sup\left\{n^{1/2}\Sigma, (ndd_0^g)^{1/2}, D\right\}.$$

□

4 Argument de compacité

Dans cette partie on montre une version particulière à notre contexte et explicite du résultat suivant (voir [3], Chap VII, App 1, lemme 2) :

Proposition 4.1. *Soient $G = \mathrm{GL}_n(\mathbb{R})$, une représentation dans un espace vectoriel réel V et un vecteur $v \in V$ dont l'orbite $v \cdot G$ est fermée dans V. Soient $C \in \mathbb{R}$ et $E = \{z \in G,\ \|v \cdot z\| \leq C\}$. Alors il existe un compact M de G tel que l'on ait $E \subset G_v \cdot M$ où G_v est le groupe d'isotropie de v.*

On utilisera notamment le résultat sur les ellipsoïdes (théo. 2.1) et les différentes estimations pour les normes calculées dans la partie précédente.

Proposition 4.2. *Soient $Z \in \mathrm{GL}_n(\mathbb{R})$, $r \in \mathcal{R}$ et $c > 0$ un réel.*

1. *Si $\|(w_0 \cdot U^{-1}) \cdot Z\|_W \leq c$ alors il existe $M_0 \in \mathrm{GL}_n(\mathbb{R})$ avec les propriétés suivantes*
   - *i)* $(w_0 \cdot U^{-1}) \cdot M_0 = (w_0 \cdot U^{-1}) \cdot Z$,
   - *ii)* $\|M_0^{-1}\|_F \leq cn\|U^{-1}\|_F |\det Z|^{-1/n}$.
2. *Si $\|(w_r \cdot U^{-1}) \cdot Z\|_W \leq c$ alors $\|Z\|_F^2 \leq c\frac{n^2}{h_0}$.*

Démonstration. Notons $B = Z^{-1}U$. On remarque d'abord que la condition $(w_0 \cdot U^{-1}) \cdot M = w_0 \cdot B$ est équivalente aux conditions (I) et (II) suivantes :

$$M^{-1}UD_iU^{-1}M = BD_iB^{-1}, \quad \forall i = 1 \dots, n \tag{I}$$
$$(\det M)^2 = (\det Z)^2 \tag{II}$$

En regardant (I) de plus près on obtient

$$\begin{aligned}
\text{(I)} &\Leftrightarrow B^{-1}M^{-1}UD_i = D_iB^{-1}M^{-1}U,\ \forall i = 1, \dots, n \\
&\Leftrightarrow B^{-1}M^{-1}U \in \mathrm{Vect}\{G_1 \dots, G_n\} \\
&\Leftrightarrow M^{-1} \in B\mathrm{Vect}\{G_1, \dots, G_n\}U^{-1}.
\end{aligned}$$

On remarque immédiatement que pour tout $x \in \mathbb{R}^n$ tel que $|\det \sum x_iG_i| \neq 0$ les matrices de la forme

$$M = |\det(\sum x_iG_i)|^{1/n} \left(B(\sum x_iG_i)U^{-1}\right)^{-1}$$

satisfont les conditions (I) et (II). Supposons pour l'instant que x ait cette propriété. On commence par trouver une majoration de la norme de la matrice $B(\sum x_iG_i)U^{-1}$. Soient $j \in \{1, \dots, n\}$ et e_j le j-ème vecteur de la base canonique de $\mathbb{R}^n$. La j-ème colonne de la matrice $B(\sum x_iG_i)$ est :

$$\begin{aligned}
B(\sum x_iG_i)e_j &= B(\sum x_i(G_ie_j)) \\
&= B(\sum x_i(D_je_i)) \\
&= BD_j \sum x_ie_i \\
&= BD_jx \\
&= BD_jB^{-1}(Bx)
\end{aligned}$$

et donc (car $\|w_0 \cdot B^{-1}\|_W \leq c$)

$$\|B(\sum x_i G_i)e_j\|_2 \leq \|BD_jB^{-1}\|_F\|Bx\|_2 \leq c\|Bx\|_2.$$

On en déduit

$$\begin{aligned}\|B(\sum x_iG_i)U^{-1}\|_F^2 &\leq \|B(\sum x_iG_i)\|_F^2\|U^{-1}\|_F^2\\ &\leq n\max_j \|B(\sum x_iG_i)e_j\|_2^2\|U^{-1}\|_F^2\\ &\leq c^2n\|U^{-1}\|_F^2\|Bx\|_2^2.\end{aligned}$$

Donc si $|\det \sum x_iG_i| \neq 0$, la norme de la matrice M^{-1} est bornée par

$$\|M^{-1}\|_F^2 \leq c^2n\|U^{-1}\|_F^2\frac{\|Bx\|_2^2}{|\det\sum x_iG_i|^{2/n}}.$$

On rappelle que $(\alpha_1,\ldots,\alpha_n)$ est la $\mathbb{Z}$-base de $\mathrm{End}(A)$ choisie dans (9). On considère l'application

$$\begin{aligned}\alpha : \mathbb{R}^n &\to \mathfrak{A}\\ x &\mapsto \sum x_i\alpha_i.\end{aligned}$$

Avec cette notation, trouver $x \in \mathbb{R}^n$ tel que $|\det\sum x_iG_i| \neq 0$ revient à trouver $y \in \mathfrak{A}$ tel que $|N_{\mathfrak{A}/\mathbb{R}}(y)| \neq 0$ et poser ensuite $x = \alpha^{-1}(y)$. On aura donc

$$\frac{\|Bx\|_2^2}{|\det\sum x_iG_i|^{2/n}} = \frac{\|B\alpha^{-1}(y)\|_2^2}{|N_{\mathfrak{A}/\mathbb{R}}(y)|^{2/n}}.$$

Pour trouver un tel y on utilise le theorème 2.1.

