LA CONJECTURE D'OPPENHEIM ET SA VERSION QUANTITATIVE

EMMANUEL BREUILLARD

Mémoire de DEA sous la direction de Martine Babillot

Date: janvier 2000 .

Je tiens à remercier Martine Babillot et Yves Benoist qui m'ont apporté une aide précieuse pour la rédaction de ce mémoire.

Table des matières

Première partie 1. Introduction

Dans les années 1930, Oppenheim a formulé la conjecture suivante pour $n \geq 5$ et, plus tard, dans les années 1950, Davenport la reformula pour $n \geq 3$:

Conjecture 0.1. *(conjecture d'Oppenheim) Soit q une forme quadratique sur $\mathbb{R}^n$ ($n \geq 3$), non-dégénérée, indéfinie et irrationnelle. Alors $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}$.*

"Irrationnelle" signifie "non proportionnelle à une forme à coefficients entiers". Cet énoncé très simple a résisté aux mathématiciens jusqu'en 1987, date à laquelle G. Margulis le démontra. De nombreuses études avaient été effectuées auparavant utilisant essentiellement des techniques de théorie analytique des nombres, notamment dans les années 1950 autour de Davenport. D'ailleurs, la conjecture avait été démontrée dans certains cas particuliers comme les formes diagonales et dans le cas général pour $n \geq 21$. Dans les années 1970, Raghunathan a établi un lien entre cette conjecture et des questions concernant l'adhérence des orbites de certains groupes dans les espaces homogènes. Son idée était de traduire la conjecture d'Oppenheim en termes topologiques en passant dans l'espace des réseaux de la géométrie des nombres $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. En réalité, cette idée avait déjà été formulée sous forme implicite par Cassels et Swinnerton-Dyer (cf. [CS]) dans les années 1950, mais jusque là semble être restée sans suite. Raghunathan énonça donc une autre conjecture dont il montra qu'elle entraînait facilement la conjecture d'Oppenheim et même plus : si $\mathcal{P}$ désigne l'ensemble des points primitifs de $\mathbb{Z}^n$ (i.e. dont les coordonnées sont premières entre elles) alors $q(\mathcal{P})$ est déjà dense dans $\mathbb{R}$ (cf. §6.2.).

Conjecture 0.2. *(Conjecture de Raghunathan) Soit G un groupe de Lie connexe, U un sous-groupe unipotent de G et Γ un réseau de G. Alors pour tout $x \in G/\Gamma$, il existe un sous-groupe fermé L de G tel que $\overline{U \cdot x} = L \cdot x$.*

La nouvelle approche suggérée par Raghunathan permit à Margulis de réduire la conjecture d'Oppenheim à un cas particulier de la conjecture de Raghunathan (cf. thm 8.1.) pour

$G = SL_3(\mathbb{R})$ et $\Gamma = SL_3(\mathbb{Z})$. La preuve qu'a donnée Margulis de ce cas particulier, bien que difficile, est très élémentaire.

La conjecture de Raghunathan a finalement été démontrée en 1990 par M. Ratner. Ce résultat remarquable est en réalité lié aux propriétés ergodiques des mesures sur G/Γ invariantes par l'action de certains groupes. Dans la preuve de Ratner, la conjecture de Raghunathan apparaît comme conséquence de deux théorèmes (cf. §6.1.) : l'un est une classification des mesures invariantes pour l'action d'un sous-groupe unipotent de G, l'autre est un théorème d'équirépartition qui montre en particulier l'équidistribution de tout point sous l'action de flots unipotents pour une certaine mesure portée par l'orbite.

Il est remarquable qu'un problème de théorie des nombres comme la conjecture d'Oppenheim soit lié à de telles considérations de théorie des groupes de Lie et de théorie ergodique.

Une fois la conjecture d'Oppenheim démontrée, un problème naturel se posait : compter les points de $\mathbb{Z}^n$ situés entre deux surfaces de niveau. Si $V^q_{a,b}(\mathbb{Z})$ désigne $\{x \in \mathbb{Z}^n \mid a < q(x) < b\}$ et B_T la boule centrée en 0 de rayon T, $\left|V^q_{a,b}(\mathbb{Z}) \cap B_T\right|$ tend vers l'infini puisque $q(\mathbb{Z}^n)$ est dense, mais à quelle vitesse ? On parle de la version quantitative de la conjecture d'Oppenheim. En 1994, Eskin, Margulis et Mozes ont résolu ce problème par le théorème suivant, qui en définitive montre l'équirépartition des valeurs de q aux points entiers lorsque q est irrationnelle :

Théorème 0.1. ***(Version quantitative)*** *Soit q une forme quadratique réelle irrationnelle et de signature $(p, n-p)$ avec $n \geqslant 4$ et $p \geqslant 3$, alors*

$$\lim_{T\to\infty} \frac{\left|V^q_{a,b}(\mathbb{Z}) \cap B_T\right|}{\left|V^q_{a,b}(\mathbb{R}) \cap B_T\right|} = 1$$

où $V^q_{a,b}(\mathbb{R})$ désigne $\{x \in \mathbb{R}^n \mid a < q(x) < b\}$.

La preuve utilise de façon cruciale un théorème d'équirépartition de grandes sphères, ici déduit des travaux généraux de Ratner sur les actions de groupes unipotents, en particulier de son théorème d'équirépartition. Il s'avère que la lim inf dans l'expression ci-dessus est obtenue assez rapidement. C'est surtout la lim sup qui requiert un travail important. Notamment, une des difficultés vient du fait que le théorème d'équirépartition de Ratner n'est valide que pour des fonctions continues bornées, alors que l'on a affaire dans ce problème à des fonctions non bornées sur G/Γ.

Le cas de basses signatures (signatures (2,2) et (2,1)) est plus complexe. Comme souvent, des structures plus riches apparaissent en basse dimension. Cependant le théorème est encore vrai pour presque toute forme quadratique (cf. §12).

Ce mémoire a pour but d'expliquer en détail ce qui vient d'être introduit. La partie 2, la plus longue, est consacrée à des préliminaires où sont introduites toutes les notions dont nous aurons besoin dans la suite. Les premiers paragraphes (§1 à 3) sont très classiques, ainsi que le début du quatrième. Dans le cinquième paragraphe, nous rappelons d'abord quelques propriétés bien connues des formes quadratiques, puis nous faisons quelques premières remarques simples à propos de la conjecture d'Oppenheim et nous expliquons ce qui se passe quand $n = 2$. Enfin, dans le dernier paragraphe de ces préliminaires, on énonce les théorèmes de Ratner (seuls résultats admis ici) et on explique comment la conjecture de Raghunathan résout la conjecture d'Oppenheim. Bien évidemment, ces préliminaires contiennent ce que, à titre personnel, je considère nécessaire d'être rappelé.

La partie 3 donne la preuve de Margulis de la conjecture d'Oppenheim et la partie 4 traite la version quantitative et évoque ses généralisations.

Je me suis efforcé de rendre la lecture des deux dernières parties la plus indépendante possible des préliminaires. Lorsqu'un résultat des préliminaires est utilisé, il est toujours précisé avec sa référence.

Deuxième partie 2. Préliminaires

1. Actions continues et différentiables

1.1. **Définitions.** Rappelons qu'un **groupe topologique** est un groupe G muni d'une topologie pour laquelle la multiplication ($G \times G \to G$) et l'inversion sont continues. Un **groupe de Lie** est un groupe topologique qui est de plus une variété différentiable sur $\mathbb{R}$ ou $\mathbb{C}$ telle que les opérations de multiplication et d'inversion soient différentiables. Le sens que prend le mot "différentiable" n'a pas d'importance car tous les groupes de Lie sont en fait des variétés analytiques et les opérations associées sont aussi analytiques.

Soit G un groupe topologique. Si H est un sous-groupe, on peut considérer l'espace quotient $G/H = \{gH/g \in G\}$ des classes à gauche de G (orbites pour l'action à droite de H). On le munit naturellement de la **topologie quotient** héritée de celle de G. Les ouverts de G/H sont par définition les parties U telles que $\pi^{-1}(U)$ soit ouvert, où π est la surjection canonique $G \longrightarrow G/H$. **Le saturé** d'une partie A de G est l'ensemble $\pi^{-1}(\pi(A)) = AH$.

On a les propriétés suivantes :

1. la surjection canonique π est continue et ouverte, c'est-à-dire que l'image de tout ouvert est ouverte.
2. la topologie de G/H est séparée si et seulement si H est fermé dans G.

Si X est un espace topologique (resp. variété différentielle), on dit que G **agit continûment** (resp. différentiablement) sur X si l'application associée de $G \times X$ dans X est continue (resp. différentiable). Chaque élément de G fournit alors un homéomorphisme (resp. difféomorphisme) de X.

Enfin, si G est un groupe de Lie, les sous-groupes de Lie de G (c'est-à-dire les sous-groupes de G qui sont aussi des variétés différentiables) sont précisément les sous-groupes fermés de G (théorème de Cartan). De plus, dans cette situation, il existe une et une seule structure différentielle sur G/H telle que π soit une fibration de fibre H et d'espace total G. L'action à gauche de G sur G/H est alors différentiable (voir par exemple [OnV]).

1.2. **Espaces homogènes.** Dans cet exposé, les groupes qui nous intéresserons seront des groupes de Lie, donc localement compacts (c'est-à-dire séparés et tels que tout point a un voisinage compact). Les propriétés ci-dessus entraînent que si G est localement compact et H fermé, alors G/H est aussi localement compact. Avec ces hypothèses on dit que G/H **est un espace homogène** (plus généralement, mais c'est en fait la même chose comme le montre la prop. 1.3., il s'agit d'un espace localement compact sur lequel un groupe G opère continûment et transitivement). Lorsque H est discret, la projection π est un revêtement de G sur G/H. C'est le cas de l'exemple le plus important d'espace homogène que nous rencontrerons dans cet exposé : l'espace des réseaux $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. La propriété suivante caractérise les compacts de G/H.

Proposition 1.1. *Soit G un groupe topologique localement compact et H un sous-groupe fermé. Alors les compacts de G/H sont précisément les images par π des compacts de G.*

***Preuve*:** π étant continue et G/H séparé, l'image d'un compact de G est compacte. Réciproquement, à tout point x de G/H on associe un voisinage compact V_x, dans G, d'un représentant de x. Alors $\pi(V_x)$ est un voisinage compact de x dans G/H. Un compact K de G/H est recouvert par un nombre fini d'entre eux, $K \subset \bigcup_i \pi(V_{x_i})$. Alors $K' = \pi^{-1}(K) \cap \bigcup_i V_{x_i}$ est bien un compact de G tel que $\pi(K') = K$.■

Un espace homogène apparaît dès que l'on a une action continue de G, localement compact, dans un espace topologique X. L'action de G sur un point x quelconque de X se factorise en une bijection continue de G/G_x sur $G \cdot x$, où G_x est le stabilisateur de x pour l'action de G qui est un groupe fermé de G. G/G_x est donc un espace homogène. La proposition suivante donne une condition nécessaire et suffisante pour que cette bijection soit un homéomorphisme.

Proposition 1.2. *Soit G un groupe topologique localement compact et dénombrable à l'infini qui agit continûment sur un espace localement compact X. Alors pour tout $x \in X$, la bijection induite $G/G_x \overset{\phi_x}{\to} G \cdot x$ est un homéomorphisme si et seulement si l'orbite $G \cdot x$ est localement fermée dans X.*

***Preuve*:** Quitte à considérer l'adhérence de $G \cdot x$, on peut supposer que $G \cdot x$ est dense dans X. Si ϕ_x est un homéomorphisme, alors $G \cdot x$ est localement compacte. On peut donc trouver dans $G \cdot x$ un compact d'intérieur non-vide K ; c'est-à-dire qu'il existe un ouvert U de X tel que $\overset{\circ}{K} = U \cap G \cdot x$. Mais $U \cap G \cdot x$ est dense dans U, donc $K = \overline{U \cap G \cdot x} \supset U$. Donc $G \cdot x$ est d'intérieur non-vide, donc ouverte. Réciproquement, supposons $G \cdot x$ localement fermée (c'est-à-dire ici ouverte). Il suffit de montrer que ϕ_x est ouverte, on encore, car $G \cdot x$ est ouverte, que $f : g \longmapsto g \cdot x$ $G \longrightarrow X$ est ouverte. Par translation on se ramène à montrer que l'image par f de tout voisinage du neutre e est un voisinage de x. Il suffit même de voir que cette image est d'intérieur non vide (soit V un tel voisinage de e, prendre W un autre voisinage ouvert de e tel que $WW^{-1} \subset V$, si $w \cdot x$ est intérieur à $W \cdot x$, alors x est intérieur à $w^{-1}W \cdot x \subset V \cdot x$). Soit V un voisinage quelconque de e, on choisit un voisinage compact W de e inclus dans V. Puisque G est dénombrable à l'infini, il s'écrit $\bigcup K_n$, et chaque K_n est compact et recouvert par $\bigcup_{g \in G} g\overset{\circ}{W}$. En extrayant un sous-recouvrement fini pour chaque n, on a l'existence d'une suite g_n d'éléments de G telle que $G = \bigcup g_n W$, d'où $G \cdot x = \bigcup g_n W \cdot x$, union dénombrable de compacts, donc de fermés. Maintenant, puisque X est localement compact, il est de Baire et, comme $G \cdot x$ est ouverte, l'un des $g_n W \cdot x$ est d'intérieur non vide, donc $W \cdot x$ et $V \cdot x$ le sont aussi, ce qui achève la preuve.■

Remarque 1.1. *Le fait essentiel ici est que X soit* **de Baire** *(et séparé). La proposition est donc encore vraie si X est métrique complet.*

L'hypothèse "localement fermé" est satisfaite dès que l'action est transitive (par exemple, nous utiliserons souvent le fait que $U \cdot x$ est ouvert dans G/H si $x \in G/H$ et U est un ouvert de G, mais dans ce cas précis la proposition découle simplement de 1.1.1.) ; ou encore si G est compact ; enfin nous verrons que c'est le cas si G est un groupe linéaire algébrique et si l'action est algébrique.

Lorsque G est un groupe de Lie agissant différentiablement sur une variété différentiable X, pour tout point $x \in X$, l'application

$$\begin{array}{ccc} \alpha_x & : & G \to X \\ g & \mapsto & g \cdot x \end{array}$$

est différentiable et **de rang constant** (cf. [OnV]). En particulier, le stabilisateur G_x est un sous-groupe de Lie de G, et l'application induite ϕ_x est une immersion injective de G/G_x dans X. Toute immersion injective qui est en outre un homéomorphisme est en fait un plongement (i.e. un difféomorphisme sur son image). On déduit de la proposition précédente le

Corollaire 1.1. *Soit G un groupe de Lie dénombrable à l'infini qui agit différentiablement sur une variété différentiable X. Alors pour tout $x \in X$, $G \cdot x$ est une sous-variété de X et la bijection induite $G/G_x \xrightarrow{\phi_x} G \cdot x$ est un difféomorphisme si et seulement si l'orbite $G \cdot x$ est localement fermée dans X.*

1.3. **Groupes connexes.** On a les propriétés faciles suivantes en ce qui concerne la connexité. On se donne un groupe topologique G.

1. Si G est connexe, il est engendré par tout voisinage du neutre e.
2. La composante connexe de e dans G est un sous-groupe fermé de G distingué dans G. On l'appelle composante neutre de G, soit G_0. Si G est localement connexe (par exemple de Lie), G_0 est ouverte.
3. Si H est un sous-groupe fermé connexe, alors l'image réciproque par π de tout connexe de G/H est connexe.

1.4. **Structure uniforme et métriques sur les espaces homogènes.**

1.4.1. *Structure uniforme.* Tout groupe topologique G est muni d'une structure uniforme naturelle donnée par l'ensemble fondamental d'entourages $\mathcal{V} = \{V_i\}_{i \in I}$, où

$$V_i = \left\{(g, g') \in G \times G \mid g^{-1}g' \in U_i\right\}$$

et $(U_i)_{i \in I}$ est un système fondamental de voisinages de e dans G. Ceci définit la **structure uniforme à gauche** sur G (cf. [Bou1]). De même sur tout espace homogène G/H on définit la structure uniforme à gauche par le système fondamental d'entourages $\mathcal{W} = \{W_i\}_{i \in I}$, où

$$W_i = \{(\Delta, \Delta') \in G/H \times G/H \mid \exists g \in U_i \ \Delta' = g\Delta\} \tag{1}$$

Ceci permet de parler naturellement de continuité uniforme sur l'espace homogène G/H. (Remarquons que si H est trivial, on obtient la structure uniforme à droite sur G...)

Rappelons que tout espace métrique est doté d'une structure uniforme naturelle en prenant le système fondamental d'entourages $V_i = \left\{(x, y) \in E \times E \mid d(x, y) < \frac{1}{i}\right\}$ pour $i \in \mathbb{N}^*$.

1.4.2. *Métriques invariantes.* Naturellement, nous sommes ammenés à chercher une distance sur G ou G/H qui induise la structure uniforme à gauche que l'on vient de décrire. C'est le cas pour toute distance sur G compatible avec la topologie de G et invariante à gauche (c'est-à-dire telle que $d(gx, gy) = d(x, y)$ pour tous x, y, g dans G).

De même, une distance d invariante à droite sur G, induit naturellement une distance sur G/H donnée par la distance minimale entre deux classes à gauche de G/H.

$$\widetilde{d}(gH, g'H) = \inf_{h, h' \in H} d(gh, g'h') = \inf_{h \in H} d(g, g'h)$$

Notons que ceci définit bien une distance sur G/H, car d a été choisie invariante à droite. D'autre part, la topologie induite par $\widetilde{d}$ est bien la topologie quotient et la structure uniforme induite est la structure uniforme à gauche sur G/H (puisque, avec les notations de 1, $I =]0, \infty[$, et $U_i = \{g | d(e, g) < i\}$, on a $\widetilde{d}(\Delta, \Delta') < i \Leftrightarrow (\Delta, \Delta') \in W_i$).

Sur un groupe topologique à base dénombrable d'ouverts, on peut toujours construire une distance invariante à gauche compatible avec la topologie initiale (voir [HeR]). Plus simplement, sur tout groupe de Lie, il est immédiat de construire une métrique riemannienne invariante à gauche par G (prendre un produit scalaire $(,)$ quelconque sur l'algèbre de Lie associée et définir $(g \cdot x, g \cdot y)_g = (x, y)$ pour tous x, y dans $\mathfrak{g}$). La distance riemannienne associée fournit une distance invariante à gauche sur G qui est compatible avec la topologie.

Dans les applications nous serons toujours dans le cas $G = SL_n(\mathbb{R})$ et $H = SL_n(\mathbb{Z})$. Par conséquent nous munirons G d'une distance riemannienne invariante à gauche et G/H de la distance induite par une distance riemannienne invariante à droite comme ci-dessus.

2. Mesure de Haar. Intégration dans les espaces homogènes

Dans cette section, nous rappelons quelques faits classiques sur la mesure de Haar et les mesures invariantes dans les espaces homogènes.

2.1. **Mesure de Haar.**

2.1.1. *Définition et propriétés.* En 1933, Haar a montré l'existence et l'unicité à un scalaire près d'une mesure invariante à gauche sur un groupe localement compact quelconque (cf. par exemple [Hal] ou [Wei]). Les mesures que l'on considère ici sont des mesures de Radon, c'est-à-dire des mesures positives, finies sur les compacts, sur la tribu des boréliens complétée. D'après le théorème de représentation de Riesz (cf. par exemple [Rud]), il revient au même de se donner une mesure de Radon sur un espace localement compact X ou une forme linéaire positive sur l'espace des fonctions continues à support compact, noté $C_c(X)$.

Théorème 2.1. *Soit G un groupe localement compact. Il existe une mesure de Radon ($\neq 0$) sur G invariante à gauche par G. Elle est unique à multiplication par un scalaire près.*

L'invariance à gauche signifie que pour tout borélien A et tout $g \in G$ on a $\mu(gA) = \mu(A)$. Toute mesure invariante à gauche sur G s'appelle une **mesure de Haar** sur G. On note μ_G une mesure de Haar de G. Rappelons maintenant les propriétés classiques de μ_G.

1. μ_G est strictement positive sur les ouverts.
2. μ_G est finie si et seulement si G est compact.
3. μ_G est sans atome si et seulement si G n'est pas discret.

Lorsque G est un groupe de Lie, l'existence et l'unicité de la mesure de Haar se déduit de l'existence d'une unique (à un scalaire près) forme volume invariante à gauche sur G. En particulier, si G est muni d'une métrique riemannienne, la mesure de Haar est absolument continue par rapport au volume riemannien.

2.1.2. *Module.* Soit ϕ un automorphisme continu de G dans G. Alors, la mesure $A \longmapsto \mu_G(\phi(A))$ est aussi une mesure de Radon invariante à gauche. Par l'unicité de la mesure de Haar, elle est donc proportionnelle à μ_G. Le coefficient de proportionnalité s'appelle le **module** de ϕ et se note $mod(\phi)$. Il est bien sûr indépendant du choix initial de μ_G. En particulier ϕ peut être la conjugaison par $g \in G$, $\phi : \ x \mapsto gxg^{-1}$. Dans ce dernier cas, le module de ϕ est noté $\Delta_G(g)$. La fonction Δ_G s'appelle la **fonction module** de G. On a donc :

1. Pour tout $f \in C_c(G)$ et $g \in G$,
$$\int_G f(\phi^{-1}(x))\mu_G(dx) = (mod(\phi)) \int_G f(x)\mu_G(dx)$$
2. Δ_G est un morphisme de groupe continu de G dans $\mathbb{R}_+^*$.
3. Pour tout $f \in C_c(G)$,

$$\int_G f(x)\mu_G(dx) = \int_G f(x^{-1})\Delta_G(x)\mu_G(dx) \tag{2}$$

Définition 2.1. *On dit que G est* ***unimodulaire*** *si Δ_G est trivial ($\Delta_G(g) = 1\ \forall g$).*

Il revient au même de dire que la mesure de Haar est aussi invariante à droite par G.

Proposition 2.1. *Si G est discret, si G est compact ou si G est égal à l'adhérence de son groupe dérivé, alors G est unimodulaire.*

Ceci permet par exemple de voir que $SL_n(\mathbb{R})$ est unimodulaire ($SL_n(\mathbb{R})$ est engendré par les transvections qui sont des commutateurs). En fait, on montre que tout groupe de Lie connexe semi-simple ou nilpotent est unimodulaire.

2.2. Mesures invariantes sur les espaces homogènes.

2.2.1. *Mesure sur G associée à une mesure sur G/H.* Soit H un sous-groupe fermé de G et μ_H une mesure de Haar sur H. En décomposant G en orbites modulo H, on peut effectuer des "moyennes orbitales" d'une fonction sur G. Ceci fournit une fonction de G/H, et comme on s'y attend, on va définir une mesure sur G en disant que la moyenne totale sur G coïncide avec la moyenne sur G/H des moyennes orbitales.

Si $f \in C_c(G)$ fonction continue à support compact, on définit la moyenne orbitale de f par :

$$\overline{f}(\dot{g}) = \int_H f(gh)\mu_H(dh)$$

Clairement $\overline{f} \in C_c(G/H)$. La proposition suivante est cruciale pour la suite :

Proposition 2.2. *L'application $f \longmapsto \overline{f}$ est surjective de $C_c(G)$ sur $C_c(G/H)$ et de $C_c^+(G)$ sur $C_c^+(G/H)$ (fonctions continues à support compact positives)*

***Preuve*:** Il s'agit de construire une fonction sur G dont les moyennes orbitales sont données. Pour cela fixons $\phi \in C_c(G/H)$ et donnons-nous un ouvert O relativement compact de G tel que le support de ϕ soit inclus dans $\pi(O)$ (π est comme toujours la projection canonique ; l'existence de O découle de la proposition 1.2.). Soit $\psi \in C_c^+(G)$ égale à 1 sur tout O (l'existence de ψ découle par exemple du lemme de prolongement de Tietse). Pour tout $g \in O$ il existe un voisinage de l'identité V dans H tel que $gV \subset O$. Alors on voit que $\overline{\psi}(\dot{g}) \geqslant \mu_H(V) > 0$. Cela permet de définir ξ comme suit :

$$\begin{aligned} \xi(x) &= \frac{\phi(x)}{\overline{\psi}(x)} \text{ si } x \in \pi(G) \\ &= 0 \text{ sinon} \end{aligned}$$

Clairement $\xi \in C_c(G/H)$ (et positive si ϕ l'est) et on remarque finalement que $\phi = \overline{\psi}\xi = \overline{\psi(\xi \circ \pi)}$.■

Nous allons maintenant préciser le principe décrit au début de ce paragraphe qui permet d'associer les mesures sur G à celles sur G/H. Tout d'abord, si μ est une mesure de Radon sur G/H alors la forme linéaire positive $f \longmapsto \int_{G/H} \overline{f} d\mu$ définit une mesure de Radon sur G que l'on note $\overline{\mu}$. Ainsi pour tout $f \in C_c(G)$:

$$\int_G f d\overline{\mu} = \int_{G/H} \overline{f} d\mu$$

De plus on remarque que $\overline{f \circ \tau_g}(x) = \overline{f}(gx)$ (resp. $\overline{f \circ \delta_h}(x) = \Delta_H(h)\overline{f}(x)$) où τ_g (resp. δ_h) désigne la translation à gauche par $g \in G$ (resp. à droite par $h \in H$). Par suite,

$$\int_G f(gx)\overline{\mu}(dx) = \int_{G/H} \overline{f}(gx)\mu(dx) \tag{3}$$

$$\int_G f(xh)\overline{\mu}(dx) = \Delta_H(h) \int_G f(x)\overline{\mu}(dx) \tag{4}$$

et on en déduit la propriété suivante :

Propriété: μ est invariante à gauche par G si et seulement si $\overline{\mu}$ l'est. Dans ce cas $\overline{\mu}$ est une mesure de Haar sur G et $\Delta_H(h) = \Delta_G(h)$ pour tout $h \in H$.

2.2.2. *Mesure sur G/H associée à une mesure sur G.* On vient de construire une mesure sur G à partir d'une mesure sur G/H. Inversement, la proposition suivante montre que toutes les mesures sur G qui vérifient 4 sont obtenues par ce procédé.

Proposition 2.3. *Soit ν une mesure de Radon sur G qui vérifie 4. Alors il existe une unique mesure de Radon μ sur G/H telle que $\nu = \overline{\mu}$. On la note $\mu = \nu/\mu_H$.*

***Preuve*:** L'unicité est claire compte tenu de l'équation 3 et du fait que $f \longmapsto \overline{f}$ est surjective. La surjectivité de cette application permet en particulier, étant donnée $\phi \in C_c(G/H)$, de trouver $f \in C_c(G)$ telle que $\phi = \overline{f}$. On voudrait alors définir une forme linéaire positive sur $C_c(G/H)$ en associant $\int_G f d\nu$ à ϕ. Il suffit de montrer que cette intégrale ne dépend pas du choix de f, ou encore de voir que $\overline{f} = 0 \Rightarrow \int_G f d\nu = 0$. Pour cela on se donne $f, k \in C_c(G)$ telles que $\overline{k} \equiv 1$ sur $\pi(Supp(f))$ et $\overline{f} = 0$. Il vient alors en appliquant le théorème de Fubini :

$$\begin{aligned}
0 &= \int_G k(g) \int_H f(gh)\mu_H(dh)\nu(dg) \\
&= \int_H \int_G k(g)f(gh)\nu(dg)\mu_H(dh) \\
&= \int_H \Delta_H(h) \int_G k(gh^{-1})f(g)\nu(dg)\mu_H(dh) \\
&= \int_G f(g) \int_H k(gh)\mu_H(dh)\nu(dg) \\
&= \int_G f(g)\nu(dg)
\end{aligned}$$

la dernière égalité résulte du fait que $\overline{k} \equiv 1$ sur $\pi(Supp(f))$.■

Remarque 2.1. *Au lieu d'associer ν/μ_H à ν, le plus naturel serait d'associer la mesure image de ν par la projection canonique $\pi^*\nu$. Mais en général, cette mesure n'est pas de Radon. Cependant lorsque H est compact, elle l'est car le saturé d'un compact est compact, et dans ce cas elle coïncide avec ν/μ_H.*

Corollaire 2.1. *G/H admet une mesure de Radon invariante à gauche par G si et seulement si Δ_H coïncide avec Δ_G sur H. Une telle mesure est unique à multiplication par un scalaire près.*

***Preuve*:** Si G/H admet une mesure invariante μ, alors $\overline{\mu}$ est invariante donc de Haar sur G et de plus vérifie 4, donc Δ_H coïncide avec Δ_G sur H. Réciproquement si l'on suppose que ces deux modules coïncident sur H, alors la mesure de Haar μ_G sur G vérifie 4 et par la proposition précédente s'écrit aussi $\overline{\mu}$ où μ est une mesure de Radon sur G/H. $\overline{\mu}$ est invariante par G donc μ aussi. L'unicité est claire par la proposition précédente.■

Remarque 2.2. *Une application intéressante de ce corollaire est la suivante. Toute mesure de Radon μ sur $\mathbb{R}^n$ $(n \geqslant 2)$ invariante par l'action de $G = SL_n(\mathbb{R})$ est de la forme $c_0\lambda + c_1\delta_0$ (où c_0 et c_1 sont des constantes positives, δ_0 la masse de Dirac en 0 et λ la mesure de Lebesgue). En effet μ se décompose en $c_1\delta_0$ et une mesure de Radon invariante sur $\mathbb{R}^n - \{0\}$. Mais si G_x désigne le stabilisateur d'un point $x \in \mathbb{R}^n - \{0\}$, alors d'après la proposition 1.3., $\mathbb{R}^n - \{0\}$ est homéomorphe à G/G_x car $SL_n(\mathbb{R})$ agit transitivement sur $\mathbb{R}^n - \{0\}$. Mais la mesure de Lebesgue est bien invariante par G (formule de changement de variable). D'après l'unicité de la mesure invariante, on en déduit bien le résultat souhaité.*

2.3. **Mesure de Haar d'un groupe $G = HK$, $H \cap K = 1$.** Dans ce paragraphe, nous allons considérer un groupe localement compact G de la forme HK où H et K sont des sous-groupes fermés de G d'intersection triviale, et nous allons montrer comment la mesure de Haar sur G se déduit de celles sur H et sur K. Pour cela, nous allons faire apparaître G comme un espace homogène. En effet, le groupe produit $H \times K$ agit continûment et transitivement sur G par l'action $(h,k) \cdot g = hgk^{-1}$, et le stabilisateur de l'identité est le sous-groupe trivial $(1,1)$. Nous supposerons de plus que G est dénombrable à l'infini, ce qui permet d'appliquer la proposition 1.3. et d'avoir un homéomorphisme entre l'espace homogène $H \times K$ et le groupe G donné par $\phi : (h,k) \to hk^{-1}$.

Proposition 2.4. *Une mesure de Haar μ_G sur G $(G = HK,\ H \cap K = 1)$ est, à un scalaire près, l'image par ϕ de la mesure $\mu_H \otimes (\Delta_G)^{-1}\mu_K$ sur $H \times K$, où μ_H et μ_K sont des mesures de Haar sur H et K respectivement. De façon équivalente, une fonction mesurable f sur G est intégrable pour μ_G si et seulement si $(h,k) \to f(hk)\Delta_G(k)\Delta_K(k^{-1})$ est intégrable pour $\mu_H \otimes \mu_K$ et dans ce cas,*

$$\int_G f d\mu_G = \alpha \int_{H\times K} f(hk)\Delta_G(k)\Delta_K(k^{-1})\mu_H(dh) \otimes \mu_K(dk) \tag{5}$$

où α est une constante strictement positive indépendante de f.

***Preuve*:** Soit μ l'image de μ_G par ϕ^{-1} et $f \in C_c(H \times K)$. Alors $f \circ \phi^{-1} \in C_c(G)$ et pour tous $h_0 \in H$, $k_0 \in K$, on a :

$$\begin{aligned}\int_{H\times K} f(h_0h, k_0k)d\mu(h,k) = \int_{H\times K} & f \circ \phi^{-1}(h_0\phi(h,k)k_0^{-1})d\mu(h,k) \\ &= \int_G f \circ \phi^{-1}(h_0gk_0^{-1})d\mu_G(g) \\ &= \Delta_G(k_0^{-1}) \int_G f \circ \phi^{-1} d\mu_G \\ &= \Delta_G(k_0^{-1}) \int_{H\times K} f(h,k)d\mu(h,k)\end{aligned}$$

On en déduit que $\mu = \mu_H \otimes (\Delta_G)^{-1} \mu_K$ ce qui prouve la première assertion. Donc f est intégrable sur G si et seulement si $(h,k) \to f(hk^{-1})\Delta_G(k)^{-1}$ est intégrable pour $\mu_H \otimes \mu_K$, ou encore en utilisant 2, si et seulement si $(h,k) \to f(hk)\Delta_G(k)\Delta_K(k)^{-1}$ est intégrable pour $\mu_H \otimes \mu_K$. De façon analogue, on obtient 5.■

Lorsque K est distingué, alors G/K est un groupe localement compact, donc admet une mesure de Haar, qui est par suite G-invariante. D'après le corollaire 2. on déduit que Δ_K et Δ_G coïncident sur K. La formule 5 se simplifie donc et en fait μ_G est l'image de $\mu_H \otimes \mu_K$ par l'application $(h,k) \to hk$. De plus dans ce cas on peut exprimer Δ_G en fonction des données pour H et K.

Proposition 2.5. *On suppose K est distingué (c'est-à-dire $G = HK$, $H \cap K = 1$, est le produit semi-direct H par K). L'image de $\mu_H \otimes \mu_K$ par le produit $(h,k) \to hk$ de $H \times K$ dans G, est une mesure de Haar sur G. Si int_h désigne l'automorphisme intérieur $k \to h^{-1}kh$ de K, alors on a :*

$$\Delta_G(hk) = \Delta_H(h)\Delta_K(k) mod(int_h) \tag{6}$$

***Preuve*:** Il reste à montrer la dernière assertion. Puisque Δ_G est un morphisme et qu'il coïncide avec Δ_K sur K, il suffit de montrer 6 pour $k = 1$. Soit $f \in C_c(G)$, et $\mu_G = \mu_H \otimes \mu_K$, on a

$$\begin{aligned}
\Delta_G(h_0)\int_G f d\mu_G = \int_G f(gh_0^{-1})\mu_G(dg) &= \int_{H\times K} f(hh_0^{-1}h_0kh_0^{-1})\mu_H(dh)\otimes\mu_K(dk) \\
&= mod(int_{h_0})\int_{H\times K} f(hh_0^{-1}k)\mu_H(dh)\otimes\mu_K(dk) \\
&= \Delta_H(h_0)mod(int_{h_0})\int_{H\times K} f(hk)\mu_H(dh)\otimes\mu_K(dk) \\
&= \Delta_H(h_0)mod(int_{h_0})\int_G f d\mu_G
\end{aligned}$$

Cela achève la preuve.■

2.4. Exemples de mesures invariantes.

Nous allons donner ici explicitement les mesures de Haar de certains groupes classiques. Nous en aurons besoin dans la suite.

2.4.1. *Mesure de Haar pour $GL_n(\mathbb{R})$.* On munit l'espace $M_n(\mathbb{R})$ des matrices carrées de taille n de la mesure de Lebesgue en l'identifiant à $\mathbb{R}^{n^2}$. C'est une mesure de Haar pour le groupe additif sous-jacent. Tout $g \in GL_n(\mathbb{R})$ définit un automorphisme du groupe additif de $M_n(\mathbb{R})$ par $M \longmapsto gM$. On vérifie facilement (soit en utilisant la formule de changement de variable, soit en le vérifiant directement pour les transvections et dilatations) que son module est la valeur absolue du déterminant de l'application linéaire définie par cet automorphisme dans $\mathbb{R}^{n^2}$. Enfin, une simple vérification montre que ce déterminant est précisément $(\det g)^n$. $GL_n(\mathbb{R})$ étant un ouvert de $M_n(\mathbb{R})$, on déduit donc :

Proposition 2.6. *Une mesure de Haar sur $GL_n(\mathbb{R})$ est donnée par*

$$\frac{1}{(\det g)^n} \bigotimes_{i,j} dg_{ij}$$

où dg_{ij} représente la mesure de Lebesgue pour la coordonnée g_{ij} de la matrice g.

2.4.2. *Décomposition d'Iwasawa.* Traditionnellement, on note K le groupe des matrices orthogonales, A le groupe des matrices diagonales à coefficients strictement positifs, N le groupe des matrices unipotentes triangulaires supérieures. Rappelons le fait classique suivant :

Théorème 2.2. ***(Décomposition d'Iwasawa)*** *L'application de $K \times A \times N$ sur $GL_n(\mathbb{R})$ donné par la multiplication $(k, a, n) \to kan$ est un homéomorphisme.*

Elle est obtenue en prenant l'orthonormalisé de Schmidt de $g \in GL_n(\mathbb{R})$, ce qui donne $g = kt$ avec t triangulaire supérieure à coefficients diagonaux strictement positifs. Puis on écrit $t = an$. Remarquons que si $e_1, ..., e_n$ désignent les vecteurs colonnes de g, $(c_1, ..., c_n)$ la base orthonormalisée, alors les coefficents de a sont les produits scalaires $(e_i \mid c_i)$ et donc les distances de e_i au sous-espace $Vect(e_1, ..., e_{i-1})$. L'unicité de la décomposition provient de l'unicité de la base orthonormalisée.

