Rend. Sem. Mat. Univ. Padova, Vol. 130 (2013)
DOI 10.4171/RSMUP/130-9

Le théorème de Schanuel pour un corps non commutatif

Gaël Rémond (*) - Christine Zehrt-Liebendörfer (**)

Abstract - We prove a version of Schanuel's theorem in the noncommutative case : we provide an asymptotic formula for the number of one-dimensional left subspaces of D^N of height at most H, where D is a finite dimensional rational division algebra, N a positive integer and H a real number. The height, as considered in a previous paper, is defined with the help of a maximal order in D and a positive anti-involution. We give a completely explicit main term involving class number, regulator, discriminant and zeta function of D. We also compute an explicit error term.

Mathematics Subject Classification (2010). 11G50 (11R52).

Keywords. Hauteur, corps non commutatif, théorème de Schanuel, ordre maximal, anti-involution.

1. Introduction

Dans toute la suite, D est un corps de dimension finie n sur $\mathbb{Q}$. Nous fixons aussi un entier naturel $N \geq 2$. Nous cherchons à estimer, pour un réel $H \geq 0$, le nombre $\mathcal{N}(N, H)$ de sous-espaces vectoriels à gauche V de D^N de dimension 1 et de hauteur au plus H. Notre but consiste à établir la majoration

$$|\mathcal{N}(N, H) - c_{\text{princ}} H^{Nn}| \leq c_{\text{erreur}} H^{Nn-1}$$

pour des valeurs entièrement explicites de c_{princ} et c_{erreur}.

(*) Indirizzo dell'A.: Institut Fourier, UMR 5582, BP 74, 38402 Saint-Martin-d'Hères Cedex, France.
E-mail: Gael.Remond@ujf-grenoble.fr
(**) Indirizzo dell'A.: Mathematisches Institut, Universität Basel, Rheinsprung 21, 4051 Basel, Suisse.
E-mail: Christine.Zehrt@unibas.ch

Pour expliciter notre formule, il nous faut fixer la hauteur employée. Nous utilisons la hauteur considérée dans [LR]. Soient donc $\mathcal{O}$ un ordre maximal de D et $\star$ une anti-involution positive sur $D \otimes \mathbb{R}$; la positivité signifie que la formule $|x|^2 = \mathrm{Tr}(xx^\star)$ où $x \in D \otimes \mathbb{R}$ et Tr est la trace de la $\mathbb{R}$-algèbre $D \otimes \mathbb{R}$ définit une norme euclidienne $|\cdot|$ sur $D \otimes \mathbb{R}$. Les données $\mathcal{O}$ et $\star$ resteront fixées par la suite et nous leur associons toujours cette norme $|\cdot|$ sur $D \otimes \mathbb{R}$ ainsi que l'extension à l'espace $(D \otimes \mathbb{R})^m$ où m est un entier. Les éléments de $(D \otimes \mathbb{R})^m$ sont vus comme des vecteurs colonnes. Grâce à la norme sur $D \otimes \mathbb{R}$ et $(D \otimes \mathbb{R})^N$, nous définissons la hauteur d'un sous-espace (à droite ou à gauche) V de D^N de dimension M par (voir [LR])

$$H^{\mathcal{O},\star}(V) = \left(\frac{\mathrm{vol}(V \cap \mathcal{O}^N)}{\mathrm{vol}(\mathcal{O})^M} \right)^{1/n}$$

en écrivant vol pour le covolume d'un réseau dans un espace euclidien. Nous écrirons alors précisément $\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,M,H)$ pour le nombre de tels sous-espaces à gauche V qui vérifient $H^{\mathcal{O},\star}(V) \leq H$ et de même $\mathcal{N}^{\mathcal{O},\star}_{\mathrm{dte}}(N,M,H)$ pour les sous-espaces à droite.

Pour un anneau $\mathfrak{A}$ nous notons $\mathrm{Mat}_{ml}(\mathfrak{A})$ l'anneau des matrices sur $\mathfrak{A}$ avec $m \geq 1$ lignes et $\ell \geq 1$ colonnes. Décrivons ensuite les ingrédients qui apparaissent dans les constantes c_{princ} et c_{erreur}. Il s'agit tout d'abord des entiers d, r_1, r_2 et r_3 définis par l'existence d'un isomorphisme

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

où $\mathbb{H}$ est le corps des quaternions de Hamilton et r_3 est nul si d est impair (voir le lemme 1.1 de [LR] ; d^2 est la dimension de D sur son centre). Nous utilisons aussi des valeurs réelles de la fonction zêta de D donnée par

$$\zeta_D(s) = \sum_I \mathrm{Card}(\mathcal{O}/I)^{-s}$$

pour $s > 1$ où la somme porte sur les idéaux à droite non nuls de $\mathcal{O}$ (voir partie 3). Nous notons $\Delta_{D/\mathbb{Q}}$ le discriminant absolu du corps D : avec les notations précédentes, nous avons $|\Delta_{D/\mathbb{Q}}| = d^{-n}\mathrm{vol}(\mathcal{O})^2$ (voir lemme 2.3 ci-dessous).

En guise de nombre de classes, nous notons $h' = \sum_I [\mathcal{O}^\times : \mathcal{O}_g(I)^\times]$ où la somme porte sur un ensemble de représentants des classes d'isomorphie (comme $\mathcal{O}$-modules) des idéaux à droite non nuls de $\mathcal{O}$, $\mathcal{O}_g(I)$ est l'ordre à gauche $\{x \in D \mid xI \subset I\}$ de I et $[\mathcal{O}^\times : \mathcal{O}_g(I)^\times]$ désigne $[\mathcal{O}^\times : \mathcal{O}^\times \cap \mathcal{O}_g(I)^\times]/[\mathcal{O}_g(I)^\times : \mathcal{O}^\times \cap \mathcal{O}_g(I)^\times]$ (voir partie 4).

Finalement nous avons besoin d'une notion de régulateur. Nous définissons $\mathfrak{R}'$ comme le volume d'un domaine fondamental de $\{x \in D \otimes \mathbb{R} \mid |\mathrm{Nm}(x)| \leq 1\}$ modulo l'action à gauche de $\mathcal{O}^\times$. Ici Nm est la norme de l'algèbre $D \otimes \mathbb{R}$. Nous pouvons écrire un peu plus explicitement $\mathfrak{R}' = \mathfrak{R}/w$ avec $w = \mathrm{Card}\{x \in \mathcal{O}^\times \mid xx^\star = 1\}$ et

$$\mathfrak{R} = \mathrm{vol}\{x \in (D \otimes \mathbb{R})^\times \mid |\mathrm{Nm}(x)| \leq 1 \text{ et } \forall u \in \mathcal{O}^\times \ |x| \leq |ux|\}.$$

Nous étudierons en détail cet ensemble en partie 6. Nous montrerons en particulier qu'il est borné et nous notons ρ le supremum de la norme sur cet ensemble.

Nous notons encore $\omega_i = \pi^{i/2}\Gamma(i/2+1)^{-1}$ le volume de la boule unité de l'espace euclidien $\mathbb{R}^i$. Pour $m, m', k \geq 1$ nous écrivons

$$m!_{[k]} = \prod_{i=1}^{m} i\omega_{ki} \qquad \text{et} \qquad \binom{m}{m'}_{[k]} = \frac{m!_{[k]}}{m'!_{[k]}(m-m')!_{[k]}}.$$

Nous sommes en mesure d'énoncer notre résultat.

THÉORÈME 1.1. *Nous avons pour tout réel $H \geq 0$*

$$|\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,1,H) - c_{\mathrm{princ}} H^{Nn}| \leq c_{\mathrm{erreur}} H^{Nn-1}$$

avec

$$c_{\mathrm{princ}} = \frac{h'\mathfrak{R}'}{\zeta_D(N)|\Delta_{D/\mathbb{Q}}|^{N/2}} \frac{2^{(N-1)d^2(r_2+r_3/2)}}{Nd^{n/2}} \binom{Nd}{d}_{[1]}^{r_1} \binom{Nd}{d}_{[2]}^{r_2} \binom{Nd/2}{d/2}_{[4]}^{r_3}$$

et

$$c_{\mathrm{erreur}} = h'(Nn\rho)^{7N^2n^2}.$$

Un résultat antérieur de Franke, Manin et Tschinkel [FMT], établi dans le cadre plus général des variétés de drapeaux généralisés (voir la partie 9 de [LR] pour la traduction en termes de hauteur de sous-espaces), donnait déjà le comportement asymptotique ci-dessus mais sans indication sur le terme reste. Dans le terme principal, la constante donnée n'était pas explicitée comme ici en fonction de N et des invariants du corps D. Elle est en revanche exprimée en termes de mesure de Tamagawa sur la variété de drapeaux correspondante dans le travail de Peyre [P]. Enfin la méthode est très différente de celle que nous employons.

Lorsque D est commutatif, notre théorème s'apparente au résultat de Schanuel [Scha] à ceci près qu'il considère la hauteur de Weil d'un point projectif (définie avec la norme du supremum aux places infinies) alors que

nous employons une hauteur légérement différente (définie avec la norme hermitienne standard sur $\mathbb{C}^N$). Dans ce cas commutatif, notre terme principal se retrouve tel quel dans le travail de Thunder [T2], qui a été repris en termes plus arakeloviens par Gasbarri [G] puis Christensen et Gubler [CG]. Dans toutes ces références, cependant, le terme reste n'est pas explicite. Cet aspect est donc nouveau même pour les corps de nombres.

Pour permettre la comparaison avec les références citées, nous devons remarquer que si D est commutatif alors w est le cardinal des racines de l'unité dans D tandis que $\Re$ est relié au régulateur usuel Reg_D des corps des nombres par la formule $\mathrm{Reg}_D = 2^{r_1}(2\pi)^{r_2}\Re$ (ceci est essentiellement la formule encadrée page 133 de [La] ; la différence d'un facteur 2^{r_2} provient du choix légèrement différent de norme sur $D \otimes \mathbb{R}$). Dans le terme reste, il est également possible de majorer ρ en fonction de Reg_D et n. Toutefois l'estimation obtenue est exponentielle en Reg_D (voir lemme 9.2) alors que l'on sait qu'un argument dû à Schmidt permet d'obtenir un terme reste linéaire en Reg_D : voir la partie 8 de [W] (là encore il ne semble pas que ce terme ait été calculé explicitement).

Revenant au cas non commutatif, nous remarquons que nous avons

$$\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,M,H) = \mathcal{N}^{\mathcal{O},\star}_{\mathrm{dte}}(N,N-M,H)$$

par dualité ([LR] théorème 7.1). Pour cette raison, nous compterons en fait dans la suite du texte les sous-espaces à droite de dimension $N-1$. Le principe de ce décompte sera décrit ci-dessous mais, auparavant, nous examinons comment notre résultat principal dépend des données : comme la hauteur elle-même nécessite le choix d'un ordre maximal et d'une involution (ainsi que le choix d'une orientation gauche/droite), il est naturel de se demander comment cela influe sur notre formule asymptotique.

Pour cette analyse, et seulement celle-ci, nous considérons d'autres ordres maximaux et involutions que $\mathcal{O}$ et $\star$. Pour les ordres maximaux, nous rappelons d'abord qu'il n'y a qu'un nombre fini de classes de conjugaisons de tels ordres dans D : c'est une conséquence du théorème de Jordan-Zassenhaus (voir [R] page 232, exercice 26.8 ; deux ordres $\mathcal{O}'$ et $\mathcal{O}''$ sont conjugués s'il existe $x \in D^\times$ avec $\mathcal{O}'' = x\mathcal{O}'x^{-1}$). Par ailleurs, pour un ordre maximal $\mathcal{O}'$ de D, nous notons $h_{\mathrm{bil}}(\mathcal{O}')$ le nombre de classes d'isomorphie d'idéaux bilatères de $\mathcal{O}'$. Nous notons aussi $\Re'_{\mathcal{O}'}$ le quasi-régulateur défini comme $\Re'$ pour $\mathcal{O}$ (nous vérifierons que celui-ci ne dépend pas de l'involution) et nous généralisons aussi la notation ρ en $\rho_{\mathcal{O}',\star'}$ pour une anti-involution $\star'$. Enfin nous notons D^{op} le corps opposé de D.

PROPOSITION 1.2. *Le terme c_{princ} est indépendant de $\mathcal{O}$ et $\star$. Nous pouvons écrire*

$$h'\mathfrak{R}' = \sum_{\mathcal{O}'} h_{\text{bil}}(\mathcal{O}')\mathfrak{R}'_{\mathcal{O}'}$$

où $\mathcal{O}'$ parcourt un système de représentants des ordres maximaux de D à conjugaison près. De plus toutes ces quantités sont les mêmes pour D et D^{op}.

Comme cette proposition le suggère, nous vérifierons aussi que les quantités $h_{\text{bil}}(\mathcal{O}')$ et $\mathfrak{R}'_{\mathcal{O}'}$ ne dépendent pas du choix de $\mathcal{O}'$ à l'intérieur d'une classe de conjugaison d'ordre maximaux.

Au vu de ces résultats d'invariance, il ne faut pas perdre de vue que la hauteur dépend réellement des données. Elle dépend de l'ordre $\mathcal{O}$: lorsque V et $\star$ sont fixés on peut avoir $\sup_{\mathcal{O}'} H^{\mathcal{O}',\star}(V) = +\infty$ (où $\mathcal{O}'$ parcourt les ordres maximaux de D) ; et, de même, la hauteur dépend réellement de l'involution contrairement à ce qui est affirmé page 225 de [B] : on trouve également des exemples où, à V et $\mathcal{O}$ fixés, on a $\sup_{\star'} H^{\mathcal{O},\star'}(V) = +\infty$ (où $\star'$ parcourt les involutions positives sur $D \otimes \mathbb{R}$).

Nous montrerons aussi que le nombre $\mathcal{N}^{\mathcal{O},\star}_{\text{gche}}(N, M, H)$ peut dépendre de l'involution $\star$. De même le cardinal w dépend également de l'involution (en particulier, il n'y a pas d'interpretation intrinsèque de w qui généraliserait le nombre des racines de l'unité dans le cas commutatif).

Enfin le paramètre le plus délicat de notre estimation, le nombre ρ, dépend de l'ordre et de l'involution mais le résultat suivant montre que l'on peut le remplacer par une quantité finie indépendante de tout choix.

PROPOSITION 1.3. *La famille des réels ρ obtenus en changeant d'ordre, d'involution et d'orientation est bornée. Plus précisément on a $\rho_{x^{-1}\mathcal{O}x,\star} \leq \rho^n_{\mathcal{O},\star}$, $\rho_{\mathcal{O},\star'} \leq \rho^n_{\mathcal{O},\star}$ et $\rho_{\mathcal{O}^{\text{op}},\star^{\text{op}}} \leq \rho^{n-1}_{\mathcal{O},\star}$.*

Stratégie

Pour expliquer le principe du décompte que nous allons mettre en œuvre, commençons par examiner le cas des sous-espaces de codimension M sur $\mathbb{Q}$ (il est certes tout à fait distinct du cas que nous considérerons mais l'algèbre non commutative $\text{Mat}_{MM}(\mathbb{Q})$ y joue un rôle un peu analogue à celui du corps D). Il s'agit donc de compter les sous-espaces $V \subset \mathbb{Q}^N$ de codimension M de hauteur bornée. Un tel sous-espace peut être vu comme

le noyau d'une application linéaire surjective $\varphi\colon \mathbb{Q}^N \to \mathbb{Q}^M$. Si V est fixé, φ est déterminé modulo un automorphisme de $\mathbb{Q}^M$. On restreint le choix si l'on impose de plus $\varphi(\mathbb{Z}^N) = \mathbb{Z}^M$. Dans ce cadre, φ est donné par une matrice $A \in \mathrm{Mat}_{MN}(\mathbb{Z})$ de rang M déterminée par V modulo $\mathrm{GL}_M(\mathbb{Z})$, le groupe des matrices inversibles d'ordre M sur $\mathbb{Z}$. La hauteur de V s'exprime par $H(V) = \det(A\,{}^tA)^{1/2}$, où ${}^tA$ est la transposée de A, donc nous cherchons à évaluer le cardinal de

$$\{A \in \mathrm{Mat}_{MN}(\mathbb{Z}) \mid \det(A\,{}^tA) \leq H^2,\ A\mathbb{Z}^N = \mathbb{Z}^M\}/GL_M(\mathbb{Z}).$$

La condition $A\mathbb{Z}^N = \mathbb{Z}^M$ n'est pas facile à traiter, par opposition par exemple à $A\mathbb{Z}^N \subset \mathbb{Z}^M$ qui signifie simplement $A \in \mathrm{Mat}_{MN}(\mathbb{Z})$. Nous pouvons nous ramener à une condition de ce type par inversion de Möbius (cette idée, très classique, est déjà celle exploitée par Schanuel). En effet, si nous définissons pour tout sous-module $\mathcal{A}$ de $\mathbb{Z}^M$ de rang M

$$f_{\mathcal{A}}(H) = \mathrm{Card}(\{A \in \mathrm{Mat}_{MN}(\mathbb{Z}) \mid \det(A\,{}^tA) \leq H^2,\ A\mathbb{Z}^N = \mathcal{A}\}/GL_M(\mathbb{Z}))$$

et

$$g_{\mathcal{A}}(H) = \mathrm{Card}(\{A \in \mathrm{Mat}_{MN}(\mathbb{Z}) \mid 0 < \det(A\,{}^tA) \leq H^2,\ A\mathbb{Z}^N \subset \mathcal{A}\}/GL_M(\mathbb{Z})),$$

alors on constate sans peine que

$$g_{\mathcal{A}}(H) = \sum_{\mathcal{B} \subset \mathcal{A}} f_{\mathcal{B}}(H)$$

donc par la formule d'inversion de Möbius (voir partie 3), la quantité que nous voulons calculer qui se trouve être $f_{\mathbb{Z}^M}(H)$ s'exprime

$$f_{\mathbb{Z}^M}(H) = \sum_{\mathcal{A} \subset \mathbb{Z}^M} \mu(\mathcal{A}) g_{\mathcal{A}}(H),$$

où μ est la fonction de Möbius définie sur l'ensemble des sous-modules de $\mathbb{Z}^M$ de rang M. Pourquoi ceci représente-t-il un progrès ? La condition $A\mathbb{Z}^N \subset \mathcal{A}$ apparaissant dans $g_{\mathcal{A}}(H)$ signifie que les colonnes de A appartiennent à $\mathcal{A}$ ou encore que $A \in \mathrm{Mat}_{MN}(\mathbb{Z}) \simeq (\mathbb{Z}^M)^N$ se trouve dans le sous-réseau $\mathcal{A}^N$. Par conséquent la quantité $g_{\mathcal{A}}(H)$ est le cardinal de l'intersection de ce réseau $\mathcal{A}^N$ avec un domaine fondamental du quotient

$$\{A \in \mathrm{Mat}_{MN}(\mathbb{R}) \mid 0 < \det(A\,{}^tA) \leq H^2\}/GL_M(\mathbb{Z}).$$

Ceci s'écrit plus agréablement

$$g_{\mathcal{A}}(H) = \mathrm{Card}(\mathcal{A}^N \cap H^{1/M} S)$$

si S désigne un domaine fondamental pour le quotient $\{A \in \mathrm{Mat}_{MN}(\mathbb{R}) \mid 0 < \det(A\,{}^tA) \leq 1\}/GL_M(\mathbb{Z})$. Notre travail se réduit donc à un problème classique de géométrie des nombres : estimer le nombre de points d'un réseau dans un domaine fixé. Le principe général est que ce nombre doit être proche du rapport du volume du domaine par le covolume du réseau ce qui s'écrit dans notre situation

$$g_{\mathcal{A}}(H) \approx \frac{\mathrm{vol}(H^{1/M}S)}{\mathrm{vol}(\mathcal{A}^N)} = \frac{\mathrm{vol}(S)}{\mathrm{vol}(\mathcal{A})^N} H^N.$$

Si l'on croit à ce principe, il reste pour calculer le terme principal à évaluer le volume de S et la somme $\sum_{\mathcal{A}} \mu(\mathcal{A})\mathrm{vol}(\mathcal{A})^{-N}$. Cette dernière s'exprime sans peine à l'aide de la fonction ζ (voir parties 3 et 5). La difficulté consiste à estimer l'erreur que l'on fait dans cette approximation. Ici deux cas se distinguent nettement : si le domaine S est borné, des estimations explicites générales se trouvent dans la littérature (nous rappelons la situation en partie 7) ; si, en revanche, il n'est pas borné, il semble qu'il faille travailler séparément sur chaque ensemble S. Cette distinction explique que nous nous restreignons à $M = 1$: en effet, notre S est borné si et seulement si $M = 1$ (dans le cas $D = \mathbb{Q}$ décrit jusqu'ici si $M = 1$ alors S est une demi-boule unité de $\mathbb{R}^N$).

Voyons maintenant comment l'on peut adapter le plan ci-dessus pour passer de $D = \mathbb{Q}$ à D quelconque. Écrire V comme le noyau de $\varphi : D^N \to D^M$ ne pose pas problème mais nous ne pouvons pas remplacer la condition $\varphi(\mathbb{Z}^N) = \mathbb{Z}^M$ par son analogue évident $\varphi(\mathcal{O}^N) = \mathcal{O}^M$. Nous devons faire apparaître ici les classes d'isomorphie de sous-modules de $\mathcal{O}^M$. Ceci introduit plusieurs complications puisque si nous nous intéressons aux morphismes φ tels que $\varphi(\mathcal{O}^N) = \mathcal{C}$ alors il nous faut quotienter leur ensemble par le groupe des automorphismes du $\mathcal{O}$-module à droite $\mathcal{C}$ (noté $W_{\mathcal{C}}$) et non par $\mathrm{Mat}_{MM}(\mathcal{O})^\times$ (qui est $W_{\mathcal{O}^M}$). Cela nous obligera à quelques acrobaties pour comparer les deux groupes tout au long de la partie 4 dont la clef est le lemme 4.1 qui assure que l'on ne manipule que des groupes d'indices finis.

Le présent article s'organise comme suit. Nous donnons dans la partie suivante quelques préliminaires. Les trois parties 3, 4 et 5 reprennent le schéma décrit ci-dessus pour M quelconque à l'exception de l'estimation centrale du nombre de points dans l'intersection d'un domaine et d'un réseau. Celle-ci fait l'objet des parties 6 et 7 où nous décrivons le domaine fondamental et son bord pour $M = 1$. Enfin, la partie 8 est consacrée au calcul du volume de S tandis que la dernière partie conclut la preuve et démontre les autres assertions de l'introduction (propositions 1.2 et 1.3 et exemples).

2. Préliminaires

Pour une algèbre $\mathfrak{A}$ de dimension finie sur $\mathbb{R}$ nous notons toujours $\mathrm{Nm} : \mathfrak{A} \longrightarrow \mathbb{R}$ la norme comme $\mathbb{R}$-algèbre.

Rappelons maintenant l'écriture matricielle de la hauteur d'un sous-espace à droite V de D^N de codimension M. Si A est une matrice de $\mathrm{Mat}_{MN}(\mathcal{O})$ de rang M telle que $V = \{x \in D^N \mid Ax = 0\}$, alors

$$H^{\mathcal{O},\star}(V) = H^{\mathcal{O},\star}(A) = \mathrm{Nm}(AA^\star)^{1/2Mn}[\mathcal{O}^M : A\mathcal{O}^N]^{-1/n}$$

(voir propositions 6.1 et 6.3 de [LR] où nous avions utilisé la norme réduite au lieu de la norme Nm sur $\mathrm{Mat}_{MM}(D \otimes \mathbb{R})$).

LEMME 2.1. *Pour toute matrice $A \in \mathrm{Mat}_{MN}(D)$ de rang M on a*

$$H^{\mathcal{O},\star}(A) \geq 1.$$

DÉMONSTRATION. Soit $V \subset D^N$ le sous-espace à droite sur D de codimension M défini par $V = \{X \in D^N | AX = 0\}$. On choisit une projection orthogonale $p : D^N \to D^{N-M}$ obtenue en oubliant M coordonnées et dont la restriction à V est surjective (et donc bijective, car $\dim V = N - M$). On a donc $\mathrm{vol}(V \cap \mathcal{O}^N) \geq \mathrm{vol}(p(V \cap \mathcal{O}^N))$, mais $p(V \cap \mathcal{O}^N) \subset \mathcal{O}^{N-M}$, d'où $\mathrm{vol}(\mathcal{O})^{N-M} = \mathrm{vol}(\mathcal{O}^{N-M}) \leq \mathrm{vol}(p(V \cap \mathcal{O}^N))$. Ceci donne $H^{\mathcal{O},\star}(A) = H^{\mathcal{O},\star}(V) \geq 1$. □

Rappelons que $|\cdot|$ est définie par $|x|^2 = \mathrm{Tr}(xx^\star)$. Le lemme suivant rassemble quelques propriétés de base de cette norme euclidienne.

LEMME 2.2. *Si $x, y \in D \otimes \mathbb{R}$ on a*

(1) $|xy| \leq |x||y|$.

(2) $|\mathrm{Tr}(x)| \leq \sqrt{n}|x|$.

(3) *Si x est inversible,* $|x^{-1}| \leq \dfrac{|x|^{n-1}}{|\mathrm{Nm}(x)|}$.

(4) $|\mathrm{Nm}(x)|^{1/n} \leq \dfrac{1}{\sqrt{n}}|x|$ *avec égalité si et seulement si $xx^\star \in \mathbb{R}$.*

DÉMONSTRATION. Le problème se ramène à des identités sur les matrices réelles en considérant la représentation régulière (à gauche ou à droite) $\tau : D \otimes \mathbb{R} \hookrightarrow \mathrm{Mat}_{nn}(\mathbb{R})$ donnée par une base orthonormée de $D \otimes \mathbb{R}$ de sorte que $\mathrm{Tr}(x)$ est la trace de la matrice $\tau(x)$, $\mathrm{Nm}(x)$ son déterminant et $\tau(x^\star)$ sa transposée. Ainsi $|x|^2$ est la somme des carrés des coefficients de

$\tau(x)$ ou encore la somme des valeurs propres de la matrice symétrique positive $\tau(x)\,{}^t\tau(x)$. L'assertion (1) résulte d'un calcul direct avec les matrices $\tau(x)$ et $\tau(y)$. Pour l'assertion (2) soient $a_1, \dots, a_n$ les coefficients de $\tau(x)$ sur la diagonale. On a $\mathrm{Tr}(x) = a_1 + \cdots + a_n$ et $a_1^2 + \cdots + a_n^2 \leq |x|^2$. L'inégalité souhaitée s'obtient donc en appliquant Cauchy-Schwarz aux vecteurs $(a_1, \dots, a_n)$ et $(1, \dots, 1)$. L'assertion (3) traduit l'inégalité

$$\lambda_1^{-1} + \cdots + \lambda_n^{-1} \leq \frac{(\lambda_1 + \cdots + \lambda_n)^{n-1}}{\lambda_1 \cdots \lambda_n}$$

pour les valeurs propres de $\tau(x)\,{}^t\tau(x)$ tandis que l'assertion (4) exprime que la moyenne géométrique de ces mêmes valeurs propres est inférieure à leur moyenne arithmétique. Il y a égalité si et seulement si toutes les valeurs propres sont égales. Ceci équivaut à dire que la matrice $\tau(x)\,{}^t\tau(x) = \tau(xx^\star)$ est scalaire donc de la forme $\tau(z)$ pour un réel z. On conclut par injectivité de τ. □

On rappelle que la norme Nm prend des valeurs entières sur $\mathcal{O}$ ou plus généralement sur $\mathrm{Mat}_{MM}(\mathcal{O})$. Par suite, elle vaut 1 ou -1 sur $\mathcal{O}^\times$ et $\mathrm{Mat}_{MM}(\mathcal{O})^\times$.

Nous notons $N(\mathcal{I})$ la norme d'un idéal non nul de $\mathcal{O}$ c'est-à-dire $N(\mathcal{I}) = \mathrm{Card}(\mathcal{O}/\mathcal{I})$. De la même façon si $\mathcal{D}$ est un sous-$\mathcal{O}$-module de rang M de $\mathcal{O}^M$ nous notons $N(\mathcal{D}) = \mathrm{Card}(\mathcal{O}^M/\mathcal{D})$.

LEMME 2.3. *Pour tout ordre maximal $\mathcal{O}$ de D et toute involution positive $\star$ sur $D \otimes \mathbb{R}$, nous avons* $\mathrm{vol}(\mathcal{O}) = (d^n|\Delta_{D/\mathbb{Q}}|)^{1/2}$.

DÉMONSTRATION. Soit $e_1, \dots, e_n$ une base de $\mathcal{O}$ sur $\mathbb{Z}$. Par définition $\Delta_{D/\mathbb{Q}} = \det(\mathrm{tr}(e_i e_j))_{1\leq i,j\leq n}$ (voir [R] page 218) où tr est la trace réduite, reliée à la trace par $\mathrm{Tr} = d\mathrm{tr}$ (voir [R] (9.17) page 119). Par ailleurs, $\mathrm{vol}(\mathcal{O})^2$ vaut $\det(\mathrm{Tr}(e_i e_j^\star))_{1\leq i,j\leq n}$ par définition de la structure euclidienne associée à $\star$. Ceci nous montre $\mathrm{vol}(\mathcal{O})^2 = d^n \Delta_{D/\mathbb{Q}} \det M$ où M est la matrice de $\star$ dans la $\mathbb{R}$-base $e_1, \dots, e_n$ de $D \otimes \mathbb{R}$. Comme $\star$ est une involution, on a $M^2 = I$ donc $|\det M| = 1$. □

Au passage, ceci nous montre que la mesure vol sur $D \otimes \mathbb{R}$ est indépendante de $\star$ et, en particulier, le quasi-régulateur $\mathfrak{R}'$ ne dépend pas de $\star$.