On pose

$$\gamma = \sqrt{n}\frac{|\det B|^{1/n}}{\sqrt{D^{1/n}}}$$

et on considère la forme quadratique réelle sur $\mathfrak{A}$ définie par $q(y) = \frac{1}{\gamma^2}\|B\alpha^{-1}(y)\|_2^2$. Calculons le volume de l'ellipsoïde défini par q où on considère le volume associé à la mesure de Haar pour la norme $\|y\|_\alpha = \|\alpha^{-1}(y)\|_2$:

$$\begin{aligned}\mathrm{vol}\{y\in\mathfrak{A}, q(y)\leq 1\} &= \frac{\gamma^n}{|\det B|}\mathrm{vol}\{y\in\mathfrak{A}, \|\alpha^{-1}(y)\|_2\leq 1\}\\ &= \frac{\gamma^n}{|\det B|}\mathrm{vol}(B_{1,\|\,\|_\alpha}).\end{aligned}$$

De même on calcule $\mathrm{vol}\{y \in \mathfrak{A}, \mathrm{Tr}(yy^\dagger) \leq n\} = \dfrac{\sqrt{n}^n\mathrm{vol}(B_{1,\|\,\|_\alpha})}{\sqrt{D}}$. On voit donc que les deux ellipsoïdes ont le même volume et par le théorème 2.1 il existe $y_1 \in \mathfrak{A}$ tel que $q(y_1) \leq 1$ et $|N_{\mathfrak{A}/\mathbb{R}}(y_1)| \geq 1$. On pose $x = \alpha^{-1}(y_1)$ et $M_0 = |\det(\sum x_iG_i)|^{\frac{1}{n}}(Z^{-1}U(\sum x_iG_i)U^{-1})^{-1}$ il s'en suit que

$$\begin{aligned}\|M_0^{-1}\|_F &\leq cn^{1/2}\|U^{-1}\|_F\gamma\\ &\leq cn\|U^{-1}\|_F|\det B|^{1/n}D^{-1/2n}\\ &\leq cn\|U^{-1}\|_F|\det Z|^{-1/n}\end{aligned}$$

donc M_0 vérifie bien les conditions de la proposition.

Pour la deuxième partie de l'énoncé, voyons qu'à partir de $\|w_r \cdot U^{-1} \cdot Z\| \leq c$ on déduit la borne attendue pour $\|Z\|_F$. Soit $h \in \mathbb{R}^s$ tel que $h^2 = r$ et notons $H = U\rho(h)U^{-1}$. En utilisant le lemme 3.5 on remarque que

$$\begin{aligned} H &= U^{-1}Q\rho(h)U^{-1} \\ &= U^{-1t}\rho(h)QU^{-1} \\ &= U^{-1t}\rho(h)U \\ &= {}^tH. \end{aligned}$$

Ainsi H est symétrique et $H^2 = U\rho(r)U^{-1}$. L'hypothèse $\|w_r \cdot U^{-1} \cdot Z\| \leq c$ implique $\|d_0\, {}^tZU^{-1}Q\rho(r)U^{-1}Z\| \leq c$ et donc $\|d_0\, {}^t(HZ)(HZ)\|_F \leq c$.

Chaque coefficient de ${}^t(HZ)(HZ)$ est donc borné en valeur absolue par $\frac{c}{d_0}$ et alors $\|HZ\|_F^2 = \mathrm{tr}({}^t(HZ)(HZ)) \leq \frac{nc}{d_0}$.

On écrit $Z = H^{-1}.HZ$ et d'après le lemme 3.13 on a

$$\|Z\|_F^2 \leq \|H^{-1}\|_F^2 \|HZ\|_F^2 \leq \frac{nc}{d_0}\|H^{-1}\|_F^2.$$

En modifiant légèrement le calcul de $\|U\rho(r)U^{-1}\|_F$ effectué dans le lemme 3.15 et avec les bornes de la proposition 3.7 on trouve

$$\|H^{-1}\|_F^2 = \sum_{i=1}^{s} \mathrm{tr}(\rho(r_i^{-1})) \leq \sum_{i=1}^{s} n_i r_i^{-1} \leq nh_0.$$

On en déduit finalement $\|Z\|_F^2 \leq c\frac{n^2}{h_0}$. □

5 Ensembles de Siegel

Dans cette partie on démontre le deuxième résultat clé de la preuve. Il s'agit d'une version effective d'un lemme de finitude de Borel ([1], lemme 6.2 p. 39) adapté à notre problème. On rappelle d'abord quelques notions et résultats classiques de réduction dans $\mathrm{GL}_n(\mathbb{R})$.