Remarque 2.3. *La restriction de cet homéomorphisme à $K^* \times A^* \times N$ (où $K^* = K \cap SL_n(\mathbb{R})$ et $A^* = A \cap SL_n(\mathbb{R})$) est encore un homéomorphisme sur $SL_n(\mathbb{R})$.*

2.4.3. *Mesure de Haar sur A et A^*.* Notons $\mathfrak{a}$ et $\mathfrak{a}^*$ les sous-espaces des matrices diagonales et diagonales de trace nulle respectivement. Les mesure de Haar sur ces groupes additifs sont des multiples de la mesure de Lebesgue. Or, l'exponentielle réalise un isomorphisme bicontinu entre ces groupes additifs et les groupes mutliplicatifs A et A^* respectivement. Elle transporte donc les mesures de Haar. D'où :

Proposition 2.7. *Des mesures de Haar sur A et A^* sont données respectivement par :*

$$\underset{1 \leqslant i \leqslant n}{\otimes} \frac{da_i}{a_i} \quad et \quad \underset{1 \leqslant i \leqslant n-1}{\otimes} \frac{da_i}{a_i}$$

où les a_i sont les coefficients diagonaux de la matrice et da_i est la restriction de la mesure de Lebesgue à $\mathbb{R}_+^*$.

Remarquons enfin que A et A^* sont unimodulaires parce qu'abéliennes.

2.4.4. *Mesure de Haar sur N.* On procède ici exactement comme pour $GL_n(\mathbb{R})$. L'application de N sur $\mathbb{R}^{\frac{n(n-1)}{2}}$ donnée par $n \to (n_{ij})_{i<j}$ est un homéomorphisme. On vérifie de plus que la multiplication à gauche ou à droite par un élément de N définit un automorphisme de $\mathbb{R}^{\frac{n(n-1)}{2}}$ de module 1 pour le groupe additif de $\mathbb{R}^{\frac{n(n-1)}{2}}$ muni de la mesure de Lebesgue. Il s'ensuit que l'image de la mesure de Lebesgue par l'homéomorphisme réciproque est une mesure de Haar biinvariante sur N, soit :

Proposition 2.8. *Une mesure de Haar sur N est donnée par*

$$\underset{i<j}{\otimes} dn_{ij}$$

où dn_{ij} représente la mesure de Lebesgue pour la coordonnée n_{ij} de la matrice $n \in N$.

2.4.5. *Mesure de Haar sur $SL_n(\mathbb{R})$.* Nous allons maintenant recueillir le fruit de notre travail en utilisant les résultats ci-dessus avec ceux de la section précédente pour expliciter une mesure de Haar sur $SL_n(\mathbb{R})$. Notons $G = SL_n(\mathbb{R})$, $B^* = A^*N$ puis μ_{K^*}, μ_{A^*}, μ_N et μ_{B^*} respectivement des mesures de Haar sur K^*, A^*, N et B^*. On a $G = K^*B^*$. On a vu que les groupes G, K^*, A^* et N sont unimodulaires. On peut alors exprimer la proposition 2.4. en disant qu'une mesure de Haar sur G s'identifie à l'image de $\mu_{K^*} \otimes (\Delta_{B^*})^{-1}\mu_{B^*}$ par $(k, b) \to kb$.

Pour connaître μ_{B^*}, on procède de même. On remarque que N est distingué dans B^*, ce qui permet d'appliquer la proposition 2.5. et de déduire que l'on peut choisir pour μ_{B^*}

la mesure image de $\mu_{A^*} \otimes \mu_N$ par $(a, n) \to an$. La deuxième partie de cette proposition permet d'affirmer que $\Delta_{B^*}(an) = mod(int_a)$. Mais d'après le calcul de la mesure de Haar sur N, ce module est la valeur absolue du déterminant de l'automorphisme qu'induit la conjugaison par a sur $\mathbb{R}^{\frac{n(n-1)}{2}}$. Une vérification immédiate (considérer les matrices de la base canonique de $M_n(\mathbb{R}^n)$) montre que ce déterminant est

$$\rho(a) = \prod_{i<j} \frac{a_i}{a_j}$$

lorsque a est la matrice diagonale de coefficients a_i. On a donc démontré la

Proposition 2.9. *Une mesure de Haar μ_G sur $SL_n(\mathbb{R})$ est donnée par l'image de la mesure $\mu_{K^*} \otimes \rho\mu_{A^*} \otimes \mu_N$ par l'homéomorphisme de la décomposition d'Iwasawa. Ainsi pour toute fonction f à support compact sur $SL_n(\mathbb{R})$, on a :*

$$\int_{SL_n(\mathbb{R})} f d\mu_G = \int_{K^* \times A^* \times N} \rho(a) f(kan) \mu_{K^*}(dk) \otimes \mu_{A^*}(da) \otimes \mu_N(dn)$$

2.5. **Sous groupes discrets et réseaux.** Dans le cas où H est un groupe discret, nous allons préciser les résultats obtenus dans les paragraphes précédents.

Proposition 2.10. *Supposons que G est unimodulaire et Γ est un sous-groupe discret de G. Alors G/Γ admet une mesure de Radon G-invariante à gauche. Elle est unique à un scalaire près.*

***Preuve*:** C'est clair par le corollaire 2.1. puisque Γ et G sont unimodulaires (Γ est discret, donc unimodulaire).■

Remarque 2.4. *Si G n'est pas unimodulaire, on montre que G/Γ admet une mesure relativement invariante de caractère Δ_G (i.e. $\mu(gA) = \Delta_G(g)\mu(A)$).*

Définition 2.2. *Un sous-groupe discret Γ de G est appelé un* ***réseau*** *de G si G/Γ admet une mesure de Radon G-invariante à gauche finie.*

Proposition 2.11. *Si G possède un réseau Γ, alors G est unimodulaire.*

***Preuve*:** D'après le corollaire 3. Δ_Γ coïncide avec Δ_G sur Γ. Puisque Γ est discret, $\Delta_\Gamma = 1$, $\Gamma \subset \ker \Delta_G$. Si ν est la mesure invariante sur G/Γ, p la projection canonique $G/\ker \Delta_G$ et $p^*\nu$ la mesure image de ν sur $G/\ker \Delta_G$ qui est un groupe, $p^*\nu$ est G-invariante et finie car ν l'est. Il en résulte que $\Delta_G(G) \cong G/\ker \Delta_G$ est un groupe compact (cf. 2.1.1.) de $\mathbb{R}_+^*$, donc est trivial. Ainsi $G = \ker \Delta_G$ et G est unimodulaire.■

Proposition 2.12. *Si Γ est discret et G/Γ compact, alors Γ est un réseau. Dans ce cas Γ est appelé réseau uniforme.*

***Preuve*:** G/Γ admet une mesure de Radon μ relativement invariante de module Δ_G qui est finie car G/Γ est compact. D'où $\mu(G/\Gamma) = \Delta_G(g)\mu(G/\Gamma)$ pour tout g dans G, c'est-à-dire que $\Delta_G = 1$. Donc μ est en fait G-invariante à gauche et finie. Γ est donc un réseau.■

Ce qui suit va permettre de préciser la mesure invariante sur l'espace quotient G/Γ d'un réseau Γ et en particulier de la relier à l'intégration sur un domaine fondamental par rapport à la mesure de Haar sur G.

Définition 2.3. *Soit Γ un groupe discret. On appelle* ***domaine fondamental*** *tout borélien F tel que la restriction à F de la projection canonique $\pi : G \to G/\Gamma$ soit bijective.*

Proposition 2.13. *Soit Γ un réseau de G, μ_G une mesure de Haar sur G, m la mesure de comptage sur Γ (qui est une mesure de Haar), et $\nu = \mu_G/m$ la mesure G-invariante associée sur G/Γ. Soit A un borélien tel que $\pi(A) = G/\Gamma$ où π est la projection canonique. Alors pour tout f positive mesurable sur G/Γ on a :*

$$\int_{G/\Gamma} f d\nu \leqslant \int_A (f \circ \pi)\, d\mu_G \tag{7}$$

Si A est un domaine fondamental, alors pour tout $f \in L^1(G/\Gamma)$, $f \circ \pi$ est intégrable sur A et,

$$\int_{G/\Gamma} f d\nu = \int_A (f \circ \pi)\, d\mu_G \tag{8}$$

***Preuve*:** Supposons f positive et mesurable sur G/Γ.

$$\begin{aligned}\int_G 1_A\,(f \circ \pi)\, d\mu_G &= \int_{G/\Gamma}\int_\Gamma 1_A(x\gamma) f \circ \pi(x\gamma) dm(\gamma) d\nu(\dot{x}) \\ &= \int_{G/\Gamma} f(\dot{x}) \int_\Gamma 1_A(x\gamma) dm(\gamma) d\nu(\dot{x})\end{aligned}$$

Etant donné que $\pi(A) = G/\Gamma$, pour tout x de G, il existe au moins un γ dans Γ tel que $x\gamma \in A$, d'où 7, et il en existe un seul si A est un domaine fondamental, d'où 8 lorsque f est positive. Pour f dans $L^1(G/\Gamma)$ il suffit de prendre les parties positives et négatives de f.■

Remarque 2.5. *Lorsque G est dénombrable à l'infini, alors Γ est au plus dénombrable et par conséquent $\int_\Gamma dm = \sum_{\gamma \in \Gamma}$.*

Enfin, on a la proposition suivante qui nous sera utile dans la suite:

Proposition 2.14. *On suppose G à base dénombrable d'ouverts et on se donne H un sous-groupe fermé de G et Γ un réseau de G. Si $H \cap \Gamma$ est aussi un réseau de H alors $H\Gamma$ est fermé dans G, de façon équivalente, l'orbite de Γ dans G/Γ par l'action à gauche de H est fermée, ou encore l'injection canonique*

$$H/H \cap \Gamma \to G/\Gamma$$

est propre.

La preuve résulte du lemme suivant :

Lemme 2.1. *On suppose G à base dénombrable d'ouverts et on se donne un réseau Γ de G. Une suite (x_n) de G/Γ n'admet pas de valeur d'adhérence si et seulement s'il existe une suite (γ_n) d'éléments de G distincts de l'identité et une suite (g_n) dans G telles que $g_n\Gamma = x_n$ et*

$$g_n \gamma_n g_n^{-1} \underset{n\to\infty}{\to} id$$

***Preuve*:** Notons π la projection canonique de G sur G/Γ. Supposons l'existence des suites (γ_n) et $(g_n)_n$ correspondant à (x_n) et supposons de plus, par l'absurde, que (x_n) ait une valeur d'adhérence. Considérons une sous-suite convergente vers $x = \pi(g) \in G/\Gamma$, que l'on note encore (x_n). En repassant dans G, cela signifie qu'il existe une suite $\gamma_n' \in \Gamma$, telle que $g_n\gamma_n' \to g$. Il vient alors, $\gamma_n'\gamma_n\gamma_n'^{-1} \to id$. Puisque Γ est discret, cette suite est stationnaire. On en déduit que γ_n est aussi stationnaire, ce qui contredit l'hypothèse faite sur les γ_n.

Réciproquement, supposons que (x_n) est une suite quelconque de G/Γ sans valeur d'adhérence. Puisque G a une base dénombrable d'ouverts, on peut se munir d'une suite croissante de compacts (K_p) de G telle que $\bigcup K_p = G$, ainsi que d'une base de voisinages compacts U_p de id telle que

$$\mu_G(U_p) > \nu(G/\Gamma - \pi(K_p))$$

où l'on a noté ν la probabilité G-invariante sur G/Γ et μ_G la mesure de Haar sur G correspondante (i.e. telle que $\nu = \mu_G/m$). C'est possible car $\varepsilon_p = \nu(G/\Gamma - \pi(K_p)) \to 0$. Notons $V_p = U_p^{-1}U_p$. C'est encore une base de voisinages compacts de id. Donc $\pi(V_pK_p)$ est compact, et d'après l'hypothèse faite sur (x_n), pour tout p, il existe un rang n_p tel que $n \geq n_p$ entraîne

$$x_n \notin \pi(V_pK_p) \Leftrightarrow U_p \cdot x_n \cap U_p \cdot \pi(K_p) \neq \emptyset$$

Il en résulte $U_p \cdot x_n \subseteq G/\Gamma - \pi(K_p)$, puis $\nu(\pi(U_pg_n)) = \nu(U_p \cdot x_n) \leq \varepsilon_p$. Or $\mu_G(U_pg_n) = \mu_G(U_p) < \varepsilon_p$. Par suite

$$\nu(\pi(U_pg_n)) < \mu_G(U_pg_n)$$

En revenant à la définition de ν, cette inégalité s'écrit aussi,

$$\int_{G/\Gamma} \left(\sum_{\gamma\in\Gamma} 1_{U_pg_n}(g\gamma) - 1_{\pi(U_pg_n)}(\dot{g}) \right) d\nu(\dot{g}) > 0$$

On en déduit l'existence d'un $u_n^p \in U_p$ et d'un $\gamma_n^p \in \Gamma$, $\gamma_n^p \neq id$, tels que $u_n^p g_n \gamma_n^p \in U_pg_n$, d'où pour tout $n \geq n_p$

$$g_n\gamma_n^p g_n^{-1} \in V_p$$

On peut choisir $(n_p)_p$ strictement croissante en p et poser $\gamma_n = \gamma_n^p$ si $n_p \leq n < n_{p+1}$. Puisque les V_p forment une base de voisinage de id, on voit que la suite (γ_n) convient.■

***Preuve* de la proposition:** Soit $h_n\gamma_n$ une suite de $H\Gamma$ qui converge vers un certain point $g \in G$. Soit γ'_n une suite de $\Gamma - \{id\}$ comme dans le lemme, telle que $h_n\gamma'_n h_n^{-1} \to id$. Il vient $\gamma_n^{-1}\gamma'_n\gamma_n \to id$, donc cette suite stationne en l'identité, ce qui est impossible d'après l'hypothèse faite sur (γ'_n). Le lemme affirme donc l'existence d'une valeur d'adhérence pour la suite $\pi(h_n)$ dans $H/(H \cap \Gamma)$. Il existe donc $h \in H$, et une sous-suite h_{n_k} telle que $h_{n_k}\gamma''_k \underset{k\to\infty}{\to} h$ pour une certaine suite $\gamma''_k \in \Gamma$. Par hypothèse $h_{n_k}\gamma_{n_k} \underset{k\infty}{\to} g$. On en déduit $g \in h\Gamma \subseteq H\Gamma$, ce qu'il fallait démontrer.■

3. Groupes algébriques

3.1. Définitions et propriétés de base.

3.1.1. *Définitions.* Soit k un corps algébriquement clos. On appelle **groupe linéaire algébrique** (ou simplement dans la suite groupe algébrique), une variété algébrique affine G sur k, munie d'une structure de groupe telle que la multiplication et l'inversion soient des morphismes de variétés algébriques affines, ou plus brièvement, des **morphismes algébriques**. On peut toujours plonger une variété algébrique affine dans k^n, mais dans nos applications, G sera déjà un sous-ensemble de k^n constitué des zéros d'une famille de polynômes de $k[X_1, ..., X_n]$. Dire que la multiplication et l'inversion sont des morphismes algébriques, c'est dire que les coordonnées de xy ou x^{-1} $(x, y \in G)$ dans k^n sont des fonctions polynômiales des coordonnées de x et y. Dans ce cas, on note $I(G)$ l'idéal de $k[X_1, ..., X_n]$

formé des polynômes qui s'annulent sur G. On note aussi $k[G] = k[X_1, ..., X_n]/I(G)$ l'anneau des **fonctions régulières** sur G. On munit G de la **topologie de Zariski** héritée de sa structure de variété algébrique affine. Les fermés de G sont les ensembles de zéros d'une famille de fonctions régulières. Un fermé de G est dit **irréductible** s'il n'est pas réunion de deux fermés distincts de lui-même. Un morphisme de groupes algébriques est un morphisme de groupes qui est aussi un morphisme algébrique. Une **représentation** linéaire de G dans un k-espace vectoriel V est dite **algébrique,** ou rationnelle, si $\rho : G \to GL(V)$ est un morphisme de groupes algébriques. Rappelons quelques propriétés importantes (cf. [Hum]) :

1. Tout sous-groupe fermé de G est un groupe algébrique.
2. Tout groupe algébrique admet un plongement dans $GL_n(k)$ pour un certain entier n (ce plongement est obtenu comme une sous-représentation de la représentation régulière gauche $f \mapsto (h \mapsto f(gh))$ pour $f \in k[G]$).
3. G a un nombre fini de composantes irréductibles et celles-ci coïncident avec ses composantes connexes.

3.1.2. *Eléments semi-simples et unipotents ; décomposition de Jordan.*

Définition 3.1. *Un élément $g \in G$ est appelé semi-simple (resp. unipotent) si pour toute représentation algébrique de dimension finie de G, la matrice de g est diagonalisable (resp. unipotente).*

On a alors le théorème suivant, qui généralise la décomposition de Jordan-Dunford dans $GL_n(k)$, (cf. [Hum]) :

Théorème 3.1. *Soit G un groupe algébrique sur k, et $g \in G$. Alors il existe un unique couple $(g_s, g_u) \in G^2$, avec g_s semi-simple et g_u unipotent, tel que $g = g_s g_u = g_u g_s$.*

En particulier, si G est un sous-groupe algébrique de $GL_n(k)$ et $g \in G$, on voit que g_s et g_u sont respectivement des matrices diagonalisable et unipotente, et par conséquent coïncident avec les matrices obtenues par la décomposition de Jordan-Dunford usuelle dans $GL_n(k)$, d'après l'unicité de celle-ci. Donc, par exemple, toute matrice unipotente de G est un élément unipotent de G.

Comme conséquence évidente de la définition, il nous faut remarquer la proposition suivante.

Proposition 3.1. *Soit ρ un morphisme de groupes algébriques $G_1 \to G_2$. Alors l'image par ρ d'un élément semi-simple (resp. unipotent) est semi-simple (resp. unipotent).*

3.1.3. *Groupes algébriques réels et complexes.* Lorsque $k = \mathbb{C}$, G est un groupe algébrique complexe. On appelle **$\mathbb{R}$-groupe**, tout sous-groupe G Zariski fermé dans $GL_n(\mathbb{C})$ et **défini sur** $\mathbb{R}$, c'est-à-dire tel que $I(G)$ est engendré par des polynômes à coefficients réels. On appelle **groupe algébrique réel** tout groupe $G_{\mathbb{R}}$ de la forme $G \cap GL_n(\mathbb{R})$ où G est un $\mathbb{R}$-groupe.

Tout groupe algébrique complexe est une variété algébrique affine non-singulière, et possède donc une structure de variété différentiable. Par suite, tout groupe algébrique complexe est aussi un groupe de Lie complexe. De même tout groupe algébrique réel est un groupe de Lie réel. La proposition suivante dit que les composantes irréductibles (ou Zariski connexes, d'après 3.1.1.3.) d'un groupe algébrique coïncident avec les composantes connexes de sa topologie de groupe de Lie (cf. [OnV] thm 3.3.1.) :

Proposition 3.2. *Soit G un groupe algébrique réel ou complexe. Les composantes neutres de la topologie de Zariski et de la topologie de groupe de Lie coïncident.*

Ceci permet de parler de l'algèbre de Lie d'un groupe algébrique réel ou complexe.

3.2. **Actions algébriques.** Soit X une variété algébrique et G un groupe algébrique sur k, algébriquement clos. Une action de G sur X est dite algébrique si l'application associée $G \times X \to X$ est un morphisme de variétés algébriques.

L'intérêt essentiel des actions algébriques pour les systèmes dynamiques réside dans la propriété suivante :

Théorème 3.2. *Les orbites d'une action algébrique sont localement fermées pour la topologie de Zariski.*

Ceci résulte immédiatement du théorème de Chevalley qui affirme que l'image d'un morphisme de variétés contient un ouvert de son adhérence (cf. [Hum]).

En particulier, on voit que si G est un groupe algébrique complexe agissant sur une variété algébrique compexe non-singulière, les orbites sont des sous-variétés différentiables et la bijection induite $G/G_x \overset{\phi_x}{\to} G \cdot x$ est *toujours un difféomorphisme* (cf. prop. 1.3., la topologie de Zariski est moins fine que la topologie usuelle, donc les orbites sont aussi localement fermées pour la topologie usuelle). On évite ainsi les complications qui apparaissent pour les actions des groupes de Lie quelconques, comme l'enroulage dense d'un sous-groupe immergé du tore...

Dans la suite, nous serons amenés à considérer une action algébrique d'un groupe algébrique réel sur un $\mathbb{R}$-espace vectoriel. Soit X un fermé de Zariski de $\mathbb{C}^n$ défini sur $\mathbb{R}$, et $X_{\mathbb{R}} = X \cap \mathbb{R}^n$ l'ensemble de ses points $\mathbb{R}$-rationnels. On considère une $\mathbb{R}$-action d'un $\mathbb{R}$-groupe G sur X (c'est-à-dire une action algébrique définie sur $\mathbb{R}$, i.e. donnée par des polynômes à coefficients réels). On note $G_{\mathbb{R}}$ le groupe algébrique réel associé à G ; il agit sur $X_{\mathbb{R}}$. Le théorème précédent est en défaut car $\mathbb{R}$ n'est pas algébriquement clos (considérer par exemple l'action à gauche de $\mathbb{R}^*$ sur lui-même $g \cdot x = g^2 x$). Cependant, le résultat suivant reste valide :

Théorème 3.3. *Les orbites de $G_{\mathbb{R}}$ dans $X_{\mathbb{R}}$ sont localement fermées pour la topologie usuelle de $\mathbb{R}^n$.*

***Preuve*:** Soit $x \in X_{\mathbb{R}}$. Puisque $G \cdot x$ est localement fermé dans $\mathbb{C}^n$, il suffit de montrer que $G_{\mathbb{R}} \cdot x$ est ouvert dans $G \cdot x \cap \mathbb{R}^n$, puis, par translation, que $G_{\mathbb{R}} \cdot x$ contient un ouvert de $G \cdot x \cap \mathbb{R}^n$. Soit H le stabilisteur de x dans G. On note $\mathfrak{g}$, $\mathfrak{h}$, $\mathfrak{g}_{\mathbb{R}}$ et $\mathfrak{h}_R$ les algèbres de Lie de G, H, $G_{\mathbb{R}}$ et $H_{\mathbb{R}}$ ($\mathfrak{g}_{\mathbb{R}} = Re\mathfrak{g}$ et $\mathfrak{h}_{\mathbb{R}} = Re\mathfrak{h}$). Il existe alors un sous-espace supplémentaire $\mathfrak{p}$ de $\mathfrak{h}$ dans $\mathfrak{g}$ tel que l'espace tangent T_x à $G \cdot x$ en x soit $\mathfrak{p} \cdot x$. De plus $G_{\mathbb{R}} \cdot x$ est une sous-variété immergée de $\mathbb{R}^n$ dont l'espace tangent T'_x en x est $\mathfrak{p}_{\mathbb{R}} \cdot x$. D'autre part, puisque G est un $\mathbb{R}$-groupe et $x \in X_{\mathbb{R}}$, $\mathfrak{g}$ et $\mathfrak{h}$ sont stables par conjugaison complexe, et donc $\mathfrak{p}$ aussi. Il en résulte que $\mathfrak{g} = \mathfrak{g}_{\mathbb{R}} \oplus i\mathfrak{g}_{\mathbb{R}}$ et $\mathfrak{p} = \mathfrak{p}_{\mathbb{R}} \oplus i\mathfrak{p}_{\mathbb{R}}$. Donc $\mathfrak{p}_{\mathbb{R}} = \mathfrak{p} \cap \mathbb{R}^n$, d'où $T'_x = T_x \cap \mathbb{R}^n$. Par suite, $G_{\mathbb{R}} \cdot x$ contient un ouvert de $G \cdot x \cap \mathbb{R}^n$.■

Par conséquent, la proposition 3.1. s'applique encore, si bien que les orbites d'un groupe algébrique réel sur l'ensemble des $\mathbb{R}$-points d'une variété algébrique complexe non-singulière sont bien des sous-variétés différentiables et la bijection induite $G/G_x \overset{\phi_x}{\to} G \cdot x$ est un difféomorphisme.

3.3. **Le théorème de densité de Borel.** Dans ce paragraphe, nous allons donner la preuve de H. Furstenberg (cf. [Fus]) du "théorème de densité de Borel", remarquable par sa simplicité et son élégance.

Tout d'abord, nous dirons qu'un groupe localement compact a la **propriété (map)** si tout homomorphisme continu de G dans un groupe compact est trivial (en anglais, *minimally almost periodic*). En particulier, tout groupe de Lie semi-simple connexe sans facteur compact (i.e. sans sous-groupe de Lie distingué dont le quotient est compact) a la propriété (map) car l'image par un homomorphisme continu d'un groupe semi-simple dans un groupe de Lie est fermée. On remarque aussi qu'un groupe qui a la propriété (map) n'a pas de sous-groupe propre H d'indice fini, puisque le passage au quotient définirait un homomorphisme continu non trivial de G dans l'ensemble (fini!) des permutations de G/H.

Le théorème principal est le suivant :

Théorème 3.4. *Soit G un groupe localement compact ayant la propriété (map) et H un sous-groupe fermé de G tel que G/H possède une probabilité G-invariante. Soit ρ une représentation continue de G dans un espace V de dimension finie. Alors tout sous-espace de V invariant par $\rho(H)$ est invariant par $\rho(G)$.*

On en déduit le

Corollaire 3.1. ***(théorème de densité de Borel)*** *Soit G un groupe de Lie algébrique réel, semi-simple, connexe et sans facteur compact. Alors tout réseau Γ de G est Zariski-dense dans G.*

***Preuve* du corollaire:** Soit L l'adhérence de Zariski de Γ. C'est un sous-groupe de G, car G est algébrique. Soit L_0 sa composante neutre (cf. 3.1.3.) et $\mathfrak{l}$ son algèbre de Lie. Comme L_0 est distingué dans L (cf. §1.3.2.), donc Γ normalise L_0 et par suite ad_Γ laisse $\mathfrak{l}$ invariante. G a la propriété (map) puisqu'il est semi-simple et sans facteur compact. De plus, G/Γ possède une probabilité G-invariante car Γ est un réseau. On peut donc appliquer le théorème à la représentation adjointe de G et au sous-groupe Γ laissant invariant $\mathfrak{l}$. Il s'ensuit que ad_G laisse $\mathfrak{l}$ invariante et donc L_0 est distingué dans G.

Puisque Γ est un réseau de G, G/Γ possède une mesure G-invariante finie et donc, par projection, G/L aussi. Comme L est algébrique L_0 est d'indice fini dans L, donc G/L_0 possède aussi une mesure G-invariante finie. Mais comme la mesure de Haar sur G/L_0 est finie, d'après §2.1.1. il s'ensuit que le groupe G/L_0 est compact. Enfin, la propriété (map) entraîne que $L_0 = L = G$. Donc Γ est Zariski-dense dans G.■

Remarque 3.1. *On peut aussi voir ce corollaire comme conséquence directe du théorème ci-dessus et du théorème de Chevalley qui affirme l'existence d'une représentation rationnelle dans laquelle L est le stabilisateur d'une droite.*

Passons à la preuve du théorème. Elle s'appuit essentiellement sur le lemme suivant :

Lemme 3.1. *Soit G un groupe localement compact qui possède la propriété (map). Soit ρ une représentation de G dans un espace vectoriel réel E de dimension finie. Soit $\overline{\rho}$ la représentation induite dans l'espace projectif $\mathbb{P}(E)$. Si $\overline{\rho}(G)$ préserve une mesure finie μ sur $\mathbb{P}(E)$, alors les points du support de μ sont $\overline{\rho}(G)$-invariants.*

***Preuve*:** $\rho(G)$ n'est pas relativement compact, à moins qu'il ne soit trivial. On peut donc supposer ρ non triviale et trouver une suite (g_p) de G telle que $\overline{\rho}(g_p)$ converge vers un élément π de $\mathbb{P}(End(E))$ (compact!) qui n'est pas inversible. Notons $\ker \pi$ et $Im\pi$ les noyau et image dans E d'un représentant de π (indépendant du choix de ce représentant dans $End(E)$). Quitte à extraire une sous-suite, on peut supposer que $E_1 = \lim_{p\to\infty} \rho(g_p)(\ker \pi)$ existe. On pose $E_2 = Im\pi$. E_1 et E_2 sont deux sous-espaces distincts de E. Si $x \in \mathbb{P}(\ker \pi)$ alors toute valeur d'adhérence de $\overline{\rho}(g_p)(x)$ quand $p \to \infty$ se situe dans $\mathbb{P}(E_1)$. Inversement, si $x \notin \mathbb{P}(\ker \pi)$, alors $\overline{\rho}(g_p)(x) \to \pi(x) \in \mathbb{P}(E_2)$.

Par suite, si ϕ est une fonction à support compact inclus dans $\mathbb{P}(E) - (\mathbb{P}(E_1) \cup \mathbb{P}(E_2))$, alors $\phi \circ \overline{\rho}(g_p)(x) \to 0$ pour tout $x \in \mathbb{P}(E)$. Par convergence dominée et invariance de μ, on obtient

$$\int_{\mathbb{P}(E)} \phi d\mu = \int_{\mathbb{P}(E)} \phi \circ \overline{\rho}(g_p) d\mu \to 0 \text{ donc } \int_{\mathbb{P}(E)} \phi d\mu = 0$$

C'est-à-dire $Supp(\mu) \subseteq \mathbb{P}(E_1) \cup \mathbb{P}(E_2)$, réunion de deux sous-variétés linéaires projectives propres de $\mathbb{P}(E)$. Par noethérianité, il existe X minimal, qui contienne $Supp(\mu)$ et qui soit réunion finie de sous-variétés linéaires projectives. Puisque μ est invariante par $\overline{\rho}(G)$, tout élément de $\overline{\rho}(G)$ doit permuter les composantes irréductibles de X (i.e. les sous-variétés linéaires projectives qui composent X). Le stabilisateur dans $\overline{\rho}(G)$ de l'une de ces composantes est un sous-groupe d'indice fini de $\overline{\rho}(G)$ donc est le groupe tout entier, vu que G n'a pas de sous-groupe d'indice fini en raison de la propiété (map). Donc tout élément $\overline{\rho}(g)$ stabilise chaque composante de X. Soit F un sous-espace de E correspondant à une composante. Il s'agit de montrer que la restriction de $\overline{\rho}(G)$ à $\mathbb{P}(F)$ est triviale. Raisonnons par l'absurde. Comme $\dim F < \dim E$, le même raisonnement que ci-dessus appliqué à F et aux restrictions de $\overline{\rho}(G)$ et μ à $\mathbb{P}(F)$ met en évidence l'existence d'une réunion finie Y de sous-variétés linéaires projectives propres de $\mathbb{P}(F)$ qui pourrait remplacer $\mathbb{P}(F)$ dans la décomposition de X (car $Supp(\mu) = \bigcup\limits_i Supp(\mu_{|F_i})$ si les F_i sont les composantes de X). Cela contredit la minimalité de X.■

***Preuve* du théorème:** Soit W un sous-espace de V fixé par $\rho(H)$. On considère la représentation $\Lambda^r\rho$ induite par ρ sur $\Lambda^r V$, où $r = \dim W$. H fixe donc une droite de $\Lambda^r V$, puis en passant au projectif, un point de $\mathbb{P}(\Lambda^r V)$ soit w. En passant au quotient, on définit donc une application continue G-équivariante $G/H \to \mathbb{P}(\Lambda^r V)$. L'image de la probabilité G-invariante sur G/H fournit une probabilité G-invariante μ sur $\mathbb{P}(\Lambda^r V)$. Clairement, $w \in Supp(\mu)$. Le lemme précédent s'applique et montre que w est invariant par G, c'est-à-dire que W est invariant par $\rho(G)$.■

4. Réseaux de $\mathbb{R}^n$

4.1. **L'espace des réseaux.** On appelle **réseau** d'un $\mathbb{R}$-espace vectoriel $\mathbb{E}$ de dimension n tout sous-groupe additif discret de $\mathbb{E}$ dont le sous-espace vectoriel engendré est $\mathbb{E}$ tout entier. On montre que les réseaux de $\mathbb{E}$ sont précisément les parties de la forme $\mathbb{Z}e_1 \oplus ... \oplus \mathbb{Z}e_n$ où $(e_1, ..., e_n)$ est une base de $\mathbb{E}$ (cf. [reseau]). Plus généralement, pour tout sous-groupe additif G de $\mathbb{E}$, il existe une décomposition $U \oplus V$ de $Vect(G)$ en deux sous-espaces supplémentaires telle que $G \cap U$ soit un réseau de U, et $G \cap V$ soit dense dans V. Etant donné un réseau Δ, toute base $(e_1, ..., e_n)$ de $\mathbb{E}$ telle que $\mathbb{Z}e_1 \oplus ... \oplus \mathbb{Z}e_n = \Delta$ est appelée **base de** Δ. L'ensemble $[0,1[e_1 + ... + [0,1[e_n$ est appelé un **domaine fondamental de** Δ, parce que c'est un systeme de représentants du quotient $\mathbb{E}/\Delta$. Ce quotient est de mesure de Lebesgue finie et donc les réseaux de $\mathbb{E}$ sont aussi les réseaux du groupe topologique $(\mathbb{E}, +)$ au sens de la section précédente. On passe d'une base de Δ à une autre par une transformation linéaire dont la matrice dans ces bases appartient à $GL_n(\mathbb{Z})$. Ainsi le module du déterminant d'une base de Δ ne dépend pas de la base, on note $\det(\Delta)$ cette valeur commune qu'on appelle **déterminant** de Δ. On appelle **sous-réseau** de Δ tout sous-groupe de Δ. La proposition suivante précise la structure des sous-réseaux d'un réseau Δ et résulte du théorème de structure des modules sur un anneau principal (cf. [Sam]) :

Proposition 4.1. *Si Γ est un sous-réseau de Δ, il existe une base de Δ, $(e_1, ..., e_n)$ et des entiers $a_1, ..., a_r$ $(r \leq n)$, uniques au signe près tels que $a_1 \mid ... \mid a_r$ et $\Gamma = \mathbb{Z}a_1e_1 \oplus ... \oplus \mathbb{Z}a_re_r$.*

On dit que Δ est **unimodulaire** si $\det(\Delta) = 1$. On note X l'ensemble des réseaux unimodulaires de $\mathbb{R}^n$. $SL_n(\mathbb{R})$ agit naturellement sur X en associant à tout réseau son image. Cette action est transitive et par conséquent passe au quotient ; fournissant une bijection entre X et l'espace homogène $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$: à chaque $g \in SL_n(\mathbb{R})$ est associé le réseau $g(\mathbb{Z}^n)$.

4.2. **Géométrie des nombres.**

4.2.1. *Deux théorèmes de Minkowski.* Rappelons le théorème de Minkowski qui est à l'origine de la "géométrie des nombres" (voir [Cas] ou [Sam]).

Théorème 4.1. *Soit Δ un réseau de $\mathbb{R}^n$ et C un sous-ensemble convexe, mesurable par rapport à la mesure de Lebesgue λ et symétrique par rapport à 0. Si $\lambda(C) > 2^n \det(\Delta)$ ou si $\lambda(C) \geqslant 2^n \det(\Delta)$ et C compact, alors C contient un point non nul de Δ.*

Ceci permet de déterminer si un sous-ensemble de $\mathbb{R}^n$ contient un point non trivial de Δ. Mais on a parfois besoin de savoir si ce sous-ensemble contient un domaine fondamental tout entier de Δ. Pour cela, on introduit les **minima successifs** associés au réseau Δ. On note $\lambda_1 = \min(\|x\|, x \in \Delta \backslash \{0\})$ où $\|\cdot\|$ désigne la norme euclidienne canonique de $\mathbb{R}^n$, et on choisit un vecteur e_1 de Δ de norme λ_1. Puis λ_i et e_i étant construits, on définit $\lambda_{i+1} = \min(\|x\|, x \in \Delta \backslash vect(e_1, ..., e_i))$ et on choisit un vecteur e_{i+1} de Δ de norme λ_{i+1}. Les nombres $\lambda_1 \leqslant ... \leqslant \lambda_n$ sont appelés les minima successifs de Δ. Les e_i forment donc une base de Δ. On a alors le théorème suivant dû également à Minkowski :

Théorème 4.2. *Soit $\lambda_1 \leqslant ... \leqslant \lambda_n$ les minima successifs d'un réseau Δ. Alors, on a l'encadrement :*

$$\det(\Delta) \leqslant \lambda_1 \cdot ... \cdot \lambda_n \leqslant \det(\Delta) \times \frac{2^n}{V_n}$$

où V_n désigne le volume de la boule euclidienne unité de $\mathbb{R}^n$.

***Preuve*:** Soit M la matrice dont les vecteurs colonnes sont les coordonnées des vecteurs de base $e_1, ..., e_n$. Comme déjà évoqué pour la décomposition d'Iwasawa (cf. 2.4.2.), on prend l'orthonormalisé de Schmidt de cette base. Cela fournit une matrice orthonormale O et une matrice triangulaire supérieure T (on a $M = OT$), dont les coefficients diagonaux sont les distances euclidiennes de e_i à $vect(e_1, ..., e_{i-1})$. Ceci fournit déjà l'inégalité de gauche, qui est l'inégalité classique d'Hadamard. Ensuite, remarquons que par définition des minima successifs, si X est un vecteur à coordonnées entières dont la $i-ème$ coordonnée x_i est non nulle, alors $\|MX\| = \|TX\| \geqslant \lambda_i$. On en déduit que si D est la matrice diagonale de coefficients $\lambda_1, ..., \lambda_n$, alors pour tout X, vecteur non nul à coordonnées entières, $\|D^{-1}TX\| \geqslant 1$. Le théorème précédent montre alors que $V_n \leqslant 2^n \left|\det(D^{-1}T)\right|$, ce qui est précisément l'inégalité de droite.■

Ce théorème permet en particulier de majorer λ_n et donc de trouver une boule dans laquelle il y a un domaine fondamental de Δ. Nous aurons aussi besoin de compter le nombre de points d'un réseau dans une boule de $\mathbb{R}^n$.

