

Hauteurs de sous-espaces sur les corps non commutatifs

Christine Liebendörfer · Gaël Rémond

Received: 25 May 2005 / Accepted: 26 June 2006 /
Published online: 31 August 2006
© Springer-Verlag 2006

Abstract We study heights of subspaces of D^N where D is a finite-dimensional rational division algebra and N a positive integer. We define them in terms of volumes of Euclidean lattices by extending a formula of W. Schmidt so that we recover the classical height if D is commutative. We review basic properties, prove a Siegel Lemma over D , a duality theorem and a new formula for the degree of certain abelian varieties. We further give matrix versions and compare our notion with the height defined through algebraic groups by J. Franke, Y. Manin and Y. Tschinkel.

Mots-Clefs Hauteurs · Corps non commutatifs · Lemme de Siegel · Variétés abéliennes

Mathematics Subject Classification 11G50 · 11R52 · 11G10

0 Introduction

Un corps de nombres K et un entier N étant donnés, il est aujourd’hui classique de munir tout sous-espace vectoriel V de K^N d’une hauteur $H(V)$. Cet article a pour thème l’extension de ce procédé à un corps non commutatif D de dimension finie sur \mathbb{Q} . Nous explorons les différentes définitions possibles et donnons deux applications : l’une concerne un lemme de Siegel sur D , l’autre le degré des variétés abéliennes.

Dans le cas commutatif, la façon la plus naturelle de définir $H(V)$ transite par la grassmannienne : celle-ci est une variété projective sur K munie du plongement de

C. Liebendörfer (✉)

Institut de Mathématiques B, École Polytechnique Fédérale de Lausanne (EPFL),
1015 Lausanne, Switzerland
e-mail: Christine.Liebendoerfer@epfl.ch

G. Rémond

Institut Fourier, UMR 5582, BP 74, 38402 Saint-Martin-d’Hères Cedex, France
e-mail: Gael.Remond@ujf-grenoble.fr

Plücker dans un espace projectif donc d’une hauteur canonique ; autrement dit, $H(V)$ est la hauteur des coordonnées grassmanniennes de V . Cette approche ne se transpose pas immédiatement à D : il n’y a pas de coordonnées grassmanniennes. En revanche, il est possible de voir la grassmannienne sur D comme une variété projective sur un corps de nombres (par exemple le centre de D ou même \mathbb{Q}), à savoir une variété de drapeaux généralisée. J. Franke, Y. Manin et Y. Tschinkel ont décrit des hauteurs sur ces variétés dépendant de choix adéliques. Nous ferons le lien avec cette approche mais nous préférons nous baser sur une définition plus élémentaire.

Nous nous inspirons d’une formule de W. Schmidt de 1967 pour donner une définition à la fois très simple et très générale en termes de volume de réseaux euclidiens. Celle-ci suffit pour établir les propriétés de base de la hauteur et même un lemme de Siegel. Au-delà, nous écrirons la hauteur en termes matriciels, en particulier pour faire apparaître une décomposition en produit de facteurs locaux.

Toute notre démarche généralise celle de [6–9]. Ces articles traitent du cas des quaternions sur \mathbb{Q} mais contiennent déjà la plupart des idées mises en œuvre ci-après. Ils fournissent en outre des exemples (ou contre-exemples) concrets.

Dans tout l’article, D sera donc un corps de dimension finie sur \mathbb{Q} (autrement dit une algèbre à division selon la terminologie de certains auteurs). Signalons qu’à plusieurs reprises existera le choix de voir D comme une extension soit de son centre soit de \mathbb{Q} . Nous avons toujours privilégié la seconde possibilité afin de voir le cas des corps de nombres apparaître comme cas particulier de la théorie plutôt que comme prérequis.

1 Définition

Nous basons notre approche sur la notion de volume d’un réseau euclidien. Rappelons-la brièvement : si Λ est un \mathbb{Z} -module libre de rang fini tel que $\Lambda \otimes \mathbb{R}$ est muni d’une structure d’espace euclidien, nous notons $\text{vol}(\Lambda)$ le volume d’un domaine fondamental du réseau Λ dans $\Lambda \otimes \mathbb{R}$. De manière équivalente, il s’agit du volume de $(\Lambda \otimes \mathbb{R})/\Lambda$ et, si $\lambda_1, \dots, \lambda_n$ est une base de Λ , il se calcule par la formule

$$\text{vol}(\Lambda)^2 = \det(\langle \lambda_i, \lambda_j \rangle)_{1 \leq i, j \leq n}$$

où $\langle \cdot, \cdot \rangle$ désigne le produit scalaire sur $\Lambda \otimes \mathbb{R}$.

Nous appelons réseau d’un espace vectoriel E sur \mathbb{Q} un sous-groupe abélien libre Λ de E tel que $\Lambda \otimes \mathbb{Q} = E$. Voici notre définition de hauteur.

Définition 1.1 *Soient D un corps de dimension finie sur \mathbb{Q} , Λ un réseau de D et $|\cdot|$ une norme euclidienne sur $D \otimes \mathbb{R}$. Pour tout entier naturel N et tout sous-espace vectoriel V à gauche ou à droite sur D de D^N , la hauteur de V relativement à Λ et $|\cdot|$ est*

$$H^{\Lambda, |\cdot|}(V) = \left(\frac{\text{vol}(V \cap \Lambda^N)}{\text{vol}(\Lambda)^{\dim V}} \right)^{1/[D:\mathbb{Q}]}$$

Il est entendu qu’ici la dimension de V est sur D et que $|\cdot|$ induit une norme euclidienne $|\cdot|_N$ sur $(D \otimes \mathbb{R})^N$ (par $|(x_1, \dots, x_N)|_N^2 = \sum_{i=1}^N |x_i|^2$) qui donne un sens à $\text{vol}(V \cap \Lambda^N)$. Notons aussi que la définition s’interprète naturellement en des termes arakeloviens : nous avons muni le corps D d’un modèle formé d’une structure entière

Λ et d'une métrique à l'infini $|\cdot|$; en nous limitant à des sous-espaces de D^N , nous avons forcé l'extension du modèle à V .

Remarquons encore que la définition s'exprime uniquement en termes d'espaces vectoriels sur \mathbb{Q} : quitte à écrire $\dim_{\mathbb{Q}} V/[D : \mathbb{Q}]$ au lieu de $\dim V$, nous aurions pu supposer simplement que V est un sous-espace de D^N sur \mathbb{Q} (et, si l'on veut, D lui-même pourrait n'être qu'un \mathbb{Q} -espace vectoriel). Ceci explique que certains résultats généraux sur la hauteur s'obtiendront uniquement en travaillant sur \mathbb{Q} ; les énoncés intéressants apparaîtront lorsqu'entrera en jeu la structure supplémentaire sur D .

Avant de recenser les propriétés de base de cette hauteur (voir partie suivante), nous discutons du choix du couple $(\Lambda, |\cdot|)$. Nous nous intéressons particulièrement aux cas où ce couple présente une certaine compatibilité avec la structure de corps de D . De manière précise, nous considérons les restrictions possibles suivantes :

- Λ est un ordre de D ,
- Λ est un ordre maximal de D ,
- il existe une anti-involution $\iota : D \otimes \mathbb{R} \rightarrow D \otimes \mathbb{R}$ telle que $|x|^2 = \text{Tr}(\iota(x)x)$ pour tout $x \in D \otimes \mathbb{R}$.

Rappelons qu'un ordre de D est un réseau de D qui est simultanément un sous-anneau de D . La maximalité se comprend au sens de l'inclusion. Nous appelons anti-involution un \mathbb{R} -automorphisme ι tel que $\iota(xy) = \iota(y)\iota(x)$ et $\iota(\iota(x)) = x$ pour $x, y \in D \otimes \mathbb{R}$. La trace $\text{Tr}(x)$ d'un élément $x \in D \otimes \mathbb{R}$ est celle de l'endomorphisme $y \mapsto xy$ de $D \otimes \mathbb{R}$. L'anti-involution ι est dite positive lorsque la forme quadratique $x \mapsto \text{Tr}(\iota(x)x)$ est définie positive.

Lorsque la norme $|\cdot|$ provient d'une anti-involution ι nous noterons aussi $H^{\Lambda, \iota}$ pour $H^{\Lambda, |\cdot|}$.

Nous pouvons remarquer que pour tout D il existe des ordres, au moins un ordre maximal (tout ordre est même inclus dans un ordre maximal, voir [12, (10.4) p. 127]) et au moins une involution positive sur $D \otimes \mathbb{R}$ (voir plus bas). En revanche, il n'est pas en général possible de trouver une anti-involution $D \rightarrow D$ (sur \mathbb{Q}) dont l'extension à \mathbb{R} est positive (par exemple pour un corps de nombres de degré 3). Notons quand même que c'est le cas dans l'exemple important où $D = \text{End}(X) \otimes \mathbb{Q}$ pour une variété abélienne simple X .

Ainsi il semble que la meilleure façon de choisir une hauteur sur D soit de fixer un ordre maximal \mathcal{O} de D ainsi qu'une involution positive ι sur $D \otimes \mathbb{R}$ et de considérer $H^{\mathcal{O}, \iota}$. Cette impression se verra confirmée par nos résultats (extensions, variétés abéliennes, écriture de facteurs locaux, dualité) mais il serait dommage de se limiter dès le départ à cette situation. Par exemple le cadre plus large réseau-norme par rapport à ordre-involution permet de traiter simultanément le problème des extensions et celui des variétés abéliennes ; de plus, pour une variété abélienne X , il est assez naturel de considérer l'ordre non nécessairement maximal $\text{End}(X)$.

Nous pouvons maintenant examiner le cas particulier des corps de nombres, c'est-à-dire celui où D est commutatif. Notons plutôt $K = D$. Au regard de la discussion précédente, les corps commutatifs possèdent deux propriétés merveilleuses :

- K admet un unique ordre maximal, à savoir l'anneau des entiers \mathcal{O}_K ,
- il existe une unique (anti-)involution positive sur $K \otimes \mathbb{R} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, à savoir l'application $(x_i, z_j) \mapsto (x_i, \bar{z}_j)$.

Notons que la première condition caractérise les corps de nombres tandis qu'ils partagent la seconde avec les algèbres de quaternions définies positives sur les corps

de nombres totalement réels (pour lesquelles $D \otimes \mathbb{R} \simeq \mathbb{H}^r$ où \mathbb{H} est le corps des quaternions de Hamilton ; c'est le cas, avec $r = 1$, dans [6–9]) à l'exclusion de tout autre corps (voir lemme ci-dessous).

Quoi qu'il en soit, il y a donc un choix canonique pour la hauteur sur un corps de nombres. La formule de W. Schmidt (voir [13], théorème 1) montre que l'on retrouve la notion usuelle de hauteur de V définie à l'aide de ses coordonnées grassmanniennes.

Nous rappelons maintenant pourquoi $D \otimes \mathbb{R}$ admet toujours une involution positive en donnant une description de toutes celles-ci. Pour un anneau R nous notons $\text{Mat}_{mn}(R)$ l'anneau des matrices sur R avec $m \geq 1$ lignes et $n \geq 1$ colonnes.

Si \mathbb{K} est l'un des trois corps \mathbb{R}, \mathbb{C} ou \mathbb{H} , nous appelons conjugaison l'unique anti-involution positive sur \mathbb{K} (c'est l'identité sur \mathbb{R} , la conjugaison usuelle sur \mathbb{C} tandis que sur $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, avec $i^2 = j^2 = k^2 = ijk = -1$, le conjugué de $\alpha + \beta i + \gamma j + \delta k$ est $\alpha - \beta i - \gamma j - \delta k$; noter que, dans les trois cas, les points fixes de l'involution sont les réels). Pour tout entier $n \geq 1$, elle induit une involution $M \mapsto {}^t\bar{M}$ sur $\text{Mat}_{nn}(\mathbb{K})$ que nous nommons transconjugaison. Une matrice carrée M sur \mathbb{K} sera ici dite hermitienne si ${}^t\bar{M} = M$. Si $M \in \text{Mat}_{nn}(\mathbb{K})$ est hermitienne, ${}^t\bar{X}MX$ est un nombre réel pour tout $X \in \text{Mat}_{n1}(\mathbb{K})$. Lorsque ${}^t\bar{X}MX > 0$ pour tout tel X non nul, M est dite définie positive.

Lemme 1.1 *Soit D un corps de dimension finie sur \mathbb{Q} . Il existe quatre entiers naturels d, r_1, r_2 et r_3 soumis aux conditions $d \geq 1$ et d pair si $r_3 \neq 0$ de sorte que l'on ait un isomorphisme de \mathbb{R} -algèbres*

$$D \otimes \mathbb{R} \simeq \text{Mat}_{dd}(\mathbb{R})^{r_1} \times \text{Mat}_{dd}(\mathbb{C})^{r_2} \times \text{Mat}_{d/2,d/2}(\mathbb{H})^{r_3}.$$

Dans cette écriture, une anti-involution ι est positive si et seulement s'il existe des matrices hermitiennes définies positives A_1, \dots, A_f (où $f = r_1 + r_2 + r_3$) telles que

$$\iota(M_1, \dots, M_f) = (A_1 {}^t\bar{M}_1 A_1^{-1}, \dots, A_f {}^t\bar{M}_f A_f^{-1}).$$

En particulier, si ι positive est fixée, on peut choisir l'isomorphisme de sorte que ι soit donnée par la transconjugaison sur chaque facteur.

Démonstration: Par semi-simplicité de $D \otimes \mathbb{R}$, cette algèbre s'écrit comme produit d'anneaux de matrices sur \mathbb{R}, \mathbb{C} et \mathbb{H} . D'autre part, si Z est le centre de D , nous avons un isomorphisme $D \otimes_Z \mathbb{C} \simeq \text{Mat}_{dd}(\mathbb{C})$. Par suite, en notant $e = [Z : \mathbb{Q}]$, il vient $D \otimes_{\mathbb{Q}} \mathbb{C} \simeq \text{Mat}_{dd}(\mathbb{C})^e$ (puisque $Z \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C}^e$). Ceci montre que le produit de matrices est bien de la forme annoncée en vertu des isomorphismes

$$\text{Mat}_{nn}(\mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} \simeq \text{Mat}_{nn}(\mathbb{C}), \quad \text{Mat}_{nn}(\mathbb{C}) \otimes_{\mathbb{R}} \mathbb{C} \simeq \text{Mat}_{nn}(\mathbb{C})^2$$

$$\text{et} \quad \text{Mat}_{nn}(\mathbb{H}) \otimes_{\mathbb{R}} \mathbb{C} \simeq \text{Mat}_{2n,2n}(\mathbb{C}).$$

On peut noter qu'alors $e = r_1 + 2r_2 + r_3$.