On notera $\mathcal{D}$ le groupe des matrices diagonales à coefficients strictement positifs, $\mathcal{K}$ le groupe orthogonal et $\mathcal{T}$ le groupe des matrices triangulaires supérieures de valeurs propres égales à un.

Définition 5.1. *On appelle ensemble de Siegel de* $\mathrm{GL}_n(\mathbb{R})$ *tout ensemble de la forme* $\mathfrak{S}_{t,u} = \mathcal{K}\mathcal{D}_t\mathcal{T}_u$ *pour* t, u *des réels positifs où*

$$\begin{aligned} \mathcal{D}_t &= \{a \in \mathcal{D} \mid a_{ii} \leq t a_{i+1,i+1} \quad (i = 1, \ldots, n-1)\} \\ \mathcal{T}_u &= \{b \in \mathcal{T} \mid |b_{ij}| \leq u \quad (1 \leq i < j \leq n)\}. \end{aligned}$$

Ces ensembles ont la propriété fondamentale suivante (voir [1], théo. 1.4 p. 14) :

Théorème 5.2. *Pour tous* $t \geq 2/\sqrt{3}$ *et* $u \geq 1/2$ *on a*

$$\mathrm{GL}_n(\mathbb{R}) = \mathfrak{S}_{t,u}\mathrm{GL}_n(\mathbb{Z}).$$

En utilisant la propriété 3.12 on sait donc que l'ensemble qu'on cherche à borner s'injecte dans

$$(\Omega \cap w_0 \cdot U^{-1}\mathfrak{S}) \times \bigcup_{r \in \mathcal{R}} (\Omega \cap w_r \cdot U^{-1}\mathfrak{S})$$

avec $\mathfrak{S} = \mathfrak{S}_{\frac{2}{\sqrt{3}},\frac{1}{2}}$. Dans cette partie on calcule des bornes pour les normes des éléments de $w_r \cdot U^{-1}\mathfrak{S}$ avec $r \in \mathcal{R} \cup \{0\}$. On fera ceci en se servant de la proposition 4.2.

Dans toute la suite on notera $\mathfrak{S}$ l'ensemble de Siegel $\mathfrak{S}_{\frac{2}{\sqrt{3}},\frac{1}{2}}$ et pour $x \in \mathfrak{S}$, on notera $x = k_x a_x b_x$ sa décomposition d'Iwasawa et $y_x = x a_x^{-1}$.

Lemme 5.3. *Soient $v \in W$ et $x \in \mathfrak{S}$. Alors*

$$\|v \cdot y_x\|_W \leq n^{\frac{n}{2}+1} \left(\frac{2}{\sqrt{3}}\right)^{n(n-1)} \|v\|_W$$

Démonstration. On vérifie facilement que les coefficients de la matrice $a_x b_x a_x^{-1}$ sont de la forme $(a_x b_x a_x^{-1})_{ij} = \frac{a_{ii}}{a_{jj}} b_{ij}$ pour $i \leq j$, et nuls autrement. Ils sont donc bornés en valeur absolue par $(\frac{2}{\sqrt{3}})^{n-1}$. On en déduit

$$\|y_x\|_F = \|k_x a_x b_x a_x^{-1}\|_F = \|a_x b_x a_x^{-1}\|_F \leq n \left(\frac{2}{\sqrt{3}}\right)^{n-1}.$$

Puisque $y_x^{-1} = a_x b_x^{-1} a_x^{-1\,t}k_x$, on en déduit (avec le lemme 3.13)

$$\|y_x^{-1}\|_F = \|(a_x b_x a_x^{-1})^{-1} k_x^{-1}\|_F = \|(a_x b_x a_x^{-1})^{-1}\|_F \leq n^{\frac{n}{2}} \left(\frac{2}{\sqrt{3}}\right)^{(n-1)^2}.$$

Maintenant lorsqu'on fait agir y_x sur v on a

$$\begin{aligned}\|v \cdot y_x\|_W &\leq \sup\{\|y_x\|_F \|y_x^{-1}\|_F, \|y_x\|_F^2, \det(y_x)^2, \det(y_x)^{-2}\} \|v\|_W \\ &\leq n^{\frac{n}{2}+1} \left(\frac{2}{\sqrt{3}}\right)^{n(n-1)} \|v\|_W.\end{aligned}$$

□

Pour démontrer le lemme suivant, on décompose l'espace W en une somme directe de sous-espaces et on travaille dans les projections. Rappelons que $\mathcal{D}$ désigne l'ensemble des matrices diagonales à coefficients strictement positifs. On remarque dans un premier temps :

Fait 1 : Soit $(e_1, \ldots, e_N)$ la base canonique de W ($N = n^2(n+1)+2$). Alors $\forall a \in \mathcal{D}$, $\forall l \in \mathbb{N}$, $1 \leq l \leq N$, il existe $\mu(a) \in \mathbb{R}$ tel que

$$e_l \cdot a = \mu(a) e_l.$$

En effet si E_{ij} est la matrice dont le coefficient i, j est 1 et les autres sont nuls l'action de a est donnée par