4.2.2. *Nombre de points d'un réseau dans la boule unité.* Pour cela, nous aurons besoin des définitions suivantes.

Définition 4.1. *Un sous-espace F de $\mathbb{R}^n$ est dit Δ-rationnel si $F \cap \Delta$ est un réseau de F. Nous noterons $\alpha_0(\Delta) = 1$ et pour $i \geqslant 1$:*

$$\alpha_i(\Delta) = \sup \left\{ \frac{1}{\det_F(F \cap \Delta)} \mid F \text{ sous-espace } \Delta - \text{rationnel de dim } i \right\}$$

$$\alpha(\Delta) = \max_{0 \leqslant i \leqslant n} \alpha_i(\Delta)$$

En particulier, $\alpha_n(\Delta) = (\det \Delta)^{-1}$.

Remarque 4.1. *D'après le théorème précédent, on obtient immédiatement*

$$\frac{1}{\lambda_1 ... \lambda_i} \leq \alpha_i(\Delta) \leq \frac{2^i / V_i}{\lambda_1 ... \lambda_i}$$

Proposition 4.2. *Si $N(r, \Delta)$ désigne le nombre de points de Δ de norme euclidienne plus petite ou égale à $r \geqslant 0$, alors il existe une constante positive c_n, ne dépendant que de la dimension, telle que :*

$$N(r, \Delta) \leqslant c_n \alpha(\Delta) \max(1, r^n)$$

***Preuve*:** Comme $\alpha(\Delta/r) \leq \max(1, r^n)\alpha(\Delta)$, on peut se ramener par homothétie au cas $r = 1$. On raisonne alors par récurrence sur n. Pour $n = 0$, c'est évident. Supposons la propriété vraie à l'ordre $n-1$, et considérons les minima successifs de Δ. Ceci fournit une base $(e_1, ..., e_n)$ de Δ et un parallélépipède fondamental P de volume $\frac{1}{\alpha_n}$. A chaque point x du réseau intérieur à la boule de rayon 1, on associe $x + P$. Ceci fournit un recouvrement de la boule et l'inégalité :

$$N(1, \Delta) \leqslant V(1 + n\lambda_n) \cdot \alpha_n(\Delta)$$

où $V(1 + n\lambda_n)$ désigne le volume de la boule euclidienne de $\mathbb{R}^n$ de rayon $1 + n\lambda_n$ avec λ_n comme précédemment. Si $\lambda_n \leqslant 1$, alors ce volume est inférieur à $V(1 + n)$, et sinon cela signifie que les points de Δ qui sont dans la boule unité sont en fait dans l'hyperplan $vect(e_1, ..., e_{n-1})$, qui est Δ-rationnel. On peut donc appliquer l'hypothèse de récurrence qui donne :

$$N(1, \Delta) \leqslant c_{n-1} \cdot \max_{0 \leqslant i \leqslant n-1} \alpha_i(\Delta)$$

Alors la constante $c_n = \max\{c_{n-1}, V(1+n)\}$ convient.■

4.3. **Topologie sur l'espace des réseaux.**

4.3.1. *Métrique de Hausdorff.* L'identification entre $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ et l'ensemble X des réseaux unimodulaires de $\mathbb{R}^n$, permet de donner à X la topologie quotient de $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. Ainsi X est localement compact, séparé, et séparable (i.e. ayant une base dénombrable d'ouverts). Il est donc métrisable par le théorème de métrisabilité d'Urysohn (cf [HoY]), ou encore d'après les observations faites au §1.4.2. : on peut munir $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ d'une distance induite par distance invariante à droite sur $SL_n(\mathbb{R})$. Mais, une distance naturelle sur X est donnée par la distance de Hausdorff pour les fermés de $\mathbb{R}^n$. Plus précisément, notons K_n la boule euclidienne de rayon n, et d_n la distance de Hausdorff pour les compacts de K_n. Définissons la distance d sur X par :

$$d(\Delta, \Delta') = \sum_{n \geqslant 0} \frac{1}{2^n} d_n(\Delta \cap K_n, \Delta' \cap K_n)$$

Comme les compacts de K_n considérés sont finis, d_n est en fait

$$\max\left\{\max_{x\in\Delta\cap K_n} dist(x,\Delta'\cap K_n),\ \max_{x'\in\Delta'\cap K_n} dist(x',\Delta\cap K_n)\right\}$$

où $dist$ est issue de la distance euclidienne. X ainsi muni de la distance d est alors homéomorphe à $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$:

Proposition 4.3. $\Phi : SL_n(\mathbb{R})/SL_n(\mathbb{Z}) \longrightarrow (X,d),\ \dot{g} \longrightarrow g(\mathbb{Z}^n)$ *est un homéomorphisme.*

***Preuve*:** Notons π la surjection canonique associée à $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. Φ est continue (resp. ouverte) si et seulement si $\Phi\circ\pi$ est continue (resp. ouverte). Si $g_k \longrightarrow g$ dans $SL_n(\mathbb{R})$ alors pour tout point x de $\mathbb{R}^n$ $g_k(x)\longrightarrow g(x)$ et donc $g_k(\mathbb{Z}^n)\cap K_p \xrightarrow{d_p} g(\mathbb{Z}^n)\cap K_p$ pour tout p. Donc on a bien $g_k(\mathbb{Z}^n) \xrightarrow{d} g(\mathbb{Z}^n)$ et Φ est continue. Montrons que Φ est ouverte. Soit g dans $SL_n(\mathbb{R})$ et $\Delta=\Phi(\dot{g})=g(\mathbb{Z}^n)$. Fixons $\varepsilon>0$ et notons $g_1,...,g_n$ les vecteurs colonnes de g et choisissons $p\geqslant 0$ de sorte que ces vecteurs soient dans K_p. Alors pour tout réseau Δ' tel que $d(\Delta,\Delta')\leqslant\frac{\varepsilon}{2^p}$, il existe des vecteurs $f_1,...,f_n$ de ce réseau tels que $\|f_i-g_i\|\leqslant\varepsilon$. Puisque les g_i forment une base de Δ, on voit que si ε est pris suffisamment petit en fonction de Δ, les f_i forment eux-aussi une base de Δ'. Et si f est la matrice colonne de vecteurs f_i, $f\in SL_n(\mathbb{R})$ et $\|f-g\|\leqslant\varepsilon\sqrt{n}$. Ainsi l'image de tout voisinage de g contient un voisinage de $\Phi\circ\pi(g)$.$\blacksquare$

Ce point de vue permet aussi de donner une démonstration géométrique du **critère de Mahler**, qui fournit une caractérisation simple des compacts de X.

4.3.2. *Critère de compacité.*

Théorème 4.3. ***(critère de Mahler)*** *Soit A une partie de X, les assertions suivantes sont équivalentes :*

1. $\inf\{\|x\| \mid x\in\Delta-\{0\},\Delta\in A\}>0$
2. *Il existe une constante $C\geqslant 0$ telle que tout réseau de A possède une base de vecteurs de norme inférieure à C.*
3. *A est d'adhérence compacte (on dit aussi que A est relativement compacte ou plus simplement bornée)*

***Preuve*:** Montrons (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1). La première implication est une conséquence facile du théorème de Minkowski sur les minima successifs (théorème 3.2.) : si ε désigne la valeur de l'inf, on a donc $\lambda_n(\Delta)\leqslant\frac{2^n}{\varepsilon^{n-1}V_n}$ pour tout Δ dans A, ce qui donne (2). Ensuite supposons (2) et donnons-nous une suite (Δ_k) dans A. On peut donc trouver une base $(g_1^k,...,g_n^k)$ de Δ_k dans la boule de rayon C. Quitte à extraire une sous-suite, on peut supposer que cette base converge vers un n-uplet $(g_1,...,g_n)$. Par continuité du déterminant ces vecteurs forment une matrice g de $SL_n(\mathbb{R})$. Donc $g^k\longrightarrow g$ et en appliquant Φ on a $\Delta_k\longrightarrow\Phi(g)$, d'où (3). Enfin, si l'inf de (1) était nul, il existerait une suite Δ_k de réseaux et $x_k\in\Delta_k-\{0\}$, telle que $x_k\longrightarrow 0$. Mais, par compacité, une sous-suite de (Δ_k) convergerait vers un certain Δ, et en particulier le nombre de points de Δ_k dans la boule unité resterait borné, ce qui est une contradiction.$\blacksquare$

4.4. **Ensembles de Siegel.** Dans cette section, on va chercher à préciser un domaine fondamental pour l'espace des réseaux $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. En fait nous ne mettrons en évidence qu'un domaine plus gros (un ensemble de Siegel) qui contient un système de représentants, mais qui nous suffira pour calculer des intégrales par rapport à la mesure invariante de $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. Nous montrons ici en particulier que $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ est de volume fini (et donc $SL_n(\mathbb{Z})$ est un réseau de $SL_n(\mathbb{R})$).

4.4.1. *Domaines fondamentaux.* Pour s et $t > 0$, on note A_s^* l'ensemble des matrices $diag(a_1, ..., a_n)$ telles que $a_i \leqslant s a_{i+1}$ pour tout $i \leqslant n-1$, et on note N_t l'ensemble des matrices (n_{ij}) de N dont les coefficients au-dessus de la diagonale sont tels que $|n_{ij}| \leqslant t$ pour $i < j$. Tout ensemble de la forme $K^* A_s^* N_t$ s'appelle un **ensemble de Siegel**.

Proposition 4.4. *L'ensemble de Siegel* $\mathrm{S} = K^* A_s^* N_t$ *avec* $s = \frac{2}{\sqrt{3}}$ *et* $t = \frac{1}{2}$ *vérifie* $SL_n(\mathbb{R}) = \mathrm{S} \cdot SL_n(\mathbb{Z})$.

***Preuve*:** Soit $g \in SL_n(\mathbb{R})$, et $\Delta = g(\mathbb{Z}^n)$. On choisit un point de Δ de distance à 0 minimale soit e_1, et un supplémentaire Δ_0 tel que $\Delta = \Delta_0 \oplus \mathbb{Z} e_1$. Soit p la projection orthogonale parallèlement à e_1. $p(\Delta_0)$ est un réseau de $p(\mathbb{R}^n)$ et par récurrence sur la dimension, on peut trouver dans Δ_0 une base $e_2, ..., e_n$ telle que $a_i \leqslant \frac{2}{\sqrt{3}} a_{i+1}$ pour $2 \leqslant i \leqslant n-1$ où $a_i = d(p(e_i), Vect(p(e_2), ..., p(e_{i-1})))$ pour $i \geqslant 3$ et $a_2 = \|e_2\|$. Mais, puisque p est orthogonale, on a aussi $a_i = d(e_i, Vect(e_1, ..., e_{i-1}))$ pour $i \geqslant 2$. D'autre part, on vérifie qu'aucun point de $\Delta - \mathbb{Z} e_1$ n'est à une distance inférieure à $\frac{\sqrt{3}}{2} \|e_1\|$ de $\mathbb{R} e_1$ (sinon en translatant par $\pm e_1$ on obtiendrait un point de Δ dans la boule de centre 0 et de rayon $\|e_1\|$). Donc aussi $a_1 \leqslant \frac{2}{\sqrt{3}} a_2$.

En se rappelant l'interprétation géométrique de a dans la décomposition d'Iwasawa (cf. 2.4.2.), on remarque que les a_i sont précisément les coefficients de la matrice a dans la décomposition d'Iwasawa de $g\gamma \in K^* A^*_{\frac{2}{\sqrt{3}}} N$ pour un certain $\gamma \in SL_n(\mathbb{Z})$. Mais il est facile de voir $N = N_{\frac{1}{2}} \cdot (N \cap SL_n(\mathbb{Z}))$ (si $u \in N$ choisir convenablement des entiers m_{ij} tels que $|(um)_{ij}| = |m_{ij} + u_{i,i+1} m_{i+1,j} + ... + u_{ij}| \leqslant \frac{1}{2}$ en commençant par $m_{n-1,n}$). Cela achève la preuve.■

Comme K^* et N_t sont compacts, l'information concernant l'infini dans l'espace des réseaux $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$, se trouve dans A_s^*. En particulier on peut retrouver le critère de Malher à partir de cette remarque (un ensemble de réseaux sera relativement compact si et seulement si un ensemble correspondant de représentants dans S est relativement compact, ce qui équivaut à une minoration de a_1 par une constante strictement positive). De même, comme l'ensemble de Siegel S contient un système de représentants, on va pouvoir traiter les problèmes d'intégrabilité sur $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ en regardant l'intégrabilité sur S et en fait sur A_s^*.

4.4.2. *Volume de l'espace des réseaux.* Nous allons montrer que l'espace des réseaux est de volume fini pour la mesure $SL_n(\mathbb{R})$-invariante (cf prop. 2.10.). Ainsi $SL_n(\mathbb{Z})$ apparaîtra comme un réseau du groupe $SL_n(\mathbb{R})$.

Théorème 4.4. *$SL_n(\mathbb{Z})$ est un réseau de $SL_n(\mathbb{R})$*

***Preuve*:** Pour expliciter une mesure invariante sur $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$, on va utiliser la forme explicite de la mesure de Haar sur $SL_n(\mathbb{R})$ trouvée en 2.4.5., ainsi que la proposition 2.9. Un ensemble de Siegel S est un borélien de $SL_n(\mathbb{R})$ qui se surjecte sur $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ par la projection canonique d'après la proposition précédente. La proposition 2.9. montre donc que le volume invariant de l'espace des réseaux vérifie

$$vol(SL_n(\mathbb{R})/SL_n(\mathbb{Z})) \leqslant \int_{\mathrm{S}} d\mu_G$$

où μ_G est une mesure de Haar sur G qui induit la mesure invariante considérée sur l'espace des réseaux. Quitte à multiplier par un scalaire on peut supposer que $\mu_G = \mu_{K^*} \otimes \rho\mu_{A^*} \otimes \mu_N$. En notant $C = \int_{K^*} d\mu_{K^*} \times \int_{N_t} d\mu_N$ (K^* et N_t sont compacts) et en prenant S$= K^* A_s^* N_t$ il vient

$$\int_{\mathrm{S}} d\mu_G = C \int_{A_s^*} \rho(a) d\mu_{A^*}(a)$$

Il est pratique d'effectuer un changement de variables à ce niveau en posant $\frac{a_i}{a_{i+1}} = e^{-\beta_i}$ pour $1 \leqslant i \leqslant n-1$. La condition $a \in A_s^*$ s'exprime par $\beta_i \geqslant -\ln s$ pour $1 \leqslant i \leqslant n-1$. On vérifie que le jacobien de cette transformation est $\prod\limits_{1 \leqslant i \leqslant n-1} \frac{1}{a_i}$. On vérifie aussi qu'alors $\rho(a) = \prod\limits_{1 \leqslant i \leqslant n-1} e^{-i(n-i)\beta_i}$. Compte tenu de la mesure de Haar sur A^* calculée au 2.4.3. on a,

$$\int_{\mathrm{S}} d\mu_G = C \prod_{1 \leqslant i \leqslant n-1} \int_{-\ln s}^{+\infty} e^{-i(n-i)\beta_i} d\beta_i < \infty$$

Le volume invariant de $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ est donc fini.■

4.5. **Fonction α.** Donnons ici quelques propriétés de la fonction α définie en 4.2.2. Tout d'abord remarquons que la définition donnée en 4.2.2. s'écrit aussi

$$\frac{1}{\alpha_i(\Delta)} = \inf \left\{ \|x_1 \wedge ... \wedge x_i\| \mid x_1 \wedge ... \wedge x_i \in \Lambda^i(\Delta) - \{0\} \right\} \tag{9}$$

où $\Lambda^*(\mathbb{R}^n)$ désigne l'algèbre extérieure. La norme sur $\Lambda^i(\mathbb{R}^n)$ est la norme euclidienne standard qui rend la bas canonique de $\Lambda^i(\mathbb{R}^n)$ orthonormée. Rappelons que dans ce cas, le carré de la norme est aussi le déterminant de Gram des vecteurs considérés, c'est-à-dire

$$\|x_1 \wedge ... \wedge x_i\|^2 = \det\left((x_k \mid x_l)\right)_{kl}$$

où $(\cdot \mid \cdot)$ désigne le produit scalaire canonique de $\mathbb{R}^n$.

De cette écriture, il résulte que la borne inférieure dans l'expression 9 est atteinte, car elle est prise sur un ensemble discret. De plus α a les propriétés de régularité suivantes :

Proposition 4.5. $\ln \alpha$ *est uniformément continue pour la structure uniforme à gauche sur* $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ *(i.e. pour une distance induite par une distance invariante à droite sur* $SL_n(\mathbb{R})$*, voir 1.4.1.). En particulier* α *est continue sur* $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$*.*

***Preuve*:** Si $g \in SL_n(\mathbb{R})$, on note $\Lambda^i g$ l'automorphisme de $\Lambda^i(\mathbb{R})$ qu'il induit. On définit $\lambda(g)$ par

$$e^{\lambda(g)} = \max\left\{ \left\|\Lambda^i g\right\|, \left\|\Lambda^i g^{-1}\right\|^{-1}, 1 \leqslant i \leqslant n \right\} \geq 1$$

Pour tout $\varepsilon > 0$, il existe un voisinage U de id dans $SL_n(\mathbb{R})$ tel que $\lambda(g) < \varepsilon$ si $g \in U$. Pour tous points $x_1, ..., x_i$ de Δ on a $\left\|\Lambda^i g(x_1 \wedge ... \wedge x_i)\right\| = \|gx_1 \wedge ... \wedge gx_i\| \leqslant \left\|\Lambda^i g\right\| \|x_1 \wedge ... \wedge x_i\|$. On en déduit $\alpha_i^{-1}(g\Delta) \leqslant e^{\lambda(g)} \alpha_i^{-1}(\Delta)$ puis,

$$|\ln \alpha(g\Delta) - \ln \alpha(\Delta)| \leqslant \lambda(g)$$

Cela prouve la continuité uniforme de $\ln \alpha$ et la continuité de α.■

Par abus de notation, nous écrirons $\alpha(g)$ pour désigner $\alpha(g\mathbb{Z}^n)$. On remarque que si $g = a \in A^*$, alors

$$\alpha_i(a) = \left(\min\left\{a_{k_1} ... a_{k_i} \mid 1 \leqslant k_1 < ... < k_i \leqslant n\right\}\right)^{-1} \tag{10}$$

Lemme 4.1. *Si $g = kan$ est la décomposition d'Iwasawa de g alors $\alpha(g) \leqslant \alpha(a)$*

***Preuve*:** Soit $(\varepsilon_1, ..., \varepsilon_n)$ la base canonique de $\mathbb{R}^n$, alors la base canonique de $\Lambda^i(\mathbb{R})$ est $(\varepsilon_{k_1} \wedge ... \wedge \varepsilon_{k_i})_{k_1 < ... < k_i}$ ordonnée par l'ordre lexicographique. Dans cette base $\Lambda^i n$ est aussi triangulaire supérieure avec des 1 sur la diagonale. Soit $x_1 \wedge ... \wedge x_i \in \Lambda^i(\mathbb{Z}^n) - \{0\}$ et $l \in \mathbb{Z} - \{0\}$ sa dernière coordonnée non nulle dans la base canonique. Alors on remarque que l est aussi la dernière coordonnée non nulle de $\Lambda^i n(x_1 \wedge ... \wedge x_i)$. Si cette coordonnée correspond au vecteur de base $\varepsilon_{k_1} \wedge ... \wedge \varepsilon_{k_i}$, alors

$$\|g(x_1 \wedge ... \wedge x_i)\| = \|an(x_1 \wedge ... \wedge x_i)\| \geqslant |a_{k_1} ... a_{k_i}| \geqslant (\alpha(a))^{-1}$$

On en déduit l'inégalité souhaitée.■

Proposition 4.6. *La fonction α est dans $L^r(SL_n(\mathbb{R})/SL_n(\mathbb{Z}))$, pour $1 \leqslant r < n$*

***Preuve*:** Comme dans le calcul du volume de l'espace des réseaux on peut se contenter de montrer l'intégrabilité de α^r sur un ensemble de Siegel S. D'après le lemme précédent il suffit de montrer l'intégrabilité de $\alpha^r(a_g)$. D'après la forme de la mesure de Haar sur $SL_n(\mathbb{R})$ (cf. 2.4.5.), et puisque K^* et N_t sont compacts, il suffit de montrer l'intégrabilité de $a \to \rho(a)\alpha^r(a)$ sur A_s^*. Mais comme $a \in A_s^*$, $sa_{i+1} \geqslant a_i$ pour tout $i \leqslant n-1$ donc $a_{k_1} ... a_{k_i} \geqslant \frac{1}{s^{n^i}} a_1 ... a_i$. Compte tenu de 10, il suffit donc de montrer l'intégrabilité de $a \to \rho(a)\, (a_1 ... a_i)^{-r}$ sur A_s^* pour $i \leqslant n-1$. On effectue le changement de variable habituel (cf. thm 4.4.) $\frac{a_i}{a_{i+1}} = e^{-\beta_i}$, $i \leqslant n-1$. On fixe i et on calcule alors le produit $(a_1 ... a_i)^{-1} = e^{c_1\beta_1 + ... + c_{n-1}\beta_{n-1}}$ où $c_k = \frac{k(n-i)}{n}$ pour $k \leqslant i$ et $c_k = \frac{i(n-k)}{n}$ pour $k \geq i$. En particulier, on a toujours $c_k \leq \frac{k(n-k)}{n}$. Alors

$$\int_{A_s^*} \rho(a)\, (a_1 ... a_i)^{-r}\, d\mu_{A^*} \leqslant \prod_{1 \leqslant k \leqslant i} \int_{-\ln s}^{+\infty} e^{(c_k r - k(n-k))\beta_k} d\beta_k$$

L'expression de droite est finie dès que $r < n$. Cela achève la preuve.■

4.6. **La formule de Siegel.** Soit f une fonction continue sur $\mathbb{R}^n$ et à support compact. On peut alors définir la **transformée de Siegel** $\widetilde{f}$ sur $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ par la somme des valeurs de f en tous les points du réseau, soit :

$$\widetilde{f}(\dot{g}) = \sum_{x \in g\mathbb{Z}^n} f(v)$$

La somme est à support fini car f est à support compact. De plus, d'après la proposition 4.2., si le support de f est inclus dans la boule de centre 0 et de rayon r alors $\left|\widetilde{f}\right|$ est majoré par $C\alpha$ où $C = c_n \max(1, r^n) \sup_{x \in \mathbb{R}^n} f(x)$ (avec c_n la constante apparaissant dans la proposition 4.2.). Enfin on remarque que $\widetilde{f}$ est continue, mais non bornée.

Le théorème suivant présente une très belle formule trouvée par Siegel en 1945 :

Théorème 4.5. *Soit f continue à support compact sur $\mathbb{R}^n$ ($n \geqslant 2$), $G = SL_n(\mathbb{R})$, $\Gamma = SL_n(\mathbb{Z})$, ν la mesure de probabilité G-invariante sur G/Γ, et λ la mesure de Lebesgue. Alors $\widetilde{f}$ est intégrable sur G/Γ et :*

$$\int_{G/\Gamma} \widetilde{f} d\nu = \int_{\mathbb{R}^n} f d\lambda + f(0)$$

***Preuve*:** Tout d'abord, remarquons que $\widetilde{f}$ est intégrable car α l'est. Ainsi l'application $f \longmapsto \int_{G/\Gamma} \widetilde{f} d\nu$ définit une forme linéaire positive sur $C_c(\mathbb{R}^n)$ (fonctions continues à support compact), donc une mesure de Radon μ sur $\mathbb{R}^n$. Puisque ν est invariante sous l'action de G, μ est aussi invariante par G. D'après la remarque 2.2. μ est de la forme $c_0\lambda + c_1\delta_0$ (où c_0 et c_1 sont des constantes positives, δ_0 la masse de Dirac en 0, et λ la mesure de Lebesgue). On remarque d'abord que $c_1 = 1$ (prendre par exemple une suite de fonctions f_r dont le support est inclus dans la boule de centre 0 et de rayon r et telles que $f_r(0) = 1$, et faire tendre r vers 0 ; l'intégrale par rapport à ν de $\widetilde{f}_r$ tend vers 1 en utilisant la majoration par α). Puis on observe que $c_0 = 1$ en considérant les fonctions $f_t(x) = t^n f(tx)$ et en faisant tendre t vers 0. En effet, puisque f est continue, l'expression

$$\widetilde{f}_t(\dot{g}) = t^n \sum_{v \in g\mathbb{Z}^n} f(tv)$$

qui est une somme de Riemann, converge vers $\int_{\mathbb{R}^n} f d\lambda$ (un domaine fondamental du réseau unimodulaire $tg\mathbb{Z}^n$ est de volume t^n pour la mesure de Lebesgue λ). De plus on peut appliquer le théorème de convergence dominée à la suite $\widetilde{f}_t$ sur G/Γ puisque $\left|\widetilde{f}_t\right| \leqslant 2c_n\,(\sup f)\,\alpha$ pour $t \leq 1$ ($Supp(f_t) = \frac{1}{t}Supp(f)$). Cela achève la preuve.■

Remarque 4.2. *Un argument de classe monotone et troncature (cf. [DeM]) permet aisément de voir qu'une fonction intégrable quelconque $f \in L^1(\mathbb{R}^n, \lambda + \delta_0)$ définit ν-presque partout une fonction $\widetilde{f}$ intégrable sur G/Γ et que la formule ci-dessus est encore valide.*

5. Formes quadratiques. Groupes orthogonaux

Dans la conjecture d'Oppenheim, il est question d'une forme quadratique à coefficients réels, irrationnelle, indéfinie et non-dégénérée. Précisons ces termes et montrons que si la conjecture est vraie pour la dimension n_0, alors elle est vraie pour toute dimension supérieure. Tout d'abord, rappelons que l'on appelle "déterminant d'une forme quadratique" le déterminant de la matrice qui la représente dans la base canonique de $\mathbb{R}^n$. On dit que la forme q représente le réel α s'il existe $x \in \mathbb{Z}^n$ tel que $q(x) = \alpha$. Rappelons quelques faits de base à propos des formes quadratiques.

Le groupe linéaire $GL_n(\mathbb{R})$ agit sur l'ensemble des formes quadratiques réelles de façon naturelle par $(g, q) \to q \circ g^{-1}$. On dit que deux formes sont équivalentes si elles sont dans la même orbite pour cette action. La classification des formes quadratiques sur $\mathbb{R}^n$ nous dit que deux formes réelles sont équivalentes si et seulement si elles ont même signature. De même, deux formes sont dans la même orbite pour l'action restreinte à $SL_n(\mathbb{R})$ si et seulement si elles ont **même signature et même déterminant** ; et donc deux formes de même signature sont équivalentes à un scalaire positif près modulo $SL_n(\mathbb{R})$.

5.1. Formes rationnelles.

En reprenant la définition de 4.2.2. :

Définition 5.1. *Soit q une forme quadratique sur un $\mathbb{R}$-espace vectoriel $\mathbb{E}$ de dimension finie n, F un sous-espace de $\mathbb{E}$ et Δ un réseau de $\mathbb{E}$. Alors :*

1. *F est dit Δ-rationnel si $F \cap \Delta$ est un réseau de F.*
2. *q est dite Δ-rationnelle si sa matrice dans une base de Δ (qui est donc aussi une base de $\mathbb{E}$) est proportionnelle à une matrice à coefficients rationnels.*

Remarque 5.1. *Lorsque $\mathbb{E} = \mathbb{R}^n$ on dit simplement que F (resp. q) est rationnel s'il est $\mathbb{Z}^n$-rationnel.*

Par la proposition 4.1. on voit aussitôt que si F est Δ-rationnel, alors il existe une base $(e_1, ..., e_n)$ de Δ telle que $F = Vect(e_1, ..., e_p)$ où $p = \dim F$. $\{0\}$ est Δ-rationnel pour tout Δ.

Aussi, un sous-espace de $\mathbb{R}^n$ est rationnel si et seulement si il est engendré par des vecteurs de $\mathbb{Q}^n$. De même, une forme irrationnelle (i.e. non rationnelle) dans $\mathbb{R}^n$ est une forme dont deux coefficients sont incommensurables.

Remarque 5.2. *Un sous-réseau Γ de Δ est un facteur direct de Δ (c'est-à-dire admet un supplémentaire) si et seulement si $Vect(\Gamma) \cap \Delta = \Gamma$.*

Le théorème suivant permet de réduire la conjecture d'Oppenheim au cas $n = 3$.

Théorème 5.1. *Soit q une forme quadratique sur $\mathbb{R}^n$ indéfinie, non-dégénérée et irrationnelle. Alors pour tout entier m, $2 \leqslant m \leqslant n$, il existe un sous-espace rationnel F de dimension m tel que $q_{|F}$ soit irrationnelle, indéfinie, et non-dégénérée.*

***Preuve*:** Il suffit de démontrer l'assertion pour $m = 2$. En effet, si F est un sous-espace rationnel non-isotrope de dimension $m < n$, on peut toujours trouver un vecteur x de $\mathbb{R}^n$ tel que $F \oplus \mathbb{R}x$ soit rationnel et non-isotrope (fixer une base rationnelle $f_1, ..., f_m$ de F et considérer le déterminant de la matrice de q par rapport aux vecteurs $f_1, ..., f_m, x$ où x parcourt $\mathbb{R}^n$; cette application est non nulle car, q étant non-dégénérée, $F^\perp$ est non-isotrope ; et par densité de $\mathbb{Q}^n$ ce déterminant est non-nul en au moins un point $x \in \mathbb{Q}^n$). Cherchons donc un plan rationnel sur lequel q est indéfinie, irrationnelle et non-dégénérée. On peut trouver $x \in \mathbb{Q}^n$ tel que $q(x) \neq 0$. Donc quitte à multiplier q par un scalaire, on peut supposer $q(x) = 1$. Il s'agit de montrer l'existence d'un vecteur $w \in \mathbb{Q}^n$ tel que $0 > q(w) \notin \mathbb{Q}$. Soit B la forme bilinéaire symétrique associée à q. Comme q est irrationnelle, $B(\mathbb{Q}^n, \mathbb{Q}^n) \nsubseteq \mathbb{Q}$ et donc $q(\mathbb{Q}^n) \nsubseteq \mathbb{Q}$. On trouve alors $y \in \mathbb{Q}^n$ tel que $q(y) \notin \mathbb{Q}$. Si $q(y) < 0$, $w = y$ convient. On peut donc supposer $q(y) > 0$. Mais q étant indéfinie, et par densité de $\mathbb{Q}^n$, on trouve $z \in \mathbb{Q}^n$ tel que $q(z) < 0$. Alors pour $r \in \mathbb{Q}$ assez petit $w = z + ry$ ou $z - ry$ convient, car $q(z - ry) + q(z + ry) = 2r^2 q(y) \notin \mathbb{Q}$.■

Corollaire 5.1. *Si la conjecture d'Oppenheim est vraie pour la dimension 3 alors elle est vraie pour toute dimension supérieure.*

***Preuve*:** Soit donc q une forme quadratique de $\mathbb{R}^n$ (avec $n \geqslant 3$), indéfinie, irrationnelle et non-dégénérée. D'après le théorème, on peut trouver un sous-espace rationnel F de dimension 3 de $\mathbb{R}^n$, tel que $q_{|F}$ soit encore indéfinie, irrationnelle et non-dégénérée. On peut alors envoyer la base canonique de $\mathbb{R}^3$ sur une base rationnelle de F par une matrice u à coefficients entiers. Alors $q \circ u$ est irrationnelle, indéfinie et non-dégénérée sur $\mathbb{R}^3$ donc $q \circ u(\mathbb{Z}^3)$ est dense dans $\mathbb{R}$ et $q(\mathbb{Z}^n) \supset q \circ u(\mathbb{Z}^3)$ aussi.■

5.2. **Cône isotrope et groupe orthogonal.** La seule donnée géométrique du cône isotrope d'une forme quadratique (ou de la quadrique projective associée) la détermine à multiplication par un scalaire près ; et donc détermine aussi son groupe orthogonal. Montrons-le.

Proposition 5.1. *Soit q, q' deux formes quadratiques non-dégénérées sur un corps k de caractéristique différente de 2. On suppose qu'elles ont même cône isotrope C, et que celui-ci est non réduit à 0. Alors il existe un scalaire non nul λ tel que $q' = \lambda q$.*

***Preuve*:** Soit x_0 un élément non nul de C. Soit H l'orthogonal de x_0 pour q. Montrons que c'est aussi l'orthogonal pour q'. Fixons $x \in k^n$, alors $\forall \alpha \in k$, $q(x_0 + \alpha x) = 0 \Leftrightarrow$

$q'(x_0 + \alpha x) = 0$. Donc $\forall \alpha \in k$, $-2\alpha B(x_0, x) = q(x) \Leftrightarrow -2\alpha B'(x_0, x) = q'(x)$ où B et B' sont les formes bilinéaires symétriques associées. En distinguant selon que x appartient à C ou non, on voit aisément que $B(x_0, x) = 0 \Leftrightarrow B'(x_0, x) = 0$. Donc les deux orthogonaux coïncident et B et B' sont proportionnelles par un certain coefficient λ. Alors si $x \notin H$ il existe α tel que $-2\alpha B(x_0, x) = q(x)$ et donc $-2\alpha B'(x_0, x) = q'(x)$ d'où $q'(x) = \lambda q(x)$. Puis, si x et y ne sont pas dans H, $x + y$ ou $x - y$ n'est pas dans H. En développant $q(x \pm y)$ on voit alors que $B'(x, y) = \lambda B(x, y)$. Puis si $x \in H$, on peut choisir $y \notin H$ (q non-dégénérée), alors en écrivant $q(x) = q(x + y) + q(y) - 2B(x + y, y)$, on voit que $q'(x) = \lambda q(x)$.■

Remarque 5.3. *Si le corps k est algébriquement clos, la proposition précédente est évidente par le Nullstellensatz.*

De même, la donnée du groupe orthogonal de la forme quadratique la détermine à multiplication par un scalaire près. Voyons d'abord une conséquence remarquable du théorème de Witt (cf. [Ser]).

