Existence et équidistribution des matrices de dénominateur n dans les groupes unitaires et orthogonaux

Antonin Guilloux

EXISTENCE ET ÉQUIDISTRIBUTION DES MATRICES DE DÉNOMINATEUR n DANS LES GROUPES UNITAIRES ET ORTHOGONAUX

par

Antonin Guilloux

Abstract. — Let $\mathbf{G}$ be a simply-connected $\mathbb{Q}$-quasisimple and $\mathbb{R}$-anisotropic algebraic $\mathbb{Q}$-group. Let $\mathbb{A}^f$ be the finite part of the adele $\mathbb{A}$ of $\mathbb{Q}$. Let (H_n) be a sequence of bounded subset of $\mathbf{G}(\mathbb{A}^f)$ which are bi-invariant by a compact open subgroup of $\mathbf{G}(\mathbb{A}^f)$. Let Γ_n be the projection in $\mathbf{G}(\mathbb{R})$ of the sets $\mathbf{G}(\mathbb{Q})\cap(\mathbf{G}(\mathbb{R})\times H_n)$. Suppose that the volume of the compacts $\mathbf{G}(\mathbb{R})\times H_n$ tends to ∞ with n.

We prove the equidistribution in $\mathbf{G}(\mathbb{R})$ of the Γ_n with respect to the Haar probability on $\mathbf{G}(\mathbb{R})$. Our strategy is to use a mixing result for the action of $\mathbf{G}(\mathbb{A})$ on the space $L^2(\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{Q}))$.

As an application, we are able to study the existence and the repartition of rational unitary matrices having a given denominator. We prove a local-global principle for this problem and the equirepartition of the sets of denominator n-matrices when they are not empty.

In a second time, we study the more complicated case of non simply-connected group applying it to quadratic forms.

1. Introduction

La théorie des formes quadratiques définies positives à coefficients entiers répond de manière satisfaisante aux deux questions suivantes :

– À quelles conditions une forme quadratique donnée représente un entier n (c'est à dire qu'il existe un vecteur entier de norme $\sqrt{n}$) ?
– Quand un entier n est représenté, quelle est la répartition des vecteurs entiers sur l'ellipsoïde des vecteurs de norme $\sqrt{n}$?

Citons les résultats les plus simples, qui sont obtenus quand le rang de la forme quadratique est plus grand que 5 :

Théorème 1.1 **(W. Tartakowsky ([15]), C. Pommerenke ([13]))**
Soit q une forme quadratique définie positive de rang $k \geq 5$ à coefficients entiers. Alors il existe un entier N_0 tel que pour tout $n \geq N_0$, on a l'équivalence entre les deux assertions suivantes :

1. *Pour tout p premier, n appartient à $q(\mathbb{Z}_p^k)$*

2. *n appartient à $q(\mathbb{Z}^k)$*

De plus, l'ensemble des vecteurs v de $\mathbb{Z}^k$ vérifiant $q(v) = n$ s'équirépartit sur l'ellipsoïde $q(x) = n$ quand n tend vers l'infini.

Nous reviendrons dans la partie 5 sur ce théorème et sur le cas des formes de petit rang. Nous nous intéressons dans ce chapitre à un analogue dans le cadre des groupes unitaires ou orthogonaux de ce résultat. Présentons dans cette introduction nos résultats dans le cas unitaire (pour le cas orthogonal, on renvoie à nouveau à la partie 5). Soit pour $k \geq 2$, $H \in \mathcal{M}(k, \mathbb{Z}[i])$ une matrice hermitienne définie positive, h la forme hermitienne associée. Définissons le dénominateur d'une matrice à coefficients dans $\mathbb{Q}[i]$:

Définition 1.2. — Soient k un entier et A un matrice de $\mathcal{M}(k, \mathbb{Q}[i])$.
Le dénominateur d de A est défini comme le plus petit entier $d \in \mathbb{N}^*$ tel que dA soit une matrice de $\mathcal{M}(k, \mathbb{Z}[i])$.

Nous voulons comprendre le comportement de l'ensemble des matrices de $SU(h, \mathbb{Q})$ de dénominateur n : à quelles conditions cet ensemble est non vide, et dans ce cas, quelle est sa répartition dans le groupe $SU(h, \mathbb{R})$. On peut reformuler le problème de la façon suivante : A désigne un des anneaux $\mathbb{Z}$ ou $\mathbb{Z}_p$ pour p premier, et $A_i = \mathbb{Z}[i] \otimes_{\mathbb{Z}} A$.
On note alors, pour tout entier n, $\mathcal{T}(n, H, A)$ l'ensemble des matrices $M \in \mathcal{M}(k, A_i)$ de déterminant n^k telles que :
– les coefficients de M sont premiers entre eux,
– M est solution de l'équation (E_n) : $M^* H M = n^2 H$.

Dans le cas $A = \mathbb{Z}$ et pour tout entier n, une matrice M est dans $\mathcal{T}(n, H, \mathbb{Z})$ si et seulement si la matrice $\frac{1}{n}M$ est un élément de $SU(h, \mathbb{Q})$ de dénominateur n. De même dans le cas $A = \mathbb{Z}_p$, une matrice M est dans $\mathcal{T}(n, H, \mathbb{Z}_p)$ si et seulement si la matrice $\frac{1}{n}M$ est un élément de $SU(h, \mathbb{Q}_p)$ tel que le sup de la norme p-adique des coefficients soitt la norme p-adique de $\frac{1}{n}$.
On note enfin $\mathcal{U}(H, A)$ l'ensemble des $n \in \mathbb{Z}$ tels qu'il existe $M \in \mathcal{T}(n, H, A)$, et $\mathcal{U}_l(H) = \bigcap_{p \text{ premier}} \mathcal{U}(H, \mathbb{Z}_p)$.
Bien sûr, pour qu'il existe des matrices de dénominateur n dans $SU(h, \mathbb{Q})$, il faut que n soit dans $\mathcal{U}(H, \mathbb{Z})$, et donc il faut que n soit dans $\mathcal{U}_l(H)$.
Le théorème suivant montre que pour n suffisamment grand, c'est la seule condition :

Théorème 1.3. — *Soient $k \geq 2$, $H \in \mathcal{M}(k, \mathbb{Z}[i])$ une matrice hermitienne définie positive. Alors il existe $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0$, les deux assertions suivantes sont équivalentes :*

1. *n appartient à $\mathcal{U}_l(H)$*
2. *n appartient à $\mathcal{U}(H, \mathbb{Z})$*

La méthode pour prouver ce théorème est de prouver un résultat plus fort, à savoir l'équirépartition dans $SU(q,\mathbb{R})$ de l'ensemble Γ_n des matrices de dénominateur n, quand n tend vers l'infini dans $\mathcal{U}_l(H)$. Voilà l'énoncé :

Théorème 1.4. — *Soient $k \geq 2$, $H \in \mathcal{M}(k,\mathbb{Z}[i])$ une matrice hermitienne définie positive et h la forme hermitienne associée. Notons μ la probabilité de Haar sur $SU(h,\mathbb{R})$.*

Pour tout entier n, soit Γ_n l'ensemble des $\frac{1}{n}M$ pour $M \in \mathcal{T}(n,H,\mathbb{Z})$.

Alors quand n tend vers l'infini dans $\mathcal{U}_l(H)$, les Γ_n s'équirépartissent dans $SU(h,\mathbb{R})$, c'est-à-dire :

$$\frac{1}{Card(\Gamma_n)} \sum_{\gamma \in \Gamma_n} \delta_\gamma \xrightarrow[n \in \mathcal{U}_l(H)]{n \to \infty} \mu \ .$$

Remarque 1.5. — Pour vérifier la condition $n \in \mathcal{U}_l(H)$, il suffit de vérifier que l'ensemble $\mathcal{T}(n,H,\mathbb{Z}_p)$ est non vide uniquement pour les nombres premiers p divisant n. En effet, si p ne divise pas n, la matrice $n \cdot Id$ appartient à $\mathcal{T}(n,H,\mathbb{Z}_p)$.

La question de la répartition des points rationnels de dénominateur n dans le groupe des points réels d'un groupe algébrique $\mathbf{G}$ défini sur $\mathbb{Q}$ quand n tend vers l'infini a déjà été étudiée par plusieurs auteurs.