$a^{-1} E_{ij} a = a_{jj} a_{ii}^{-1} E_{ij}$ pour les n^3 premiers vecteurs de la base,

${}^t a E_{ij} a = a_{ii} a_{jj} E_{ij}$ pour les n^2 vecteurs suivants, ou encore pour les deux derniers vecteurs de la base

$$(\det a)^2.1 = (\prod_i a_{ii}^2).1 \quad \text{et}$$
$$(\det a)^{-2}.1 = (\prod_i a_{ii}^{-2}).1.$$

On note

$$W_\mu = \{w \in W \mid \forall a \in \mathcal{D}, \ \ w \cdot a = \mu(a)w\}.$$

Fait 2 : On dispose de $\frac{n(3n-1)}{2} + 3$ fonctions $\mu : \mathcal{D} \to \mathbb{R}$ différentes. En effet, d'après la description faite plus haut on vérifie facilement que μ parcourt l'ensemble des fonctions suivantes :

$$\mu(a) = a_{ii}a_{jj}^{-1} \text{ où } 1 \leq i,j \leq n,\, i \neq j$$
$$\mu(a) = 1$$
$$\mu(a) = a_{ii}a_{jj} \text{ où } 1 \leq i \leq j \leq n$$
$$\mu(a) = \prod_i a_{ii}^2$$
$$\mu(a) = \prod_i a_{ii}^{-2}.$$

On a une somme directe

$$W = \bigoplus_\mu W_\mu$$

et on notera $E_\mu : W \to W_\mu$ la projection de W sur W_μ. On remarque que chaque vecteur e_i de la base précédemment choisie pour W appartient à un des sous-espaces W_μ.

Fait 3 : Si $v \in \Omega$ et $E_\mu(v) \neq 0$ alors $\|E_\mu(v)\|_W \geq 1$.

En effet on vérifie facilement que si $v \in \Omega$ alors $E_\mu(v) \in \Omega$ et de façon évidente, si $E_\mu(v) \neq 0$, $\|E_\mu(v)\|_W \geq 1$.

Lemme 5.4. *Soient $v \in W$, $x \in \mathfrak{S}$ et $z_x = xa_x^{-2}$. Si $v \cdot x \in \Omega$ alors*

$$\|v \cdot z_x\|_W \leq \sqrt{2}n\|v \cdot y_x\|_W^2.$$

Démonstration. Posons $c = \|v \cdot y_x\|_W$. En utilisant la projection décrite ci-dessus, on a que $\|E_\mu(v \cdot y_x)\|_W$ est aussi majoré par exemple par c. Puisque $\forall w \in W$, $\forall t \in \mathrm{GL}_n(\mathbb{R}), \forall a \in \mathcal{D}$, on a $E_\mu((w \cdot t) \cdot a) = \mu(a)E_\mu(w \cdot t)$, on en déduit

$$E_\mu(v \cdot z_x) = E_\mu(v \cdot y_x a_x^{-1}) = \mu(a_x^{-1})E_\mu(v \cdot y_x).$$

D'autre part

$$E_\mu(v \cdot y_x) = \mu(a_x^{-1})E_\mu(v \cdot x).$$

En utilisant le fait 3, si $E_\mu(v \cdot y_x) \neq 0$ on a

$$c \geq \|E_\mu(v \cdot y_x)\|_W \geq |\mu(a_x)^{-1}|$$

et alors $|\mu(a_x)^{-1}| \leq c$. On a finalement

$$\|E_\mu(v \cdot z_x)\|_W \leq c^2$$

et en sommant pour tous les μ on obtient

$$\begin{aligned}
\|v \cdot z_x\|_W^2 &\leq \sum_\mu \|E_\mu(v \cdot z_x)\|_W^2 \\
&\leq \sum_\mu c^4 \\
&\leq \left(\frac{n(3n-1)}{2} + 3\right) c^4 \\
&\leq 2n^2 \|v \cdot y_x\|_W^4.
\end{aligned}$$

□

Proposition 5.5. *Soient $r \in \mathcal{R} \cup \{0\}$, $v_r = w_r \cdot U^{-1}$ et $x \in \mathfrak{S}$ tels que $v_r \cdot x \in \Omega$. On pose $c_r = \sqrt{2} n^{n+3} \left(\frac{2}{\sqrt{3}}\right)^{2n(n-1)} \|v_r\|_W^2$. Alors*

1. *Si $r = 0$ il existe une matrice M_0 telle que $v_0 \cdot z_x = v_0 \cdot M_0$,*

$$\|v_0 \cdot x\|_W \leq \|v_0\|_W \sup \left\{ D^{-1/2} n^{\frac{n}{2}+3} \left(\frac{4}{3}\right)^{n(n-1)} \|M_0^{-1}\|_F^n, D \right\}$$

et $\|M_0^{-1}\| \leq c_0 n \|U^{-1}\|_F D^{\frac{1}{2n}}$.