Lemme 5.1. *Soit q une forme quadratique non-dégénérée sur un corps k de caractéristique différente de 2. Le groupe orthogonal $O(q)$ (et même $SO(q)$) agit transitivement sur chaque surface de niveau $\{x \neq 0 \mid q(x) = constante\}$.*

***Preuve*:** Soit x et y non nuls tels que $q(x) = q(y)$. Notons $F = Vect(x, y)$, et définissons l'endomorphisme g de F par $g(x) = y$ et, si F est de dimension 2, $g(y) = x$. Alors g préserve $q_{|F}$, donc se prolonge en un élément de $O(q)$ par le théorème de Witt. Quitte à composer au besoin par un endomorphisme orthogonal de déterminant -1 et qui fixe x, on voit que l'on peut choisir g dans $SO(q)$.■

Proposition 5.2. *Soit q, q' deux formes quadratiques non-dégénérées sur un corps k de caractéristique différente de 2. On suppose qu'elles ont même groupe spécial orthogonal $SO(q) = SO(q')$. Alors il existe un scalaire non nul λ tel que $q' = \lambda q$.*

***Preuve*:** Soit $x \neq 0$ isotrope pour q. Soit λ un scalaire $\neq \pm 1$. Alors par le lemme, x et λx sont dans la même orbite par $SO(q')$. Donc $q'(x) = 0$. Par symétrie, q et q' ont les mêmes cônes isotropes, donc sont proportionnelles. Reste le cas où les deux cônes isotropes sont réduits à 0. Soit x tel que $q(x) \neq 0$, il existe λ tel que $q'(x) = \lambda q(x)$. Mais q et q' sont définies, donc pour tout y il existe un scalaire μ_y tel que $q(y) = q(\mu_y x)$ (prendre une base dans laquelle la matrice de q a des coefficients ± 1 sur la diagonale et 0 ailleurs, alors les coefficients sont tous du même signe sinon on aurait un vecteur non nul dans le cône isotrope de q). On peut alors choisir $h \in SO(q)$ tel que $y = h(\mu_y x)$ et donc $q'(y) = \lambda q(y)$. Par symétrie, λ est non nul.■

5.3. **Petites valeurs des formes quadratiques réelles.** Dans cette section, on va montrer que la densité de $q(\mathbb{Z}^n)$ est une conséquence facile du fait que q représente des valeurs arbitrairement petites et non nulles. Par homogénéité de q, la densité de $q(\mathbb{Z}^n)$ dans $\mathbb{R}$ se ramène à l'existence de valeurs strictement positives arbitrairement petites et des valeurs strictement négatives arbitrairement petites représentées par q. Le problème est donc de montrer que si q représente des valeurs non nulles arbitrairement petites alors elle représente des valeurs arbitrairement petites positives et négatives. Pour cela nous allons d'abord donner une majoration de la borne inférieure des valeurs strictement positives de q sur les points entiers. La proposition suivante est due à H. Blaney (cf. [Bla]) :

Proposition 5.3. *Soit q une forme quadratique réelle non-dégénérée positive ou indéfinie. Alors il existe $x \in \mathbb{Z}^n$ tel que $0 < q(x) \leqslant 2^{n-1} |\det(q)|^{\frac{1}{n}}$.*

***Preuve*:** On observe qu'on peut se ramener à $|\det(q)| = 1$ puis on procède par récurrence sur n. Pour $n = 1$, c'est clair. On suppose le résultat vrai pour $n - 1 \geqslant 0$ et on note m la borne inférieure des valeurs strictement positives de q aux points entiers. Si $m = 0$ il n'y a rien à prouver. Sinon il existe $\varepsilon > 0$ arbitrairement petit tel que $q(x) = \frac{m}{1-\varepsilon}$ pour un certain $x \in \mathbb{Z}^n$ que l'on peut supposer primitif (c'est-à-dire tel que ses coordonnées soient des entiers premiers entre eux). En considérant le sous-réseau engendré par x et en appliquant la proposition 4.1., on peut compléter x en une base de $\mathbb{Z}^n$, ce qui fournit $u \in SL_n(\mathbb{Z})$ tel que $q \circ u(\varepsilon_1) = \frac{m}{1-\varepsilon}$ où $(\varepsilon_i)_{0 \leqslant i \leqslant n}$ est la base canonique de $\mathbb{R}^n$. On peut dès-lors remplacer q par $q \circ u$, car ces formes représentent les mêmes valeurs. On peut donc écrire dans les coordonnées de $\mathbb{R}^n$,

$$\frac{1-\varepsilon}{m} q(x) = (x_1 + a_2 x_2 + ... + a_n x_n)^2 + q_1(x_2, ..., x_n) \tag{11}$$

où q_1 est une forme quadratique de $\mathbb{R}^{n-1}$. Et par définition de m, le terme de droite ci-dessus est supérieur ou égal à $1 - \varepsilon$. Soit q_1 soit $-q_1$ satisfait l'hypothèse de récurrence, ce qui fournit des entiers $x_2, ..., x_n$ tels que :

$$0 < |q_1(x_2, ..., x_n)| \leqslant 2^{n-2} \left(\frac{1-\varepsilon}{m} \right)^{n/n-1}$$

Alors le terme de droite dans la dernière inégalité est plus grand ou égal à $\frac{1}{4}$. En effet, si $0 < q_1(x_2, ..., x_n) < \frac{1}{4}$, on peut trouver x_1 tel que

$$|x_1 + a_2 x_2 + ... + a_n x_n| \leqslant \frac{1}{2}$$

ce qui contredit la définition de m. Si $\varepsilon < -q_1(x_2, ..., x_n) < \frac{1}{4}$ on choisit de même x_1 tel que $\frac{1}{2} \leqslant |x_1 + a_2 x_2 + ... + a_n x_n| \leqslant 1$ pour obtenir la même contradiction. Et enfin si $0 < -q_1(x_2, ..., x_n) < \varepsilon$ on se ramène au cas précédent en multipliant $x_2, ..., x_n$ par un entier convenable. On en déduit :

$$2^{n-2} \left(\frac{1-\varepsilon}{m} \right)^{n/n-1} \geqslant \frac{1}{4}$$

ou encore,

$$q(x) = \frac{m}{1-\varepsilon} \leqslant 2^{n-1}$$

ce qui achève la preuve. ■

Remarque 5.4. *Indépendamment de ce théorème et en utilisant les résultats de géométrie des nombres énoncés plus haut, il est aisé d'obtenir une majoration de la borne inférieure des valeurs atteintes par $|q|$ sur $\mathbb{Z}^n$ pour une forme quadratique réelle non-dégénérée q. On obtient qu'il existe $x \in \mathbb{Z}^n - \{0\}$ tel que $|q(x)| \leqslant \frac{4}{(V_n)^{2/n}} |\det q|^{1/n}$. (le faire d'abord pour q définie positive en appliquant le théorème 4.2. à $\Delta = u(\mathbb{Z}^n)$ où $q = q_0 \circ u$ et q_0 est le produit scalaire canonique. Puis pour q quelconque se ramener à ce cas en trouvant q' définie positive telle que $|q| \leqslant q'$ et $\det q' = \det q$.)*

La proposition précédente permet alors de déduire le corollaire suivant dû à Oppenheim :

Corollaire 5.2. *Soit q une forme quadratique non-dégénérée et indéfinie sur $\mathbb{R}^n$ $(n \geqslant 2)$. Si $a > 0$ est représenté par q alors il existe $-b < 0$ représenté par q tel que*

$$b^{2n-2} \leqslant 2^{3n-3} a^{n-2} |\det q|$$

***Preuve*:** Pour $n = 2$ c'est une conséquence directe de l'énoncé de la proposition précédente. Alors soit $x = (x_1, ..., x_n) \in \mathbb{Z}^n$ tel que $q(x) = a > 0$. On peut supposer x primitif, c'est-à-dire $pgcd(x_1, ..., x_n) = 1$. On procède alors exactement comme dans la preuve précédente en complétant en une base de $\mathbb{Z}^n$. On obtient l'équation 11 avec $\frac{q(x)}{a}$ pour terme de gauche. Alors $\det(q) = a \det(q_1)$, et on applique la proposition précédente à $-q_1$, ce qui fournit des entiers $x_2, ..., x_n$ tels $0 < q_1(x_2, ..., x_n) = c \leqslant 2^{n-2} |\det q_1|$. On fixe $x_2, ..., x_n$, puis on considère la forme binaire en u et v $q(u, vx_2, ..., vx_n)$, dont le déterminant est $-ac$. Le résultat pour $n = 2$ montre alors que cette forme, et donc q aussi, représente un réel $-b < 0$ tel que $0 < b \leqslant 2\sqrt{ac}$ c'est-à-dire $b^{2n-2} \leqslant 2^{3n-3} a^{n-2} |\det q|$.■

On en déduit aussitôt la propriété énoncée au début de ce paragraphe :

Corollaire 5.3. *Si q est une forme quadratique non-dégénérée et indéfinie sur $\mathbb{R}^n$ $(n \geqslant 3)$ telle que $q(\mathbb{Z}^n) \cap \mathbb{R}_+$ admet 0 pour point d'accumulation, alors $q(\mathbb{Z}^n) \cap \mathbb{R}_-$ admet aussi 0 pour point d'accumulation.*

Corollaire 5.4. *Si q est une forme quadratique non-dégénérée et indéfinie sur $\mathbb{R}^n$ $(n \geqslant 3)$ telle que $\forall \varepsilon > 0 \exists x \in \mathbb{Z}^n$ tel que $0 < |q(x)| < \varepsilon$, alors $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}$.*

Remarque 5.5. *Ces corollaires sont faux si $n = 2$, voir ci-dessous.*

5.4. **Autres cas (q rationnelle, dégénérée...)** Dans ce paragraphe, on considère toujours une forme quadratique q sur $\mathbb{R}^n$.

5.4.1. *q rationnelle.* Si q est rationnelle, il existe un réel λ tel que $\lambda^{-1} q$ soit à coefficients entiers. On en déduit que $q(\mathbb{Z}^n) \subset \lambda\mathbb{Z}$, et donc que pour $x \in \mathbb{Z}^n$, $q(x) = 0$ ou $|q(x)| \geqslant |\lambda|$. Donc $q(\mathbb{Z}^n)$ n'est pas dense dans $\mathbb{R}$. De plus, si le rang de q est supérieur ou égal à 5, le théorème de Meyer (cf. [Ser]) dit que q représente 0.

5.4.2. *q définie.* Si q est définie, par exemple définie positive, il est clair qu'il existe $\varepsilon > 0$ tel que $q(x) > \varepsilon$ dès que $x \in \mathbb{Z}^n - \{0\}$. Donc $q(\mathbb{Z}^n)$ n'est pas dense dans $\mathbb{R}$.

5.4.3. *q dégénérée.* Bien entendu, on va ramener le cas où q est dégénérée au cas non-dégénéré. La forme réduite de Gauss de q s'écrit :

$$q(x) = (l_1(x))^2 \pm ... \pm (l_{n-1}(x))^2$$

et $\{x \in \mathbb{R}^n \mid |l_1(x)| \leqslant \varepsilon \text{ pour tout } 1 \leqslant i \leqslant n-1\}$ est un convexe mesurable de mesure de Lebesgue infinie quel que soit $\varepsilon > 0$. Par le théorème de Minkowski (thm 4.1.), on en déduit que $\forall \varepsilon > 0\ \exists x \in \mathbb{Z}^n\ |q(x)| < \varepsilon$. Mais il se peut que q représente 0. On considère donc $\widetilde{q}$ la forme quadratique induite par q sur $\mathbb{R}^n / \ker q$. Bien sûr, $q(\mathbb{Z}^n) = \widetilde{q}(\pi(\mathbb{Z}^n))$ où π est la projection canonique et $\ker q$ est rationnel dès que q l'est. La proposition suivante précise le passage au quotient :

Proposition 5.4. *Soit $\mathbb{E}$ un $\mathbb{R}$-espace vectoriel de dimension finie n, F un sous-espace de $\mathbb{E}$, π la projection canonique de $\mathbb{E}/F$, et Δ un réseau de $\mathbb{E}$. Alors F est Δ-rationnel si et seulement si $\pi(\Delta)$ est un réseau de $\mathbb{E}/F$.*

***Preuve*:** $\pi(\Delta)$ est un $\mathbb{Z}$-module libre de rang $\dim \mathbb{E} - rang(\Delta \cap F)$ (car de type fini et sans torsion sur $\mathbb{Z}$). Si F est Δ-rationnel, il en résulte que $\pi(\Delta)$ est un réseau de $\mathbb{E}/F$. Sinon, le rang de $\pi(\Delta)$ est supérieur à la dimension de $\mathbb{E}/F$ donc $\pi(\Delta)$ n'est pas un réseau de $\mathbb{E}/F$.■

Il en résulte que si $\ker q$ est irrationnel, alors $\pi(\mathbb{Z}^n)$ n'est pas discret dans $\mathbb{R}^n / \ker q$. Par le théorème de classification des groupes additifs d'un espace vectoriel réel de dimension finie (cf. le début de 4.1.) il existe donc un vecteur non nul v de $\pi(\mathbb{Z}^n)$ tel que $\pi(\mathbb{Z}^n) \cap \mathbb{R}v$ soit dense dans $\mathbb{R}v$. Si q est positive (resp. négative, resp. indéfinie) alors $\widetilde{q}$ est positive (resp. négative, resp. indéfinie). Il en résulte que $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}_+$ (resp. $\mathbb{R}_-$, resp. $\mathbb{R}$). C'est evident dans les cas où q est positive ou négative. Dans le cas indéfini, comme $\widetilde{q}$ est non-dégénérée, on peut trouver $x \in \mathbb{R}^n / \ker q$ tel que $\widetilde{\phi}(x,v)^2 - \widetilde{q}(x)\widetilde{q}(v) < 0$. On en déduit (par exemple par densité de $Vect_{\mathbb{Q}}(\pi(\mathbb{Z}^n))$ dans $\mathbb{R}^n / \ker q$) qu'on peut choisir x dans $\pi(\mathbb{Z}^n)$. Alors $\widetilde{q}(x + tv)$, où $tv \in \pi(\mathbb{Z}^n)$, prend des valeurs arbitrairement petites positives et négatives, ce qui entraîne la densité de $q(\mathbb{Z}^n)$ dans $\mathbb{R}$.

Lorsque $\ker q$ est rationnel, $\pi(\mathbb{Z}^n)$ est un réseau de $\mathbb{R}^n / \ker q$ et q est rationnelle si et seulement si $\widetilde{q}$ est $\pi(\mathbb{Z}^n)$-rationnelle. On s'est donc ramené au cas non-dégénéré. On peut finalement énoncer le théorème suivant dont la conjecture d'Oppenheim apparaît comme un cas particulier (mais le seul cas difficile) :

Théorème 5.2. *Soit q une forme quadratique sur $\mathbb{R}^n$ de rang $\geqslant 3$.*

1. *Si q est indéfinie, $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}$ si et seulement si q est irrationnelle.*
2. *Si q est positive (resp. négative), $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}_+$ (resp. $\mathbb{R}_-$) si et seulement si $\ker q$ est irrationnel*

5.4.4. *rang(q)*$\leqslant$ 2. Ce cas-ci est à part. Il se peut que $q(\mathbb{Z}^2)$ ne soit pas dense dans $\mathbb{R}$, même si q est non-dégénérée, irrationnelle et indéfinie. En particulier, le corollaire 5.3. ne s'applique pas. Donnons un exemple éclairant. Pour la forme quadratique $q_\alpha(x,y) = xy - \alpha y^2$, la question dépend des propriétés diophantiennes de α. Rappelons la définition classique suivante (cf. [Sch2]) :

Définition 5.2. *On dit que le nombre α est bien approchable si*

$$\liminf_{n\to\infty} n \,\|n\alpha\| = 0$$

où $n \in \mathbb{N}$ et $\|x\| = dist(x, \mathbb{Z})$.

Remarquons que α est bien approchable si et seulement si $q_\alpha(\mathbb{Z}^2)$ admet des valeurs arbitrairement petites. Presque tout réel est bien approchable, c'est la conséquence du célèbre théorème de Khintchine dont on rappelle ici l'énoncé :

Théorème 5.3. *Soit ψ une fonction continue décroissante* : $[1,\infty[\to]0,\infty[$. *Pour presque tout réel α (au sens de la mesure de Lebesgue), il existe une infinité (resp. qu'un nombre fini) d'entiers naturels n, tels que*

$$\|n\alpha\| \leq \psi(n)$$

dès que $\int_1^\infty \psi(x)dx$ diverge (resp. converge).

En prenant $\psi(x) = \frac{1}{x \ln x}$, qui n'est pas intégrable, on voit que presque tout réel α est bien approchable.

Il existe de nombreuses preuves de ce résultat (voir [Sch2] thm 3.A., [Sul] et [Bil] pour trois différentes preuves).

Cependant, pour déterminer si $q(\mathbb{Z}^2)$ est dense dans $\mathbb{R}^2$, on a besoin de savoir si q admet des valeurs arbitrairement petites négatives *et* positives (car le corollaire 5.3. ne s'applique pas), autrement dit de savoir si α est bien approchable à gauche et à droite. Pour cela, nous suivons la preuve du théorème de Khintchine donnée dans [Bil]. Elle utilise les fractions continues et la théorie ergodique.

Pour tout irrationnel α, notons $\alpha = [a_0, a_1, ..., a_n, ...]$ le développement de α en fractions continues ($a_i \in \mathbb{Z}$ pour tout $i \geq 0$ et $a_i \geq 1$ pour tout $i \geq 1$). On considère les réduites $\frac{p_i}{q_i}$ de α et l'on note $\alpha_i = [a_i, a_{i+1}, ...]$. D'après un résultat classique sur les fractions continues, (cf. [Lan2]), on sait que pour tout $i \geq 1$

$$\alpha = \frac{p_i \alpha_{i+1} + p_{i-1}}{q_i \alpha_{i+1} + q_{i-1}} \text{ et } p_i q_{i-1} - p_{i-1} q_i = (-1)^i$$

On en déduit

$$q_i p_i - \alpha q_i^2 = (-1)^i \delta_i \text{ avec } \frac{1}{\delta_i} = \alpha_{i+1} + \frac{q_{i-1}}{q_i}$$

En particulier

$$\frac{1}{2 + a_{i+1}} < \delta_i < \frac{1}{a_{i+1}} \tag{12}$$

On voit donc que si $\limsup a_i = \infty$, α doit être bien approchable. Réciproquement si α est bien approchable, $\limsup a_i = \infty$ car les réduites réalisent les meilleures approximations rationnelles de α (plus précisément le lemme de Legendre dit que si $\left|pq - \alpha q^2\right| \leq \frac{1}{2}$ alors $\frac{p}{q}$ est une réduite $\frac{p_i}{q_i}$ de α, cf [Lan2]). De même, 12 montre que α est bien approchable à gauche (resp. à droite) si $\limsup a_{2i+1} = \infty$ (resp. $\limsup a_{2i} = \infty$). Résumons :

Proposition 5.5. *Un irrationnel $\alpha = [a_0, a_1, ..., a_n, ...]$ est bien approchable si et seulement si* $\limsup a_i = \infty$. *Il est bien approchable à droite (resp. à gauche) si et seulement si* $\limsup a_{2i} = \infty$ *(resp.* $\limsup a_{2i+1} = \infty$*).*

Nous allons en fait montrer que presque tout réel est bien approchable à gauche et à droite. Pour cela, il nous faut introduire l'application de Gauss. Il s'agit de la fonction qui associe à $x \in]0, 1[$ la partie fractionnaire de $\frac{1}{x}$. Notons-la T. Elle est reliée aux fractions continues, car on a $a_i = [\frac{1}{T^{i-1}\alpha}]$ pour tout $i \geq 1$ si $\alpha = [a_0, a_1, ..., a_n, ...]$ et dans cette représentation, T est le décalage $[a_0, a_1, ..., a_n, ...] \to [a_1, a_2, ..., a_n, ...]$.

On remarque que la mesure $m = \frac{dx}{1+x}$ est invariante par T. D'autre part, on montre aisément en calculant $\lambda(T^{-n}[x, y[\cap I_\omega)$ (où λ est la mesure de Lebesgue et I_ω l'ensemble des x dont la fraction continue commence par le mot ω de longueur n) que T est mélangeante, c'est-à-dire que pour tous boréliens A et B,

$$m(A \cap T^{-n}B) \underset{n \to \infty}{\to} m(A)m(B)$$

T est même exacte, c'est-à-dire que la tribu asymptotique n'a que des événements de mesure 0 ou 1, propriété qui entraîne le mélange par le théorème de Lévy sur les martingales inverses (cf. [Bil]). On en déduit donc l'ergodicité de T et T^2 pour cette mesure. Puisque cette dernière est équivalente à la mesure de Lebesgue, tout ensemble T ou T^2 invariant est de mesure de Lebesgue 1 ou 0. En particulier, presque partout $\limsup a_i(\alpha) = \infty \Leftrightarrow \liminf T^i \alpha = 0$ et on a l'analogue pour a_{2i} et a_{2i+1}. Puisque T est ergodique pour la mesure de Lebesgue, presque partout $\liminf T^i \alpha = 0$. De même, l'ergodicité de T^2 montre que presque partout $\limsup a_{2i}(\alpha) = \infty$ et $\limsup a_{2i+1}(\alpha) = \infty$. Finalement on a prouvé le résultat suivant :

Proposition 5.6. *Presque tout réel est bien approchable à gauche et à droite. Et donc pour presque tout α, $q_\alpha(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$.*

On a donc obtenu ce que l'on désirait en se passant du théorème de Khintchine. Mais on a en fait presque démontré ce dernier théorème : en effet, le mélange de T combiné au lemme de Borel-Cantelli permet aisément d'en déduire l'énoncé de Khintchine (cf. [Bil]).

Considérons maintenant une forme quadratique réelle q de rang 2, quelconque. Si $\ker q$ est irrationnel, $q(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$, comme on l'a vu au paragraphe précédent. Sinon, quitte à restreindre q à un plan convenable, on peut supposer que q est non dégénérée et à deux variables. Toute forme indéfinie dans le plan s'écrit comme produit de deux formes linéaires. Si q n'est pas proportionnelle à q_α pour un certain α, c'est que q est proportionnelle à une forme du type $q_{\beta,\beta'} = (x-\beta y)(x-\beta' y)$. On voit que pour $y \in \mathbb{N}$ assez grand,

$$\inf_{x,y\in\mathbb{Z}} |q_{\beta,\beta'}(x,y)| \leq \|\beta y\| \left(|\beta-\beta'|\, y + \frac{1}{2}\right) \leq 2\,|\beta-\beta'|\, \|\beta y\|\, y$$

Donc, si β est bien approchable, $q_{\beta,\beta'}$ prend des valeurs arbitrairement petites sur les points entiers. De même, si β est bien approchable à gauche et à droite, $q_{\beta,\beta'}(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$. Il en résulte aisément :

Proposition 5.7. *Dans l'espace des formes quadratiques indéfinies de $\mathbb{R}^2$, presque toute forme q est telle que $q(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$.*

5.5. **Structure des groupes orthogonaux.** Comme ci-dessus, on se donne une forme quadratique q sur $\mathbb{R}^n$, non-dégénérée, et de signature $(p, n-p)$ avec $p \geq 1$ et $n \geq 3$. Les groupes orthogonaux $O(q)$ et $SO(q)$ sont des sous-groupes de Lie algébriques de $GL_n(\mathbb{R})$. Ce sont donc des "**groupes algébriques réels**" (cf. 3.1.3.). Nous allons maintenant préciser la structure du groupe de Lie $SO(q)$ en dégageant quelques renseignements utiles pour la suite.

Tout d'abord, $O(q)$ est de dimension $\frac{n(n-1)}{2}$ (par exemple, considérer l'action de $GL_n(\mathbb{R})$ sur l'espace vectoriel $S_n(\mathbb{R})$ des matrices symétriques : l'orbite d'une matrice non-dégénérée est un ouvert, et son stabilisateur est isomorphe à $O(q)$ donc $\dim O(q) = \dim SO(q) = \dim GL_n(\mathbb{R}) - \dim S_n = \frac{n(n-1)}{2}$).

5.5.1. *Théorème de Chevalley.* Ensuite, rappelons le théorème suivant de Chevalley (cf. [MnT]) :

Théorème 5.4. *Soit G un groupe algébrique réel stable par adjonction. Soit $O_n(\mathbb{R})$ le groupe orthogonal euclidien, $S_n(\mathbb{R})$ l'espace vectoriel des matrices symétriques réelles et $\mathfrak{g}$ l'algèbre de Lie de G. Alors la décomposition polaire*

$$\begin{aligned} O_n(\mathbb{R}) \times S_n(\mathbb{R}) &\to GL_n(\mathbb{R}) \\ (o,s) &\mapsto oe^s \end{aligned}$$

est interne à G et réalise le difféomorphisme

$$(G \cap O_n(\mathbb{R})) \times (\mathfrak{g} \cap S_n(\mathbb{R})) \simeq G$$

Appliqué à $G = O(q)$, qui vérifie évidemment les hypothèses de l'énoncé précédent, ce théorème précise la structure différentielle de G

$$\begin{aligned} G \cap O_n(\mathbb{R}) &= \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},\ A \in O_p(\mathbb{R}) \text{ et } B \in O_{n-p}(\mathbb{R}) \right\} \\ \mathfrak{g} \cap S_n(\mathbb{R}) &= \left\{ \begin{pmatrix} 0 & C \\ C^* & 0 \end{pmatrix},\ C \in M_{p,n-p}(\mathbb{R}) \right\} \end{aligned}$$

Et par conséquent, $O(q)$ est difféomorphe à $O_p(\mathbb{R}) \times O_{n-p}(\mathbb{R}) \times \mathbb{R}^{p(n-p)}$. En particulier, $O(q)$ a quatre composantes connexes, et $SO(q)$ est la réunion de deux d'entre elles (rappelons que $SO_n(\mathbb{R})$ est connexe).

5.5.2. *Sous-groupes compacts maximaux.* D'autre part, le fait que la décomposition polaire soit interne à G, implique aisément que $G \cap O_n(\mathbb{R})$ est un sous-groupe compact maximal de G (en fait ces sous-groupes sont tous conjugués dans G, cf. [OnV]).

Notons $\mathfrak{l} = A_n(\mathbb{R}) \cap \mathfrak{g}$ et $\mathfrak{p} = S_n(\mathbb{R}) \cap \mathfrak{g}$ où $A_n(\mathbb{R})$ désigne l'ensemble des matrices antisymétriques, qui n'est autre que l'algèbre de Lie de $O_n(\mathbb{R})$. Le théorème précédent fournit la décomposition suivante :

$$\mathfrak{g} = \mathfrak{l} \oplus \mathfrak{p}$$

Il s'agit de la **décomposition de Cartan** de $\mathfrak{g}$. Une telle décomposition existe en fait pour toute algèbre de Lie semi-simple réelle (cf. [OnV]). Remarquons que $\mathfrak{l}$ est l'algèbre de Lie du sous-groupe compact maximal $G \cap O_n(\mathbb{R})$. D'autre part, on vérifie qu'on a les relations

$$[\mathfrak{l}, \mathfrak{l}] \subseteq \mathfrak{l} \; [\mathfrak{p}, \mathfrak{p}] \subseteq \mathfrak{l} \quad [\mathfrak{l}, \mathfrak{p}] \subseteq \mathfrak{p}$$

En particulier, $\mathfrak{l}$ est une sous-algèbre de $\mathfrak{g}$ et $ad_{\mathfrak{l}}$ agit sur $\mathfrak{p}$. De même, ces relations montrent que si l'algèbre de Lie $\mathfrak{g}$ est simple (c'est-à-dire sans idéal non trivial), alors $\mathfrak{l}$ est une sous-algèbre de Lie maximale de $\mathfrak{g}$. Dans ce cas, on en déduit que la composante neutre de $G \cap O_n(\mathbb{R})$ est en fait **maximale parmi tous les sous-groupes de Lie connexes** de G. Puisque tous les sous-groupes compacts maximaux sont conjugués, le même résultat est vrai pour tous les sous-groupes compacts maximaux de G, dès que G est simple (i.e. son algèbre de Lie est simple).

Il résulte de la classification des algèbres de Lie semi-simples complexes que $O(q)$ et $SO(q)$ sont des groupes de Lie semi-simples (la complexification de l'algèbre de Lie de $O(q)$ est précisément l'algèbre de Lie de $O_n(\mathbb{C})$ c'est-à-dire $\mathfrak{so}_n(\mathbb{C})$, qui est semi-simple). Si $(n,p) \neq (2,2)$, **l'algèbre de Lie de $O(q)$ est même simple**. Dans ce cas, la propriété de maximalité ci-dessus a bien lieu.

5.5.3. *Décomposition KAK.* On considère toujours un groupe algébrique réel G stable par adjonction, $K = G \cap O_n(\mathbb{R})$ sous-groupe maximal compact, et $\mathfrak{g} = \mathfrak{l} \oplus \mathfrak{p}$ la décomposition de Cartan. L'ensemble des matrices diagonales de $\mathfrak{sl}_n(\mathbb{R})$ est une sous-algèbre abélienne maximale de $S_n(\mathbb{R})$. Lle théorème suivant qui précise la structure des sous-algèbres abéliennes maximales de $\mathfrak{p}$ (cf. [Kna] thm 5.13.) :

Théorème 5.5. *Soit $\mathfrak{a}$ et $\mathfrak{a}_1$ deux sous-espaces maximaux abéliens de $\mathfrak{p}$. Alors il existe $k \in K$ tel que $\mathfrak{a}_1 = k^{-1}\mathfrak{a}k$.*

Fixons une sous-algèbre abélienne maximale $\mathfrak{a}$ de $\mathfrak{p}$. Tout élément $s \in \mathfrak{p} = S_n(\mathbb{R}) \cap \mathfrak{g}$ s'écrit donc $s = k^{-1}ak$ pour un certain $k \in K$ et $a \in \mathfrak{a}$. Si $G = SL_n(\mathbb{R})$ on retrouve le résultat classique d'algèbre linéaire que des matrices symétriques de G qui commutent deux à deux sont diagonalisables dans une même base orthonormale. Compte tenu du fait que la décompostion polaire est interne à G par le théorème de Chevalley, il vient :

Théorème 5.6. ***(décomposition** KAK**)*** *Soit G un groupe algébrique réel stable par adjonction, $K = G \cap O_n(\mathbb{R})$, $\mathfrak{a}$ une sous-algèbre abélienne maximale de $\mathfrak{p} = S_n(\mathbb{R}) \cap \mathfrak{g}$ et $A = \exp \mathfrak{a}$. Alors $G = KAK$.*

5.5.4. *Maximalité de $SO(q)$.* On a la propriété suivante :

Proposition 5.8. *La composante neutre $SO^0(q)$ est maximale parmi tous les sous-groupes connexes de $SL_n(\mathbb{R})$.*

***Preuve*:** Soit L un sous-groupe connexe tel que $SO^0(q) \subseteq L \subseteq SL_n(\mathbb{R})$. Soient $\mathfrak{h} \subseteq \mathfrak{l} \subseteq \mathfrak{g}$ les algèbres de Lie correspondantes et $\mathfrak{h}_{\mathbb{C}}$, $\mathfrak{l}_{\mathbb{C}}$ et $\mathfrak{g}_{\mathbb{C}}$ leurs complexifiées. $\mathfrak{l}_{\mathbb{C}}/\mathfrak{h}_{\mathbb{C}}$ est une sous-algèbre de $\mathfrak{g}_\mathbb{C}/\mathfrak{h}_\mathbb{C}$, en particulier c'est un $SO_n(\mathbb{C})$-module pour la représentation adjointe. Mais $\mathfrak{h}_\mathbb{C}$ est précisément l'ensemble des matrices antisymétriques de $\mathbb{C}^n$ et $\mathfrak{g}_\mathbb{C}$ l'ensemble des matrices complexes de trace nulle. Donc $\mathfrak{g}_\mathbb{C}/\mathfrak{h}_\mathbb{C}$ s'identifie à l'ensemble des matrices complexes symétriques de trace nulle. Or l'action de $SO_n(\mathbb{C})$ sur cet espace est irréductible, ce qui prouve que $\mathfrak{l} = \mathfrak{g}$ ou $\mathfrak{l} = \mathfrak{h}$, soit $L = SL_n(\mathbb{R})$ ou $L = SO^0(q)$.■

5.5.5. *Groupes U-engendrés et groupes sans facteur compact.*

5.5.6. *Isomorphisme $SO^0_{1,2} \simeq PSL_2(\mathbb{R})$.* Soit V l'espace vectoriel réel $\mathfrak{sl}_2(\mathbb{R})$ assimilé à l'espace des matrices carrées de taille 2 et de trace nulle. En posant $q(m) = \det m$, on obtient une forme quadratique de signature $(1,2)$ sur V. On fait agir $PSL_2(\mathbb{R})$ sur V, en constatant que si $m \in V$ et $g \in PSL_2(\mathbb{R})$, $\phi_g(m) = gmg^{-1} \in V$. De plus ϕ_g conserve q, donc $\phi_g \in O(q)$. Par connexité, on a en fait $\phi_g \in SO^0(q) \simeq SO^0_{2,1}(\mathbb{R})$. On obtient alors le morphisme de groupe de Lie suivant :

$$\begin{array}{rcl} \phi \;\; PSL_2(\mathbb{R}) & \to & SO^0(q) \\ g & \mapsto & \phi_g \end{array}$$

Il est facile de vérifier que ϕ est en fait en isomorphisme ($Im\phi$ est aussi de dimension 6 car $d\phi$ est injective en l'identité, et $\ker\phi$ commute à V, donc est trivial).

6. Ergodicité

Dans cette section, nous allons énoncer les résultats de Ratner à propos de la conjecture de Raghunathan, ainsi que les théorèmes ergodiques qui les accompagnent. Ces résultats difficiles datent de 1990 et permettent en particulier de démontrer la conjecture d'Oppenheim très facilement. Nous expliquerons comment un peu plus loin. Cependant, dans la deuxième partie du mémoire, nous donnerons une preuve élémentaire de la conjecture d'Oppenheim, telle qu'elle a été démontrée par Margulis en 1987. Nous ne donnerons donc pas de preuves dans la présente section. Dans la troisième partie de ce mémoire nous utiliserons le théorème d'équirépartition de Ratner (ci-dessous thm 6.2) pour résoudre une version quantitative de la conjecture d'Oppenheim.

6.1. **La conjecture de Raghunathan et le théorème d'équirépartition de Ratner.** Dans les années 1970, Raghunathan a remarqué que la conjecture d'Oppenheim pouvait être vue comme la conséquence simple d'un résultat concernant l'adhérence de l'orbite de certains groupes dans l'espace des réseaux. Rappelons ce résultat énoncé en introduction :

Conjecture 6.1. ***(Conjecture de Raghunathan)*** *Soit G un groupe de Lie connexe, U un sous-groupe unipotent de G et Γ un réseau de G. Alors pour tout $x \in G/\Gamma$, il existe un sous-groupe fermé L de G tel que $\overline{U \cdot x} = L \cdot x$.*

Précisons que "unipotent" (on dit aussi Ad-unipotent) signifie ici que la représentation adjointe de U agit par matrices unipotentes. Pour un groupe algébrique connexe à centre trivial, cela correspond à la définition usuelle). Dans le cas le plus simple où $G = \mathbb{R}^n$, $\Gamma = \mathbb{Z}^n$, $G/\Gamma = \mathbb{T}^n$, tout élément de G est unipotent et le sous-groupe $(tv)_{t\in\mathbb{R}}$, $v = (v_1, ..., v_n) \in \mathbb{R}^n$, est un sous-groupe unipotent à un paramètre de G. La conjecture traduit seulement le fait bien connu que l'adhérence d'une orbite est toujours un sous-tore (par exemple, si les v_i sont deux à deux commensurables, les orbites sont périodiques, en revanche si $(1, v_1, ..., v_n)$ sont $\mathbb{Q}$-linéairement dépendants, elles sont denses et équidistribuées). Cette conjecture a d'abord été démontrée dans de nombreux cas particuliers, mais c'est M.Ratner (cf. [Rat]) qui l'a finalement prouvée à ce niveau de généralité en 1990. Depuis, d'autres preuves ainsi que de nombreuses généralisations, notamment pour G algébrique sur un corps local, ont été trouvées (cf. en particulier [MaT]). Dans sa preuve, Ratner démontre en fait deux résultats remarquables, un théorème de classification des mesures invariantes et un théorème d'équidistribution des orbites que nous appellerons le théorème d'équirépartition de Ratner. Avant de poursuivre, il nous faut faire quelques rappels et définitions.

Tout d'abord, donnons-nous un espace mesurable $(E, \mathcal{E})$, et un groupe G qui agit sur E par bijections mesurables. Rappelons qu'une mesure μ sur $(E, \mathcal{E})$ est dite G-invariante lorsque $\mu(gA) = \mu(A)\ \forall g \in G, \forall A \in \mathcal{E}$. De plus, on dit qu'une probabilité μ, G-invariante, est **ergodique** pour l'action de G (on dit aussi que l'action de G est ergodique quand il n'y a pas d'ambiguité sur la mesure) si tout ensemble mesurable $A \in \mathcal{E}$ invariant par G est de μ-mesure 0 ou 1. Lorsque E est l'espace homogène G/Γ, avec G un groupe de Lie connexe et Γ un réseau de G, et $\mathcal{E}$ est la tribu borélienne de E, on dit que la probabilité μ est **algébrique** si elle est invariante par H et si son support est une orbite de la forme $H \cdot x$ où $x \in G/\Gamma$ et H est un sous-groupe fermé de G. On peut maintenant énoncer le premier théorème de Ratner sur la classification des mesures :

Théorème 6.1. *(classification des mesures ergodiques) Soit G un groupe de Lie connexe, U un sous-groupe de G engendré par ses éléments unipotents et Γ un réseau de G. Toute probabilité sur G/Γ U-invariante et ergodique est algébrique.*

Dans le cas des rotations du tore, ce théorème traduit le fait classique que les mesures invariantes par $(tv)_{t\in\mathbb{R}}$ sont précisément celles portées par les sous-tores invariants.

Le second théorème porte sur l'équidistribution des orbites pour l'action d'un sous-groupe unipotent à un paramètre.

Théorème 6.2. *(théorème d'équirépartition de Ratner) Soit G un groupe de Lie connexe et $U = \{u_t \mid t \in \mathbb{R}\}$ un sous-groupe unipotent à un paramètre de G. Alors, pour tout réseau Γ de G et tout point $x \in G/\Gamma$, il existe un sous-groupe connexe fermé L de G contenant U tel que $\overline{U \cdot x} = L \cdot x$, et une mesure de probabilité μ, portée par $L \cdot x$, L-invariante et U-ergodique. De plus, pour toute fonction f continue bornée sur G/Γ,*

$$\lim_{t\to\infty} \frac{1}{t} \int_0^t f(u_s x) ds = \int_{G/\Gamma} f d\mu \tag{13}$$

On constate que ce dernier théorème prouve la conjecture de Raghunathan dans le cas d'un groupe U unipotent à un paramètre. Mais c'est en réalité un résultat beaucoup plus fort. Ces deux derniers théorèmes sont utilisés par Ratner pour démontrer la forme suivante de la conjecture de Raghunathan :

Théorème 6.3. *Soit G un groupe de Lie connexe, U un sous-groupe engendré par ses éléments unipotents et Γ un réseau de G. Alors, pour tout $x \in G/\Gamma$, il existe un sous-groupe connexe fermé L de G contenant U, un sous-groupe unipotent à un paramètre V de U tels que $\overline{V \cdot x} = \overline{U \cdot x} = L \cdot x$ et une mesure de probabilité μ, portée par $L \cdot x$, L-invariante et V-ergodique.*

Nous allons maintenant montrer comment la conjecture d'Oppenheim se déduit de la conjecture de Raghunathan.

6.2. Déduction de la conjecture d'Oppenheim.

6.2.1. *Conjecture d'Oppenheim et généralisations.* On se donne une forme quadratique réelle q indéfinie, non-dégénérée et irrationnelle à $n \geq 3$ variables. On note $H_q = SO(q)$ le groupe orthogonal spécial de q. On a vu (cf. §5.5.5.) que la composante neutre H_q^0 de

H_q est engendrée par ses éléments unipotents (car $n \geq 3$) et qu'elle est maximale parmi les sous-groupes fermés propres de $G = SL_n(\mathbb{R})$. Puisque $\Gamma = SL_n(\mathbb{Z})$ est un réseau de G, il existe d'après le théorème 6.3. un sous-groupe fermé L de G, contenant H_q^0, tel que $\overline{H_q^0 \cdot z} = L \cdot z$ où $H_q^0 \cdot z$ est l'orbite de $z = \mathbb{Z}^n$ dans l'espace des réseaux G/Γ. Mais par maximalité de H_q^0, L est G ou H_q^0. Il s'agit de montrer que $L = G$, car alors l'orbite $H_q \cdot z$ sera dense dans G/Γ et par suite $q(\mathbb{Z}^n) = q(H_q \cdot z)$ sera dense dans $\mathbb{R}$.