Dans le cas où $\mathbf{G}(\mathbb{R})$ est non-compact, A. Eskin et H. Oh (Cf [**9**]) ont montré que ces points étaient équidistribués suivant la mesure de Haar de $\mathbf{G}(\mathbb{R})$. Pour cela ils utilisent la présence de sous-groupes unipotents dans $\mathbf{G}(\mathbb{R})$ et concluent grâce à des théorèmes de Ratner et Dani-Margulis. Cependant, dans le cas où $\mathbf{G}(\mathbb{R})$ est compact, il n'y a pas d'unipotents dans $\mathbf{G}(\mathbb{R})$, donc on ne peut pas appliquer ces théorèmes.

Une autre méthode pour montrer des théorèmes d'équirépartition est d'utiliser le mélange. On renvoie à l'article d'A. Eskin et C. McMullen ([**8**]) pour une présentation très claire de cette méthode. Pour pouvoir l'utiliser dans notre cas, il faut disposer d'un résultat de décroissance des coefficients de l'action de $\mathbf{G}$ sur $L^2\left(\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{Q})\right)$ (on rappelle que, dans ce cadre $\mathbf{G}(\mathbb{Q})$ est un réseau du groupe des points sur les adèles $\mathbf{G}(\mathbb{A})$). De tels résultats sont prouvés dans l'article de L. Clozel, H. Oh et E. Ullmo ([**5**]), et complétés dans un article de L. Clozel ([**4**]), puis de A. Gorodnik, F. Maucourant et H. Oh ([**10**]) où une décroissance des coefficients de l'action de $\mathbf{G}$ sur $L^2\left(\mathbf{G}(\mathbb{A})/\mathbf{G}(\mathbb{Q})\right)$ est montrée sous les hypothèses que $\mathbf{G}$ est un groupe algébrique défini sur un corps de nombres, connexe et absolument quasi-simple (on renvoie au théorème 2.1 pour l'énoncé exact).

C'est ce dernier résultat que nous utiliserons. Commençons par rappeler quelques résultats sur les groupes algébriques et leurs réseaux arithmétiques, ce qui permettra de fixer le cadre de la preuve.

Groupes algébriques et réseaux arithmétiques. — Nous définissons dans cette partie les notations dont nous nous servirons dans ce chapitre. Il nous faudra pour cela faire appel à des résultats sur les groupes algébriques et adéliques. Pour leur preuve, nous renvoyons le lecteur d'une part à l'article [**16**] de J. Tits (et ses références) pour les résultats

spécifiques aux points sur $\mathbb{Q}_p$ d'un groupe algébrique, et d'autre part au livre de V. Platonov et A. Rapinchuk (Cf [**12**]) pour les propriétés adéliques.

Fixons une fois pour toutes un groupe $\mathbf{G}$ défini sur un corps de nombres K, connexe, quasi-K-simple. Soit $\mathcal{V}$ l'ensemble des places de K. On note $\mathbb{A}$ (resp. $\mathbb{A}^f$, resp. $\mathbb{A}^\infty$) l'anneau des adèles de K (resp. des adèles finies, resp. infinies). On note de plus $G = \mathbf{G}(\mathbb{A})$, et $G^f = \mathbf{G}(\mathbb{A}^f)$, et $G^\infty = \mathbf{G}(\mathbb{A}^\infty)$. On supposera toujours que G^∞ est compact.

Nous disposons alors du sous-groupe $\mathbf{G}(K)$. On rappelle, d'après [**12**], que c'est un réseau de G, qu'il est irréductible car $\mathbf{G}$ est quasi-K-simple ; et enfin qu'il est cocompact car $\mathbf{G}$ est K-anisotrope.

On appelle réseau arithmétique de G tout sous-groupe Γ tel que $\Gamma \cap \mathbf{G}(K)$ est d'indice fini dans Γ et dans $\mathbf{G}(K)$. D'après ce qui précède, tout réseau arithmétique Γ de G est irréductible et cocompact. On se fixe un tel réseau Γ, ainsi qu'un sous-groupe compact ouvert U de G^f.

On dira qu'une suite d'éléments (g_n) de G tend vers l'infini si pour tout compact C de G, pour n suffisament grand, g_n n'appartient pas à C.

Fixons les dernières notations : on note τ^∞ la projection de G sur G^∞, τ^f la projection de G sur G^f, et enfin π la projection de G sur G/Γ. De plus on note λ la mesure de Haar sur G^f normalisée par $\lambda(U) = 1$; μ la probabilité de Haar sur G^∞. On note enfin m la probabilité sur G/Γ localement proportionnelle à $\mu \otimes \lambda$ et on l'appelle probabilité de Haar sur G/Γ. Le diagramme ci-dessous résume ces données :

$$\begin{array}{ccccc} & & G\ ,\ \mu\otimes\lambda & & \\ & \tau^\infty \swarrow & \tau^f \downarrow & \searrow \pi & \\ G^\infty = G^f\backslash G\ ,\ \mu & & G^f\ ,\ \lambda & & G/\Gamma\ ,\ m \end{array}$$

Enfin, pour les applications, on supposera toujours fixée une base sur $\mathbb{Z}^k$ et $\mathbb{Z}[i]^k$. Ainsi, nous supposons fixée une fois pour toute l'identification entre formes quadratiques (resp. hermitienne) et matrices symétriques (resp. hermitiennes).

Application de la décroissance des coefficients. — On remarque qu'une matrice est de dénominateur n si et seulement si pour tout nombre premier p, le max de la norme p-adique de ses coefficients est la norme p-adique de $\frac{1}{n}$. Donc on peut réénoncer notre problème comme un problème de répartition dans G^∞ de sous-ensembles de Γ définis par certaines conditions sur leur projection dans G^f. C'est dorénavant sous cet angle que nous travaillerons.

Nous montrons dans ce cadre le résultat d'équirépartition suivant (rappelons que U est un sous-groupe compact ouvert fixé de G^f) : pour une suite d'ensembles $H_n \subset G^f$ bi-U-invariants, notons Γ_n l'ensemble des points de Γ dont la projection dans G^f appartient à H_n. Alors, si le cardinal des Γ_n tend vers l'infini, ils s'équirépartissent dans G^∞ vers la mesure de Haar sur G^∞.

C'est l'objet du théorème suivant :

Théorème 1.6. — *Soit* $\mathbf{G}$ *un* K*-groupe, quasi-*K*-simple, connexe avec* $G^\infty = \mathbf{G}(\mathbb{A}^\infty)$ *compact. Soient* U *un sous-groupe compact ouvert de* $G^f = \mathbf{G}(\mathbb{A}^f)$ *et* (H_n) *une suite de sous-ensembles compacts bi-*U*-invariants de* G^f*.*

Soit Γ *un sous-groupe arithmétique de* $G = \mathbf{G}(\mathbb{A})$ *et* $\Gamma_n = \Gamma \cap (G^\infty \times H_n)$*. Notons* τ^∞ *la projection de* G *sur* G^∞*, et* μ *la probabilité de Haar sur* G^∞*. Pour* g *dans* G*, on note* $\delta_{\tau^\infty(g)}$ *la mesure de Dirac en* $\tau^\infty(g) \in G^\infty$*.*

Supposons que $Card(\Gamma_n)$ *tende vers* $+\infty$*. Alors on a la limite suivante, dans l'espace des probabilités sur* G^∞ *:*

$$\lim_{n\to\infty} \frac{1}{Card(\Gamma_n)} \sum_{\gamma\in\Gamma_n} \delta_{\tau^\infty(\gamma)} = \mu \ .$$

Nous obtiendrons en outre avec le théorème 3.1 un équivalent de $Card(\Gamma_n)$. Ce théorème sera prouvé dans la partie 3. De plus, on notera toujours $G_n = G^\infty \times H_n$.

2. Représentation unitaire et décroissance des coefficients

Nous présentons dans cette partie le théorème de A. Gorodnik, F. Maucourant et H. Oh. Pour cela, il nous faut comprendre la représentation de G dans l'espace $L^2(G/\Gamma)$.