2. *Si $r \neq 0$,*

$$\begin{aligned}
&\|v_r \cdot x\|_W \leq \|v_r\|_w \\
&\quad \times \sup \left\{ n^{\frac{n}{2}+3} \left(\frac{4}{3}\right)^{n(n-1)} \|z_x\|_F^n D^{1/2}, n^{6-n} \left(\frac{4}{3}\right)^{2(n-1)} \|z_x\|_F^{2(n-1)} D, D \right\}
\end{aligned}$$

et $\|z_x\|_F^2 \leq c_r n^2 h_0^{-1}$.

Démonstration. On applique les lemmes 5.4 et 5.3 à $v = v_r$ et x. On obtient

$$\|v_r \cdot z_x\|_W \leq n\sqrt{2} \|v_r \cdot y_x\|_W^2 \leq \sqrt{2} n^{n+3} \left(\frac{2}{\sqrt{3}}\right)^{2n(n-1)} \|v_r\|_W^2.$$

On remarque que si $v_r \cdot x \in \Omega$ alors (en regardant les deux dernières coordonnées de cet uplet) $\frac{(\det x)^2}{D}$ et $\frac{D}{(\det x)^2}$ sont des entiers positifs ; on en déduit $\det x = \pm D^{1/2}$ et donc $\det z_x = \pm D^{-1/2}$. On applique maintenant la proposition 4.2. Si $r = 0$, on en déduit l'existence d'une matrice M_0 telle que $v_0 \cdot z_x = v_0 \cdot M_0$ et

$$\|M_0^{-1}\|_F \leq c_0 n \|U^{-1}\|_F |\det z_x|^{-1/n} = c_0 n \|U^{-1}\|_F D^{1/2n}.$$

Soit $S_0 \in \mathrm{Iso}(v_0)$ tel que $z_x = S_0 M_0$. On rappelle que d'après le lemme 3.10, $\mathrm{Iso}(v_0)$ est stable par transposition. On écrit

$$\begin{aligned}
z_x &= x a_x^{-2} \\
&= (k_x a_x^{-1})(a_x^2 b_x a_x^{-2}) \text{ et donc} \\
k_x a_x^{-1} &= S_0 M_0 (a_x^2 b_x^{-1} a_x^{-2}).
\end{aligned}$$

D'autre part ${}^t(k_x a_x^{-1})^{-1} = x b_x^{-1}$ donc

$$x b_x^{-1} = {}^tS_0^{-1}\, {}^tM_0^{-1}(a_x^{-2}\, {}^tb_x a_x^2)$$

et donc

$$x = {}^tS_0^{-1}\, {}^tM_0^{-1}(a_x^{-2}\, {}^tb_x a_x^2) b_x.$$

On fait agir x sur v_0 ; on a $v_0 \cdot x = v_0 \cdot ({}^tM_0^{-1} a_x^{-2}\, {}^tb_x a_x^2 b_x)$. Notons

$$C_0 = {}^tM_0^{-1} a_x^{-2}\, {}^tb_x a_x^2 b_x.$$

On en déduit

$$\|v_0 \cdot x\|_W \leq \|v_0\|_W \sup\{\|C_0\|_F \|C_0^{-1}\|_F, \det(C_0)^2, \det(C_0)^{-2}\}$$

et, comme on l'a remarqué ci-dessus, puisque $v_0 \cdot C_0 \in \Omega$, $\det C_0 = \pm D^{1/2}$. De la même façon que dans la démonstration du lemme 5.3, les coefficients de la matrice $a_x^{-2}\, {}^tb_x a_x^2$ sont de la forme $(a_x^{-2}\, {}^tb_x a_x^2)_{ij} = \frac{a_{jj}^2}{a_{ii}^2} b_{ji}$ (pour $i \geq j$ et nuls autrement). Ils sont donc bornés en valeur absolue par $(\frac{4}{3})^{n-1}$. En majorant $\|b_x\|_F^2$ par n^2 on trouve alors

$$\begin{aligned}
\|C_0\|_F^2 &\leq \|M_0^{-1}\|_F^2 \|a_x^{-2}\, {}^tb_x a_x^2\|_F^2 \|b_x\|_F^2 \\
&\leq \|M_0^{-1}\|_F^2 n^4 \left(\frac{4}{3}\right)^{2(n-1)}
\end{aligned}$$

et de façon similaire (en utilisant le lemme 3.13)

$$\begin{aligned}
\|C_0^{-1}\|_F^2 &\leq \|b_x^{-1}\|_F^2 \|(a_x^{-2}\, {}^tb_x a_x^2)^{-1}\|_F^2 \|M_0\|_F^2 \\
&\leq n^{2n} \left(\frac{4}{3}\right)^{2(n-1)^2} \|M_0\|_F^2 \\
&\leq D^{-1} n^{n+2} \left(\frac{4}{3}\right)^{2(n-1)^2} \|M_0^{-1}\|_F^{2(n-1)}.
\end{aligned}$$