Nous appellerons symétrique un élément y de $D \otimes \mathbb{R}$ tel que $y = y^\star$. Nous lui associons la forme quadratique $x \mapsto \mathrm{Tr}(x^\star y x)$ sur $D \otimes \mathbb{R}$ et nous dirons que y est positif ou défini positif lorsque c'est la cas de la forme quadratique qu'il définit. Nous désignons par $(D \otimes \mathbb{R})_{\mathrm{sym}}$, $(D \otimes \mathbb{R})_{\mathrm{sym}}^{\geq 0}$ et

$(D \otimes \mathbb{R})^{>0}_{\mathrm{sym}}$ les parties de $D \otimes \mathbb{R}$ formées des éléments symétriques, positifs et définis positifs respectivement. Ces définitions s'explicitent facilement dès que l'on choisit un isomorphisme

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

En effet, si $\mathbb{K}$ est l'un des trois corps $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, nous noterons $A \mapsto A^\star$ la transconjugaison sur $\mathrm{Mat}_{mm}(\mathbb{K})$ puis $\mathcal{H}_m(\mathbb{K}) = \{A \in \mathrm{Mat}_{mm}(\mathbb{K}) \mid A = A^\star\}$ le sous-espace des matrices hermitiennes (voir [LR], page 552, où la transconjuguée était notée ${}^t\bar{A}$). Nous introduisons de manière analogue l'ensemble des matrices positives $\mathcal{H}^{\geq 0}_m(\mathbb{K})$ et celui des matrices définies positives $\mathcal{H}^{>0}_m(\mathbb{K})$. Alors, à travers l'isomorphisme précédent, nous avons

$$(D \otimes \mathbb{R})_{\mathrm{sym}} \simeq \mathcal{H}_d(\mathbb{R})^{r_1} \times \mathcal{H}_d(\mathbb{C})^{r_2} \times \mathcal{H}_{d/2}(\mathbb{H})^{r_3}$$

et de même en introduisant partout l'exposant ≥ 0 ou > 0.

Nous utiliserons encore le groupe unitaire $U_m(\mathbb{K}) = \{K \in \mathrm{Mat}_{mm}(\mathbb{K}) \mid KK^\star = I\}$ et l'ensemble $\Delta_m \subset \mathrm{Mat}_{mm}(\mathbb{K})$ des matrices diagonales réelles avec les variantes $\Delta^{\geq 0}_m$ et $\Delta^{>0}_m$ lorsque l'on impose aux coefficients diagonaux d'être positifs ou strictement positifs. Remarquons que l'on a $\Delta_m \subset \mathcal{H}_m(\mathbb{K})$ et $\Delta^{\geq 0}_m = \Delta_m \cap \mathcal{H}^{\geq 0}_m(\mathbb{K})$, $\Delta^{>0}_m = \Delta_m \cap \mathcal{H}^{>0}_m(\mathbb{K})$.

Citons le résultat de diagonalisation des matrices hermitiennes.

LEMME 2.4. *Pour tout $A \in \mathcal{H}_m(\mathbb{K})$, il existe $B \in \Delta_m$ et $K \in U_m(\mathbb{K})$ tels que $A = KBK^{-1}$. De plus B est unique à permutations des coefficients diagonaux près et l'on a $A \in \mathcal{H}^{\geq 0}_m(\mathbb{K}) \Longleftrightarrow B \in \Delta^{\geq 0}_m$, $A \in \mathcal{H}^{>0}_m(\mathbb{K}) \Longleftrightarrow B \in \Delta^{>0}_m$.*

DÉMONSTRATION. Ceci est tout à fait classique si $\mathbb{K} \neq \mathbb{H}$. Pour $\mathbb{H}$ on consultera par exemple [FP]. □

Nous pouvons donc parler des valeurs propres d'une matrice hermitienne A : ce sont les coefficients diagonaux de B comme dans le lemme.

COROLLAIRE 2.1. *L'application $x \mapsto x^2$ induit une bijection $(D \otimes \mathbb{R})^{\geq 0}_{\mathrm{sym}} \to (D \otimes \mathbb{R})^{\geq 0}_{\mathrm{sym}}$ et*

$$(D \otimes \mathbb{R})^{>0}_{\mathrm{sym}} = \{xx^\star \mid x \in (D \otimes \mathbb{R})^\times\}.$$

DÉMONSTRATION. Pour la première assertion, montrons que l'élévation au carré est une bijection $\mathcal{H}^{\geq 0}_m(\mathbb{K}) \to \mathcal{H}^{\geq 0}_m(\mathbb{K})$. Pour la surjectivité, il suffit d'écrire $A \in \mathcal{H}^{\geq 0}_m$ sous la forme KBK^{-1} par le lemme ; comme $B \in \Delta^{\geq 0}_m$ il existe $C \in \Delta^{\geq 0}_m$ avec $B = C^2$ et cela donne $A = (KCK^{-1})^2$.

Pour l'injectivité supposons que l'on ait $X^2 = Y^2$ avec $X, Y \in \mathcal{H}_m^{\geq 0}(\mathbb{K})$. Écrivons $Y = KBK^{-1}$ par le lemme et posons $Z = K^{-1}XK \in \mathcal{H}^{\geq 0}(\mathbb{K})$. Nous avons $Z^2 = K^{-1}X^2K = K^{-1}Y^2K$ donc $Z^2 = B^2$. Remarquons que ce calcul permet déjà de conclure si X est une matrice scalaire aI (avec $a \in \mathbb{R}$, $a \geq 0$). En effet, dans ce cas, $Z = K^{-1}(aI)K = aI$ donc $B^2 = a^2I$. Comme B est diagonale et positive, cela force $B = aI$ d'où $Y = K^{-1}(aI)K = aI = X$.

En revenant au cas général (X quelconque), nous notons que $Z^2 = B^2$ entraîne que Z commute avec la matrice B^2. Si $a_1, \ldots, a_m$ sont les coefficients diagonaux réels de B et z_{ij} les coefficients de Z alors $ZB^2 = B^2Z$ s'écrit $z_{ij}a_j^2 = a_i^2 z_{ij}$ $(1 \leq i, j \leq m)$ donc $z_{ij} = 0$ dès que $a_i^2 \neq a_j^2$ c'est-à-dire dès que $a_i \neq a_j$. Par conséquent Z est une matrice diagonale par blocs où chaque bloc correspond à un élément $a \in \{a_1, \ldots, a_m\}$: on forme le bloc Z_a en retenant les coefficients z_{ij} où $i, j \in \{1 \leq k \leq n \mid a_k = a\}$. L'égalité $Z^2 = B^2$ se traduit par $Z_a^2 = a^2I$ pour tout a. D'après le cas des matrices scalaires déjà traité, on a $Z_a = aI$ (la matrice Z_a se trouve dans $\mathcal{H}_{m'}^{\geq 0}(\mathbb{K})$ pour $m' \leq m$) d'où $Z = B$. Ceci entraîne alors $X = Y$.

Pour la deuxième assertion, si $x \in (D \otimes \mathbb{R})^\times$, la forme quadratique $z \mapsto \mathrm{Tr}(z^\star xx^\star z)$ est définie positive car égale à $z \mapsto |z^\star x|^2$. Ceci montre $\{xx^\star \mid x \in (D \otimes \mathbb{R})^\times\} \subset (D \otimes \mathbb{R})_{\mathrm{sym}}^{>0}$. Réciproquement si $y \in (D \otimes \mathbb{R})_{\mathrm{sym}}^{>0}$ il existe $x \in (D \otimes \mathbb{R})_{\mathrm{sym}}^{\geq 0}$ avec $y = x^2 = xx^\star$ et x est inversible car y l'est. □

3. Fonction de Möbius

Dans cette partie, nous étudions la fonction de Möbius des modules et des idéaux. La notion de fonction de Möbius peut être définie pour des ensembles partiellement ordonnés plus généraux (voir par exemple le paragraphe 8.6 page 480 de [J] ou le paragraphe 3.7 page 116 de [St]) mais nous nous contentons de rappeler la définition dans le cadre restreint dans lequel nous nous placerons.

Soient $\mathfrak{A}$ un anneau et $\mathcal{M}$ un $\mathfrak{A}$-module à droite. Considérons l'ensemble $\mathcal{S}(\mathcal{M})$ des sous-$\mathfrak{A}$-modules à droite $\mathcal{N}$ de $\mathcal{M}$ tels que $\mathcal{M}/\mathcal{N}$ est de cardinal fini. On construit une fonction $\mu(\cdot, \mathcal{M})$ de $\mathcal{S}(\mathcal{M})$ vers $\mathbb{Z}$ en imposant les conditions $\mu(\mathcal{M}, \mathcal{M}) = 1$ et, si $\mathcal{N} \in \mathcal{S}(\mathcal{M}) \setminus \{\mathcal{M}\}$,

$$\sum_{\mathcal{N} \subset \mathcal{N}' \in \mathcal{S}(\mathcal{M})} \mu(\mathcal{N}', \mathcal{M}) = 0 \,.$$

Ceci a bien un sens car l'ensemble $\{\mathcal{N}' \in \mathcal{S}(\mathcal{M}) \mid \mathcal{N} \subset \mathcal{N}'\}$ est fini. On le voit par exemple en notant que l'ensemble des sous-groupes de $\mathcal{M}$ contenant $\mathcal{N}$ est en bijection avec l'ensemble des sous-groupes du groupe

abélien fini $\mathcal{M}/\mathcal{N}$. Par récurrence sur le cardinal du groupe $\mathcal{M}/\mathcal{N}$ on montre facilement que les formules données ci-dessus définissent de façon unique une fonction $\mu(\cdot, \mathcal{M}) : \mathcal{S}(\mathcal{M}) \to \mathbb{Z}$.

Citons maintenant le résultat simple mais fondamental qui justifie l'introduction de cette fonction et qui porte le nom de *formule d'inversion de Möbius*.

LEMME 3.1. *Soient $\mathfrak{A}$ un anneau, $\mathcal{M}$ un $\mathfrak{A}$-module à droite et $f : \mathcal{S}(\mathcal{M}) \to \mathbb{R}$ une application telle que $f(\mathcal{N}) = 0$ sauf pour un nombre fini de $\mathcal{N} \in \mathcal{S}(\mathcal{M})$. Si l'on pose pour $\mathcal{N} \in \mathcal{S}(\mathcal{M})$*

$$g(\mathcal{N}) = \sum_{\mathcal{N}' \in \mathcal{S}(\mathcal{N})} f(\mathcal{N}'),$$

alors

$$f(\mathcal{M}) = \sum_{\mathcal{N} \in \mathcal{S}(\mathcal{M})} \mu(\mathcal{N}, \mathcal{M})\, g(\mathcal{N}).$$

DÉMONSTRATION. On a

$$\begin{aligned} \sum_{\mathcal{N} \in \mathcal{S}(\mathcal{M})} \mu(\mathcal{N}, \mathcal{M})\, g(\mathcal{N}) &= \sum_{\mathcal{N} \in \mathcal{S}(\mathcal{M})} \sum_{\mathcal{N}' \in \mathcal{S}(\mathcal{N})} \mu(\mathcal{N}, \mathcal{M}) f(\mathcal{N}') \\ &= \sum_{\mathcal{N}' \in \mathcal{S}(\mathcal{M})} f(\mathcal{N}') \sum_{\mathcal{N}' \subset \mathcal{N} \in \mathcal{S}(\mathcal{M})} \mu(\mathcal{N}, \mathcal{M}) \,. \end{aligned}$$

Par définition même, la deuxième somme est nulle pour tout $\mathcal{N}' \neq \mathcal{M}$ et égale à $\mu(\mathcal{M}, \mathcal{M}) = 1$ pour $\mathcal{N}' = \mathcal{M}$. Ceci montre le lemme. □

Dans la suite de cette partie, nous nous intéressons à un cas particulier de cette fonction de Möbius. Soit $\mathfrak{D}$ une algèbre centrale simple de dimension finie sur un corps de nombres Z et soit $\mathcal{O}$ un ordre maximal de $\mathfrak{D}$. On spécialise $\mathfrak{A} = \mathcal{M} = \mathcal{O}$ dans les notations ci-dessus, de sorte que $\mathcal{S}(\mathcal{O})$ est l'ensemble des idéaux à droite de $\mathcal{O}$ qui sont des $\mathbb{Z}$-modules de rang $[\mathfrak{D} : \mathbb{Q}]$. On obtient donc une fonction $\mu(\mathcal{I}, \mathcal{O}) = \mu(\mathcal{I})$ pour $\mathcal{I} \in \mathcal{S}(\mathcal{O})$ qui est définie par $\mu(\mathcal{O}) = 1$ et

$$\sum_{\mathcal{I} \subset \mathcal{J} \in \mathcal{S}(\mathcal{O})} \mu(\mathcal{J}) = 0$$

pour tout $\mathcal{I} \in \mathcal{S}(\mathcal{O}) \setminus \{\mathcal{O}\}$.

L'objet principal de cette partie est de majorer la fonction de Möbius d'un idéal de $\mathcal{S}(\mathcal{O})$. Pour énoncer notre résultat, notons $d^2 = [\mathfrak{D} : Z]$.

THÉORÈME 3.1. *Tout élément $\mathcal{I}$ de $\mathcal{S}(\mathcal{O})$ vérifie*

$$|\mu(\mathcal{I})| \leq N(\mathcal{I})^{(1/2)-(1/2d)}.$$

Remarquons que, si $\mathfrak{D} = Z$ est un corps de nombres, nous trouvons donc $\mu(\mathcal{I}) \in \{-1, 0, 1\}$ comme dans le cas classique de la fonction de Möbius usuelle sur les entiers. Cela se prouve aussi directement en factorisant l'idéal $\mathcal{I}$ en produit d'idéaux premiers dans l'anneau de Dedekind $\mathcal{O} = \mathcal{O}_Z$ (entiers de Z).

Pour démontrer le théorème, nous utiliserons la fonction de Möbius plus générale introduite au début de cette partie. Chaque fois que l'on dispose d'une bijection croissante entre sous-modules, l'on voit apparaître une relation entre fonctions de Möbius. De manière précise, nous utiliserons les résultats suivants.

LEMME 3.2. *Soient $\mathfrak{A}$ et $\mathfrak{B}$ deux anneaux.*

(1) *Si $\mathcal{M}$ est un $\mathfrak{A}$-module à droite et $\mathcal{N} \in \mathcal{S}(\mathcal{M})$ alors $\mu(\mathcal{N}, \mathcal{M}) = \mu(0, \mathcal{M}/\mathcal{N})$.*
(2) *Si $\mathcal{M}$ est un $\mathfrak{A}$-module à droite, $\mathcal{M}'$ un $\mathfrak{B}$-module à droite, $\mathcal{N} \in \mathcal{S}(\mathcal{M})$ et $\mathcal{N}' \in \mathcal{S}(\mathcal{M}')$ alors $\mathcal{M} \times \mathcal{M}'$ est un $\mathfrak{A} \times \mathfrak{B}$-module à droite, $\mathcal{N} \times \mathcal{N}' \in \mathcal{S}(\mathcal{M} \times \mathcal{M}')$ et $\mu(\mathcal{N} \times \mathcal{N}', \mathcal{M} \times \mathcal{M}') = \mu(\mathcal{N}, \mathcal{M})\mu(\mathcal{N}', \mathcal{M}')$.*
(3) *Si $\mathcal{I}$ est un idéal à droite de l'anneau $\mathrm{Mat}_{mm}(\mathfrak{A})$ (pour un entier naturel $m \geq 1$) et si $\mathcal{M}$ est le sous-$\mathfrak{A}$-module de $\mathfrak{A}^m$ formé des colonnes des éléments de $\mathcal{I}$ alors $\mathrm{Card}(\mathrm{Mat}_{mm}(\mathfrak{A})/\mathcal{I}) = \mathrm{Card}(\mathfrak{A}^m/\mathcal{M})^m$. Si de plus ces quantités sont finies alors $\mu(\mathcal{I}, \mathrm{Mat}_{mm}(\mathfrak{A})) = \mu(\mathcal{M}, \mathfrak{A}^m)$ (où l'on regarde $\mathrm{Mat}_{mm}(\mathfrak{A})$ comme $\mathrm{Mat}_{mm}(\mathfrak{A})$-module et $\mathfrak{A}^m$ comme $\mathfrak{A}$-module).*

DÉMONSTRATION. (1) L'assertion est conséquence immédiate de la bijection croissante entre les sous-modules de $\mathcal{M}$ contenant $\mathcal{N}$ et les sous-modules de $\mathcal{M}/\mathcal{N}$.

(2) L'isomorphisme $(\mathcal{M} \times \mathcal{M}')/(\mathcal{N} \times \mathcal{N}') \simeq (\mathcal{M}/\mathcal{N}) \times (\mathcal{M}'/\mathcal{N}')$ montre $\mathcal{N} \times \mathcal{N}' \in \mathcal{S}(\mathcal{M} \times \mathcal{M}')$. De plus, tout sous-$(\mathfrak{A} \times \mathfrak{B})$-module de $\mathcal{M} \times \mathcal{M}'$ est de la forme $\mathcal{P} \times \mathcal{P}'$ pour un sous-$\mathfrak{A}$-module $\mathcal{P}$ de $\mathcal{M}$ et un sous-$\mathfrak{B}$-module $\mathcal{P}'$ de $\mathcal{M}'$. Nous notons aussi que la formule est claire si $\mathcal{N} = \mathcal{M}$ et $\mathcal{N}' = \mathcal{M}'$. Nous supposons donc $\mathcal{N} \neq \mathcal{M}$ ou $\mathcal{N}' \neq \mathcal{M}'$. Par conséquent, on a par définition de μ

$$\sum_{\mathcal{N} \subset \mathcal{P} \in \mathcal{S}(\mathcal{M})} \mu(\mathcal{P}, \mathcal{M}) = 0 \qquad \text{ou} \qquad \sum_{\mathcal{N}' \subset \mathcal{P}' \in \mathcal{S}(\mathcal{M}')} \mu(\mathcal{P}', \mathcal{M}') = 0$$

et donc en multipliant

$$\sum_{\mathcal{N}\times\mathcal{N}'\subset\mathcal{P}\times\mathcal{P}'\in\mathcal{S}(\mathcal{M}\times\mathcal{M}')} \mu(\mathcal{P},\mathcal{M})\mu(\mathcal{P}',\mathcal{M}') = 0\ .$$

Ceci montre que la fonction $\mathcal{P}\times\mathcal{P}'\mapsto\mu(\mathcal{P},\mathcal{M})\mu(\mathcal{P}',\mathcal{M}')$ remplit bien les conditions définissant la fonction $\mu(\cdot,\mathcal{M}\times\mathcal{M}')$.

(3) L'application qui à $\mathcal{I}$ associe $\mathcal{M}$ est une bijection croissante de l'ensemble des idéaux à droite de $\mathrm{Mat}_{mm}(\mathfrak{A})$ vers celui des sous-$\mathfrak{A}$-modules à droite de $\mathfrak{A}^m$ (la réciproque associe à un module $\mathcal{M}$ l'idéal $\mathcal{I}$ formé des matrices dont toutes les colonnes appartiennent à $\mathcal{M}$). Le résultat s'en déduit directement, en notant pour les cardinaux que l'on a un isomorphisme de $\mathfrak{A}$-modules $\mathcal{I}\simeq\mathcal{M}^m$. □

Nous étudions maintenant le cas des modules sur un anneau local fini.

PROPOSITION 3.2. *Soient $\mathfrak{A}$ un anneau local fini, $\mathfrak{m}$ son idéal maximal et $\mathcal{M}$ un $\mathfrak{A}$-module à droite fini.*

(1) *Si $\mathfrak{A}$ est un corps autrement dit si $\mathfrak{m}=0$ alors pour tout entier naturel m on a $\mu(0,\mathfrak{A}^m)=(-1)^m(\mathrm{Card}\,\mathfrak{A})^{m(m-1)/2}$.*
(2) *Si $\mathcal{M}\mathfrak{m}=0$ alors il existe un entier naturel m tel que $\mathcal{M}$ est isomorphe à $(\mathfrak{A}/\mathfrak{m})^m$ et $\mu(0,\mathcal{M})=(-1)^m(\mathrm{Card}\mathcal{M})^{(m-1)/2}$.*
(3) *Si $\mathcal{M}\mathfrak{m}\neq 0$ alors $\mu(0,\mathcal{M})=0$.*

DÉMONSTRATION. (1) Voir exemple 3.10.2 page 126 de [St] ou exercice 4 page 488 de [J]. On peut calculer explicitement le nombre de sous-espaces vectoriels de dimension donnée de $\mathfrak{A}^m$ et en déduire la formule.

(2) Lorsque $\mathcal{M}\mathfrak{m}=0$, le $\mathfrak{A}$-module $\mathcal{M}$ est un $(\mathfrak{A}/\mathfrak{m})$-module c'est-à-dire un $(\mathfrak{A}/\mathfrak{m})$-espace vectoriel. En notant m sa dimension nous avons $\mathcal{M}\simeq(\mathfrak{A}/\mathfrak{m})^m$ et le résultat de (1) s'applique (les sous-$\mathfrak{A}$-modules de $\mathcal{M}$ sont eux aussi des $(\mathfrak{A}/\mathfrak{m})$-espaces vectoriels).

(3) Nous montrons cette assertion par récurrence sur $\mathrm{Card}(\mathcal{M})$. Si $\mathrm{Card}(\mathcal{M})=1$ on a $\mathcal{M}=0$ et $\mathcal{M}\mathfrak{m}=0$: l'assertion est donc vraie (car l'hypothèse est fausse). Soit maintenant $\mathcal{M}$ avec $\mathrm{Card}(\mathcal{M})\geq 2$; nous supposons $\mathcal{M}\mathfrak{m}\neq 0$ et que l'assertion est vraie pour tout module de cardinal $<\mathrm{Card}(\mathcal{M})$. Pour montrer $\mu(0,\mathcal{M})=0$, nous devons établir, par définition de la fonction de Möbius,

$$\sum_{\mathcal{N}\in\mathcal{S}(\mathcal{M})\setminus\{0\}} \mu(\mathcal{N},\mathcal{M}) = 0.$$

Or, si $\mathcal{N}\in\mathcal{S}(\mathcal{M})\setminus\{0\}$, nous avons $\mu(\mathcal{N},\mathcal{M})=\mu(0,\mathcal{M}/\mathcal{N})$ et $\mathrm{Card}(\mathcal{M}/\mathcal{N})<$

Card($\mathcal{M}$). Par conséquent, notre hypothèse de récurrence montre $\mu(\mathcal{N},\mathcal{M})=0$ dès que $(\mathcal{M}/\mathcal{N})\mathfrak{m}\neq 0$. Il nous suffit donc de prouver

$$\sum_{\mathcal{N}\in\mathcal{S}(\mathcal{M}),\ (\mathcal{M}/\mathcal{N})\mathfrak{m}=0}\mu(\mathcal{N},\mathcal{M})=0\ .$$

Maintenant, la condition $(\mathcal{M}/\mathcal{N})\mathfrak{m}=0$ équivaut à $\mathcal{M}\mathfrak{m}\subset\mathcal{N}$. De la sorte, la formule ci-dessus est vraie par définition de μ pour le sous-module $\mathcal{M}\mathfrak{m}$ de $\mathcal{M}$, en remarquant que $\mathcal{M}\mathfrak{m}\neq\mathcal{M}$ par le lemme de Nakayama (voir [R] (6.11) page 81). □

Nous utiliserons seulement la conséquence suivante.

COROLLAIRE 3.1. *Si $\mathfrak{A}$ est un anneau local fini et $\mathcal{M}$ un sous-$\mathfrak{A}$-module à droite de $\mathfrak{A}^m$ alors*

$$|\mu(\mathcal{M},\mathfrak{A}^m)|\leq \mathrm{Card}(\mathfrak{A}^m/\mathcal{M})^{(m-1)/2}\ .$$

DÉMONSTRATION. Notons $\mathfrak{m}$ l'idéal maximal de $\mathfrak{A}$. Si $(\mathfrak{A}^m/\mathcal{M})\mathfrak{m}\neq 0$, nous avons par l'assertion (3) de la proposition $\mu(\mathcal{M},\mathfrak{A}^m)=0$ donc la majoration est certainement vraie. Si $(\mathfrak{A}^m/\mathcal{M})\mathfrak{m}=0$, le module $\mathfrak{A}^m/\mathcal{M}$ est un $(\mathfrak{A}/\mathfrak{m})$-espace vectoriel de dimension disons ℓ. La proposition 3.2 donne donc $\mu(\mathcal{M},\mathfrak{A}^m)=\mu(0,\mathfrak{A}^m/\mathcal{M})=(-1)^\ell\mathrm{Card}(\mathfrak{A}^m/\mathcal{M})^{(\ell-1)/2}$. Maintenant $\mathfrak{A}^m/\mathcal{M}$ est clairement engendré par m éléments donc $\ell\leq m$ et la majoration s'ensuit. □

Nous savons à ce stade évaluer la fonction de Möbius d'un module sur un anneau local fini donc, par le lemme, nous savons contrôler celle d'un idéal d'un produit d'anneaux de matrices sur de tels anneaux locaux finis. Le lien avec notre situation initiale apparaît dans l'énoncé suivant.

PROPOSITION 3.3. *Si a est un entier naturel non nul, nous avons un isomorphisme d'anneaux de la forme*

$$\mathcal{O}/a\mathcal{O}\simeq\prod_{i=1}^{r}\mathrm{Mat}_{m_im_i}(\mathfrak{A}_i)$$

où r est un entier naturel et, pour $1\leq i\leq r$, $\mathfrak{A}_i$ est un anneau local fini et $1\leq m_i\leq d$.

DÉMONSTRATION. Si l'on omet la condition $m_i\leq d$, ceci est démontré dans [LR] : voir proposition 7.3 et la démonstration du lemme 7.2 qui établit

que $\mathcal{O}/a\mathcal{O}$ en vérifie les hypothèses. Quitte à permuter les facteurs, nous supposons que la suite m_i est décroissante de sorte qu'il nous reste seulement à montrer $m_1 \leq d$. Notons $m = m_1$, $\mathfrak{A} = \mathfrak{A}_1$, $\mathfrak{m}$ son idéal maximal et $k = \mathfrak{A}/\mathfrak{m}$. Le produit $\mathrm{Mat}_{mm}(\mathfrak{m}) \times \prod_{i=2}^{r} \mathrm{Mat}_{m_i m_i}(\mathfrak{A}_i)$ est un idéal bilatère de $\mathcal{O}/a\mathcal{O}$ donc son image réciproque dans $\mathcal{O}$ est un idéal bilatère $\mathcal{I}$ de $\mathcal{O}$ tel que $\mathcal{O}/\mathcal{I} \simeq \mathrm{Mat}_{mm}(k)$. Remarquons que l'on a donc $N(\mathcal{I}) = \mathrm{Card}(k)^{m^2}$ puis, grâce à l'assertion (3) du lemme 3.2, $\mu(\mathcal{I}) = (-1)^m \mathrm{Card}(k)^{m(m-1)/2} = (-1)^m N(\mathcal{I})^{(1/2)-(1/2m)}$ (ceci ne sert pas dans la présente preuve mais montre que $m \leq d$ est indispensable pour avoir le théorème).

Nous notons $\mathcal{O}_Z = \mathcal{O} \cap Z$ et $\mathfrak{p} = \mathcal{I} \cap Z$. L'anneau $\mathcal{O}_Z$ est l'anneau des entiers de Z par maximalité de $\mathcal{O}$: si $x \in Z$ est entier sur $\mathbb{Z}$ de degré disons e l'ensemble $\mathcal{O}' = \mathcal{O} + x\mathcal{O} + \cdots + x^{e-1}\mathcal{O}$ est un anneau (car x est central) donc un ordre de $\mathfrak{D}$ d'où $\mathcal{O}' = \mathcal{O}$ et $x \in \mathcal{O}$. Par ailleurs, $\mathfrak{p}$ est un idéal de $\mathcal{O}_Z$. L'anneau $\mathcal{O}_Z/\mathfrak{p}$ est un sous-anneau de $\mathcal{O}/\mathcal{I} \simeq \mathrm{Mat}_{mm}(k)$ et, comme Z est le centre de $\mathfrak{D}$, l'image de $\mathcal{O}_Z/\mathfrak{p}$ est incluse dans le centre de $\mathrm{Mat}_{mm}(k)$ c'est-à-dire k (matrices scalaires). Ainsi $\mathcal{O}_Z/\mathfrak{p}$ s'identifie à un sous-corps k' de k (en particulier $\mathfrak{p}$ est maximal).

Pour terminer, considérons $\mathfrak{p}\mathcal{O}$: c'est un idéal bilatère de $\mathcal{O}$ inclus dans $\mathcal{I}$. Il y a donc un morphisme d'anneaux surjectif $\mathcal{O}/\mathfrak{p}\mathcal{O} \to \mathcal{O}/\mathcal{I}$. De plus, $\mathcal{O}/\mathfrak{p}\mathcal{O}$ est isomorphe à $(k')^{d^2}$ comme $\mathcal{O}_Z$-module : en effet,

$$\mathcal{O}/\mathfrak{p}\mathcal{O} = \mathcal{O} \otimes_{\mathcal{O}_Z} k' = \mathcal{O} \otimes_{\mathcal{O}_Z} \mathcal{O}_{Z,\mathfrak{p}} \otimes_{\mathcal{O}_{Z,\mathfrak{p}}} k'$$

où $\mathcal{O}_{Z,\mathfrak{p}}$ est le localisé de Z en $\mathfrak{p}$; comme $\mathcal{O}_Z$ est un anneau de Dedekind, $\mathcal{O}_{Z,\mathfrak{p}}$ est un anneau de valuation discrète donc le $\mathcal{O}_{Z,\mathfrak{p}}$-module $\mathcal{O} \otimes_{\mathcal{O}_Z} \mathcal{O}_{Z,\mathfrak{p}}$ (sans torsion car naturellement inclus dans $\mathfrak{D}$) est libre de rang $[\mathfrak{D} : Z] = d^2$ (puisque si l'on fait le produit tensoriel avec Z on retrouve $\mathfrak{D}$). Nous avons donc une surjection de k'-espaces vectoriels $(k')^{d^2} \to \mathrm{Mat}_{mm}(k)$ d'où $(\mathrm{Card}k')^{d^2} \geq (\mathrm{Card}k)^{m^2}$. Enfin, avec $\mathrm{Card}k \geq \mathrm{Card}k' > 1$, il vient $d^2 \geq m^2$ puis $m \leq d$. □

Nous pouvons maintenant conclure.