On note $<,>$ le produit scalaire canonique dans $L^2(G/\Gamma)$ et $g.f$ l'action de $g \in G$ sur une fonction f de $L^2(G/\Gamma)$. Considérons l'ensemble des sous-représentations de dimension 1 dans $L^2(G/\Gamma)$; chacune de ces représentations est associée à un caractère unitaire de G, invariant par Γ. Nous noterons $L^2_0(G/\Gamma)$ le sous-espace stable de $L^2(G/\Gamma)$ orthogonal à toutes les sous-représentations de dimension 1. Notons Λ l'ensemble des caractères unitaires de G triviaux sur Γ. Ils forment une base de l'orthogonal de $L^2_0(G/\Gamma)$.

Nous pouvons maintenant citer le théorème de A. Gorodnik, F. Maucourant et H. Oh (Cf **[10]**, théorème 1.13) :

Théorème 2.1. — *Soit* $\mathbf{G}$ *un groupe défini sur un corps de nombres* K*, connexe et absolument quasi-simple. Alors pour toutes fonctions* f *et* h *de* $L^2_0(G/\Gamma)$*, on a :*

$$| < f, g.h > | \xrightarrow{g\to\infty} 0$$

Remarquons que dans **[10]**, le produit scalaire est majoré grâce à une fonction $\bar{\xi}$ construite de manière explicite. Nous n'utiliserons pas ici cette estimée. De plus l'hypothèse d'absolue simplicité de $\mathbf{G}$ n'est pas génante, ainsi que cela avait été noté dans **[10]** : il existe une extension finie L de K, et $\mathbf{H}$ un L-groupe absolument quasi-simple tels que $\mathbf{G}$ est défini comme la restriction des scalaires de L à K de $\mathbf{H}$ (Cf **[1]**, 6.21.ii). A partir de maintenant, nous supposons donc que le groupe $\mathbf{G}$ est absolument quasi-simple.

Pour appliquer ce théorème, nous devons comprendre comment s'écrit une fonction dans la décomposition de $L^2(G/\Gamma)$ en $L^2_0(G/\Gamma)$ et son orthogonal. Or les fonctions que nous étudierons seront toutes invariantes par le sous-groupe compact ouvert U.

Notons alors Λ_U l'ensemble des caractères unitaires U-invariants de Λ et $G_U = Ker(\Lambda_U)$ l'intersection de tous les $Ker(\chi)$ pour χ appartenant à Λ_U. On dispose alors du lemme suivant, tiré du lemme 3.2 de **[10]** :

Lemme 2.2. — 1. *l'ensemble $UG^\infty\Gamma$ est inclus dans G_U.*

2. *G_U est d'indice fini N_U dans G.*

3. *on a l'égalité $\sum_{\chi\in\Lambda_U} \chi = N_U 1_{G_U}$ (1_{G_U} étant la fonction caractéristique de G_U).*

4. *Si $f \in L^2(G/\Gamma)$ est définie sur $\pi(G_U)$ et est U-invariante, alors on a :*

$$f - \left(\int_{\pi(G_U)} f dm\right) 1_{\pi(G_U)} \in L^2_0(G/\Gamma)$$

Démonstration. — Le premier point est une conséquence de la continuité des caractères, et du fait que G^∞ est connexe car $\mathbf{G}$ est connexe et $\mathbb{R}$-anisotrope. On en déduit le deuxième car, d'après le théorème 5.1 de **[12]**, l'ensemble $G^\infty U\backslash G/\Gamma$ est fini. Enfin le troisième point exprime le fait que les deux groupes abéliens finis G/G_U et Λ_U sont en dualité.

Pour le dernier point : soit $\chi \in \Lambda$. On veut calculer $< f, \chi >$. Dans un premier temps, si U n'est pas dans le noyau de χ, alors ce produit scalaire est nul. Ensuite, si $\chi \in \Lambda_U$, alors $< f, \chi >= \int_{\pi(G_U)} f dm$. □

Nous pouvons maintenant montrer le théorème 1.6.

3. Dualité

Nous allons en réalité montrer un théorème plus précis que le théorème 1.6. En effet, dans les hypothèses de ce théorème, on avait besoin de supposer que $Card(\Gamma_n)$ tend vers l'infini. Cette hypothèse est en pratique difficile à vérifier. Par exemple dans le cadre unitaire décrit dans l'introduction, il faudrait pour appliquer le théorème 1.6 connaître a priori un grand nombre de solutions entières de l'équation (E_n).

Dans le théorème suivant, cette hypothèse est remplacée par l'hypothèse que les compacts $G_n \cap G_U$ sont deux à deux distincts. On remarque que cette hypothèse est à priori plus simple à vérifier, car nous n'avons plus besoin de trouver des solutions entières. Nous reviendrons là-dessus pour les applications dans les parties 4 et 5.

Théorème 3.1. — *Soit $\mathbf{G}$ un K-groupe, quasi-K-simple, connexe avec $G^\infty = \mathbf{G}(\mathbb{A}^\infty)$ compact. Soient U un sous-groupe compact ouvert de $G^f = \mathbf{G}(\mathbb{A}^f)$ et (H_n) une suite de sous-ensembles compacts de G^f bi-U-invariants. On note $G_n = G^\infty \times H_n$ et on suppose que les ensembles $G_n \cap G_U$ sont deux à deux distincts.*

Soit Γ un sous-groupe arithmétique de $G = \mathbf{G}(\mathbb{A})$ et $\Gamma_n = \Gamma \cap (\mathbf{G}(\mathbb{A}^\infty) \times H_n)$. Notons τ^∞ la projection de G sur G^∞, et μ la probabilité de Haar sur G^∞, et λ la mesure de Haar sur G^f qui donne poids 1 à U. Pour g dans G, on note $\delta_{\tau^\infty(g)}$ la mesure de Dirac en $\tau^\infty(g) \in G^\infty$.

Alors on a la limite suivante :

$$lim_{n\to\infty}\frac{\mu\otimes\lambda(G/\Gamma)}{\mu\otimes\lambda(G_n\cap G_U)}\sum_{\gamma\in\Gamma_n}\delta_{\tau^\infty(\gamma)}=\mu$$

Notamment, $Card(\Gamma_n)$ est équivalent à $\frac{\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)}$

Démonstration. — Fixons une fonction φ continue à support compact sur G^∞, ainsi qu'une suite H_n bi-U-invariante. Nous voulons montrer la limite suivante :

$$\lim_{n\to\infty}\frac{\mu\otimes\lambda(G/\Gamma)}{\mu\otimes\lambda(G_n\cap G_U)}\sum_{\gamma\in\Gamma_n}\varphi(\tau^\infty(\gamma))=\int_{G^\infty}\varphi d\mu$$

Pour cela, nous définissons la fonction f sur $\mathbf{G}(\mathbb{A})$ en posant $f(g_\infty,g_f)=\varphi(g_\infty)$. Nous posons ensuite $F_n(g,h)=\sum_{\gamma\in\Gamma}f(g\gamma h^{-1})1_{G_n}(g\gamma h^{-1})$ (1_{G_n} étant la fonction caractéristique de G_n).

On remarque alors que pour tout u_1, u_2 dans U et γ_1, γ_2 dans Γ, on a

$$F_n(u_1g\gamma_1,u_2h\gamma_2)=F_n(g,h)$$

Ainsi F_n est une fonction continue bornée définie sur $(G/\Gamma)^2$, invariante par l'action à gauche de $U\times U$. De plus, on remarque - en notant e l'élément neutre de G - que :

$$F_n(e,e)=\sum_{\gamma\in\Gamma_n}\varphi(\tau^\infty(\gamma))$$

La fonction φ est continue sur le compact G/Γ, elle est donc uniformément continue. Ainsi, soient $\varepsilon>0$ et U_ε un voisinage de l'identité dans G^∞ tels que pour tout u et $v\in U_\varepsilon$, pour tout $g\in G^\infty$, $|\varphi(ugv)-\varphi(g)|\leq\varepsilon$. Notons β la fonction $\frac{1}{\mu(U_\varepsilon)}1_{U_\varepsilon}$ - ici 1_{U_ε} est la fonction caractéristique de U_ε dans G^∞. On pose maintenant :

$$\bar\alpha(g_\infty,g_f)=\beta(g_\infty)1_U(g_f)$$

$$\text{et }\alpha(g)=\mu\otimes\lambda(G/\Gamma)\sum_{\gamma\in\Gamma}\bar\alpha(g\gamma)$$

On voit que α est une fonction dans $L^2(G/\Gamma)$, définie sur $\pi(G_U)$, et d'intégrale par rapport à m égale à 1.