En combinant les deux dernières bornes on a

$$\|C_0^{-1}\|_F^2 \|C_0\|_F^2 \leq D^{-1} n^{n+6} \left(\frac{4}{3}\right)^{2n(n-1)} \|M_0^{-1}\|_F^{2n}$$

et finalement

$$\|v_0 \cdot x\|_W \leq \|v_0\|_W \sup\left\{ D^{-1/2} n^{\frac{n}{2}+3} \left(\frac{4}{3}\right)^{n(n-1)} \|M_0^{-1}\|_F^n, D \right\}.$$

Si $r \neq 0$ et $x \in \mathfrak{S}$ sont tels que $v_r \cdot x \in \Omega$, alors le lemme 5.4 et la proposition 4.2 nous permettent de déduire une borne pour z_x. On écrit comme au début de la preuve

$$x = {}^tz_x^{-1}(a_x^{-2}\, {}^tb_x a_x^2) b_x,$$

et on calcule comme ci-dessus des bornes pour $\|x\|_F$ et $\|x^{-1}\|_F$. On obtient

$$\|x\|_F \leq n^2 \left(\frac{4}{3}\right)^{n-1} \|z_x^{-1}\|_F \leq n^{3-\frac{n}{2}} \left(\frac{4}{3}\right)^{n-1} \|z_x\|_F^{n-1} D^{1/2}$$

et

$$\|x^{-1}\|_F \leq \|b_x^{-1}\|_F \|(a_x^{-2}\, {}^t\!b_x a_x^2)^{-1}\|_F \|z_x\|_F \leq n^n \left(\frac{4}{3}\right)^{(n-1)^2} \|z_x\|_F.$$

On en déduit

$$\begin{aligned}
&\|v_r \cdot x\|_W \leq \sup\{\|x\|_F\|x^{-1}\|_F, \|x\|_F^2, \det(x)^2, \det(x)^{-2}\}\|v_r\|_W \\
&\leq \|v_r\|_W \sup\left\{ n^{\frac{n}{2}+3}\left(\frac{4}{3}\right)^{n(n-1)} \|z_x\|_F^{\frac{n}{2}} D^{1/2}, n^{6-n}\left(\frac{4}{3}\right)^{2(n-1)} \|z_x\|_F^{2(n-1)} D, D \right\}
\end{aligned}$$

□

6 Conclusion

Pour conclure, on n'a plus qu'à réunir les résultats démontrés précédemment. Nous donnons un énoncé légèrement plus précis.

Théorème 6.1. *Soient A une variété abélienne sur un corps K et d un entier naturel non nul. Soient $\mathcal{L}_0$ une polarisation sur A et $h_0 = h^0(A, \mathcal{L}_0)$ la racine de son degré. On note P l'ensemble de classes de polarisations sur A de degré d pour l'action naturelle de* $\operatorname{Aut} A$. *Alors*

$$\operatorname{Card}(P) \leq n^{12n^6} D^{4n^5} h_0^{2n^6 g} d^{(2n-1)n^3}$$

où $g = \dim A$, $n = \operatorname{rg}(\operatorname{End}(A))$ et D est le discriminant de $\operatorname{End}(A)$.

Démonstration. On commence par reprendre les bornes trouvées dans la proposition 5.5 et en donner des nouvelles en fonction uniquement de n, D, h_0, g et d. Soient $r \in \mathcal{R} \cup \{0\}$, $v_r = w_r \cdot U^{-1}$ et $x \in \mathfrak{S}$ tels que $v_r \cdot x \in \Omega$. D'après le lemme 3.15,

$$\|v_0\|_W \leq \sup\left\{\frac{1}{2} n^{\frac{n+3}{2}} D^{1/2} h_0^{\frac{n-1}{2}}, D\right\} \leq \frac{1}{2} n^{\frac{n+3}{2}} D h_0^{\frac{n-1}{2}}.$$

Dans un premier temps, on remplace $\|v_0\|_W$ par la borne ci-dessus dans la borne pour c_0. On a

$$c_0 \leq 2^{-3/2}\left(\frac{4}{3}\right)^{n(n-1)} n^{2(n+3)} D^2 h_0^{n-1},$$

et on déduit

$$\begin{aligned}
\|M_0^{-1}\|_F &\leq c_0 n \|U^{-1}\|_F D^{1/2n} \\
&\leq 2^{-n-\frac{1}{2}}\left(\frac{4}{3}\right)^{n(n-1)} n^{\frac{n^2+5n+13}{2}} D^{\frac{n}{2}+1+\frac{1}{2n}} h_0^{\frac{(n^2-1)}{2}}.
\end{aligned}$$