Rappelons que par maximalité de H_q^0 (cf. §5.5.4.) L ne peut être que H_q^0 ou G tout entier. Raisonnons par l'absurde et supposons que $L = H_q^0$. Alors l'orbite de $H_q^0 \cdot z$ est fermée, donc $H_q^0 \cdot z \simeq H_q^0/(H_q^0 \cap \Gamma)$ (cf. prop. 1.3.). De plus, d'après le théorème 6.3., l'orbite est support d'une mesure finie invariante par H_q^0, donc $H_q^0 \cap \Gamma$ est un réseau de H_q^0. Mais, d'après §5.5., H^0 satisfait les hypothèses du théorème de densité de Borel (cf. thm 3.1.) : donc $H_q^0 \cap \Gamma$ est Zariski-dense dans H_q^0 et par suite $H_q \cap \Gamma$ est Zariski-dense dans H_q. Mais, pour tout $\sigma \in Gal(\mathbb{C} \mid \mathbb{Q})$, $H_q \cap \Gamma = \sigma(H_q \cap \Gamma) \subseteq \sigma(H_q) = H_{\sigma q}$. Il en résulte que $H_q \subseteq H_{\sigma q}$ pour tout $\sigma \in Gal(\mathbb{C} \mid \mathbb{Q})$ et donc $H_q = H_{\sigma q}$ (σq est la forme quadratique complexe dont les coefficients sont les images par σ de ceux de q). Par la proposition 5.2. σq est proportionnelle à q pour tout $\sigma \in Gal(\mathbb{C} \mid \mathbb{Q})$, ce qui implique que q est proportionnelle à une forme rationnelle (le corps des invariants de $Gal(\mathbb{C} \mid \mathbb{Q})$ est bien $\mathbb{Q}$) et apporte la contradiction souhaitée.

On a même obtenu ainsi un résultat plus fort que celui annoncé dans la conjecture d'Oppenheim. On a montré que $H_q \cdot z$ est dense dans G/Γ quand q est irrationnelle. Deux questions se posent naturellement. Tout d'abord que se passe-t-il si q est rationnelle? et ensuite $U \cdot z$ est-il encore dense pour $U \subseteq H_q^0$ unipotent?

La proposition suivante répond aisément à la première question :

Proposition 6.1. *Soit q une forme quadratique réelle, indéfinie et non-dégénérée à $n \geq 3$ variables. Alors q est rationnelle si et seulement si l'orbite $H_q \cdot \mathbb{Z}^n$ est fermée dans G/Γ.*

***Preuve*:** Si q est irrationnelle, on a vu que $H_q \cdot \mathbb{Z}^n$ est dense, mais ne peut être G/Γ tout entier car $q(\mathbb{Z}^n) = q(H_q \cdot \mathbb{Z}^n)$ est dénombrable, donc $H_q \cdot \mathbb{Z}^n$ n'est pas fermé. Reste le cas ou q est rationnelle. Toute suite $(a_k)_k$ de $H_q\Gamma$ convergente vers un certain b dans G est telle que $q \circ a_k$ est stationnaire vu que $q(\mathbb{Z}^n)$ est discret. Donc $b \in H_q a_k \subset H_q\Gamma$. Ainsi $H_q\Gamma$ est fermé dans G, ce qui revient à dire que l'orbite $H_q \cdot \mathbb{Z}^n$ est fermée dans G/Γ.■

Nous verrons au début de la partie suivante qu'en fait, les formes rationnelles qui ne représentent pas 0 sont précisément celles dont l'orbite $H_q \cdot \mathbb{Z}^n$ est compacte. Cela ne peut avoir lieu que si $n \leq 4$ (théorème de Meyer, cf. [Ser]).

Enfin, le fait que $H_q \cdot \mathbb{Z}^n$ soit dense entraîne beaucoup plus que la conjecture d'Oppenheim. On a en réalité la conséquence suivante, beaucoup plus forte :

Théorème 6.4. *Soit q une forme quadratique réelle non-dégénérée, indéfinie, irrationnelle, à $n \geq 3$ variables. Quels que soient les $n-1$ réels $\mu_1, ..., \mu_{n-1}$, et quel que soit $\delta > 0$, il existe une base $(e_1, ..., e_n)$ de $\mathbb{Z}^n$ telle que*

$$|q(e_i) - \mu_i| \leq \delta \ \forall i \in [1, n-1]$$

En particulier $q(\mathcal{P})$ est dense dans $\mathbb{R}$, où $\mathcal{P}$ désigne l'ensemble des éléments primitifs de $\mathbb{Z}^n$ (i.e. $x = (x_1, ..., x_n)$ tel que $pgcd(x_1, ..., x_n) = 1$).

***Preuve*:** Comme q est non-dégénérée et indéfinie, les surfaces de niveau $\{q(x) = \mu\}$ ne sont contenues dans aucun hyperplan. Il en résulte que l'on peut trouver une base unimodulaire de $\mathbb{R}^n$ (i.e. de déterminant 1 dans la base canonique), soit $(f_1, ..., f_n)$, telle que $q(f_i) = \mu_i$ pour tout $i \in [1, n-1]$. Puisque $H_q \cdot \mathbb{Z}^n$ est dense dans G/Γ, il existe $h \in H_q$ et des entiers l_i tels que $l_i h\varepsilon_i$ soit très proche de f_i pour tout $i \in [1, n]$ (où (ε_i) désigne la base canonique) de sorte que

$$|q(l_i\varepsilon_i) - q(f_i)| = |q(l_i h\varepsilon_i) - q(f_i)| \leq \delta \ \forall i \in [1, n]$$

Comme $\det(f_1, ..., f_n) = 1$ et $\det(l_1 h\varepsilon_1, ..., l_n h\varepsilon_n) = l_1...l_n$, en prenant h convenable, on peut supposer que les l_i valent ± 1. Donc $(l_1\varepsilon_1, ..., l_n\varepsilon_n)$ est une base de $\mathbb{Z}^n$.■

6.2.2. *Structure de l'ensemble des points singuliers.* La réponse à la seconde question est négative (il suffit de prendre U tel que $U \cap \Gamma$ soit un réseau de U). Cependant on peut préciser la structure de l'ensemble des points singuliers. Pour cela, on revient au cas général où G est un groupe de Lie connexe et Γ un réseau de G. L'ensemble des points singuliers est par définition

$$\mathcal{S}(U) = \{x \in G/\Gamma \mid U \cdot x \text{ n'est pas dense}\}$$

Notons $X(H, U) = \{g \in G \mid Ug \subseteq gH\}$ pour tout sous-groupe H de G, puis $\mathcal{H}$ la classe des sous-groupes fermés propres H de G tels que $H \cap \Gamma$ soit un réseau de H. On vérifie aisément que si $H\Gamma = G$, alors $H = G$ (G est un groupe de Lie). Par conséquent, si $x \in X(H, U)\Gamma/\Gamma$ avec $H \in \mathcal{H}$, $H\Gamma$ est fermé dans G (puisque $H \cap \Gamma$ est un réseau de H d'après la prop. 2.14.), strictement inclus dans G donc l'orbite $U \cdot x \subseteq gH\Gamma/\Gamma$ n'est pas dense et $x \in \mathcal{S}(U)$. Réciproquement, d'après la conjecture de Raghunathan, pour tout $x \in \mathcal{S}(U)$, il existe un sous-groupe fermé propre F de G contenant U tel que $\overline{U \cdot x} = F \cdot x$ et tel que $F \cdot x$ est le support d'une mesure finie F-invariante. En écrivant $x = g\Gamma$ pour un certain $g \in G$, on a donc $g^{-1}Fg \in \mathcal{H}$, soit $x \in X(g^{-1}Fg, U)\Gamma/\Gamma$. On en déduit:

$$\mathcal{S}(U) = \bigcup_{H \in \mathcal{H}} X(H, U)\Gamma/\Gamma$$

Puisque chaque H est un sous-groupe de Lie propre de G, H est une sous-variété analytique de dimension inférieure à celle de G. De même l'ensemble $X(H, U)$ est une sous-variété analytique de dimension inférieure ou égale à celle de H. C'est donc en particulier un ensemble de mesure nulle. En fait, Dani et Margulis ont démontré que l'on pouvait restreindre $\mathcal{H}$ à une de ses parties dénombrables (cf. [DaM] proposition 2.3.). Ainsi, $\mathcal{S}(U)\Gamma$ apparaît comme une réunion dénombrable de sous-variétés analytiques propres de G. En particulier $\mathcal{S}(U)\Gamma$ est de mesure nulle.

Troisième partie 3. Preuve de la conjecture d'Oppenheim

Dans cette partie, nous allons donner une preuve élémentaire de la conjecture d'Oppenheim. Hormis le théorème de densité de Borel, qui est utilisé au tout début de cette partie pour montrer que la conjecture d'Oppenheim est équivalente à une propriété topologique des orbites dans l'espace des réseaux, seules des notions très élémentaires sur les groupes topologiques et les espaces homogènes sont utilisées.

Cette preuve est indépendante de la conjecture de Raghunathan ainsi que des théorèmes de Ratner. La preuve donnée ici est due à Margulis (cf. [Mar1] pour l'article original de 1987, donc antérieur aux travaux de Ratner) bien que la démonstration de certaines étapes intermédiaires ait été simplifiée.

7. Traduction du problème

Nous allons ici présenter une seconde traduction (cf. §6) de la conjecture d'Oppenheim en termes topologiques. La démonstration de cette version topologique occupera les paragraphes suivants.

La question est de déterminer les formes quadratiques réelles q qui atteignent aux points entiers des valeurs non nulles arbitrairement petites (ou encore, de façon équivalente par le corollaire 5.3., qui sont telles que $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}$).

Notations 7.1. *On note $H_q = SO(q)$ le groupe spécial orthogonal de q,*
$m(q) = \inf\{|q(x)| \mid x \in \mathbb{Z}^n - \{0\}\}$ *et*
$m^*(q) = \inf\{|q(x)| \mid x \in \mathbb{Z}^n, q(x) \neq 0\}$.

Si q ne représente pas 0, $m(q) = m^*(q)$. La conjecture d'Oppenheim (voir son énoncé en introduction) dit exactement que si q est non-dégénérée, indéfinie et irrationnelle sur $\mathbb{R}^n$ $(n \geqslant 3)$, alors $m^*(q) = 0$. Si q est rationnelle, il est clair que $m^*(q) > 0$ et que $m(q) = 0$ si et seulement si q représente 0.

Le théorème suivant traduit la condition $m(q) > 0$ en termes topologiques.

Proposition 7.1. *Soit q une forme quadratique sur $\mathbb{R}^n$. Les assertions suivantes sont équivalentes*

1. $m(q) > 0$
2. $H_q \cdot \mathbb{Z}^n$ *est relativement compact dans l'espace des réseaux.*

***Preuve*:** Supposons $m(q) > 0$ et choisissons un $\varepsilon > 0$ et $< m(q)$. On a $q \circ H_q(\mathbb{Z}^n) = q(\mathbb{Z}^n)$. Donc $H_q \cdot \mathbb{Z}^n - \{0\}$ ne rencontre pas $q^{-1}\{]-\varepsilon, \varepsilon[\}$. C'est-à-dire que les points non nuls des réseaux de $H_q \cdot \mathbb{Z}^n$ sont tous en dehors d'un voisinage bien déterminé de 0. Le critère de Malher (cf. thm 3.3) nous dit précisément que ceci implique la compacité relative de $H_q \cdot \mathbb{Z}^n$. Réciproquement, si $H_q \cdot \mathbb{Z}^n$ est relativement compact, le critère de Malher nous fournit un voisinage V de 0 qui ne rencontre pas $H_q \cdot \mathbb{Z}^n - \{0\}$. Comme ce dernier ensemble est stable sous l'action de H_q, on a que $H_q V$ est disjoint de $\mathbb{Z}^n - \{0\}$. Mais par le lemme 3.3.2. $H_q V$ contient $q^{-1}\{]-\varepsilon, \varepsilon[\}$ pour un certain $\varepsilon > 0$. C'est donc que $m(q) > 0$.■

Comme l'on sait (prop.6.1.) que q est proportionnelle à une forme rationnelle si et seulement si $H_q \cdot \mathbb{Z}^n$ est fermé dans l'espace des réseaux, on a en fait le résultat suivant :

Proposition 7.2. *Soit q une forme quadratique sur $\mathbb{R}^n$. Les assertions suivantes sont équivalentes*

1. $H_q \cdot \mathbb{Z}^n$ *est compact dans l'espace des réseaux.*
2. q *est proportionnelle à une forme rationnelle et ne représente pas* 0.

Comme la proposition 6.1. a été déduite des théorèmes de Ratner, nous donnons ici une preuve directe.

***Preuve*:** Seule l'implication $1 \Rightarrow 2$ est à prouver. L'idée est la même qu'au §6.2.1., si $H_q \cdot \mathbb{Z}^n$ est compact, alors l'espace homogène H_q/S_q est aussi compact, où $S_q = H_q \cap SL_n(\mathbb{Z}^n)$ est le stabilisateur de $\mathbb{Z}^n$ (cf. prop. 1.3.). Donc S_q est un réseau uniforme de H_q (cf. prop. 2.12.). Le théorème de densité de Borel (cf. §3.3.) entraîne que S_q est Zariski-dense dans H_q. Par suite, comme au §6.2.1., $H_q = H_{\sigma q}$ pour tout $\sigma \in Gal(\mathbb{C} \mid \mathbb{Q})$, puis q est proportionnelle à une forme rationnelle.■

On en déduit que si q est irrationnelle, $H_q \cdot \mathbb{Z}^n$ n'est pas compact. Pour montrer que $m(q) = 0$ ($\Leftrightarrow H_q \cdot \mathbb{Z}^n$ non relativement compact, d'après 7.1.), il suffirait donc de montrer qu'en général, toute orbite relativement compacte est compacte. En fait, on montre de façon similaire, que pour montrer que $m^*(q) = 0$ (conjecture d'Oppenheim), il suffit de montrer que toute orbite relativement compacte est compacte (voir [Mar1]).

8. Schéma de la démonstration

Nous avons vu en 3.2. comment la conjecture d'Oppenheim se ramène au cas $n = 3$. En dimension 3, toutes les formes indéfinies non-dégénérées sont équivalentes modulo $GL_3(\mathbb{R})$ et sont équivalentes à un scalaire près modulo $SL_3(\mathbb{R})$. Pour montrer que toute orbite par H_q relativement compacte est compacte, il suffit donc de le prouver pour une forme quadratique. On peut donc choisir $q(x) = 2x_1x_3 - x_2^2$. D'après ce qui précède, la conjecture d'Oppenheim se réduit à l'énoncé suivant dont nous présentons ici la preuve:

Théorème 8.1. *(Margulis) Soit H le groupe spécial orthogonal de $q(x) = 2x_1x_3 - x_2^2$, $G = SL_3(\mathbb{R})$ et $\Gamma = SL_3(\mathbb{Z})$ et $z \in G/\Gamma$ un réseau unimodulaire de $\mathbb{R}^3$. Si l'orbite $H \cdot z$ est relativement compacte, alors elle est compacte.*

L'étude de l'action de certains sous-groupes à un paramètre de G va jouer un rôle crucial dans la démonstration.

8.1. **Notations.** On note, outre $G = SL_3(\mathbb{R})$, $\Gamma = SL_3(\mathbb{Z})$ et $H = SO(q)$:

1. $U_1 = \left\{ u_1(t) = \begin{pmatrix} 1 & t & \frac{t^2}{2} \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}, t \in \mathbb{R} \right\} = \{\exp(At), t \in \mathbb{R}\}$ où $A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$
2. $U_2 = \left\{ u_2(t) = \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, t \in \mathbb{R} \right\} = \{\exp(Bt), t \in \mathbb{R}\}$ où $B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
   et $U_2^{\pm} = \{u_2(t), t \in \mathbb{R}_{\pm}\}$
3. $D = \left\{ d(t) = \begin{pmatrix} t & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{t} \end{pmatrix}, t > 0 \right\}$

Alors on a aisément les faits suivants:

1. $AB = BA = 0$, donc U_1U_2 est un groupe commutatif unipotent (i.e. constitué de matrices unipotentes).
2. $d(s)e^{At}d(s)^{-1} = e^{Ast}$ et $d(s)e^{Bt}d(s)^{-1} = e^{Bs^2t}$ donc en particulier, D normalise U_1 et U_2 et DU_1, DU_2, DU_1U_2 sont des sous-groupes de G.
3. Si $x \in G$ vérifie $xe^{At}x^{-1} = e^{As}$ $t \neq 0$ alors $x = d(s/t)e^{At+Bs}$ et donc le normalisateur de U_1 dans G, noté $N_G(U_1)$ est précisément DU_1U_2.
4. D et U_1 sont des sous-groupes de H.

8.2. **Lemmes.** La preuve du théorème 8.1. va découler des trois lemmes suivants:

Lemme 8.1. *Soit $z \in G/\Gamma$ tel que $H \cdot z$ soit relativement compacte mais pas compacte, $X \subset \overline{H \cdot z}$ un compact H-invariant minimal (pour l'inclusion) et K un compact U_1-invariant minimal de X. On pose $M = \{g \in G \mid g^{-1}K \cap \overline{H \cdot z} \neq \emptyset\}$. Alors $\{id\} \subsetneq U_2 \cap M$.*

Lemme 8.2. *Soit $z \in G/\Gamma$ tel que $H \cdot z$ soit relativement compacte. Soit K un compact U_1-invariant minimal du compact $\overline{H \cdot z}$. On pose $M = \{g \in G \mid g^{-1}K \cap K \neq \emptyset\}$. Alors la composante connexe de l'identité de l'adhérence du groupe engendré par $DU_2 \cap M$ est un sous-groupe de Lie connexe non trivial de DU_2.*

Lemme 8.3. *Pour tout $x \in G/\Gamma$, $DU_1U_2^+ \cdot x$ (resp. $DU_1U_2^- \cdot x$) n'est pas relativement compact.*

Dans la dernière section de cette partie, on démontre le théorème 8.1. en utilisant seulement ces trois résultats. Les preuves des lemmes 8.1. et 8.2. sont indépendantes, bien que très semblables et reposent sur le lemme suivant :

Lemme 8.4. *Soit G un sous-groupe algébrique de $GL_n(\mathbb{R})$ qui agit algébriquement sur un $\mathbb{R}$-espace vectoriel de dimension finie E. Soit $p \in E$, S le stabilisateur de p dans G, U un sous-groupe unipotent (i.e. constitué de matrices unipotentes) à un paramètre de S, et M une partie de G telle que*

1. *M est invariante à gauche par U et à droite par S,*
2. *M est fermée*

On note $N = \{g \in G \mid g^{-1}Ug \subset S\}$ (N/S correspond aux points fixes de U dans G/S) Et on suppose l'existence d'une suite (g_n) dans $M - S$ telle que $g_n \longrightarrow id$.

Alors la classe de id est non isolée dans $(M \cap N)/S$.

Ce dernier lemme est une conséquence du résultat suivant (cf. [Sik]) qui donne l'existence d'un chemin de points fixes pour un sous-groupe unipotent à un paramètre de G.

Lemme 8.5. *Soit E un $\mathbb{R}$-espace vectoriel de dimension finie, $U = (u(t))_{t\in\mathbb{R}}$ un sous-groupe à un paramètre d'automophismes unipotents de E. Soit p un point de E fixe par tous les éléments de U. On note F l'ensemble de tous ces points fixes et on se donne une partie P de $E - F$ telle que $p \in \overline{P} \cap F$. Alors $\exists f : \mathbb{R} \to \overline{UP} \cap F$ continue et non constante telle que $f(0) = p$.*

Nous allons maintenant présenter la preuve de ces lemmes et du théorème 8.1. dans l'ordre logique des choses.

9. Preuves

9.1. **Lemme 8.5.** Nous suivons ici la formulation donnée dans [Ben]. Le groupe U est constitué de transformations unipotentes de la forme $u(t) = \exp(at) = \sum_{k=0}^{N} t^k \frac{a^k}{k!}$ où a est un endomorphisme nilpotent de E et $N = \dim E$. Soit $(p_n)_n$ une suite de points de P qui converge vers p. Les applications $t \to u(t)p_n$ sont polynomiales à coefficients dans E et de degré $\leqslant N$. Elles sont aussi non constantes car $p_n \notin F$, et donc non bornées. En supposant p_n assez proche de p, on voit qu'on peut alors choisir $\tau_n > 0$ tel que $\sup_{t\in[-1,1]} \|u(\tau_n t)p_n - p\| = 1$. De plus comme l'application $(t,q) \longmapsto \|u(t)q - p\|$ est continue sur $\mathbb{R} \times E$, l'uniforme continuité sur tout compact montre que $q \longmapsto \sup_{t\in[-1,1]} \|u(Tt)q - p\|$ est continue pour tout $T > 0$. Puisque $p \in F$ cette fonction s'annule en q ; il s'ensuit que $\tau_n \to +\infty$. Les $f_n(t) = u(\tau_n t)p_n$ sont des fonctions polynomiales de degré $\leqslant N$ à coefficients dans E et bornées sur $[-1,1]$. On peut donc en extraire une suite qui converge uniformément sur $[-1,1]$ vers une fonction continue f (par exemple en prenant une suite extraite de chaque coefficient, la limite est alors encore polynomiale). On a alors $f(0) = p$ et $\sup_{t\in[-1,1]} \|f(t) - p\| = 1$ donc f n'est pas constant. Et par construction, l'image de f est dans $F \cap \overline{UP}$, car pour tout s et t réels, $u(t)f(s) = \lim u(t)f_n(s) = \lim f_n(s + \frac{t}{\tau_n}) = f(s)$ par uniforme continuité.■

9.2. **Lemme 8.4.** Quitte à extraire une sous-suite de (g_n) on peut évidemment supposer que $g_n \notin N$ pour tout n. On considère $F = \{x \in E \mid U \cdot x = x\}$ et $P = \{g_n \cdot p \mid n \in \mathbb{N}\}$. Comme $p \in S \supset U$, $p \in F$. Et puisque $g_n \to id$, $p \in \overline{P}$. Pour tout n, $Ug_n \cdot p \neq g_n \cdot p$ donc $P \cap F = \emptyset$. On peut alors appliquer le lemme précédent 9.5. à cette situation en conservant les mêmes notations et en prenant pour groupe unipotent l'image de U par la représentation de G dans E (cette image est bien unipotente car la représentation est algébrique, prop.3.1.). On obtient une fonction continue non constante $\phi : \mathbb{R} \to \overline{U \cdot P} \cap F$ telle que $\phi(0) = p$. Or $U \cdot P \subset M \cdot p \subset G \cdot p$ (car M est invariant à gauche par U). De plus, l'action de G est algébrique et par conséquent $G \cdot p$ est difféomorphe à G/S (cf. §3.2.). D'autre part M est fermé et saturé dans G, donc M/S est fermé dans G/S c'est-à-dire $M \cdot p$ fermé dans $G \cdot p$. Il vient $\overline{U \cdot P} \subset M \cdot p$ et donc $Im\phi \subset G \cdot p$. On en déduit l'existence d'une fonction non constante $f : \mathbb{R} \to G/S$ telle que $\phi = f \cdot p$. Vu que $Im\phi \subset F \cap M \cdot p$, $Imf \subset (M \cap N)/S$. Alors le fait que f soit continue, non constante, et égale à la classe de id en 0 entraîne que la classe de id est non isolée dans $(M \cap N)/S$.■

9.3. **Lemmes 8.1. et 8.2.: applications du lemme 8.4.**

9.3.1. *Lemme 8.1.* On va bien sûr chercher à appliquer le lemme 8.4. à cette situation. On reprend les notations de ce dernier lemme, avec $G = SL_3(\mathbb{R})$, E l'espace des formes quadratiques sur $\mathbb{R}^3$ et p la forme quadratique $q = 2x_1x_3 - x_2^2$. On considère l'action naturelle de G sur E. Alors le stabilisateur S est précisément $H = SO(q)$, et pour U on prend le sous-groupe unipotent à un paramètre U_1 de G comme défini dans les notations. Il reste à vérifier que l'ensemble M de l' énoncé satisfait les hypothèses du lemme 8.4.. Vu que K est invariant à gauche par $U = U_1$, il en est de même de M. Et puisque $\overline{H \cdot z}$ est invariant à gauche par $S = H$, M est invariant à droite par S. De la compacité de K, on déduit aussitôt que M est fermée. Soit $x \in K \subset X$. Supposons d'abord $H \cdot x \subsetneq X$ et fixons $y \in X - H \cdot x$. Par minimalité de X, $X = \overline{H \cdot y}$. Donc il existe (cf. prop. 1.3.) une suite (h_n) d'éléments de H et une suite (g_n) dans G qui tend vers id, telle que $(g_n)^{-1} \cdot x = h_n \cdot y$ et $g_n \notin H$. Ainsi $g_n \in M - H$. Dans l'autre cas, $X = H \cdot x$ et, comme $H \cdot z$ n'est pas compact, $x \notin H \cdot z$. Pourtant $x \in \overline{H \cdot z}$ donc il existe une suite (h'_n) d'éléments de H et une suite (g'_n) dans G qui tend vers id, telle que $(g'_n)^{-1} \cdot x = h_n \cdot z$ et $g_n \notin H$. Donc à nouveau $g'_n \in M - H$. On est donc, dans les deux cas, exactement dans les hypothèses du lemme 8.4.

Dans ce cas particulier, N peut être précisé. En fait $N = N_G(U_1)H$. L'inclusion $N_G(U_1)H \subset N$ est claire par définition de N. Réciproquement, si $g \in G$ vérifie $g^{-1}U_1g \subset H$, alors $g^{-1}Ag$ est dans l'algèbre de Lie de H (rappelons que A désigne la matrice nilpotente définie dans les notations). Mais on a l'isomorphisme de groupes de Lie $SO^0_{2,1} \cong PGL_2(\mathbb{R})$ (cf. §5.5.) et $H \cong SO_{2,1}$. De plus, $PGL_2(\mathbb{R})$ est localement isomorphe à $SL_2(\mathbb{R})$ en l'identité. Donc l'algèbre de Lie de H est isomorphe à $\mathrm{sl}_2(\mathbb{R})$. Deux éléments nilpotents de $\mathrm{sl}_2(\mathbb{R})$ sont conjugués dans $GL_2(\mathbb{R})$ et donc dans $SL_2(\mathbb{R}) \cup SL_2^-(\mathbb{R})$ (une seule réduite de Jordan). Par suite A et $g^{-1}Ag$ sont conjuguées dans H. Ainsi, il existe $h \in H$ tel que $g^{-1}U_1g = h^{-1}U_1h$ et donc $gh^{-1} \in N_G(U_1)$ ou $g \in N_G(U_1)H$, ce qui prouve l'autre inclusion. Mais d'après les remarques faites après les notations, $N_G(U_1) = DU_1U_2 = DU_2U_1 = DU_2D^{-1}DU_1 = U_2DU_1$ et donc $N = N_G(U_1)H = U_2H$.

Le lemme 8.4. entraîne alors que $(M \cap U_2H)/H$ est non trivial. Comme M est invariant à droite par H, on en déduit que $M \cap U_2$ n'est pas réduit à $\{id\}$.■

9.3.2. *Lemme 8.2.* Là encore, on va chercher à appliquer le lemme 8.4. à cette situation. On reprend les notations de ce dernier lemme, toujours avec $G = SL_3(\mathbb{R})$, mais cette fois $E = Q(\mathbb{R}^3) \times \mathbb{R}^3$ où $Q(\mathbb{R}^3)$ est l'espace des formes quadratiques sur $\mathbb{R}^3$. Le point p est $(q, (1, 0, 0))$ où q est encore la forme quadratique $q = 2x_1x_3 - x_2^2$. On considère l'action naturelle de G sur E, soit $g \cdot (q_1, r) = (q_1 \circ g^{-1}, g(r))$. Un simple calcul montre que le stabilisateur S de p est précisément U_1 (la représentation de G a été choisie pour cela). On prend alors $U = U_1 = S$. Il faut vérifier que l'ensemble M de l'énoncé satisfait les hypothèses du lemme 8.4.. Etant donné que K est par définition invariant à gauche par U, il résulte que M est invariante à gauche et à droite par M. De plus la compacité de K implique immédiatement que M est fermée.

Reste à montrer l'existence de la suite g_n. Il suffit pour cela de montrer que K n'est pas une orbite compacte. En effet, comme dans le lemme 8.1., on fixe alors $x \in K$ et $y \in K - U \cdot x$ et par minimalité de K, $K = \overline{U \cdot y}$. On en déduit l'existence d'une suite (u_n) d'éléments de U et une suite (g_n) dans G qui tend vers id telle que $(g_n)^{-1} \cdot x = u_n \cdot y$ et $g_n \notin U$. Ainsi $g_n \in M - U$. et on est dans les hypothèses du lemme 8.4.. Montrons maintenant que K n'est pas une orbite compacte. Raisonnons par l'absurde en fixant x dans K compact. Alors (toujours d'après la proposition 1.3.), $K = U \cdot x \cong U/U_x$ où U_x est le stabilisateur de x dans U. Mais puisque U n'est pas compact, U_x n'est pas réduit à $\{id\}$. Il existe donc $t \neq 0$ tel que $u_1(t) \cdot x = x$. Soit $v = (v_1, v_2, v_3)$ un vecteur du réseau x tel que $v_3 \neq 0$. Alors un calcul immédiat montre que $(u_1(t) - id)^2 v = (v_3 t^2, 0, 0)$. Ce dernier vecteur est donc encore dans x. Mais alors pour tout $s > 0$, $d(s)(v_3 t^2, 0, 0) = (s v_3 t^2, 0, 0)$ est un vecteur non nul de $d(s) \cdot x \in H \cdot x \subset \overline{H \cdot z}$. On fait tendre s vers 0, et le critère de Mahler (cf. théorème 2.3.) contredit la compacité de $\overline{H \cdot z}$.

On peut donc appliquer le lemme 8.4.. Mais dans ce cas particulier, puisque $S = U = U_1$, $N = N_G(U_1) = DU_1U_2 = DU_2U_1$, et $N/S = DU_2U_1/U_1 \cong DU_2$ (car D normalise U_2 et $DU_2 \cap U_1 = \{id\}$). Par conséquent, $(M \cap N)/S \cong DU_2 \cap M$. Soit Ψ le sous-groupe de DU_2 engendré par $DU_2 \cap M$. $\overline{\Psi}$ est un sous-groupe fermé du groupe de Lie DU_2. C'est donc un sous-groupe de Lie de DU_2. Notons C sa composante neutre. Elle est ouverte dans $\overline{\Psi}$ (conséquence de 1.3.2. car un groupe de Lie est localement connexe). Mais le lemme 8.4. nous dit précisément que l'identité n'est pas isolée dans $DU_2 \cap M$ donc dans $\overline{\Psi}$. Puisque C est ouverte, il s'ensuit que C est non trivial. ■

9.4. **Lemme 8.3. et théorème 8.1.**

9.4.1. *Lemme 8.3.* Le réseau x contient un vecteur $v = (v_1, v_2, v_3)$ tel que $v_3 > 0$ et $q(v) < 0$ (q est toujours la forme quadratique $2x_1x_3 - x_2^2$). Soit $g(t) = d(t)u_1(\frac{-v_2}{v_3})u_2(\frac{-q(v)}{2v_3}) \in DU_1U_2^+$. Un calcul immédiat donne $g(t)v = (0, 0, tv_3)$. En faisant tendre t vers 0, on voit par le critère de Mahler (cf. théorème 4.3.) que $DU_1U_2^+ \cdot x$ n'est pas relativement compact. On a la même preuve avec U_2^- (prendre $v_3 < 0$).

9.4.2. *Théorème 8.1.* Soit $z \in G/\Gamma$ tel que $H \cdot z$ soit relativement compacte. Par le lemme de Zorn, on peut trouver un compact $X \subset \overline{H \cdot z}$, H-invariant et minimal pour cette propriété (l'ensemble des compacts H-invariants est inductif car $\overline{H \cdot z}$ est compact). De même on peut trouver un compact $K \subset X$, U_1-invariant et minimal pour cette propriété.

Montrons que K est D-invariant. Pour cela, posons $M_1 = \{g \in G \mid g^{-1}K \cap K \neq \emptyset\}$. Si $g \in DU_2 \cap M_1$, g normalise U_1, donc $g^{-1}K \cap K$ est non vide et U_1-invariant. Par minimalité de K, on a donc $g^{-1}K = K$, c'est-à-dire que K est $DU_2 \cap M_1$-invariant. Soit C_0 la composante neutre du groupe fermé engendré par $DU_2 \cap M_1$. K est donc aussi C_0-invariant. Il suffit donc de voir que C_0 contient D. D'après le lemme 8.2. C_0 est un sous-groupe de Lie connexe non trivial de DU_2. Son algèbre de Lie est donc aussi non triviale, et C_0 contient un sous-groupe à un paramètre non trivial. Un calcul immédiat fournit l'algèbre de Lie

$$Lie(DU_2) = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & 0 & 0 \\ 0 & 0 & -a \end{pmatrix} ; a, b \in \mathbb{R} \right\}$$

Il existe donc dans C_0 un groupe à un paramètre non trivial de la forme

$$c(t) = \begin{pmatrix} e^{at} & 0 & 2bt(e^{at} - e^{-at}) \\ 0 & 1 & 0 \\ 0 & 0 & e^{-at} \end{pmatrix}$$

Si $a = 0$, en faisant varier t, on voit que ce groupe contient U_2 ; donc K est U_1U_2-invariant, et DU_1U_2 fixe le compact $\overline{H \cdot z}$. Mais ceci contredit évidemment le lemme 8.3. et par suite $a \neq 0$. Le sous-groupe à un paramètre c est alors précisément $u_2(b)Du_2(b)^{-1}$. Mais $u_2(\frac{b}{t^2} - b) = d(-t)u_2(b)d(t)u_2(-b) \in DC_0$. Donc si $b \neq 0$ on voit que U_2^+ ou U_2^- est inclus dans DC_0 et fixe $\overline{H \cdot z}$. On obtient la même contradiction avec le lemme 8.3.. Finalement, $b = 0$ et $D \subset C_0$ donc K est bien D-invariant.

Maintenant posons $M_2 = \left\{g \in G \mid g^{-1}K \cap \overline{H \cdot z} \neq \emptyset\right\}$. De même, si $g \in M_2 \cap N_G(U_1)$ alors $g^{-1}K \subset \overline{H \cdot z}$ par minimalité de K. Supposons par l'absurde que $H \cdot z$ n'est pas compacte. Pour obtenir une contradiction avec le lemme 8.3., il suffit comme précédemment de montrer que $U_2^{\pm}K \subset X$. Il suffit donc de voir que U_2^+ ou U_2^- appartient à M_2, car U_2 normalise déjà U_1. Mais le lemme 8.1. nous dit que $U_2 \cap M_2$ est non trivial, donc contient un certain $u_2(b)$ avec $b \neq 0$, et le fait que K soit D-invariant entraîne que M_2 est invariant par conjugaison par D ; on a donc $u_2(\frac{b}{t^2}) = d(-t)u_2(b)d(t) \in M_2$ pour tout t et cela implique que U_2^+ ou $U_2^- \subset M_2$.■

Quatrième partie 4. Version quantitative de la conjecture d'Oppenheim

Dans cette quatrième partie, qui constitue le second axe de ce mémoire, nous allons démontrer l'estimée asymptotique donnée en introduction qui concerne le nombre de points entiers compris entre deux lignes de niveau d'une forme non dégénérée irrationnelle q. Introduisons quelques notations.

Notations 9.1. *On note Ω un ouvert étoilé en 0 de la forme $\{x \in \mathbb{R}^n \mid \|x\| < \rho(x/\|x\|)\}$ où ρ est une fonction continue strictement positive sur la sphère unité S^{n-1}.*

On note aussi

$$\begin{aligned} V^q_{a,b}(\mathbb{R}) &= \{x \in \mathbb{R}^n \mid a < q(x) < b\} \\ V^q_{a,b}(\mathbb{Z}) &= \{x \in \mathbb{Z}^n \mid a < q(x) < b\} \end{aligned}$$

Un calcul facile, que nous effectuerons au §14, et qui précise l'asymptotique du volume de $V^q_{a,b}(\mathbb{R})$, montre que lorsque $T \to \infty$,

$$\lambda(V^q_{a,b}(\mathbb{R}) \cap T\Omega) \sim c_{q,\Omega}(b-a)T^{n-2} \tag{14}$$

où λ est la mesure de Lebesgue et $c_{q,\Omega}$ est une constante qui peut s'exprimer ainsi :

$$c_{q,\Omega} = \int_{C(q)\cap\Omega} \frac{ds}{\|\nabla q\|} \tag{15}$$

où ds est la mesure de surface sur le cône isotrope de q, $C(q)$.

Dans ce qui suit nous nous intéresserons au comportement asymptotique du cardinal $\left|V^q_{a,b}(\mathbb{Z}) \cap T\Omega\right|$ lorsque $T \to \infty$. Le théorème principal sera le suivant :

Théorème 9.1. *Soit q une forme quadratique réelle irrationnelle et de signature $(p, n-p)$ avec $n \geqslant 4$ et $p \geqslant 3$, alors pour tous $a < b$,*

$$\left|V^q_{a,b}(\mathbb{Z}) \cap T\Omega\right| \sim c_{q,\Omega}(b-a)T^{n-2} \tag{16}$$

Ce résultat peut être interprété comme l'équidistribution de la suite des points de $q(\mathbb{Z}^n \cap T\Omega)$ dans $\mathbb{R}$. La restriction sur la signature de q est nécessaire et nous exhiberons des contre-exemples. Pour ce qui est des généralisations de ce théorème ainsi que le cas des signatures $(2,2)$ et $(2,1)$ on se reportera à la dernière section de cette partie.