Ensuite, si ι est une anti-involution, sa composée avec la transconjugaison est un automorphisme de $D \otimes \mathbb{R}$ qui est intérieur par le théorème de Skolem-Noether. Ceci donne l'existence des matrices A_i (données chacune à multiplication par une matrice centrale près). Notons $\mathbb{K}_i \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$ le corps sur lequel est définie A_i . La relation $\iota \circ \iota = \text{id}$ montre que $A_i {}^t\bar{A}_i^{-1}$ est centrale donc $A_i = \lambda_i {}^t\bar{A}_i$ où λ_i appartient au centre de \mathbb{K}_i . En appliquant la transconjugaison, on a ${}^t\bar{A}_i = \bar{\lambda}_i A_i$ donc $\lambda_i \bar{\lambda}_i = 1$. Si $\mathbb{K}_i = \mathbb{C}$, on choisit μ_i avec $\mu_i^2 = \lambda_i$ et l'on remplace A_i par $\mu_i^{-1} A_i$ pour avoir $A_i = {}^t\bar{A}_i$. Si $\mathbb{K}_i = \mathbb{R}$

ou \mathbb{H} on a $A_i = \pm {}^t \bar{A}_i$. Si ι est positive, nous savons que pour toute matrice M sur \mathbb{K}_i non nulle (de même taille que A_i) on a $\text{Tr}(A_i {}^t M A_i^{-1} M) > 0$. En choisissant $M = A_i M'$ où M' est une matrice dont seule la première colonne (notée X) est non nulle, il vient $\text{Tr}(a_{11} \cdot {}^t \bar{X} {}^t A_i X) > 0$ où a_{11} est le coefficient d'indice $(1, 1)$ de A_i . En particulier, nous devons avoir $a_{11} \neq 0$. Si $\mathbb{K}_i = \mathbb{R}$ la matrice A_i n'est donc pas antisymétrique donc $A_i = {}^t \bar{A}_i$. Dans le cas $\mathbb{K}_i = \mathbb{H}$, la relation $A_i = -{}^t \bar{A}_i$ entraînerait $a_{11} = -\bar{a}_{11}$ donc l'existence de $z \in \mathbb{H} \setminus \{0\}$ avec $z a_{11} = -\bar{a}_{11} z$ (si $a_{11} = \beta i + \gamma j + \delta k$ choisir $z = \beta' i + \gamma' j + \delta' k$ avec $\beta\beta' + \gamma\gamma' + \delta\delta' = 0$) ; mais alors ${}^t X = (z \ 0 \ \dots \ 0)$ donnerait $\text{Tr}(a_{11} {}^t \bar{X} {}^t A_i X) = \text{Tr}(a_{11} \bar{z} a_{11} z) = \text{Tr}(z a_{11} \bar{a}_{11} z) = -\text{Tr}(z a_{11} \bar{z} a_{11}) < 0$ en contradiction avec notre hypothèse. Ainsi dans tous les cas A_i est hermitienne donc $a_{11} \in \mathbb{R}$ et, quitte à remplacer A_i par $-A_i$ si nécessaire, nous supposons $a_{11} > 0$. L'inégalité $\text{Tr}(a_{11} \cdot {}^t \bar{X} {}^t A_i X) > 0$ devient alors ${}^t \bar{X} A_i X > 0$, ce qui montre bien que A_i est définie positive.

Réciproquement, il s'agit de vérifier que si les matrices A_i sont définies positives alors la formule de l'énoncé donne bien une anti-involution positive. Pour cela, nous écrivons $A_i = B_i {}^t \bar{B}_i$ pour certaines matrices B_i : il s'agit simplement de décomposer en somme de carrés la forme hermitienne donnée par A_i ; concrètement si ${}^t \bar{X} A_i X = \sum_{i,j} \bar{x}_i a_{ij} x_j$ (où $\bar{a}_{ij} = a_{ji}$), l'on pose $y_1 = a_{11}^{-1/2} \sum_j a_{1j} x_j$ de sorte que $\sum_{i,j} \bar{x}_i a_{ij} x_j - \bar{y}_1 y_1$ ne fait plus intervenir que x_2, x_3, \dots et l'on recommence.

Nous pouvons alors composer l'isomorphisme initial avec le produit des changements de base donnés par les B_i . De la sorte, l'application définie par les A_i est maintenant donnée par la transconjugaison sur chaque facteur. C'est donc clairement une anti-involution positive. Au passage, nous avons également établi la dernière assertion. □

Remarquons ici que ce lemme montre que pour toute anti-involution ι sur $D \otimes \mathbb{R}$ nous avons $\text{Tr}(\iota(x)) = \text{Tr}(x)$ pour $x \in D \otimes \mathbb{R}$ (ceci vaut en fait plus généralement pour toute anti-involution sur une algèbre semi-simple et séparable sur un corps) et, en particulier, le produit scalaire associé à la norme provenant de ι est donné par $\langle x, y \rangle = \text{Tr}(\iota(xy))$ pour $x, y \in D \otimes \mathbb{R}$.

Les deux parties suivantes n'utilisent que la définition pour un couple général $(\Lambda, |\cdot|)$; à partir de la partie 4, nous verrons intervenir des couples formés d'un ordre maximal et d'une anti-involution positive ; enfin, dans la partie 6 et les suivantes, nous utiliserons une écriture matricelle de la hauteur.

2 Propriétés

Soient E un espace vectoriel sur \mathbb{Q} de dimension finie et Λ et Λ' deux réseaux de E . Si $\Lambda' \subset \Lambda$, l'indice $[\Lambda : \Lambda']$ est défini comme le cardinal du quotient Λ/Λ' . En général, nous étendons cette notation de la manière suivante : $\Lambda \cap \Lambda'$ est un réseau de E et nous posons $[\Lambda : \Lambda'] = [\Lambda : \Lambda \cap \Lambda'] / [\Lambda' : \Lambda \cap \Lambda']$. Ce nouvel « indice » est un élément de $\mathbb{Q}_{>0}$. Les propriétés naturelles de l'indice s'étendent sans peine. Par exemple, si Λ'' est un troisième réseau, nous avons la relation $[\Lambda : \Lambda'] [\Lambda' : \Lambda''] = [\Lambda : \Lambda'']$. Si de plus $E \otimes \mathbb{R}$ est muni d'une norme euclidienne, on a $\text{vol}(\Lambda') = [\Lambda : \Lambda'] \text{vol}(\Lambda)$.

Commençons par quelques résultats élémentaires de stabilité de la hauteur.

Lemme 2.1 *Soient $D, \Lambda, |\cdot|$ et N comme dans la définition.*

- (1) *La hauteur $H^{\Lambda, |\cdot|}$ est stable par permutation des coordonnées de D^N .*
- (2) *Si $V \subset D^M \times \{0\}^{N-M}$, il revient au même de calculer $H^{\Lambda, |\cdot|}(V)$ dans D^M ou D^N .*

- (3) Si V est un sous-espace \ll standard \gg de D^N (engendré par une partie de la base canonique) $H^{\Lambda,|\cdot|}(V) = 1$.
- (4) Si $x \in D \setminus \{0\}$ et $\mu \in \mathbb{R}_{>0}$ on a $H^{x\Lambda,\mu|\cdot|}(V) = H^{\Lambda,|\cdot|}(V)$ si V est un sous-espace à gauche et $H^{\Lambda x,\mu|\cdot|}(V) = H^{\Lambda,|\cdot|}(V)$ si V est un sous-espace à droite.

Démonstration: (1) est clair car une telle permutation laisse stable Λ^N et induit une isométrie sur $(D \otimes \mathbb{R})^N$. (2) est évident et (3) en découle avec (1) et $H^{\Lambda,|\cdot|}(D^N) = 1$. Dans (4), le réel μ disparaît immédiatement des formules. Ensuite nous pouvons écrire (pour V espace à gauche)

$$\text{vol}(x\Lambda) = [\Lambda : x\Lambda]\text{vol}(\Lambda) \quad \text{et}$$

$$\text{vol}(V \cap (x\Lambda)^N) = [V \cap \Lambda^N : V \cap (x\Lambda)^N]\text{vol}(V \cap \Lambda^N).$$

Ici $V \cap (x\Lambda)^N = x(V \cap \Lambda^N)$. Puisque V est un espace vectoriel sur D , il contient un réseau Λ_V isomorphe à $\Lambda^{\dim V}$. Alors nous avons

$$\begin{aligned} [\Lambda_V : x(V \cap \Lambda^N)] &= [\Lambda_V : x\Lambda_V][x\Lambda_V : x(V \cap \Lambda^N)] \\ &= [\Lambda_V : V \cap \Lambda^N][V \cap \Lambda^N : x(V \cap \Lambda^N)]. \end{aligned}$$

Maintenant les indices $[x\Lambda_V : x(V \cap \Lambda^N)]$ et $[\Lambda_V : V \cap \Lambda^N]$ coïncident car la multiplication par x est un automorphisme de V . Comme d'autre part $[\Lambda_V : x\Lambda_V] = [\Lambda : x\Lambda]^{\dim V}$ nous avons $[V \cap \Lambda^N : x(V \cap \Lambda^N)] = [\Lambda : x\Lambda]^{\dim V}$ d'où $H^{x\Lambda,|\cdot|}(V) = H^{\Lambda,|\cdot|}(V)$. Bien entendu, le cas où V est un espace à droite se traite de manière identique. \square

Nous examinons à présent la variation de la hauteur avec le couple $(\Lambda, |\cdot|)$.

Lemme 2.2 Soient $D, \Lambda, |\cdot|, N$ et V comme dans la définition. Soient Λ' un réseau de D et $|\cdot|'$ une norme euclidienne sur $D \otimes \mathbb{R}$. Alors

$$\frac{H^{\Lambda,|\cdot|}(V)}{H^{\Lambda',|\cdot|'}(V)} \leq \left(\max \{ [\Lambda : \Lambda \cap \Lambda'], [\Lambda' : \Lambda \cap \Lambda'] \} \left(\sup_{x,y \in D \setminus \{0\}} \frac{|x||y|'}{|x'| |y|} \right) \right)^{\dim V}.$$

Démonstration: Notons $\lambda = [\Lambda : \Lambda \cap \Lambda']$, $\lambda' = [\Lambda' : \Lambda \cap \Lambda']$, $\omega = \sup_{x \in D \setminus \{0\}} |x|/|x'|$ et $\omega' = \sup_{x \in D \setminus \{0\}} |x'|/|x|$. Clairement, il suffit de traiter séparément les deux cas particuliers où $\Lambda' = \Lambda$ ou bien $|\cdot|' = |\cdot|$. Par densité de D dans $D \otimes \mathbb{R}$ nous avons $\omega^{-1}|x'| \leq |x| \leq \omega|x|'$ pour tout $x \in D \otimes \mathbb{R}$ et la même formule vaut pour les normes sur $(D \otimes \mathbb{R})^N$. Par conséquent, pour un réseau M de rang r , il vient $\omega'^{-r} \text{vol}'(M) \leq \text{vol}(M) \leq \omega^r \text{vol}'(M)$. Ceci entraîne $\text{vol}(V \cap \Lambda^N) \leq \omega^{[D:\mathbb{Q}]\dim V} \text{vol}'(V \cap \Lambda^N)$ ainsi que $\text{vol}'(V) \leq \omega'^{[D:\mathbb{Q}]\dim V} \text{vol}(\Lambda)$ d'où, par quotient,

$$H^{\Lambda,|\cdot|}(V) \leq (\omega\omega')^{\dim V} H^{\Lambda',|\cdot|'}(V)$$

qui est la relation cherchée pour $\Lambda = \Lambda'$. D'un autre côté, nous avons

$$\frac{\text{vol}(\Lambda)}{\text{vol}(\Lambda')} = [\Lambda' : \Lambda] = \frac{\lambda'}{\lambda}.$$

De plus, comme $\lambda\Lambda \subset \Lambda \cap \Lambda' \subset \Lambda'$, nous pouvons écrire

$$\text{vol}(V \cap (\Lambda')^N) \leq \text{vol}(V \cap (\lambda\Lambda)^N) = \lambda^{[D:\mathbb{Q}]\dim V} \text{vol}(V \cap \Lambda^N)$$

et donc avec la relation précédente

$$\frac{\text{vol}(V \cap (\Lambda')^N)}{\text{vol}(\Lambda')^{\dim V}} \leq \lambda^{([D:\mathbb{Q}]-1)\dim V} \lambda'^{\dim V} \frac{\text{vol}(V \cap \Lambda^N)}{\text{vol}(\Lambda)^{\dim V}}$$

puis

$$H^{\Lambda', |\cdot|}(V) \leq \max(\lambda, \lambda')^{\dim V} H^{\Lambda, |\cdot|}(V)$$

qui donne le résultat. □

En pratique, pour comparer efficacement deux couples, on peut combiner ce résultat avec l’assertion (4) du lemme précédent.

La hauteur introduite satisfait une propriété de finitude.

Lemme 2.3 *Soient $D, \Lambda, |\cdot|$ et N comme dans la définition. Pour tout réel H l’ensemble des sous-espaces V de D^N vérifiant $H^{\Lambda, |\cdot|}(V) \leq H$ est fini.*

Démonstration: En écrivant la majoration $\text{vol}(V \cap \Lambda^N) \leq H^{[D:\mathbb{Q}]} \text{vol}(\Lambda)^{\dim V}$ et en remarquant $V = \mathbb{Q}(V \cap \Lambda^N)$, il nous suffit de montrer qu’il n’y a qu’un nombre fini de sous-groupes de Λ^N de volume borné. Maintenant, ceci est une conséquence tout à fait classique du second théorème de Minkowski. □

Nous pouvons étendre un résultat de W. Schmidt (voir [14]).

Lemme 2.4 *Soient $D, \Lambda, |\cdot|$ et N comme dans la définition. Si V et W sont deux sous-espaces de D^N alors $H^{\Lambda, |\cdot|}(V + W)H^{\Lambda, |\cdot|}(V \cap W) \leq H^{\Lambda, |\cdot|}(V)H^{\Lambda, |\cdot|}(W)$.*

Démonstration: La formule à montrer équivaut à

$$\text{vol}((V + W) \cap \Lambda^N) \text{vol}(V \cap W \cap \Lambda^N) \leq \text{vol}(V \cap \Lambda^N) \text{vol}(W \cap \Lambda^N)$$

ou encore si l’on choisit une décomposition en somme directe $V = (V \cap W) \oplus F$ à

$$\begin{aligned} \text{vol}((V + W) \cap \Lambda^N) \text{vol}(V \cap W \cap \Lambda^N) \text{vol}(F \cap \Lambda^N) \\ \leq \text{vol}(V \cap \Lambda^N) \text{vol}(W \cap \Lambda^N) \text{vol}(F \cap \Lambda^N) \end{aligned}$$

qui se réécrit

$$\begin{aligned} \text{vol}((V + W) \cap \Lambda^N) \text{vol}(V \cap W \cap \Lambda^N \oplus F \cap \Lambda^N) \\ \leq \text{vol}(V \cap \Lambda^N) \text{vol}(W \cap \Lambda^N \oplus F \cap \Lambda^N). \end{aligned}$$

En termes d’indices cela devient exactement

$$[V \cap \Lambda^N : V \cap W \cap \Lambda^N \oplus F \cap \Lambda^N] \leq [(V + W) \cap \Lambda^N : W \cap \Lambda^N \oplus F \cap \Lambda^N].$$

Notons $\Lambda_1 = (V + W) \cap \Lambda^N$ et $\Lambda_2 = W \cap \Lambda^N \oplus F \cap \Lambda^N$. Nous remarquons $\Lambda_1 \cap V = V \cap \Lambda^N$ et $\Lambda_2 \cap V = V \cap W \cap \Lambda^N \oplus F \cap \Lambda^N$ (si $x \in \Lambda_2 \cap V$ on a $x = y + z$ avec $y \in W \cap \Lambda^N$ et $z \in F \cap \Lambda^N \subset V$ donc $x - z = y \in V$ puis $y \in V \cap W \cap \Lambda^N$). La formule que nous voulons établir est donc

$$[V \cap \Lambda_1 : V \cap \Lambda_2] \leq [\Lambda_1 : \Lambda_2]$$

qui découle clairement de l’injection $V \cap \Lambda_1 / V \cap \Lambda_2 \hookrightarrow \Lambda_1 / \Lambda_2$. □

3 Lemme de Siegel

Pour toute cette partie, nous notons $n = [D : \mathbb{Q}]$. De plus, si m est un entier naturel, τ_m désigne la racine m -ième du volume (par rapport à la norme euclidienne usuelle) de la boule unité dans \mathbb{R}^m .