Démostration du théorème 3.1. Nous choisissons $a > 0$ dans $\mathcal{I} \cap \mathbb{Z}$ de sorte que $a\mathcal{O} \subset \mathcal{I}$. Nous écrivons $\mathcal{O}/a\mathcal{O} \simeq \prod_{i=1}^{r} \mathrm{Mat}_{m_i m_i}(\mathfrak{A}_i)$ comme dans la proposition précédente. L'image $\mathcal{I}/a\mathcal{O}$ de $\mathcal{I}$ dans cet anneau est un produit $\prod_{i=1}^{r} \mathcal{J}_i$ d'idéaux. D'après le lemme 3.2, nous avons (avec l'isomor-

phisme $\mathcal{O}/\mathcal{I} \simeq (\mathcal{O}/a\mathcal{O})/(\mathcal{I}/a\mathcal{O})$)

$$\mu(\mathcal{I}) = \mu(\mathcal{I}, \mathcal{O}) = \mu(0, \mathcal{O}/\mathcal{I}) = \mu(\mathcal{I}/a\mathcal{O}, \mathcal{O}/a\mathcal{O})$$
$$= \mu\left(\prod_{i=1}^{r} \mathcal{J}_i, \prod_{i=1}^{r} \mathrm{Mat}_{m_i m_i}(\mathfrak{N}_i)\right) = \prod_{i=1}^{r} \mu(\mathcal{J}_i, \mathrm{Mat}_{m_i m_i}(\mathfrak{N}_i)) = \prod_{i=1}^{r} \mu(\mathcal{M}_i, \mathfrak{N}_i^{m_i})$$

si $\mathcal{M}_i$ est le sous-module des colonnes des éléments de $\mathcal{J}_i$. Par application du corollaire 3.1, il vient

$$|\mu(\mathcal{I})| \leq \prod_{i=1}^{r} \mathrm{Card}(\mathfrak{N}^{m_i}/\mathcal{M}_i)^{(m_i-1)/2} = \prod_{i=1}^{r} \mathrm{Card}(\mathrm{Mat}_{m_i m_i}(\mathfrak{N}_i)/\mathcal{J}_i)^{(1/2)-(1/2m_i)}.$$

Puisque $m_i \leq d$, nous obtenons

$$|\mu(\mathcal{I})| \leq \left(\prod_{i=1}^{r} \mathrm{Card}(\mathrm{Mat}_{m_i m_i}(\mathfrak{N}_i)/\mathcal{J}_i)\right)^{(1/2)-(1/2d)} = N(\mathcal{I})^{(1/2)-(1/2d)}$$

comme prévu. □

Terminons cette partie en reliant la fonction de Möbius d'un idéal de $\mathcal{S}(\mathcal{O})$ à la fonction zêta de $\mathfrak{D}$ qui est définie par

$$\zeta_{\mathfrak{D}}(s) = \sum_{\mathcal{I} \in \mathcal{S}(\mathcal{O})} \frac{1}{N(\mathcal{I})^s}$$

pour $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$. Cette définition ne dépend pas du choix de l'ordre maximal $\mathcal{O}$ (voir page 130 de [De]).

LEMME 3.3. *On a*

$$\sum_{\mathcal{I} \in \mathcal{S}(\mathcal{O})} \frac{\mu(\mathcal{I})}{N(\mathcal{I})^s} = \frac{1}{\zeta_{\mathfrak{D}}(s)}$$

pour tout $s \in \mathbb{C}$ *avec* $\mathrm{Re}(s) > \dfrac{3}{2} - \dfrac{1}{2d}$.

DÉMONSTRATION. Pour un idéal $\mathcal{I} \in \mathcal{S}(\mathcal{O})$, soient $\mathcal{O}_d(\mathcal{I})$ et $\mathcal{O}_g(\mathcal{I})$ les ordres à droite et à gauche de $\mathcal{I}$ définis par

$$\mathcal{O}_d(\mathcal{I}) = \{x \in \mathfrak{D} \mid \mathcal{I}x \subset \mathcal{I}\} \quad \text{et} \quad \mathcal{O}_g(\mathcal{I}) = \{x \in \mathfrak{D} \mid x\mathcal{I} \subset \mathcal{I}\}.$$

Ici $\mathcal{O}_d(\mathcal{I}) = \mathcal{O}$ et, comme $\mathcal{O}$ est maximal, l'ordre $\mathcal{O}_g(\mathcal{I})$ est également maximal (voir le théorème 17.6 page 173 et la remarque 18.8 (ii) page 179 de [R]). De plus $\mathcal{I} \subset \mathcal{O}_d(\mathcal{I})$ entraîne $\mathcal{I} \subset \mathcal{O}_g(\mathcal{I})$ (théorème 22.8 page 193

de [R]). Puisque la définition de $\zeta_{\mathfrak{D}}$ ne dépend pas du choix de l'ordre maximal, on peut écrire

$$\left(\sum_{\mathcal{I}\in\mathcal{S}(\mathcal{O})}\frac{\mu(\mathcal{I})}{N(\mathcal{I})^s}\right)\zeta_{\mathfrak{D}}(s)=\sum_{\mathcal{I}\in\mathcal{S}(\mathcal{O})}\frac{\mu(\mathcal{I})}{N(\mathcal{I})^s}\sum_{\mathcal{I}'\in\mathcal{S}(\mathcal{O}_g(\mathcal{I}))}\frac{1}{N(\mathcal{I}')^s}\ . \tag{1}$$

Comme $\mathcal{O}_d(\mathcal{I}')=\mathcal{O}_g(\mathcal{I})$, le produit $\mathcal{I}'\mathcal{I}$ est défini et $\mathcal{J}=\mathcal{I}'\mathcal{I}\in\mathcal{S}(\mathcal{O})$ avec $\mathcal{J}\subset\mathcal{I}$. De plus, $N(\mathcal{J})=N(\mathcal{I}')N(\mathcal{I})$ par le théorème 24.4 page 211 de [R]. Les deux sommes du membre de droite de (1) convergent absolument pour $\mathrm{Re}(s)>\dfrac{3}{2}-\dfrac{1}{2d}$ (pour la première somme on utilise le théorème 3.1) ; on peut donc réarranger les termes des deux sommes de sorte que le membre de droite de (1) devient

$$\sum_{\mathcal{I}\in\mathcal{S}(\mathcal{O})}\sum_{\mathcal{J}\in\mathcal{S}(\mathcal{I})}\frac{\mu(\mathcal{I})}{N(\mathcal{J})^s}=\sum_{\mathcal{J}\in\mathcal{S}(\mathcal{O})}\frac{1}{N(\mathcal{J})^s}\sum_{\mathcal{J}\subset\mathcal{I}\in\mathcal{S}(\mathcal{O})}\mu(\mathcal{I})=1$$

ce qui montre le lemme. □

4. Inversion

L'objet de cette partie est de démontrer la proposition 4.1 ci-dessous qui exprime le nombre $\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,M,H)$ de sous-espaces à l'aide du nombre de points d'intersection entre un réseau (variable) et les multiples d'un certain domaine fixé.

Dans cette partie, tous les sous-$\mathcal{O}$-modules de D^M considérés sont des sous-modules à droite. On fixe un ensemble R de représentants $\mathcal{C}\subset\mathcal{O}^M$ des classes d'isomorphie de sous-$\mathcal{O}$-modules de D^M de rang M. On remarquera que deux tels sous-modules $\mathcal{A}$ et $\mathcal{B}$ sont isomorphes si et seulement s'il existe une matrice inversible T de $\mathrm{Mat}_{MM}(D)$ telle que $T\mathcal{A}=\mathcal{B}$. On sait en outre que R est fini d'après le théorème de Jordan-Zassenhaus (voir (26.4) page 228 de [R]).

Pour un sous-$\mathcal{O}$-module $\mathcal{A}$ de D^M de rang M, nous notons simplement $\mathcal{A}^N$ l'ensemble des matrices formées de N colonnes éléments de $\mathcal{A}$, c'est-à-dire que nous écrivons

$$\mathcal{A}^N=\{A\in\mathrm{Mat}_{MN}(D)\mid A\mathcal{O}^N\subset\mathcal{A}\}\ .$$

Par ailleurs, nous définissons le sous-groupe $W_{\mathcal{A}}$ de $\mathrm{Mat}_{MM}(D)^\times$ par

$$W_{\mathcal{A}}=\{T\in\mathrm{Mat}_{MM}(D)^\times\mid T\mathcal{A}=\mathcal{A}\}\ .$$

Si $\mathcal{A} = \mathcal{O}^M$, nous écrivons $W = W_{\mathcal{O}^M} = \mathrm{Mat}_{MM}(\mathcal{O})^\times$. Ce groupe agit à gauche sur l'ensemble

$$\Theta = \{A \in \mathrm{Mat}_{MN}(D \otimes \mathbb{R}) \mid 0 < \mathrm{Nm}(AA^\star) \leq 1\} \tag{2}$$

(puisque si $T \in W$ on a $\mathrm{Nm}(TT^\star) = 1$). Soit S un système de représentants de l'ensemble quotient Θ/W. Finalement, on note $R' = WR$ et, pour $\mathcal{D} \in R'$, on pose $w_{\mathcal{D}} = 1/[W_{\mathcal{D}} : W \cap W_{\mathcal{D}}]$.

Voici le résultat principal de cette partie.

PROPOSITION 4.1. *Pour $H > 0$, on a l'égalité*

$$\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N, M, H) = \sum_{\mathcal{D} \in R'} \sum_{\mathcal{A} \subset \mathcal{D}} w_{\mathcal{D}}\, \mu(\mathcal{A}, \mathcal{D})\, \mathrm{Card}\big(\mathcal{A}^N \cap H^{1/M} N(\mathcal{D})^{1/Mn} S\big),$$

où tous les termes de la double somme sont nuls sauf un nombre fini. Plus précisément, R' est fini et la seconde somme, qui porte sur tous les sous-$\mathcal{O}$-modules de $\mathcal{D}$ de rang M, peut être restreinte à ceux qui vérifient $N(\mathcal{A}) \leq H^n N(\mathcal{D})$.

Pour la démonstration de cette proposition, nous avons besoin de quelques lemmes préliminaires. Commençons par le résultat ci-dessous qui montre notamment que R' est fini et que $w_{\mathcal{D}}$ n'est jamais nul.

LEMME 4.1. *Soient $\mathcal{A}$ et $\mathcal{B}$ deux sous-$\mathcal{O}$-modules de $\mathcal{O}^M$ de rang M. Alors le sous-groupe $W_{\mathcal{A}} \cap W_{\mathcal{B}}$ est d'indice fini dans $W_{\mathcal{A}}$. De plus l'ensemble R' est fini.*

DÉMONSTRATION. On peut supposer $\mathcal{B} \subset \mathcal{A}$. En effet, il existe un entier non nul m tel que $m\mathcal{B} \subset \mathcal{A}$ et $W_{m\mathcal{B}} = W_{\mathcal{B}}$ car $T(m\mathcal{B}) = m\mathcal{B}$ si et seulement si $T\mathcal{B} = \mathcal{B}$.

On considère maintenant l'ensemble $\mathcal{F} = \{\mathcal{B}' \subset \mathcal{A} | N(\mathcal{B}') = N(\mathcal{B})\}$. Pour $\mathcal{A}$ et $\mathcal{B}$ fixés, c'est un ensemble fini car il n'y a qu'un nombre fini de sous-groupes de $\mathcal{A}$ de volume fixé. Si $T \in W_{\mathcal{A}}$ et $\mathcal{B}' \in \mathcal{F}$, alors $\mathcal{A}/\mathcal{B}' \simeq \mathcal{A}/T\mathcal{B}'$ et donc $N(T\mathcal{B}') = N(\mathcal{B}')$. Ceci implique que $W_{\mathcal{A}}$ agit sur $\mathcal{F}$ et on a un morphisme de groupes φ de $W_{\mathcal{A}}$ vers le groupe $\mathfrak{S}_{\mathcal{F}}$ des applications bijectives de $\mathcal{F}$ dans $\mathcal{F}$. Il suit que le noyau $\mathrm{Ker}\varphi$ est d'indice fini dans $W_{\mathcal{A}}$.

Enfin, si $T \in \mathrm{Ker}\varphi$, alors T agit comme l'identité sur $\mathcal{F}$. En particulier $T\mathcal{B} = \mathcal{B}$, d'où $T \in W_{\mathcal{B}}$. On a donc $\mathrm{Ker}\varphi \subset W_{\mathcal{A}} \cap W_{\mathcal{B}} \subset W_{\mathcal{A}}$ ce qui montre que $W_{\mathcal{A}} \cap W_{\mathcal{B}}$ est d'indice fini dans $W_{\mathcal{A}}$.

De la même façon, si $\mathcal{C} \in R$, les éléments de la forme $T\mathcal{C}$ avec $T \in W$ sont des sous-$\mathcal{O}$-modules de $\mathcal{O}^M$ de même norme que $\mathcal{C}$ donc en nombre fini. Par suite la finitude de R implique celle de $R' = WR$. □

Si $\mathcal{A}$ et $\mathcal{B}$ sont comme dans le lemme, nous définissons

$$[W_{\mathcal{A}} : W_{\mathcal{B}}] = \frac{[W_{\mathcal{A}} : W_{\mathcal{A}} \cap W_{\mathcal{B}}]}{[W_{\mathcal{B}} : W_{\mathcal{A}} \cap W_{\mathcal{B}}]} \ .$$

De plus, si Γ est un sous-groupe d'indice fini de $W_{\mathcal{A}}$, l'intersection $W_{\mathcal{B}} \cap \Gamma = W_{\mathcal{B}} \cap W_{\mathcal{A}} \cap \Gamma$ est d'indice fini dans Γ et $W_{\mathcal{A}} \cap W_{\mathcal{B}}$ donc dans $W_{\mathcal{B}}$. Nous posons alors de même

$$[W_{\mathcal{B}} : \Gamma] = \frac{[W_{\mathcal{B}} : W_{\mathcal{B}} \cap \Gamma]}{[\Gamma : W_{\mathcal{B}} \cap \Gamma]} \ .$$

Pour la suite, nous utiliserons la description de la hauteur d'un sous-espace en termes matriciels pour relier l'ensemble des sous-espaces de hauteur bornée à des éléments de l'ensemble Θ. Nous considérons d'abord l'ensemble

$$E = E(H) = \{A \in \mathrm{Mat}_{MN}(D) | 0 < \mathrm{Nm}(AA^\star) \leq H^{2Mn}[\mathcal{O}^M : A\mathcal{O}^N]^{2M}\}$$

et les deux sous-ensembles

$$F_{\mathcal{C}} = F_{\mathcal{C}}(H) = \{A \in E | A\mathcal{O}^N = \mathcal{C}\} \ , \quad \tilde{F}_{\mathcal{C}} = \tilde{F}_{\mathcal{C}}(H) = \{A \in E | A\mathcal{O}^N \simeq \mathcal{C}\} \ ,$$

où $\mathcal{C}$ est un sous-$\mathcal{O}$-module de $\mathcal{O}^M$ de rang M. On note que le groupe $\mathrm{Mat}_{MM}(D)^\times$ agit à gauche sur E car $H^{\mathcal{O},\star}(BA) = H^{\mathcal{O},\star}(A)$ pour tout $B \in \mathrm{Mat}_{MM}(D)^\times$ (voir proposition 6.1 de [LR]). Comme $BA\mathcal{O}^N \simeq A\mathcal{O}^N$, le groupe $\mathrm{Mat}_{MM}(D)^\times$ laisse stables les sous-ensembles $\tilde{F}_{\mathcal{C}}$ de E. Enfin, le groupe $W_{\mathcal{C}}$ agit à gauche sur $F_{\mathcal{C}}$.

LEMME 4.2. *Il y a une bijection naturelle entre $F_{\mathcal{C}}/W_{\mathcal{C}}$ et $\tilde{F}_{\mathcal{C}}/\mathrm{Mat}_{MM}(D)^\times$.*

DÉMONSTRATION. L'inclusion $F_{\mathcal{C}} \subset \tilde{F}_{\mathcal{C}}$ induit une application ψ de $F_{\mathcal{C}}$ vers le quotient $\tilde{F}_{\mathcal{C}}/\mathrm{Mat}_{MM}(D)^\times$. Cette application est surjective : si $A \in \tilde{F}_{\mathcal{C}}$, alors $A\mathcal{O}^N \simeq \mathcal{C}$, ce qui veut dire qu'il existe $B \in \mathrm{Mat}_{MM}(D)^\times$ tel que $BA\mathcal{O}^N = \mathcal{C}$. Donc $BA \in F_{\mathcal{C}}$ et l'image de BA par ψ est dans la même orbite que A.

En outre, on a $\psi(A) = \psi(A')$ pour $A, A' \in F_{\mathcal{C}}$ si et seulement s'il existe $T \in \mathrm{Mat}_{MM}(D)^\times$ tel que $TA = A'$. Mais $\mathcal{C} = A\mathcal{O}^N = A'\mathcal{O}^N = TA\mathcal{O}^N = T\mathcal{C}$, d'où $T \in W_{\mathcal{C}}$. Ainsi $\psi(A) = \psi(A')$ si et seulement si $A' = TA$ avec $T \in W_{\mathcal{C}}$ ce qui montre le lemme. □

Nous pouvons à présent calculer le nombre de sous-espaces de hauteur au plus H en fonction des ensembles quotient $F_{\mathcal{C}}/W_{\mathcal{C}}$. Pour cela, on introduit la fonction

$$f_{\mathcal{C}}(H) = \frac{\mathrm{Card}(F_{\mathcal{C}}(H)/W_{\mathcal{C}})}{[W : W_{\mathcal{C}}]}.$$

LEMME 4.3. *On a*

$$\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,M,H) = \mathcal{N}^{\mathcal{O},\star}_{\mathrm{dte}}(N,N-M,H) = \sum_{\mathcal{C}\in R} [W : W_{\mathcal{C}}] f_{\mathcal{C}}(H)\ .$$

DÉMONSTRATION. Soit V un sous-espace (à droite) de D^N de codimension M. Il existe une matrice $A \in \mathrm{Mat}_{MN}(D)$ telle que $V = \{X \in D^N | AX = 0\}$ et on a

$$H^{\mathcal{O},\star}(V) = H^{\mathcal{O},\star}(A) = \mathrm{Nm}(AA^\star)^{1/2Mn}[\mathcal{O}^M : A\mathcal{O}^N]^{-1/n}$$

par les propositions 6.1 et 6.3 de [LR]. La matrice A est unique à multiplication à gauche par une matrice $B \in \mathrm{Mat}_{MM}(D)^\times$ près. Le nombre $\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,M,H)$ est donc égal au nombre d'orbites à gauche de E sous l'action de $\mathrm{Mat}_{MM}(D)^\times$.

Nous écrivons $E = \bigcup_{\mathcal{C}\in R} \tilde{F}_{\mathcal{C}}$ où l'union est disjointe. Comme les $\tilde{F}_{\mathcal{C}}$ sont stables sous $\mathrm{Mat}_{MM}(D)^\times$, on a

$$E/\mathrm{Mat}_{MM}(D)^\times = \bigcup_{\mathcal{C}\in R} \tilde{F}_{\mathcal{C}}/\mathrm{Mat}_{MM}(D)^\times.$$

Ainsi, par le lemme 4.2,

$$\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N,M,H) = \sum_{\mathcal{C}\in R} \mathrm{Card}\big(\tilde{F}_{\mathcal{C}}/\mathrm{Mat}_{MM}(D)^\times\big) = \sum_{\mathcal{C}\in R} \mathrm{Card}\big(F_{\mathcal{C}}/W_{\mathcal{C}}\big)$$

ce qui donne l'identité souhaitée par définition de $f_{\mathcal{C}}(H)$. □

Il nous reste à calculer $f_{\mathcal{C}}(H)$ pour $\mathcal{C} \in R$. Pour faire ceci nous considérons l'ensemble

$$G_{\mathcal{C}} = G_{\mathcal{C}}(H) = \{A \in \mathrm{Mat}_{MN}(D) \mid 0 < \mathrm{Nm}(AA^\star) \le H^{2Mn},\ A\mathcal{O}^N \subset \mathcal{C}\}\ ,$$

où $\mathcal{C}$ est un sous-$\mathcal{O}$-module de $\mathcal{O}^M$ de rang M. Le groupe $W_{\mathcal{C}}$ agit à gauche sur $G_{\mathcal{C}}$. En effet, si $A \in G_{\mathcal{C}}$ et $T \in W_{\mathcal{C}}$, alors $TA\mathcal{O}^N \subset T\mathcal{C} = \mathcal{C}$ et $\mathrm{Nm}((TA)(TA)^\star) = \mathrm{Nm}(AA^\star)\mathrm{Nm}(T)^2 = \mathrm{Nm}(AA^\star) \le H^{2Mn}$ car $T\mathcal{C} = \mathcal{C}$ entraîne $\mathrm{Nm}(T) = \pm 1$ *via* $N(T\mathcal{C}) = N(\mathcal{C})|\mathrm{Nm}(T)|^{1/M}$.

On pose

$$g_{\mathcal{C}}(H) = \frac{\mathrm{Card}(G_{\mathcal{C}}(H)/W_{\mathcal{C}})}{[W : W_{\mathcal{C}}]} \ .$$

LEMME 4.4. *On a*

$$g_{\mathcal{C}}(H) = \sum_{\mathcal{A}\subset\mathcal{C}} f_{\mathcal{A}}(HN(\mathcal{A})^{-1/n}) \ ,$$

où la somme porte sur tous les sous-$\mathcal{O}$-modules $\mathcal{A}$ de $\mathcal{C}$ de rang M. C'est une somme finie.

DÉMONSTRATION. Soit $A \in G_{\mathcal{C}}(H)$. Alors $\mathcal{A} = A\mathcal{O}^N \subset \mathcal{C}$ est un sous-$\mathcal{O}$-module de $\mathcal{O}^M$ de rang M et, comme $0 < \mathrm{Nm}(AA^\star) \leq H^{2Mn}$, on voit que $A \in F_{\mathcal{A}}(H_{\mathcal{A}})$, où $H_{\mathcal{A}} = HN(\mathcal{A})^{-1/n}$. On peut donc écrire

$$G_{\mathcal{C}}(H) = \bigcup_{\mathcal{A}\subset\mathcal{C}} F_{\mathcal{A}}(H_{\mathcal{A}}) \tag{3}$$

où l'union est disjointe.

De plus, si $A \in F_{\mathcal{A}}(H_{\mathcal{A}})$, alors

$$N(\mathcal{A}) = [\mathcal{O}^M : A\mathcal{O}^N] \leq \mathrm{Nm}(AA^\star)^{1/2M} \leq H^n \ , \tag{4}$$

puisque $H^{\mathcal{O},\star}(A) \geq 1$ (voir lemme 2.1). Donc $F_{\mathcal{A}}(H_{\mathcal{A}})$ est vide si $\mathcal{A} \subset \mathcal{C}$ avec $N(\mathcal{A}) > H^n$. Comme il n'y a qu'un nombre fini de sous-groupes $\mathcal{A}$ de $\mathcal{C}$ de norme bornée, l'union dans l'équation (3) est finie.

On pose maintenant

$$\Gamma = \bigcap_{\substack{\mathcal{A}\subset\mathcal{C}\\ N(\mathcal{A})\leq H^n}} W_{\mathcal{A}}$$

et on note que Γ est d'indice fini dans $W_{\mathcal{C}}$ (c'est une intersection finie de sous-groupes d'indices finis). Le groupe Γ agit à gauche sur $G_{\mathcal{C}}(H)$ et il laisse stable $F_{\mathcal{A}}(H_{\mathcal{A}})$ pour tout $\mathcal{A} \subset \mathcal{C}$. En utilisant que $\mathrm{Card}(G_{\mathcal{C}}(H)/\Gamma) = \mathrm{Card}(G_{\mathcal{C}}(H)/W_{\mathcal{C}})[W_{\mathcal{C}} : \Gamma]$, on trouve que

$$g_{\mathcal{C}}(H) = \frac{\mathrm{Card}(G_{\mathcal{C}}(H)/\Gamma)}{[W : \Gamma]} = \sum_{\mathcal{A}\subset\mathcal{C}} \frac{\mathrm{Card}(F_{\mathcal{A}}(H_{\mathcal{A}})/\Gamma)}{[W : \Gamma]} = \sum_{\mathcal{A}\subset\mathcal{C}} f_{\mathcal{A}}(H_{\mathcal{A}}) \ .$$

C'est une somme finie car $f_{\mathcal{A}}(H_{\mathcal{A}}) = 0$ si $N(\mathcal{A}) > H^n$. □

DÉMONSTRATION DE LA PROPOSITION 4.1. Pour calculer $f_{\mathcal{C}}(H)$, $\mathcal{C} \in R$, nous utilisons la formule d'inversion de Möbius (lemme 3.1) : à partir du

lemme 4.4, elle donne directement

$$f_{\mathcal{C}}(HN(\mathcal{C})^{-1/n}) = \sum_{\mathcal{A}\subset\mathcal{C}} \mu(\mathcal{A},\mathcal{C})\, g_{\mathcal{A}}(H). \tag{5}$$

En utilisant l'inégalité (4) on voit que $g_{\mathcal{A}}(H) = 0$ si $N(\mathcal{A}) > H^n$. La somme dans (5) est donc finie et porte sur tout $\mathcal{A} \subset \mathcal{C}$ avec $N(\mathcal{A}) \leq H^n$.

Soit Γ comme dans la démonstration du lemme 4.4. Nous démontrons maintenant que

$$g_{\mathcal{A}}(H) = \frac{1}{[W:\Gamma]} \sum_{T\in\Gamma\backslash W} \mathrm{Card}\big((T^{-1}\mathcal{A})^N \cap H^{1/M} S\big). \tag{6}$$

On note d'abord $\mathrm{Card}(G_{\mathcal{A}}(H)/W\cap W_{\mathcal{A}}) = \mathrm{Card}(G_{\mathcal{A}}(H)/W_{\mathcal{A}})[W_{\mathcal{A}} : W\cap W_{\mathcal{A}}]$, d'où

$$g_{\mathcal{A}}(H) = \frac{1}{[W : W\cap W_{\mathcal{A}}]} \mathrm{Card}\big((\mathcal{A}^N \cap H^{1/M}\Theta)/W\cap W_{\mathcal{A}}\big) \tag{7}$$

avec Θ défini par (2).

Soit S un domaine fondamental de Θ sous l'action de W comme dans l'énoncé de la proposition 4.1. Si $\{T_i\}$ représentent les classes à droite de W modulo $W\cap W_{\mathcal{A}}$, alors $\bigcup_i T_i S$ représente Θ modulo $W\cap W_{\mathcal{A}}$. En effet, si $A\in\Theta$ il existe $T\in W$, $B\in S$ tels que $A = TB$. De plus, $T = T'T_i$, où $T'\in W\cap W_{\mathcal{A}}$. Donc $A\in (W\cap W_{\mathcal{A}})T_iB$. En outre, si $T'T_iB = T_jB'$ avec $T'\in W\cap W_{\mathcal{A}}$ et $B,B'\in S$, alors $T_j^{-1}T'T_iB = B'$, où $T_j^{-1}T'T_i\in W$. Donc $B = B'$. Il suit que $T'T_i = T_j$, d'où $T_j\in (W\cap W_{\mathcal{A}})T_i$ ce qui signifie que $T_j = T_i$.

On conclut que

$$\begin{aligned}
&\mathrm{Card}\big((\mathcal{A}^N \cap H^{1/M}\Theta)/W\cap W_{\mathcal{A}}\big)\\
&\quad= \mathrm{Card}\Big(\mathcal{A}^N \cap \Big(\bigcup_i H^{1/M} T_i S\Big)\Big)\\
&\quad= \sum_{i=1}^{[W:W\cap W_{\mathcal{A}}]} \mathrm{Card}\big(\mathcal{A}^N \cap H^{1/M} T_i S\big)\\
&\quad= \sum_{i=1}^{[W:W\cap W_{\mathcal{A}}]} \mathrm{Card}\big((T_i^{-1}\mathcal{A})^N \cap H^{1/M} S\big)\\
&\quad= \frac{1}{[W\cap W_{\mathcal{A}} : \Gamma]} \sum_{T\in\Gamma\backslash W} \mathrm{Card}\big((T^{-1}\mathcal{A})^N \cap H^{1/M} S\big)\ .
\end{aligned}$$

Avec (7) ceci montre bien (6).