Ce résultat implique évidemment la conjecture d'Oppenheim dans le cas de ces signatures. En fait, dans la preuve de ce théorème, nous utiliserons un résultat beaucoup plus fort, le théorème d'équirépartition de Ratner (cf. thm 6.2.).

10. Schéma de la démonstration

10.1. **Résumé de la preuve.** Donnons tout d'abord une idée de l'intuition sous-jacente à la preuve du théorème 9.1. Tout d'abord, notons que l'équivalent 16 se ramène au suivant

$$\left|V^q_{a,b}(\mathbb{Z}) \cap T\left]\frac{1}{2}, 1\right]\partial\Omega\right| \underset{T\to\infty}{\sim} c'_{q,\Omega}(b-a)T^{n-2} \tag{17}$$

où $c'_{q,\Omega} = c_{q,\Omega}(1 - \frac{1}{2^{n-2}})$, comme le montre un résultat classique sur les séries numériques. Notons χ la fonction indicatrice de $\left]-\frac{1}{2}, 1\right]\partial\Omega \times]a,b[$. Le problème se résume donc à trouver la limite suivante :

$$\lim_{T\to\infty} \frac{1}{T^{n-2}} \sum_{v\in\mathbb{Z}^n} \chi(v/T, q(v))$$

Et de montrer ensuite qu'elle coïncide avec la limite de la même expression où l'on remplace la somme par l'intégrale sur $\mathbb{R}^n$ par rapport à la mesure de Lebesgue. Comme pour montrer l'équirépartition d'une suite réelle, on va approcher χ par des fonctions continues.

L'idée de la démonstration est de se placer dans l'espace des réseaux G/Γ pour y exploiter le théorème d'équirépartition de Ratner. Un moyen naturel pour passer d'une fonction de $\mathbb{R}^n$ à une fonction sur l'espace des réseaux est de faire sa somme sur tous les points du réseau, comme en 4.6.

$$\widetilde{f}(\dot{g}) = \sum_{v\in\mathbb{Z}^n} f(gv)$$

où $f \in C_c(\mathbb{R}^n)$ (fonctions continues à support compact) ; et la formule de Siegel relie l'intégration de $\widetilde{f}$ dans l'espace des réseaux à celle de f dans $\mathbb{R}^n$.

Dans la suite, on va chercher à approximer $\frac{1}{T^{n-2}}\chi(v/T, q(v))$, et c'est assez technique (voir §13), par une intégrale d'une fonction f convenable par rapport à la mesure de Haar d'un sous-groupe maximal compact K_q du groupe orthogonal H_q de q, soit une expression de la forme $\int_{K_q} f(a_T kv)dk$, où (a_t) est un certain sous-groupe à un paramètre de H_q (ou plutôt ici $a_T a_S = a_{TS}$). De sorte que le problème se ramène à l'étude de la limite quand $T \to \infty$ de l'expression suivante :

$$\int_{K_q} \widetilde{f}(a_T k)dk = \sum_{v\in\mathbb{Z}^n} \int_{K_q} f(a_T kv)dk$$

C'est là que le théorème d'équirépartition de Ratner va intervenir. Seulement, le théorème de Ratner n'est valable d'une part que pour des flots unipotents, et d'autre part que pour des fonctions continues bornées de l'espace des réseaux.

La première difficulté est aisément levée (voir §12.1.) : le sous-groupe (a_t) est en fait un analogue dans H_q du flot géodésique de $PSL_2(\mathbb{R})$ en géométrie hyperbolique. Mais les grandes sphères dans le demi-plan de Poincaré sont très bien approchables par des horocyles. Cette propriété classique permet d'approcher $\int_{K_q} \widetilde{f}(a_T k)dk$ par une moyenne orbitale de Birkhoff du type $\frac{1}{\varepsilon T}\int_T^{(1+\varepsilon)T}\int_{K_q}\widetilde{f}(u_t k)dkdt$ où u_t est l'image du flot horocyclique (i.e. est unipotent) à laquelle s'applique directement le théorème de Ratner 6.2. Or $k\mathbb{Z}^n$ n'est pas singulier pour $U=\{u_t\}$ pour presque tout $k\in K_q$ car q est irrationnelle (voir la structure de l'ensemble singulier en 6.2.2.), donc pour presque tout k, les orbites sont équidistribuées dans G/Γ pour la mesure de probabilité invariante μ sur G/Γ (voir thm 6.2.). On s'attend donc à obtenir la limite suivante :

$$\int_{K_q}\widetilde{f}(a_T k)dk \underset{T\to\infty}{\to} \int_{G/\Gamma}\widetilde{f}d\mu=\int_{\mathbb{R}^n} f dx \tag{18}$$

L'égalité de droite est la formule de Siegel. Alors, il ne reste plus qu'à relier l'intégrale de f à celle de χ pour obtenir 17.

La deuxième difficulté est en fait le coeur du problème. Le fait que $\int_{K_q}\widetilde{f}(a_T k)dk$ converge quand $T\to\infty$ doit impliquer en particulier que cette expression est bornée! Mais ça n'a rien d'évident à priori car $\widetilde{f}$ est certes continue, mais jamais bornée sur l'espace des réseaux. D'autre part un simple argument de troncature (voir §12.2.) montre que si $\int_{K_q}\left(\widetilde{f}(a_T k)\right)^{\theta}dk$ est borné quand T varie pour un certain $\theta>1$, alors la convergence de $\int_{K_q}\widetilde{f}(a_T k)dk$ se déduit du cas où $\widetilde{f}$ est remplacée par une fonction continue à support compact. Etant donné que les fonctions $\widetilde{f}$ sont toutes majorées par la fonction α (voir 4.2.2. pour sa définition et 4.5. et 4.6. pour quelques-unes de ses propriétés) il suffit donc de montrer l'existence d'un $\theta>1$ tel que

$$\sup_{T\geqslant 0}\int_{K_q}(\alpha(a_T k))^{\theta}\,dk<\infty \tag{19}$$

Il s'agit d'étudier de près le comportement de la fonction α au voisinage de l'infini dans l'espace des réseaux. On sait déjà que $\ln\alpha$ est uniformément continue et que α est dans L^r pour $1\leqslant r<n$ (voir §4.5.), mais cela ne suffit pas. On va donc d'abord s'intéresser aux intégrales $\int_{K_q}\frac{1}{\|a_T kx\|^{\theta}}dk$ et montrer qu'elles tendent vers 0 quand T tend vers l'infini, uniformément quand $x=x_1\wedge\ldots\wedge x_i\in\Lambda^i(\mathbb{Z}^n)$ varie dans un certain compact. Cela nous donnera une inégalité intégrale pour la fonction $\alpha(g)$ (qui n'est autre que la borne supérieure des $\frac{1}{\|gx\|}$ quand $x=x_1\wedge\ldots\wedge x_i\in\Lambda^i(\mathbb{Z}^n)$ et i varient) d'où on déduira 19.

Dans la suite de ce mémoire, nous allons mener la preuve décrite ci-dessus en détail. On donnera tout d'abord la preuve du **résultat d'intégrabilité** 19 qui requiert une compréhension détaillée de la structure combinatoire de l'espace des réseaux. Ensuite, nous verrons comment ce résultat, conjugué au théorème d'équirépartition de Ratner, permet d'obtenir la limite 18 qui constitue le principal **résultat d'ergodicité** de cette preuve. Enfin, nous expliquerons en détail **l'approximation de** χ par les intégrales du type $\int_{K_q} f(a_T kv)dk$, et nous montrerons finalement comment le théorème est déduit de 18.

Dans le paragraphe suivant, nous fixons les notations.

10.2. **Notations.** En plus des notations déjà introduites au début de cette partie, nous fixerons les suivantes :

On note ici aussi $G=SL_n(\mathbb{R})$, $\Gamma=SL_n(\mathbb{Z})$.

On fixe $n \geqslant 3$, $p \geqslant 2$, $(e_1, ..., e_n)$ la base canonique de $\mathbb{R}^n$ et $\|\cdot\|$ la norme euclidienne. On note pour $x = x_1 e_1 + ... + x_n e_n$,

$$q_0(x) = 2x_1 x_n + \sum_{i=2}^{p} x_i^2 - \sum_{i=p+1}^{n-1} x_i^2$$

On remarque que dans le théorème 9.1., on peut se ramener à un multiple de q. Comme q, de signature $(p, n-p)$ est de discriminant $(-1)^{n-p}$, un certain multiple de q est de déterminant précisément $(-1)^{n-p}$ donc il existe $g \in G$ tel que $q = q_0 \circ g$.

On note $H = SO(q_0)$ le groupe orthogonal spécial de q_0 et $K = H \cap O_n(\mathbb{R})$ les matrices orthogonales qui appartiennent à H.

On note (a_t) le sous-groupe à un paramètre de H défini par $a_t e_1 = e^{-t} e_1$, $a_t e_i = e_i$ pour $1 < i < n$ et $a_t e_n = e^t e_n$.

La base $(f_1, ..., f_n)$ définie par $f_i = e_i$ pour $1 < i < n$ et $f_1 = \frac{1}{\sqrt{2}}(e_1 + e_n)$, $f_n = \frac{1}{\sqrt{2}}(e_1 - e_n)$ est orthonormale pour le produit scalaire euclidien et orthogonale pour q_0.

Le sous-espace $L_1 = vect(f_1, ..., f_p)$ est le sous-espace propre de la matrice de q_0 correspondant à la valeur propre 1, et son orthogonal (au sens de q_0) est le sous-espace $L_2 = vect(f_{p+1}, ..., f_n)$ qui est aussi le sous-espace propre associé à -1. Cette remarque permet de voir immédiatement que K est précisément l'ensemble des matrices de H qui laissent invariant L_1. K s'identifie donc avec $S(O(p) \times O(n-p))$ où chacun des facteurs correspond au groupe orthogonal de chaque espace L_i pour la base (f_i).

De plus, vu que H est un groupe algébrique stable par adjonction, $H \cap U(n) = K$ est un sous-groupe compact maximal de H (cf. §5.5.).

On note dk la mesure de Haar normalisée sur K.

On note S_i pour $i = 1$ ou 2, la sphère unité de L_i.

On note γ_n le volume usuel de la sphère S^{n-1} et $c_p = \gamma_{p-1}\gamma_{n-p-1}/2^{(n-2)/2}$.

α est la fonction sur G/Γ définie en 4.5.

χ est la fonction indicatrice de $\left]\frac{1}{2}, 1\right] \partial\Omega \times]a, b[$.

Remarque 10.1. *Les résultats mentionnés dans le résumé de la preuve on été énoncés pour q irrationnelle quelconque par rapport au réseau $\mathbb{Z}^n$. Il revient au même de fixer q (ici q_0) et de faire varier le réseau. C'est ce que nous faisons dans la suite.*

11. Résultat d'intégrabilité

Dans ce paragraphe, nous allons donner la preuve du résultat d'intégrabilité 19 mentionné plus haut, qui est l'étape essentielle en vue d'utiliser le théorème d'équirépartition de Ratner (thm 6.2.). D'après la remarque précédente, ceci peut être formulé de la façon suivante :

Théorème 11.1. *Si $p \geqslant 3$ et $0 < s < 2$, alors pour tout réseau unimodulaire Δ,*

$$\sup_{t \geqslant 0} \int_K (\alpha(a_t k \Delta))^s \, dk < \infty$$

Cet énoncé est faux lorsque $p \leqslant 2$ même pour $s = 1$. C'est la raison pour laquelle le théorème principal ne s'applique pas à ces signatures.

Comme il a été mentionné plus haut, nous allons d'abord nous intéresser au comportement de $\int_K \frac{dk}{\|a_t k v\|^s}$ quand $t \to \infty$, où $v = x_1 \wedge ... \wedge x_i$.

11.1. **Intégrabilité pour la fonction $\frac{1}{\|v\|}$.** On va s'employer ici à démontrer le résultat suivant.

Proposition 11.1. *On suppose $p \geqslant 3$, et on note*

$$F(i) = \left\{v = x_1 \wedge ... \wedge x_i \in \Lambda^i(\mathbb{R}^n) \text{ tels que } \|v\| = 1\right\}$$

où la norme est la norme euclidienne sur $\Lambda^i(\mathbb{R}^n)$ (i.e. dont une base orthogonale est la base canonique $(e_{k_1} \wedge ... \wedge e_{k_i})_{k_1<...<k_i}$).. Alors, pour tout $0 < s < 2$,

$$\lim_{t\to\infty} \sup_{v\in F(i)} \int_K \frac{dk}{\|a_t kv\|^s} = 0$$

Nous allons déduire cette proposition des trois lemmes qui suivent ($Lie(G)$ désigne l'algèbre de Lie du groupe G).

Lemme 11.1. *Soit E un espace euclidien, K_0 un sous-groupe connexe fermé du groupe orthogonal $O(E)$, F un compact de la sphère unité de E et A un endomorphisme autoadjoint de E dont les valeurs propres sont 1, 0 et -1. On note E^+, E^0 et E^- les sous-espaces propres associés respectivement et on suppose de plus que :*

1. *$\forall v \in F$, $K_0 v \nsubseteq E^- + E^0$*
2. *$\forall v \in E^- - \{0\}$, $codim\{x \in Lie(K_0) \mid xv \in E^-\} \geq 2$*

Alors, pour tout $s \in]0, 2[$,

$$\lim_{t\to\infty} \sup_{v\in F} \int_{K_0} \frac{dk}{\|\exp(tA)kv\|^s} = 0 \tag{20}$$

où dk est la mesure de Haar de masse 1 sur K_0.

***Preuve*:** On considère p la projection orthogonale sur $E^+ \oplus E^0$, p^+ celle sur E^+. On note alors pour $v \in S$ (sphère unité) et $r \geq 0$,

$$\begin{aligned} D(v,r) &= \{k \in K_0 \mid \|p(kv)\| \leq r\} \\ D^+(v,r) &= \{k \in K_0 \mid \left\|p^+(kv)\right\| \leq r\} \end{aligned}$$

On note enfin $f_v(k) = p(kv)$. On a $Im(d_k f_v) = p(Lie(K_0) \cdot kv)$. Donc la condition 2 de l'énoncé entraîne que le rang de f_v en un point k tel que $p(kv) = 0$ est au moins 2. Le rang étant semi-continu inférieurement, il en résulte que pour tout $k \in K_0$ et $v \in S$ tels que $p(kv) = 0$, le rang de f_w en k' est encore au moins 2, lorsque k et w varient dans un voisinage de (k, v). Par compacité de $K_0 \times S$, on en déduit l'existence de $\varepsilon > 0$, tel que f_v est de rang au moins 2 en k dès que $\|p(kv)\| < \varepsilon$. La condition sur le rang implique que dans un système de coordonnées locales au voisinage de (k, v), f_v s'écrit $f_v(x_1, ..., x_m) = (x_1, x_2, \phi_3(x, v), ..., \phi_n(x, v))$. On peut recouvrir $\{(k, v) | \|p(kv)\| < \varepsilon\}$ par N tels voisinages où f_v a cette forme. Soit V un tel voisinage et $V_v = \{k|(k, v) \in V\}$, on a alors

$$dk(D(v,r) \cap V_v) \leq cr^2$$

où c est une constante qui de dépend que de dk. En notant $C = cN$, il vient pour tout $v \in S$,

$$dk(D(v,r)) \leq Cr^2$$

puis

$$\sup_{v\in S, r>0} \frac{dk(D(v,r))}{r^2} \leq C < \infty \tag{21}$$

Ensuite, on remarque que lorsque $v \in F$, $D^+(v,0)$ est une sous-variété algébrique stricte (condition 1 de l'énoncé) de K_0. Puisque K_0 est connexe, on a nécessairement $dk(D^+(v,0)) = 0$. Mais

$$dk(D^+(v,r)) \underset{r\to 0}{\downarrow} dk(D^+(v,0)) = 0$$

Cette décroissance et la compacité de F entraînent alors

$$\lim_{r\to 0} \sup_{v\in F} dk(D^+(v,r)) = 0 \tag{22}$$

Enfin, en décomposant $x \in E$ dans la base de vecteurs propres de A, on obtient pour $t \geq 0$,

$$\|\exp(tA)x\|^s \geq \max\left\{\|p(x)\|^s, e^{ts}\left\|p^+(x)\right\|^s\right\} \tag{23}$$

Il vient d'après 21 et l'inégalité précédente, pour tout $v \in S$,

$$\int_{D(v,r)-D(v,r/2)} \frac{dk}{\|\exp(tA)kv\|^s} \leq \frac{Cr^2}{(r/2)^s} = 2^s Cr^{2-s}$$

En prenant $r = r_0/2^n$, la série des intégrales obtenue converge, il vient puisque $dk(D(v,0)) \leq dk(D^+(v,0)) = 0$, pour tout $v \in F$, et $r_0 > 0$,

(24)

$$\int_{D(v,r_0)} \frac{dk}{\|\exp(tA)kv\|^s} = \sum_{n=0}^{\infty} \int_{D(v,r_0/2^n)-D(v,r_0/2^{n+1})} \frac{dk}{\|\exp(tA)kv\|^s} \leq \frac{4C}{2^{2-s}-1} r_0^{2-s}$$

Enfin, si $r_1 \leq r_0$, en appliquant à nouveau l'inégalité 23, on a

$$\begin{aligned} \int_{K_0-D(v,r_0)} \frac{dk}{\|\exp(tA)kv\|^s} &\leq \int_{K_0-D^+(v,r_1)} \frac{dk}{\|\exp(tA)kv\|^s} + \int_{D^+(v,r_1)-D(v,r_0)} \frac{dk}{\|\exp(tA)kv\|^s} \\ &\leq e^{-ts} r_1^{-s} + dk(D^+(v,r_1)) r_0^{-s} \end{aligned} \tag{25}$$

Il reste à prendre le sup de 24 et 25 sur les $v \in F$, puis prendre r_0 assez petit pour que le terme de droite de 24 soit petit, prendre ensuite r_1 assez petit pour que $\sup_{v\in F} dk(D^+(v,r_1)) r_0^{-s}$ soit arbitrairement petit (ce qui est rendu possible par 22), et enfin faire tendre t vers l'infini pour rendre le terme de droite de 25 arbitrairement petit. On a donc bien

$$\lim_{t\to\infty} \sup_{v\in F} \int_{K_0} \frac{dk}{\|\exp(tA)kv\|^s} = 0$$

■

Dans le lemme suivant, nous allons montrer que les hypothèses du lemme précédent sont vérifiées dans le cas particulier qui va nous intéresser ensuite.

Lemme 11.2. *On reprend les notations du lemme précédent, mais, à la place des hypothèses 1 et 2 on suppose :*

1. $\forall v \in F$, $K_0 v \nsubseteq E^0$
2. *Il existe un sous-groupe fermé, stable par adjonction,* H_1 *de* $GL(E)$*, localement isomorphe à* $SO_{3,1}$*, tel que* $H_1 \cap K_0$ *est un sous-groupe compact maximal de* H_1*, et tel que* $A \in Lie(H_1)$*.*

Alors les conditions 1 et 2 du lemme précédent sont vérifiées et, en particulier on a 20.

***Preuve*:** Après une renormalisation convenable, on peut supposer que les valeurs propres de adA sont précisément $-1, 0$ et 1. Alors

$$Lie(H_1) = \mathfrak{h}^- \oplus \mathfrak{h}^0 \oplus \mathfrak{h}^+$$

où

$$\begin{aligned} \mathfrak{h}^- &= \{x \in Lie(H_1) \mid [A, x] = -x\} \\ \mathfrak{h}^0 &= \{x \in Lie(H_1) \mid [A, x] = 0\} \\ \mathfrak{h}^+ &= \{x \in Lie(H_1) \mid [A, x] = x\} \end{aligned}$$

Alors $\mathfrak{h}^-$, $\mathfrak{h}^+$ et $\mathfrak{h}^0$ sont des sous-algèbres de $Lie(H_1)$ et pour tout $x \in \mathfrak{h}^+$ il existe un unique $\alpha(x) \in \mathfrak{h}^-$ tel que $[x, \alpha(x)] = A$. Alors x, A et $\alpha(x)$ forment un $\mathfrak{sl}_2(\mathbb{R})$-triplet. D'autre part, on remarque que pour tout $v \in E^- + E^+$, $v \notin E^-$ on a,

$$\left\{x \in Lie(H_1) \mid xv \in E^+ + E^0\right\} = \mathfrak{h}^- \oplus \mathfrak{h}^0 \tag{26}$$

Mais l'intersection de l'algèbre de Lie de tout sous-groupe compact stable par adjonction de H_1 avec $\mathfrak{h}^- \oplus \mathfrak{h}^0$ est en fait dans $\mathfrak{h}^0$, donc

$$Lie(K_0) \cap (\mathfrak{h}^- \oplus \mathfrak{h}^0) \subseteq \mathfrak{h}^0 \tag{27}$$

Enfin, comme $K_0 v \nsubseteq E^0$ pour tout $v \in F$, on obtient par 26 et 27 que $K_0 v \nsubseteq E^- + E^0$ ce qui est la première hypothèse du lemme précédent. D'autre part, on a $\dim(K_0 \cap H_1) = 3$ et $\dim(Lie(K_0) \cap \mathfrak{h}^0) = 1$ donc au vu de 26 et 27, la condition 2 du lemme précédent est aussi vérifiée.■

Finalement, l'énoncé qui suit va nous permettre d'appliquer le lemme précédent à la situation de la proposition 11.1.

Lemme 11.3. *Soit G un groupe de Lie simple connexe inclus dans $SL_n(\mathbb{R})$ qui agit irréductiblement sur $\mathbb{R}^n$. On suppose que G possède un sous-groupe compact maximal K qui contient le centre de G. Pour tout sous-espace vectoriel non trivial L de $\mathbb{R}^n$, on note*

$$G_L = \{g \in G \mid g(kL) = kL \ \forall k \in K\}$$

Alors $G_L^0 \subseteq K$.

***Preuve*:** Puisque KL est invariant par K, $K \subseteq N_G(G_L)$ normaliseur de G_L (qui sont tous deux des sous-groupes de Lie de G). Mais puisque G est simple et K compact maximal de G, K (qui est alors connexe) est maximal parmi tous les sous-groupes de Lie connexes de G. Donc $N_G(G_L) = G$ ou $N_G(G_L)^0 = K$. Dans le second cas, $G_L^0 \subseteq K$. Dans le premier cas, G_L est donc distingué dans G. Mais puisque G est simple, on a $G_L = G$ ou $G_L^0 = \{id\}$. Le premier cas est impossible car L est non trivial et G agit irrédutiblement sur $\mathbb{R}^n$. Le second cas entraîne que G_L est dans le centre de G (tout sous-groupe discret et normal d'un groupe topologique connexe est central), donc dans K.■

Nous pouvons désormais passer à la preuve de la proposition 11.1.

***Preuve de la proposition*:** On peut écrire $a_t = \exp(tA)$, où A est un endomorphisme autoadjoint de $\mathbb{R}^n$ dont les valeurs propres sont $-1, 0$ et 1 ($A = diag(-1, 0, ..., 0, 1)$). Soit H_0 le sous-groupe de H qui laisse fixe $(e_4, ..., e_{n-1})$. On a $a_t \in H_0 \simeq SO_{3,1}$. On considère l'action de $GL_n(\mathbb{R})$ sur l'algèbre extérieure $\Lambda^*(\mathbb{R}^n)$. Alors $\Lambda^i(A)$ est encore autoadjoint et ses valeurs propres sont -1, 0 et 1. Il suffit de vérifier les hypothèses du lemme 11.2. avec $E = \Lambda^i(\mathbb{R}^n)$, $K_0 = \Lambda^i(K)$ et $F = F(i)$ et $H_1 = \Lambda^i(H_0)$. Les hypothèses concernant H_1 sont satisfaites. Il reste à voir que $Kv \nsubseteq E^0$ pour tout $v \in F(i)$. Mais, on constate que pour tout $t \neq 0$,

(28) $$E^0 = \{v \in \Lambda^i(\mathbb{R}^n) \mid a_t v = v\}$$

Par ailleurs, si L désigne le sous-espace de $\mathbb{R}^n$ associé à $v \in F(i)$, L est strict et non nul car $0 < i < n$. On peut alors appliquer le lemme précédent à $G = H^0$ (qui est simple dès que $(p, n-p) \neq (2,2)$ et agit irreductiblement sur $\mathbb{R}^n$ car il agit transitivement sur les surfaces de niveaux (cf. lemme 5.1.) lesquelles ne sont contenues dans aucun hyperplan). Donc avec les notations du lemme précédent :

(29) $$G_L^0 \subseteq K$$

Etant donné que $a_t \notin K$ pour tout $t \neq 0$, il existe $t \neq 0$ petit tel que $a_t \notin G_L$. 28 implique donc que $Kv \nsubseteq E^0$ pour tout $v \in F(i)$. ■

11.2. **Inégalité intégrale pour α.** Comme il a été annoncé dans le résumé de la preuve, la proposition 11.1. fournit une inégalité intégrale pour α. Plus précisément,

Proposition 11.2. *Soit* $1 \leqslant i \leqslant n-1$ *et* $s \in \,]0,2[$. *Alors* $\forall \varepsilon > 0$ $\exists t_0 \geqslant 0$, $\forall t \geqslant t_0$ $\forall \Delta \in G/\Gamma$,

$$\int_K \alpha_i(a_t k\Delta)^s dk \leqslant \frac{\varepsilon}{2}\alpha_i(\Delta)^s + e^{4t} \max_{0<j\leqslant \min\{i,n-i\}} (\alpha_{i+j}(\Delta)\alpha_{i-j}(\Delta))^{\frac{s}{2}}$$

***Preuve*:** Rappelons que $F(i) = \{v = x_1 \wedge \ldots \wedge x_i \in \Lambda^i(\mathbb{R}^n) \text{ tels que } \|v\| = 1\}$. On a donc d'après la proposition 11.1. l'existence d'un t_0 tel que $\forall t \geq t_0$

$$\sup_{v \in F(i)} \int_K \frac{dk}{\|a_t k v\|^s} \leq \frac{\varepsilon}{2}$$

On fixe maintenant $t \geq t_0$ et $\Delta \in G/\Gamma$. Si l'on note

$$F_\Delta(i) = \{v = x_1 \wedge \ldots \wedge x_i \in \Lambda^i(\Delta) - \{0\}\}$$

on a, pour tout $v \in F_\Delta(i)$,

(30) $$\int_K \frac{dk}{\|a_t k v\|^s} \leq \frac{\varepsilon}{2}\frac{1}{\|v\|^s} \leq \frac{\varepsilon}{2} \sup_{v \in F_\Delta(i)} \frac{1}{\|v\|^s} = \frac{\varepsilon}{2}\alpha_i(\Delta)^s$$

Or, puisque $\left\{\frac{1}{\|v\|}, v \in F_\Delta(i)\right\}$ est discret, il existe $v \in F_\Delta(i)$ tel que $\frac{1}{\|v\|} = \alpha_i(\Delta)$. On écrit $v = x_1 \wedge \ldots \wedge x_i$ et on note $L_i = Vect(x_1, \ldots, x_i)$. On a alors $\|v\| = d_\Delta(L_i)$ où l'on note pour tout sous-espace Δ-rationnel F, $d_\Delta(F) = \det_F(F \cap \Delta)$. Mais $(a_t k x_1, \ldots, a_t k x_i)$ est une base de $a_t k L_i \cap a_t k \Delta$ pour tout $k \in K$ donc $\|a_t k v\| = d_{a_t k \Delta}(a_t k L_i)$. Avec ce v, 30 devient

$$\int_K \frac{dk}{(d_{a_t k\Delta}(a_t k L_i))^s} \leq \frac{\varepsilon}{2}\alpha_i(\Delta)^s$$

Mais $\alpha_i(a_t k\Delta) = \sup\left\{\frac{1}{d_{a_t k\Delta}(a_t k L)} \mid L\ \Delta\text{-rationnel et } \dim L = i\right\}$ par définition. Si $L = L_i$ réalise cette borne supérieure pour tout $k \in K$, alors 30 donne

(31) $$\int_K \alpha_i(a_t k\Delta)^s dk \leq \frac{\varepsilon}{2}\alpha_i(\Delta)^s$$

Dans le cas contraire, il existe un sous-espace L de dimension i et Δ-rationnel tel que pour un certain $k_0 \in K$,

$$d_{a_t k_0 \Delta}(a_t k_0 L) < d_{a_t k_0 \Delta}(a_t k_0 L_i)$$

d'où

$$d_\Delta(L) \leq \omega_i d_{a_t k_0 \Delta}(a_t k_0 L) < \omega_i d_{a_t k_0 \Delta}(a_t k_0 L_i) \leq \omega_i^2 d_\Delta(L_i) \tag{32}$$

où $\omega_i = \max\left\{\left\|\Lambda^i(a_t)\right\|, \left\|\Lambda^i(a_t)^{-1}\right\|^{-1}\right\} = e^t$. Or on a le lemme suivant

Lemme 11.4. *Soient L et M deux sous-espaces Δ-rationnels, alors $d_\Delta(L)d_\Delta(M) \geq d_\Delta(L \cap M)d_\Delta(L+M)$*

***Preuve*:** On considère la projection $\pi : \mathbb{R}^n \to \mathbb{R}^n/(L\cap M)$. Quitte à passer au quotient par π, on peut supposer que $L\cap M = \{0\}$. En effet, $\pi(\Delta)$ est un réseau de $\mathbb{R}^n/(L\cap M)$ (cf. proposition 5.4.) et $d_{\pi(\Delta)}(\pi(L))d_\Delta(L\cap M) = d_\Delta(L)$ et $d_{\pi(\Delta)}(\pi(M))d_\Delta(L\cap M) = d_\Delta(M)$, donc l'inégalité à démonter équivaut à

$$d_{\pi(\Delta)}((L))d_{\pi(\Delta)}(\pi(M)) \geq d_{\pi(\Delta)}(\pi(L+M))$$

Mais, dans le cas où $L \cap M = \{0\}$, on peut choisir une base $(e_1, ..., e_l)$ de L et $(e_{l+1}, ..., e_{l+m})$ de M telles que $e_1 \wedge ... \wedge e_{l+m} \in (L+M) \cap \Delta - \{0\}$. Par suite,

$$d_\Delta(L+M) \leq \|e_1 \wedge ... \wedge e_{l+m}\| \leq \|e_1 \wedge ... \wedge e_l\| \, \|e_{l+1} \wedge ... \wedge e_{l+m}\| = d_\Delta(L)d_\Delta(M)$$

■

Le lemme nous dit ici que $d_\Delta(L_i)d_\Delta(L) \geq d_\Delta(L_i \cap L)d_\Delta(L_i + L)$. Il vient pour tout $k \in K$,

$$\begin{aligned}\alpha_i(a_t k\Delta) &= \sup_{v\in F_\Delta(i)} \frac{1}{\|a_t k v\|} \leq e^t \sup_{v\in F_\Delta(i)} \frac{1}{\|v\|} = e^t \alpha_i(\Delta) = e^t \frac{1}{d_\Delta(L_i)} \\ &\leq e^{2t} \frac{1}{\sqrt{d_\Delta(L_i)d_\Delta(L)}}\end{aligned}$$

d'après 32. Puis d'après le lemme,

$$\alpha_i(a_t k\Delta) \leq e^{2t} \frac{1}{\sqrt{d_\Delta(L_i \cap L)d_\Delta(L_i + L)}} \leq e^{2t}\sqrt{\alpha_{i+j}(\Delta)\alpha_{i-j}(\Delta)}$$

où l'on note $\dim(L + L_i) = i + j > i$ car $L \neq L_i$. D'où

$$\int_K \alpha_i(a_t k\Delta)^s dk \leq e^{4t}\left(\alpha_{i+j}(\Delta)\alpha_{i-j}(\Delta)\right)^{\frac{s}{2}} \leq e^{4t} \max_{0<j\leqslant \min\{i,n-i\}} \left(\alpha_{i+j}(\Delta)\alpha_{i-j}(\Delta)\right)^{\frac{s}{2}} \tag{33}$$

Enfin, on obtient l'inégalité souhaitée en combinant 33 et 31.■

On va chercher à utiliser cette inégalité intégrale pour montrer le théorème 11.1. Pour cela, on montre d'abord la proposition suivante qui, appliquée à une fonction f convenable, permettra d'obtenir la borne supérieure souhaitée pour α.

Proposition 11.3. *Soit $\mathcal{A}$ un ensemble de fonctions f strictement positives et invariantes à gauche et à droite par les éléments de K, telles que de plus les $\ln f$ soient uniformément équicontinues pour la structure uniforme à gauche sur H (i.e. par rapport à une distance invariante sur G, cf. 1.4.). Alors, il existe une constante $c_0 > 0$, ne dépendant que de $\mathcal{A}$, telle que si $f \in \mathcal{A}$ vérifie la condition suivante*

$$\exists t \geq 0 \ \exists b > 0 \ \textit{tels que} \int_K f(a_t k h)dk \leq c_0 f(h) + b \ \forall h \in H \tag{34}$$

alors

$$\sup_{s>0} f(a_s) < \infty$$

Avant de démontrer cette proposition, il nous faut faire la remarque suivante, qui constitue essentiellement le "Wave Front lemma" de [EsM] :

Lemme 11.5. *Pour tout voisinage V de l'identité dans H, il existe un voisinage U de l'identité dans K, tel que*

$$a_tUa_s \subseteq KVa_ta_sK$$

pour tous $t \geq 0$ et $s \geq 0$.

***Preuve*:** Soit $\mathfrak{a}$ une sous-algèbre abélienne de dimension maximale de $\mathfrak{p} = S_n(\mathbb{R}) \cap \mathfrak{h}$ telle que $A = \exp \mathfrak{a}$ contienne $(a_t)_t$, où $\mathfrak{h}$ est l'algèbre de Lie de H. Pour tout $g \in G$, on considère sa décomposition KAK (cf. 5.5.3.), $g = k_g a_g k'_g$ avec k_g et k'_g dans K, et a_g une matrice de $A = \exp \mathfrak{a}$. L'ensemble des matrices diagonales de $\mathfrak{sl}_n(\mathbb{R})$ est une sous-algèbre abélienne maximale, donc d'après le théorème 5.5. (ou par un résultat élémentaire d'algèbre linéaire), il existe $o \in O_n(\mathbb{R})$ tel que $A \subseteq oDo^{-1}$ où D est l'ensemble des matrices diagonales. De plus, on note D^+ est l'ensemble des matrices diagonales. $diag(\lambda_1, ..., \lambda_n)$ avec $\lambda_1 \geq ... \geq \lambda_n > 0$ et $\lambda_i(g)$ la i-ème plus grande valeur propre de a_g (qui ne dépend que de g!). En considérant toujours la norme euclidienne, on remarque que $\|g\| = \lambda_1(g)$. Enfin, on se donne un voisinage V de l'identité dans H et on remarque qu'il existe $\varepsilon > 0$ tel que tout $a \in A$ qui vérifie $\left|\lambda_i(a^{-1}) - 1\right| \leq \varepsilon$ pour tout $i \in [1, n]$ est dans V.

D'autre part, il existe un voisinage U de l'identité dans K, tel que $\forall k \in U$, $\forall d_1, d_2 \in D^+$,$\forall i \in [1, n]$,

$$\left|\frac{\lambda_i(d_1kd_2)}{\lambda_i(d_1)\lambda_i(d_2)} - 1\right| \leq \varepsilon \tag{35}$$

La preuve de cette dernière assertion procède en considérant la représentation de G sur $\Lambda^i(\mathbb{R}^n)$. En effet, on remarque que, avec des notations évidentes, $\Lambda^i(g) = \Lambda^i(k_g)\Lambda^i(a_g)\Lambda^i(k'_g)$ et $\lambda_1(\Lambda^i(g)) = \lambda_1(g)...\lambda_i(g)$, donc

$$\lambda_i(g) = \frac{\lambda_1(\Lambda^i(g))}{\lambda_1(\Lambda^{i-1}(g))}$$

Il suffit donc de démontrer l'existence d'un voisinage U pour lequel $\forall k \in U$, $\forall d_1, d_2 \in D^+$,

$$\left|\frac{\lambda_1(\Lambda^i(d_1kd_2))}{\lambda_1(\Lambda^i(d_1))\lambda_1(\Lambda^i(d_2))} - 1\right| \leq \varepsilon$$

ce qui est clair s'il on prend pour $U = \left\{k \in K \mid (\Lambda^i(k)e_1 \wedge ... \wedge e_i, e_1 \wedge ... \wedge e_i) > 1 - \varepsilon\right\}$ car

$$\begin{aligned}\lambda_1(\Lambda^i(d_1kd_2)) &= \left\|\Lambda^i(d_1kd_2)\right\| \geq \left\|\Lambda^i(d_1kd_2)e_1 \wedge ... \wedge e_i\right\| \\ &\geq (1-\varepsilon)\lambda_1(\Lambda^i(d_1))\lambda_1(\Lambda^i(d_2))\end{aligned}$$

et

$$\lambda_1(\Lambda^i(d_1kd_2)) = \left\|\Lambda^i(d_1kd_2)\right\| \leq \left\|\Lambda^i(d_1)\right\| \left\|\Lambda^i(k)\right\| \left\|\Lambda^i(d_2)\right\| = \lambda_1(\Lambda^i(d_1))\lambda_1(\Lambda^i(d_2))$$

On fixe donc un tel U qui vérifie 35, et pour conclure il reste à observer que $(a_t)^{-1}$ est dans $D^+ \cap H$ dès que $t \geq 0$, et que pour tout $k \in U$ et $s, t \geq 0$ on a $a_tka_s = k_1ak_2 \in KAK$, et

$$\left|\lambda_i(a_ta_sa^{-1}) - 1\right| = \left|\frac{\lambda_i(a_t)\lambda_i(a_s)}{\lambda_i(a)} - 1\right| = \left|\frac{\lambda_i((a_tka_s)^{-1})}{\lambda_i(a_t^{-1})\lambda_i(a_s^{-1})} - 1\right| \leq \varepsilon$$

d'où $a \in Va_ta_s \Rightarrow a_tka_s \in KVa_ta_sK$.■

Passons maintenant à la démonstration de la proposition.