Théorème 3.1 Soient L, N des entiers naturels tels que $0 < L < N$, soient Λ un réseau de D et $|\cdot|$ une norme euclidienne sur $D \otimes \mathbb{R}$. Alors, tout sous-espace vectoriel V sur D de D^N de dimension L admet une base formée d'éléments X_1, \dots, X_L de Λ^N telle que

$$|X_1|_N \cdots |X_L|_N \leq \left(\frac{2\text{vol}(\Lambda)^{1/n}}{\tau_{nL}} \right)^L H^{\Lambda, |\cdot|}(V).$$

Démonstration: Nous cherchons des « petits » points du réseau $V \cap \Lambda^N$ du sous-espace vectoriel réel $W = V \otimes \mathbb{R}$ de $(D \otimes \mathbb{R})^N$. En choisissant une \mathbb{R} -base de $D \otimes \mathbb{R}$ qui est orthonormale pour le produit scalaire associé à $|\cdot|$ nous identifions le couple $(D \otimes \mathbb{R}, |\cdot|)$ avec \mathbb{R}^n et la norme euclidienne usuelle sur \mathbb{R}^n . Posons $S = W \cap B_N$, où B_N est la boule

$$B_N = \{Y \in (D \otimes \mathbb{R})^N \mid |Y|_N \leq 1/\tau_{nL}\}.$$

Ainsi S est une boule de rayon $r = 1/\tau_{nL}$ et de dimension nL , ce qui donne

$$\text{vol}(S) = \tau_{nL}^{nL} r^{nL} = 1.$$

Par le second théorème de Minkowski les minima successifs μ_1, \dots, μ_{nL} du réseau $V \cap \Lambda^N$ par rapport à S satisfont à l'inégalité

$$\mu_1 \cdots \mu_{nL} \leq 2^{nL} \text{vol}(V \cap \Lambda^N). \tag{1}$$

Maintenant nous choisissons $Y_1, \dots, Y_{nL} \in V \cap \Lambda^N$, linéairement indépendants sur \mathbb{Q} , tels que $Y_k \in \mu_k S$ ($1 \leq k \leq nL$). Il suit que

$$|Y_k|_N \leq \mu_k / \tau_{nL}$$

pour tout $1 \leq k \leq nL$. En utilisant (1), nous obtenons

$$|Y_1|_N \cdots |Y_{nL}|_N \leq (2/\tau_{nL})^{nL} \text{vol}(V \cap \Lambda^N).$$

Il nous reste à trouver L vecteurs suffisamment petits parmi Y_1, \dots, Y_{nL} qui soient linéairement indépendants sur D . Pour faire ceci, nous renommons Y_1, \dots, Y_{nL} , en oubliant leur relation avec μ_1, \dots, μ_{nL} , de sorte que

$$|Y_1|_N \leq |Y_2|_N \leq \cdots \leq |Y_{nL}|_N.$$

Commençons par prendre $X_1 = Y_1$. Alors $|X_1|_N \leq |Y_k|_N$ pour $1 \leq k \leq n$. Comme Y_1, \dots, Y_{nL} sont linéairement indépendants sur \mathbb{Q} , il existe $k \leq n+1$ tel que X_1 et Y_k sont linéairement indépendants sur D . Posons $X_2 = Y_k$. Ainsi $|X_2|_N \leq |Y_{k'}|_N$ pour $n+1 \leq k' \leq 2n$. Ensuite, de la même manière, il existe $k' \leq 2n+1$ tel que la famille $(X_1, X_2, Y_{k'})$ est libre sur D ; posons $X_3 = Y_{k'}$ et ainsi de suite. Par ce procédé nous trouvons X_1, \dots, X_L parmi Y_1, \dots, Y_{nL} qui sont linéairement indépendants sur D et vérifient

$$|X_1|_N^n \cdots |X_L|_N^n \leq |Y_1|_N \cdots |Y_{nL}|_N.$$

Ceci donne le résultat. □

Dans le théorème précédent, on peut également mesurer la base de V en utilisant une autre norme. Par exemple, on peut définir pour tout vecteur $X \in D^N$

$$|X|_{\max} = \max\{|x_1|, \dots, |x_N|\},$$

où x_1, \dots, x_N sont les composantes de X . Puisque $|X|_{\max} \leq |X|_N$, les vecteurs X_1, \dots, X_L du théorème 3.1 satisfont la même majoration par rapport à la norme $|\cdot|_{\max}$. Mais on peut faire mieux si on applique le théorème de Minkowski à l'ensemble $S = W \cap B_1^N$, où $B_1 = \{y \in D \otimes \mathbb{R} \mid |y| \leq 1/\tau_n\}$. Maintenant on ne peut plus calculer le volume de S facilement, mais grâce au théorème de *cube slicing* de J. Vaaler (voir [18], corollaire du théorème 1) on sait que $\text{vol}(S) \geq 1$. Ceci suffit pour montrer comme ci-dessus qu'il existe une base X_1, \dots, X_L de V dans Λ^N telle que

$$|X_1|_{\max} \cdots |X_L|_{\max} \leq \left(\frac{2\text{vol}(\Lambda)^{1/n}}{\tau_n} \right)^L H^{\Lambda, |\cdot|}(V).$$

Le résultat suivant montre que dans la majoration du théorème 3.1 la dépendance en la hauteur de V est optimale.

Proposition 3.2 *Étant donné des entiers naturels L et N tels que $0 < L < N$, il existe une constante $C = C(L, N) > 0$ avec la propriété suivante. Pour tout corps D de dimension finie sur \mathbb{Q} avec un réseau Λ et pour tout nombre réel $H > 0$, il existe un sous-espace (à gauche et à droite) V sur D de dimension L et une norme euclidienne $|\cdot|$ sur $D \otimes \mathbb{R}$ tels que $H^{\Lambda, |\cdot|}(V) > H$ et*

$$|X|_N \geq C^{-1} H^{\Lambda, |\cdot|}(V)^{1/L}$$

pour tout vecteur $X \neq 0$ de V dans Λ^N . En particulier, $C = 2^{N-L}(\sqrt{N})^{(N-L)/L}$ convient.

Démonstration: Il existe un sous-espace U de \mathbb{Q}^N de dimension L , construit par W. Schmidt [15], (p. 2), tel que $H(U) > H$ pour la hauteur classique sur \mathbb{Q} et tel que tout vecteur $Y = (y_1, \dots, y_N) \neq 0$ de U dans \mathbb{Z}^N satisfait

$$\max\{|y_1|, \dots, |y_N|\} \geq C^{-1} H(U)^{1/L},$$

avec $C = C(L, N) = 2^{N-L}(\sqrt{N})^{(N-L)/L} > 0$ (voir [7], p. 132). Nous posons $V = U \otimes_{\mathbb{Q}} D$.

Soit $\lambda_1, \dots, \lambda_n$ une \mathbb{Z} -base de Λ . Nous définissons un produit scalaire sur $D \otimes \mathbb{R}$ par $\langle \lambda_i, \lambda_j \rangle = 0$ si $i \neq j$ et $\langle \lambda_i, \lambda_i \rangle = |\lambda_i|^2 = 1$. Ainsi, si $x \in D \otimes \mathbb{R}$ a comme coordonnées $x_1, \dots, x_n \in \mathbb{R}$, on a $|x|^2 = x_1^2 + \dots + x_n^2 \geq \max\{|x_1|, \dots, |x_n|\}^2$. Par suite, en écrivant $X \in (D \otimes \mathbb{R})^N$ comme combinaison linéaire des $\lambda_1, \dots, \lambda_n$ avec des coefficients $X_1, \dots, X_n \in \mathbb{R}^N$, nous avons

$$|X|_N \geq \max_{1 \leq i \leq n} \max\{|x_{i1}|, \dots, |x_{iN}|\},$$

où x_{i1}, \dots, x_{iN} sont les composantes de X_i ($1 \leq i \leq n$).

Supposons maintenant que $X \neq 0$ est dans $\Lambda^N \cap V$. Alors X_1, \dots, X_n sont dans $U \cap \mathbb{Z}^N$ et au moins un vecteur est non nul. Les deux inégalités précédentes impliquent donc que

$$|X|_N \geq C^{-1} H(U)^{1/L}$$

et la proposition est démontrée parce qu'on peut vérifier par un calcul direct que $H(U) = H^{\Lambda, |\cdot|}(V)$ (voir aussi plus bas la remarque après le corollaire 4.1). \square

La version originale du lemme de Siegel (voir [16]) correspond au cas $\Lambda = \mathbb{Z}$ dans $D = \mathbb{Q}$. L'énoncé était exprimé en termes de petites solutions d'un système d'équations linéaires. Nous pourrions traduire notre théorème dans ce langage lorsque

nous aurons introduit dans la partie 6 la hauteur d’une matrice A sur D et montré qu’elle coïncide avec la hauteur de l’espace des solutions de $AX = 0$.

Jusqu’ici tout ce que nous avons fait est valable pour un couple quelconque $(\Lambda, |\cdot|)$. Pour aller plus loin, il nous faut des hypothèses supplémentaires. Ainsi toutes les parties suivantes feront intervenir un couple (\mathcal{O}, \star) formé d’un ordre maximal et d’une involution positive. En particulier, nous pourrons revenir sur le lemme de Siegel (voir partie 8), reformuler le théorème 3.1 en termes de hauteur de vecteurs et améliorer la proposition 3.2 à V fixé.

4 Extensions

Dans cette partie, nous nous intéressons au comportement de la hauteur à travers une extension de corps $D \subset D'$. Nous donnons en fait d’abord un résultat un peu plus général qui permet d’englober la situation que nous rencontrerons dans la partie suivante en lien avec le degré des variétés abéliennes.

Proposition 4.1 *Soient D un corps de dimension finie sur \mathbb{Q} , \mathcal{O} un ordre maximal de D , \star une anti-involution positive sur $D \otimes \mathbb{R}$ et V un sous-espace à droite de D^N . Considérons un \mathcal{O} -module à gauche Ω de type fini et sans torsion ainsi qu’un produit scalaire $\langle \cdot, \cdot \rangle$ sur $\Omega \otimes \mathbb{R}$ tel que si $\alpha, \beta \in \Omega \otimes \mathbb{R}$ et $x \in D \otimes \mathbb{R}$ alors $\langle x\alpha, \beta \rangle = \langle \alpha, x^*\beta \rangle$. Dans ces conditions*

$$\frac{\text{vol}((V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N)}{\text{vol}(\Omega)^{\dim V}} = H^{\mathcal{O}, \star}(V)^{\text{rang}_{\mathbb{Z}} \Omega}.$$

Nous commençons par expliquer comment nous exploitons la maximalité de \mathcal{O} . Pour chaque nombre premier p , nous notons (ici et dans toute la suite) $D_p = D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ le complété p -adique de D puis $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ celui de \mathcal{O} . Nous savons alors grâce au lemme 4 de [8] que \mathcal{O}_p est un ordre maximal de D_p et est principal à droite et à gauche, c’est-à-dire que tout idéal à droite (resp. à gauche) de \mathcal{O}_p peut s’écrire comme $\delta \mathcal{O}_p$ (resp. $\mathcal{O}_p \delta$) pour un certain $\delta \in \mathcal{O}_p$. On prendra toutefois garde au fait que \mathcal{O}_p n’est pas en général intègre.

En particulier, la principalité de \mathcal{O}_p donne lieu au résultat suivant.

Lemme 4.1 *Si \mathcal{O} est un ordre maximal de D , tout \mathcal{O} -module à gauche (resp. à droite) Ω de type fini et sans torsion est plat. Pour tout nombre premier p , le \mathcal{O}_p -module $\mathcal{O}_p \otimes \Omega$ (resp. $\Omega \otimes \mathcal{O}_p$) est libre.*

Démonstration: L’hypothèse que Ω est sans torsion implique $\Omega \subset D \otimes_{\mathcal{O}} \Omega$. En choisissant dans Ω une base de l’espace vectoriel $D \otimes_{\mathcal{O}} \Omega$ nous pouvons écrire $\mathcal{O}^k \subset \Omega \subset D^k$ puis, comme $D = \mathbb{Q}\mathcal{O}$ et Ω de type fini, $\mathcal{O}^k \subset \Omega \subset (n^{-1}\mathcal{O})^k$ pour un certain $n \in \mathbb{Z} \setminus \{0\}$. Il vient $\mathcal{O}_p^k \subset \mathcal{O}_p \otimes \Omega \subset (n^{-1}\mathcal{O}_p)^k$ et, puisque \mathcal{O}_p est principal, ceci entraîne facilement $\mathcal{O}_p \otimes \Omega \simeq \mathcal{O}_p^k$. En particulier, ce module est plat sur \mathcal{O}_p . Comme ceci est vrai pour tout p , le module Ω est également plat sur \mathcal{O} (puisque, pour tester l’exactitude d’une suite de \mathbb{Z} -modules, il suffit de le faire après produit tensoriel avec chacun des \mathbb{Z}_p). Les mêmes arguments s’appliquent si Ω est un module à droite. \square
 Démonstration de la Proposition 4.1: Comme première conséquence du lemme, nous notons par platitude de Ω

$$(V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N = (V \otimes_{\mathcal{O}} \Omega) \cap (\mathcal{O}^N \otimes_{\mathcal{O}} \Omega) \simeq (V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \Omega.$$

Si jamais Ω est libre sur \mathcal{O} , cette formule permet facilement de relier le volume de $(V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N$ à celui de $V \cap \mathcal{O}^N$. Dans le cas général, nous introduisons un sous-module $\Omega' \subset \Omega$ de même rang sur \mathbb{Z} et libre sur \mathcal{O} . Nous écrivons

$$\Omega' = \bigoplus_{i=1}^k \mathcal{O}v_i$$

où $v_i \in \Omega$ et $k = (\text{rang}_{\mathbb{Z}} \Omega) / [D : \mathbb{Q}]$. Puisque le \mathcal{O} -module à droite $V \cap \mathcal{O}^N$ est plat par le lemme, nous trouvons

$$(V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \Omega' \subset (V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \Omega = (V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N$$

puis, en notant encore $L = \dim V$,

$$\frac{\text{vol}((V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N)}{\text{vol}(\Omega)^L} = \frac{[\Omega : \Omega']^L}{[(V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \Omega : (V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \Omega']^L} \cdot \frac{\text{vol}((V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \Omega')}{\text{vol}(\Omega')^L}.$$

Montrons d'abord que le rapport des indices vaut 1. Il suffit pour cela de considérer les p -parties et donc de vérifier

$$[(V \cap \mathcal{O}^N) \otimes_{\mathcal{O}p} \otimes_{\mathcal{O}} \Omega : (V \cap \mathcal{O}^N) \otimes_{\mathcal{O}p} \otimes_{\mathcal{O}} \Omega'] = [\mathcal{O}p \otimes_{\mathcal{O}} \Omega : \mathcal{O}p \otimes_{\mathcal{O}} \Omega']^L;$$

or ceci est clair car $(V \cap \mathcal{O}^N) \otimes_{\mathcal{O}} \mathcal{O}p \simeq \mathcal{O}p^L$ d'après le lemme 4.1. Nous avons donc à présent

$$\frac{\text{vol}((V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N)}{\text{vol}(\Omega)^L} = \frac{\text{vol}(\bigoplus_{i=1}^k (V \cap \mathcal{O}^N)v_i)}{(\text{vol}(\bigoplus_{i=1}^k \mathcal{O}v_i))^L}$$

pour toute famille (v_1, \dots, v_k) de Ω libre sur \mathcal{O} . La formule reste valable si l'on divise tous les v_i par un même entier non nul donc elle vaut pour toute famille de $\Omega \otimes_{\mathbb{Z}} \mathbb{Q}$ libre sur D . Bien plus, le second membre a un sens pour toute famille de $\Omega \otimes \mathbb{R}$ libre sur $D \otimes \mathbb{R}$ et, par densité de $\Omega \otimes \mathbb{Q}$ dans $\Omega \otimes \mathbb{R}$, l'égalité a encore lieu dans ce cas.