Si $\mathcal{A} \subset \mathcal{C}$, alors $T^{-1}\mathcal{A} \subset T^{-1}\mathcal{C}$ et $\mu(\mathcal{A},\mathcal{C}) = \mu(T^{-1}\mathcal{A}, T^{-1}\mathcal{C})$, donc les équations (5) et (6) donnent

$$f_{\mathcal{C}}(H) = \frac{1}{[W : \Gamma]} \sum_{T \in \Gamma\backslash W} \sum_{\mathcal{A} \subset T^{-1}\mathcal{C}} \mu(\mathcal{A}, T^{-1}\mathcal{C}) \operatorname{Card}(\mathcal{A}^N \cap H^{1/M} N(\mathcal{C})^{1/Mn} S) \,.$$

Ensuite, la somme sur tout $T \in \Gamma\backslash W$ peut être remplacée par $[W \cap W_{\mathcal{C}} : \Gamma]$ fois la somme sur tout $T \in W \cap W_{\mathcal{C}}\backslash W$. En utilisant le lemme 4.3 et $[W : \Gamma] = [W : W_{\mathcal{C}}][W_{\mathcal{C}} : W \cap W_{\mathcal{C}}][W \cap W_{\mathcal{C}} : \Gamma]$ on trouve que le nombre $\mathcal{N}^{\mathcal{O},\star}_{\text{gche}}(N, M, H)$ est égal à

$$\sum_{\mathcal{C} \in R} \frac{1}{[W_{\mathcal{C}} : W \cap W_{\mathcal{C}}]} \sum_{T \in W \cap W_{\mathcal{C}}\backslash W} \sum_{\mathcal{A} \subset T^{-1}\mathcal{C}} \mu(\mathcal{A}, T^{-1}\mathcal{C}) \operatorname{Card}(\mathcal{A}^N \cap H^{1/M} N(\mathcal{C})^{1/Mn} S) \,.$$

Enfin, on peut remplacer les deux sommes sur $\mathcal{C} \in R$ et $T \in W \cap W_{\mathcal{C}}\backslash W$ par la somme sur $\mathcal{D} \in R'$, car $T\mathcal{C} = T'\mathcal{C}$ pour $T, T' \in W$ si et seulement si T et T' sont dans la même classe modulo $W \cap W_{\mathcal{C}}$. De plus, il y a une bijection entre $W_{\mathcal{C}}$ et $W_{\mathcal{D}}$ pour $\mathcal{C} \in R$, $T \in W$ et $\mathcal{D} = T\mathcal{C}$. En effet, $T' \in W_{\mathcal{C}}$ si et seulement si $TT'T^{-1} \in W_{\mathcal{D}}$. Donc $[W_{\mathcal{C}} : W \cap W_{\mathcal{C}}] = [W_{\mathcal{D}} : W \cap W_{\mathcal{D}}] = w_{\mathcal{D}}^{-1}$ et on trouve le résultat souhaité en notant que l'on a $N(\mathcal{C}) = N(\mathcal{D})$ car $\operatorname{Nm}(T) = \pm 1$ pour tout $T \in W$. □

REMARQUE. L'argument final de cette démonstration montre aussi que l'on a

$$\sum_{\mathcal{D} \in R'} w_{\mathcal{D}} = \sum_{\mathcal{C} \in R} [W : W_{\mathcal{C}}]$$

(ces deux sommes sont égales à $\sum_{\mathcal{C} \in R} \sum_{T \in W \cap W_{\mathcal{C}}\backslash W} [W_{\mathcal{C}} : W \cap W_{\mathcal{C}}]^{-1}$).

5. Sommation sur les sous-modules

Nous conservons les notations de la partie précédente. En particulier, soient $\mathcal{A}$ et $\mathcal{D}$ deux sous-$\mathcal{O}$-modules à droite de $\mathcal{O}^M$ de rang M tels que $\mathcal{A} \subset \mathcal{D}$. Dans cette partie, nous établissons une estimation de $\mathcal{N}^{\mathcal{O},\star}_{\text{gche}}(N, M, H)$ sous la condition qu'un résultat de la forme

$$(\dagger) \qquad \left| \operatorname{Card}(\mathcal{A}^N \cap H^{1/M} N(\mathcal{D})^{1/Mn} S) - c_1 \frac{H^{Nn}}{[\mathcal{D} : \mathcal{A}]^N} \right| \leq c_2 \frac{H^{Nn-1/M}}{[\mathcal{D} : \mathcal{A}]^{N-1/Mn}}$$

existe, où c_1 et c_2 sont des constantes indépendantes de $\mathcal{A}$ et $\mathcal{D}$.

Nous démontrerons (†) seulement pour $M = 1$ dans la partie 7 et nous donnerons des constantes explicites c_1 et c_2.

Pour énoncer notre résultat, notons $h' = \sum_{\mathcal{C}\in R} [W : W_{\mathcal{C}}]$. Dans le cas où $M = 1$ il s'agit bien du nombre h' défini dans l'introduction.

THÉORÈME 5.1. *Sous l'hypothèse* (†) *et si* $N > 3M/2 - 1/2d + 1/Mn$, *on a*

$$\left| \mathcal{N}^{\mathcal{O},\star}_{\text{gche}}(N, M, H) - \frac{c_1 h' H^{Nn}}{\zeta_D(N)\cdots\zeta_D(N-M+1)} \right| \leq c_2 h' (N^2 n)^n H^{Nn-1/M}.$$

L'inégalité sur N peut se simplifier de la manière suivante : dans presque tous les cas, le nombre $3M/2 - 1/2d + 1/Mn$ est contenu dans l'intervalle ouvert $](3M-1)/2, 3M/2[$ qui ne contient pas d'entiers donc la condition est équivalente à $N \geq 3M/2$. Les exceptions sont les cas où $Mn \leq 2d$ c'est-à-dire où (M, n, d) est l'un des triplets $(1,1,1)$, $(2,1,1)$, $(1,2,1)$ ou $(1,4,2)$. En examinant ces cas, on voit que la condition peut s'écrire $N \geq 3$ dans le premier cas et $N \geq 2M$ dans les autres.

Pour la démonstration de ce théorème nous utiliserons deux résultats sur la fonction zêta de $\mathrm{Mat}_{MM}(D)$.

LEMME 5.1. *Soit* $m > 3M/2 - 1/2d$ *un entier naturel et* $\mathcal{D}$ *un sous-*$\mathcal{O}$*-module à droite de* $\mathcal{O}^M$ *de rang* M. *Alors*

$$\sum_{\mathcal{A}\subset\mathcal{D}} \frac{\mu(\mathcal{A}, \mathcal{D})}{[\mathcal{D} : \mathcal{A}]^m} = \zeta_{\mathrm{Mat}_{MM}(D)}(m/M)^{-1}.$$

DÉMONSTRATION. Nous utilisons la bijection (voir l'assertion (3) du lemme 3.2) qui associe à un sous-$\mathcal{O}$-module à droite $\mathcal{A}$ de $\mathcal{O}^M$ de rang M l'idéal à droite $\mathcal{I}_{\mathcal{A}}$ de $\mathrm{Mat}_{MM}(\mathcal{O})$ formé des matrices dont toutes les colonnes appartiennent à $\mathcal{A}$. Par le lemme 3.2 on a $\mu(\mathcal{A}, \mathcal{D}) = \mu(\mathcal{I}_{\mathcal{A}}, \mathcal{I}_{\mathcal{D}})$ et $[\mathcal{D} : \mathcal{A}] = [\mathcal{I}_{\mathcal{D}} : \mathcal{I}_{\mathcal{A}}]^{1/M}$.

Notons, comme dans la démonstration du lemme 3.3, $\mathcal{O}_g(\mathcal{I}_{\mathcal{D}})$ l'ordre à gauche de $\mathcal{I}_{\mathcal{D}}$. Par le théorème 22.19 (ii) page 197 de [R] on a $\mathcal{I}_{\mathcal{A}} \subset \mathcal{I}_{\mathcal{D}}$ si et seulement s'il existe un idéal à droite $\mathcal{I}$ de $\mathcal{O}_g(\mathcal{I}_{\mathcal{D}})$ tel que $\mathcal{I}_{\mathcal{A}} = \mathcal{I}\mathcal{I}_{\mathcal{D}}$. Donc $[\mathcal{I}_{\mathcal{D}} : \mathcal{I}_{\mathcal{A}}] = [\mathcal{I}_{\mathcal{D}} : \mathcal{I}\mathcal{I}_{\mathcal{D}}] = N(\mathcal{I})$ et $\mu(\mathcal{I}_{\mathcal{A}}, \mathcal{I}_{\mathcal{D}}) = \mu(\mathcal{I}, \mathcal{O}_g(\mathcal{I}_{\mathcal{D}})) = \mu(\mathcal{I})$. Par conséquent,

$$\sum_{\mathcal{A}\subset\mathcal{D}} \frac{\mu(\mathcal{A}, \mathcal{D})}{[\mathcal{D} : \mathcal{A}]^m} = \sum_{\mathcal{I}_{\mathcal{A}}\subset\mathcal{I}_{\mathcal{D}}} \frac{\mu(\mathcal{I}_{\mathcal{A}}, \mathcal{I}_{\mathcal{D}})}{[\mathcal{I}_{\mathcal{D}} : \mathcal{I}_{\mathcal{A}}]^{m/M}} = \sum_{\mathcal{I}\in\mathcal{S}(\mathcal{O}_g(\mathcal{I}_{\mathcal{D}}))} \frac{\mu(\mathcal{I})}{N(\mathcal{I})^{m/M}}$$

et en utilisant le lemme 3.3 on trouve l'identité souhaitée. □

Le lemme suivant fait le lien entre les fonctions zêta de $\mathrm{Mat}_{MM}(D)$ et de D et en donne une majoration simple.

LEMME 5.2. *Pour tout $s \in \mathbb{C}$ avec $\mathrm{Re}(s) > 1$ on a*

$$\zeta_{\mathrm{Mat}_{MM}(D)}(s) = \prod_{i=0}^{M-1} \zeta_D(Ms - i)$$

et

$$|\zeta_{\mathrm{Mat}_{MM}(D)}(s)| \leq \left(\frac{\mathrm{Re}(s)}{\mathrm{Re}(s)-1}\right)^{[Z:\mathbb{Q}]}.$$

DÉMONSTRATION. La formule de Käte Hey (voir (4) page 130 de [De]) s'écrit

$$\zeta_{\mathrm{Mat}_{MM}(D)}(s) = \prod_{\mathfrak{p}} \prod_{\substack{i=0 \\ e_{\mathfrak{p}}|i}}^{Md-1} \left(1 - \frac{1}{N(\mathfrak{p})^{Mds-i}}\right)^{-1}$$

où $\mathfrak{p}$ parcourt les idéaux premiers non nuls de $\mathcal{O}_Z$ (rappelons que Z est le centre de D donc de $\mathrm{Mat}_{MM}(D)$) et $e_{\mathfrak{p}}$ est l'indice de ramification de $\mathfrak{p}$ dans $\mathrm{Mat}_{MM}(\mathcal{O})$. Comme $\mathrm{Mat}_{MM}(\mathcal{O})$ n'est pas ramifié au-dessus de $\mathcal{O}$, l'indice $e_{\mathfrak{p}}$ ne dépend pas de M et il divise $d = [D : Z]^{1/2}$. Ainsi en posant $i = dj + k$ nous avons

$$\prod_{\substack{i=0 \\ e_{\mathfrak{p}}|i}}^{Md-1} 1 - \frac{1}{N(\mathfrak{p})^{Mds-i}} = \prod_{j=0}^{M-1} \prod_{\substack{k=0 \\ e_{\mathfrak{p}}|k}}^{d-1} 1 - \frac{1}{N(\mathfrak{p})^{d(Ms-j)-k}}$$

qui donne par produit la première formule de l'énoncé. Pour la seconde, on a

$$|\zeta_{\mathrm{Mat}_{MM}(D)}(s)| \leq \prod_{\mathfrak{p}} \prod_{i=0}^{Md-1} \left(1 - \frac{1}{N(\mathfrak{p})^{Md\mathrm{Re}(s)-i}}\right)^{-1} = \prod_{i=0}^{Md-1} \zeta_Z(Md\mathrm{Re}(s) - i).$$

Nous utilisons ensuite pour $x > 1$ la majoration $\zeta_Z(x) \leq \zeta_{\mathbb{Q}}(x)^{[Z:\mathbb{Q}]}$ (voir corollaire 3 page 315 de [N]) et l'estimation facile $\zeta_{\mathbb{Q}}(x) \leq 1 + \int_1^{\infty} t^{-x} dt = x/(x-1)$. Finalement on trouve

$$|\zeta_{\mathrm{Mat}_{MM}(D)}(s)| \leq \prod_{i=0}^{Md-1} \left(\frac{Md\mathrm{Re}(s) - i}{Md\mathrm{Re}(s) - i - 1}\right)^{[Z:\mathbb{Q}]} = \left(\frac{\mathrm{Re}(s)}{\mathrm{Re}(s)-1}\right)^{[Z:\mathbb{Q}]}.$$

□

DÉMOSTRATION DU THÉORÈME 5.1. Soit $\mathcal{D} \in R'$. Écrivons

$$\sum_{\mathcal{A}\subset\mathcal{D}} \mu(\mathcal{A},\mathcal{D})\mathrm{Card}(\mathcal{A}^N \cap H^{1/M}N(\mathcal{D})^{1/Mn}S) = \alpha(\mathcal{D}) + \beta(\mathcal{D})$$

où

$$\alpha(\mathcal{D}) = c_1 H^{Nn} \sum_{\mathcal{A}\subset\mathcal{D}} \frac{\mu(\mathcal{A},\mathcal{D})}{[\mathcal{D}:\mathcal{A}]^N}$$

et

$$\beta(\mathcal{D}) = \sum_{\mathcal{A}\subset\mathcal{D}} \mu(\mathcal{A},\mathcal{D})\left\{\mathrm{Card}(\mathcal{A}^N \cap H^{1/M}N(\mathcal{D})^{1/Mn}S) - \frac{c_1 H^{Nn}}{[\mathcal{D}:\mathcal{A}]^N}\right\}.$$

Par les lemmes 5.1 et 5.2 on a immédiatement

$$\alpha(\mathcal{D}) = \frac{c_1 H^{Nn}}{\zeta_{\mathrm{Mat}_{MM}(D)}(N/M)} = \frac{c_1 H^{Nn}}{\zeta_D(N)\cdots\zeta_D(N-M+1)}$$

si $N > 3M/2 - 1/2d$.

Pour l'estimation du terme $\beta(\mathcal{D})$ nous obtenons

$$|\beta(\mathcal{D})| \le c_2 H^{Nn-1/M} \sum_{\mathcal{A}\subset\mathcal{D}} \frac{|\mu(\mathcal{A},\mathcal{D})|}{[\mathcal{D}:\mathcal{A}]^{N-1/Mn}}$$

grâce à la majoration (†). Par la dernière formule de la démonstration du lemme 5.1, la somme du membre de droite est égale à

$$\begin{aligned}\sum_{\mathcal{I}\in\mathcal{S}(\mathcal{O}_g(\mathcal{I}_\mathcal{D}))} \frac{|\mu(\mathcal{I})|}{N(\mathcal{I})^{N/M-1/M^2n}} &\le \sum_{\mathcal{I}\in\mathcal{S}(\mathcal{O}_g(\mathcal{I}_\mathcal{D}))} \frac{1}{N(\mathcal{I})^{N/M-1/M^2n+1/2Md-1/2}} \\ &= \zeta_{\mathrm{Mat}_{MM}(D)}(N/M - 1/M^2n + 1/2Md - 1/2)\end{aligned}$$

en utilisant le théorème 3.1 pour l'algèbre $\mathrm{Mat}_{MM}(D)$ lorsque $N > 3M/2 - 1/2d + 1/Mn$. Ici le rationnel $s = N/M - 1/M^2n + 1/2Md - 1/2$ vérifie $s > 1$ et $2M^2ns \in \mathbb{Z}$ donc $s \ge 1 + 1/2M^2n$. Par suite le lemme 5.2 montre

$$\zeta_{\mathrm{Mat}_{MM}(D)}(s) \le (1 + 2M^2n)^{[Z:\mathbb{Q}]} \le (N^2n)^n.$$

Nous aboutissons donc à $|\beta(\mathcal{D})| \le c_2(N^2n)^n H^{Nn-1/M}$.

Par la proposition 4.1 ceci nous donne le résultat car $\sum_{\mathcal{D}\in R'} w_\mathcal{D} = h'$. □

6. Domaine fondamental

Dans cette partie, nous nous attachons à la description de l'ensemble S apparu dans la partie 4 en vue de démontrer (dans la partie suivante) la

majoration (†) de la partie 5. Alors que tout ce que nous avons fait jusqu'ici vaut pour M quelconque, nous nous limiterons désormais au cas $M = 1$ c'est-à-dire au cas des sous-espaces de (co)dimension 1 comme dans le théorème 1.1. Cette restriction trouve son origine dans le fait suivant : il est possible de choisir S borné exclusivement lorsque $M = 1$.

Lorsque $M = 1$ nous avons $W = \mathcal{O}^\times$ avec les notations de la partie 4. Nous faisons donc agir le groupe $\mathcal{O}^\times$ à gauche. Pour commencer, considérons son action sur $(D \otimes \mathbb{R})^\times$. Trouver un domaine fondamental revient à choisir un point dans chaque orbite. Une idée naturelle consiste à choisir un point de norme minimale. Ceci nous amène à poser

$$F = \{x \in (D \otimes \mathbb{R})^\times \mid \forall u \in \mathcal{O}^\times \ |x| \leq |ux|\}.$$

Ce domaine est visiblement stable par homothéties (si $x \in F$ alors $\mathbb{R}^\times x \subset F$). Nous considérons aussi

$$F^{\leq 1} = \{x \in F \mid |\mathrm{Nm}(x)| \leq 1\}.$$

Notre première tâche est de montrer que $F^{\leq 1}$ est borné. En d'autres termes, il s'agit de montrer la finitude de

$$\rho = \sup_{x \in F^{\leq 1}} |x| = \sup_{x \in F} \frac{|x|}{|\mathrm{Nm}(x)|^{1/n}}.$$

Nous faisons ceci après un lemme préliminaire (également utile dans la partie suivante) qui illustre les contraintes qu'impose aux minima successifs d'un réseau le fait que ce réseau soit un $\mathcal{O}$-module. Rappelons que le i-ème minimum μ_i d'un réseau est l'infimum des μ pour lesquels il existe i vecteurs indépendants dans ce réseau de norme euclidienne plus petite que μ.

Lemme 6.1. *Soit M un sous-$\mathcal{O}$-module (à droite ou à gauche) de type fini et sans torsion de $D \otimes \mathbb{R}$ et soient $\mu_1 \leq \cdots \leq \mu_n$ ses minima successifs. Alors*

(1) $\mathrm{vol}(M) \leq \mu_1 \cdots \mu_n \leq \sqrt{n}^{\,n} \mathrm{vol}(M)$.

(2) $\mathrm{vol}(M)^{1/n} \leq \mu_n \leq \sqrt{n}\, \mathrm{vol}(\mathcal{O})^{1-1/n} \mathrm{vol}(M)^{1/n}$.

(3) $\sqrt{n}\, \dfrac{\mathrm{vol}(M)^{1/n}}{\mathrm{vol}(\mathcal{O})^{1/n}} \leq \mu_1 \leq \sqrt{n}\, \mathrm{vol}(M)^{1/n}$.

Démonstration. L'inégalité de gauche dans (1) résulte de l'inégalité d'Hadamard, celle de droite du second théorème de Minkowski : la constante qui apparaît est $(4/\pi)^{n/2}\Gamma(n/2+1)$ dont on vérifie facilement qu'elle

n'excède pas $n^{n/2}$. Ensuite l'inégalité de gauche dans (2) et celle de droite dans (3) découlent immédiatement de (1).

Lorsque $x \in M$ est non nul, nous avons $|x| \geq \sqrt{n}\,|\mathrm{Nm}(x)|^{1/n}$ par l'assertion (4) du lemme 2.2. Si M' est le sous-module de M engendré par x alors $|\mathrm{Nm}(x)| = \mathrm{vol}(M')/\mathrm{vol}(\mathcal{O}) \geq \mathrm{vol}(M)/\mathrm{vol}(\mathcal{O})$. En combinant, ceci démontre (3). Pour terminer d'établir (2), nous utilisons $\mu_n \leq (\mu_1 \cdots \mu_n)/\mu_1^{n-1} \leq \sqrt{n}^{\,n}\,\mathrm{vol}(M)/\mu_1^{n-1}$ et la minoration de μ_1 que nous venons d'établir. □

Ceci nous permet de montrer à présent que ρ est fini.

LEMME 6.2. *Le domaine $F^{\leq 1}$ est borné. Plus précisément, si ξ est un réel tel que tout idéal principal à droite de $\mathcal{O}$ de norme $\leq \mathrm{vol}(\mathcal{O})$ admet un générateur b avec $|b| \leq \xi$ alors*

$$\sqrt{n} \leq \rho \leq \sqrt{n}\,\mathrm{vol}(\mathcal{O})^{1/n}\xi^{n-1}.$$

DÉMONSTRATION. Soit $x \in F^{\leq 1}$. On considère $M = \mathcal{O}x$ qui est un $\mathcal{O}$-module à gauche sans torsion (x étant inversible) et μ_1 son premier minimum. D'après le lemme précédent, $\mu_1 \leq \sqrt{n}\,\mathrm{vol}(\mathcal{O}x)^{1/n}$. Choisissons ensuite $y \in \mathcal{O}x$ avec $|y| = \mu_1$ et considérons également le sous-$\mathcal{O}$-module $M' = \mathcal{O}y \subset M$. Celui-ci admet visiblement encore μ_1 comme premier minimum et donc, à nouveau par le lemme précédent, $\mu_1 \geq \sqrt{n}\,\mathrm{vol}(\mathcal{O}y)^{1/n}/\mathrm{vol}(\mathcal{O})^{1/n}$. En combinant les deux inégalités, il vient

$$|\mathrm{Nm}(yx^{-1})| = \frac{\mathrm{vol}(\mathcal{O}y)}{\mathrm{vol}(\mathcal{O}x)} \leq \mathrm{vol}(\mathcal{O})$$

où l'on utilise $\mathrm{vol}(\mathcal{O}x) = |\mathrm{Nm}(x)|\mathrm{vol}(\mathcal{O})$ et de même pour y. Puisque $y \in \mathcal{O}x$, on a $yx^{-1} \in \mathcal{O}$ et donc $yx^{-1}\mathcal{O}$ est un idéal à droite de $\mathcal{O}$ de norme majorée par $\mathrm{vol}(\mathcal{O})$. Par hypothèse, il existe donc $b \in \mathcal{O}$ avec $yx^{-1}\mathcal{O} = b\mathcal{O}$ et $|b| \leq \xi$. Maintenant l'égalité des idéaux se traduit par l'existence de $u \in \mathcal{O}^\times$ tel que $yx^{-1} = bu$. En écrivant ceci $b^{-1}y = ux$, nous avons

$$|x| \leq |ux| = |b^{-1}y| \leq |b^{-1}|\,|y| \leq \frac{|b|^{n-1}}{|\mathrm{Nm}(b)|}|y| \leq \xi^{n-1}|y|$$

où la première inégalité vient de $x \in F$ tandis que les autres découlent du lemme 2.2 (et $b \in \mathcal{O} \setminus \{0\}$ donne $|\mathrm{Nm}(b)| \geq 1$). Enfin, avec $|y| = \mu_1 \leq \sqrt{n}\,\mathrm{vol}(\mathcal{O}x)^{1/n} = \sqrt{n}\,|\mathrm{Nm}(x)|^{1/n}\mathrm{vol}(\mathcal{O})^{1/n}$ et $|\mathrm{Nm}(x)| \leq 1$ (car $x \in F^{\leq 1}$), nous trouvons $|x| \leq \sqrt{n}\,\xi^{n-1}\,\mathrm{vol}(\mathcal{O})^{1/n}$ comme prévu. Ceci montre bien que $F^{\leq 1}$ est borné car il est évident qu'il existe un réel ξ comme dans l'énoncé (puisque l'ensemble des idéaux de norme bornée est fini). La minoration de ρ par $|1| = \sqrt{n}$ découle simplement de $1 \in F$. □

L'étape suivante consiste à montrer qu'un nombre fini de conditions de la forme $|x| \leq |ux|$ permettent de définir F. Si nous imposons une borne sur $|x|$, c'est immédiat.

LEMME 6.3. *Pour tout réel $r \geq \rho$ on a*

$$F = \{x \in (D \otimes \mathbb{R})^\times \mid |x| \leq r|\mathrm{Nm}(x)|^{1/n} \text{ et } \forall u \in \mathcal{O}^\times \ |u| \leq r^n \Rightarrow |x| \leq |ux|\}.$$

DÉMONSTRATION. Appelons F' l'ensemble à droite de l'égalité. Par définition de ρ on a clairement $F \subset F'$. Montrons l'inclusion inverse en choisissant $x \in F'$. Il nous suffit de voir que si $u \in \mathcal{O}^\times$ vérifie $|u| \geq r^n$ alors $|x| \leq |ux|$. Or l'on a

$$|u|\,|x| = |uxx^{-1}|\,|x| \leq |ux|\,|x^{-1}|\,|x| \leq |ux|\,\frac{|x|^n}{|\mathrm{Nm}(x)|} \leq |ux|r^n \leq |ux|\,|u|$$

à l'aide du lemme 2.2. □

Nous pouvons maintenant nous affranchir de la condition $|x| \leq r|\mathrm{Nm}(x)|^{1/n}$. Pour la suite, nous notons $\mathcal{U} = \{u \in \mathcal{O}^\times \mid |u| \leq \rho^n\}$.

PROPOSITION 6.1. *L'ensemble $\mathcal{U}$ est de cardinal au plus $(2\rho^n/\sqrt{n}+1)^n$ et on a*

$$F = \{x \in (D \otimes \mathbb{R})^\times \mid \forall u \in \mathcal{U} \ |x| \leq |ux|\}.$$

DÉMONSTRATION. Le premier minimum du réseau $\mathcal{O}$ est $\sqrt{n}$ donc les boules ouvertes de rayon $\sqrt{n}/2$ centrées en les points de $\mathcal{U}$ sont toutes disjointes et contenues dans la boule de centre 0 et de rayon $\rho^n + \sqrt{n}/2$. En comparant les volumes il vient

$$(\mathrm{Card}\,\mathcal{U})(\sqrt{n}/2)^n \leq (\rho^n + \sqrt{n}/2)^n$$

qui donne bien $\mathrm{Card}(\mathcal{U}) \leq (2\rho^n/\sqrt{n}+1)^n$. Pour le reste de cette démonstration, nous considérons

$$\mathcal{Z} = \{z \in D \otimes \mathbb{R} \mid \exists x \in (D \otimes \mathbb{R})^\times \ z = xx^\star \text{ et } \forall u \in \mathcal{U} \ |x| \leq |ux|\}.$$

Cet ensemble est convexe : en effet, d'une part les conditions $|x| \leq |ux|$ s'écrivent $\mathrm{Tr}(z) \leq \mathrm{Tr}(uzu^\star)$ donc sont linéaires en z et définissent des demi-espaces dont l'intersection est convexe ; d'autre part l'ensemble des éléments de la forme $xx^\star$ avec $x \in (D \otimes \mathbb{R})^\times$ est le cône convexe $(D \otimes \mathbb{R})^{>0}_{\mathrm{sym}}$ des éléments définis positifs de $D \otimes \mathbb{R}$ d'après le corollaire 2.1. Notons aussi $1 \in \mathcal{Z}$.

Puisque $\mathcal{Z}$ est convexe, l'image $f(\mathcal{Z})$ d'une fonction continue $f\colon \mathcal{Z} \to \mathbb{R}$ est un intervalle. Nous appliquons ceci à la fonction donnée par $f(z) = \mathrm{Tr}(z)\mathrm{Nm}(z)^{-1/n}$ (noter que si $z \in \mathcal{Z}$ alors $\mathrm{Nm}(z) > 0$). Montrons par l'absurde que son image $f(\mathcal{Z})$ est contenue dans $[0, \rho^2]$. Pour faire ceci, nous utilisons le lemme 6.3. Comme $\mathcal{O}$ est discret, il existe $r > \rho$ avec

$$\mathcal{U} = \{u \in \mathcal{O}^\times \mid |u| \leq \rho^n\} = \{u \in \mathcal{O}^\times \mid |u| \leq r^n\}.$$

Si $f(\mathcal{Z}) \not\subset [0, \rho^2]$, il existe $z \in \mathcal{Z}$ avec $f(1) = n \leq \rho^2 < f(z) \leq r^2$. Écrivons $z = xx^\star$ alors $f(z) = |x|^2|\mathrm{Nm}(x)|^{-2/n} \leq r^2$ donc $|x| \leq r|\mathrm{Nm}(x)|^{1/n}$. Cette condition jointe au fait que $|u| \leq r^n \Rightarrow u \in \mathcal{U} \Rightarrow |x| \leq |ux|$ entraîne au vu du lemme 6.3 que l'on a $x \in F$. Mais ceci force $|x|\,|\mathrm{Nm}(x)|^{-1/n} \leq \rho$ par définition de ρ donc $f(z) \leq \rho^2$, ce qui est la contradiction cherchée.