***Preuve de la proposition*:** L'équicontinuité uniforme des $\ln f$ ($f \in \mathcal{A}$) pour la structure uniforme à gauche sur H se traduit par l'existence d'un voisinage V de l'identité dans H tel que

$$\forall f \in \mathcal{A}, \forall h \in H, \forall u \in V, \frac{1}{2}f(h) \leq f(uh) \leq 2f(h)$$

D'après le lemme qui précède, il existe un voisinage U de l'identité dans K tel que $a_tUa_s \subseteq KVa_ta_sK$ pour tous $t \geq 0$ et $s \geq 0$. D'où en utilisant l'invariance par K et la stricte positivité de f,

$$\int_K f(a_tka_s)dk \geq \int_{U\cap K} f(a_tka_s)dk \geq \frac{f(a_ta_s)}{2}dk(U\cap K) \tag{36}$$

Posons $c_0 = \frac{1}{4}dk(U\cap K) > 0$ (la mesure de Haar est strictement positive sur les ouverts). Choisissons maintenant une fonction $f \in \mathcal{A}$, telle que

$$\exists t \geq 0 \; \exists b > 0 \text{ tels que } \int_K f(a_tkh) \leq c_0 f(h) + b \; \forall h \in H$$

Alors 36 entraîne que pour tout $s \geq 0$

$$f(a_ta_s) \leq \frac{1}{2}f(a_s) + \frac{2b}{c_0}$$

On en déduit aussitôt par récurrence que

$$\forall l \in \mathbb{N}, \; f(a_{lt}) \leq 2\max\{f(1), \frac{2b}{c_0}\}$$

Enfin, la continuité uniforme de $\ln f$ implique

$$\sup_{h\in H,\, 0\leq r\leq t} \frac{f(a_rh)}{f(h)} < \infty$$

Ce qui termine la preuve puisqu'alors

$$\sup_{s>0} f(a_s) \leq \sup_{l\in\mathbb{N}} \sup_{0\leq r\leq t} f(a_{lt+r}) < \infty$$

■

11.3. **Preuve du théorème 11.1.** Nous allons finalement exploiter la proposition 11.2. pour se mettre dans les hypothèses de la dernière proposition. Fixons $\Delta \in G/\Gamma$ et notons, pour $0 \leq i \leq n$,

$$f_i(h) = \int_K (\alpha_i(hk\Delta))^s \, dk$$

En prenant pour $\mathcal{A}$ le cône convexe engendré par les f_i, $\mathcal{A} = \left\{\sum_{i=0}^n \beta_i f_i, \, \beta_i > 0\right\}$ vérifie les hypothèses de la dernière proposition, puisque les α_i sont, d'après leur définition, invariantes à gauche par K et les $\ln \alpha_i$ uniformément continues pour la structure à gauche sur G (cf. 3.5.). Soit c_0 la constante donnée par la proposition. Il suffit alors de trouver un élément f de $\mathcal{A}$ vérifie l'hypothèse 34 de la proposition, c'est-à-dire

$$\exists t \geq 0 \; \exists b > 0 \text{ tels que } \int_K f(a_tkh) \leq c_0 f(h) + b \; \forall h \in H$$

Car alors, la proposition impliquera

$$\sup_{t>0} f(a_t) < \infty$$

ce qui entraîne

$$\forall i \;\sup_{t>0} f_i(a_t) < \infty$$

et il s'ensuit la conclusion souhaitée

$$\sup_{t>0} \int_K (\alpha(a_t k\Delta))^s < \infty$$

Posons donc, avec des $\beta_i > 0$,

$$f = \sum_{i=0}^{n} \beta_i f_i$$

D'après la proposition 11.2., on peut trouver t_0 assez grand tel que $\forall i, 0 < i < n$, $\forall h \in H$

$$\int_K \alpha_i(a_{t_0} kh\Delta)^s dk \leqslant \frac{c_0}{2}\alpha_i(h\Delta)^s + e^{4t_0} \max_{0<j\leqslant\min\{i,n-i\}} (\alpha_{i+j}(h\Delta)\alpha_{i-j}(h\Delta))^{\frac{s}{2}}$$

On remarque que α_0 et α_n sont constantes égales à 1. En sommant, il vient

$$\begin{aligned}\int_K \sum_{i=0}^{n} \beta_i\alpha_i(a_{t_0}kh\Delta)^s dk \quad &\leq \quad \beta_0 + \beta_n + \frac{c_0}{2}\sum_{i=0}^{n}\beta_i\alpha_i(h\Delta)^s \\ &\quad + e^{4t_0}\left[\sum_{i=1}^{n-1}\beta_i \max_{0<j\leqslant\min\{i,n-i\}} \frac{1}{2\sqrt{\beta_{i+j}\beta_{i-j}}}\right]\sum_{i=0}^{n}\beta_i\alpha_i(h\Delta)^s\end{aligned}$$

On cherche des β_i de sorte que le terme $\left[\sum_{i=0}^{n}\beta_i \max_{0<j\leqslant\min\{i,n-i\}} \frac{1}{2\sqrt{\beta_{i+j}\beta_{i-j}}}\right]$ soit petit. Pour cela on pose pour tout i,

$$\beta_i = \varepsilon^{i(n-i)}$$

et on trouve

$$\left[\sum_{i=0}^{n}\beta_i \max_{0<j\leqslant\min\{i,n-i\}} \frac{1}{2\sqrt{\beta_{i+j}\beta_{i-j}}}\right] \leq \varepsilon$$

Par suite en prenant $\varepsilon = \frac{c_0}{2ne^{4t_0}}$, on obtient que $\forall h \in H$,

$$\int_K \sum_{i=0}^{n}\beta_i\alpha_i(a_{t_0}kh\Delta)^s dk \leq 2 + c_0\sum_{i=0}^{n}\beta_i\alpha_i(h\Delta)^s$$

On remplaçant finalement h par hk' et en intégrant par rapport à k', il vient $\forall h \in H$,

$$\int_K f(a_{t_0}kh)dk \leq 2 + c_0 f(h)$$

Donc 34 est vérifiée, et d'après les remarques faites au début de la preuve, cela achève la démonstration du théorème 11.1.■

12. Résultat d'ergodicité

Comme mentionné plus haut, la borne supérieure que l'on vient de démontrer, conjuguée au théorème d'équirépartition de Ratner et au principe d'approximation des grands cercles par les horocycles permet de démontrer le principal résultat d'ergodicité utilisé ici :

Théorème 12.1. *Soit $p \geqslant 3$, σ une fonction continue sur K et ϕ une fonction continue sur l'espace des réseaux unimodulaires G/Γ telle que pour une certaine constante $C \geqslant 0$ et un certain s, $0 < s < 2$, on ait,*

$$|\phi| \leqslant C\alpha^s$$

Soit de plus $z \in G/\Gamma$ tel que $H \cdot z$ soit dense. Alors,

$$\lim_{t \to +\infty} \int_K \phi(a_t kz)\sigma(k)dk = \int_K \sigma(k)dk \int_{G/\Gamma} \phi(x)d\nu(x)$$

où ν est la probabilité G-invariante sur G/Γ (voir 2.5. pour sa définition et 4.4.2. pour sa finitude).

Ce théorème fournira en particulier la limite 18 annoncée dans le résumé de la preuve. Nous démontrons d'abord le résultat lorsque ϕ est continue à support compact dans G/Γ.

12.1. **Preuve pour une fonction test à support compact.**

Notons $u_T = \begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}$ le flot horocyclique dans $SL_2(\mathbb{R})$, $d_T = \begin{pmatrix} T & 0 \\ 0 & \frac{1}{T} \end{pmatrix}$ pour $T > 0$, $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, puis

$$\begin{aligned} b_T &= \frac{1}{\sqrt{1+T^{-2}}} \begin{pmatrix} 1 & 0 \\ -T^{-1} & 1+T^{-2} \end{pmatrix} \\ k_T &= \frac{1}{\sqrt{1+T^{-2}}} \begin{pmatrix} 1 & T^{-1} \\ -T^{-1} & 1 \end{pmatrix} \end{aligned}$$

On vérifie facilement que w et $k_T \in SO_2(\mathbb{R})$ puis que,

$$\begin{aligned} d_T &= b_T u_T k_T w \\ \lim_{T \to +\infty} b_T &= \lim_{T \to +\infty} k_T = id \end{aligned}$$

Soit H_1 le sous-groupe de H^0 qui laisse fixe $\{e_3, ..., e_{n-1}\}$. On a $H_1 \simeq SO^0_{1,2}$. Rappelons que l'on a un isomorphisme canonique entre $PSL_2(\mathbb{R})$ et $SO^0_{1,2}$ (voir §5.5.7.). On en déduit aisément l'existence d'un morphisme algébrique $\rho' : SL_2(\mathbb{R}) \to H_1$ tel que $\rho'(d_{e^{t/2}}) = a_t$ et $\rho'(SO_2(\mathbb{R})) \subseteq K$. On note d'_T (resp. b'_T, u'_T, k'_T, et w') les images par ρ' de d_T (resp. b_T, u_T k_T, et w). Alors u'_T est unipotente et k'_T et w' sont dans K.

On a alors pour toutes fonctions $\phi \in C_c(G/\Gamma)$ et $\sigma \in C(K)$ et pour tout $z \in G/\Gamma$,

$$\begin{aligned} \int_K \phi(d'_T kz)\sigma(k)dk &= \int_K \phi(b'_T u'_T k'_T w' kz)\sigma(k)dk \\ &= \int_K \phi(b'_T u'_T kz)\sigma(w'^{-1} k'^{-1}_T k)dk \end{aligned} \tag{37}$$

Puis on remarque, en utilisant 37 pour la dernière ligne, que pour $r > 0$ et $T > 0$

$$\begin{aligned}
&\left|\int_K \phi(d'_T kz)\sigma(k)dk - \int_K \phi(u'_{rT} kz)\sigma(w'^{-1}k)dk\right| \leqslant \\
&\left|\int_K \left(\phi(d'_T kz) - \phi(d'_{rT} kz)\right)\sigma(k)dk\right| + \left|\int_K \left(\phi(d'_{rT} kz)\sigma(k) - \phi(u'_{rT} kz)\sigma(w'^{-1}k)\right) dk\right| \\
= &\left|\int_K \left(\phi(d'_T kz) - \phi(d'_r d'_T kz)\right)\sigma(k)dk\right| + \left|\int_K \left(\phi(b'_{rT} u'_{rT} kz)\sigma(w'^{-1} k'^{-1}_{rT} k) - \phi(u'_{rT} kz)\sigma(w'^{-1}k)\right) dk\right|
\end{aligned}$$

Les fonctions ϕ et σ étant continues à support compact, elles sont uniformément continues et b'_T et k'_T tendent vers la matrice identité de G. Donc si l'on fixe un $\varepsilon > 0$, il existe $T_0 \geqslant 0$ et $\eta > 0$ tels que l'on ait

$$\left|\int_K \phi(d'_T kz)\sigma(k)dk - \int_K \phi(u'_{rT} kz)\sigma(w'^{-1}k)dk\right| \leqslant \frac{\varepsilon}{2} \tag{38}$$

quels que soient T et r avec $T > T_0$ et $|r-1| \leqslant \eta$. On intègre donc l'expression 38 par rapport à r entre 1 et $1+\eta$. D'où pour tout $T > T_0$,

$$\left|\int_K \phi(d'_T kz)\sigma(k)dk - \frac{1}{\eta T}\int_T^{(1+\eta)T}\int_K \phi(u'_t kz)\sigma(w'^{-1}k)dkdt\right| \leqslant \frac{\varepsilon}{2} \tag{39}$$

Considérons maintenant un réseau z soit tel que $H \cdot z$ soit dense. D'après §6.1. ceci est équivalent au fait que la forme quadratique $q_0 \circ g$ où $z = g\mathbb{Z}^n$ est irrationnelle. Dans ce cas (cf. §6.2.2.) on sait que pour tout sous-groupe à un paramètre unipotent U de H, l'ensemble des points singuliers $\mathcal{S}(U)\Gamma$, qui correspond aux points d'orbites non dense, est une réunion dénombrable de sous-variétés analytiques propres de G. Par suite, $Kg \cap \mathcal{S}(U)\Gamma$ est aussi un réunion dénombrable de sous-variétés analytiques de Kg. Supposons par l'absurde que l'une d'entre elles est de même dimension que Kg. Elle contient donc un ouvert de Kg. Puisque Kg est connexe et par le principe du prolongement analytique elle coïncide avec Kg. D'après la forme de $\mathcal{S}(U)$, en reprenant les notations du §6.2.2. on a donc un sous-groupe fermé propre F de G tel que $F \cap \Gamma$ est un réseau de F et $\gamma \in \Gamma$ tels que $Kg \subseteq X(F,U)\gamma$.

Montrons que cela contredit l'hypothèse faite sur z, à savoir $H \cdot z$ dense. $Kg \subseteq X(F,U)\gamma$ s'écrit encore $k^{-1}Uk \subseteq g\gamma^{-1}F\gamma g^{-1}$ pour tout $k \in K$. Notons L le sous-groupe fermé engendré par $\bigcup_{k\in K} kUk^{-1}$. Son normalisateur dans H^0, $N_{H^0}(L)$, est un sous-groupe de Lie de H_0 qui contient K et U, donc contient strictement K. Or, puisque $p \geq 3$, H^0 est un groupe de Lie simple (cf. §5.1.), donc K est maximal parmi tous les sous-groupes de H^0. Il s'ensuit que L est distingué dans H^0. Comme L n'est pas inclus dans le centre de H^0, il s'ensuit de même que $L = H^0$. D'où $H^0 \subseteq g\gamma^{-1}F\gamma g^{-1}$ et par suite $H^0 \cdot z \subseteq g\gamma^{-1}F \cdot \mathbb{Z}^n$. Cela implique que $F \cdot \mathbb{Z}^n$ est dense dans l'espace des réseaux. Mais cette orbite est déjà fermée puisque $F \cap \Gamma$ est un réseau de F (cf. §2.5.) donc elle est égale à G/Γ tout entier et cela contredit le fait que F est un sous-groupe propre de G.

On en déduit donc que toutes les sous-variétés analytiques dont $Kg \cap \mathcal{S}(U)\Gamma$ est la réunion dénombrable sont de dimension inférieure à la dimension de Kg. $Kg \cap \mathcal{S}(U)\Gamma$ est donc de mesure nulle pour le volume Riemannien de Kg. Enfin, puisque la mesure de Haar sur K est absolument continue par rapport au volume Riemannien, dk-presque partout kz n'est pas singulier.

En particulier ce qui précède est valable pour $U = \{u'_t \mid t \in \mathbb{R}\}$. Le théorème d'équirépartition de Ratner (cf. thm 6.) affirme alors que l'on a la limite suivante dk-presque partout:

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T f(u'_t kz)dt = \int_{G/\Gamma} f d\nu$$

où $d\nu$ est la probabilité G-invariante sur G/Γ et f n'importe quelle fonction continue bornée. De façon équivalente on a pour tout $\eta > 0$,

$$\lim_{T\to\infty}\frac{1}{\eta T}\int_T^{(1+\eta)T} f(u'_t kz)dt = \int_{G/\Gamma} f d\nu \tag{40}$$

d'où dk-presque partout :

$$\lim_{T\to\infty}\frac{1}{\eta T}\int_T^{(1+\eta)T} \phi(u'_t kz)\sigma(w'^{-1}k)dt = \sigma(w'^{-1}k)\int_{G/\Gamma}\phi d\nu$$

Le terme de gauche dont on prend la limite est évidemment borné par le sup de ϕ et σ. Par convergence dominée, on a donc,

$$\lim_{T\to\infty}\int_K \frac{1}{\eta T}\int_T^{(1+\eta)T}\phi(u'_t kz)\sigma(w'^{-1}k)dtdk = \int_K \sigma(w'^{-1}k)dk\int_{G/\Gamma}\phi d\nu = \int_K \sigma(k)dk\int_{G/\Gamma}\phi d\nu$$

De 39 on déduit la limite souhaitée en appliquant Fubini et en rappelant que $d'_{e^{t/2}} = a_t$

$$\lim_{t\to\infty}\int_K \phi(a_t kz)\sigma(k)dk = \int_K \sigma(k)dk\int_{G/\Gamma}\phi d\nu$$

12.2. **Réduction à ce dernier cas.** On se place maintenant dans le cas général. On considère donc ici une fonction ϕ qui satisfait les hypothèses du théorème 10.2., c'est-à-dire continue et majorée par $C\alpha^s$ pour $0 < s < 2$. Notons pour $r > 1$, $A(r) = \{x \in G/\Gamma \mid \alpha(x) \leqslant r\}$. Puisque α est continue, $A(r)$ et le complémentaire de l'intérieur de $A(r+1)$ sont deux fermés disjoints. On peut donc trouver (G/Γ est métrisable) une fonction continue g_r sur G/Γ, à valeurs dans $[0,1]$, nulle sur $A(r)$ et égale à 1 sur le complémentaire de $A(r+1)$. Alors $\phi - \phi g_r$ est continue à support dans $A(r+1)$. Mais $A(r+1)$ est compact (c'est une conséquence du critère de Mahler (cf. 4.3.2.) et de la définition de α (cf. 4.2.2.)). D'après le paragraphe précédent, on a donc

$$\lim_{t\to\infty}\int_K (\phi - \phi g_r)(a_t kz)\sigma(k)dk = \int_K \sigma(k)dk\int_{G/\Gamma}(\phi - \phi g_r)d\nu \tag{41}$$

La partie ϕg_r conserve ce qu'il reste de ϕ à l'infini. C'est ici que l'on va utiliser le résultat d'intégrabilité. En effet, on écrit avec $\beta = 2 - s > 0$

$$|\phi|\, g_r \leqslant C\alpha^s g_r \leqslant C\alpha^{2-\frac{\beta}{2}} g_r \alpha^{-\frac{\beta}{2}} \leqslant C\alpha^{2-\frac{\beta}{2}} r^{-\frac{\beta}{2}}$$

car $g_r(x) = 0$ si $\alpha(x) < r$ et $g_r \leqslant 1$. D'où pour tout r et t,

$$\left|\int_K (\phi g_r)(a_t kz)\sigma(k)dk\right| \leqslant C r^{-\frac{\beta}{2}}\int_K \sigma(k)\left(\alpha(a_t kz)\right)^{2-\frac{\beta}{2}} dk$$

Mais, puisque $\beta > 0$, le théorème 10.1. dit que le membre de droite est uniformément borné en t. Plus précisément,

$$\sup_{t\geqslant 0}\int_K \left(\alpha(a_t kz)\right)^{2-\frac{\beta}{2}} dk = C' < \infty$$

D'où, pour tout $t \geqslant 0$ et pour tout r,

$$\left|\int_K (\phi g_r)(a_t kz)\sigma(k)dk\right| \leqslant CC'(\sup_K \sigma) r^{-\frac{\beta}{2}} \tag{42}$$

Fixons maintenant $\varepsilon > 0$. Puisque α^s est intégrable sur G/Γ (cf. prop. 3.6.) ϕ l'est aussi. De plus, la suite des $A(r)$ est croissante et de réunion G/Γ. On a donc pour r assez grand, $\left|\int_{G/\Gamma} \phi g_r d\nu\right| \leqslant \frac{\varepsilon}{3\sup\sigma}$. De plus, pour r assez grand on a aussi $CC'(\sup_K \sigma) r^{-\frac{\beta}{2}} \leqslant \frac{\varepsilon}{3}$. On choisi donc un tel r qui vérifie ces deux inégalités. D'après 41, on peut trouver $t_0 > 0$, tel que pour tout $t \geqslant t_0$ les deux termes de 41 soient proches à $\frac{\varepsilon}{3}$ près. L'inégalité 42 étant valable quel que soit t, on en déduit que

$$\left|\int_K \phi(a_t kz)\sigma(k)dk - \int_K \sigma(k)dk \int_{G/\Gamma} \phi d\nu\right| \leqslant \varepsilon$$

ce qui prouve le théorème.■

13. Approximation de χ et preuve de l'équivalent

Comme il a été annoncé au début de cette partie, pour relier le dernier théorème au problème de dénombrement initial, il nous faut faire le lien entre l'expression $\int_K \widetilde{f}(a_t kz)dk = \sum_{v\in\mathbb{Z}^n} \int_K f(a_t kv)dk$ et $\frac{1}{T^{n-2}} \sum_{v\in\mathbb{Z}^n} \chi(v/T, q(v))$ quand $T = e^t$ tend vers l'infini. Dans la dernière somme, les seuls termes non nuls sont ceux tels que v/T reste borné. On cherche donc le comportement de $\int_K f(a_t kv)dk$ lorsque t tend vers l'infini et v/e^t reste borné. Nous allons montrer que l'équivalent est de la forme $e^{-(n-2)t} h(v/e^t, q_0(v))$ pour une certaine fonction h. Ensuite, nous allons voir que lorsque f est prise arbitraire, la fonction h est alors suffisamment générale pour pouvoir approximer χ convenablement.

13.1. **Comportement asymptotique des intégrales $\int_K f(a_t kv)dk$.** Décrivons intuitivement le comportement à l'infini de l'intégrale $\int_K f(a_t kv)dk$. L'intégrale par rapport à la mesure de Haar de K, n'est rien d'autre que l'intégrale sur les sphères unité de L_1 et L_2 par rapport à la mesure de surface usuelle convenablement normalisée par un coefficient que l'on note $\frac{1}{c_p}$. A l'aide d'un dessin en dimension 3 pour le cas où $q_0 = 2x_1x_3 - x_2^2$, on se convainc facilement que lorsque t et v tendent vers l'infini de sorte que $e^{-t}v$ reste borné (par des valeurs ne dépendant que du support de f que l'on fixe dans le demi-espace $x > 0$), les "cercles" $\{a_t kv \mid k \in K\}$ se déforment tout en restant sur la surface de niveau $q_0 = q_0(v)$. Ils s'approchent de plus en plus de la coupe faite à l'abscisse $e^{-t}(v, e_1) \simeq e^{-t}\|v\|$ de la surface de niveau $q_0 = q_0(v)$. L'intégrale $c_p \int_K f(a_t kv)dk$ se rapproche donc de l'intégrale de f prise sur ces grands "cercles" déformés par rapport à la mesure usuelle sur les grandes sphères de rayon $\|v\|$. Mais comme l'on reste dans un domaine borné, cette mesure tend vers la mesure de Lebesgue $\frac{1}{\|v\|^{n-2}}dx_2...dx_{n-1}$. On voit donc, d'après cet enchaînement d'arguments heuristiques que l'intégrale est équivalente quand t tend vers l'infini à $e^{-(n-2)t} J_f(e^{-t}\|v\|, q_0(v))$ où J_f est l'intégrale sur la coupe faite à l'abscisse $e^{-t}\|v\|$ de l'hyperboloïde :

$$J_f(r,\zeta) = \frac{1}{r^{n-2}} \int_{\mathbb{R}^{n-2}} f(r, x_2, ..., x_{n-1}, \kappa(\zeta, x_2, ..., x_{n-1}))dx_2...dx_{n-1} \tag{43}$$

où $r = e^{-t}\|v\|$, $\zeta = q_0(v)$, et $\kappa = (\zeta - q_0(0, x_2, ..., x_{n-1}, 0))/2r$ est choisi de tel sorte que $q_0(r, x_2, ..., x_{n-1}, \kappa) = \zeta$.

Résumons ce qui précède par le lemme suivant.

Lemme 13.1. *Soit f une fonction continue dont le support est compact et inclus dans $\mathbb{R}^n_+ = \{x \in \mathbb{R}^n \mid x_1 = (x, e_1) > 0\}$, σ une fonction continue sur la sphère S^{n-1} et $\varepsilon > 0$. Alors, pour tout $v \in \mathbb{R}^n$ et $t \in \mathbb{R}$ assez grands, on a*

$$\left| c_p e^{(n-2)t} \int_K f(a_t kv)\sigma(k^{-1}e_1)dk - J_f(e^{-t}\|v\|, q_0(v))\sigma(\frac{v}{\|v\|}) \right| \leqslant \varepsilon \tag{44}$$

où J_f est la fonction que l'on vient de définir en 43 et $c_p = \gamma_{p-1}\gamma_{n-p-1}/2^{(n-2)/2}$ avec γ_n le volume usuel de la sphère S^{n-1}.

***Preuve*:** La vérification rigoureuse des arguments heuristiques donnés ci-dessus est technique.

Tout d'abord, il suffit de montrer 44 lorsque $v \neq 0$ et $t \geqslant 0$ sont tels que $J_f(\|v\| e^{-t}, q_0(v)) \neq 0$ ou $f(a_t kv) \neq 0$ pour au moins un $k \in K$. Remarquons qu'il existe une constante $C > 0$, ne dépendant que du support de f, telle que

$$\left\{ \begin{array}{c} J_f(\|v\| e^{-t}, q_0(v)) \neq 0 \\ \text{ou } f(a_t kv) \neq 0 \end{array} \right\} \Longrightarrow \left\{ \begin{array}{c} \frac{1}{C} \leqslant \|v\| e^{-t} \leqslant C \\ \text{et } |q_0(v)| \leqslant C \end{array} \right\} \tag{45}$$

En effet, pour J_f, c'est clair car J_f est à support compact. Pour f, on remarque d'abord que, comme $a_t k \in H$, $q_0(a_t kv) = q_0(v) \subset q_0(Supp(f))$, d'où la seconde inégalité. Pour la première, observons que

$$f(a_t kv) = f(e^{-t}(kv, e_1), (kv, e_2), ..., (kv, e_{n-1}), e^t(kv, e_n))$$

Puis, comme $Supp(f) \subset \mathbb{R}^n_+ = \{x \in \mathbb{R}^n \mid x_1 = (x, e_1) > 0\}$, il existe une constante $A > 0$ telle que

$$\left\{ \begin{array}{c} \frac{1}{A} \leqslant e^{-t}(kv, e_1) \leqslant A \\ |(kv, e_i)| \leqslant A \text{ pour } 1 < i < n \\ |e^t(kv, e_n)| \leqslant A \end{array} \right\} \tag{46}$$

d'où,

$$\frac{1}{A^2} e^{2t} \leqslant \|kv\|^2 = \|v\|^2 \leqslant (n-2)A^2 + A^2 e^{-2t} + A^2 e^{2t}$$

ce qui montre l'existence de C pour la deuxième inégalité. On prend le plus grand des C ainsi trouvés.

Maintenant que 45 est acquis, fixons v et t satisfaisant à ces conditions. Si $k \in K$ est tel que $f(a_t kv) \neq 0$, les inégalités 46 montrent l'existence d'une constante $B > 0$ indépendante de v et de t (en fait, ne dépendant que de $Supp(f)$) telle que

$$\left\| \frac{kv}{\|v\|} - e_1 \right\| \leqslant B e^{-t} \tag{47}$$

Ecrivons maintenant v dans la base (f_i) orthogonale pour q_0 et orthonormale (voir les notations en 10.2.). On a $v = v_1 + v_2$ où $v_i \in L_i$. Notons $v_i = r_i \omega_i$ avec $r_i = \|v_i\|$. Alors $\|v\|^2 = r_1^2 + r_2^2$ et $q_0(v) = r_1^2 - r_2^2$. D'où $2r_1^2 = \|v\|^2 + q_0(v)$ et $2r_2^2 = \|v\|^2 - q_0(v)$. On en déduit,

$$\left| \sqrt{2} r_i - \|v\| \right| = \frac{\left| 2r_i^2 - \|v\|^2 \right|}{\left| \sqrt{2} r_i + \|v\| \right|} \leqslant C^2 e^{-t} \tag{48}$$

D'où l'existence de C' telle que $\frac{1}{C'} \leqslant r_i e^{-t} \leqslant C'$. On écrit alors

$$\left\| r_1 k\omega_1 - r_1 \frac{f_1}{\sqrt{2}} \|v\| \right\|^2 + \left\| r_2 k\omega_2 - r_2 \frac{f_n}{\sqrt{2}} \|v\| \right\|^2 = \|kv - \|v\| e_1\|^2 \leqslant \|v\| Be^{-t} \leqslant BC \tag{49}$$

Combinant cette dernière égalité avec 48, on obtient finalement l'existence d'une constante $D > 0$ telle que

$$\left\{ \begin{array}{l} \|k\omega_1 - f_1\| \leqslant De^{-t} \\ \|k\omega_2 - f_n\| \leqslant De^{-t} \end{array} \right\} \tag{50}$$

Notons $K_{t,v}$ l'ensemble des $k \in K$ qui vérifient les deux inégalités de 50. On a donc $f(a_t kv) \neq 0 \Rightarrow k \in K_{t,v}$. Remaquons qu'inversement s'il on suppose seulement $k \in K_{t,v}$, alors 49 montre l'existence d'une constante B' telle que 47 ait lieu avec B' à la place de B. On a donc pour $k \in K_{t,v}$,

$$\left|(a_t kv, e_1) - \|v\| e^{-t}\right| \leqslant e^{-t} \|v\| \left(\frac{kv}{\|v\|} - e_1, e_1 \right) \leqslant \frac{B'}{C} e^{-t}$$

et,

$$\left|(a_t kv, e_n) - \frac{(kv, e_1)(kv, e_n)}{e^{-t}\|v\|}\right| \leqslant e^t \left|(kv, e_n)\right| \left| 1 - \frac{(kv, e_1)}{\|v\|} \right| \leqslant AB' e^{-t}$$

Puis, par continuité uniforme de f et de σ, on déduit de ces deux inégalités (et de 47 pour σ) que pour tout $\delta > 0$ il existe $T_1 > 0$ tel que pour tout $t \geqslant T_1$, tout v tel que v et t satisfont les conditions 45, et pour tout $k \in K_{t,v}$, on a,

$$\left| f(a_t kv)\sigma(k^{-1}e_1) - f(\|v\| e^{-t}, (kv, e_2), ..., (kv, e_{n-1}), \kappa)\sigma(\frac{v}{\|v\|}) \right| < \delta \tag{51}$$

où $\kappa = \frac{(kv,e_1)(kv,e_n)}{e^{-t}\|v\|}$ est en fait choisi pour que $q_0(\|v\| e^{-t}, (kv, e_2), ..., (kv, e_{n-1}), \kappa) = q_0(v)$. On va maintenant intégrer 51 sur $K_{t,v}$. Mais, puisque $f(a_t kv) = 0$ si $k \notin K_{t,v}$, il vient,

(52)

$$\left| \int_K f(a_t kv)\sigma(k^{-1}e_1)dk - \sigma(\frac{v}{\|v\|}) \int_{K_{t,v}} f(\|v\| e^{-t}, (kv, e_2), ..., (kv, e_{n-1}), \kappa)dk \right| < \delta \int_{K_{t,v}} dk$$

Il nous faut maintenant préciser pourquoi l'on peut assimiler la mesure dk à la mesure de Lebesgue sur $\mathbb{R}^{n-2}$ comme décrit plus haut. Tout d'abord, par unicité de la mesure de Haar sur $K^0 \simeq SO(p) \times SO(n-p)$ (la mesure usuelle de surface sur la sphère est invariante par isométries) on a pour toute fonction g à support compact,

$$\int_K g(kv)dk = \int_{S_1 \times S_2} g(r_1\omega_1 + r_2\omega_2) \frac{d\omega_1}{\gamma_{p-1}} \frac{d\omega_2}{\gamma_{n-p-1}} \tag{53}$$

où $d\omega_i$ est la mesure de surface sur S_i (qui, rappelons-le est la sphère unité de L_i, voir le paragraphe de notations). Ceci permet déjà de voir que

$$\int_{K_{t,v}} dk = \int_{S_1} 1_{\|\omega_1 - f_1\| \leqslant De^{-t}} d\omega_1 \int_{S_2} 1_{\|\omega_2 - f_n\| \leqslant De^{-t}} d\omega_2 = O(e^{-(n-2)t}) \tag{54}$$

Ensuite, on a le lemme suivant,

Lemme 13.2. *Soit h une fonction continue sur $\mathbb{R}^k \times Vect(e_2, ..., e_{n-1})$ dont le support est inclus dans $\mathbb{R}^k \times S$ où S est un compact. Soit π la projection orthogonale* *de* $\mathbb{R}^n$ *sur* $Vect(e_2, ..., e_{n-1})$. *Soit* U_1 *(resp.* U_2*) un voisinage assez petit de* f_1 *dans* S_1 *(resp. de* f_n *dans* S_2*). Alors*

(55)
$$\lim_{r_1, r_2 \to \infty} r_1^{p-1} r_2^{n-p-1} \int_{U_1 \times U_2} h(y, \pi(r_1\omega_1 + r_2\omega_2)) d\omega_1 d\omega_2 = \int_{\mathbb{R}^{n-2}} h(y, x_2, ..., x_{n-1}) dx_1 ... dx_{n-1}$$

où la limite est uniforme quand y *varie dans un compact de* $\mathbb{R}^k$.