Ainsi, pour toute famille (v'_1, \dots, v'_k) de $\Omega \otimes \mathbb{R}$ libre sur $D \otimes \mathbb{R}$, nous avons maintenant

$$\frac{\text{vol}((V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N)}{\text{vol}(\Omega)^L} = \frac{\text{vol}(\bigoplus_{i=1}^k (V \cap \mathcal{O}^N)v'_i)}{(\text{vol}(\bigoplus_{i=1}^k \mathcal{O}v'_i))^L}$$

Nous pouvons alors choisir cette famille de sorte que

$$\Omega \otimes \mathbb{R} = \bigoplus_{i=1}^k (D \otimes \mathbb{R})v'_i$$

avec une somme directe orthogonale pour le produit scalaire $\langle \cdot, \cdot \rangle$. En effet, on choisit $v'_1 \in \Omega \otimes \mathbb{R}$ sans $(D \otimes \mathbb{R})$ -torsion et l'on vérifie que $((D \otimes \mathbb{R})v'_1)^\perp$ est un $(D \otimes \mathbb{R})$ -module libre : si $\alpha \in ((D \otimes \mathbb{R})v'_1)^\perp$ et $x \in D \otimes \mathbb{R}$ on a, pour tout $y \in D \otimes \mathbb{R}$,

$$\langle x\alpha, yv'_1 \rangle = \langle \alpha, x^*yv'_1 \rangle = 0$$

donc $x\alpha \in ((D \otimes \mathbb{R})v'_1)^\perp$. L'on peut donc choisir v'_2 dans $((D \otimes \mathbb{R})v'_1)^\perp$ et recommencer.

Une telle famille étant choisie, la restriction de $\langle \cdot, \cdot \rangle$ à $(D \otimes \mathbb{R})v'_i$ munit $D \otimes \mathbb{R}$ d'un produit scalaire f_i (par $f_i(x, y) = \langle xv'_i, yv'_i \rangle$) et nous notons vol_i le volume

correspondant. Notre formule devient alors

$$\frac{\text{vol}((V \otimes_{\mathcal{O}} \Omega) \cap \Omega^N)}{\text{vol}(\Omega)^L} = \prod_{i=1}^k \frac{\text{vol}_i(V \cap \mathcal{O}^N)}{\text{vol}_i(\mathcal{O})^L}.$$

Si tous les vol_i coïncident avec le volume induit par le produit scalaire $(x, y) \mapsto \text{Tr}(x^*y)$ alors, vu la valeur de k , le membre de droite est exactement $H^{\mathcal{O}, \star}(V)^{\text{rang}_{\mathbb{Z}} \Omega}$ et la proposition est vraie. Il ne nous reste donc qu'à montrer que l'on peut faire en sorte que chaque f_i soit exactement ce produit scalaire.

Nous considérons la forme linéaire $x \mapsto f_i(1, x)$ sur $D \otimes \mathbb{R}$. Puisque $D \otimes \mathbb{R}$ est un produit d'espaces de matrices sur $\mathbb{K} = \mathbb{R}, \mathbb{C}$ ou \mathbb{H} (voir lemme 1.1), nous obtenons une famille de formes linéaires de la forme $\text{Mat}_m(\mathbb{K}) \rightarrow \mathbb{R}$. Nous pouvons écrire évidemment une telle forme \mathbb{R} -linéaire comme la trace d'une forme \mathbb{K} -linéaire $\text{Mat}_m(\mathbb{K}) \rightarrow \mathbb{K}$. Maintenant, sur un corps quelconque \mathbb{K} , une telle forme linéaire s'écrit $A \mapsto \text{Tr}(AB)$ pour une matrice $B \in \text{Mat}_m(\mathbb{K})$. De cette façon, nous constatons qu'il existe $b = b_i \in D \otimes \mathbb{R}$ tel que $f_i(1, x) = \text{Tr}(xb)$ pour tout $x \in D \otimes \mathbb{R}$.

Cette relation entraîne pour tous $x, y \in D \otimes \mathbb{R}$

$$f_i(x, y) = \langle xv'_i, yv'_i \rangle = \langle v'_i, x^*yv'_i \rangle = f_i(1, x^*y) = \text{Tr}(x^*yb).$$

Par symétrie du produit scalaire nous avons $\text{Tr}(x^*yb) = \text{Tr}(y^*xb) = \text{Tr}(b^*x^*y)$ ce qui entraîne $b = b^*$. De plus, $\text{Tr}(x^*xb) > 0$ pour tout $x \in (D \otimes \mathbb{R}) \setminus \{0\}$. Sous la forme $\text{Tr}(xbx^*) > 0$ cela traduit le fait que si nous choisissons dans le lemme 1.1 un isomorphisme tel que \star est donnée par la transconjugaison alors b est constitué de matrices hermitiennes définies positives. En conséquence, nous pouvons écrire $b = cc^*$ avec $c \in D \otimes \mathbb{R}$ (inversible). Maintenant, nous calculons

$$\langle xc^{-1}v'_i, yc^{-1}v'_i \rangle = \text{Tr}((c^{-1})^*x^*yc^{-1}b) = \text{Tr}(x^*y)$$

et, en choisissant $c^{-1}v'_i$ au lieu de v'_i , la démonstration est terminée. □

Voici ce que nous pouvons dire sur les extensions de corps (bien entendu, nous pourrions énoncer à la fois la proposition et ce corollaire en échangeant les mots gauche et droite).

Corollaire 4.1 *Soient D un corps de dimension finie sur \mathbb{Q} , \mathcal{O} un ordre maximal de D et \star une anti-involution positive sur $D \otimes \mathbb{R}$. Soient D' une extension finie de D , Λ un réseau de D' qui est un \mathcal{O} -module à gauche et $|\cdot|$ une norme euclidienne sur $D' \otimes \mathbb{R}$ telle que le produit scalaire associé vérifie $\langle xy, z \rangle = \langle y, x^*z \rangle$ pour $x \in D \otimes \mathbb{R}$ et $y, z \in D' \otimes \mathbb{R}$. Pour tout entier naturel N et tout sous-espace à droite V de D^N on a*

$$H^{\Lambda, |\cdot|}(V \otimes_D D') = H^{\mathcal{O}, \star}(V).$$

Démonstration: Par définition le membre de gauche est

$$\left(\frac{\text{vol}((V \otimes_D D') \cap \Lambda^N)}{\text{vol}(\Lambda)^{\dim V \otimes D'}} \right)^{1/[D':\mathbb{Q}]}$$

Il nous suffit donc de noter $\dim_{D'} V \otimes D' = \dim_D V$, $[D' : \mathbb{Q}] = \text{rang}_{\mathbb{Z}} \Lambda$ et $V \otimes_D D' = V \otimes_{\mathcal{O}} \Lambda$ (puisque $D' = \mathbb{Q}\Lambda$) pour appliquer la proposition avec $\Omega = \Lambda$ et le résultat s'ensuit. □

Notons que si $D = \mathbb{Q}$ alors on a $\mathcal{O} = \mathbb{Z}$ et $\star = \text{id}$, ce qui entraîne que les conditions sur Λ et $|\cdot|$ sont automatiquement vérifiées.

Remarquons aussi que si \mathcal{O}' est un ordre de D' qui contient \mathcal{O} alors c'est un module à gauche et à droite sur \mathcal{O} ; de même s'il existe une anti-involution \star' sur $D' \otimes \mathbb{R}$ induisant \star sur $D \otimes \mathbb{R}$ alors l'hypothèse sur le produit scalaire est clairement satisfaite ; ainsi si \mathcal{O}' et \star' remplissent ces deux conditions nous avons $H^{\mathcal{O}',\star'}(V \otimes D') = H^{\mathcal{O},\star}(V)$. Signalons que, étant donné (\mathcal{O}, \star) , il existe toujours un tel couple (\mathcal{O}', \star') .

5 Variétés abéliennes

Nous montrons ici comment l'on peut calculer le degré d'une sous-variété abélienne de manière naturelle en termes de la hauteur que nous avons introduite.

Nous nous plaçons dans la situation suivante: soient X une variété abélienne simple sur \mathbb{C} et Y une sous-variété abélienne de X^N où $N \geq 1$. Nous posons $\mathcal{O} = \text{End}(X)$ et $D = \mathcal{O} \otimes \mathbb{Q}$. Comme X est simple, D est un corps et \mathcal{O} un ordre. Nous associons à Y le sous-espace à droite

$$V = \{ \varphi \in \text{Hom}(X, X^N) \mid \varphi(X) \subset Y \} \otimes_{\mathbb{Z}} \mathbb{Q} \subset \text{Hom}(X, X^N) \otimes_{\mathbb{Z}} \mathbb{Q} = D^N.$$

Pour définir à la fois le degré de Y et la hauteur de V (que nous souhaitons comparer), nous avons besoin d'une polarisation sur X c'est-à-dire un faisceau inversible ample \mathcal{L}_0 . D'une part, le degré de Y est défini en termes de nombres d'intersection par $\text{deg}_{\mathcal{L}} Y = \mathcal{L}^{\dim Y} \cdot Y$ où $\mathcal{L} = \bigotimes_{i=1}^N p_i^* \mathcal{L}_0$ sur X^N et d'autre part est associée à \mathcal{L}_0 une anti-involution positive sur D que l'on appelle involution de Rosati, que nous notons \dagger et qui permet donc de parler de la hauteur $H^{\mathcal{O},\dagger}(V)$ de V .

La relation entre ces deux quantités, conjecturée dans [6], (appendice B), est la suivante.

Théorème 5.1 *Si l'ordre \mathcal{O} est maximal alors*

$$\frac{\text{deg}_{\mathcal{L}} Y}{(\dim Y)!} = \left(\frac{\text{deg}_{\mathcal{L}_0} X}{(\dim X)!} \right)^L H^{\mathcal{O},\dagger}(V)^{2g}$$

où $g = \dim X$ et $gL = \dim Y$.

Démonstration: Nous utilisons la description analytique des variétés abéliennes complexes (voir par exemple [11]). Ainsi voyons-nous X comme un tore complexe E_0/Π_0 où E_0 est un espace vectoriel sur \mathbb{C} de dimension g et Π_0 un réseau de E_0 (vu comme espace sur \mathbb{R}). Nous notons aussi $F_0 = \mathbb{Q}\Pi_0 \subset E_0$. Dans ce cadre, la polarisation \mathcal{L}_0 donne naissance à une forme de Riemann c'est-à-dire une forme $H_0: E_0 \times E_0 \rightarrow \mathbb{C}$ hermitienne définie positive telle que $(\text{Im}H_0)(\Pi_0 \times \Pi_0) \subset \mathbb{Z}$. Par ailleurs, \mathcal{O} (resp. D) s'identifie à l'ensemble des applications \mathbb{C} -linéaires $\varphi: E_0 \rightarrow E_0$ telles que $\varphi(\Pi_0) \subset \Pi_0$ (resp. $\varphi(F_0) \subset F_0$). En particulier, Π_0 a une structure de \mathcal{O} -module à gauche, F_0 de D -espace vectoriel à gauche et E_0 de $D \otimes \mathbb{R}$ -module à gauche. Finalement l'involution de Rosati est caractérisée par $H_0(\varphi x, y) = H_0(x, \varphi^\dagger y)$ pour tous $x, y \in E_0$ et $\varphi \in D$.

Venons-en à X^N et Y . Comme tore complexe $X^N = E/\Pi$ où $\Pi = \bigoplus_{i=1}^N \Pi_0 \subset \bigoplus_{i=1}^N E_0 = E$ et la polarisation se reflète dans la forme de Riemann $H: E \times E \rightarrow \mathbb{C}$ donnée par

$$H((x_1, \dots, x_N), (y_1, \dots, y_N)) = \sum_{i=1}^N H_0(x_i, y_i).$$

La sous-variété abélienne Y quant à elle correspond à un sous-espace vectoriel complexe W de E tel que $W \cap \Pi$ soit un réseau (de sorte que $Y = W/W \cap \Pi$). Notons que W n'est pas en général un sous-espace vectoriel sur D de E . Dans ce cadre, nous pouvons calculer les degrés comme volumes euclidiens (nous précisons le produit scalaire utilisé en indice pour éviter les confusions):

$$\text{deg}_{\mathcal{L}_0} X = (\dim X)! \text{vol}_{\text{Re}H_0}(\Pi_0) \quad \text{et} \quad \text{deg}_{\mathcal{L}} Y = (\dim Y)! \text{vol}_{\text{Re}H}(W \cap \Pi).$$

Pour en finir avec les notations générales, nous posons $F = \bigoplus_{i=1}^N F_0 = \mathbb{Q}\Pi \subset E$.

Nous faisons à présent le lien entre $V \cap \mathcal{O}^N$, qui sert à calculer $H^{\mathcal{O}, \dagger}(V)$, et $W \cap \Pi$, qui sert à calculer $\text{deg}_{\mathcal{L}} Y$. Nous partons de l'isomorphisme évident $D^N \otimes_D E_0 = E$ qui reflète l'action de $D^N = \text{Hom}(X, X^N) \otimes \mathbb{Q}$ sur $X^N = E/\Pi$. Par définition de V , nous avons alors $V \otimes_D E_0 \subset W$ et, en particulier, $V \otimes_D F_0 \subset W \cap F$. Maintenant V est aussi isomorphe à $\text{Hom}(X, Y) \otimes \mathbb{Q}$ et, comme Y est isogène à X^L , nous trouvons $\dim_D V = L$. Par conséquent, $\dim_{\mathbb{Q}}(V \otimes_D F_0) = 2Lg = \dim_{\mathbb{Q}} W \cap F$ et donc $V \otimes_D F_0 = W \cap F$. Comme $F_0 = \mathbb{Q}\Pi_0 = \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O} \otimes_{\mathcal{O}} \Pi_0 = D \otimes_{\mathcal{O}} \Pi_0$ cette dernière relation s'écrit aussi $V \otimes_{\mathcal{O}} \Pi_0 = W \cap F$. Ainsi nous avons $(V \otimes_{\mathcal{O}} \Pi_0) \cap \Pi = W \cap \Pi$.

Par ailleurs, nous sommes en mesure d'appliquer la proposition 4.1 avec $\Omega = \Pi_0$ et le produit scalaire $\text{Re}H_0$ sur $E_0 = \Omega \otimes \mathbb{R}$. Il vient donc

$$\frac{\text{vol}_{\text{Re}H}((V \otimes \Pi_0) \cap \Pi)}{\text{vol}_{\text{Re}H_0}(\Pi_0)^L} = H^{\mathcal{O}, \dagger}(V)^{\text{rang}_{\mathbb{Z}} \Pi_0}.$$

Cela s'écrit ensuite

$$\text{vol}_{\text{Re}H}(W \cap \Pi) = \text{vol}_{\text{Re}H_0}(\Pi_0)^L \cdot H^{\mathcal{O}, \dagger}(V)^{2g}$$

et donne exactement la relation cherchée. □

Cet énoncé généralise un résultat de D. Bertrand et D. Masser (voir [1]). Leur démonstration, écrite dans le cas des quaternions, suit un cheminement sensiblement différent de la nôtre (même si la façon dont intervient l'hypothèse cruciale que \mathcal{O} est maximal s'avère assez proche). Elle pourrait vraisemblablement s'adapter au cas général en utilisant les résultats des deux parties suivantes, en particulier le théorème de dualité 7.1 et la proposition 7.2.

Une fois établi le théorème 5.1, il semble naturel de se demander ce qu'il en advient lorsque l'on ne suppose pas \mathcal{O} maximal. On souhaiterait penser, à première vue, qu'il reste vrai tel quel mais ce n'est malheureusement pas le cas. Si \mathcal{O} n'est pas maximal, la donnée de V (et de \mathcal{O}) ne comporte pas assez d'information pour déterminer le rapport des degrés. Un contre-exemple concret s'obtient de la manière suivante.