Notons que pour tout $(x,y)\in(G/\Gamma)^2$, si $\alpha(x)\alpha(y)\neq0$, alors x et y s'écrivent $x=uu_\varepsilon\Gamma$ et $y=vv_\varepsilon\Gamma$ avec u_ε et v_ε dans U_ε, et u et v dans U. Ainsi, on a $F_n(x,y)=\sum_{\gamma\in\Gamma}\varphi(u_\varepsilon\gamma v_\varepsilon^{-1})1_{G_n}(u_\varepsilon\gamma v_\varepsilon^{-1})$. On en déduit que dans ce cas on a :

$$|F_n(x,y)-F_n(e,e)|\leq\varepsilon Card(\Gamma\cap G_n)$$

Cela se traduit par l'inégalité :

$$|F_n(e,e)-\int_{G/\Gamma}\int_{G/\Gamma}F_n(x,y)\alpha(x)\alpha(y)dm(x)dm(y)|\leq\varepsilon Card(\Gamma\cap G_n)$$

Pour fixer les notations, fixons X un relevé de G/Γ dans G. On note $\tilde{\alpha}$ le relevé de α : $\tilde{\alpha} = \alpha \circ \pi$, et on note $\tilde{m} = \frac{\mu \otimes \lambda}{\mu \otimes \lambda(X)}$. Enfin notons $I_{n,\varepsilon}$ l'intégrale :

$$I_{n,\varepsilon} = \int_{G/\Gamma} \int_{G/\Gamma} F_n(x,y)\alpha(x)\alpha(y)dm(x)dm(y)$$

On fait alors le calcul suivant :

$$\begin{aligned} I_{n,\varepsilon} &= \int_X \int_X F_n(x,y)\tilde{\alpha}(x)\tilde{\alpha}(y)d\tilde{m}(x)d\tilde{m}(y) \\ &= \int_X \int_X \sum_{\gamma \in \Gamma} f(x\gamma y^{-1}) 1_{G_n}(x\gamma y^{-1})\tilde{\alpha}(x)\tilde{\alpha}(y)d\tilde{m}(x)d\tilde{m}(y) \end{aligned}$$

On fait pour tout $\gamma \in \Gamma$ le changement de variable $x\gamma = g$, ce qui permet d'obtenir :

$$I_{n,\varepsilon} = \int_G \int_X f(gy^{-1}) 1_{G_n}(gy^{-1})\tilde{\alpha}(g)\tilde{\alpha}(y)d\tilde{m}(g)d\tilde{m}(y)$$

On fait maintenant le changement de variables $h = gy^{-1}$ pour tout $g \in G$. On obtient finalement :

$$I_{n,\varepsilon} = \int_G f(h) 1_{G_n}(h) \int_X \tilde{\alpha}(hy)\tilde{\alpha}(y)d\tilde{m}(y)d\tilde{m}(h)$$

Or, d'après le théorème 2.1 et le lemme 2.2, on sait que l'intégrale $\int_{G/\Gamma} \alpha(hy)\alpha(y)dm(y)$ tend vers 1 quand h tend vers l'infini dans G_U. En outre, si h n'appartient pas à G_U, car on ne peut pas avoir à la fois y et hy qui appartiennent à G_U. Donc dans ce cas l'intégrale $\int_X \tilde{\alpha}(hy)\tilde{\alpha}(y)d\tilde{m}(y)$ est nulle .

Nous avons besoin du lemme suivant, sans doute déjà connu :

Lemme 3.2. — *Soit C_n une suite de compacts bi-U-invariants 2 à 2 distincts de G^f. Alors on a la limite :* $\lim_{n\to\infty} \lambda(C_n) = +\infty$

Démonstration. — Ce lemme est une conséquence de diverses formules de dénombrement du volume d'une double-classe pour la décomposition de Cartan dans un groupe p-adique. On peut trouver de telles formules dans **[2]**, paragraphe 1.5, ou bien **[11]**, 7.3. Nous en donnons une preuve dans la partie 6. □

On en déduit, en posant C_n la projection de $G_n \cap G_U$ sur G^f que $\lambda(C_n) = \mu \otimes \lambda(G_n \cap G_U)$ tend vers l'infini :

$$\mu \otimes \lambda(G_n \cap G_U) \xrightarrow{n\to\infty} \infty$$

Donc on peut continuer le calcul : il existe un compact C de G_U, tel que pour tout $h \in G_U - C$, on a $|\int_{G/\Gamma} \alpha(hy)\alpha(y)dm(y) - 1| \leq \varepsilon$. De plus, par définition de f, on a :

$$\int_G f(h) 1_{G_n}(h) d\tilde{m}(h) = \frac{\mu \otimes \lambda(G_n \cap G_U)}{\mu \otimes \lambda(G/\Gamma)} \int_{G^\infty} \varphi d\mu$$

Et alors, pour n suffisament grand, on a :

$$\begin{aligned}|I_{n,\varepsilon} - \frac{\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)}\int_{G^\infty}\varphi d\mu| &\leq \varepsilon\frac{\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)}\int_{G^\infty}\varphi d\mu + \mu\otimes\lambda(C)\|\varphi\|_\infty\|\tilde{\alpha}\|_\infty^2 \\ &\leq \varepsilon\frac{2\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)}\end{aligned}$$

On en déduit que pour n grand, on a l'inégalité

$$|F_n(e,e) - \frac{\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)}\int_{G^\infty}\varphi d\mu| \leq \left(\frac{2\mu\otimes\lambda(G_n\cap G_U)}{\mu\otimes\lambda(G/\Gamma)} + Card(\Gamma\cap G_n)\right)\varepsilon$$

C'est à dire qu'on a pour tout $\varepsilon > 0$:

$$\begin{aligned}limsup_{n\to\infty}\frac{\mu\otimes\lambda(G/\Gamma)}{\mu\otimes\lambda(G_n\cap G_U)}(F_n(e,e) - \varepsilon Card(\Gamma\cap G_n)) &\leq \int_{G^\infty}\varphi d\mu + 2\varepsilon \\ limin f_{n\to\infty}\frac{\mu\otimes\lambda(G/\Gamma)}{\mu\otimes\lambda(G_n\cap G_U)}(F_n(e,e) + \varepsilon Card(\Gamma\cap G_n)) &\geq \int_{G^\infty}\varphi d\mu - 2\varepsilon\end{aligned}$$

On conclut en deux étapes : tout d'abord, on applique les deux inégalités précédentes à $\varphi = 1$, auquel cas $F_n(e,e) = Card(\Gamma\cap G_n)$. On en déduit (en faisant tendre ε vers 0) que :

$$\frac{\mu\otimes\lambda(G/\Gamma)}{\mu\otimes\lambda(G_n\cap G_U)}card(\Gamma\cap G_n) \xrightarrow{n\to\infty} 1$$

Enfin, on utilise ce résultat pour traiter le cas général : pour tout $\varepsilon > 0$, on a :

$$\begin{aligned}limsup_{n\to\infty}\frac{\mu\otimes\lambda(G/\Gamma)}{\mu\otimes\lambda(G_n\cap G_U)}F_n(e,e) &\leq \int_{G^\infty}\varphi d\mu + 3\varepsilon \\ limin f_{n\to\infty}\frac{\mu\otimes\lambda(G/\Gamma)}{\lambda(G_n\cap G_U)}F_n(e,e) &\geq \int_{G^\infty}\varphi d\mu - 3\varepsilon\end{aligned}$$

On peut maintenant faire tendre ε vers 0 pour obtenir la limite voulue. Ainsi, le théorème 3.1 est prouvé, et donc aussi le théorème 1.6. □

4. Cas des groupes unitaires

Nous prouvons dans cette partie le théorème 1.4, et donc le théorème 1.3. Nous reprenons les notations donnée dans l'introduction.

Preuve du théorème 1.4. — On va appliquer le théorème 3.1 dans le cas suivant : le groupe $\mathbf{G}$ est le $\mathbb{Q}$-groupe $SU(h)$. On note qu'il vérifie bien les hypothèses du théorème et de plus qu'il est simplement connexe (Cf **[12]**, paragraphe 2.3.3). On choisit $\Gamma = SU(h,\mathbb{Q})$, et U le produit pour p premier des compacts ouverts $SU(h,\mathbb{Z}_p)$.