Pour conclure, soit $x \in (D \otimes \mathbb{R})^\times$ avec $|x| \leq |ux|$ pour tout $u \in \mathcal{U}$. Comme $z = xx^* \in \mathcal{Z}$ on a $f(z) \leq \rho^2$ ce qui s'écrit à nouveau $|x| \leq \rho|\mathrm{Nm}(x)|^{1/n}$. En appliquant maintenant le lemme 6.3 avec $r = \rho$, nous trouvons bien $x \in F$. □

Nous savons maintenant que $F^{\leq 1}$ est défini par un nombre fini de conditions mais il ne constitue pas encore un domaine fondamental pour l'action de $\mathcal{O}^\times$: en effet, nous avons considéré tous les points de norme minimale dans leur orbite mais il peut très bien y avoir plusieurs tels points dans une orbite. Pour éliminer ce problème, la prise en compte du sous-groupe fini

$$G = \{u \in \mathcal{O} \mid uu^\star = 1\}$$

de $\mathcal{O}^\times$ s'impose car si $u \in G$ on a toujours $|ux| = |x|$ ($|ux|^2 = \mathrm{Tr}(uxx^\star u^\star) = \mathrm{Tr}(u^\star uxx^\star) = |x|^2$). En particulier F et $F^{\leq 1}$ sont stables par multiplication à gauche par G et il nous faut encore prendre des représentants pour cette action. Suivant le même principe que précédemment, pour distinguer les points d'une orbite sous l'action de G, nous pouvons choisir celui qui est le plus proche d'un élément non nul fixé (arbitraire). Même si cela ne définit pas exactement un domaine fondamental, c'est suffisant pour nos besoins.

Nous mettons en œuvre ce qui précède mais, pour aboutir au résultat précis utilisé dans la partie suivante, nous envisageons désormais l'action de $\mathcal{O}^\times$ sur $\Theta = \{v \in (D \otimes \mathbb{R})^N \mid 0 < \mathrm{Nm}(vv^\star) \leq 1\}$ et non plus seulement sur $(D \otimes \mathbb{R})^\times$ (qui correspond à $N = 1$).

Ceci nous amène à fixer un vecteur non nul $v_0 \in (D \otimes \mathbb{R})^N$ puis à définir $F_N^+ \subset (D \otimes \mathbb{R})^N$ comme la partie formée du vecteur nul 0 et des vecteurs v

qui vérifient

1. $0 < \mathrm{Nm}(vv^\star) \leq 1$,
2. $|v| \leq |uv|$ pour tout $u \in \mathcal{U}$ et
3. $|v - v_0| \leq |uv - v_0|$ pour tout $u \in G$.

De la même façon nous introduisons $F_N^- \subset (D \otimes \mathbb{R})^N$ l'ensemble des vecteurs v qui vérifient

1. $0 < \mathrm{Nm}(vv^\star) < 1$,
2. $|v| < |uv|$ pour tout $u \in \mathcal{U} \setminus G$ et
3. $|v - v_0| < |uv - v_0|$ pour tout $u \in G \setminus \{1\}$.

Il nous faut étendre le résultat de la proposition 6.1 à ce cadre vectoriel.

LEMME 6.4. *On ne change pas les définitions de F_N^+ et F_N^- en y remplaçant $\mathcal{U}$ par $\mathcal{O}^\times$. En outre*

$$\rho = \sup_{v \in F_N^+} |v| = \sup_{v \in F_N^+} \frac{|v|}{\mathrm{Nm}(vv^\star)^{1/2n}}.$$

DÉMONSTRATION. La condition $\mathrm{Nm}(vv^\star) > 0$ montre que $vv^\star$ est défini positif donc qu'il existe $x \in (D \otimes \mathbb{R})^\times$ avec $vv^\star = xx^\star$. Pour un tel x la proposition 6.1 montre

$$\forall u \in \mathcal{O}^\times \ |x| \leq |ux| \Longleftrightarrow \forall u \in \mathcal{U} \ |x| \leq |ux|.$$

Puisque $|x| = |v|$ et $|ux| = |uv|$, ceci montre que la définition de F_N^+ ne change pas si on remplace $\mathcal{U}$ par $\mathcal{O}^\times$. Nous en déduisons également que $v \in F_N^+$ entraîne $x \in F$ donc $|x| \leq \rho |\mathrm{Nm}(x)|^{1/n} \leq \rho$. Par suite, comme dans la démonstration du lemme 6.3, si $|u| > \rho^n$ alors $|x| < |ux|$ et ceci montre que dans la définition de F_N^- les $u \notin \mathcal{U}$ sont inutiles. L'égalité

$$\sup_{v \in F_N^+} |v| = \sup_{v \in F_N^+} \frac{|v|}{\mathrm{Nm}(vv^\star)^{1/2n}}$$

vient de ce que si v est dans F_N^+ alors tout tv, $t \geq 0$ réel, vérifie les deux dernières conditions de la définition de F_N^+ (c'est clair pour la seconde ; pour la troisième il suffit de constater que $|v - v_0| \leq |uv - v_0|$ se réécrit $\mathrm{Tr}((u-1)vv_0^\star + v_0 v^\star(u^\star - 1)) \leq 0$ en tirant parti de $u \in G$) ; en choisissant $t = \mathrm{Nm}(vv^\star)^{-1/2n}$ on voit que $tv \in F_N^+$. Finalement $\sup_{v \in F_N^+} |v| \leq \rho$ a été vue et pour montrer l'égalité il suffit de vérifier que l'on peut associer à tout $x \in F^{\leq 1}$ un élément v de F_N^+ de même norme. Or $v = (x, 0, \ldots, 0)$ satisfait les

deux premières conditions et s'il ne satisfait pas la troisième c'est le cas d'un des uv avec $u \in G$ qui a la même norme. □

Nous pouvons conclure cette partie par le résultat suivant.

PROPOSITION 6.2. *Il existe un domaine fondamental S pour l'action de $\mathcal{O}^\times$ sur Θ dont l'adhérence est F_N^+ et l'intérieur F_N^-.*

DÉMONSTRATION. Nous allons vérifier successivement que F_N^- est ouvert, que F_N^+ est fermé, que F_N^- est l'intérieur de F_N^+ et finalement que l'on peut choisir S avec $F_N^- \subset S \subset F_N^+$. Ces quatre assertions réunies sont équivalentes à l'énoncé.

L'ensemble F_N^- est ouvert car il est défini par des conditions ouvertes. L'ensemble F_N^+ est défini par un nombre fini de conditions toutes fermées sauf $\mathrm{Nm}(vv^\star) > 0$. Il se pourrait donc que F_N^+ ait des points adhérents avec $\mathrm{Nm}(vv^\star) = 0$. Toutefois l'inégalité $|v| \leq \rho \mathrm{Nm}(vv^\star)^{1/2n}$ valable pour $v \in F_N^+$ montre qu'une suite qui tend vers un tel point tend nécéssairement vers $0 \in F_N^+$. Ainsi F_N^+ est fermé.

Soit maintenant v un point intérieur de F_N^+. Si $\mathrm{Nm}(vv^\star) = 1$ alors dans tout voisinage de v il existe un point de la forme tv avec $\mathrm{Nm}(tv(tv)^\star) > 1$, ce qui est absurde. Ainsi $\mathrm{Nm}(vv^\star) < 1$. De la même façon, on a $|v - v_0| < |uv - v_0|$ pour tout $u \in G \setminus \{1\}$ car si la forme linéaire $v_1 \mapsto |v_1 - v_0|^2 - |uv_1 - v_0|^2$ s'annule en un point elle change de signe sur tout voisinage de ce point (elle n'est pas identiquement nulle car $u \neq 1$ donne $uv_0 \neq v_0$ donc la forme linéaire ne s'annule pas en v_0). En particulier, avec $u = -1 \in G$, on voit $v \neq 0$ donc $\mathrm{Nm}(vv^\star) > 0$. Supposons enfin que $|v| = |uv|$ pour un $u \in \mathcal{U} \setminus G$. Cela signifie que la forme quadratique $v_1 \mapsto |uv_1|^2 - |v_1|^2$ s'annule en $v_1 = v$ tout en restant positive dans un voisinage. Ceci n'est possible que si la forme quadratique est positive sur $(D \otimes \mathbb{R})^N$ tout entier. Or cela signifie $|v_1| \leq |uv_1|$ pour tout v_1 ; en choisissant $v_1 = (u^{-1}, 0, \ldots, 0)$, il vient $|u^{-1}| \leq \sqrt{n}$. Comme $1 = |\mathrm{Nm}(u^{-1})|^{1/n} \leq |u^{-1}|/\sqrt{n}$ par le lemme 2.2, il y a égalité, ce qui montre que $uu^\star$ est réel. Enfin $\mathrm{Nm}(uu^\star) = 1$ force $uu^\star = 1$ donc $u \in G$, contrairement à notre hypothèse. Ceci finit de prouver $v \in F_N^-$.

Construisons S de la manière suivante : dans chaque orbite de Θ sous l'action de $\mathcal{O}^\times$ nous considérons les éléments v de norme $|v|$ minimale et, parmi ceux-ci, ceux qui minimisent la quantité $|v - v_0|$. Dans chaque orbite, nous choisissons un tel élément. Ceci forme S. Si v appartient à S, tous les uv avec $u \in G$ ont même norme que v donc doivent être plus loin de v que v_0 c'est-à-dire $|v - v_0| \leq |uv - v_0|$. Ceci montre $S \subset F_N^+$. Si maintenant

$v \in F_N^-$ alors les seuls éléments de norme minimale de l'orbite de v sont les uv avec $u \in G$ et v est plus près de v_0 que tous ceux-ci donc $v \in S$. Ceci termine la démonstration. □

7. Intersection avec un réseau

Le but de cette partie est d'établir (†) dans le cas $M = 1$ c'est-à-dire d'estimer le nombre de points de S dans un réseau (explicitement $H^{-1}N(\mathcal{D})^{-1/n}\mathcal{A}^N$). Nous nous appuyons donc sur un résultat de la forme

$$\left|\mathrm{Card}(S \cap \Lambda) - \frac{\mathrm{vol}(S)}{\mathrm{vol}(\Lambda)}\right| \leq \text{ erreur}$$

où S est une partie bornée mesurable et Λ un réseau de $\mathbb{R}^m$. Il faut imposer des conditions de régularité sur S pour obtenir un terme d'erreur explicite. Ce type de majorations abonde dans la littérature : on pourra consulter l'article de 1951 de Davenport [Da] qui en attribue le principe à Lipschitz (cette approche est développée dans [T2, partie 5], voir aussi [W]) ou le livre de Lang [La] où apparaissent des fonctions lipschitziennes. Nous suivons cette deuxième méthode qui est aussi celle employée par exemple par Schanuel [Scha] ou Schmidt [Schm]. De manière précise, nous nous basons sur un résultat de Masser et Vaaler [MV, lemme 2, page 437] dont une version explicite est donnée par Widmer [W]. Nous en redonnons une démonstration pour faire le lien avec les notions introduites par [Schm] que nous utiliserons dans la suite.

Nous faisons usage de la terminologie suivante.

DÉFINITION 7.1. *Soient $L \geq 0$ un réel et $P \geq 1$, $m \geq 0$ des entiers.*

(1) *Une application $\psi\colon \mathfrak{A} \to \mathfrak{B}$ entre parties d'espaces normés est dite L-lipschitzienne si pour tous $a, a' \in \mathfrak{A}$*

$$|\psi(a) - \psi(a')| \leq L|a - a'|.$$

(2) *Une application $\psi\colon \mathfrak{A} \to \mathfrak{B}$ entre parties d'espaces normés est dite L-spéciale si pour tous $a, a' \in \mathfrak{A}$*

$$|a - a'| \leq |\psi(a) - \psi(a')| \leq L|a - a'|.$$

(3) *On désigne par $\mathrm{Lip}_m(1, L)$ l'ensemble des parties $\mathfrak{B}$ de $\mathbb{R}^m$ pour lesquelles il existe une partie $\mathfrak{A}$ de $[0,1]^{m-1}$ et une application L-lipschitzienne $\psi\colon \mathfrak{A} \to \mathbb{R}^m$ avec $\mathfrak{B} \subset \psi(\mathfrak{A})$.*

(4) *Une partie* $\mathfrak{B}$ *de* $\mathbb{R}^m$ *est dite* L*-spéciale s'il existe une partie* $\mathfrak{A}$ *de* $\mathbb{R}^{m-1}$ *et une application* L*-spéciale* $\psi\colon \mathfrak{A} \to \mathbb{R}^m$ *avec* $\mathfrak{B} \subset \psi(\mathfrak{A})$.

(5) *On note* $\mathrm{Lip}_m(P, L)$ *l'ensemble des parties de* $\mathbb{R}^m$ *qui sont l'union de* P *parties appartenant à* $\mathrm{Lip}_m(1, L)$.

(6) *Une partie de* $\mathbb{R}^m$ *est dite* (P, L)*-spéciale si elle est l'union de* P *parties* L*-spéciales.*

(7) *Si* $\mathfrak{B}$ *est une partie de* $\mathbb{R}^m$ *et* $\delta > 0$ *un réel, on appelle* δ*-filet pour* $\mathfrak{B}$ *un ensemble* $\mathfrak{F} \subset \mathbb{R}^m$ *avec la propriété suivante : pour tout* $x \in \mathfrak{B}$ *il existe* $y \in \mathfrak{F}$ *tel que* $|x - y| < \delta$.

Les définitions (2), (4), (6) et (7) viennent de [Schm] (voir (2.4) page 41 et page 59). La notation $\mathrm{Lip}_m(P, L)$ est voisine de celle adoptée dans [W]. La plupart des auteurs imposent $\mathfrak{A} = [0, 1]^{m-1}$ dans (3) : nous nous autorisons un peu plus de souplesse mais la différence est inessentielle comme le montre le lemme 16 page 62 de [Schm]. Le lemme suivant relie les notions (5), (6) et (7).

LEMME 7.1. *Soient* $L \geq 0$ *un réel,* $P, m \geq 1$ *des entiers et* $\mathfrak{B}$ *une partie de* $\mathbb{R}^m$.

(1) *Si* $\mathfrak{B}$ *est* (P, L)*-spéciale et de diamètre fini* ρ *alors* $\mathfrak{B} \in \mathrm{Lip}_m(P, L\rho)$.

(2) *Si* $\mathfrak{B} \in \mathrm{Lip}_m(P, L)$ *alors, pour tout réel* $\delta > 0$*, il existe un* δ*-filet* $\mathfrak{F}$ *pour* $\mathfrak{B}$ *avec*

$$\mathrm{Card}\,\mathfrak{F} \leq P\left(\frac{L\sqrt{m}}{\delta} + 1\right)^{m-1}.$$

DÉMONSTRATION. Visiblement, nous pouvons supposer $P = 1$ dans les deux cas.

(1) Si $\mathfrak{B}$ est L-spéciale, il existe $\mathfrak{A} \subset \mathbb{R}^{m-1}$ et $\psi\colon \mathfrak{A} \to \mathbb{R}^m$ une application L-spéciale avec $\mathfrak{B} \subset \psi(\mathfrak{A})$. Si $a, a' \in \mathfrak{A} \cap \psi^{-1}(\mathfrak{B})$ nous avons $|a - a'| \leq |\psi(a) - \psi(a')| \leq \rho$. Quitte à faire une translation, nous pouvons supposer que $\mathfrak{A}' = \mathfrak{A} \cap \psi^{-1}(\mathfrak{B})$ est inclus dans le cube $[0, \rho]^{m-1}$. Nous définissons alors $\psi'\colon \rho^{-1}\mathfrak{A}' \to \mathbb{R}^m$ par $\psi'(a) = \psi(\rho a)$. Il est clair que $\mathfrak{B} \subset \psi'(\rho^{-1}\mathfrak{A}')$ et si $a, a' \in \rho^{-1}\mathfrak{A}'$ alors

$$|\psi'(a) - \psi'(a')| = |\psi(\rho a) - \psi(\rho a')| \leq L|\rho a - \rho a'| = L\rho|a - a'|.$$

(2) Si $\mathfrak{B} \in \mathrm{Lip}_m(1, L)$, il existe $\mathfrak{A} \subset [0, 1]^{m-1}$ et $\psi\colon \mathfrak{A} \to \mathbb{R}^m$ une application L-lipschitzienne avec $\mathfrak{B} \subset \psi(\mathfrak{A})$. Posons $Q = [L\sqrt{m}/\delta] + 1 \in \mathbb{N} \setminus \{0\}$. Nous découpons $[0, 1]$ en Q intervalles de longueur $1/Q$ et donc $[0, 1]^{m-1}$ en Q^{m-1} petits cubes de côté $1/Q$. Nous construisons $\mathfrak{F}$ ainsi : pour chaque tel

cube $\mathfrak{C}$, si $\mathfrak{A} \cap \mathfrak{C}$ est non vide, nous choisissons $a_{\mathfrak{C}} \in \mathfrak{A} \cap \mathfrak{C}$ et $\mathfrak{F}$ est l'ensemble des $\psi(a_{\mathfrak{C}})$. Nous avons bien $\operatorname{Card} \mathfrak{F} \leq Q^{m-1}$ et, si $x \in \mathfrak{B}$, il existe $a \in \mathfrak{A}$ avec $\psi(a) = b$. Le point a est dans l'un des cubes $\mathfrak{C}$ donc $|a - a_{\mathfrak{C}}| \leq \sqrt{m-1}/Q < \sqrt{m}/Q \leq \delta/L$ puis $|\psi(a) - \psi(a_{\mathfrak{C}})| \leq L|a - a_{\mathfrak{C}}| < \delta$, ce qui est le résultat puisque $\psi(a_{\mathfrak{C}}) \in \mathfrak{F}$. □

Voici à présent le résultat qui est au cœur du principe de décompte : nous reproduisons un argument de D. Masser (voir proposition 5.2 de [W] sans filet).

PROPOSITION 7.1 (Masser). *Soient $m \geq 1$ un entier, $\delta > 0$ un réel, $\mathfrak{B}$ une partie de $\mathbb{R}^m$ et $\mathfrak{F}$ un δ-filet pour $\mathfrak{B}$. Pour tout réseau $\Lambda \subset \mathbb{R}^m$ de minima successifs $\lambda_1, \ldots, \lambda_m$ il existe un domaine fondamental F pour $\mathbb{R}^m/\Lambda$ tel que*

$$\operatorname{Card}\{v \in \Lambda \mid \mathfrak{B} \cap (F + v) \neq \emptyset\} \leq \operatorname{Card} \mathfrak{F} \prod_{i=1}^{m} \left(\frac{2m^{2m-2}\delta}{\lambda_i} + 2 \right).$$

DÉMONSTRATION. Un lemme de Mahler et Weyl (voir [Ca] lemme 8 page 135) montre qu'il est possible de trouver une base $e_1, \ldots, e_m$ de Λ avec $\lambda_i \leq |e_i| \leq \max(1, i/2)\lambda_i$ pour $1 \leq i \leq m$. Posons $F = \{z_1 e_1 + \cdots + z_m e_m \mid 0 \leq z_i < 1 \text{ pour } 1 \leq i \leq m\}$.

Pour clarifier, commençons par traiter le cas où $\mathfrak{F} = \{x_0\}$ et $\mathfrak{B}$ est la boule ouverte de centre x_0 et de rayon δ. Soient $v, v' \in \Lambda$ tels que $\mathfrak{B} \cap (F + v) \neq \emptyset$ et $\mathfrak{B} \cap (F + v') \neq \emptyset$. Nous écrivons $v = a_1 e_1 + \cdots + a_m e_m$. Il existe $x \in \mathfrak{B} \cap (F + v)$ donc $x = (a_1 + z_1)e_1 + \cdots + (a_m + z_m)e_m$ avec $0 \leq z_i < 1$. De même il existe $x' \in \mathfrak{B} \cap (F + v')$ que nous écrivons $x' = (a'_1 + z'_1)e_1 + \cdots + (a'_m + z'_m)e_m$. Puisque $\mathfrak{B}$ est de diamètre 2δ on a $|x - x'| < 2\delta$. En posant $\rho_i = a_i + z_i - a'_i - z'_i$ on a $\rho_1 e_1 + \cdots + \rho_m e_m = x - x'$ et, en utilisant l'inégalité d'Hadamard, il vient

$$|\rho_i| = \left| \frac{\det(e_1, \ldots, x - x', \ldots, e_m)}{\det(e_1, \ldots, e_m)} \right| \leq \frac{|e_1| \cdots |x - x'| \cdots |e_m|}{\operatorname{vol}(\Lambda)} \leq \frac{|e_1| \cdots |e_m|}{\operatorname{vol}(\Lambda)} \frac{2\delta}{|e_i|}.$$

D'après le choix des e_i et le théorème de Minkowski (avec la même majoration que dans le lemme 6.1)

$$|\rho_i| \leq \frac{m!}{2^{m-2}} \frac{\lambda_1 \cdots \lambda_m}{\operatorname{vol}(\Lambda)} \frac{\delta}{\lambda_i} \leq 2m! m^{m/2} \frac{\delta}{\lambda_i} \leq 2m^{2m-2} \frac{\delta}{\lambda_i}.$$

Par suite, $|a_i - a'_i| = |\rho_i + z'_i - z_i| < 2m^{2m-2}\delta/\lambda_i + 1$ car $-1 < z'_i - z_i < 1$.

Ceci montre que lorsque $v = a_1e_1 + \cdots + a_me_m$ varie dans $\{v \in \Lambda \mid \mathfrak{B} \cap (F+v) \neq \emptyset\}$, la coordonnée a_i est contenue dans un intervalle de longueur $< 2m^{2m-2}\delta/\lambda_i + 1$. Comme elle est entière, elle prend au plus $2m^{2m-2}\delta/\lambda_i + 2$ valeurs. En multipliant, on a le résultat.

Dans le cas général, $\mathfrak{B}$ est contenue dans l'union de $\operatorname{Card}\mathfrak{F}$ boules ouvertes de rayon δ. □

Cette estimation permet de donner la version effective suivante du lemme 2 page 437 de [MV], due à M. Widmer [W].

LEMME 7.2 (Widmer). *Soient $m \geq 1$ un entier, Λ un réseau de $\mathbb{R}^m$ de premier minimum λ_1 et S une partie bornée de $\mathbb{R}^m$ telle que $\partial S \in \operatorname{Lip}_m(P, L)$. Alors S est mesurable et*

$$\left|\operatorname{Card}(S \cap \Lambda) - \frac{\operatorname{vol}(S)}{\operatorname{vol}(\Lambda)}\right| \leq 3^m P\left(\frac{m^{2m}L}{\lambda_1} + 1\right)^{m-1}.$$

DÉMONSTRATION. Pour la mesurabilité, nous renvoyons à [Le, page 294]. Nous posons $\delta = \lambda_1/2m^{2m-2}$. En combinant l'assertion (2) du lemme 7.1 et la proposition 7.1, nous voyons qu'il existe un domaine fondamental F pour $\mathbb{R}^m/\Lambda$ tel que

$$\operatorname{Card}\{v \in \Lambda \mid \partial S \cap (F+v) \neq \emptyset\} \leq P\left(\frac{2\sqrt{m}\, m^{2m-2}L}{\lambda_1} + 1\right)^{m-1} \prod_{i=1}^{m}\left(\frac{\lambda_1}{\lambda_i} + 2\right)$$

où $\lambda_1 \leq \cdots \leq \lambda_m$ sont les minima de Λ. Le membre de droite de l'inégalité précédente n'excède pas $3^m P(2m^{2m-1}L/\lambda_1 + 1)^{m-1} \leq 3^m P(m^{2m}L/\lambda_1 + 1)^{m-1}$. Il reste donc à voir

$$\left|\operatorname{Card}(S \cap \Lambda) - \frac{\operatorname{vol}(S)}{\operatorname{vol}(\Lambda)}\right| \leq \operatorname{Card}\{v \in \Lambda \mid \partial S \cap (F+v) \neq \emptyset\}.$$

Ceci est vrai très généralement pour tous Λ, S (borné, mesurable) et tout domaine fondamental connexe F de Λ. On obtient la majoration en comparant le volume de l'union des translatés de F contenus dans S et le volume de l'union des translatés rencontrant S (voir par exemple [La] page 112). □

Pour l'application que nous avons en vue, la borne précédente présente l'inconvénient (mineur) que le terme d'erreur ne peut pas tendre vers 0 même si λ_1 est grand. Nous pallions ce défaut en imposant une condition supplémentaire.

COROLLAIRE 7.1. *Soient $m \geq 1$ un entier, Λ un réseau de $\mathbb{R}^m$ de premier minimum λ_1 et S une partie bornée de $\mathbb{R}^m$ telle que $\partial S \in \mathrm{Lip}_m(P, L)$. Si l'on suppose de plus que $0 \notin S$, que S est contenu dans la boule de centre 0 et de rayon L et que $c \geq 1$ est un réel tel que $\lambda_1 \mathrm{vol}(\Lambda)^{-1/m}$ appartient à l'intervalle $[c^{-1}, c]$ alors*

$$\left| \mathrm{Card}(S \cap \Lambda) - \frac{\mathrm{vol}(S)}{\mathrm{vol}(\Lambda)} \right| \leq P m^{2m^2} \frac{(cL)^{m-1}}{\mathrm{vol}(\Lambda)^{1-1/m}}.$$

DÉMONSTRATION. Si $m = 1$ la majoration est immédiatement vraie (S est l'union d'au plus $P - 1$ intervalles). On suppose donc $m \geq 2$ et l'on distingue deux cas.

Si $\lambda_1 > L$, le seul point de Λ dans la boule de centre 0 et de rayon L est 0 donc $S \cap \Lambda = \emptyset$. Le membre de gauche de l'inégalité à démontrer est donc $\mathrm{vol}(S)/\mathrm{vol}(\Lambda)$. Nous estimons $\mathrm{vol}(S) \leq (2L)^m \leq 2^m L^{m-1} \lambda_1 \leq 2^m L^{m-1} c\, \mathrm{vol}(\Lambda)^{1/m}$ et cela donne bien

$$\frac{\mathrm{vol}(S)}{\mathrm{vol}(\Lambda)} \leq 2^m \frac{(cL)^{m-1}}{\mathrm{vol}(\Lambda)^{1-1/m}} \leq P m^{2m^2} \frac{(cL)^{m-1}}{\mathrm{vol}(\Lambda)^{1-1/m}}.$$

Si $\lambda_1 \leq L$, nous appliquons le lemme précédent et écrivons

$$3^m P \left(\frac{m^{2m} L}{\lambda_1} + 1 \right)^{m-1} \leq 3^m P (m^{2m} + 1)^{m-1} \left(\frac{L}{\lambda_1} \right)^{m-1}.$$

Il reste à constater $L/\lambda_1 \leq cL/\mathrm{vol}(\Lambda)^{1/m}$ et $3^m (m^{2m} + 1)^{m-1} \leq m^{2m^2}$ pour conclure. □

On peut noter que la condition sur S n'est pas extrêmement restrictive : par exemple si S est connexe alors $\partial S \in \mathrm{Lip}_m(P, L)$ entraîne que S est de diamètre au plus $PL\sqrt{m-1}$.

Munis de ce résultat de décompte, nous souhaitons l'appliquer à l'ensemble S défini dans la partie précédente. Puisque $S \subset (D \otimes \mathbb{R})^N \simeq \mathbb{R}^{Nn}$ nous utilisons $m = Nn$.

PROPOSITION 7.2. *Si l'ensemble S vérifie les conditions de la proposition 6.2 alors*

$$\partial S \in \mathrm{Lip}_{Nn}(3^{n+1} Nn \rho^{n^2}, 6(Nn)^{4n} \rho^{2n+1}).$$

DÉMONSTRATION. D'après la proposition 6.2, le bord ∂S de S est inclus dans l'union de l'ensemble $\mathfrak{B}_1 = \{v \in (D \otimes \mathbb{R})^N \mid |v| \leq \rho \text{ et } \mathrm{Nm}(vv^\star) = 1\}$ et d'ensembles $\mathfrak{B}_u$ pour $u \in \mathcal{U} \setminus \{1\}$ avec $\mathfrak{B}_u = \{v \in (D \otimes \mathbb{R})^N \mid |v| \leq \rho$ et

$|v| = |uv|\}$ si $u \notin G$ et $\mathfrak{B}_u = \{v \in (D \otimes \mathbb{R})^N \mid |v| \leq \rho$ et $|v - v_0| = |uv - v_0|\}$ pour $u \in G \setminus \{1\}$. Chaque $\mathfrak{B}_u$ est défini par une condition quadratique ou linéaire donc d'après le lemme 8 page 50 de [Schm] est $(2Nn, 3Nn)$-spécial ; par le lemme 7.1 on a $\mathfrak{B}_u \in \mathrm{Lip}_{Nn}(2Nn, 3Nn\rho)$ puis $\bigcup_{u \in \mathcal{U}\setminus\{1\}} \mathfrak{B}_u \in \mathrm{Lip}_{Nn}(2Nn(\mathrm{Card}\,\mathcal{U} - 1), 3Nn\rho)$.

Il reste à paramétrer $\mathfrak{B}_1$. Nous le faisons en le projetant sur un cube. Nous fixons une base orthonormée de $D \otimes \mathbb{R}$ dont on déduit une base orthonormée $e_1, \ldots, e_{Nn}$ de $(D \otimes \mathbb{R})^N$. Commençons par remarquer que l'application

$$\begin{aligned} (D \otimes \mathbb{R})^N &\longrightarrow \mathbb{R} \\ w &\longmapsto \mathrm{Nm}(ww^\star) \end{aligned}$$

est un polynôme homogène de degré $2n$ dont la longueur, c'est-à-dire la somme des valeurs absolues des coefficients, est majorée par $n!(Nn)^{3n}$. En effet, grâce à la base choisie, nous pouvons écrire cette application comme la composée de l'application linéaire $\tau\colon (D \otimes \mathbb{R})^N \hookrightarrow \mathrm{Mat}_{nn}(\mathbb{R})^N$ et de l'application

$$\begin{aligned} f\colon \mathrm{Mat}_{nn}(\mathbb{R})^N &\longrightarrow \mathbb{R} \\ (B_1, \ldots, B_N) &\longmapsto \det(B_1\,{}^tB_1 + \cdots + B_N\,{}^tB_N). \end{aligned}$$

Il est clair que f est donnée par un polynôme homogène de degré $2n$ donc il en va de même de $w \mapsto \mathrm{Nm}(ww^\star)$. Pour la longueur, si nous considérons la base canonique de $\mathrm{Mat}_{nn}(\mathbb{R})$ alors celle de f est au plus $n!(Nn)^n$ étant donné que chaque coefficient du déterminant est la somme de Nn termes. Par ailleurs, l'image d'un élément de la base de $D \otimes \mathbb{R}$ dans $\mathrm{Mat}_{nn}(\mathbb{R})$ est une matrice C telle que $\mathrm{Tr}(C\,{}^tC) = 1$ (puisqu'un tel élément e de $D \otimes \mathbb{R}$ vérifie $|e| = 1$) donc chaque coefficient de C est de valeur absolue ≤ 1. Ceci entraîne que la matrice de τ a elle aussi des coefficients de valeur absolue ≤ 1. Par conséquent dans l'écriture $\mathrm{Nm}(ww^\star) = f(\tau(w))$ chaque coordonnée de $\tau(w)$ dans la base canonique de $\mathrm{Mat}_{nn}(\mathbb{R})^N$ est une combinaison linéaire des Nn coordonnées de w donc les coefficients sont de valeur absolue ≤ 1. Si nous développons $f(\tau(w))$ nous obtenons bien une longueur de $n!(Nn)^{3n}$.