Nous posons $D = \mathbb{Q}(i)$. D'après [11], (p. 202–203), il existe une variété abélienne X sur \mathbb{C} de dimension $g = 3$ avec $\text{End}(X) \otimes \mathbb{Q} \simeq D$. Ainsi, avec les notations de la démonstration, $F_0 = \mathbb{Q}\Pi_0$ est un espace de dimension $2g/[D : \mathbb{Q}] = 3$ sur D . Nous écrivons $F_0 = De_1 \oplus De_2 \oplus De_3$. Nous considérons maintenant trois autres réseaux de F_0 à savoir

$$\Pi_0^{(1)} = (\mathbb{Z} \oplus i\mathbb{Z})e_1 \oplus (\mathbb{Z} \oplus i\mathbb{Z})e_2 \oplus (\mathbb{Z} \oplus \frac{i}{2}\mathbb{Z})e_3,$$

$$\Pi_0^{(2)} = (\mathbb{Z} \oplus i\mathbb{Z})e_1 \oplus (\mathbb{Z} \oplus \frac{i}{2}\mathbb{Z})e_2 \oplus (\mathbb{Z} \oplus \frac{i}{2}\mathbb{Z})e_3 \text{ et}$$

$$\Pi_0^{(3)} = (\mathbb{Z} \oplus \frac{i}{2}\mathbb{Z})e_1 \oplus (\mathbb{Z} \oplus \frac{i}{2}\mathbb{Z})e_2 \oplus (\mathbb{Z} \oplus \frac{i}{2}\mathbb{Z})e_3.$$

Puisque X est une variété abélienne, il existe une forme de Riemann H_0 telle que $(\text{Im}H_0)(\Pi_0 \times \Pi_0) \subset \mathbb{Z}$. Quitte à multiplier H_0 par un entier, nous pouvons supposer que $(\text{Im}H_0)(\Pi_0^{(j)} \times \Pi_0^{(j)}) \subset \mathbb{Z}$ pour $1 \leq j \leq 3$. Par conséquent nous obtenons trois nouvelles variétés abéliennes X_1, X_2 et X_3 (isogènes à X). Nous avons clairement $\text{End}(X_j) \otimes \mathbb{Q} \simeq D$ et nous pouvons calculer

$$\text{End}(X_j) \simeq \{z \in D \mid z\Pi_0^{(j)} \subset \Pi_0^{(j)}\} = \mathbb{Z} \oplus 2i\mathbb{Z}$$

pour $1 \leq j \leq 3$. Nous trouvons donc le même anneau \mathcal{O} d'endomorphismes dans les trois cas et ce n'est certes pas un ordre maximal de D . L'involution de Rosati est la conjugaison sur D (c'est l'unique involution positive).

Considérons alors $V = \{(x, ix) \mid x \in D\} \subset D^2$. Nous avons $V \otimes_D F_0 \subset F = F_0^2$ et nous pouvons définir $W \subset E = E_0^2$ comme le sous-espace sur \mathbb{C} engendré par $V \otimes_D F_0$. Ce sous-espace fournit une sous-variété abélienne Y_j de X_j^2 pour chaque $1 \leq j \leq 3$ (avec $V = \{\varphi \in \text{Hom}(X_j, X_j^2) \mid \varphi(X_j) \subset Y_j\} \otimes_{\mathbb{Z}} \mathbb{Q}$). Grâce à la base (e_1, e_2, e_3) de F_0 , le sous-espace $V \otimes_D F_0 = W \cap F$ de F s'identifie à $V^3 \subset D^6$. Avec $\Pi_j = (\Pi_0^{(j)})^2 \subset D^6$, nous calculons explicitement dans les trois cas

$$W \cap \Pi_j = \{(x, y, z, ix, iy, iz) \mid x, y, z \in \mathbb{Z} \oplus i\mathbb{Z}\}$$

(il suffit de voir $V \cap (\mathbb{Z} \oplus i\mathbb{Z})^2 = V \cap (\mathbb{Z} \oplus (i/2)\mathbb{Z})^2$). Par conséquent, $\text{deg } Y_1 = \text{deg } Y_2 = \text{deg } Y_3$ tandis que $\text{deg } X_j = 2 \text{deg } X_{j+1}$ puisque $[\Pi_0^{(j+1)} : \Pi_0^{(j)}] = 2$ si $1 \leq j \leq 2$. De cette façon, la formule du théorème ne peut être vraie que dans au plus un des trois cas puisque tous les facteurs y apparaissant sont identiques, excepté le degré de X_j .

Signalons finalement que l'on aurait pu imaginer qu'une hypothétique formule valable pour un ordre quelconque fasse intervenir plutôt la hauteur du dual de V (voir partie 7) puisque celle-ci coïncide avec celle de V pour un ordre maximal et puisque la démarche de [1] utilise cette dualité. Bien entendu, cela est également contredit par l'exemple ci-dessus car une quantité ne dépendant que de V est insuffisante (et, en fait, la formule de dualité vaut pour l'espace V considéré).

6 Expressions matricielles

Soient M, N des entiers naturels tels que $1 \leq M \leq N$ et soit A une matrice de $\text{Mat}_{MN}(D)$ de rang M (dans cette partie le rang d'une matrice signifie toujours le rang à gauche des lignes). Pour un réseau Λ de D , l'image $A\Lambda^N$ est un réseau de D^M . Nous posons

$$H_{\text{fin}}^\Lambda(A) = [A\Lambda^N : \Lambda^M]^{1/[D:\mathbb{Q}]}$$

D'autre part A induit une application \mathbb{R} -linéaire $f: (D \otimes \mathbb{R})^N \rightarrow (D \otimes \mathbb{R})^M$. Si $D \otimes \mathbb{R}$ a une structure euclidienne $|\cdot|$, nous pouvons alors considérer l'adjoint ${}^t f: (D \otimes \mathbb{R})^M \rightarrow (D \otimes \mathbb{R})^N$ (nous notons ${}^t f$ l'adjoint plutôt que f^* pour éviter la confusion avec l'involution \star ci-dessous). Tandis que f est aussi un morphisme de $D \otimes \mathbb{R}$ -modules, ${}^t f$ est seulement \mathbb{R} -linéaire. Comme f est surjective, $f \circ {}^t f$ est un \mathbb{R} -automorphisme de $(D \otimes \mathbb{R})^M$ et nous posons

$$H_{\text{inf}}^{|\cdot|}(A) = \det(f \circ {}^t f)^{1/2[D:\mathbb{Q}]}$$

Nous définissons la hauteur de A par

$$H^{\Lambda, |\cdot|}(A) = H_{\text{fin}}^{\Lambda}(A)H_{\text{inf}}^{|\cdot|}(A).$$

Proposition 6.1 *Soient D, Λ et $|\cdot|$ comme ci-dessus et $N \geq 1$ un entier naturel. Alors pour tout sous-espace vectoriel à droite strict V sur D de D^N on a*

$$H^{\Lambda, |\cdot|}(V) = H^{\Lambda, |\cdot|}(A),$$

dès que A est une matrice de $\text{Mat}_{MN}(D)$ de rang $M = N - \dim V$ telle que $V = \{X \in D^N \mid AX = 0\}$.

Démonstration: Soit n la dimension de l'espace vectoriel réel $D \otimes \mathbb{R}$ sur \mathbb{R} . Comme dans la partie 3 nous identifions la paire $(D \otimes \mathbb{R}, |\cdot|)$ avec \mathbb{R}^n et la norme euclidienne usuelle sur \mathbb{R}^n .

Nous pouvons donc utiliser la formule

$$\text{vol}(V \cap \Lambda^N)\text{vol}(f(\Lambda^N)) = \det(f \circ {}^t f)^{1/2} \text{vol}(\Lambda^N).$$

Si f s'identifie avec la projection orthogonale de \mathbb{R}^{nN} sur $\mathbb{R}^{nM} = \mathbb{R}^{nM} \times \{0\}$, cette formule est bien connue (voir, par exemple, la proposition 1.2.9 de [10]). Pour f plus générale, on peut se ramener à ce cas précédent en remplaçant f par ufv et Λ^N par $v^{-1}(\Lambda^N)$, où v et u sont des transformations linéaires orthogonales et inversibles, respectivement.

Comme $\text{vol}(\Lambda^m) = \text{vol}(\Lambda)^m$ pour tout entier naturel m , nous en déduisons que

$$H^{\Lambda, |\cdot|}(V)^n = \det(f \circ {}^t f)^{1/2} \text{vol}(\Lambda)^M / \text{vol}(f(\Lambda^N)).$$

Par définition, nous avons

$$\det(f \circ {}^t f)^{1/2} = H_{\text{inf}}^{|\cdot|}(A)^n.$$

De plus,

$$\text{vol}(f(\Lambda^N)) = \text{vol}(A\Lambda^N) = [\Lambda^M : A\Lambda^N] \text{vol}(\Lambda^M),$$

d'où

$$\text{vol}(\Lambda)^M / \text{vol}(f(\Lambda^N)) = [\Lambda^M : A\Lambda^N]^{-1} = [A\Lambda^N : \Lambda^M] = H_{\text{fin}}^{\Lambda}(A)^n.$$

Ceci montre le résultat. □

Si le réseau $\Lambda = \mathcal{O}$ est un ordre maximal de D nous pouvons exprimer $H_{\text{fin}}^{\mathcal{O}}(A)$ comme un produit de facteurs locaux. Rappelons que la maximalité de \mathcal{O} entraîne la principalité de l'anneau \mathcal{O}_p pour tout nombre premier p .

Étant donné des éléments b_1, \dots, b_r de \mathcal{O}_p nous pouvons donc définir un plus grand facteur gauche commun $\delta = \text{pgfgc}(b_1, \dots, b_r)$ comme un élément de \mathcal{O}_p satisfaisant $b_1\mathcal{O}_p + \dots + b_r\mathcal{O}_p = \delta\mathcal{O}_p$. Si $b_1D_p + \dots + b_rD_p = D_p$, alors ce pgfgc est déterminé uniquement à multiplication à droite par une unité près. Si les éléments b_1, \dots, b_r sont dans \mathcal{O} , nous écrivons pgfgc_p pour souligner la dépendance de p .

Nous pouvons étendre ces considérations à $\text{Mat}_{MM}(D)$ au lieu de D . Comme $\text{Mat}_{MM}(\mathcal{O})$ est un ordre maximal de $\text{Mat}_{MM}(D)$, le lemme 4 de [8] entraîne que $\text{Mat}_{MM}(\mathcal{O}_p)$ est principal pour tout nombre premier p . Nous pouvons donc définir un pgfgc des éléments de $\text{Mat}_{MM}(\mathcal{O}_p)$ de la même façon que pour des éléments de \mathcal{O}_p .

Ensuite nous notons nr la norme réduite $\text{Mat}_{MM}(D \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p$ (voir [12], p. 119). On a $|\text{nr}(U)|_p = 1$ pour toute unité U de $\text{Mat}_{MM}(\mathcal{O}_p)$, où $|\cdot|_p$ désigne la

valeur absolue p -adique usuelle sur \mathbb{Q}_p . Par conséquent, si B_1, \dots, B_r sont des éléments de $\text{Mat}_{MM}(\mathcal{O}_p)$ tels que $B_1 \text{Mat}_{MM}(D_p) + \dots + B_r \text{Mat}_{MM}(D_p) = \text{Mat}_{MM}(D_p)$, la p -partie de la norme réduite $\text{nr}(\text{pgfgc}(B_1, \dots, B_r))$ est bien définie.

De nouveau, si les éléments B_1, \dots, B_r sont dans $\text{Mat}_{MM}(\mathcal{O})$ nous écrivons pgfgc_p pour souligner la dépendance de p .

Notons que si B_1, \dots, B_r , où $r = \binom{m}{l}$ pour $1 \leq l \leq m$, sont les mineurs d'ordre l d'une matrice $B \in \text{Mat}_{lm}(\mathcal{O}_p)$, nous avons

$$B\mathcal{O}_p^m = \Delta\mathcal{O}_p^l \tag{2}$$

pour $\Delta = \text{pgfgc}(B_1, \dots, B_r)$. Cette identité est importante dans la démonstration de la proposition 6.2 ci-dessous et nous l'utiliserons de nouveau dans la partie 8. On peut la vérifier comme suit.

Le sous- \mathcal{O}_p -module $B\mathcal{O}_p^m$ de \mathcal{O}_p^l est engendré par les colonnes de B . Chaque telle colonne est une colonne d'un mineur B_i de B et comme B_i est un multiple à droite de Δ , cette colonne est une combinaison linéaire à droite sur \mathcal{O}_p des colonnes de Δ . D'où $B\mathcal{O}_p^m \subset \Delta\mathcal{O}_p^l$. Pour l'inclusion inverse, on écrit Δ comme combinaison linéaire à droite sur $\text{Mat}_l(\mathcal{O}_p)$ des B_1, \dots, B_r . Chaque colonne de Δ est donc une combinaison linéaire à droite sur \mathcal{O}_p des colonnes de B . D'où $B\mathcal{O}_p^m \supset \Delta\mathcal{O}_p^l$ et (2) est démontré.

Finalement, si Z est le centre de D , nous notons e sa dimension sur \mathbb{Q} puis $[D : Z] = d^2$; ainsi $d^2e = [D : \mathbb{Q}]$ (ceci est cohérent avec les notations du lemme 1.1 et de sa démonstration).

Proposition 6.2 *Si $\Lambda = \mathcal{O}$ est un ordre maximal de D et $A \in \text{Mat}_{MN}(\mathcal{O})$ de rang M alors*

$$H_{\text{fin}}^{\mathcal{O}}(A) = \prod_p |\text{nr}(\text{pgfgc}_p A_0)|_p^{1/de}$$

où le produit est sur tous les nombres premiers p et le pgfgc sur les mineurs A_0 d'ordre M de A .

Démonstration: Ceci est une conséquence directe de [8], (théorème 2). □

Si $|\cdot|$ provient d'une anti-involution (positive) \star sur $D \otimes \mathbb{R}$, on note H_{inf}^{\star} pour $H_{\text{inf}}^{|\cdot|}$.

Proposition 6.3 *Pour toute anti-involution positive \star*

$$H_{\text{inf}}^{\star}(A) = \text{nr}(AA^{\star})^{1/2de}$$

où $A^{\star} \in \text{Mat}_{NM}(D \otimes \mathbb{R})$ est obtenue en transposant A et en appliquant \star à chacun de ses coefficients tandis que nr est la norme réduite $\text{Mat}_{MM}(D \otimes \mathbb{R}) \rightarrow \mathbb{R}$.

Démonstration: Nous rappelons que le produit scalaire associé à la norme provenant de \star est donné par $\langle x, y \rangle = \text{Tr}(x^{\star}y)$ pour $x, y \in D \otimes \mathbb{R}$. Nous avons alors $\langle ax, y \rangle = \langle x, a^{\star}y \rangle$ pour tout $a \in D \otimes \mathbb{R}$ et nous en déduisons que

$$\langle AX, Y \rangle = \langle X, A^{\star}Y \rangle$$

pour tous $X \in (D \otimes \mathbb{R})^N$ et $Y \in (D \otimes \mathbb{R})^M$; la matrice A^{\star} induit donc l'adjoint ${}^t f$. Il suit que

$$\det(f \circ {}^t f) = N(AA^{\star}),$$

où N est la norme $\text{Mat}_{MM}(D \otimes \mathbb{R}) \rightarrow \mathbb{R}$ de la représentation régulière à gauche. D'après [12], (9.17) (p. 119) nous trouvons

$$N(AA^*) = \text{nr}(AA^*)^d,$$

ce qui montre le résultat car $[D : \mathbb{Q}] = d^2e$. □

Remarquons que tous les résultats de cette partie sont donnés pour un sous-espace vectoriel à droite de D^N et une matrice sur D avec des lignes D -linéairement indépendantes à gauche. Évidemment des résultats analogues existent pour un sous-espace vectoriel à gauche V de D^N qui peut être décrit comme espace des solutions d'un système d'équations linéaires de la forme $XA = 0$, si X est un vecteur ligne de D^N et A une matrice de $\text{Mat}_{NM}(D)$ avec des colonnes D -linéairement indépendantes à droite, où $M = N - \dim V$. En fait, le rang à gauche des lignes coïncide avec le rang à droite des colonnes.