Pour tout p premier et r entier, on note L_{p^r} le sous ensemble de $\mathbf{G}(\mathbb{Q}_p)$ composé des matrices telles que le sup de la valeur absolue des coefficients est p^r. Enfin pour tout n entier avec $n = \prod_{p\ premier} p^{\nu_p(n)}$, on note $H_n = \prod_{p\ premier} L_{p^{\nu_p(n)}}$.

On remarque alors que un entier n appartient à $\mathcal{U}_l(H)$ si et seulement si H_n est non vide. De plus, pour toute matrice M de $\mathcal{M}(h, \mathbb{Z}[i])$, M est dans $\mathcal{T}(n, H, \mathbb{Z})$ si et seulement si $\frac{1}{n}M$ appartient à $\mathbf{G}(\mathbb{R}) \times H_n$. C'est à dire que les ensembles Γ_n définis dans l'énoncé du théorème sont bien égaux à $\Gamma \cap G_n$.

Pour pouvoir appliquer le théorème 3.1, il ne reste plus qu'à montrer que les ensembles $G_n \cap G_U$ sont distincts. Or on remarque que, pour n dans $\mathcal{U}_l(H)$, les H_n sont disjoints donc distincts. Et il en est de même des G_n. Il suffit alors de vérifier que $G_U = G$. Il suffit donc d'appliquer le lemme suivant avec $L = G_U$:

Lemme 4.1. — *Soit* $\mathbf{G}$ *un* $\mathbb{Q}$*-groupe, quasi-*$\mathbb{Q}$*-simple et simplement connexe. Alors tout sous-groupe* L *fermé normal, contenant* $\mathbf{G}(\mathbb{Q})$ *et d'indice fini dans* $\mathbf{G}(\mathbb{A})$ *est égal à* $\mathbf{G}(\mathbb{A})$.

Démonstration. — En effet, si p est un nombre premier tel que $\mathbf{G}(\mathbb{Q}_p)$ est isotrope, alors $\mathbf{G}(\mathbb{Q}_p)$ est engendré par ses unipotents (voir **[12]**, paragraphe 7.2) et notamment ne contient pas de sous-groupe d'indice fini différent de lui-même. Donc le groupe $L \cap \mathbf{G}(\mathbb{Q}_p)$ (ici, on a plongé de façon naturelle $\mathbf{G}(\mathbb{Q}_p)$ dans $\mathbf{G}(\mathbb{A})$) est égal à $\mathbf{G}(\mathbb{Q}_p)$.

Ensuite, par propriété d'approximation forte (Cf **[12]**, théorème 7.12), $\mathbf{G}(\mathbb{Q}_p)\mathbf{G}(\mathbb{Q})$ est dense dans $\mathbf{G}(\mathbb{A})$. Donc $L = \mathbf{G}(\mathbb{A})$. □

Cela finit la preuve des théorèmes 1.4 et 1.3. □

5. Cas des groupes orthogonaux

Nous nous intéressons dans cette partie au cas des groupes orthogonaux. Remarquons tout d'abord que les groupes orthogonaux ne sont pas simplement connexes (Cf **[12]**, paragraphe 2.3.2, proposition 2.14), donc le lemme 4.1 ne s'applique pas.

De fait, la question du passage du local au global pour les formes quadratiques à coefficients entiers a été beaucoup étudié, et le théorème cité au début de ce chapitre donne une réponse satisfaisante dans les cas où le rang est supérieur à 5. Esquissons, dans les grandes lignes, la stratégie pour prouver ce théorème :

On dit qu'une forme quadratique q définie positive représente (resp. représente localement) un entier naturel n si n appartient à $q(\mathbb{Z})$ (resp. à $q(\mathbb{Z}_p)$ pour tout p premier). Nous rappelons aussi la définition du genre d'une forme quadratique q : c'est l'ensemble des formes quadratiques équivalentes à q à la fois sur $\mathbb{Q}$ et sur tous les $\mathbb{Z}_p$:

Définition 5.1. — Étant données deux formes quadratiques q et q' à coefficients entiers de rang k, associées respectivement aux matrices Q et Q', on dit qu'elles sont dans le même genre si elles vérifient les propriétés suivantes :

– il existe $g \in GL(k, \mathbb{Q})$ tel que $Q' = {}^t gQg$.

– pour tout p premier, il existe un élément $g_p \in GL(k, \mathbb{Z}_p)$ tel que $Q' = {}^t g_p Q g_p$

On prouve alors que si un entier est représenté localement par une forme quadratique q, il existe une forme dans le genre de q qui le représente (Cf [**3**], chap. 9 théorème 1.3). Ensuite, on démontre, du moins quand le rang est supérieur à 5, que toutes les formes d'un même genre représentent les mêmes entiers suffisament grands. Cette dernière étape ne fonctionne pas en toute généralité en rang 4, et pas du tout en rang 3, où il faut introduire le concept de genre-spin. Nous ne décrirons pas plus ces théories, et renvoyons à l'article de W. Duke ([**6**]) pour une présentation historique de ce problème, ainsi qu'à l'article de W. Duke et R. Schulze-Pillot ([**7**]) pour l'analyse du cas de rang 3.

Présentons maintenant les résultats que nous obtenons : fixons une forme quadratique q rationnelle définie positive de rang $k \geq 3$, de matrice associée Q. Notons, pour tout entier n, et pour $A = \mathbb{Z}$ ou $\mathbb{Z}_p$, $\mathcal{S}(n, q, A)$ l'ensemble des matrices $M \in \mathcal{M}(k, A)$ de déterminant n^k telles que $\frac{1}{n}M$ est de dénominateur, c'est à dire :

– les coefficients de M sont premiers entre eux,

– M est solution de l'équation (F_n) : ${}^tMQM = n^2Q$.

Notons $\mathcal{R}_l(q)$ l'ensemble des entiers n tels que pour tout p premier, $\mathcal{S}(n, q, \mathbb{Z}_p)$ est non vide. On notera de plus $\mathcal{R}_{genre}(q)$ l'ensemble des entiers n tels qu'il existe une forme q' dans le genre de q avec $\mathcal{S}(n, q', \mathbb{Z})$ non vide.

De la même manière que dans le cas unitaire, nous cherchons des matrices dans $\mathcal{S}(n, q, \mathbb{Z})$, et à comprendre l'image de cet ensemble dans $SO(q, \mathbb{R})$.

Dans le cas des formes de rang supérieur à 5, nous montrons avec le théorème 5.2 que si n est dans $\mathcal{R}_l(q)$ avec en plus la condition que n est premier à un certain entier fixé, et que n est suffisament grand, alors $\mathcal{S}(n, q, \mathbb{Z})$ est non vide, et son image dans $SO(q, \mathbb{R})$ s'équirépartit vers la mesure de Haar.

Ensuite, nous essayons de suivre une stratégie parallèle à celle évoquée plus haut. Nous montrons, cette fois sans restriction sur le rang, que, si n est dans $\mathcal{R}_{genre}(q)$ et suffisament grand, alors $\mathcal{S}(n, q, \mathbb{Z})$ est non vide, et son image s'équirépartit dans $SO(q, \mathbb{R})$. C'est l'objet du théorème 5.7.

5.1. Formes de rang supérieur à 5. — Commençons par le cas du rang supérieur à 5 :

Théorème 5.2. — *Soient $k \geq 5$, q une $\mathbb{Q}$-forme quadratique définie positive sur $\mathbb{Q}^k$ et μ la probabilité de Haar sur $SO(q, \mathbb{R})$. Soit pour un entier n, Γ_n l'ensemble des matrices de $SO(q, \mathbb{Q})$ de dénominateur n.*

Alors il existe un entier N tel que quand n tend vers l'infini et que n est premier à N, les Γ_n s'équirépartissent dans $SO(q, \mathbb{R})$, c'est à dire :

$$\frac{1}{Card(\Gamma_n)} \sum_{\gamma \in \Gamma_n} \delta_\gamma \xrightarrow[n \text{ premier à } N]{n \to \infty} \mu$$

Nous allons à nouveau appliquer le théorème 3.1, cette fois dans le cadre suivant : on considère le groupe $\mathbf{G} = SO(q)$, qui vérifie bien les hypothèses du corollaire. On pose pour tout p premier, $U_p = SO(q, \mathbb{Z}_p)$, et U le produit sur p des U_p.