Maintenant, si $w, w' \in (D \otimes \mathbb{R})^N$ ont pour coordonnées w_i et w'_i $(1 \leq i \leq Nn)$ et si $i_1, \ldots, i_{2n}$ sont des éléments de $\{1, \ldots, Nn\}$, alors

$$\begin{aligned} \left| \prod_{j=1}^{2n} w_{i_j} - \prod_{j=1}^{2n} w'_{i_j} \right| &= \left| \sum_{k=1}^{2n} \left(\prod_{j=1}^{k-1} w_{i_j} \right) (w_{i_k} - w'_{i_k}) \left(\prod_{j=k+1}^{2n} w'_{i_j} \right) \right| \\ &\leq 2n \cdot \max(|w|, |w'|)^{2n-1} |w - w'|. \end{aligned}$$

Comme $\mathrm{Nm}(ww^\star)$ est une somme de termes $\alpha_i \prod_{j=1}^{2n} w_{i_j}$ pour différents indices $i = (i_1, \ldots, i_{2n}) \in \{1, \ldots, Nn\}^{2n}$ avec $\sum_i |\alpha_i| \leq n!(Nn)^{3n}$ on en déduit pour tous $w, w' \in (D \otimes \mathbb{R})^N$

$$|\mathrm{Nm}(ww^\star) - \mathrm{Nm}(w'w'^\star)| \leq 2n \cdot n!(Nn)^{3n} \max(|w|, |w'|)^{2n-1} |w - w'|.$$

Si de plus les réels $\mathrm{Nm}(ww^\star)$ et $\mathrm{Nm}(w'w'^\star)$ sont non nuls, il vient

$$\begin{aligned}
&|\mathrm{Nm}(ww^\star)^{1/2n} - \mathrm{Nm}(w'w'^\star)^{1/2n}| \\
&\quad = \frac{|\mathrm{Nm}(ww^\star) - \mathrm{Nm}(w'w'^\star)|}{\sum_{i=0}^{2n-1} \mathrm{Nm}(ww^\star)^{i/2n} \mathrm{Nm}(w'w'^\star)^{(2n-1-i)/2n}} \\
&\quad \leq 2n \cdot n!(Nn)^{3n} \max\left(\frac{|w|}{\mathrm{Nm}(ww^\star)^{1/2n}}, \frac{|w'|}{\mathrm{Nm}(w'w'^\star)^{1/2n}}\right)^{2n-1} |w - w'|
\end{aligned}$$

et même

$$\begin{aligned}
&\left| \frac{w}{\mathrm{Nm}(ww^\star)^{1/2n}} - \frac{w'}{\mathrm{Nm}(w'w'^\star)^{1/2n}} \right| \\
&\quad = \left| w\left(\frac{1}{\mathrm{Nm}(ww^\star)^{1/2n}} - \frac{1}{\mathrm{Nm}(w'w'^\star)^{1/2n}}\right) + \frac{w - w'}{\mathrm{Nm}(w'w'^\star)^{1/2n}} \right| \\
&\quad = \left| \frac{-w}{\mathrm{Nm}(ww^\star)^{1/2n}} \cdot \frac{\mathrm{Nm}(ww^\star)^{1/2n} - \mathrm{Nm}(w'w'^\star)^{1/2n}}{\mathrm{Nm}(w'w'^\star)^{1/2n}} + \frac{w - w'}{\mathrm{Nm}(w'w'^\star)^{1/2n}} \right| \\
&\quad \leq \frac{|w - w'|}{\mathrm{Nm}(w'w'^\star)^{1/2n}} \left(1 + 2(Nn)^{4n} \max\left(\frac{|w|}{\mathrm{Nm}(ww^\star)^{1/2n}}, \frac{|w'|}{\mathrm{Nm}(w'w'^\star)^{1/2n}}\right)^{2n}\right).
\end{aligned}$$

Comme pour tout w l'élément $v = w\mathrm{Nm}(ww^\star)^{-1/2n}$ vérifie $\mathrm{Nm}(vv^\star) = 1$, l'application $w \mapsto w\mathrm{Nm}(ww^\star)^{-1/2n}$ va nous donner le paramétrage de $\mathfrak{B}_1$ et l'inégalité ci-dessus permettra d'en montrer le caractère lipschitzien. De manière précise, nous considérons le cube

$$\mathfrak{C} = \{w_1 e_1 + \cdots + w_{Nn} e_{Nn} \mid \max_{1 \leq i \leq Nn} |w_i| \leq 1/2\}$$

et l'une de ses $2Nn$ faces $\mathfrak{F}$ (définie par $w_i = \pm 1/2$), naturellement isométrique à $[0,1]^{Nn-1}$. On pose $\mathfrak{A} = \{w \in \mathfrak{F} \mid |w| \leq \rho \mathrm{Nm}(ww^\star)^{1/2n}\}$. On remarque que si $w \in \mathfrak{F}$ on a $|w| \geq 1/2$ donc, si $w \in \mathfrak{A}$, la quantité $\mathrm{Nm}(ww^\star)^{1/2n} \geq 1/2\rho$ ne s'annule pas. Nous pouvons donc définir

$$\begin{aligned}
\psi \colon \mathfrak{A} &\longrightarrow \mathfrak{B}_1 \\
w &\longmapsto w\mathrm{Nm}(ww^\star)^{-1/2n}.
\end{aligned}$$

D'après le calcul fait plus haut, si $w, w' \in \mathfrak{A}$,

$$\begin{aligned}|\psi(w) - \psi(w')| &\leq 2\rho|w - w'|(1 + 2(Nn)^{4n}\rho^{2n}) \\ &\leq 6(Nn)^{4n}\rho^{2n+1}|w - w'|.\end{aligned}$$

Nous trouvons ainsi $\psi(\mathfrak{A}) \in \mathrm{Lip}_{Nn}(1, 6(Nn)^{4n}\rho^{2n+1})$. Enfin l'union des $2Nn$ ensembles $\psi(\mathfrak{A})$ couvre $\mathfrak{B}_1$ car, si $v \in \mathfrak{B}_1$, la demi-droite $\{tv \mid t > 0\}$ rencontre $\mathfrak{C}$ donc l'une des faces $\mathfrak{F}$; pour $w = tv \in \mathfrak{F}$ la relation $\mathrm{Nm}(vv^\star) = 1$ montre $t = \mathrm{Nm}(ww^\star)^{-1/2n}$ puis $|(1/t)w| = |v| \leq \rho$ donne $w \in \mathfrak{A}$. Finalement $\mathfrak{B}_1 \in \mathrm{Lip}_{Nn}(2Nn, 6(Nn)^{4n}\rho^{2n+1})$ et la proposition en découle avec $\mathrm{Card}\,\mathcal{U} \leq 3^n\rho^{n^2}$. □

Pour appliquer le corollaire 7.1, on pose $\Lambda = H^{-1}N(\mathcal{D})^{-1/n}\mathcal{A}^N$. On a

$$\mathrm{vol}(\Lambda) = H^{-Nn}N(\mathcal{D})^{-N}\mathrm{vol}(\mathcal{A})^N = H^{-Nn}\mathrm{vol}(\mathcal{O})^N[\mathcal{D} : \mathcal{A}]^N.$$

Par ailleurs, si λ_1 est le premier minimum de Λ et μ_1 celui de $\mathcal{A}^N$ on a par homothétie

$$\lambda_1\mathrm{vol}(\Lambda)^{-1/Nn} = \mu_1\mathrm{vol}(\mathcal{A}^N)^{-1/Nn} = \mu_1\mathrm{vol}(\mathcal{A})^{-1/n}.$$

En outre μ_1 est aussi clairement le premier minimum de $\mathcal{A}$ donc le lemme 6.1 donne

$$\sqrt{n}\mathrm{vol}(\mathcal{O})^{-1/n} \leq \mu_1\mathrm{vol}(\mathcal{A})^{-1/n} \leq \sqrt{n}.$$

Ainsi $c = \sqrt{n}\mathrm{vol}(\mathcal{O})^{1/n}$ convient pour appliquer le corollaire 7.1 à Λ. En remarquant

$$\mathrm{Card}(\Lambda \cap S) = \mathrm{Card}(\mathcal{A}^N \cap HN(\mathcal{D})^{1/n}S)$$

on a (†) avec $c_1 = \mathrm{vol}(S)\mathrm{vol}(\mathcal{O})^{-N}$ et $c_2 = P(Nn)^{2N^2n^2}\sqrt{n}^{Nn-1}L^{Nn-1}$ où $P = 3^{n+1}Nn\rho^{n^2}$ et $L = 6(Nn)^{4n}\rho^{2n+1}$ sont donnés par la proposition 7.2. En majorant $c_2 = (Nn\rho)^{6N^2n^2}$ convient également (on utilise $N \geq 2$ et $\rho \geq \sqrt{n} \geq 1$).

8. Calcul de volume

Dans cette partie, nous déterminons le volume de S. Ce calcul nécessite de faire intervenir la décomposition de $D \otimes \mathbb{R}$ en produit d'algèbres de matrices. Aussi commençons-nous par plusieurs résultats préparatoires sur des espaces de matrices $\mathrm{Mat}_{mm}(\mathbb{K})$ ou plus généralement $\mathrm{Mat}_{m\ell}(\mathbb{K})$ où $\mathbb{K}$ est l'un des trois corps $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. Nous écrirons toujours $\kappa = [\mathbb{K} : \mathbb{R}] \in \{1, 2, 4\}$.

Nous utilisons les notations $\mathcal{H}_m(\mathbb{K})$, $\mathcal{H}_m^{\geq 0}(\mathbb{K})$, $\mathcal{H}_m^{>0}(\mathbb{K})$ et $U_m(\mathbb{K})$ introduites dans la partie 2. Nous généralisons la dernière en posant pour $\ell \geq m$

$$U_{m\ell}(\mathbb{K}) = \{K \in \mathrm{Mat}_{m\ell}(\mathbb{K}) \mid KK^\star = I\}.$$

Pour $\ell = m$ nous retrouvons le groupe unitaire $U_m(\mathbb{K}) = U_{mm}(\mathbb{K})$ mais si $\ell > m$ nous n'avons pas de structure de groupe. Cet ensemble $U_{m\ell}(\mathbb{K})$ est contenu dans l'ensemble $G_{m\ell}(\mathbb{K})$ des matrices de rang m que nous pouvons écrire

$$G_{m\ell}(\mathbb{K}) = \{A \in \mathrm{Mat}_{m\ell}(\mathbb{K}) \mid \mathrm{Nm}(AA^\star) > 0\}.$$

Rappelons que Nm désigne la norme de $\mathbb{R}$-algèbre $\mathrm{Mat}_{mm}(\mathbb{K})$. Il s'agit d'une fonction homogène de degré κm^2 et nous pouvons remarquer que si $X \in \mathcal{H}_m(\mathbb{K})$ a pour valeurs propres $a_1, \ldots, a_m$ alors

$$\mathrm{Nm}(X) = \left(\prod_{i=1}^{m} a_i\right)^{\kappa m}.$$

Précisons enfin la norme euclidienne que nous utilisons sur $\mathrm{Mat}_{m\ell}(\mathbb{K})$. Le choix cohérent avec la norme sur $D \otimes \mathbb{R}$ consiste à employer la définition $|A|^2 = \mathrm{Tr}(AA^\star)$ où $\mathrm{Tr}\colon \mathrm{Mat}_{mm}(\mathbb{K}) \to \mathbb{R}$ est la trace de cette algèbre et vérifie en particulier $\mathrm{Tr}(I) = \kappa m^2$. Par ailleurs, la norme usuelle sur $\mathbb{K}$ donnée par $|z|_{\mathrm{us}}^2 = zz^\star$ induit une norme $|\cdot|_{\mathrm{us}}$ peut-être plus naturelle sur $\mathrm{Mat}_{m\ell}(\mathbb{K})$, en identifiant simplement cet espace à $\mathbb{K}^{m\ell}$. On remarque aisément $|A| = \sqrt{\kappa m}|A|_{\mathrm{us}}$, ce qui permet de passer immédiatement de l'une à l'autre. Nous recourrons *in fine* à $|\cdot|$ mais nos résultats préliminaires s'expriment un peu plus facilement avec $|\cdot|_{\mathrm{us}}$.

Lemme 8.1. *L'application $\mathcal{H}_m^{>0}(\mathbb{K}) \to \mathcal{H}_m^{>0}(\mathbb{K})$, $X \mapsto X^2$ est un difféomorphisme dont le jacobien en X est*

$$\prod_{i=1}^{m} 2a_i \cdot \prod_{i<j} (a_i + a_j)^\kappa$$

si $a_1, \ldots, a_m$ sont les valeurs propres de X.

Démonstration. Notons ψ cette application. Elle est bijective d'après le corollaire 2.1. Si $K \in U_m(\mathbb{K})$ nous avons $\psi(X) = K\psi(K^{-1}XK)K^{-1}$. En outre la multiplication à droite ou à gauche par K ou K^{-1} est une isométrie de $\mathrm{Mat}_{mm}(\mathbb{K})$ donc, pour montrer que ψ est un difféomorphisme en X de jacobien donné, il suffit de montrer que c'est le cas en $K^{-1}XK$. D'après le lemme 2.4 ceci permet de supposer $X \in \Delta_m^{>0}$ de diagonale $a_1, \ldots, a_m$. Un

point au voisinage de X dans $\mathcal{H}_m^{>0}(\mathbb{K})$ s'écrit $X+Y$ avec $Y \in \mathcal{H}_m(\mathbb{K})$ au voisinage de zéro. Nous avons $(X+Y)^2 = X^2 + XY + YX + Y^2$ et donc le jacobien cherché est la valeur absolue du déterminant de l'application linéaire $Y \mapsto XY + YX$. Celle-ci consiste à multiplier le i-ème coefficient diagonal (dans $\mathbb{R}$) de Y par $2a_i$ et le coefficient d'indice (i,j) avec $i \neq j$ (dans $\mathbb{K}$) par $a_i + a_j$. Par produit on a immédiatement le résultat. □

Nous noterons à l'occasion $X \mapsto X^{1/2}$ le difféomorphisme inverse de $X \mapsto X^2$.

Nous nous intéressons ensuite à $U_{m\ell}(\mathbb{K})$.

LEMME 8.2. *La sous-variété algébrique réelle* $U_{m\ell}(\mathbb{K})$ *de* $\mathrm{Mat}_{m\ell}(\mathbb{K})$ *est lisse de dimension* $\dim\mathrm{Mat}_{m\ell}(\mathbb{K}) - \dim\mathcal{H}_m(\mathbb{K}) = \kappa m\ell - \kappa m(m-1)/2 - m$ *et l'espace tangent à* $U_{m\ell}(\mathbb{K})$ *en un point* K *de cette sous-variété est* $T_K = \{Z \in \mathrm{Mat}_{m\ell}(\mathbb{K}) \mid ZK^\star + KZ^\star = 0\}$.

DÉMONSTRATION. L'application $f\colon \mathrm{Mat}_{m\ell}(\mathbb{K}) \to \mathcal{H}_m(\mathbb{K})$ donnée par $f(A) = AA^\star$ a pour différentielle en A l'application linéaire $df_A\colon \mathrm{Mat}_{m\ell}(\mathbb{K}) \to \mathcal{H}_m(\mathbb{K})$ donnée par $df_A(Z) = ZA^\star + AZ^\star$. Si $K \in U_{m\ell}(\mathbb{K})$, la différentielle df_K est surjective car si $Y \in \mathcal{H}_m(\mathbb{K})$ alors $df_K(YK) = 2Y$. Par conséquent f est une submersion au voisinage de K et ceci montre que $U_{m\ell}(\mathbb{K})$ est une variété de la dimension indiquée. Enfin, l'espace tangent en K est le noyau de df_K. □

La norme $|\cdot|_{\mathrm{us}}$ induit une métrique sur les espaces tangents de $U_{m\ell}(\mathbb{K})$ donc une structure riemannienne sur cette variété. Cela donne un sens à l'énoncé suivant qui est au cœur du calcul de volume.

PROPOSITION 8.1. *L'application*

$$\begin{aligned} \mathcal{H}_m^{>0}(\mathbb{K}) \times U_{m\ell}(\mathbb{K}) &\longrightarrow G_{m\ell}(\mathbb{K}) \\ (X,K) &\longmapsto XK \end{aligned}$$

est un difféomorphisme dont le jacobien en (X,K) *est*

$$\left(\prod_{i=1}^m a_i\right)^{\kappa(\ell-m+1)-1} \prod_{i<j}\left(\frac{a_i+a_j}{2}\right)^\kappa$$

si $a_1, \ldots, a_m$ *sont les valeurs propres de* X.

DÉMONSTRATION. C'est un difféomorphisme car l'inverse est donné par l'application $A \mapsto ((AA^\star)^{1/2}, (AA^\star)^{-1/2}A)$. Comme dans la démonstration du

lemme 8.1, nous pouvons nous contenter de calculer le jacobien au voisinage de (X, K) avec $X \in \Delta_m^{>0}$ car, en général, $XK = K_0((K_0^{-1}XK_0)(K_0^{-1}K))$ et les trois applications linéaires $K \mapsto K_0^{-1}K, X \mapsto K_0^{-1}XK_0$ et $A \mapsto K_0A$ sont des isométries. Nous supposons dorénavant que X est diagonale, de coefficients diagonaux $a_1, \ldots, a_m$. D'un autre côté, si $K \in U_{m\ell}(\mathbb{K})$ et si l'on note $\mathcal{A}_m(\mathbb{K})$ le sous-espace $\{T \in \mathrm{Mat}_{mm}(\mathbb{K}) \mid T + T^\star = 0\}$ des matrices anti-hermitiennes, nous avons $T_K = \{Z \in \mathrm{Mat}_{m\ell}(\mathbb{K}) \mid ZK^\star \in \mathcal{A}_m(\mathbb{K})\}$. La jacobien que nous cherchons à calculer est donc celui de

$$\begin{aligned} \mathcal{H}_m(\mathbb{K}) \times T_K &\longrightarrow \mathrm{Mat}_{m\ell}(\mathbb{K}) \\ (Y, Z) &\longmapsto (X + Y)(K + Z) \end{aligned}$$

en $(0, 0)$ soit encore, parce que XK est constant et YZ du second ordre, la valeur absolue du déterminant de l'application linéaire

$$\begin{aligned} \mathcal{H}_m(\mathbb{K}) \times T_K &\longrightarrow \mathrm{Mat}_{m\ell}(\mathbb{K}) \\ (Y, Z) &\longmapsto XZ + YK \end{aligned}$$

dans des bases orthonormées.

Notons à présent $\pi_1 \colon \mathrm{Mat}_{m\ell}(\mathbb{K}) \to \mathrm{Mat}_{mm}(\mathbb{K})$ (respectivement $\pi_2 \colon \mathrm{Mat}_{m\ell}(\mathbb{K}) \to \mathrm{Mat}_{m,\ell-m}(\mathbb{K})$) la projection consistant à ne garder que (respectivement à oublier) les m premières colonnes d'une matrice. Sans perte de généralité, nous pouvons supposer que $\pi_1(K)$ est inversible. Alors l'application linéaire

$$\begin{aligned} \varphi \colon \mathrm{Mat}_{m\ell}(\mathbb{K}) &\longrightarrow \mathrm{Mat}_{mm}(\mathbb{K}) \times \mathrm{Mat}_{m,\ell-m}(\mathbb{K}) \\ A &\longmapsto (AK^\star, \pi_2(A)) \end{aligned}$$

est un isomorphisme (son inverse est $(C, B) \mapsto ((C - B\pi_2(K)^\star)(\pi_1(K)^\star)^{-1}\ B)$ où cette dernière matrice est écrite par blocs) qui induit par restriction un isomorphisme $\varphi_{|T_K} \colon T_K \to \mathcal{A}_m(\mathbb{K}) \times \mathrm{Mat}_{m,\ell-m}(\mathbb{K})$. Considérons enfin l'application linéaire

$$\begin{aligned} \psi \colon \mathcal{H}_m(\mathbb{K}) \times \mathcal{A}_m(\mathbb{K}) \times \mathrm{Mat}_{m,\ell-m}(\mathbb{K}) &\longrightarrow \mathrm{Mat}_{mm}(\mathbb{K}) \times \mathrm{Mat}_{m,\ell-m}(\mathbb{K}) \\ (Y, T, B) &\longmapsto (XT + Y, XB + Y\pi_2(K)) \end{aligned}$$

et calculons

$$\begin{aligned} (\psi \circ (\mathrm{id}_{\mathcal{H}_m(\mathbb{K})} \times \varphi_{|T_K}))(Y, Z) &= \psi(Y, ZK^\star, \pi_2(Z)) \\ &= (XZK^\star + Y, X\pi_2(Z) + Y\pi_2(K)) \\ &= (XZK^\star + YKK^\star, \pi_2(XZ + YK)) \\ &= \varphi(XZ + YK). \end{aligned}$$

En particulier ψ est un isomorphisme (car $(Y,Z)\mapsto XZ+YK$ en est un) et donc le jacobien cherché est la valeur absolue du déterminant (dans des bases orthonormées) de $\varphi^{-1}\circ\psi\circ(\mathrm{id}_{\mathcal{H}_m(\mathbb{K})}\times\varphi_{|T_K})$, c'est-à-dire $|\det\psi|\cdot|\det\varphi_{|T_K}/\det\varphi|$. Montrons dans un premier temps que $|\det\varphi_{|T_K}|=|\det\varphi|$. Pour ce faire, nous considérons les orthogonaux de T_K et de son image par φ. D'une part $\varphi(T_K)=\mathcal{A}_m(\mathbb{K})\times\mathrm{Mat}_{m,\ell-m}(\mathbb{K})$ donc $\varphi(T_K)^\perp=\mathcal{H}_m(\mathbb{K})\times\{0\}$ (car $\mathcal{A}_m(\mathbb{K})^\perp=\mathcal{H}_m(\mathbb{K})$). D'autre part, nous avons $(T_K)^\perp=\{YK\mid Y\in\mathcal{H}_m(\mathbb{K})\}$: en effet ces deux espaces ont même dimension (comme φ est un isomorphisme $\dim(T_K)^\perp=\dim\varphi(T_K)^\perp$) et le second est inclus dans le premier car si $Y\in\mathcal{H}_m(\mathbb{K})$ et $Z\in T_K$ alors $ZK^\star\in\mathcal{A}_m(\mathbb{K})$ donc $Y\perp ZK^\star$ soit $\mathrm{Tr}(Y(ZK^\star)^\star)=0$ qui s'écrit $\mathrm{Tr}(YKZ^\star)=0$ ou encore $YK\perp Z$ donc $YK\in(T_K)^\perp$.

Comme $\varphi(YK)=(YKK^\star,\pi_2(YK))=(Y,Y\pi_2(K))$ est la somme des composantes $(Y,0)\in\varphi(T_K)^\perp$ et $(0,Y\pi_2(K))\in\varphi(T_K)$, la matrice de φ dans des bases orthonormées adaptées aux décompositions $\mathrm{Mat}_{m\ell}(\mathbb{K})=T_K\oplus(T_K)^\perp$ et $\mathrm{Mat}_{mm}(\mathbb{K})\times\mathrm{Mat}_{m,\ell-m}(\mathbb{K})=\varphi(T_K)\oplus\varphi(T_K)^\perp$ a la forme

$$\begin{pmatrix}\text{matrice de}\\ \varphi_{|T_K}\end{pmatrix}\quad\begin{matrix}\text{matrice de}\\ YK\mapsto(0,Y\pi_2(K))\end{matrix}$$
$$\begin{pmatrix}0\end{pmatrix}\quad\begin{matrix}\text{matrice de}\\ YK\mapsto(Y,0)\end{matrix}\Bigg).$$

L'application linéaire $YK\mapsto(Y,0)$ est une isométrie ($\mathrm{Tr}(YK(YK)^\star)=\mathrm{Tr}(YY^\star)$) donc de déterminant ±1. Grâce à la matrice ci-dessus, nous trouvons bien $|\det\varphi|=|\det\varphi_{|T_K}|$.

Il reste à évaluer le déterminant de ψ. Pour cela, nous pouvons supposer $\pi_2(K)=0$: en effet ψ est la composée de $(Y,T,B)\mapsto(Y,T,B+X^{-1}Y\pi_2(K))$ clairement de déterminant 1 et de $(Y,T,B')\mapsto(XT+Y,XB')$ qui n'est autre que ψ lorsque $\pi_2(K)=0$. Ainsi ψ est le produit des isomorphismes $(Y,T)\mapsto XT+Y$ et $B\mapsto XB$. Le second qui consiste à multiplier la i-ème ligne de B par a_i (on rappelle que X est diagonale) a pour déterminant $\left(\prod_{i=1}^m a_i\right)^{\kappa(\ell-m)}$.

Pour le premier, nous fixons des bases orthonormées de $\mathcal{H}_m(\mathbb{K})$, $\mathcal{A}_m(\mathbb{K})$ et $\mathrm{Mat}_{mm}(\mathbb{K})$. Notons E_{ij} la matrice dont le seul coefficient non nul vaut 1 et est d'indice (i,j). Soit ensuite $e_1,\dots,e_\kappa$ une base orthonormée de $\mathbb{K}$ sur $\mathbb{R}$ avec $e_1=1$ (ceci entraîne $e_k+e_k^\star=0$ si $k>1$). Alors

$$\{e_1E_{ii}\mid 1\le i\le m\}\cup\left\{\frac{e_kE_{ij}+e_k^\star E_{ji}}{\sqrt{2}}\mid 1\le k\le\kappa,\ 1\le i<j\le m\right\}$$

et

$$\{e_k E_{ii} \mid 2 \leq k \leq \kappa,\ 1 \leq i \leq m\} \cup \left\{ \frac{e_k E_{ij} - e_k^\star E_{ji}}{\sqrt{2}} \mid 1 \leq k \leq \kappa,\ 1 \leq i < j \leq m \right\}$$

sont respectivement des bases orthonormées de $\mathcal{H}_m(\mathbb{K})$ et $\mathcal{A}_m(\mathbb{K})$. Comme on a $\mathrm{Mat}_{mm}(\mathbb{K}) = \mathcal{H}_m(\mathbb{K}) \oplus \mathcal{A}_m(\mathbb{K})$, on peut réunir les bases de $\mathcal{H}_m(\mathbb{K})$ et $\mathcal{A}_m(\mathbb{K})$ pour obtenir une base orthonormée de $\mathrm{Mat}_{mm}(\mathbb{K})$. Maintenant l'application $(Y, T) \mapsto XT + Y$ est l'identité sur les vecteurs de base de $\mathcal{H}_m(\mathbb{K})$ et $XE_{ij} = a_i E_{ij}$ pour tous $1 \leq i, j \leq m$. La matrice de cette application est donc donnée par une matrice triangulaire où on trouve, sur la diagonale, $\dim \mathcal{H}_m(\mathbb{K})$ fois la valeur 1, $\kappa - 1$ fois $a_1, \ldots, a_m$ (correspondant aux images des vecteurs $e_k E_{ii}$, $2 \leq k \leq \kappa$, $1 \leq i \leq m$) et κ fois $(a_i + a_j)/2$, $1 \leq i < j \leq m$. Le déterminant de cette matrice est donc

$$\left(\prod_{i=1}^{m} a_i \right)^{\kappa - 1} \prod_{i<j} \left(\frac{a_i + a_j}{2} \right)^{\kappa}$$

et ceci termine la démonstration. □

Nous pouvons à présent appliquer ce qui précède à un calcul de volume.