Ainsi pour tout réseau Λ de D et toute norme euclidienne $|\cdot|$ sur $D \otimes \mathbb{R}$ nous posons

$$H^{\Lambda, |\cdot|}(V) = H^{\Lambda, |\cdot|}(A) = H_{\text{fin}}^{\Lambda}(A)H_{\text{inf}}^{|\cdot|}(A),$$

où

$$H_{\text{fin}}^{\Lambda}(A) = [\Lambda^N A : \Lambda^M]^{1/[D:\mathbb{Q}]}$$

et

$$H_{\text{inf}}^{|\cdot|}(A) = \det(f \circ {}^t f)^{1/2[D:\mathbb{Q}]}$$

avec $f: (D \otimes \mathbb{R})^N \rightarrow (D \otimes \mathbb{R})^M$ induite par A . Nous avons donc *a priori* deux façons de définir la hauteur d'une matrice. Ceci ne conduit à aucune ambiguïté puisqu'une seule est définie si les nombres de lignes et de colonnes diffèrent et que les deux définitions coïncident si A est une matrice carrée. En effet, dans ce cas, $V = \{0\}$ est le sous-espace à la fois à droite et à gauche correspondant à A , ce qui donne 1 pour sa hauteur.

Les propositions 6.2 et 6.3 peuvent bien entendu être adaptées dans ce cadre.

7 Dualité

Si V est un sous-espace à droite de D^N , nous définissons son orthogonal comme le sous-espace à gauche

$$V^{\perp} = \{x \in D^N \mid x \bullet y = 0 \text{ pour tout } y \in V\}$$

où, pour $x, y \in D^N$, nous notons $x \bullet y = \sum_{i=1}^N x_i y_i$.

Le résultat principal de cette partie est le suivant.

Théorème 7.1 *Si \mathcal{O} est un ordre maximal de D et \star une anti-involution positive sur $D \otimes \mathbb{R}$ alors*

$$H^{\mathcal{O}, \star}(V) = H^{\mathcal{O}, \star}(V^{\perp}).$$

Pour la démonstration, nous suivons la méthode introduite dans [9]. Pour commencer nous établissons le fait ci-dessous, auquel il était fait allusion dans cet article. Tous les anneaux considérés sont unitaires.

Proposition 7.2 *Soit R un anneau fini dont tous les idéaux à gauche et tous les idéaux à droite sont principaux. Pour tout élément r de R , on a $\text{Card}(Rr) = \text{Card}(rR)$.*

En raison de cette propriété, nous qualifierons les anneaux vérifiant l’hypothèse ci-dessus de symétriques, comme dans [9]. Pour démontrer la proposition, nous nous basons sur le théorème de structure suivant.

Proposition 7.3 *Soit R un anneau fini dans lequel tout idéal bilatère peut s’écrire à la fois rR et Rs pour $r, s \in R$. Il existe un isomorphisme de la forme*

$$R \simeq \prod_{i=1}^k \text{Mat}_{n_i, n_i}(R_i)$$

où k et les n_i sont des entiers naturels tandis que R_i est un anneau fini local dans lequel tout idéal à gauche ou à droite est à la fois principal et bilatère.

Démonstration: Ceci est par exemple conséquence du résultat principal de [4], où la structure des R_i est décrite bien plus précisément. □

Remarquons, sans le prouver, que l’on peut en fait supposer seulement que tout idéal bilatère est principal comme idéal à gauche et obtenir la même conclusion.

Démonstration de la Proposition 7.2: Dans la décomposition de la proposition précédente, la propriété de symétrie est vraie pour chacun des R_i puisque si $r \in R_i$ l’ensemble $R_i r$ est un idéal à droite donc contient rR_i qui, étant lui un idéal à gauche, contient $R_i r$ et donc $R_i r = rR_i$. Nous en déduisons que les anneaux $\text{Mat}_{n_i, n_i}(R_i)$ satisfont également la symétrie d’après le corollaire à la proposition 1 de [9]. Le résultat suit alors facilement par produit. □

Nous entamons à présent la démonstration du théorème 7.1. Nous notons L la dimension de V et $M = N - L$. Il est clair que si $\sigma: D^N \rightarrow D^N$ est une permutation des coordonnées alors $\sigma(V)^\perp = \sigma(V^\perp)$. Par suite, en vertu du lemme 2.1, nous pouvons montrer le résultat après une telle permutation. Aussi pouvons-nous supposer que V est défini par une matrice A de la forme $A = (aI_M \ C)$ où $a > 0$ est un élément de \mathbb{Z} et C une matrice de $\text{Mat}_{ML}(\mathcal{O})$. Nous avons donc

$$\begin{aligned} V &= \{X \in D^N \mid AX = 0\} \\ &= \{(X_1, X_2) \in D^M \times D^L \mid aX_1 + CX_2 = 0\} \\ &= \{(-a^{-1}CX_2, X_2) \mid X_2 \in D^L\}. \end{aligned}$$

Par conséquent, nous pouvons calculer l’orthogonal comme

$$\begin{aligned} V^\perp &= \{(Y_1, Y_2) \in D^M \times D^L \mid -Y_1 a^{-1}CX_2 + Y_2 X_2 = 0, \text{ pour tout } X_2 \in D^L\} \\ &= \{(Y_1, Y_2) \in D^M \times D^L \mid -a^{-1}Y_1 C + Y_2 = 0\} \\ &= \{Y \in D^N \mid YB = 0\} \end{aligned}$$

si nous posons

$$B = \begin{pmatrix} -C \\ aI_L \end{pmatrix} \in \text{Mat}_{NL}(\mathcal{O})$$

(dans tous ces calculs X, X_1, X_2 sont vus comme des vecteurs colonnes et Y, Y_1, Y_2 comme des vecteurs lignes).

Il nous reste donc à établir l'égalité $H^{\mathcal{O},\star}(A) = H^{\mathcal{O},\star}(B)$. Elle résultera, comme dans [9], d'une comparaison séparée des parties finies et infinies, qui fait l'objet des deux lemmes suivants.

Lemme 7.1 *Nous avons*

$$H_{\text{inf}}^{\star}(A) = a^{M-L}H_{\text{inf}}^{\star}(B).$$

Démonstration: En vertu de la proposition 6.3 (et de son image miroir), nous devons montrer $\text{nr}(AA^{\star}) = a^{2de(M-L)}\text{nr}(B^{\star}B)$ autrement dit

$$\text{nr}(a^2I_M + CC^{\star}) = \text{nr}(a^2)^{M-L}\text{nr}(a^2I_L + C^{\star}C).$$

Nous allons établir cette identité pour toute matrice C de $\text{Mat}_{ML}(D \otimes \mathbb{R})$. Faisons les réductions suivantes : d'une part, en remplaçant C par $a^{-1}C$, nous pouvons supposer $a = 1$; d'autre part, en échangeant le rôle de C et de C^{\star} nous pouvons également nous restreindre au cas où $M \geq L$.

Ceci fait, bâtissons une matrice \tilde{C} carrée d'ordre M en ajoutant à C des colonnes nulles (les $M - L$ dernières, disons). De la sorte, $I_M + \tilde{C}\tilde{C}^{\star} = I_M + CC^{\star}$ tandis que $I_M + \tilde{C}^{\star}\tilde{C}$ est une matrice diagonale par blocs, formée des blocs I_{M-L} et $I_L + C^{\star}C$. Ainsi l'identité pour \tilde{C} entraîne l'identité pour C ; en d'autres termes, il suffit de la montrer lorsque $M = L$ c'est-à-dire

$$\text{nr}(I_M + CC^{\star}) = \text{nr}(I_M + C^{\star}C)$$

pour C carrée d'ordre M . Si C est inversible, ceci est clair car alors

$$C^{-1}(I_M + CC^{\star})C = I_M + C^{\star}C.$$

Si nous écrivons $C = \sum_{i=1}^L x_i C_i$ dans une certaine base (C_1, \dots, C_L) du \mathbb{R} -espace vectoriel $\text{Mat}_{MM}(D \otimes \mathbb{R})$ alors les deux membres de la relation à établir sont des polynômes en les x_i . Nous avons donc une identité polynomiale vraie pour les matrices inversibles. Elle l'est donc en général puisque l'ensemble de ces matrices est dense dans $\text{Mat}_{MM}(D \otimes \mathbb{R})$ (par exemple parce que cet anneau s'écrit comme produit d'anneaux de matrices sur \mathbb{R}, \mathbb{C} ou \mathbb{H}). □

Lemme 7.2 *Nous avons*

$$H_{\text{fin}}^{\mathcal{O}}(A) = a^{L-M}H_{\text{fin}}^{\mathcal{O}}(B).$$

Démonstration: D'après les définitions, nous devons montrer

$$[\mathcal{O}^M : A\mathcal{O}^N] = a^{[D:\mathbb{Q}](M-L)}[\mathcal{O}^L : \mathcal{O}^N B].$$

Nous introduisons l'anneau fini $R = \mathcal{O}/a\mathcal{O}$. Le quotient $\mathcal{O}^M/A\mathcal{O}^N$ est en bijection avec R^M/CR^L . Ainsi

$$[\mathcal{O}^M : A\mathcal{O}^N] = \text{Card}(R^M/CR^L) = a^{[D:\mathbb{Q}]M}/\text{Card}(CR^L)$$

et de même

$$[\mathcal{O}^L : \mathcal{O}^N B] = \text{Card}(R^L/R^M C) = a^{[D:\mathbb{Q}]L}/\text{Card}(R^M C).$$

Pour montrer $\text{Card}(CR^L) = \text{Card}(R^M C)$, il suffit (voir proposition 1 de [9]) de montrer que R est un anneau symétrique. Or nous avons un isomorphisme

$$R \simeq \prod_p \mathcal{O}/p^{e_p} \mathcal{O} \simeq \prod_p \mathcal{O}_p/p^{e_p} \mathcal{O}_p$$

où e_p est la valuation p -adique de a . Par conséquent puisque, \mathcal{O} étant maximal, tous les idéaux à droite ou à gauche de \mathcal{O}_p sont principaux, il en va de même de R et le résultat est acquis par la proposition 7.2. □

La différence principale avec [9] vient du fait que l’involution \star ne fixe pas D ni, *a fortiori*, \mathcal{O} . Cela nous oblige à travailler simultanément avec des espaces à droite et à gauche. Si $D^\star = D$, l’on évite ceci en considérant comme orthogonal de V le sous-espace à droite $(V^\perp)^\star$. Cependant, le théorème de dualité ne s’écrit agréablement que si $\mathcal{O}^\star = \mathcal{O}$ puisque $H^{\mathcal{O},\star}((V^\perp)^\star) = H^{\mathcal{O},\star}(V^\perp)$ en général.

La dualité nous donne une seconde interprétation matricielle de la hauteur d’un sous-espace.

Corollaire 7.1 *Soit V un sous-espace vectoriel à droite non nul sur D de D^N , \mathcal{O} un ordre maximal de D et \star une anti-involution positive sur $D \otimes \mathbb{R}$. Alors*

$$H^{\mathcal{O},\star}(V) = H^{\mathcal{O},\star}(B)$$

dès que B est une matrice dont les colonnes forment une base de V .

Clairement, si V est un sous-espace à gauche, l’identité reste vraie si B est une matrice dont les lignes forment une base de V .

Démonstration: Comme l’orthogonal V^\perp de V se compose des solutions $Y \in D^N$ (comme vecteurs lignes) de $YB = 0$, on a $H^{\mathcal{O},\star}(B) = H^{\mathcal{O},\star}(V^\perp)$ d’après la proposition 6.1. En appliquant le théorème 7.1, nous trouvons que

$$H^{\mathcal{O},\star}(B) = H^{\mathcal{O},\star}(V^\perp) = H^{\mathcal{O},\star}(V)$$

comme prévu. □

Rappelons que la formule de dualité est en général fautive pour un ordre non maximal. Des exemples explicites se trouvent dans [9] que l’on pourra consulter pour plus de détails.

En revanche, si l’on accepte de changer de hauteur entre V et V^\perp , nous pouvons écrire, dans le prolongement de [9], (proposition 4), une relation de dualité pour tout couple $(\Lambda, |\cdot|)$. Nous introduisons les définitions suivantes : si Λ est un réseau de D , nous posons

$$\Lambda' = \{x \in D \mid \text{Tr}(x\Lambda) \subset \mathbb{Z}\}$$

tandis que, si $|\cdot|$ est une norme euclidienne sur $D \otimes \mathbb{R}$, nous écrivons pour $x \in D \otimes \mathbb{R}$

$$|x|' = \sup\{\text{Tr}(xy) \mid y \in D \otimes \mathbb{R} \text{ et } |y| = 1\}.$$

En utilisant le fait que la forme trace $D \times D \rightarrow \mathbb{Q}$ est non dégénérée, on montre aisément que Λ' est un réseau de D et que $|\cdot|'$ définit une norme euclidienne sur $D \otimes \mathbb{R}$: si (e_1, \dots, e_n) est une base de Λ (resp. une base de $D \otimes \mathbb{R}$ orthonormée pour $|\cdot|$), on considère la base duale (e'_1, \dots, e'_n) telle que $\text{Tr}(e_i e'_j) = \delta_{ij}$ et l’on constate immédiatement qu’elle forme une base de Λ' (resp. une base de $D \otimes \mathbb{R}$ orthonormée pour $|\cdot|'$).

Il est alors possible de montrer

$$H^{\Lambda',|\cdot|'}(V^\perp) = H^{\Lambda,|\cdot|}(V).$$

Cette formule s’obtient par exemple en copiant la démarche précédente avec les matrices A , B et C et en utilisant les représentations données par les bases ci-dessus à la manière de la démonstration de [9, proposition 4].

Signalons pour conclure que nous pourrions aussi retrouver le théorème 7.1 à l'aide de cette égalité. En effet, si la norme euclidienne $|\cdot|$ provient d'une anti-involution \star alors on vérifie sans peine $|\cdot|' = |\cdot|$. Lorsque \mathcal{O} est un ordre maximal de D , il n'y a pas en général égalité entre \mathcal{O}' et \mathcal{O} mais il nous suffit de noter que \mathcal{O}' est un \mathcal{O} -module à gauche et à droite. Ainsi, si les deux conditions sont simultanément réunies, on a $H^{\mathcal{O}',\star} = H^{\mathcal{O},\star}$ en utilisant la proposition 4.1 où l'on prend comme module $\Omega = \mathcal{O}'$ et le produit scalaire $\langle \cdot, \cdot \rangle$ défini par $\langle \alpha, \beta \rangle = \text{Tr}(\alpha^* \beta)$ pour $\alpha, \beta \in \Omega \otimes \mathbb{R} = D \otimes \mathbb{R}$.

8 Lemme de Siegel II

Comme dans la partie 3 on note D un corps de dimension n sur \mathbb{Q} et τ_m la racine m -ième du volume (par rapport à la norme euclidienne usuelle) de la boule unité dans \mathbb{R}^m .