Soit, pour p premier et m entier, $\tilde{H}_{p^m}$ l'ensemble des matrices de $SO(q, \mathbb{Q}_p)$ telles que le max de la norme p-adique des coefficients est p^m. Maintenant, pour un entier n, pour tout p premier, on note $\nu_p(n)$ la valuation p-adique de n. On pose alors H_n le produit sur les p premiers des $\tilde{H}_{p^{\nu_p(n)}}$. Ces ensembles H_n sont bi-U-invariants et deux à deux disjoints.

On vérifie alors que, pour tout n, l'ensemble Γ_n est exactement $SO(q, \mathbb{Q}) \cap G_n$.

Il nous faut maintenant déterminer un ensemble fini F de nombres premiers tel que si n est premier aux éléments de F, alors $G_n \cap G_U$ est non vide. Il suffira alors de choisir pour N le produit des nombres premiers dans F. Pour cela, on commence par un lemme de réduction des formes quadratiques :

Lemme 5.3. — *Soient $k \geq 5$, q une $\mathbb{Q}$-forme quadratique définie positive sur $\mathbb{Q}^k$. Alors il existe un ensemble fini F de nombres premiers tels que pour tout nombre premier p en dehors de F, on a :*

q est conjuguée par une matrice de $GL(k, \mathbb{Z}_p)$ à une forme quadratique de la forme $q'(x_1, \dots, x_k) = x_1x_2 + x_3x_4 + q''(x_5, \dots x_k)$.

Démonstration. — q est conjuguée par $A \in GL(n, \mathbb{Q})$ à une forme quadratique diagonale $\bar{q}$. Soit F l'ensemble des nombres premiers p tels que ou $p = 2$ ou bien A n'appartient pas à $GL(k, \mathbb{Z}_p)$ ou $\bar{q}$ n'est pas à coefficients dans $\mathbb{Z}_p^*$ pour la base canonique. Alors, pour tout $p \notin F$, q est conjugué sur $GL(k, \mathbb{Z}_p)$ à une forme quadratique diagonale à coefficients dans $\mathbb{Z}_p^*$.

On vérifie maintenant que pour tout p impair, toute forme quadratique r sur $\mathbb{Q}_p^5$ à coefficients dans $\mathbb{Z}_p^*$ est équivalente sur $\mathbb{Z}_p$ à une forme quadratique $y_1y_2 + +y_3y_4 + \alpha y_5^2$ pour un $\alpha \in \mathbb{Z}_p^*$ (voir [**14**]). □

On note pour tout $p \notin F$, φ_p l'isomorphisme entre $SO(q, \mathbb{Q}_p)$ et $SO(q', \mathbb{Q}_p)$ donné par le lemme précédent et pour tout m entier, J_{p^m} l'ensemble des matrices de $SO(q', \mathbb{Q}_p)$ telles que le max de la norme p-adique des coefficients est p^m. Comme le changement de base est à coefficients dans $\mathbb{Z}_p$, on a un corollaire du lemme précédent :

Corollaire 5.4. — *Pour tout $p \notin F$, pour tout $m \in \mathbb{N}$, on a $\varphi_p(\tilde{H}_{p^m}) = J_{p^m}$.*

Rappelons que G_U est défini comme l'intersection des noyaux de l'ensemble Λ_U des caractères U et $\mathbf{G}(\mathbb{Q})$ invariants de G.

Soit n un entier. On veut montrer que $G_n \cap G_U$ est non vide. Supposons qu'on dispose de $g \in G$ et $u \in U$ tel que gug^{-1} soit un élément de G_n. Alors, pour tout $\lambda \in \Lambda^U$, $\lambda(gug^{-1}) = 1$, et donc $gug^{-1} \in G_n \cap G_U$.

On voit donc que, pour montrer le théorème 5.2 il suffit de montrer que pour tout n dans $\mathcal{B}$, on peut trouver une paire $(g, u) \in G \times U$ tel que gug^{-1} est dans G_n.

D'après la définition de H_n, il suffit de trouver, pour tout p premier et $m = \nu_p(n)$ entier, une paire $(g, u) \in SO(q, \mathbb{Q}_p) \times U_p$ telle que gug^{-1} appartient encore à $\tilde{H}_{p^m}$. Si $m = 0$, ce qui est le cas notamment si $p \in F$, il suffit de trouver une matrice dans $SO(q, \mathbb{Z}_p)$: la matrice identité convient. Il reste à traiter le cas $\nu_p(n) \neq 0$, pour lequel on sait que $p \notin F$. Donc

on peut appliquer les deux lemmes précédents et utiliser l'isomorphisme φ_p. Le théorème est alors une conséquence du lemme suivant :

Lemme 5.5. — *Soient p un nombre premier impair, $m \in \mathbb{N}$, $k \geq 5$ et q' une forme quadratique sur $\mathbb{Q}_p^k$ de la forme $q'(x_1, \ldots, x_k) = x_1x_2 + x_3x_4 + q''(x_5, \ldots x_k)$.*

Alors il existe $g \in SO(q', \mathbb{Q}_p)$, et $u \in SO(q', \mathbb{Z}_p)$ tel que gug^{-1} appartient à J_{p^m}.

Démonstration. — Il suffit de prendre les matrices :

$$g = \begin{pmatrix} p^m & 0 & 0 & 0 & 0 \\ 0 & p^{-m} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & I_{k-4} \end{pmatrix} \text{ et } u = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & I_{k-4} \end{pmatrix}$$

□

On en déduit à nouveau comme corollaire un résultat d'existence :

Corollaire 5.6. — *Soient $k \geq 5$, $Q \in \mathcal{M}(k, \mathbb{Q})$ une matrice symétrique, définie positive.*

Alors il existe deux entiers N et n_0 tels que on a pour tout $n \geq n_0$:

n premire à N implique $\mathcal{S}(n, Q, \mathbb{Z})$ non vide.

5.2. Lien avec le genre. — Voilà l'énoncé qui exprime que pour des formes dans le même genre, l'ensemble des dénominateurs de matrices rationnelles dans leur groupe orthogonal sont les mêmes, du moins pour des entiers suffisament grands :

Théorème 5.7. — *Soient $k \geq 3$, q et q' deux formes quadratiques définies positives du même genre.*

Alors, pour n suffisamment grand, s'il existe une matrice rationnelle de dénominateur n dans $SO(q', \mathbb{Q})$, il en existe une dans $SO(q, \mathbb{Q})$.

Démonstration. — On se place exactement dans le cadre de la preuve du théorème 5.2 : on considère à nouveau le groupe $\mathbf{G} = SO(q)$. On pose pour tout p premier, $U_p = SO(q, \mathbb{Z}_p)$, et U le produit sur p des U_p.

On définit encore, pour p premier et m entier, $\tilde{H}_{p^m}$ l'ensemble des matrices de $SO(q, \mathbb{Q}_p)$ telles que le max de la norme p-adique des coefficients est p^m. Maintenant, pour un entier n, pour tout p premier, on note $\nu_p(n)$ la valuation p-adique de n. On pose alors H_n le produit sur les p premiers des $\tilde{H}_{p^{\nu_p(n)}}$. Ces ensembles H_n sont bi-U-invariants et deux à deux disjoints.

Soit maintenant n un entier tel qu'il existe une matrice γ de dénominateur n dans $SO(q', \mathbb{Q})$. Pour prouver le théorème, selon la méthode déjà vue, il nous suffit de montrer qu'alors $G_n \cap G_U$ est non vide. On note Q et Q' les matrices associées à q et q'.

Soient $g_{\mathbb{Q}}$ la matrice rationnelle conjuguant Q à Q', et, pour tout p premier, g_p la matrice de $GL(k, \mathbb{Z}_p)$ conjuguant Q à Q'. On notera g l'élément $(g_{\mathbb{Q}}, (g_p)_{p\, premier})$ de $GL(k, \mathbb{A})$ (ici, $g_{\mathbb{Q}}$ est vu comme un élément de $GL(k, \mathbb{Q}) \subset GL(k, \mathbb{R})$). Considérons l'élément $g\gamma g^{-1}$ de

$GL(k, \mathbb{A})$. Alors par définition de g, c'est un élément de $SO(q, \mathbb{A})$. On veut montrer qu'il est dans $G_n \cap G_U$.