LEMME 8.3. *Soit $\mathcal{X}$ une partie mesurable de $\mathcal{H}_m^{>0}(\mathbb{K})$ et posons $\mathcal{X}_\ell = \{A \in G_{m\ell} \mid AA^\star \in \mathcal{X}\}$. Alors $\mathcal{X}_\ell$ est mesurable et l'on a*

$$\mathrm{vol}(\mathcal{X}_\ell) = 2^{-m(1+\kappa(m-1)/2)} \mathrm{vol}(U_{m\ell}(\mathbb{K})) \int_{\mathcal{X}} \mathrm{Nm}(Y)^{\frac{\kappa(\ell-m+1)-2}{2\kappa m}} dY.$$

DÉMONSTRATION. Écrivons $\mathcal{X}' = \mathcal{X}_m \cap \mathcal{H}_m^{>0}(\mathbb{K}) = \{X \in \mathcal{H}_m^{>0}(\mathbb{K}) \mid X^2 \in \mathcal{X}\}$. Le difféomorphisme de la proposition précédente induit une bijection $\mathcal{X}' \times U_{m\ell}(\mathbb{K}) \to \mathcal{X}_\ell$ qui permet d'écrire, en notant $a_1, \ldots, a_m$ les valeurs propres de X,

$$\begin{aligned} \mathrm{vol}(\mathcal{X}_\ell) &= \int_{X \in \mathcal{X}'} \int_{K \in U_{m\ell}(\mathbb{K})} \left(\prod_{i=1}^{m} a_i \right)^{\kappa(\ell-m+1)-1} \prod_{i<j} \left(\frac{a_i + a_j}{2} \right)^{\kappa} dX\, dK \\ &= 2^{-\kappa m(m-1)/2} \mathrm{vol}(U_{m\ell}(\mathbb{K})) \int_{X \in \mathcal{X}'} \mathrm{Nm}(X)^{\frac{\kappa(\ell-m+1)-1}{\kappa m}} \prod_{i<j} (a_i + a_j)^{\kappa} dX. \end{aligned}$$

Maintenant nous avons une bijection $\mathcal{X}' \to \mathcal{X}, X \mapsto Y = X^2$ et le lemme 8.1

donne $dY = 2^m \mathrm{Nm}(X)^{1/\kappa m} \prod_{i<j} (a_i + a_j)^\kappa dX$ d'où

$$\mathrm{vol}(\mathcal{X}_\ell) = 2^{-\kappa m(m-1)/2-m} \mathrm{vol}(U_{m\ell}(\mathbb{K})) \int\limits_{Y\in\mathcal{X}} \mathrm{Nm}(X)^{\frac{\kappa(\ell-m+1)-2}{\kappa m}} dY$$

qui est le résultat avec $\mathrm{Nm}(X) = \mathrm{Nm}(Y)^{1/2}$. □

Il nous reste à calculer le volume de $U_{m\ell}(\mathbb{K})$. Rappelons que nous notons $\omega_i = \pi^{i/2}\Gamma(i/2+1)^{-1}$ le volume de la boule unité de $\mathbb{R}^i$.

LEMME 8.4. *Pour la norme euclidienne usuelle* $|\cdot|_{\mathrm{us}}$ *sur* $\mathrm{Mat}_{m\ell}(\mathbb{K})$ *nous avons*

$$\mathrm{vol}(U_{m\ell}(\mathbb{K})) = 2^{\kappa m(m-1)/4} \prod_{i=\ell-m+1}^{\ell} \kappa i \omega_{\kappa i}.$$

DÉMONSTRATION. L'idée consiste à appliquer la formule du lemme précédent à un ensemble $\mathcal{X}$ explicite. Pour cela, fixons pour un réel $\varepsilon > 0$ un cube $\mathfrak{C}_\varepsilon$ dans $\mathbb{K}$ de côté ε (donc de volume ε^κ), centré en 0 et stable par conjugaison. Définissons $\mathcal{X}$ comme l'ensemble des matrices $X \in \mathcal{H}_m(\mathbb{K})$ dont les coefficients diagonaux, réels, appartiennent à l'intervalle $[1-\varepsilon, 1+\varepsilon]$ et tous les autres à $\mathfrak{C}_\varepsilon$. Pour ε assez petit ceci assure $\mathcal{X} \subset \mathcal{H}_m^{>0}(\mathbb{K})$. Le volume de $\mathcal{X}$ vaut $(2\varepsilon)^m(\sqrt{2}\varepsilon)^{\kappa m(m-1)/2}$: pour les coefficients non diagonaux, on utilise $\mathrm{vol}\{(z,z^\star) \mid z \in \mathfrak{C}_\varepsilon\} = (\sqrt{2}\varepsilon)^\kappa$. Par ailleurs, comme $\mathcal{X}$ est centrée autour de la matrice I, nous avons

$$\lim_{\varepsilon\to 0} \frac{1}{\mathrm{vol}(\mathcal{X})} \int\limits_{\mathcal{X}} \mathrm{Nm}(Y)^{\frac{\kappa(\ell-m+1)-2}{2\kappa m}} dY = 1.$$

En vertu du lemme précédent, cela nous autorise à calculer $\mathrm{vol}(U_{m\ell}(\mathbb{K}))$ par la formule

$$\begin{aligned}\mathrm{vol}(U_{m\ell}(\mathbb{K})) &= 2^{m(1+\kappa(m-1)/2)} \lim_{\varepsilon\to 0} \frac{\mathrm{vol}(\mathcal{X}_\ell)}{\mathrm{vol}(\mathcal{X})} \\ &= 2^{\kappa m(m-1)/4} \lim_{\varepsilon\to 0} \frac{\mathrm{vol}(\mathcal{X}_\ell)}{\varepsilon^{m(1+\kappa(m-1)/2)}}.\end{aligned}$$

Évaluons maintenant directement $\mathrm{vol}(\mathcal{X}_\ell)$. Nous voyons $A \in \mathcal{X}_\ell$ comme la collection de ses vecteurs lignes notés $y_1, \dots, y_m$ (dans $\mathbb{K}^\ell$). La condition $AA^\star \in \mathcal{X}$ s'écrit donc $|y_i|_{\mathrm{us}}^2 \in [1-\varepsilon, 1+\varepsilon]$ pour $1 \le i \le m$ et $y_i y_j^\star \in \mathfrak{C}_\varepsilon$ pour $1 \le i \ne j \le m$. L'ensemble des valeurs possibles pour y_1 c'est-à-dire

$\{y \in \mathbb{K}^\ell \mid \sqrt{1-\varepsilon} \leq |y|_{\mathrm{us}} \leq \sqrt{1+\varepsilon}\}$ est une coquille sphérique de volume

$$\begin{aligned}\omega_{\kappa\ell}\sqrt{1+\varepsilon}^{\kappa\ell} - \omega_{\kappa\ell}\sqrt{1-\varepsilon}^{\kappa\ell} &= \omega_{\kappa\ell}\Big(1+\frac{\kappa\ell}{2}\varepsilon\Big) - \omega_{\kappa\ell}\Big(1-\frac{\kappa\ell}{2}\varepsilon\Big) + O(\varepsilon^2)\\ &= \kappa\ell\omega_{\kappa\ell}\varepsilon + O(\varepsilon^2).\end{aligned}$$

Si y_1 est fixé, étudions l'ensemble des valeurs possibles de y_2 c'est-à-dire $\{y \in \mathbb{K}^\ell \mid 1-\varepsilon \leq |y|_{\mathrm{us}}^2 \leq 1+\varepsilon \text{ et } yy_1^\star \in \mathfrak{C}_\varepsilon\}$. Pour cela, décomposons $y = \lambda y_1 + y'$ avec $\lambda \in \mathbb{K}$ et $y' \in (\mathbb{K}y_1)^\perp$. Ainsi la condition $yy_1^\star \in \mathfrak{C}_\varepsilon$ se lit simplement $\lambda \in (1/|y_1|_{\mathrm{us}}^2)\mathfrak{C}_\varepsilon$. Par conséquent, λ varie dans un cube de volume $(\varepsilon/|y_1|_{\mathrm{us}}^2)^\kappa = \varepsilon^\kappa + O(\varepsilon^{\kappa+1})$. Pour y' nous avons $|y'|_{\mathrm{us}}^2 = |y|_{\mathrm{us}}^2 - |\lambda y_1|_{\mathrm{us}}^2$ d'où $\sqrt{1-\varepsilon-|\lambda y_1|_{\mathrm{us}}^2} \leq |y'|_{\mathrm{us}} \leq \sqrt{1+\varepsilon-|\lambda y_1|_{\mathrm{us}}^2}$. Ainsi y' varie dans une coquille sphérique de $(\mathbb{K}y_1)^\perp \simeq \mathbb{K}^{\ell-1}$ dont le volume peut s'écrire $\kappa(\ell-1)\omega_{\kappa(\ell-1)}\varepsilon + O(\varepsilon^2)$ car $|\lambda y_1|_{\mathrm{us}}^2 = O(\varepsilon^2)$. Par suite

$$\mathrm{vol}\{y \in \mathbb{K}^\ell \mid 1-\varepsilon \leq |y|_{\mathrm{us}}^2 \leq 1+\varepsilon \text{ et } yy_1^\star \in \mathfrak{C}_\varepsilon\} = \kappa(\ell-1)\omega_{\kappa(\ell-1)}\varepsilon^{\kappa+1}(1+O(\varepsilon)).$$

Si nous itérons ce procédé, nous voyons que si $y_1, \ldots, y_i$ sont fixés alors le volume de $\{y \in \mathbb{K}^\ell \mid 1-\varepsilon \leq |y|_{\mathrm{us}}^2 \leq 1+\varepsilon \text{ et } yy_j^\star \in \mathfrak{C}_\varepsilon \text{ si } 1 \leq j \leq i\}$ s'écrit sous la forme $\kappa(\ell-i)\omega_{\kappa(\ell-i)}\varepsilon^{\kappa i+1}(1+O(\varepsilon))$. Par conséquent, d'après le théorème de Fubini, nous avons

$$\mathrm{vol}(\mathcal{X}_\ell) = \int_{y_1}\cdots\int_{y_m} dy_1\cdots dy_m = \left(\varepsilon^{\kappa m(m-1)/2+m}\prod_{i=\ell-m+1}^{\ell}\kappa i\omega_{\kappa i}\right)(1+O(\varepsilon))$$

et ceci donne le résultat en reportant $\mathrm{vol}(\mathcal{X}_\ell)$ dans la limite exprimant le volume de $U_{m\ell}(\mathbb{K})$. □

Nous allons maintenant traduire ces résultats pour $D \otimes \mathbb{R}$ mais faisons auparavant une remarque sur le choix de la norme. Alors que nous avons employé jusqu'ici $|\cdot|_{\mathrm{us}}$ sur $\mathrm{Mat}_{m\ell}(\mathbb{K})$, nous souhaitons à présent exprimer nos calculs à l'aide de $|\cdot| = \sqrt{\kappa m}|\cdot|_{\mathrm{us}}$. Le lemme 8.1 et la proposition 8.1 sont valables à l'identique car le jacobien ne varie pas lorsque nous changeons simultanément la norme à la source et au but par un même facteur. La même chose vaut pour le lemme 8.3 : la formule est la même que $\mathrm{vol}(\mathcal{X}_\ell)$, $\mathrm{vol}(U_{m\ell}(\mathbb{K}))$ et dY soient tous trois définis à l'aide de $|\cdot|_{\mathrm{us}}$ ou qu'ils soient définis à l'aide de $|\cdot|$. En revanche, la valeur explicite du lemme 8.4 se trouve, elle, multipliée par $\sqrt{\kappa m}^{\dim U_{m\ell}(\mathbb{K})}$.

Pour toute matrice hermitienne X sur $\mathbb{K}$ de valeurs propres a_i nous posons

$$v(X) = \left(\prod_i a_i\right)^{\kappa-1}\prod_{i<j}\left(\frac{a_i+a_j}{2}\right)^\kappa.$$

Ceci nous permet de définir par produit une fonction

$$v\colon (D\otimes\mathbb{R})_{\mathrm{sym}}\longrightarrow\mathbb{R}$$

en utilisant

$$(D\otimes\mathbb{R})_{\mathrm{sym}}\simeq\mathcal{H}_d(\mathbb{R})^{r_1}\times\mathcal{H}_d(\mathbb{C})^{r_2}\times\mathcal{H}_{d/2}(\mathbb{H})^{r_3}.$$

On vérifie immédiatement que v ne dépend pas du choix de l'isomorphisme, que si $x\in(D\otimes\mathbb{R})^{>0}_{\mathrm{sym}}$ alors $v(x)>0$, que $v(1)=1$ et que l'on a pour tout $t\in\mathbb{R}$ et $x\in(D\otimes\mathbb{R})_{\mathrm{sym}}$

$$v(tx)=t^{n-s}v(x)$$

où $s=\dim(D\otimes\mathbb{R})_{\mathrm{sym}}$. Nous définissons encore

$$G_N(D\otimes\mathbb{R})=\{v\in(D\otimes\mathbb{R})^N\mid \mathrm{Nm}(vv^\star)>0\}$$

et

$$U_N(D\otimes\mathbb{R})=\{k\in(D\otimes\mathbb{R})^N\mid kk^\star=1\}.$$

Nous résumons le travail fait jusqu'ici dans l'énoncé suivant.

LEMME 8.5. *L'application*

$$\begin{aligned}(D\otimes\mathbb{R})^{>0}_{\mathrm{sym}}\times U_N(D\otimes\mathbb{R})&\longrightarrow G_N(D\otimes\mathbb{R})\\(x,k)&\longmapsto xk\end{aligned}$$

est un difféomorphisme dont le jacobien en (x,k) est $\mathrm{Nm}(x)^{N-1}v(x)$.

L'ensemble $U_N(D\otimes\mathbb{R})$ est une sous-variété lisse de $(D\otimes\mathbb{R})^N$ de dimension $Nn-s$ et de volume

$$2^{Nd^2(r_2+\frac{r_3}{2})+\frac{d(d-1)}{4}r_1+\frac{d}{2}r_2+\frac{3d}{4}r_3}\sqrt{d}^{Nn-s}$$
$$\times\left(\prod_{i=d(N-1)+1}^{Nd}i\omega_i\right)^{r_1}\left(\prod_{i=d(N-1)+1}^{Nd}i\omega_{2i}\right)^{r_2}\left(\prod_{i=\frac{d}{2}(N-1)+1}^{\frac{Nd}{2}}i\omega_{4i}\right)^{r_3}.$$

DÉMONSTRATION. Il nous suffit d'écrire

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

et d'appliquer nos résultats à chaque facteur $\mathrm{Mat}_{m\ell}(\mathbb{K})$ avec $m=d$, $\ell=Nd$ si $\mathbb{K}\neq\mathbb{H}$ et $m=d/2$, $\ell=Nd/2$ si $\mathbb{K}=\mathbb{H}$. Il est immédiat que $G_N(D\otimes\mathbb{R})$ est le produit des $G_{m\ell}(\mathbb{K})$ et $U_N(D\otimes\mathbb{R})$ celui des $U_{m\ell}(\mathbb{K})$. Pour avoir la première assertion, nous remarquons que dans la proposition 8.1 le jacobien en (X,K) est $\mathrm{Nm}(X)^{(\ell-m)/m}v(X)$ et dans notre produit nous avons toujours

$(\ell - m)/m = N - 1$. Pour la seconde, le lecteur courageux fera le produit de

$$\sqrt{d}^{Nd^2 - \frac{d^2-d}{2} - d} 2^{d(d-1)/4} \prod_{i=d(N-1)+1}^{Nd} i\omega_i$$

élevé à la puissance r_1, de

$$\sqrt{2d}^{2Nd^2 - d^2} 2^{d(d-1)/2} 2^d \prod_{i=d(N-1)+1}^{Nd} i\omega_{2i}$$

élevé à la puissance r_2 et de

$$\sqrt{2d}^{Nd^2 - \frac{d(d-2)}{2} - \frac{d}{2}} 2^{d(d-2)/4} 2^d \prod_{i=\frac{d}{2}(N-1)+1}^{\frac{Nd}{2}} i\omega_{4i}$$

élevé à la puissance r_3 en remarquant toutefois que $\sqrt{d}$ figure à chaque fois à la puissance $\dim U_{m\ell}(\mathbb{K})$ donc finalement à la puissance $\dim G_N(D \otimes \mathbb{R}) - \dim(D \otimes \mathbb{R})^{>0}_{\mathrm{sym}} = Nn - s$. □

Ce lemme nous permettra d'écrire le volume du domaine fondamental qui nous intéresse, partie de $G_N(D \otimes \mathbb{R})$, à l'aide d'une intégrale sur une partie de $(D \otimes \mathbb{R})^{>0}_{\mathrm{sym}}$, sensiblement de la même façon que dans le lemme 8.3. Pour manipuler cette intégrale, nous présentons un dernier fait auxiliaire.

LEMME 8.6. *Soient E un espace euclidien de dimension m, $P : E \to \mathbb{R}$ un polynôme homogène de degré $k \geq 1$ et Ω une partie mesurable de E telle que $\Omega = \{\omega \in \mathbb{R}_{\geq 0}\Omega \mid 0 < |P(\omega)| \leq 1\}$. Si $f : E \to \mathbb{R}$ est une fonction intégrable homogène de degré β et $\alpha > -(m+\beta)/k$ un réel, on a*

$$\int_\Omega |P(\omega)|^\alpha f(\omega) d\omega = \frac{m+\beta}{k\alpha + m + \beta} \int_\Omega f(\omega) d\omega.$$

DÉMONSTRATION. Notons $E' = \{\omega' \in E \mid |P(\omega')| = 1\}$ et $\Omega' = \Omega \cap E'$. Par hypothèse, $\Omega = \{t\omega' | t \in]0,1],\ \omega' \in \Omega'\}$. Si nous posons $\omega = t\omega'$, il vient $|P(\omega)| = t^k$, $f(\omega) = t^\beta f(\omega')$ et $d\omega = t^{m-1} g(\omega') dt\, d\omega'$ pour une certaine fonction $g : E' \to \mathbb{R}$ (un calcul explicite montre que $g(\omega') = k/||dP_{\omega'}||$ mais cela n'a pas d'importance ici). Alors

$$\begin{aligned} \int_\Omega |P(\omega)|^\alpha f(\omega) d\omega &= \int_0^1 \int_{\Omega'} t^{k\alpha+\beta+m-1} f(\omega') g(\omega') dt\, d\omega' \\ &= \frac{1}{k\alpha + m + \beta} \int_{\Omega'} (fg)(\omega') d\omega'. \end{aligned}$$

Cette même égalité avec $\alpha = 0$ donne $\int_{\Omega'} (fg)(\omega')d\omega' = (m+\beta)\int_{\Omega} f(\omega)d\omega$. □

Nous utilisons maintenant les notations S, F_N^+ et $F^{\leq 1}$ de la partie 6 ainsi que la proposition 6.2. Nous cherchons à calculer $\mathrm{vol}(S) = \mathrm{vol}(F_N^+)$. Vu les définitions, ce volume vaut

$$\mathrm{vol}(F_N^+) = \frac{\mathrm{vol}(\{v \in (D\otimes\mathbb{R})^N \mid 0 < \mathrm{Nm}(vv^\star) \leq 1 \text{ et } \forall u \in \mathcal{U},\ |v| \leq |uv|\})}{\mathrm{Card}G}.$$

Si nous notons $F_N^{\leq 1}$ l'ensemble dont le volume apparaît ci-dessus et $F_{\mathrm{sym}}^{\leq 1} = F^{\leq 1} \cap (D\otimes\mathbb{R})_{\mathrm{sym}}^{>0}$, nous remarquons que $F_N^{\leq 1}$ est défini uniquement par des conditions sur $vv^\star \in (D\otimes\mathbb{R})_{\mathrm{sym}}^{>0}$ et donc en écrivant $vv^\star = x^2$ pour $x \in (D\otimes\mathbb{R})_{\mathrm{sym}}^{>0}$ nous avons

$$F_N^{\leq 1} = \{xk \mid k \in U_N(D\otimes\mathbb{R}) \text{ et } x \in F_{\mathrm{sym}}^{\leq 1}\}.$$

Par suite avec le lemme 8.5

$$\begin{aligned}\mathrm{vol}(F_N^{\leq 1}) &= \int_{F_{\mathrm{sym}}^{\leq 1}} \int_{U_N(D\otimes\mathbb{R})} \mathrm{Nm}(x)^{N-1} v(x)dx\,dk \\ &= \mathrm{vol}(U_N(D\otimes\mathbb{R})) \int_{F_{\mathrm{sym}}^{\leq 1}} \mathrm{Nm}(x)^{N-1} v(x)dx.\end{aligned}$$

Nous appliquons alors le lemme 8.6 avec $E = (D\otimes\mathbb{R})_{\mathrm{sym}}$, $m = s$, $P = \mathrm{Nm}$, $k = n$, $\Omega = F_{\mathrm{sym}}^{\leq 1}$, $f = v$, $\beta = n - s$ et $\alpha = N - 1$. Nous trouvons

$$\mathrm{vol}(F_N^{\leq 1}) = \frac{1}{N}\mathrm{vol}(U_N(D\otimes\mathbb{R})) \int_{F_{\mathrm{sym}}^{\leq 1}} v(x)dx.$$

Cette formule avec $N = 1$ donne aussi

$$\mathrm{vol}(F^{\leq 1}) = \mathrm{vol}(U_1(D\otimes\mathbb{R})) \int_{F_{\mathrm{sym}}^{\leq 1}} v(x)dx$$

donc

$$\mathrm{vol}(F_N^{\leq 1}) = \frac{\mathrm{vol}(U_N(D\otimes\mathbb{R}))}{N\mathrm{vol}(U_1(D\otimes\mathbb{R}))}\mathrm{vol}(F^{\leq 1}).$$

Finalement, nous avons

$$\mathrm{vol}(S) = \frac{\mathrm{vol}(U_N(D\otimes\mathbb{R}))}{N\mathrm{vol}(U_1(D\otimes\mathbb{R}))}\,\frac{\mathrm{vol}(F^{\leq 1})}{\mathrm{Card}G}.$$

Deux applications du lemme 8.5 montrent

$$\frac{\mathrm{vol}(U_N(D\otimes\mathbb{R}))}{\mathrm{vol}(U_1(D\otimes\mathbb{R}))}=2^{(N-1)d^2(r_2+r_3/2)}\sqrt{d}^{\,(N-1)n}\binom{Nd}{d}_{[1]}^{r_1}\binom{Nd}{d}_{[2]}^{r_2}\binom{Nd/2}{d/2}_{[4]}^{r_3}$$

avec les notations de l'introduction. Il vient donc

$$\mathrm{vol}(S)=\frac{\Re'}{N}\left(2^{d^2(r_2+\frac{r_3}{2})}d^{\frac{n}{2}}\right)^{N-1}\binom{Nd}{d}_{[1]}^{r_1}\binom{Nd}{d}_{[2]}^{r_2}\binom{Nd/2}{d/2}_{[4]}^{r_3}.$$

9. Conclusion et exemples

Dans cette partie, nous démontrons les énoncés de l'introduction.

Pour le théorème principal 1.1, il s'agit simplement de rassembler les renseignements obtenus plus haut, à l'exception d'un cas que nous devons traiter à part car il est exclu par le théorème 5.1 : c'est celui où $N=2$ et $n=1$ c'est-à-dire $D=\mathbb{Q}$. Nous nous trouvons donc face au problème classique de compter les points de hauteur bornée dans $\mathbb{P}^1(\mathbb{Q})$. En voici une version effective qui nous suffit ici.

LEMME 9.1. *Pour tout réel $H\geq 0$ on a $|\mathcal{N}^{\mathbb{Z},\mathrm{id}}_{\mathrm{gche}}(2,1,H)-(3/\pi)H^2|\leq 24607H$.*

DÉMONSTRATION. Nous écrivons simplement $\mathcal{N}(H)$ pour $\mathcal{N}^{\mathbb{Z},\mathrm{id}}_{\mathrm{gche}}(2,1,H)$. Nous pouvons clairement supposer $H\geq 1$. Nous utilisons la formule d'inversion

$$\mathcal{N}(H)=\frac{1}{2}\sum_{m=1}^{[H]}\mu(m)\,\mathrm{Card}\Big((m\mathbb{Z})^2\cap H\Theta\Big)$$

où $\Theta=\{(x,y)\in\mathbb{R}^2\mid 0<x^2+y^2\leq 1\}$ et μ est la fonction de Möbius ordinaire sur les entiers. Dans nos notations, $\mu(m)=\mu(m\mathbb{Z},\mathbb{Z})$ et la formule est exactement celle de la proposition 4.1 avec $\mathcal{D}=\mathbb{Z}$ et $\mathcal{A}=m\mathbb{Z}$ (mais elle est bien sûr tout à fait classique et plus facile à établir). Nous avons ensuite

$$\Big|\mathrm{Card}\Big((m\mathbb{Z})^2\cap H\Theta\Big)-\pi(H/m)^2\Big|\leq 16401(H/m)^{2/3}$$

d'après le résultat de [Ch] (version effective du problème du cercle de Gauss ; nous avons ajouté 1 pour tenir compte de $0\notin\Theta$). Cette estimation plus précise remplace (†) qui ne permet pas de conclure ici. En combinant,

nous trouvons

$$\left| \mathcal{N}(H) - \frac{\pi}{2} \sum_{m=1}^{+\infty} \mu(m) \left(\frac{H}{m}\right)^2 \right| \leq \frac{\pi}{2} \sum_{m=[H]+1}^{+\infty} \left(\frac{H}{m}\right)^2 + 8201 \sum_{m=1}^{[H]} \left(\frac{H}{m}\right)^{2/3}.$$

Pour conclure nous majorons simplement

$$\sum_{m=[H]+1}^{+\infty} m^{-2} \leq \sum_{m=[H]+1}^{+\infty} (m^2 - m)^{-1} = \frac{1}{[H]} \leq \frac{2}{H}$$

et

$$\sum_{m=1}^{[H]} m^{-2/3} \leq 1 + \int_1^H x^{-2/3} dx = 3H^{1/3} - 2.$$

Ceci donne le résultat (avec $\zeta(2) = \pi^2/6$). □

Nous pouvons maintenant conclure le décompte.

Démonstration du théorème 1.1. Lorsque $N = 2$ et $n = 1$ le lemme ci-dessus donne la conclusion car ici $h' = \rho = 1$ donc $h'(Nn\rho)^{7N^2n^2} = 2^{28} \geq 24607$. Dans tous les autres cas, la condition $N \geq 2$ entraîne l'inégalité $N > 3/2 - 1/2d + 1/n$ sous laquelle est établie le théorème 5.1 lorsque $M = 1$. En tenant compte des valeurs de c_1 et c_2 déterminées à la fin de la partie 7, celui-ci nous fournit la formule (établie pour $H > 0$ mais bien sûr valable si $H = 0$)

$$\left| \mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(N, 1, H) - \frac{h' \mathrm{vol}(S) H^{Nn}}{\mathrm{vol}(\mathcal{O})^N \zeta_D(N)} \right| \leq h'(Nn\rho)^{7N^2n^2} H^{Nn-1}.$$

Nous insérons ensuite la valeur de $\mathrm{vol}(\mathcal{O})$ (voir lemme 2.3) et celle de $\mathrm{vol}(S)$ obtenue à la fin de la partie précédente. Nous trouvons alors la formule annoncée pour c_{princ} et la démonstration est terminée. □

Nous établissons maintenant les énoncés concernant l'influence sur le décompte des choix de l'ordre maximal et de l'involution. Commençons par le terme principal.