Nous définissons maintenant la hauteur des vecteurs de D^N . Comme d'habitude, cette notion sera double. Si nous considérons D^N comme D -espace à droite alors nous voyons un élément non nul X de D^N comme un vecteur colonne et nous définissons sa hauteur en tant que tel (hauteur d'une matrice $N \times 1$ de rang 1). Ainsi il est clair que $H^{\Lambda,|\cdot|}(Xx) = H^{\Lambda,|\cdot|}(X)$ pour tout $x \neq 0$ de D ce qui donne une hauteur projective des vecteurs. Symétriquement, on définit la hauteur d'un vecteur non nul X du D -espace à gauche D^N comme la hauteur d'une matrice ligne et l'on a $H^{\Lambda,|\cdot|}(xX) = H^{\Lambda,|\cdot|}(X)$ pour tout $x \neq 0$ de D . Dans les énoncés des propositions de ce paragraphe, nous ne précisons pas si V est un espace à droite ou à gauche étant entendu que de cela dépend la notion de hauteur que nous utilisons pour les vecteurs.

Proposition 8.1 *Soient L et N des entiers naturels tels que $0 < L < N$ puis \mathcal{O} un ordre maximal de D et \star une anti-involution positive sur $D \otimes \mathbb{R}$. Alors tout sous-espace vectoriel V sur D de D^N de dimension L admet une base formée d'éléments X_1, \dots, X_L de \mathcal{O}^N telle que*

$$H^{\mathcal{O},\star}(X_1) \cdots H^{\mathcal{O},\star}(X_L) \leq \left(\frac{2\text{vol}(\mathcal{O})^{1/n}}{\sqrt{n}\tau_{nL}} \right)^L H^{\mathcal{O},\star}(V).$$

Ce résultat était démontré pour le cas des quaternions dans [7]. C'est une généralisation du lemme de Siegel bien connu sur les corps de nombres, démontré par E. Bombieri et J. Vaaler [2], (théorème 9) et dont J. Thunder a donné une version un peu plus fine [17], (théorème 3). C'est d'ailleurs la méthode de ce dernier article que nous avons suivie dans notre démonstration du théorème 3.1.

La proposition 8.1 est une conséquence directe du théorème 3.1 et du lemme suivant.

Lemme 8.1 *Pour tout $X \in \mathcal{O}^N$ on a*

$$H^{\mathcal{O},\star}(X) \leq \frac{1}{\sqrt{n}} |X|_N.$$

Démonstration: Nous supposons que X est un vecteur colonne, c'est-à-dire, que D^N est un D -espace à droite. La démonstration serait identique pour X un vecteur ligne du D -espace à gauche D^N .

Si x_1, \dots, x_N sont les composantes de X , on a par définition

$$H_{\text{fin}}^{\mathcal{O}}(X)^n = [\mathcal{O}x_1 + \cdots + \mathcal{O}x_N : \mathcal{O}] = 1/[\mathcal{O} : \mathcal{O}x_1 + \cdots + \mathcal{O}x_N] \leq 1$$

puisque x_1, \dots, x_N appartiennent à \mathcal{O} . En vertu de l'image miroir de la proposition 6.3 et de la dernière remarque de sa preuve, nous avons

$$H_{\text{inf}}^*(X)^n = \text{nr}(X^*X)^{d/2} = N(X^*X)^{1/2}.$$

La norme N est donnée par $N(X^*X) = \det \varrho(X^*X)$, où ϱ est la représentation à droite définie par rapport à une \mathbb{R} -base de $D \otimes \mathbb{R}$. Nous choisissons une base qui est orthonormale par rapport au produit scalaire associé à la norme $|x|^2 = \text{Tr}(x^*x)$, $x \in D \otimes \mathbb{R}$. Ainsi, si $f: D \otimes \mathbb{R} \rightarrow (D \otimes \mathbb{R})^N$ est l'application induite par X , on a $N(X^*X) = \det({}^t f \circ f) = \det {}^t \varrho(X)\varrho(X)$ et alors $\varrho(X^*X) = {}^t \varrho(X)\varrho(X)$ est une matrice symétrique définie positive. Si nous écrivons que la moyenne géométrique de ses valeurs propres est inférieure à leur moyenne arithmétique, nous obtenons

$$N(X^*X) = \det \varrho(X^*X) \leq (\text{trace}(\varrho(X^*X))/n)^n = (\text{Tr}(X^*X)/n)^n.$$

Par conséquent

$$H^{\mathcal{O},*}(X) \leq (\text{Tr}(X^*X)/n)^{1/2} = \frac{1}{\sqrt{n}}|X|_N$$

comme prévu. □

La borne suivante montre que dans la majoration de la proposition 8.1 la dépendance de la hauteur de l'espace V est optimale pour tout espace V dans D^N (ce qui améliore la proposition 3.2). C'est une généralisation de [8](proposition 3).

Proposition 8.2 *Soient L et N des entiers naturels tels que $0 < L < N$ puis \mathcal{O} un ordre maximal de D et \star une anti-involution positive sur $D \otimes \mathbb{R}$. Alors pour tout sous-espace vectoriel V sur D de D^N de dimension L et toute base de V formée d'éléments X_1, \dots, X_L de \mathcal{O}^N on a*

$$H^{\mathcal{O},*}(X_1) \cdots H^{\mathcal{O},*}(X_L) \geq H^{\mathcal{O},*}(V).$$

Cette proposition se déduit du corollaire 7.1 et du lemme suivant.

Lemme 8.2 *Soient L et N des entiers naturels tels que $1 \leq L \leq N$ puis \mathcal{O} un ordre maximal de D et \star une anti-involution positive sur $D \otimes \mathbb{R}$. Alors pour toute matrice B de $\text{Mat}_{NL}(D)$ de rang L avec des colonnes X_1, \dots, X_L nous avons*

$$H^{\mathcal{O},*}(B) \leq H^{\mathcal{O},*}(X_1) \cdots H^{\mathcal{O},*}(X_L).$$

Démonstration: Nous pouvons supposer que les coefficients de B sont dans \mathcal{O} . Nous écrivons $B = (X_1 \ B_1)$, où $B_1 \in \text{Mat}_{N,L-1}(\mathcal{O})$ a pour colonnes X_2, \dots, X_L . Nous voulons montrer que

$$H^{\mathcal{O},*}(B) \leq H^{\mathcal{O},*}(X_1)H^{\mathcal{O},*}(B_1). \tag{3}$$

Avec ϱ comme dans la preuve de la proposition 8.1 nous trouvons que $\varrho(B^*B) = {}^t \varrho(B)\varrho(B)$ est une matrice symétrique définie positive et, en utilisant une inégalité de Fischer (voir [3]), nous obtenons

$$\det \varrho(B^*B) = \det \begin{pmatrix} \varrho(X_1^*X_1) & \varrho(X_1^*B_1) \\ \varrho(B_1^*X_1) & \varrho(B_1^*B_1) \end{pmatrix} \leq \det \varrho(X_1^*X_1) \det \varrho(B_1^*B_1).$$

Donc

$$H_{\text{inf}}^*(B) \leq N(X_1^*X_1)^{1/2n}N(B_1^*B_1)^{1/2n} = H_{\text{inf}}^*(X_1)H_{\text{inf}}^*(B_1).$$

Ensuite, si x_1, \dots, x_N désignent les composantes de X_1 , nous notons $u_p = \text{pgfcd}_p(x_1, \dots, x_N)$ le plus grand facteur droit commun de x_1, \dots, x_N dans \mathcal{O}_p ainsi que $U_p \in \text{Mat}_{L-1, L-1}(\mathcal{O}_p)$ le pgfcd_p des mineurs d'ordre $L - 1$ de B_1 . Formons la matrice

$$R_p = \begin{pmatrix} u_p & 0 \\ 0 & U_p \end{pmatrix} \in \text{Mat}_{LL}(\mathcal{O}_p).$$

Nous prétendons que $\mathcal{O}_p^N B \subset \mathcal{O}_p^L R_p$. En effet, rappelons que $B = (X_1 \ B_1)$, d'où $\mathcal{O}_p^N B \subset \mathcal{O}_p^N X_1 \oplus \mathcal{O}_p^N B_1 \subset \mathcal{O}^L$. Par définition de u_p , nous avons $\mathcal{O}_p^N X_1 = \mathcal{O}_p x_1 + \dots + \mathcal{O}_p x_N = \mathcal{O}_p u_p$. De plus, la duale de la formule (2) de la partie 6 dit que $\mathcal{O}_p^N B_1 = \mathcal{O}_p^{L-1} U_p$. Par conséquent, $\mathcal{O}_p^N B \subset \mathcal{O}_p u_p \oplus \mathcal{O}_p^{L-1} U_p = \mathcal{O}_p^L R_p$.

Comme $\mathcal{O}_p^N B = \mathcal{O}_p^L \Delta_p$ pour Δ_p le pgfcd_p des mineurs d'ordre L de B (en utilisant de nouveau la formule (2)), la matrice R_p divise Δ_p . En prenant le produit sur tous les nombres premiers p et par la proposition 6.2 miroir nous arrivons à

$$H_{\text{fin}}^{\mathcal{O}}(B)^{de} \leq \prod_p |\text{nr}(R_p)|_p = \prod_p |\text{nr}(u_p)|_p |\text{nr}(U_p)|_p = H_{\text{fin}}^{\mathcal{O}}(X_1)^{de} H_{\text{fin}}^{\mathcal{O}}(B_1)^{de}.$$

Ceci montre (3) et le lemme suit par l'application répétée de cette inégalité à $B_1 = (X_2 \ B_2)$, puis à B_2 et ainsi de suite. □

Bien entendu, nous pourrions également énoncer le lemme pour une matrice B de $\text{Mat}_{LN}(D)$ de rang L avec des lignes X_1, \dots, X_L .

Terminons par quelques estimations. Si nous écrivons le majorant de la proposition 8.1 sous la forme $\kappa_{n,L} \text{vol}(\mathcal{O})^{L/n} H^{\mathcal{O},*}(V)$ alors on a (pour $nL > 1$)

$$\sqrt{\frac{2L}{\pi e}}^L \leq \kappa_{n,L} \leq \sqrt{\frac{2L}{\pi}}^L.$$

De plus, les propositions 8.1 et 8.2 donnent la minoration

$$\text{vol}(\mathcal{O}) \geq \frac{n^{n/2}}{2^n} \tau_{nL}^n = \kappa_{n,L}^{-n/L}$$

(indépendante de l'involution positive qui sert à définir $\text{vol}(\mathcal{O})$). La minoration est optimale pour $L = 1$ et si l'on utilise l'encadrement précédent, il vient (si $n > 1$)

$$\text{vol}(\mathcal{O}) \geq \sqrt{\frac{\pi}{2}}^n.$$

Nous obtenons donc une minoration de même nature que celles connues pour les corps de nombres (dont nous retrouvons une version faible).

9 Variétés de drapeaux

Cette partie vise à interpréter la hauteur que nous avons introduite dans le cadre général présenté par J. Franke, Y. Manin et Y. Tschinkel dans [5], (p. 426). Ces auteurs construisent une hauteur sur un quotient $P \backslash G$, où G est un groupe algébrique linéaire sur \mathbb{Q} et P un sous-groupe parabolique de G , à l'aide d'un caractère χ de P sur \mathbb{Q} et d'une famille de sous-groupes compacts maximaux K_p de $G(\mathbb{Q}_p)$ où p parcourt les places de \mathbb{Q} .

Étant donné un corps D de dimension finie sur \mathbb{Q} , un ordre maximal \mathcal{O} de D , une anti-involution positive \star de $D \otimes \mathbb{R}$ et des entiers naturels $M \leq N$, nous allons montrer comment choisir de manière naturelle G, P, χ et des K_p de sorte que d'une part $(P \backslash G)(\mathbb{Q})$ s'identifie à l'ensemble des sous-espaces vectoriels à droite sur D de D^N de codimension M et d'autre part la hauteur donnée par χ et les K_p sur celui-ci coïncide avec une puissance de $H^{\mathcal{O}, \star}$ (voir proposition 9.1).

Nous notons E l'espace vectoriel à droite D^N et V_0 le sous-espace engendré par les $N - M$ premiers vecteurs de la base canonique. Nous utilisons V_0 comme sous-espace standard de codimension M . Nous considérons alors l'application

$$\begin{aligned} \text{Aut}_D(E) &\longrightarrow \{\text{sous-espaces de } E\} \\ \varphi &\longmapsto \varphi^{-1}(V_0). \end{aligned}$$

Il est clair que l'image de cette application coïncide avec l'ensemble des sous-espaces de codimension M et que φ et φ' ont même image si et seulement si $\varphi' \circ \varphi^{-1}$ appartient au stabilisateur de V_0 . Ainsi nous pouvons réaliser l'ensemble qui nous intéresse comme $\text{Stab}(V_0) \backslash \text{Aut}_D(E)$.

Nous écrivons donc

$$G = \text{Aut}_D(E)$$

avec sa structure de groupe algébrique sur \mathbb{Q} : $\text{Aut}_D(E)$ est le groupe $G(\mathbb{Q})$ des points rationnels et, pour tout corps commutatif K de caractéristique nulle, $G(K) = \text{Aut}_{D \otimes K}(E \otimes K)$. Nous désignons ensuite par $P = \text{Stab}_G(V_0)$ le sous-groupe de G défini par la condition $\varphi(V_0) = V_0$. C'est un sous-groupe parabolique de G défini sur \mathbb{Q} . Nous formons $W = P \backslash G$ la variété de drapeaux généralisée correspondante.

Nous définissons maintenant un caractère χ de P . Nous notons $\pi : E \rightarrow E/V_0$. Comme tout élément de $P(\mathbb{Q})$ laisse stable V_0 , nous avons une application naturelle

$$n : P(\mathbb{Q}) \longrightarrow \text{Aut}_D(E/V_0)$$

caractérisée par $\pi \circ p = n(p) \circ \pi$ si $p \in P(\mathbb{Q})$. Par composition avec la norme réduite $\text{nr} : \text{Aut}_D(E/V_0) \rightarrow \mathbb{Q}^\times$ nous obtenons $\chi : P(\mathbb{Q}) \rightarrow \mathbb{Q}^\times$ dont on vérifie facilement qu'il est un caractère du groupe algébrique P .

Le caractère χ définit un faisceau inversible \mathcal{L}_χ sur W de la façon suivante : si U est un ouvert de W d'image réciproque U' dans G

$$\Gamma(U, \mathcal{L}_\chi) = \{f \in \Gamma(U', \mathcal{O}_G) \mid f(pg) = \chi(p)f(g) \text{ pour tous } p \in P, g \in G\}$$

(voir [5], (2.1)). Dans le cas présent, nous savons décrire une famille génératrice de sections globales de \mathcal{L}_χ . Pour tout $\psi \in \text{Hom}_D(E/V_0, E)$, nous considérons

$$\begin{aligned} f_\psi : G(\mathbb{Q}) &\longrightarrow \mathbb{Q} \\ g &\longmapsto \text{nr}(\pi \circ g \circ \psi) \end{aligned}$$

avec la norme réduite $\text{nr} : \text{End}_D(E/V_0) \rightarrow \mathbb{Q}$. Encore une fois, cette application est donnée par un polynôme donc provient d'une section $f_\psi \in \Gamma(G, \mathcal{O}_G)$. De plus

$$f_\psi(pg) = \text{nr}(\pi \circ p \circ g \circ \psi) = \text{nr}(n(p) \circ \pi \circ g \circ \psi) = \chi(p)f_\psi(g).$$

Ainsi f_ψ donne naissance à une section $s_\psi \in \Gamma(W, \mathcal{L}_\chi)$. Si U_ψ est l'ouvert de W correspondant aux sous-espaces V de E tels que $V \oplus \psi(E/V_0) = E$ alors s_ψ engendre la restriction de \mathcal{L}_χ à U_ψ . En effet, si $g \in G(\mathbb{Q})$ avec $g^{-1}(V_0) = V \in U_\psi$ nous trouvons $\text{Ker}(\pi \circ g \circ \psi) = \psi^{-1}(V) = 0$ donc $\pi \circ g \circ \psi$ est une bijection d'où $f_\psi(g) \neq 0$.