Pour cela, commençons par remarquer que pour tout p premier, g_p est dans $GL(k, \mathbb{Z}_p)$. Donc l'élément $g\gamma g^{-1}$ est bien dans G_n (on n'a pas changé la norme p-adique de γ en le conjuguant par g_p).

Soit ensuite λ un caractère de Λ_U, c'est à dire U et Γ-invariant. On veut montrer que $\lambda(g\gamma g^{-1})$ vaut 1.

Définissons sur $SO(q', \mathbb{A})$ le caractère λ' par : pour tout $h \in SO(q', \mathbb{A})$, $\lambda'(h) = \lambda(g_{\mathbb{Q}} h g_{\mathbb{Q}}^{-1})$ (ici $g_{\mathbb{Q}}$ est vu comme l'élément rationel de $GL(k, \mathbb{A})$ dont chaque composant dans $GL(k, \mathbb{R})$ et les $GL(k, \mathbb{Q}_p)$ est la matrice $g_{\mathbb{Q}}$). Comme $g_{\mathbb{Q}}$ est une matrice rationnelle, λ' est $SO(q', \mathbb{Q})$-invariant.

Or on a $\lambda(g\gamma g^{-1}) = \lambda'(g_{\mathbb{Q}}^{-1} g\gamma g^{-1} g_{\mathbb{Q}})$. De plus, par construction, $g^{-1} g_{\mathbb{Q}}$ est un élément de $SO(q', \mathbb{A})$, et γ est un élément de $SO(q', \mathbb{Q})$..

Donc, on a montré le résultat voulu :

$$\lambda(g\gamma g^{-1}) = \lambda'(g_{\mathbb{Q}}^{-1} g\gamma g^{-1} g_{\mathbb{Q}}) = \lambda'(\gamma) = 1$$

Cela termine la preuve : il suffit d'appliquer le théorème 3.1. □

5.3. Application à la forme canonique. — Dans cette section, on applique nos résultats au cas de la forme quadratique canonique. On note q_k la forme quadratique canonique $x_1^2 + \ldots + x_k^2$ sur $\mathbb{Z}^k$. La stratégie est la même, mais la différence notable est qu'on sait construire en rang 3 des matrices rationnelles de tout dénominateur impair dans $SO(q_3, \mathbb{Q})$, donc nous n'avons plus de problèmes avec le groupe G_U.

Corollaire 5.8. — *Soient $k \geq 3$ et μ la probabilité de Haar sur $SO(q_k, \mathbb{R})$. Soit pour un entier n, Γ_n l'ensemble des matrices de $SO(q_k, \mathbb{Q})$ de dénominateur n.*

Alors quand n est impair tend vers l'infini, les Γ_n s'équirépartissent dans $SO(q_k, \mathbb{R})$, c'est à dire :

$$\frac{1}{Card(\Gamma_n)} \sum_{\gamma \in \Gamma_n} \delta_\gamma \xrightarrow[n \text{ impair}]{n \to \infty} \mu$$

Démonstration. — Soit n un entier impair. Commençons par construire une matrice rationnelle de dénominateur n :

Lemme 5.9. — *Pour tout entier impair n, il existe une matrice de dénominateur n dans $SO(k, \mathbb{Q})$.*

Démonstration. — Il suffit de le faire pour $SO(q_3, \mathbb{Q})$. Soit alors n un entier impair, et $x = a + ib + jc + kd$ un quaternion à coefficients entiers premiers entre eux de norme n.

Considérons la matrice de l'action de x par conjugaison sur les quaternions purs. Elle s'écrit :

$$\frac{1}{n} \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2(bc - ad) & 2(ac + bd) \\ 2(ad + bc) & a^2 - b^2 + c^2 - d^2 & 2(cd - ab) \\ 2(bd - ac) & 2(ab + cd) & a^2 - b^2 - c^2 + d^2 \end{pmatrix}$$

On vérifie alors qu'elle est bien de dénominateur n (il n'y a pas de simplification possible). De plus, par construction c'est une matrice de $SO(q_3, \mathbb{Q})$. □

On en déduit (avec les notations des preuves précédentes) que pour tout n impair, $G_n \cap G_U$ est non vide, car il contient une matrice rationnelle. On en déduit immédiatement le résultat du corollaire, comme application du théorème 3.1. □

6. Volume des doubles classes dans la décomposition de Cartan

Nous voulons donner ici une preuve du lemme 3.2. Soit donc $\mathbf{G}$ un groupe algébrique défini sur $\mathbb{Q}$, U un sous-groupe compact ouvert de G^f, et λ la mesure de Haar sur G^f telle que $\lambda(U) = 1$. On veut montrer que si g tend vers l'infini dans G^f, $\lambda(UgU)$ tend aussi vers l'infini.

Remarquons dans un premier temps qu'on a $\lambda(UgU) = Card\,(UgU/U)$. De plus, on peut changer de sous-groupe compact ouvert en vertu du lemme suivant :

Lemme 6.1. — *Si $V \subset U$ est un autre sous groupe compact ouvert de G^f, il existe une constante $c > 1$ telle que pour tout g dans G, on a : $\lambda(VgV) \leq \lambda(UgU) \leq c\lambda(VgV)$*

Démonstration. — Tout d'abord, comme $V \subset U$, il est clair qu'on a $\lambda(VgV) \leq \lambda(UgU)$.

De plus, soit c l'indice $[U : V]$. Alors on fait le calcul :

$$\begin{aligned} Card\,(UgU/U) &= Card\left(U/U \cap gUg^{-1}\right) \\ &\leq Card\left(U/V \cap gVg^{-1}\right) \\ &\leq cCard\left(V/V \cap gVg^{-1}\right) \end{aligned}$$

Les deux inégalités sont ainsi prouvées. □

Fixons un nombre premier p et raisonnons dans le groupe $\mathbf{G}(\mathbb{Q}_p)$. Pour les résultats sur les groupes p-adiques, nous nous réferrons à l'article de J. Tits (**[16]**), dont nous reprenons les notations.

Résumons les objets fournis par la théorie des groupes p-adiques dont nous aurons besoin : on dispose dans $\mathbf{G}(\mathbb{Q}_p)$ d'un tore maximal $\mathbb{Q}_p$-déployé T_p, et on note N_p son normalisateur et Z_p son centralisateur (ce sont des $\mathbb{Q}_p$-sous-groupes de $\mathbf{G}$).

De plus on définit les objets suivants :

1. Les groupes $X^* = Hom_{\mathbb{Q}_p}(T_p, Mult)$ et $X_* = Hom_{\mathbb{Q}_p}(Mult, T_p)$ des caractères définis sur $\mathbb{Q}_p$ et co-caractères définis sur $\mathbb{Q}_p$ du tore, ainsi que $X^*(Z) = Hom_{\mathbb{Q}_p}(Z_p, Mult)$.
2. L'espace vectoriel $V = \mathbb{R} \otimes X_*$, et le système de racines restreintes $\Phi \subset X^*$ associé au tore T_p.
3. une application ν de $N_p(\mathbb{Q}_p)$ dans le groupe des transformations affines d'un espace A sous V, définie en 1.2 de **[16]** comme l'unique extension de l'application de $Z_p(\mathbb{Q}_p)$ vérifiant (en notant v_p la valuation p-adique) :

$$\forall\, z \in Z_p(\mathbb{Q}_p) \text{ et } \chi \in X^*(Z), \text{ on a } \chi(\nu(z)) = v_p(\chi(z))$$

4. ${}^vW = N_p(\mathbb{Q}_p)/Z_p(\mathbb{Q}_p)$ le groupe de Weyl fini et $\tilde{W} = N_p(\mathbb{Q}_p)/ker\nu$ qui contient le groupe de Weyl affine W comme sous-groupe distingué d'indice fini. On identifie $\tilde{W}$ comme un sous-groupe des transformations affines de V en choisissant dans A un point spécial comme origine. ${}^vW$ est alors l'ensemble des automorphismes de $\tilde{W}$ fixant l'origine.
5. un choix d'un ensemble Φ^+ de racines positives dans Φ, et donc une chambre C contenant 0 dans V définie comme l'ensemble des points v de V tels que pour tout $\chi \in \Phi^+$, on a $\chi(v) \geq 0$.
6. la chambre vectorielle $Y^+ = \mathbb{R}^+ \otimes C$ de V et un sous-groupe compact ouvert U_p de $\mathbf{G}(\mathbb{Q}_p)$ (le fixateur du point spécial) tels que $\mathbf{G}(\mathbb{Q}_p)$ est l'union des doubles classes $U_p a U_p$ pour $a \in Z_p^+ = \nu^{-1}(Y^+)$ (décompostion de Cartan)

De plus, si $n \in Z_p$ est tel que $\nu(n)$ est dans ${}^vW$, alors n appartient à U_p.