Démonstration de la proposition 1.2. Comme dans la partie 4 (mais avec ici $M = 1$) nous notons R un ensemble de représentants des classes

d'isomorphie d'idéaux à droite de $\mathcal{O}$. Nous avons donc $h' = \sum_{I \in R} [\mathcal{O}^\times : \mathcal{O}_g(I)^\times]$. D'après la définition de $\Re'$ comme volume de domaine fondamental, il vient $[\mathcal{O}^\times : \mathcal{O}_g(I)^\times]\Re' = \Re'_{\mathcal{O}_g(I)}$. De plus, pour tout $x \in D^\times$, nous avons $\Re'_{\mathcal{O}_g(I)} = \Re'_{x\mathcal{O}_g(I)x^{-1}}$ car l'application $D \otimes \mathbb{R} \to D \otimes \mathbb{R}$, $y \mapsto xyx^{-1}$ préserve le volume (son déterminant est égal à 1). Par suite, nous pouvons écrire

$$h'\Re' = \sum_{\mathcal{O}'} f(\mathcal{O}')\Re'_{\mathcal{O}'}$$

où $\mathcal{O}'$ parcourt un système de représentants des ordres maximaux de D à conjugaison près et $f(\mathcal{O}')$ désigne le nombre de $I \in R$ tels que $\mathcal{O}_g(I)$ et $\mathcal{O}'$ sont conjugués. Pour obtenir la formule annoncée, il nous suffit de voir que $f(\mathcal{O}') = h_{\text{bil}}(\mathcal{O}')$. Pour cela, nous choisissons un idéal à gauche M de $\mathcal{O}$ tel que $\mathcal{O}_d(M) = \mathcal{O}'$ (voir [R] (22.21) page 198). Alors l'application $I \mapsto IM$ induit une bijection entre les idéaux fractionnaires à droite de $\mathcal{O}$ tels que $\mathcal{O}_g(I) = \mathcal{O}'$ et les idéaux bilatères fractionnaires de $\mathcal{O}'$. Cette bijection préserve les classes d'isomorphie car deux idéaux bilatères sont isomorphes si et seulement s'ils sont isomorphes comme idéaux à droite (ou à gauche). Elle montre donc que $h_{\text{bil}}(\mathcal{O}')$ est égal au nombre de classes de I avec $\mathcal{O}_g(I) = \mathcal{O}'$ ou encore au nombre de $I \in R$ tels qu'il existe $x \in D^\times$ avec $\mathcal{O}_g(xI) = \mathcal{O}'$. La formule $\mathcal{O}_g(xI) = x\mathcal{O}_g(I)x^{-1}$ donne alors bien $f(\mathcal{O}') = h_{\text{bil}}(\mathcal{O}')$. La définition même de f montre que $f(\mathcal{O}')$ ne dépend que de la classe de conjugaison de $\mathcal{O}'$ tandis que $h_{\text{bil}}(\mathcal{O}') = h_{\text{bil}}((\mathcal{O}')^{\text{op}})$ est clair. Il nous reste donc seulement à vérifier $\Re'_{\mathcal{O}} = \Re'_{\mathcal{O}^{\text{op}}}$. En d'autres termes nous devons montrer que des domaines fondamentaux pour les actions à droite et à gauche du groupe $\mathcal{O}^\times$ ont le même volume. On considère pour cela l'involution $\imath$ de $(D \otimes \mathbb{R})^\times$ définie par $\imath(x) = |\text{Nm}(x)|^{2/n}x^{-1}$. Elle vérifie $\imath(xy) = \imath(y)\imath(x)$ et $\text{Nm}(\imath(x)) = \text{Nm}(x)$ pour tous $x, y \in (D \otimes \mathbb{R})^\times$ tandis que $\imath(u) = u^{-1}$ si $u \in \mathcal{O}^\times$. Notons aussi $\Theta = \{x \in (D \otimes \mathbb{R})^\times \mid |\text{Nm}(x)| \leq 1\}$. Si $S_g \subset \Theta$ est un domaine fondamental pour l'action à gauche de $\mathcal{O}^\times$ sur Θ alors $S_d = \imath(S_g)$ est un domaine fondamental pour l'action à droite de $\imath(\mathcal{O}^\times) = \mathcal{O}^\times$ sur $\imath(\Theta) = \Theta$. Pour montrer que S_g et S_d ont le même volume il nous suffit de voir que $\imath$ conserve le volume ou encore que son déterminant jacobien vaut ± 1 en tout point x. Or d'après la formule $\imath(y) = \imath(x^{-1}y)\imath(x)$ ce jacobien est le produit des jacobiens des applications $y \mapsto x^{-1}y$ au point x, $\imath$ au point 1 et $z \mapsto zx$ au point 1. Ces jacobiens valent respectivement $\text{Nm}(x^{-1})$, ± 1 et $\text{Nm}(x)$: les première et troisième applications sont linéaires tandis que $\imath$ étant une involution qui fixe 1 sa différentielle en ce point est également une involution donc de déterminant ± 1. Par produit, nous avons le résultat souhaité. □

Faisons encore deux remarques sur cet énoncé. D'une part lorsque la *condition d'Eichler* (voir [R] (34.3) page 293) est satisfaite, c'est-à-dire avec nos notations $(r_1, r_2, d) \neq (0, 0, 2)$, alors le théorème d'Eichler [R] (34.9) montre que $h_{\text{bil}}(\mathcal{O}')$ est indépendant de $\mathcal{O}'$ (car l'isomorphisme de [R] (22.21) préserve la norme d'un idéal). D'autre part, il n'est pas vrai en général que h' est égal au nombre h des classes d'isomorphie d'idéaux à droite non nuls d'un ordre maximal (on rappelle que ce nombre h ne dépend ni de l'ordre ni de l'orientation, voir [R] exercice 27.7 page 232). Pour le vérifier, il nous suffit de trouver deux ordres maximaux $\mathcal{O}_1$ et $\mathcal{O}_2$ tels que $[\mathcal{O}_1^\times : \mathcal{O}_2^\times] \neq 1$. Ceci montrera aussi que $\mathfrak{R}'_{\mathcal{O}}$ n'est pas indépendant de $\mathcal{O}$. Pour donner un exemple explicite, on peux choisir l'algèbre de quaternions $D = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ avec $i^2 = -1$, $j^2 = -11$, $k = ij = -ji$ puis $\mathcal{O}_1 = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}(1+j)/2 \oplus \mathbb{Z}(i+k)/2$ et $\mathcal{O}_2$ un ordre maximal contenant l'élément $\zeta = (2+i+k)/4$. On vérifie alors $\mathcal{O}_1^\times = \{\pm 1, \pm i\}$ donc $\operatorname{Card} \mathcal{O}_1^\times = 4$ tandis que $\zeta^3 = -1$ donc $\operatorname{Card} \mathcal{O}_2^\times \geq 6$.

Nous incluons un exemple qui illustre la dépendance de la hauteur en l'ordre maximal.

EXEMPLE 9.1. Soient $D = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k \subset \mathbb{H}$ et $\mathcal{O}$ l'ordre maximal $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}(1+i+j+k)/2$. Soit $V = \{(a, b) \in D^2 \mid a = ib\}$. Alors

$$\sup_{x \in D^\times} H^{x\mathcal{O}x^{-1},\star}(V) = +\infty$$

où $\star$ est la conjugaison (l'unique involution positive sur $D \otimes \mathbb{R} = \mathbb{H}$).

DÉMONSTRATION. Nous choisissons $x = 1 + 2mj$ pour un entier $m \in \mathbb{Z}$. D'après l'expression matricielle de la hauteur (voir début de la partie 2) nous avons avec $A = (1 \;\; -i) \in \operatorname{Mat}_{12}(D)$

$$H^{x\mathcal{O}x^{-1},\star}(V) = \operatorname{Nm}(AA^\star)^{1/8} [x\mathcal{O}x^{-1} : A(x\mathcal{O}x^{-1})^2]^{-1/4}.$$

Ici $\operatorname{Nm}(AA^\star) = \operatorname{Nm}(1 - i^2) = \operatorname{Nm}(2) = 16$ est bien sûr indépendant de x tandis que

$$\begin{aligned}
[x\mathcal{O}x^{-1} : A(x\mathcal{O}x^{-1})^2] &= [x\mathcal{O}x^{-1} : x\mathcal{O}x^{-1} + ix\mathcal{O}x^{-1}] \\
&= [x\mathcal{O} : x\mathcal{O} + ix\mathcal{O}] \\
&= [\mathcal{O} : \mathcal{O} + x^{-1}ix\mathcal{O}] \\
&= [x^{-1}ix\mathcal{O} : \mathcal{O} \cap x^{-1}ix\mathcal{O}]^{-1}.
\end{aligned}$$

Le calcul montre ensuite $x^{-1}ix = (4mk + (1 - 4m^2)i)/(1 + 4m^2)$. Puisque

l'on a $(\mathbb{Q}i \oplus \mathbb{Q}k) \cap \mathcal{O} = \mathbb{Z}i \oplus \mathbb{Z}k$, ceci entraîne $\{t \in \mathbb{Z} \mid tx^{-1}ix \in \mathcal{O}\} = (1+4m^2)\mathbb{Z}$ donc $[x^{-1}ix\mathcal{O} : \mathcal{O} \cap x^{-1}ix\mathcal{O}] \geq 1+4m^2$ (on peut en fait voir en poussant les calculs que la valeur exacte est $(1+4m^2)^2$). Nous avons finalement $H^{x\mathcal{O}x^{-1},\star}(V) \geq \sqrt{|m|}$, ce qui démontre notre assertion. □

L'exemple suivant nous permet de corriger l'erreur apparaissant dans l'article de Borek [B] page 225, formule (14) (l'erreur est dans la formule précédente : par non-commutativité les éléments $x_i u_i^{-1} y_i^\star u_i$ et $x_i y_i^\star$ n'ont aucune raison d'avoir la même trace) où il affirme que la hauteur est indépendante de l'involution (cette erreur est d'autant plus regrettable que nous avions déjà signalé à l'auteur qu'elle figurait dans sa thèse et lui avions donné un contre-exemple explicite).

Exemple 9.2. Soient D un corps tel que $D \otimes \mathbb{R} \simeq \mathrm{Mat}_{22}(\mathbb{R})$ et $\mathcal{O}$ un ordre maximal quelconque de D. Il existe un sous-espace V de D^2 pour lequel

$$\sup_\star H^{\mathcal{O},\star}(V) = +\infty$$

où $\star$ parcourt les anti-involutions positives sur $D \otimes \mathbb{R}$.

Démonstration. Nous choisissons V de la forme $V = \{(a,b) \in D^2 \mid a = bx\}$ pour $x \in D$ à choisir. Vu l'expression matricielle de la hauteur, il suffit de montrer que l'on a $\sup_\star \mathrm{Nm}(1+xx^\star) = +\infty$. D'après la description des involutions positives (voir lemme 1.1 de [LR]), ceci s'écrit $\sup_{A \in \mathcal{H}_2^{>0}(\mathbb{R})} \det(I + MA\,{}^tMA^{-1}) = +\infty$ si M est la matrice image de x dans $D \otimes \mathbb{R}$ identifié à $\mathrm{Mat}_{22}(\mathbb{R})$. Choisissons

$$A_m = \begin{pmatrix} 1+m & 1 \\ 1 & 1 \end{pmatrix} \in \mathcal{H}_2^{>0}(\mathbb{R})$$

où m est un entier naturel non nul. Dans ce cas, $\det(I + MA_m\,{}^tMA_m^{-1})$ s'écrit $P_{-2}m^{-2} + P_{-1}m^{-1} + P_0 + P_1 m + P_2 m^2$ où les P_i sont des polynômes en les coefficients de M. Nous avons

$$P_2 = \det\left(M\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}{}^tM\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right) = 0$$

tandis que le polynôme P_1 n'est pas identiquement nul comme le montre l'égalité

$$\det\left(I + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} A_m \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} A_m^{-1}\right) = m + 3 + \frac{1}{m}.$$

Par conséquent, il existe $x \in D$ tel que pour la matrice M correspondante on ait $P_1 \neq 0$. Pour ce choix de x nous avons bien $\sup_{m\geq 1} \det(I + MA_m\, {}^t\!MA_M^{-1}) = +\infty$. □

Nous vérifions maintenant que l'entier w et la fonction de comptage dépendent bien de l'involution.

EXEMPLE 9.3. Soient D le corps des quaternions $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ avec $i^2 = -1$, $j^2 = 3$ et $ij = -ji = k$, $\mathcal{O}$ un ordre maximal contenant i et $\star$ l'involution positive de $D \otimes \mathbb{R}$ fixant j et k. On a $w_{\mathcal{O},\star} \geq 4$ et il existe une involution $\star'$ et un réel H avec

$$w_{\mathcal{O},\star'} = 2 \qquad et \qquad \mathcal{N}_{\mathrm{gche}}^{\mathcal{O},\star'}(2,1,H) \neq \mathcal{N}_{\mathrm{gche}}^{\mathcal{O},\star}(2,1,H).$$

DÉMONSTRATION. Nous avons $-ji = k = k^\star = (ij)^\star = j^\star i^\star = ji^\star$ d'où $i^\star = -i$ puis $ii^\star = 1$. Ainsi le groupe $G = \{x \in \mathcal{O} \mid xx^\star = 1\}$ contient ± 1 et $\pm i$ d'où $w_{\mathcal{O},\star} \geq 4$ (il y a en fait égalité). Identifions maintenant $D \otimes \mathbb{R}$ avec $\mathrm{Mat}_{22}(\mathbb{R})$ en envoyant i sur $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et j sur $\begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{pmatrix}$. Avec cette convention $\star$ correspond à la transposition. Nous définissons $\star'$ par $M \mapsto \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} {}^t\!M \begin{pmatrix} \pi^{-1} & 0 \\ 0 & \pi \end{pmatrix}$. Les éléments x de D tels que $xx^{\star'} = 1$ s'identifient à des matrices $M \in \mathrm{Mat}_{22}(\mathbb{Q}(\sqrt{3}))$ vérifiant $M \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix} {}^t\!M = \begin{pmatrix} \pi & 0 \\ 0 & \pi^{-1} \end{pmatrix}$. Par transcendance de π ceci entraîne $M \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} {}^t\!M = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $M \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} {}^t\!M = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. On en déduit $M\, {}^t\!M = I$ puis que M commute avec toute matrice diagonale donc est diagonale puis $M = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. En particulier, comme $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ correspond à $j/\sqrt{3} \notin D$, on a $\{x \in \mathcal{O} \mid xx^{\star'} = 1\} = \{1, -1\}$ et $w_{\mathcal{O},\star'} = 2$. Considérons ensuite $V = \{(x, y) \in D^2 \mid x = iy\}$. En calculant matriciellement comme dans les exemples précédents, on trouve facilement $H^{\mathcal{O},\star'}(V) = \sqrt{\pi + \pi^{-1}}$. D'un autre côté, pour tout sous-espace W on a $H^{\mathcal{O},\star}(W) \in \overline{\mathbb{Q}}$ donc $H^{\mathcal{O},\star}(W) \neq \sqrt{\pi + \pi^{-1}}$. Par finitude, il existe un réel $\varepsilon > 0$ avec $\mathcal{N}_{\mathrm{gche}}^{\mathcal{O},\star}(2,1,\sqrt{\pi+\pi^{-1}} - \varepsilon) = \mathcal{N}_{\mathrm{gche}}^{\mathcal{O},\star}(2,1,\sqrt{\pi+\pi^{-1}})$ tandis que $\mathcal{N}_{\mathrm{gche}}^{\mathcal{O},\star'}(2,1,\sqrt{\pi+\pi^{-1}} - \varepsilon) < \mathcal{N}_{\mathrm{gche}}^{\mathcal{O},\star'}(2,1,\sqrt{\pi+\pi^{-1}})$. On en déduit le résultat souhaité avec $H = \sqrt{\pi + \pi^{-1}}$ ou $H = \sqrt{\pi + \pi^{-1}} - \varepsilon$. □

Terminons nos exemples en montrant que le nombre de sous-espaces à gauche n'est pas en général égal au nombre de sous-espaces à droite. Pour cela, nous devons chercher au-delà des corps de quaternions (pour lesquels $D \simeq D^{\mathrm{op}}$).

EXEMPLE 9.4. Soient D un corps tel que $D \otimes \mathbb{R} \simeq \mathrm{Mat}_{33}(\mathbb{R})$ et $\mathcal{O}$ un ordre maximal de D. Il existe une involution $\star$ et un réel H tels que

$$\mathcal{N}^{\mathcal{O},\star}_{\mathrm{gche}}(3,2,H) \neq \mathcal{N}^{\mathcal{O},\star}_{\mathrm{dte}}(3,2,H).$$

DÉMONSTRATION. Nous pouvons choisir l'isomorphisme $D \otimes \mathbb{R} \simeq \mathrm{Mat}_{33}(\mathbb{R})$ de sorte que l'image de D soit contenue dans $\mathrm{Mat}_{33}(\overline{\mathbb{Q}})$ (car il existe un corps de nombres K tel que $D \otimes K \simeq \mathrm{Mat}_{33}(K)$). Nous identifions $a \in D$ à son image $(a_{ij})_{1\leq i,j\leq 3} \in \mathrm{Mat}_{33}(\overline{\mathbb{Q}})$. Nous définissons $\star$ par la formule $M^\star = N\,{}^tMN^{-1}$ où

$$N = \begin{pmatrix} \pi & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{H}_3^{>0}(\mathbb{R}).$$

Pour $a, b, c \in D$ non tous nuls, nous considérons les sous-espaces $V = \{(x,y,z) \in D^3 \mid ax + by + cz = 0\}$ (à droite) et $W = \{(x,y,z) \in D^3 \mid xa + yb + zc = 0\}$ (à gauche). Tous les sous-espaces de D^3 de dimension 2 de D^3 sont obtenus ainsi. Pour la hauteur nous avons

$$H^{\mathcal{O},\star}(V) = [\mathcal{O} : a\mathcal{O} + b\mathcal{O} + c\mathcal{O}]^{-1/9}\mathrm{Nm}(aa^\star + bb^\star + cc^\star)^{1/18}.$$

Ici $[\mathcal{O} : a\mathcal{O} + b\mathcal{O} + c\mathcal{O}] \in \mathbb{Q}^\times$ et $\mathrm{Nm}(aa^\star + bb^\star + cc^\star) = \det(aa^\star + bb^\star + cc^\star)^3$ dans l'identification $D \otimes \mathbb{R} = \mathrm{Mat}_{33}(\mathbb{R})$. Ainsi $H^{\mathcal{O},\star}(V)^6 \in \overline{\mathbb{Q}}^\times \cdot \det(aa^\star + bb^\star + cc^\star)$. De la même façon, nous trouvons $H^{\mathcal{O},\star}(W)^6 \in \overline{\mathbb{Q}}^\times \cdot \det(a^\star a + b^\star b + c^\star c)$. Maintenant nous avons

$$\det(a^\star a + b^\star b + c^\star c) = \pi\det({}^taN^{-1}a + {}^tbN^{-1}b + {}^tcN^{-1}c) \in \pi\overline{\mathbb{Q}}[\pi^{-1}]$$

tandis que dans l'expression

$$\det(aa^\star + bb^\star + cc^\star) = \pi^{-1}\det(aN\,{}^ta + bN\,{}^tb + cN\,{}^tc) \in \pi^{-1}\overline{\mathbb{Q}}[\pi]$$

le coefficient de π^2 vaut

$$\det\left(a\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}{}^ta + b\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}{}^tb + c\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}{}^tc\right) = \begin{vmatrix} a_{11} & b_{11} & c_{11} \\ a_{21} & b_{21} & c_{21} \\ a_{31} & b_{31} & c_{31} \end{vmatrix}^2.$$

Il est facile de trouver a, b, c dans D tels que ce déterminant soit non nul puisque D contient une base de $\mathrm{Mat}_{33}(\mathbb{R})$ sur $\mathbb{R}$. Dans ce cas, on a donc par

transcendance $\det(aa^\star + bb^\star + cc^\star) \notin \pi\overline{\mathbb{Q}}[\pi^{-1}]$. Cela nous donne un espace à droite V fixé tel que pour tout sous-espace à gauche W on ait $H^{\mathcal{O},\star}(W) \neq H^{\mathcal{O},\star}(V)$. On en déduit alors l'énoncé avec $H = H^{\mathcal{O},\star}(V)$ ou $H = H^{\mathcal{O},\star}(V) - \varepsilon$ pour $\varepsilon > 0$ assez petit en raisonnant comme dans la démonstration précédente. □

Nous terminons par une étude des variations du paramètre ρ.

Démonstration de la proposition 1.3. Si $x \in (D \otimes \mathbb{R})^\times$, $u \in \mathcal{O}^\times$ et $t \in \mathbb{R}$ on a $(tux)^{-1}\mathcal{O}(tux) = x^{-1}\mathcal{O}x$ donc pour démontrer $\rho_{x^{-1}\mathcal{O}x,\star} \leq \rho^n_{\mathcal{O},\star}$, nous pouvons supposer $x \in F_{\mathcal{O},\star} = \{z \in (D \otimes \mathbb{R})^\times \mid \forall u \in \mathcal{O}^\times \ |z| \leq |uz|\}$ et $|\mathrm{Nm}(x)| = 1$. Si $y \in F^{\leq 1}_{x^{-1}\mathcal{O}x,\star}$ il existe $u \in \mathcal{O}^\times$ avec $uxy \in F^{\leq 1}_{\mathcal{O},\star}$ donc

$$|y| \leq |x^{-1}ux \cdot y| \leq |x^{-1}| \cdot |uxy| \leq |x^{-1}|\rho_{\mathcal{O},\star} \leq |x|^{n-1}\rho_{\mathcal{O},\star} \leq \rho^n_{\mathcal{O},\star}$$

ce qui montre la relation voulue. Considérons maintenant une autre involution positive $\star'$. Par le théorème de Skolem-Noether, il existe $y \in (D \otimes \mathbb{R})^\times$ tel que $z^{\star'} = yz^\star y^{-1}$ pour tout $z \in D \otimes \mathbb{R}$. Dans la description de [LR, lemme 1.1] l'élément y correspond à des matrices définies positives donc s'écrit $y = xx^\star$ pour un $x \in (D \otimes \mathbb{R})^\times$. Par suite $\mathrm{Tr}(zz^{\star'}) = \mathrm{Tr}((x^{-1}zx)(x^{-1}zx)^\star) = |f(z)|^2$ si nous notons $f(z) = x^{-1}zx$. Ainsi, parce que f est un automorphisme du groupe $(D \otimes \mathbb{R})^\times$ préservant la fonction Nm, nous avons

$$\begin{aligned}\rho_{\mathcal{O},\star'} &= \sup\{|f(z)| \mid z \in (D \otimes \mathbb{R})^\times,\ |\mathrm{Nm}(z)| \leq 1,\ |f(z)| \leq |f(u)f(z)|\}\\ &= \sup\{|z| \mid z \in (D \otimes \mathbb{R})^\times,\ |\mathrm{Nm}(z)| \leq 1,\ |z| \leq |f(u)z|\}\\ &= \rho_{f(\mathcal{O}),\star}.\end{aligned}$$

Comme $f(\mathcal{O}) = x^{-1}\mathcal{O}x$, la première partie de la démonstration entraîne bien $\rho_{\mathcal{O},\star'} \leq \rho^n_{\mathcal{O},\star}$. Enfin $\rho_{\mathcal{O}^{\mathrm{op}},\star^{\mathrm{op}}}$ est le maximum de la fonction $|z|\,|\mathrm{Nm}(z)|^{-1/n}$ sur le domaine $\{z \in (D \otimes \mathbb{R})^\times \mid \forall u \in \mathcal{O}^\times \ |z| \leq |zu|\}$. Si z appartient à cet ensemble, nous choisissons $u \in \mathcal{O}^\times$ tel que $uz^{-1} \in F_{\mathcal{O},\star}$ puis nous majorons

$$\frac{|z|}{|\mathrm{Nm}(z)|^{1/n}} \leq \frac{|zu^{-1}|}{|\mathrm{Nm}(z)|^{1/n}} \leq \frac{|uz^{-1}|^{n-1}}{|\mathrm{Nm}(z)|^{1/n}|\mathrm{Nm}(uz^{-1})|} = \left(\frac{|uz^{-1}|}{|\mathrm{Nm}(uz^{-1})|^{1/n}}\right)^{n-1}$$

et cette dernière quantité est inférieure à $\rho^{n-1}_{\mathcal{O},\star}$. Ceci termine la preuve des inégalités de l'énoncé. Elles permettent de contrôler explicitement tous les ρ obtenus pour un ordre dans une classe de conjugaison donnée et une involution quelconque à partir de l'un d'entre eux. On déduit enfin de la finitude du nombre de classes de conjugaison que la famille de tous les ρ est bornée. □

Pour être complet nous donnons une majoration de ρ dans le cas commutatif.

LEMME 9.2. *Si D est commutatif alors* $\log\rho \leq n^n(\log 3n)^{3n}\mathrm{Reg}_D$.

DÉMONSTRATION. Comme D est un corps de nombres, on sait que si l'on note $\ell\colon D^\times \to \mathbb{R}^{r_1+r_2}$ l'application définie par $\ell(\varepsilon) = (n_v \log|\varepsilon|_v)_{v|\infty}$ où $n_v = [D_v : \mathbb{R}]$ pour une place infinie v de D alors $\ell(\mathcal{O}_D^\times)$ est un réseau de $\left\{z \in \mathbb{R}^{r_1+r_2} \mid \sum_{v|\infty} z_v = 0\right\}$ dont le covolume est $\sqrt{r_1+r_2}\,\mathrm{Reg}_D$ lorsque l'on munit $\mathbb{R}^{r_1+r_2}$ de la norme euclidienne $||\cdot||$ usuelle (voir [W, partie 6]). La hauteur logarithmique absolue h d'une unité $\varepsilon \in \mathcal{O}_D^\times$ vérifie

$$2\sqrt{n}\,h(\varepsilon) = \frac{2}{\sqrt{n}} \sum_{v|\infty} n_v \log\max(1, |\varepsilon|_v) = \frac{1}{\sqrt{n}} \sum_{v|\infty} n_v |\log|\varepsilon|_v| \leq ||\ell(\varepsilon)||$$

par Cauchy-Schwarz tandis que pour la norme $|\cdot|$ sur $D \otimes \mathbb{R} \simeq \prod_{v|\infty} D_v$ utilisée dans tout le texte nous avons

$$|\varepsilon| = \left(\sum_{v|\infty} n_v |\varepsilon|_v^2\right)^{1/2} \leq \sqrt{n}\exp(||\ell(\varepsilon)||).$$

Si nous notons $r = r_1 + r_2 - 1$ le rang du réseau $\ell(\mathcal{O}_D^\times)$ et $\mu_1, \ldots, \mu_r$ ses minima successifs alors le théorème de Minkowski donne (comme dans le lemme 6.1)

$$\mu_r \leq \mu_1^{1-r} r^{r/2} \sqrt{r+1}\,\mathrm{Reg}_D,$$

tout au moins si $r \geq 1$ ce que nous supposons temporairement. Par ce qui précède, si h_0 est la hauteur minimale d'une unité de $\mathcal{O}_D$ qui n'est pas une racine de l'unité, alors $\mu_1 \geq 2\sqrt{n}\,h_0$. D'autre part, par définition même des minima, il existe un sous-groupe d'indice fini de $\mathcal{O}_D^\times$ engendré par des unités $\varepsilon_1, \ldots, \varepsilon_r$ telles que $||\ell(\varepsilon_i)|| \leq \mu_r$. Maintenant si $x \in D \otimes \mathbb{R}$ vérifie $0 < |\mathrm{Nm}(x)| \leq 1$ alors il existe $t \in\,]0,1]$ et $\alpha_1, \ldots, \alpha_r \in\,]-1/2, 1/2]$ puis $u \in \mathcal{O}_D^\times$ tels que $\ell(t^{-1}ux) = \alpha_1\ell(\varepsilon_1) + \cdots + \alpha_r\ell(\varepsilon_r)$ d'où $||\ell(t^{-1}ux)|| \leq r\mu_r/2$. Si de plus $x \in F$ (voir partie 6) nous avons

$$|x| \leq |ux| \leq |t^{-1}ux| \leq \sqrt{n}\exp(r\mu_r/2).$$

Cette dernière borne fournit donc un majorant de ρ d'où

$$\log\rho \leq \frac{1}{2}\log n + \frac{r^{1+r/2}\sqrt{r+1}}{2(2\sqrt{n}\,h_0)^{r-1}}\,\mathrm{Reg}_D.$$

Pour terminer le calcul (toujours lorsque $r \geq 1$), nous minorons le régulateur *via* $\mu_1^r \leq r^{r/2}\sqrt{r+1}\mathrm{Reg}_D$ pour obtenir

$$\log \rho \leq \frac{r^{r/2}\sqrt{r+1}}{2(2\sqrt{n}\,h_0)^r}(\log n + 2r\sqrt{n}\,h_0)\mathrm{Reg}_D$$

et nous utilisons la minoration de Voutier [V, corollaire 2] $h_0 \geq 2n^{-1}(\log 3n)^{-3}$ (version explicite du résultat de Dobrowolski) qui entraîne le lemme après calculs (avec $1 \leq r \leq n-1$). Dans les cas restants où $r = 0$, on a ou bien $n = 2$ (D corps quadratique imaginaire) et $\rho = \sqrt{2}$ ou bien $n = 1$ ($D = \mathbb{Q}$) et $\rho = 1$. □

RÉFÉRENCES

[B] T. Borek, *Arakelov theory of noncommutative arithmetic curves*. J. Number Theory, **131** (2011), pp. 212–227.

[Ca] J. W. S. Cassels, *An introduction to the geometry of numbers.* Springer, Berlin, 1959.

[Ch] H. Chaix, *Démonstration élémentaire d'un théorème de Van der Corput.* C. R. A. S. **275** (1972), pp. 883–885.

[CG] C. Christensen - W. Gubler, *Der relative Satz von Schanuel.* Manuscripta Math, **126** (2008), pp. 505–525.

[Da] H. Davenport, *On a principle of Lipschitz*. J. London Math. Soc. **26** (1951), pp. 179–183.

[De] M. Deuring, *Algebren.* Springer, Berlin, 1968.

[FMT] J. Franke - Y. Manin - Y. Tschinkel, *Rational points of bounded height on Fano varieties*. Invent. Math. **95** (1989), pp. 421–435. Erratum *ibid.* **102** (1990), p. 463.

[FP] D. Farenick - B. Pidkowich, *The spectral theorem in quaternions*. Lin. Alg. Appl. **371** (2003), pp. 75–102.

[G] C. Gasbarri, *On the number of points of bounded height on arithmetic projective spaces*. Manuscripta Math. **98** (1999), pp. 453–475.

[J] N. Jacobson, *Basic Algebra I.* Freeman, San Francisco, 1974.

[La] S. Lang, *Algebraic number theory.* Addison-Wesley, Reading, Mass. 1970.

[Le] A. Leutbecher, *Zahlentheorie.* Springer, Berlin, 1996.

[LR] C. Liebendörfer - G. Rémond, *Hauteurs de sous-espaces sur les corps non commutatifs*. Math. Z. **255** (2007), pp. 549–577.

[MV] D. Masser - J. Vaaler, *Counting algebraic numbers with large height II*. Trans. Amer. Math. Soc. **359** (2007), pp. 427–445.

[N] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers.* Springer, Berlin, 1990.

[P] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*. Duke Math. J. **79** (1995), pp. 101–218.

[R] I. Reiner, *Maximal orders.* Academic Press, London, 1975.

[Scha] S. H. SCHANUEL, *Heights in number fields*. Bull. Soc. Math. Fr. **107** (1979), pp. 433–449.

[Schm] W. SCHMIDT, *The distribution of sublattices of* $\mathbb{Z}^m$. Monatsh. Math. **125** (1998), pp. 37–81.

[St] R. P. STANLEY, *Enumerative Combinatorics.* Volume 1, Cambridge University Press, 1997.

[T1] J. L. THUNDER, *An asymptotic estimate for heights of algebraic subspaces*. Trans. Amer. Math. Soc. **331** (1992), pp. 395–424.

[T2] J. L. THUNDER, *The number of solutions of bounded height to a system of linear equations*. J. Number Theory. **43** (1993), pp. 228–250.

[V] P. VOUTIER, *An effective lower bound for the height of algebraic numbers*. Acta Arithm. **74** (1996), pp. 81–95.

[W] M. WIDMER, *Counting primitive points of bounded height*. Trans. Amer. Math. Soc. **362** (2010), pp. 4793–4829.

SOUTIEN. Les auteurs ont reçu un soutien financier partiel dans le cadre des projets SNF 200020-113199 (Ch. Z.-L.) et ANR 2010 BLAN-0115-01 (G. R.).

Manoscritto pervenuto in redazione il 20 Settembre 2012.