On reprend la borne de la proposition 5.5 :

$$\|v_0 \cdot x\|_W \leq \|v_0\|_W \sup\left\{ D^{-1/2} n^{\frac{n}{2}+3}\left(\frac{4}{3}\right)^{n(n-1)} \|M_0^{-1}\|_F^{\frac{n}{2}}, D\right\},$$

puisque $n \geq 2$, on a $2^{-n-\frac{1}{2}} n^{\frac{n^2+5n+13}{2}} \geq 1$. On a donc

$$\begin{aligned}\|v_0 \cdot x\|_W \leq \|v_0\|_W D^{-1/2} n^{\frac{n}{2}+3} \left(\frac{4}{3}\right)^{n(n-1)} \\ \times \left(2^{-n-\frac{1}{2}} \left(\frac{4}{3}\right)^{n(n-1)} n^{\frac{n^2+5n+13}{2}} D^{\frac{n}{2}+\frac{1}{2n}+1} h_0^{\frac{(n^2-1)}{2}}\right)^n \\ \leq 2^{-n^2-\frac{n}{2}-1} \left(\frac{4}{3}\right)^{n(n^2-1)} n^{\frac{n^3+5n^2+15n+9}{2}} D^{\frac{n^2}{2}+n+1} h_0^{\frac{n^3-1}{2}}.\end{aligned}$$

Notons b_0 la borne qu'on vient de trouver et B_0 la boule de W de centre 0 et de rayon b_0. Regardons maintenant le cas où $r \neq 0$. D'après la proposition 5.5 on a

$$\|z_x\|_F^2 \leq 2^{1/2} n^{n+5} \left(\frac{4}{3}\right)^{n(n-1)} h_0^{-1} \|v_r\|_W^2$$

et donc

$$\|v_r \cdot x\|_F \leq \|v_r\|_W n^{n^2+3n+1} \left(\frac{4}{3}\right)^{(n-1)(n^2-n+2)} 2^{\frac{n-1}{2}} D \sup\{A, B, C\}$$

où

$$\begin{aligned}A &= h_0^{-\frac{n}{2}} \|v_r\|_W^n, \\ B &= h_0^{1-n} \|v_r\|_W^{2(n-1)} \\ C &= 1.\end{aligned}$$

Si on choisit une borne pour $\|v_r\|_W$ supérieure à $h_0^{1/2}$ qu'on remplace dans les termes ci-dessus, alors B l'emportera. D'après le lemme 3.15,

$$\|v_r\|_W \leq \sup\{\frac{1}{2} n^{\frac{n+3}{2}} D^{1/2} h_0^{\frac{n-1}{2}}, n^{1/2} h_0^g d^{1/2}, D\} \leq \frac{1}{2} n^{\frac{n+3}{2}} D h_0^{\frac{ng}{2}} d^{1/2},$$

et cette borne est supérieure à $h_0^{1/2}$ donc finalement

$$\|v_r \cdot x\|_F \leq n^{2n^2+\frac{11}{2}n-\frac{1}{2}} \left(\frac{4}{3}\right)^{n^3-2n^2+3n-2} 2^{\frac{1-3n}{2}} D^{2n} h_0^{1-n+(2n-1)\frac{ng}{2}} d^{n-\frac{1}{2}}.$$

Notons b_r la borne qu'on vient de trouver et $B_{\mathcal{R}}$ la boule de W de centre 0 et de rayon b_r (qui ne dépend pas du choix de $r \in \mathcal{R} \setminus \{0\}$). Dans ce qui précède nous avons donc démontré

$$\Omega \cap v_0 \cdot \mathfrak{S} \subset \Omega \cap B_0 \quad \text{et} \quad \bigcup_{r \in \mathcal{R}} (\Omega \cap v_r \cdot \mathfrak{S}) \subset \Omega \cap B_{\mathcal{R}}.$$

Puisque dans 3.12 on a trouvé une injection

$$\mathrm{Pol}_d(A) \longrightarrow (\Omega \cap w_0 \cdot U^{-1}\mathfrak{S}) \times \bigcup_{r \in \mathcal{R}} (\Omega \cap w_r \cdot U^{-1}\mathfrak{S})$$

on n'a plus qu'à majorer le cardinal des ensembles $\Omega \cap B_0$ et $\Omega \cap B_{\mathcal{R}}$. On utilisera l'estimation suivante : si B est une boule de W de centre 0 et de rayon b alors

$$|\Omega \cap B| \leq (2b+1)^{n^2(n+1)+2} \leq (3b)^{n^2+n+2}$$

et ainsi $\mathrm{Card}(P) \leq (9b_0 b_{\mathcal{R}})^{n^2+n+2}$. En utilisant $\frac{4}{3} \leq \sqrt{2}$ et $n \geq 2$, on a

$$\begin{aligned} 9b_0 b_{\mathcal{R}} &\leq 2^{7/2} b_0 b_{\mathcal{R}} \\ &\leq 2^{(n^2-1)(n-2)} n^{\frac{n^3+9n^2+26n+8}{2}} D^{\frac{n^2}{2}+3n+1} h_0^{\frac{n^3}{2}-n+\frac{1}{2}+\frac{n(2n-1)}{2}g} d^{n-\frac{1}{2}} \\ &\leq n^{\frac{3n^3+5n^2+24n+12}{2}} D^{\frac{n^2}{2}+3n+1} h_0^{\frac{n^3}{2}-n+\frac{1}{2}+\frac{n(2n-1)}{2}g} d^{n-\frac{1}{2}} \\ &\leq n^{\frac{13}{2}n^3} D^{\frac{9}{4}n^2} h_0^{n^3 g} d^{n-\frac{1}{2}}. \end{aligned}$$

On utilise ensuite $n^3 + n^2 + 2 \leq \frac{7}{4}n^3$ et on a

$$\mathrm{Card}(P) \leq n^{12n^6} D^{4n^5} h_0^{2n^6 g} d^{(2n-1)n^3}.$$

□

On en déduit immédiatement la borne donnée dans l'introduction

$$\mathrm{Card}(P) \leq (n^6 D h_0^g d)^{2n^6}.$$

Le théorème 1.3 se déduit facilement de ce résultat et des résultats de É. Gaudron et G. Rémond. Nous donnons un énoncé plus précis que celui donné dans l'introduction.