Il nous reste à choisir les sous-groupes compacts maximaux K_p . Puisque $E = D^N$ contient \mathcal{O}^N nous posons pour p une place finie de \mathbb{Q} (rappelons que $D_p = D \otimes \mathbb{Q}_p$ et $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$)

$$K_p = \text{Aut}_{\mathcal{O}_p}(\mathcal{O}_p^N) \subset \text{Aut}_{D_p}(E \otimes D_p) = G(\mathbb{Q}_p).$$

Si $p = \infty$, l’anti-involution $\star : D \otimes \mathbb{R} \rightarrow D \otimes \mathbb{R}$ munit $E \otimes_{\mathbb{Q}} \mathbb{R}$ d’un produit scalaire et nous posons

$$K_\infty = \{\text{isométries de } G(\mathbb{R})\} \subset G(\mathbb{R}) = \text{Aut}_{D \otimes \mathbb{R}}(E \otimes \mathbb{R}).$$

Nous verrons dans la preuve ci-dessous que ces sous-groupes vérifient bien la condition $G(\mathbb{Q}_p) = P(\mathbb{Q}_p)K_p$ pour tout p nécessaire pour définir la hauteur (en fait ils vérifient même la condition plus forte $G(\mathbb{Q}_p) = P_0(\mathbb{Q}_p)K_p$ pour un sous-groupe parabolique minimal P_0 comme dans [5], (p. 426) mais P_0 ne joue absolument aucun rôle ici).

Comme prévu, le caractère χ et les sous-groupes K_p permettent de bâtir une hauteur sur $W(\mathbb{Q})$. Soit donc $V \in W(\mathbb{Q})$ un sous-espace de E de codimension M . Nous choisissons $\psi \in \text{Hom}_D(E/V_0, E)$ tel que $V \in U_\psi$ et, pour chaque place p , un élément $\varphi_p \in K_p$ tel que

$$\varphi_p^{-1}(V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_p) = V \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

Alors la hauteur de V obtenue est

$$H_{\text{FMT}}^{\mathcal{O}, \star}(V) = \prod_p |\text{nr}(\pi \circ \varphi_p \circ \psi)|_p^{-1}$$

où le produit porte sur toutes les places de \mathbb{Q} et en utilisant la norme réduite $\text{nr} : \text{Aut}_{D \otimes \mathbb{Q}_p}((E/V_0) \otimes \mathbb{Q}_p) \rightarrow \mathbb{Q}_p^\times$. Ce nombre ne dépend pas des choix de ψ ou des φ_p .

Nous rappelons que nous avons écrit $[D : \mathbb{Q}] = d^2e$.

Proposition 9.1 *Avec les définitions précédentes,*

$$H_{\text{FMT}}^{\mathcal{O}, \star}(V) = H^{\mathcal{O}, \star}(V)^{de}.$$

Démonstration: Nous commençons par remarquer que les deux membres de l’égalité à prouver sont invariants par une permutation σ des coordonnées de D^N . Pour le membre de droite, cela résulte du lemme 2.1. Afin de montrer $H_{\text{FMT}}^{\mathcal{O}, \star}(\sigma(V)) = H_{\text{FMT}}^{\mathcal{O}, \star}(V)$, nous notons que si ψ et (φ_p) peuvent être utilisés pour calculer $H_{\text{FMT}}^{\mathcal{O}, \star}(V)$ c’est-à-dire

$$V \oplus \psi(E/V_0) = E \quad \text{et} \quad \varphi_p^{-1}(V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_p) = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

alors

$$\sigma(V) \oplus (\sigma \circ \psi)(E/V_0) = E \quad \text{et} \quad (\varphi_p \circ \sigma^{-1})^{-1}(V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_p) = \sigma(V) \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

Maintenant, en voyant σ dans $\text{Aut}_D(E)$, l’on vérifie immédiatement que cet élément appartient à K_p pour tout p . Ainsi $\sigma \circ \psi$ et $(\varphi_p \circ \sigma^{-1})$ permettent de calculer $H_{\text{FMT}}^{\mathcal{O}, \star}(\sigma(V))$ et σ disparaît clairement de la formule.

Grâce à cette réduction, nous pouvons supposer que la projection de $V \subset D^N$ sur les $N - M$ premières coordonnées est un isomorphisme. Autrement dit, si nous identifions E/V_0 avec D^M de sorte que $\pi : D^N \rightarrow D^M$ est la projection sur les dernières

coordonnées et définissons ψ comme l'injection $D^M \rightarrow D^N$ de ces mêmes coordonnées, nous supposons $V \in U_\psi$. Concrètement, cela permet d'écrire la hauteur de la façon suivante : si pour tout p , en termes matriciels,

$$\varphi_p = \begin{pmatrix} * & * \\ * & C_p \end{pmatrix}$$

avec $C_p \in \text{Mat}_{MM}(D_p)$ alors

$$H_{\text{FMT}}^{\mathcal{O},*}(V) = \prod_p |\text{nr}(C_p)|_p^{-1}.$$

D'un autre côté, si $A \in \text{Mat}_{MN}(\mathcal{O})$ est telle que $V = \{X \in D^N \mid AX = 0\}$, alors

$$H^{\mathcal{O},*}(V)^{de} = \left(\prod_{p \neq \infty} |\text{nr}(\text{pgfgc}_p A_0)|_p \right) \text{nr}(AA^*)^{1/2}$$

d'après les résultats de la partie 6 avec les notations attenantes.

Nous allons comparer ces expressions place par place. Débutons par $p \neq \infty$. Nous notons B_p un plus grand facteur gauche commun dans $\text{Mat}_{MM}(\mathcal{O}_p)$ des mineurs maximaux A_0 de A . De cette façon, la matrice $B_p^{-1}A$ est à coefficients dans \mathcal{O}_p et induit par multiplication à gauche une application surjective $\mathcal{O}_p^N \rightarrow \mathcal{O}_p^M$. Nous pouvons choisir $x \in \mathcal{O}_p^N$ dans le noyau de cette application de sorte que x_1, \dots, x_N n'ont pas de facteur commun à droite. Cela entraîne l'existence de $a_1, \dots, a_N \in \mathcal{O}_p$ avec $a_1x_1 + \dots + a_Nx_N = 1$. Par suite, la matrice

$$\begin{pmatrix} a_1 \cdots a_N \\ B_p^{-1}A \end{pmatrix} \in \text{Mat}_{M+1,N}(\mathcal{O}_p)$$

induit encore une surjection $\mathcal{O}_p^N \rightarrow \mathcal{O}_p^{M+1}$. En itérant ce procédé, nous aboutissons à une matrice $\varphi_p \in \text{Aut}_{\mathcal{O}_p}(\mathcal{O}_p^N)$ dont les M dernières lignes forment $B_p^{-1}A$. Maintenant $\varphi_p \in K_p$ est clair et $\varphi_p^{-1}(V_0 \otimes \mathbb{Q}_p) = \{X \in D_p^N \mid B_p^{-1}AX = 0\} = V \otimes \mathbb{Q}_p$. Ainsi, nous utilisons φ_p pour calculer $H_{\text{FMT}}^{\mathcal{O},*}(V)$ et si A s'écrit par blocs $(A_1 \ A_2)$ où $A_2 \in \text{Mat}_{MM}(\mathcal{O})$ alors

$$C_p = B_p^{-1}A_2.$$

Passons au cas $p = \infty$. Remarquons que, d'après le calcul fait dans la démonstration de la proposition 6.2 (reliant A^* et f), un élément $\varphi_\infty \in \text{Mat}_{NN}(D \otimes \mathbb{R})$ est une isométrie si et seulement si $\varphi_\infty \varphi_\infty^* = I_N$. Par analogie avec le cas des places finies, nous cherchons ce φ_∞ de sorte que ses M dernières lignes s'écrivent $B_\infty^{-1}A$ avec $B_\infty \in \text{Mat}_{MM}(D \otimes \mathbb{R})$ inversible. Bien entendu, cette dernière condition équivaut à $\varphi_\infty^{-1}(V_0 \otimes \mathbb{R}) = V \otimes \mathbb{R}$. Par conséquent, si nous avons trouvé un tel φ_∞ , nous avons (en utilisant la même écriture par blocs de A que ci-dessus)

$$C_\infty = B_\infty^{-1}A_2$$

et $B_\infty^{-1}A(B_\infty^{-1}A)^* = I_M$. Cette dernière relation s'écrit clairement $AA^* = B_\infty B_\infty^*$ donc $|\text{nr}(B_\infty)| = \text{nr}(AA^*)^{1/2}$. Par suite, avec la formule du produit pour $\text{nr}(A_2)$, nous

trouvons

$$\begin{aligned}
 H_{\text{FMT}}^{\mathcal{O},\star}(V) &= \prod_p |\text{nr}(B_p)^{-1} \text{nr}(A_2)|_p^{-1} \\
 &= \prod_p |\text{nr}(B_p)|_p \\
 &= \left(\prod_{p \neq \infty} |\text{nr}(\text{pgfgc}_p A_0)|_p \right) \text{nr}(AA^\star)^{1/2}
 \end{aligned}$$

comme prévu. Il reste à vérifier l'existence de φ_∞ , ce que nous reportons au lemme suivant. □

Lemme 9.1 *Soient D et \star comme précédemment. Si $A \in \text{Mat}_{MN}(D \otimes \mathbb{R})$ est de rang M alors il existe $B \in \text{Mat}_{MM}(D \otimes \mathbb{R})$ inversible et $A' \in \text{Mat}_{N-M,N}(D \otimes \mathbb{R})$ de sorte que si Φ est la matrice $\begin{pmatrix} A' \\ B^{-1}A \end{pmatrix}$ alors $\Phi\Phi^\star = I_N$.*

Démonstration: Notons $D_{\mathbb{R}} = D \otimes \mathbb{R}$. Examinons d'abord le cas où $D_{\mathbb{R}}$ est un corps, c'est-à-dire \mathbb{R}, \mathbb{C} ou \mathbb{H} . Nous considérons le sous-espace vectoriel à gauche Y de $D_{\mathbb{R}}^N$ engendré par les lignes de A . Pour toute matrice B comme dans l'énoncé, les lignes de $B^{-1}A$ forment une base de Y et, réciproquement, toute base de Y est de cette forme. Fixer B revient donc à fixer une base de Y . Par ailleurs, la condition $\Phi\Phi^\star = I_N$ signifie que les lignes de Φ forment une base orthonormée de $D_{\mathbb{R}}^N$. Pour démontrer le lemme dans ce cas, il suffit donc de trouver une base orthonormée de $D_{\mathbb{R}}^N$ contenant une base de Y . Ceci est tout à fait classique (au moins sur \mathbb{R} ou \mathbb{C}). Nous choisissons dans Y un vecteur $v \neq 0$. Comme vv^\star est un réel strictement positif, il existe $a \in \mathbb{R}$ tel que $(av)(av)^\star = 1$. Nous utilisons av comme premier vecteur de base et choisissons les autres dans $\{y \in Y \mid yv^\star = 0\}$ qui est un sous-espace à gauche sur $D_{\mathbb{R}}$. En itérant, cela fournit une base de Y et l'on recommence avec $Y^\perp = \{x \in D_{\mathbb{R}}^N \mid \forall y \in Y \ xy^\star = 0\}$.

Dans le cas général, $(D_{\mathbb{R}}, \star)$ peut s'identifier à un produit de $\text{Mat}_m(\mathbb{K})$ où $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$ muni de la transconjugaison. Clairement, il suffit de résoudre le problème lorsque $D_{\mathbb{R}}$ est un seul de ces facteurs. Mais si $D_{\mathbb{R}} = \text{Mat}_m(\mathbb{K})$ alors $\text{Mat}_{MN}(D_{\mathbb{R}}) = \text{Mat}_{Mn, Nn}(\mathbb{K})$ et l'énoncé pour $(D_{\mathbb{R}}, M, N)$ équivaut immédiatement à celui pour (\mathbb{K}, Mn, Nn) déjà traité. □

Remarque On peut se demander si la construction de [5] peut donner, avec d'autres choix de χ et K_p , une hauteur essentiellement différente de $H^{\mathcal{O},\star}(V)$. La réponse est non. On vérifie en fait qu'une variation sur les K_p multiplie la hauteur par une quantité bornée lorsque V varie et qu'un autre choix de χ remplace la hauteur par une puissance. En effet, on a $\text{Pic}(W) = \mathbb{Z}\mathcal{L}_\chi$ pour le caractère que nous avons utilisé.

Pour être exactement dans le cadre de [5], (p. 426), il faudrait modifier le groupe $\text{Aut}_D(E)$ pour le rendre semi-simple. La façon la plus naturelle de ce faire consiste à utiliser le quotient de $\text{Aut}_D(E)$ par son radical, ici égal à son centre, isomorphe à Z^\times (Z est le centre de D). Ceci oblige à changer de caractère χ , puisque celui que nous avons employé n'est pas trivial sur le radical, mais $\chi' = \chi^N \det^{-M}$ ferait l'affaire, remplaçant la hauteur par une puissance. Si l'on ne veut pas changer de caractère, nous pouvons aussi considérer un sous-groupe plutôt qu'un quotient: il faudrait alors se limiter aux automorphismes dont la norme réduite sur Z vaut 1.

References

1. Bertrand, D., Masser, D.: Heights and degrees: a note on a paper of C. Liebendörfer and G. Rémond. *Monatsh. Math.* **148**, 19–27 (2006)
2. Bombieri, E., Vaaler, J.: On Siegel's lemma. *Invent. math.* **73**, 11–32 (1983)
3. Fischer, E.: Über den Hadamardschen Determinantensatz. *Arch. Math. (Basel)* **13**, 32–40 (1908)
4. Fisher, J.: Finite principal ideal rings. *Canad. Math. Bull.* **19**, 277–283 (1976)
5. Franke, J., Manin, Y., Tschinkel, Y.: Rational points of bounded height on Fano varieties. *Invent. math.* **95**, 421–435 (1989)
6. Liebendörfer, C.: Linear equations and heights over division algebras. Thèse. Universität Basel (2002)
7. Liebendörfer, C.: Linear equations and heights over division algebras. *J. Number Theory* **105**, 101–133 (2004)
8. Liebendörfer, C.: Heights and determinants over quaternion algebras. *Comm. Algebra* **33**, 3699–3717 (2005)
9. Liebendörfer, C., Rémond, G.: Duality of heights over quaternion algebras. *Monatsh. Math.* **145**, 61–72 (2005)
10. Martinet, J.: Perfect lattices in Euclidean spaces. Springer, Berlin Heidelberg Newyork (2003)
11. Mumford, D.: Abelian varieties. Oxford University Press, Oxford (1974)
12. Reiner, I.: Maximal orders. Academic Press, London (1975)
13. Schmidt, W.: On heights of algebraic subspaces and diophantine approximations. *Ann. Math.* **85**, 430–472 (1967)
14. Schmidt, W.: A remark on the heights of subspaces. A tribute to Paul Erdős. Cambridge University Press, Cambridge, pp. 359–360 (1990)
15. Schmidt, W.: Diophantine Approximations and Diophantine Equations. *Lecture Notes in Mathematics*, 1467. Springer, Berlin Heidelberg Newyork (1991)
16. Siegel, C.L.: Über einige Anwendungen diophantischer Approximationen. *Abh. der Preuss. Akad. der Wissenschaften. Phys.-math. Kl. Nr.1* (1929)
17. Thunder, J.: Remarks on adelic geometry of numbers. *Number theory for the millennium. III. A.* K. Peters. Natick, MA, pp. 253–259 (2002)
18. Vaaler, J.: A geometric inequality with applications to linear forms. *Pacific J. Math.* **83**, 543–553 (1979)