Enfin, on peut définir sur $\tilde{W}$ une fonction longueur pondérée à valeur entière (voir le paragraphe 3.3 de **[16]**) de la façon suivante : on note (r_i) les symétries de W associées à un système de racines simples dans Φ^+. A chacun de ces éléments est associé un entier non nul $d(r_i)$. On écrit tout élément $w \in \tilde{W}$ sous la forme $w = r_{i_1} \dots r_{i_l} w_0$ où $w_0(C) = C$ et $r_{i_1} \dots r_{i_l}$ est un mot réduit dans W. On pose alors $l(w) = d(r_{i_1}) + \dots + d(r_{i_l})$.

Alors, d'après la section 3.3 de **[16]** (voir aussi **[11]**, 7.3), pour tout $a \in Z_p^+$, en notant $\nu(a) = w$, on a :

$$Card\,(U_p a U_p/U_p) = \frac{\sum_{y \in {}^vW w {}^vW} p^{l(y)}}{\sum_{y \in {}^vW} p^{l(y)}}$$

On tire le corollaire suivant de cette formule :

Corollaire 6.2. — 1. *si $a \in Z_p^+$ n'est pas dans U_p, on a $Card\,(U_p a U_p/U_p) \geq p$.*

2. *si a_n tend vers l'infini dans Z_p^+, on a $Card\,(U_p a_n U_p/U_p) \to +\infty$.*

Démonstration. — Commençons par le second point : si a_n tend vers l'infini dans $\mathbb{Z}_p^+$, alors la longueur $l(\nu(a))$ aussi, ce qui suffit.

Pour le premier point : soit a un élément de Z_p^+ qui n'est pas dans U_p. Considérons w_0 le mot le plus court dans ${}^vW\nu(a)$.

Si w_0 ne fixe pas C, alors $l(w_0) \geq 1$ et pour tout $w \in {}^vW$, on a par définition $l(ww_0) = l(w) + l(w_0)$. On en déduit que $Card\,(U_p a U_p/U_p)$ est plus grand que $p^{l(w_0)}$, donc que p.

Si w_0 fixe C, alors w_0 n'est pas dans ${}^vW$ (sinon a appartient à U_p). w_0^{-1} envoie donc l'origine de V sur un autre point x. Or il existe dans ${}^vW$ une symétrie s qui envoie x sur un point n'appartenant pas à C. Alors, le point $w_0 s w_0^{-1}$ est dans W car W est distingué dans $\tilde{W}$, mais pas dans ${}^vW$, car l'origine est envoyé sur un point en dehors de C, donc n'est pas fixée.

Donc $w_0 s$ s'écrit sous la forme rw_0, où r est dans W mais pas dans ${}^vW$. En raisonnant comme précedemment, mais pour l'ensemble ${}^vWrw_0$, on obtient aussi dans ce cas que $Card\,(U_p a U_p/U_p)$ est plus grand que p. □

Maintenant que nous disposons de tous ces objets, le lemme 3.2 peut être prouvé :

Preuve du lemme 3.2. — On fixe maintenant le compact ouvert $U_0 = \prod_{p\in\mathcal{P}} U_p$. Considérons une suite (g_n) d'élément de G^f qui tend vers l'infini. Chaque g_n s'écrit comme une suite $(g_{p,n})_{p\ premier}$ dans le produit $\prod_{p\ premier} \mathbf{G}(\mathbb{Q}_p)$. On décompose toutes les coordonées dans la décomposition de Cartan :

$$g_{p,n} \in U_p a_{p,n} U_p, \text{ avec } a_{p,n} \in Z_p^+$$

Soit maintenant A un entier positif. Alors on veut montrer qu'il existe N tel que pour tout $n \geq N$, $\lambda(U_0 g_n U_0) \geq A$.

Soit $P \geq A$ un nombre premier. Pour tout élément g_n tel que il existe $q \geq P$ avec $a_{q,n} \notin U_q$, on a d'après le premier point du corollaire 6.2 :

$$\lambda(U_0 g_n U_0) = \prod_{p\ premier} Card\,(U_p a_{p,n} U_p/U_p) \geq Card\,(U_q a_{q,n} U_q/U_q) \geq q \geq A$$

Par ailleurs, considérons la sous-suite $(g_n)_{n\in S}$ telle que pour tout $n \in S$, et pour tout $p \geq P$, $a_{p,n}$ appartient à U_p.

Si cette sous-suite est finie, le résultat voulu est prouvé. Sinon, comme (g_n) sort de tout compact, il existe un nombre premier $q \leq P$ tel que la suite $(a_{q,n})_{n\in S}$ tend vers l'infini dans Z_q^+. Alors, d'après le deuxième point du corollaire 6.2, on a :

$$\lambda(U_0 g_n U_0) = \prod_{p\ premier} Card\,(U_p a_{p,n} U_p/U_p) \geq Card\,(U_q a_{q,n} U_q/U_q) \xrightarrow{n\to\infty} +\infty$$

Ainsi pour n suffisament grand, $\lambda(U_0 g_n U_0)$ est de toute façon supérieur à A.

Cela montre le résultat pour le groupe compact ouvert U_0. Or on a vu avec le lemme 6.1 que cela suffisait. Donc on a bien le résultat voulu. □

Références

[1] A. Borel & J. Tits – « Groupes réductifs », *Inst. Hautes Etudes Sci. Publ. Math.* **27** (1965), p. 55–150.

[2] W. Casselman – *Introduction to the theory of admissible representation of p-adic reductive groups*, 1995.

[3] J. Cassels – *Rational quadratic forms*, Academic Press, London, New York, San Francisco, 1978.

[4] L. Clozel – « Démonstration de la conjecture τ », *Invent. Math.* **151** (2003), p. 297–328.

[5] L. Clozel, H. Oh & E. Ullmo – « Hecke operators and equidistribution of Hecke points », *Invent. Math.* **144** (2001), p. 327–351.

[6] W. Duke – « Some old problems and new results about quadratic forms », *Notices A.M.S* **44** (1997), p. 190–196.

[7] W. Duke & R. Schulze-Pillot – « Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids », *Invent Math* **99** (1990), p. 49–57.

[8] A. Eskin & C. McMullen – « Mixing, counting and equidistribution in Lie groups », *Duke Math. J.* **71** (1993), p. 181–209.

[9] A. Eskin & H. Oh – « Ergodic theoretic proof of equidistribution of Hecke points », *Erg. The. and Dyn. Sys.* (To appear).

[10] A. Gorodnik, F. Maucourant & H. Oh – « Manin's conjecture on rational points of bounded height and adelic mixing », *Prépublication* (2005).

[11] B. Gross – « On the Satake isomorphism », *Galois Representations in Arithmetic Algebraic Geometry* (R. T. A.J. Scholl, éd.), Cambridge University Press, 1998, p. 223–237.

[12] V. Platonov & A. Rapinchuk – *Algebraic groups and number theory*, Academic Press, Boston MA, London, Sydney, 1994.

[13] C. Pommerenke – « Über die Gleichverteilung von Gitterpunkten auf m-dimensionalen Ellipsoiden », *Acta Arithmetica* **5** (1959), p. 227–257.

[14] J. Serre – *Cours d'arithmétique*, Presses Universitaires de France, Paris, 1995.

[15] W. Tartakowsky – « La détermination de la totalité des nombres représentables par une forme quadratique positive quaternaire », *Compte Rendus de l'Académie des Sciences* **186** (1928), p. 1684–1987.

[16] J. Tits – « Reductive groups over local fields », *Proceedings of Symposia in Pure Mathematics* **33** (1979), p. 20–70.

---

15 février 2007

Antonin Guilloux, Département de Mathématiques et Applications, École Normale Supérieure, 45 rue d'Ulm, 75005 Paris, France. • *E-mail :* antonin.guilloux@ens.fr
Url : http://www.dma.ens.fr/~aguillou/