Théorème 6.2. *Soient A une variété abélienne de dimension g sur un corps de nombres K et d un entier naturel non nul. Soit P l'ensemble de classes de polarisations sur A de degré d pour l'action naturelle de* $\mathrm{Aut}\, A$. *Alors*

$$\mathrm{Card}(P) \leq 7^{5394g^{17}} g^{5168g^{17}} \left([K:\mathbb{Q}] \max(1, \log[K:\mathbb{Q}], h_F(A))\right)^{640g^{15}} d^{(2n-1)n^3}.$$

Démonstration. Dans [7] les auteurs donnent une majoration plutôt pour $\mathrm{vol}(\mathrm{End}(A))$ en fonction de $\Xi(A) = \Big((7g)^{8g^2}[K:\mathbb{Q}] \max(1, \log[K:\mathbb{Q}], h_F(A)\Big)^{2g^2}$. Pour obtenir une majoration de D on peut par exemple utiliser le lemme 2.10 de [14] où l'auteur montre que $g^{-n}D \leq \mathrm{vol}(\mathrm{End} A)^2 \leq (2g)^n D$. Notons $\xi(A) = [K:\mathbb{Q}] \max(1, \log[K:\mathbb{Q}], h_F(A))$. On remplace D et h_0 dans le théorème ci-dessus, on utilise la borne $n \leq 2g^2$ et on obtient

$$\begin{aligned} \mathrm{Card}(P) &\leq n^{12n^6} (g^n \Xi(A)^g)^{4n^5} (\frac{1}{g!}\Xi(A)^{3/2})^{2n^6 g} d^{(2n-1)n^3} \\ &\leq 2^{12n^6} 7^{80n^6 g^5} g^{80n^6 g^5 + 24n^6} \xi^{10n^6 g^3} d^{(2n-1)n^3} \\ &\leq 7^{274g^{12}+5120g^{17}} g^{5120g^{17}+48g^{17}} \xi^{640g^{15}} d^{(2n-1)n^3} \\ &\leq 7^{5394g^{17}} g^{5168g^{17}} \xi(A)^{640g^{15}} d^{(2n-1)n^3}. \end{aligned}$$

□

On en déduit facilement la borne anoncée dans l'introduction

$$\mathrm{Card}(P) \leq \left((7g)^9 \xi(A)\right)^{640g^{17}} d^{32g^8}.$$

Références

[1] Armand Borel. *Introduction aux groupes arithmétiques*. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris, 1969.

[2] Armand Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75 :485–535, 1962.

[3] Nicolas Bourbaki. *Integration. II. Chapters 7–9*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2004. Translated from the 1963 and 1969 French originals by Sterling K. Berberian.

[4] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[5] Douglas R. Farenick and Barbara A. F. Pidkowich. The spectral theorem in quaternions. *Linear Algebra Appl.*, 371 :75–102, 2003.

[6] Éric Gaudron and Gaël Rémond. Polarisations et isogénies. *Duke Math. J.*, 163(11) :2057–2108, 2014.

[7] Éric Gaudron and Gaël Rémond. Nouveaux théorèmes d'isogénie. *À paraître*, 2020.

[8] Tsuyoshi Hayashida. A class number associated with a product of two elliptic curves. *Natur. Sci. Rep. Ochanomizu Univ.*, 16 :9–19, 1965.

[9] Tsuyoshi Hayashida. A class number associated with the product of an elliptic curve with itself. *J. Math. Soc. Japan*, 20 :26–43, 1968.

[10] Herbert Lange. Abelian varieties with several principal polarizations. *Duke Math. J.*, 55(3) :617–628, 1987.

[11] Herbert Lange. Principal polarizations on products of elliptic curves. In *The geometry of Riemann surfaces and abelian varieties*, volume 397 of *Contemp. Math.*, pages 153–162. Amer. Math. Soc., Providence, RI, 2006.

[12] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay ; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[13] M. S. Narasimhan and M. V. Nori. Polarisations on an abelian variety. *Proc. Indian Acad. Sci. Math. Sci.*, 90(2) :125–128, 1981.

[14] Gaël Rémond. Conjectures uniformes sur les variétés abéliennes. *Q. J. Math.*, 69(2) :459–486, 2018.

[15] V. Rotger. Quaternions, polarization and class numbers. *J. Reine Angew. Math.*, 561 :177–197, 2003.

[16] Fuzhen Zhang. Quaternions and matrices of quaternions. *Linear Algebra Appl.*, 251 :21–57, 1997.