***Preuve*:** On écrit $\omega_i \in L_i$ en coordonnées angulaires, soit

$$\begin{aligned} \pi(\omega_1) &= (\sin\theta_2, ..., \cos\theta_2 ... \cos\theta_{p-1} \sin\theta_p) \\ \pi(\omega_2) &= (\sin\phi_2, ..., \cos\phi_2 ... \cos\phi_{n-p-1} \sin\phi_{n-p}) \end{aligned}$$

Puis on choisit U_1 et U_2 de sorte que les θ_i et ϕ_i soient dans $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ lorsque $\omega_i \in U_i$. Fixons maintenant $\varepsilon > 0$ et un compact S_1 de $\mathbb{R}^k$. Choisissons alors un module de continuité uniforme $\delta > 0$ pour h sur $S_1 \times S$ associé à ce ε. Puisque S est compact, il existe une constante $C > 0$ telle que $|(\omega_i, e_j)| \leqslant C + \delta$ pour $i = 1, 2$ et $j = 2, ..., n-1$ dès que $\pi(r_1\omega_1 + r_2\omega_2) \in S$. Enfin, on note,

$$\begin{aligned} A_{r_1} &= \left\{\theta = (\theta_2, ..., \theta_p) \in \mathbb{R}^{p-1} \mid \omega_1 \in U_1 \text{ et } |r_1(\omega_1, e_j)| \leqslant C \text{ pour } j = 2, ..., p\right\} \\ A_{r_2} &= \left\{\phi = (\phi_2, ..., \phi_{n-p}) \in \mathbb{R}^{n-p-1} \mid \omega_2 \in U_2 \text{ et } |r_2(\omega_2, e_j)| \leqslant C \text{ pour } j = p+1, ..., n-p-1\right\} \end{aligned}$$

Alors pour tout $\theta \in A_{r_1}$, et $j = 2, ..., p$, on a $(\omega_1, e_j) = O(\frac{1}{r_1})$. En remarquant que $\omega_1 \in U_1$ on en déduit que $\theta_i = O(\frac{1}{r_1})$ pour $i = 2, ..., p$. De plus $\cos\theta_i = 1 + O(\frac{1}{r_1^2})$ et $\sin\theta_i = \theta_i + O(\frac{1}{r_1^2})$. On voit alors que $|(\omega_1, e_i) - \theta_i| = |\cos\theta_2 ... \cos\theta_{i-1} \sin\theta_i - \theta_i| = O(\frac{1}{r_1^2})$ pour tout $i = 2, ..., p$. De même si $\phi \in A_{r_2}$ $|(\omega_2, e_{p+i-1}) - \phi_i| = O(\frac{1}{r_2^2})$ pour $i = 2, ..., n-p$. D'où l'existence de $R_0 \geqslant 0$ tel que pour tout r_1, $r_2 \geqslant R_0$, $\theta \in A_{r_1}$ et $\phi \in A_{r_2}$ on a $|r_1((\omega_1, e_i) - \theta_i)| \leqslant \delta$ pour $i = 2, ..., p$ et $|r_2((\omega_2, e_{p+i-1}) - \phi_i)| \leqslant \delta$ pour $i = 2, ..., n-p$. Dans ces conditions pour tout $y \in S_1$,

$$|h(y, \pi(r_1\omega_1 + r_2\omega_2)) - h(y, r_1\theta_2, ..., r_1\theta_p, r_2\phi_2, ..., r_2\phi_{n-p})| \leqslant \varepsilon$$

Enfin, on intègre cette expression en θ et ϕ sur $A_{r_1} \times A_{r_2}$, soit

$$\left| \int_{U_1 \times U_2} h(y, \pi(r_1\omega_1 + r_2\omega_2)) d\omega_1 d\omega_2 - \int_{A_{r_1} \times A_{r_2}} h(y, r_1\theta_2, ..., r_1\theta_p, r_2\phi_2, ..., r_2\phi_{n-p}) d\theta_i d\phi_i \right| \leqslant \varepsilon \int_{A_{r_1} \times A_{r_2}} d\theta_i d\phi_i$$

Mais on constate que pour r_1 et r_2 assez grands, $S \subset A_{r_1} \times A_{r_2}$. De plus $\int_{A_{r_1} \times A_{r_2}} d\theta_i d\phi_i = O(\frac{1}{r_1^{p-1} r_2^{n-p-1}}) \leqslant cste \times \frac{1}{r_1^{p-1} r_2^{n-p-1}}$. Enfin, en posant $x_2 = r_1\theta_2$, ..., $x_p = r_1\theta_p$, $x_{p+1} = r_2\phi_2$, ..., $x_{n-1} = r_2\phi_{n-p}$ on obtient pour tout $y \in S_1$,

$$\left| r_1^{p-1} r_2^{n-p-1} \int_{U_1 \times U_2} h(y, \pi(r_1\omega_1 + r_2\omega_2)) d\omega_1 d\omega_2 - \int_{\mathbb{R}^{n-2}} h(y, x_2, ..., x_{n-1}) dx_2 ... dx_{n-1} \right| \leqslant \varepsilon \times cste$$

Ce qui prouve la limite souhaitée.■

On applique ce lemme à la fonction $h(a, b, x_2, ..., x_{n-1}) = f(a, x_1, ..., x_{n-1}, \frac{b - q_0(0, x_2, ..., x_{n-1}, 0)}{2a})$. h vérifie les hypothèses du lemme : elle est continue sur $\mathbb{R}^2 \times Vect(e_2, ..., e_{n-1})$ avec pour $S = [-C, C]^{n-2}$. On choisit de plus le compact $S_1 = \left[\frac{1}{C}, C\right] \times [-C, C]$ sur lequel il y a convergence uniforme de 55 pour $(a, b) \in S_1$. On aura $a = \|v\| e^{-t}$ et $b = q_0(v)$. Enfin on choisit les voisinages $U_1 = \{\omega_1 \in S_1 \mid \|\omega_1 - f_1\| \leqslant De^{-t}\}$ et $U_2 = \{\omega_2 \in S_2 \mid \|\omega_2 - f_n\| \leqslant De^{-t}\}$. D'après le lemme, il existe $R_0 \geqslant 0$ tel que pour tout t

avec $e^t \geqslant R_0/C'$, et (v,t) satisfaisant à 45, on a, où $\kappa_g = \frac{q_0(v)-q_0(0,(r_1\omega_1+r_2\omega_2,e_2),...,(r_1\omega_1+r_2\omega_2,e_{n-1}),0)}{2\|v\|e^{-t}}$ et $\kappa_d = \frac{q_0(v)-q_0(0,x_2,...,x_{n-1},0)}{2\|v\|e^{-t}}$

(56)

$$\left|\int_{U_1\times U_2} f(\|v\|\, e^{-t}, \pi(r_1\omega_1 + r_2\omega_2), \kappa_g)d\omega_1 d\omega_2 - \frac{1}{r_1^{p-1} r_2^{n-p-1}}\int_{\mathbb{R}^{n-2}} f(\|v\|\, e^{-t}, x_2, ..., x_{n-1}, \kappa_d)d\mathbf{x}_i\right| \leqslant \delta\left(\frac{C'}{e^t}\right)^{n-2}$$

Mais le terme de gauche dans l'expression ci-dessus est aussi d'après 53, la forme des U_i et la définition de $K_{t,v}$

$$\gamma_{p-1}\gamma_{n-p-1}\int_{K_{t;v}} f(\|v\|\, e^{-t}, (kv, e_2), ..., (kv, e_{n-1}), \kappa)dk$$

où $\kappa = \frac{(kv,e_1)(kv,e_n)}{e^{-t}\|v\|} = \frac{q_0(v)-q_0(0,(kv,e_2),...,(kv,e_{n-1}),0)}{2\|v\|e^{-t}}$ est comme dans 52. En combinant 56, 54, et 52, on obtient

$$\left|c_p\int_K f(a_t kv)dk - \frac{\|v\|^{n-2}\, e^{-(n-2)t}}{2^{\frac{(n-2)}{2}} r_1^{p-1} r_2^{n-p-1}} J_f(\|v\|\, e^{-t}, q_0(v))\right| \leqslant \delta e^{-(n-2)t}\times cste$$

Enfin on obtient ce que l'on souhaitait en combinant 48 au fait que J_f est bornée.

$$\left|c_p\int_K f(a_t kv)dk - e^{-(n-2)t} J_f(\|v\|\, e^{-t}, q_0(v))\right| \leqslant \delta e^{-(n-2)t}\times cste$$

■

Il s'agit maintenant de montrer que l'on peut approcher la fonction indicatrice χ de $\left]-\frac{1}{2},1\right]\partial\Omega\times]a,b[$ par des fonctions du type J_f. C'est pour cela que l'on a introduit la fonction auxiliaire σ dans le lemme précédent. En fait, le lemme qui suit répond à la question. Il est facile de voir (par un argument semblable à celui de la proposition 2.2.) que toute fonction de $C_c(\mathbb{R}_+^*\times\mathbb{R})$ est de la forme J_f pour un certain $f\in C_c(\mathbb{R}_+^n)$ (fonctions continues à support dans $\mathbb{R}_+^n = \{x\in\mathbb{R}^n \mid x_1 = (x,e_1) > 0\}$). Le théorème de Stone-Weierstrass montre alors que l'espace vectoriel des combinaisons linéaires de fonctions du type $J_f\sigma$ est dense dans $C_c(\mathbb{R}^n - \{0\}\times\mathbb{R})$. Aurement dit,

Lemme 13.3. *L'application $f\longmapsto J_f$ de $C_c(\mathbb{R}_+^n)$ (resp. $C_c^+(\mathbb{R}_+^n)$) dans $C_c(\mathbb{R}_+^*\times\mathbb{R})$ (resp. $C_c^+(\mathbb{R}_+^*\times\mathbb{R})$) est surjective. De plus $\mathcal{L} = Vect\left\{(v,\zeta)\mapsto J_f(\|v\|,\zeta)\sigma(\frac{v}{\|v\|}) \mid f\in C_c(\mathbb{R}_+^n) \text{ et } \sigma\in C(S^{n-1})\right\}$ est dense dans $C_c(\mathbb{R}^n - \{0\}\times\mathbb{R})$ muni de la topologie de la convergence uniforme sur tout compact.*

***Preuve*:** Pour la surjectivité, la preuve est en tout point similaire à celle de la proposition 2.2.

On pose $\pi:\mathbb{R}_+^n\to\mathbb{R}_+^*\times\mathbb{R}$ $x\longmapsto (x_1, q_0(x))$ où $x_1 = (x,e_1)$. On remarque que π est continue, ouverte et surjective ($\pi(r,0,...,0,\zeta/2r) = (r,\zeta)$).

Soit $\phi\in C_c(\mathbb{R}_+^*\times\mathbb{R})$. D'après la remarque sur π, il existe un ouvert O de $\mathbb{R}_+^n$ relativement compact tel que $\pi(O)$ contienne le support de ϕ. On trouve alors une fonction $\psi\in C_c^+(\mathbb{R}_+^n)$ qui vaut 1 sur O. Si $a\in O$, alors l'ensemble des $n-2$-uplets $(x_2,...,x_{n-1})\in\mathbb{R}^{n-2}$ tels que $(a_1,x_2,...,x_{n-1},(q_0(a)-q_0(0,x_2,...,x_{n-1},0))/2a_1)$ appartienne à O est un voisinage ouvert de $(a_2,...,a_{n-1})$. On en déduit que $J_\psi(a_1,q_0(a)) > 0$. On pose alors, comme en 2.2.,

$$\begin{aligned}\xi(r,\zeta) &= \frac{\phi(r,\zeta)}{J_\psi(r,\zeta)} \text{ si } (r,\zeta)\in\pi(O)\\ &= 0 \text{ sinon}\end{aligned}$$

Alors ξ est bien définie et continue sur l'ouvert $\pi(O)$ donc partout. Enfin, on remarque que s'il on définit $f = \psi(\xi \circ \pi)$ alors $f \in C_c(\mathbb{R}_+^n)$ et $J_f = \phi$.

Montrons maitenant que $\mathcal{L}$ est dense dans $C_c(\mathbb{R}^n - \{0\} \times \mathbb{R})$. Il s'agit de montrer que pour tout compact K de $\mathbb{R}^n - \{0\} \times \mathbb{R}$ l'ensemble $\mathcal{L}_K$ des restrictions à K des fonctions de $\mathcal{L}$ est dense dans $C(K)$. On va appliquer le théorème de Stone-Weierstrass (cf. [Lan]). Vérifions les hypothèses. Tout d'abord remarquons que $\mathcal{L}$ est une algèbre de fonctions : pour tous f_1 et f_2 dans $C_c(\mathbb{R}_+^n)$, $J_{f_1} J_{f_2} \in C_c(\mathbb{R}_+^* \times \mathbb{R})$ donc s'écrit J_f pour un certain $f \in C_c(\mathbb{R}_+^n)$, d'après la surjectivité de J. De plus le produit de deux fonctions continues sur la sphère est encore continu. Donc $\mathcal{L}$ est une algèbre. Pour voir que $\mathcal{L}_K$ contient les constantes, on choisit $\varepsilon > 0$ puis a et b réels tels que $K \subset A \times [a, b]$ où A est l'anneau $\left\{v \in \mathbb{R}^n \mid \varepsilon \leqslant \|v\| \leqslant \frac{1}{\varepsilon}\right\}$. Il suffit alors de prendre f telle que J_f vale 1 sur $\left[\varepsilon, \frac{1}{\varepsilon}\right] \times [a, b]$. Pour voir que $\mathcal{L}_K$ sépare les points, et c'est précisément pour avoir cette propriété que l'on a introduit les fonctions σ sur la sphère, on choisit $(v_1, \zeta_1) \neq (v_2, \zeta_2)$ et on distingue le cas $\|v_1\| = \|v_2\|$ et $\zeta_1 = \zeta_2$ (on prend f telle que $J_f(\|v_1\|, \zeta_1) \neq 0$ et $\sigma(\frac{v_1}{\|v_1\|}) = 0$, $\sigma(\frac{v_2}{\|v_2\|}) \neq 0$) du cas contraire (on prend alors $\sigma = 1$ et f telle que J_f n'a pas la même valeur en $(\|v_1\|, \zeta_1)$ et en $(\|v_2\|, \zeta_2)$).■

13.2. **Borne inférieure pour $V_{a,b}^q(\mathbb{Z}) \cap T\Omega$.** En prenant une fonction J_f adéquate, ceci nous permet déjà, moyennant le résultat d'intégrabilité 11.1. d'obtenir une borne supérieure pour $\left|V_{a,b}^q(\mathbb{Z}) \cap T\Omega\right|$.

Théorème 13.1. *Soit q une forme quadratique quelconque de signature $(p, n-p)$ avec $n \geqslant 4$ et $p \geqslant 3$, alors il existe une constante $c > 0$ telle que pour tout $T \geqslant 1$,*

$$\left|V_{a,b}^q(\mathbb{Z}) \cap T\Omega\right| \leqslant cT^{n-2}$$

***Preuve*:** Il suffit de montrer le théorème pour un multiple de q donc pour q de la forme $q_0 \circ g$ où $g \in G$. Il suffit aussi de le montrer pour $\Omega = S^{n-1}$ car Ω borné. Choisissons $\varepsilon > 0$, $C \geqslant \|g\|$ et $\left\|g^{-1}\right\|$, puis $f \geqslant 0$ telle que $J_f \geqslant 1 + \varepsilon$ sur $\left[C^{-1}, C\right] \times [a, b]$ (cf. lemme 10.1.). Soit $v \in \mathbb{R}^n$ tel que

$$e^t \leqslant \|v\| \leqslant 2e^t \text{ et } a \leqslant q_0(gv) \leqslant b \tag{57}$$

Alors $J_f(\|gv\| e^{-t}, q_0(gv)) \geqslant 1 + \varepsilon$. Le lemme 10.1. montre alors que

$$c_p e^{(n-2)t} \int_K f(a_t kgv) dk \geqslant 1$$

On somme alors sur tous les v de $\mathbb{Z}^n$ vérifiant 57, ce qui donne puisque $f \geqslant 0$,

$$\left|V_{a,b}^q(\mathbb{Z}) \cap \left[e^t, 2e^t\right] S^{n-1}\right| \leqslant \sum_{v \in \mathbb{Z}^n} c_p e^{(n-2)t} \int_K f(a_t kgv) dk = c_p e^{(n-2)t} \int_K \widetilde{f}(a_t kg) dk$$

Enfin, d'après le théorème 11.2. en sachant que $\widetilde{f} \leqslant C\alpha$ pour une certaine constante C (voir la section 4.6.), on obtient

$$\left|V_{a,b}^q(\mathbb{Z}) \cap \left[e^t, 2e^t\right] S^{n-1}\right| \leqslant cste \times e^{(n-2)t}$$

ceci quel que soit $t \geqslant 0$. D'où pour tout $T \geqslant 1$

$$\begin{aligned}\left|V_{a,b}^{q}(\mathbb{Z}) \cap TS^{n-1}\right| &\leqslant \sum_{k\geqslant 0}\left|V_{a,b}^{q}(\mathbb{Z}) \cap \left[\frac{T}{2^{k+1}}, \frac{T}{2^{k}}\right] S^{n-1}\right| \\ &\leqslant cste \times \sum \left(\frac{T}{2^{k+1}}\right)^{n-2} \leqslant 2cste \times T^{n-2}\end{aligned}$$

ce qui achève la preuve.■

13.3. **Preuve de la version quantitative (thm 9.1.)** Nous allons maintenant rassembler les résultats des différents lemmes ci-dessus pour en déduire le théorème 9.1. En sommant 44 sur les points du réseau $g\mathbb{Z}^n$ (où $q = q_0 \circ g$), on remarque que l'on obtient $\lim_{t\to\infty} e^{-(n-2)t} \sum_{v\in\mathbb{Z}^n} h(ve^{-t}, q(v)) = \lim_{t\to\infty} c_p \int_K \widetilde{f}(a_t kv)\sigma(k^{-1}e_1)dk$ où h est du type $J_f\sigma$. Mais l'expression de droite est précisément ce que l'on calcule dans le théorème d'équirépartition. On obtient donc l'asymptotique recherchée pour de telles fonctions h. Le lemme qui précède permet d'étendre ce résultat aux fonctions continues à support compact dans $\mathbb{R}^n - \{0\} \times \mathbb{R}$, puis à la fonction χ elle-même. En posant $\chi_g(v,\zeta) = \chi(g^{-1}v, \zeta)$ pour $g \in G$, on a

Théorème 13.2. *On suppose $p \geqslant 3$. Pour tout $h \in C_c(\mathbb{R}^n - \{0\} \times \mathbb{R})$, puis pour $h = \chi_g$, et $g \in G$ tel que $q_0 \circ g$ soit irrationnelle, on a*

$$\lim_{T\to\infty} \frac{1}{T^{n-2}} \sum_{v\in g\mathbb{Z}^n} h(v/T, q_0(v)) = L(h) \tag{58}$$

où $L(h) = c_p \int_K dk \int_{\mathbb{R}} d\zeta \int_0^\infty h(rk^{-1}e_1, \zeta) r^{n-2} \frac{dr}{2r}$ avec le même $c_p = \gamma_{p-1}\gamma_{n-p-1}/2^{(n-2)/2}$.

En particulier, ceci démontre le théorème principal 9.1 à ceci près qu'il faut calculer la constante. La section suivante est consacrée à ce calcul, qui donne bien sûr $L(\chi_g) = c_{q,\Omega}(1 - \frac{1}{2^{n-2}})(b-a)$.

***Preuve*:** On va d'abord montrer le résultat pour $h(v,\zeta)$ de la forme $J_f(\|v\|, \zeta)\sigma(\frac{v}{\|v\|})$.

Etant donné $\varepsilon > 0$, on sait par le lemme 13.1. que pour tous v et t assez grands,

$$\left|c_p \int_K f(a_t kv)\sigma(k^{-1}e_1)dk - e^{-(n-2)t} J_f(e^{-t}\|v\|, q_0(v))\sigma(\frac{v}{\|v\|})\right| \leqslant \varepsilon e^{-(n-2)t} \tag{59}$$

De plus on sait que cette expression est nulle à moins que v et t ne vérifient les conditions 45. Mais d'après le théorème 13.1., le nombre de $v \in g\mathbb{Z}^n$ qui satisfont de telles relations est majoré par $cste \times e^{(n-2)t}$. On fixe donc t assez grand et on somme 59 sur les $v \in g\mathbb{Z}^n$ qui vérifient 45 conjointement avec t. Il vient pour tout t assez grand,

$$\left|c_p \int_K \widetilde{f}(a_t kg)\sigma(k^{-1}e_1)dk - e^{-(n-2)t} \sum_{v\in g\mathbb{Z}^n} J_f(e^{-t}\|v\|, q_0(v))\sigma(\frac{v}{\|v\|})\right| \leqslant \varepsilon \times cste \tag{60}$$

Or d'après le résultat d'ergodicité 12.1., vu que $\widetilde{f}$ est continue et majorée par $C\alpha$ sur l'espace des réseaux G/Γ, et que $H \cdot (g\mathbb{Z}^n)$ est dense car $q_0 \circ g$ est irrationnelle (cf. §6), on a

$$\lim_{t\to+\infty} \int_K \widetilde{f}(a_t kg)\sigma(k^{-1}e_1)dk = \int_K \sigma(k^{-1}e_1)dk \int_{G/\Gamma} \widetilde{f} d\nu \tag{61}$$

Combinant 60 et 61 on trouve,

$$\lim_{T\to\infty}\frac{1}{T^{n-2}}\sum_{v\in g\mathbb{Z}^n} h(v/T,q_0(v)) = c_p\int_K \sigma(k^{-1}e_1)dk\int_{G/\Gamma}\widetilde{f}d\nu \tag{62}$$

C'est là que la formule de Siegel intervient. Rappelons (cf. section 4.6.) que

$$\int_{G/\Gamma}\widetilde{f}d\nu = \int_{\mathbb{R}^n} fd\lambda$$

où λ est la mesure de Lebesgue. De plus, en effectuant le changement de variable $(x_1,...,x_n)\to(x_1',...,x_{n-1}',\zeta)$, avec $x_i=x_i'$ pour $i=1...n-1$, et $q_0(x_1,...,x_n)=\zeta$, on obtient

$$\int_{\mathbb{R}^n} fd\lambda = \int_{\mathbb{R}}\int_0^\infty J_f(r,\zeta)r^{n-2}\frac{dr}{2r}d\zeta$$

mais $J_f(r,\zeta)\sigma(k^{-1}e_1)=h(rk^{-1}e_1,\zeta)$, donc le terme de droite dans 62 est bien $L(h)$ comme défini dans l'énoncé. La limite est donc prouvée pour h de la forme $J_f\sigma$.

Par linéarité (L est une forme linéaire positive), la formule est vraie pour tout $h\in\mathcal{L}$. Puisque $\mathcal{L}$ est positive, elle est aussi continue sur $C_c(\mathbb{R}^n-\{0\}\times\mathbb{R})$. Soit $\varepsilon>0$, K un compact de $\mathbb{R}^n-\{0\}\times\mathbb{R}$. Il existe $\delta>0$ tel que pour tout h et h' continues à support dans K, on ait $\sup_{x\in K}|h(x)-h'(x)|\leqslant\delta\Rightarrow|L(h)-L(h')|\leqslant\varepsilon$. Pour tout choix de telles fonctions, quels que soient $v\in g\mathbb{Z}^n$ et $T\geqslant 0$,

$$\left|h(\frac{v}{T},q_0(v))-h'(\frac{v}{T},q_0(v))\right|\leqslant\delta$$

D'après le théorème 10.4.le terme de gauche ci-dessus est non-nul seulement pour un nombre de points $v\in g\mathbb{Z}^n$ inférieure à C_KT^{n-2} où C_K est une constante ne dépendant que de K. Il vient donc,

$$\left|\frac{1}{T^{n-2}}\sum_{v\in g\mathbb{Z}^n}h(\frac{v}{T},q_0(v))-\frac{1}{T^{n-2}}\sum_{v\in g\mathbb{Z}^n}h'(\frac{v}{T},q_0(v))\right|\leqslant\delta C_K$$

Puisque $\mathcal{L}$ est dense dans $C_c(\mathbb{R}^n-\{0\}\times\mathbb{R})$ on peut fixer $h\in C_c(\mathbb{R}^n-\{0\}\times\mathbb{R})$ quelconque et prendre h' dans $\mathcal{L}$ proche de h. Ce qui précède montre alors que la limite 58 est aussi vraie pour h.

Reste à voir pourquoi on peut aussi prendre $h=\chi_g$ dans 58. Tout simplement, on encadre χ_g par deux fonctions de $C_c(\mathbb{R}^n-\{0\}\times\mathbb{R})$. On peut trouver h^+ et h^- dans $C_c(\mathbb{R}^n-\{0\}\times\mathbb{R})$ telles que

$$\begin{aligned} h^- &\leqslant \chi_g\leqslant h^+\\ \left|L(h^+)-L(\chi_g)\right| &\leqslant \varepsilon\\ \left|L(h^-)-L(\chi_g)\right| &\leqslant \varepsilon \end{aligned}$$

On en déduit pour T assez grand

$$\frac{1}{T^{n-2}}\sum_{v\in g\mathbb{Z}^n}\chi_g(\frac{v}{T},q_0(v))\leqslant\frac{1}{T^{n-2}}\sum_{v\in g\mathbb{Z}^n}h^+(\frac{v}{T},q_0(v))\leqslant L(h^+)+\varepsilon\leqslant L(\chi_g)+2\varepsilon$$

et l'inégalité complémentaire avec h^-. Cela prouve 58 pour $h=\chi_g$.■

14. Estimée du volume inter-hyperboloïdes

Dans cette partie annexe, nous démontrons l'équivalent 14 et la formule 15. En posant $\chi_g(v,\zeta) = \chi(g^{-1}v,\zeta)$ pour $g \in G$, ces deux résultats découlent immédiatement du lemme suivant :

Lemme 14.1. *Pour tout $h \in C_c(\mathbb{R}^n - \{0\} \times \mathbb{R})$, puis pour $h = \chi_g$, et tout $g \in G$, on a*

$$\lim_{T\to\infty} \frac{1}{T^{n-2}} \int_{\mathbb{R}^n} h(gv/T, q_0(gv))\lambda(dv) = L(h)$$

où $L(h) = c_p \int_K dk \int_{\mathbb{R}} d\zeta \int_0^\infty h(rk^{-1}e_1,\zeta)r^{n-2}\frac{dr}{2r}$ (cf. notations pour la définition de c_p). De plus $L(\chi_g) = c_{q,\Omega}(1-\frac{1}{2^{n-2}})(b-a)$ avec $c_{q,\Omega} = \int_{C(q)\cap\Omega} \frac{ds}{\|\nabla q\|}$.

***Preuve*:** Comme $\det g = 1$, on a,

$$\int_{\mathbb{R}^n} h(\frac{gv}{T}, q_0(gv))d\lambda(v) = \int_{\mathbb{R}^n} h(\frac{v}{T}, q_0(v))d\lambda(v)$$

Dans la base (f_i) (cf. notations), on écrit (voir le lemme 13.1. vers l'équation 48) $v = r_1\omega_1 + r_2\omega_2$. Puis on effectue le changement de variable polaire :

$$\int_{\mathbb{R}^n} h(\frac{v}{T}, q_0(v))d\lambda(v) = \int_0^\infty \int_0^\infty \int_{S_1\times S_2} h(\frac{r_1\omega_1 + r_2\omega_2}{T}, r_1^2 - r_2^2)r_1^{p-1}r_2^{n-p-1}d\omega_1 d\omega_2 dr_1 dr_2$$

où, rappelons-le, $d\omega_i$ est la mesure de surface sur la sphère unité S_i de L_i. En changeant r_i et Tr_i, l'expression ci-dessus s'écrit aussi

$$\int_{\mathbb{R}_+\times\mathbb{R}_+\times S_1\times S_2} h(r_1\omega_1 + r_2\omega_2, T^2(r_1^2 - r_2^2))r_1^{p-1}r_2^{n-p-1}d\omega_1 d\omega_2 dr_1 dr_2$$

Maintenant, remarquons que puisque h est à support compact, le support de $(r_1,r_2) \mapsto h(r_1\omega_1 + r_2\omega_2, T^2(r_1^2 - r_2^2))$ est inclus dans une partie $\mathcal{P}_{\varepsilon,T}$ du plan définie par

$$\left\{ \begin{array}{c} \varepsilon \leqslant r_i \leqslant \frac{1}{\varepsilon} \text{ pour } i = 1 \text{ et } 2 \\ |r_1 - r_2| \leqslant \frac{1}{T^2\varepsilon} \end{array} \right\} \tag{63}$$

pour un certain $\varepsilon > 0$ ne dépendant que de h. De plus, on remarque que le support de $(r_1,r_2) \mapsto h(r_1(\omega_1+\omega_2), T^2(r_1^2 - r_2^2))$ est aussi inclus dans un ensemble de la forme $\mathcal{P}_{\varepsilon',T}$ pour un certain $\varepsilon' > 0$. En prenant le plus petit de ε et ε' on peut supposer que ces deux supports sont inclus dans $\mathcal{P}_{\varepsilon,T}$.

Soit $\delta > 0$. Considérons la fonction $(x,y,z,t) \mapsto h(x\omega_1 + y\omega_2, z)x^{p-1}y^{n-p-2}t$ sur le compact de $\mathbb{R}^4$ défini par $\varepsilon \leqslant u \leqslant \frac{1}{\varepsilon}$ où $u = x,y,z,$ ou t. Par continuité uniforme de cette fonction, il existe T_0 tel que pour tout $T \geqslant T_0$, tout $(r_1,r_2) \in \mathcal{P}_{\varepsilon,T}$, on ait

$$\left| h(r_1\omega_1 + r_2\omega_2, T^2(r_1^2 - r_2^2))r_1^{p-1}r_2^{n-p-1} - h(r_1(\omega_1+\omega_2), T^2(r_1^2 - r_2^2))r_1^{n-3}r_2 \right| \leqslant \frac{\delta\varepsilon^2}{4\gamma_{p-1}\gamma_{n-p-1}}$$

où, à nouveau γ_k est le volume de S^{k-1}. Puis, on intègre l'expression ci-dessus sur $D = \mathbb{R}_+ \times \mathbb{R}_+ \times S_1 \times S_2$, ce qui revient à intégrer sur $\mathcal{P}_{\varepsilon,T} \times \mathcal{P}_{\varepsilon,T} \times S_1 \times S_2$. D'où

$$\int_D \left| h(r_1\omega_1 + r_2\omega_2, T^2(r_1^2 - r_2^2))r_1^{p-1}r_2^{n-p-1} - h(r_1(\omega_1+\omega_2), T^2(r_1^2 - r_2^2))r_1^{n-3}r_2 \right| dr_i d\omega_i \leqslant \frac{\delta}{T^2}$$

car $\int_{\mathcal{P}_{\varepsilon,T}} dr \leqslant \frac{2}{\varepsilon T}$. Par suite, pour $T \geqslant T_0$, on a

(64)
$$\left| \frac{1}{T^{n-2}} \int_{\mathbb{R}^n} h(\frac{gv}{T}, q_0(gv)) d\lambda(v) - T^2 \int_D h(r_1(\omega_1 + \omega_2), T^2(r_1^2 - r_2^2)) r_1^{n-3} r_2 dr_1 dr_2 d\omega_1 d\omega_2 \right| \leqslant \delta$$

Puis, on pose $\zeta = T^2(r_1^2 - r_2^2)$. On a alors $dr_1 dr_2 = 2T^2 dr_1 d\zeta r_2$ et, en notant $D' = \mathbb{R}_+ \times \mathbb{R} \times S_1 \times S_2$

(65)
$$T^2 \int_D h(r_1(\omega_1 + \omega_2), T^2(r_1^2 - r_2^2)) r_1^{n-3} r_2 d\omega_i dr_i = \int_{D'} h(r_1(\omega_1 + \omega_2), \zeta) r_1^{n-2} \frac{dr_1}{2r_1} d\zeta d\omega_1 d\omega_2$$

Enfin en posant $r = r_1\sqrt{2}$, et en utilisant 53, on obtient

$$\int_{D'} h(r_1(\omega_1 + \omega_2), \zeta) r_1^{n-2} d\omega_1 d\omega_2 \frac{dr_1}{2r_1} = c_p \int_{\mathbb{R}_+ \times \mathbb{R} \times K} h(rk^{-1}e_1, \zeta) r^{n-2} d\zeta \frac{dr}{2r} dk$$

ce qui, conjugué à 64 montre bien que

$$\lim_{T\to\infty} \frac{1}{T^{n-2}} \int_{\mathbb{R}^n} h(gv/T, q_0(gv)) \lambda(dv) = L(h) = c_p \int_K dk \int_{\mathbb{R}} d\zeta \int_0^\infty h(rk^{-1}e_1, \zeta) r^{n-2} \frac{dr}{2r}$$

Il nous reste à prouver cette égalité pour χ_g. Il suffit, comme au §13.3. d'encadrer χ_g par des fonctions h^+ et h^- de $C_c(\mathbb{R}^n - \{0\} \times \mathbb{R})$.

Enfin, vérifions la formule $c_{q,\Omega} = \int_{C(q)\cap\Omega} \frac{ds}{\|\nabla q\|}$. On reprend l'expression 65 avec $h = \chi_g$. Il vient

$$\int_{D'} h(r_1(\omega_1 + \omega_2), \zeta) r_1^{n-2} \frac{dr_1}{2r_1} d\zeta d\omega_1 d\omega_2 = (b-a) \int_{\mathbb{R}_+ \times S_1 \times S_2} 1_{\{r(\omega_1+\omega_2) \in g]\frac{1}{2},1]\partial\Omega\}} r^{n-2} \frac{dr}{2r} d\omega_1 d\omega_2$$

D'où

$$c_{q,\Omega}(1 - \frac{1}{2^{n-2}}) = \lim_{T\to\infty} \frac{1}{T^{n-2}} \lambda(V_{0,1}^q(\mathbb{R}) \cap T \left]\frac{1}{2}, 1\right] \partial\Omega) = \int_{\mathbb{R}_+ \times S_1 \times S_2} 1_{\{r(\omega_1+\omega_2) \in g]\frac{1}{2},1]\partial\Omega\}} r^{n-2} \frac{dr}{2r} d\omega_1 d\omega_2$$

ou encore

$$c_{q,\Omega} = \lim_{T\to\infty} \frac{1}{T^{n-2}} \lambda(V_{0,1}^q(\mathbb{R}) \cap T\partial\Omega) = \int_{\mathbb{R}_+ \times S_1 \times S_2} 1_{\{r(\omega_1+\omega_2) \in g\Omega\}} r^{n-2} \frac{dr}{2r} d\omega_1 d\omega_2 \tag{66}$$

Or on a $q_0(v) = r_1^2 - r_2^2$ avec les notations précédentes. Donc le cône isotrope de q_0 est

$$C(q_0) = \{r(\omega_1 + \omega_2) \mid r \geqslant 0,\ \omega_1 \in S_1,\ \omega_2 \in S_2\}$$

De plus l'élément de surface sur $C(q_0)$ est précisément $r^{n-2}\sqrt{2} dr d\omega_1 d\omega_2$. Et le gradient de q_0 sur $C(q_0)$ vaut $2\sqrt{2}r\overrightarrow{n}$ où $\overrightarrow{n}$ est un vecteur normal à $C(q_0)$. De 66 on déduit donc

$$c_{q,\Omega} = \int_{C(q_0)\cap g\Omega} \frac{ds}{\|\nabla q_0\|}$$

Pour obtenir l'expression souhaitée, il suffit de voir que si $g \in G$ est tel que $q = q_0 \circ g$, alors pour tout $x \in C(q_0 \circ g)$, on a $\frac{ds}{\|\nabla(q_0 \circ g)\|(x)} = \frac{d(gs)}{\|\nabla q_0\|(gx)}$, car alors

$$\int_{C(q_0)\cap g\Omega} \frac{ds}{\|\nabla q_0\|} = \int_{(g^{-1}C(q_0))\cap\Omega} \frac{d(gs)}{\|\nabla q_0\|\,(gx)} = \int_{C(q_0\circ g)\cap\Omega} \frac{ds}{\|\nabla(q_0\circ g)\|} = \int_{C(q)\cap\Omega} \frac{ds}{\|\nabla q\|}$$

Soit donc $x \in C(q_0 \circ g)$, l'élément de volume $(\overrightarrow{ds}, \overrightarrow{n})$ en x est conservé par g, vu que $\det g = 1$, donc $(ds, \overrightarrow{n}) = (\overrightarrow{dgs}, \overrightarrow{gn})$ où $\overrightarrow{n}$ est un vecteur normal à $C(q_0 \circ g)$ en x. Si $\overrightarrow{n'}$ est un vecteur normal à $C(q_0)$ en gx, alors $(\overrightarrow{dgs}, \overrightarrow{gn}) = d(gs)(\overrightarrow{n'}, \overrightarrow{gn})$, or ${}^t g\overrightarrow{n'} = \left\|{}^t g\overrightarrow{n'}\right\| \overrightarrow{n}$ comme on le vérifie aisément, d'où $ds = d(gs)\left\|{}^t g\overrightarrow{n'}\right\|$. De plus, $\nabla(q_0 \circ g)(x) = {}^t g\nabla q_0(gx) = \|\nabla q_0(gx)\|\,{}^t g\overrightarrow{n'}$ donc $\|\nabla(q_0 \circ g)(x)\| = \|\nabla q_0(gx)\| \left\|{}^t g\overrightarrow{n'}\right\|$ ce qui donne bien $\frac{ds}{\|\nabla(q_0 \circ g)\|(x)} = \frac{d(gs)}{\|\nabla q_0\|(gx)}$ et achève la preuve.■

15. Cas des basses signatures et généralisations

Dans ce dernier paragraphe, nous ne ferons qu'évoquer les résultats d'Eskin, Margulis et Mozes sans donner de preuve.

15.1. **Version uniforme du théorème 9.1.** Dans le théorème 9.1. il est question d'une seule forme quadratique irrationnelle q. On peut se demander si la limite obtenue est uniforme lorsque q varie. Pour cela, il faut une version uniforme du théorème d'équirépartition de Ratner. Le reste de la démonstration du théorème 9.1. est quasiment inchangé. Une telle version du théorème de Ratner a été trouvée par Dani et Margulis (cf. [MD2], thm 3) et a permis aux auteurs de [EMM] d'obtenir le théorème suivant :

Théorème 15.1. *Soit $\mathcal{O}_{p,n-p}$ l'ensemble des formes quadratiques de signature $(p, n-p)$ et de déterminant $(-1)^{n-p}$ sur $\mathbb{R}^n$. Soit Ω et $c_{q,\Omega}$ comme en 9.1. On suppose $p \geq 3$ et $n \geq 4$, et on se donne un compact quelconque $\mathcal{D}$ de $\mathcal{O}_{p,n-p}$. Alors, pour tous $a < b$, et tout $\varepsilon > 0$, il existe un ensemble fini $\mathcal{E}$ de $\mathcal{D}$ tel que toute forme de $\mathcal{E}$ est multiple d'une forme rationnelle, et pour tout compact $\mathcal{F} \subseteq \mathcal{D} - \mathcal{E}$, il existe $t_0 \geq 0$ tel que pour tout $t \geq t_0$ et tout $q \in \mathcal{F}$, on a*

$$(1-\varepsilon)c_{q,\Omega}(b-a)T^{n-2} \leq \left|V_{a,b}^{q}(\mathbb{Z}) \cap T\Omega\right| \leq (1+\varepsilon)c_{q,\Omega}(b-a)T^{n-2}$$

15.2. **Cas des signatures (2,1) et (2,2).**

15.2.1. *Contre-exemples.* Pour de telles signatures, le résultat de 9.1. est en défaut. Pour voir cela, on regarde les formes $q_\alpha = x_1^2 + x_2^2 - \alpha^2 x_3^2$ et $\widehat{q}_\alpha = x_1^2 + x_2^2 - \alpha^2(x_3^2 + x_4^2)$. En comptant les triplets pythagoriciens on peut montrer que si α est rationnel

$$\left|\left\{x \in \mathbb{Z}^3 \mid q_\alpha(x) = 0,\ \|x\| \leq T\right\}\right| \sim c_\alpha T \ln T$$

De même on montre que

$$\left|\left\{x \in \mathbb{Z}^4 \mid \widehat{q}_\alpha(x) = 0,\ \|x\| \leq T\right\}\right| \sim c'_\alpha T^2 \ln T$$

pour des constantes > 0 c_α et c'_α. Dans [EMM], les auteurs montrent en approchant β par des rationnels α, que pour tous $\varepsilon > 0$ et $t_0 > 0$, l'ensemble des $\beta \in \mathbb{R}$, pour lesquels il existe $T > t_0$ tel que

$$\left|V_{a,b}^{q_\beta}(\mathbb{Z}) \cap T\Omega\right| \geq T\,(\ln T)^{1-\varepsilon}$$

est dense dans $\mathbb{R}$, où Ω est le même qu'en 9.1. De même l'ensemble des $\beta \in \mathbb{R}$ tels que

$$\left|V_{a,b}^{\widehat{q}_\beta}(\mathbb{Z}) \cap T\Omega\right| \geq T^2 (\ln T)^{1-\varepsilon}$$

pour un certain $T > t_0$, est dense. Ensuite, en utilisant le théorème de Baire, on montre l'existence d'un irrationnel γ et d'une suite $T_j \to \infty$, telle que pour tout $j \in \mathbb{N}$,

$$\left|V_{a,b}^{q_\gamma}(\mathbb{Z}) \cap T_j\Omega\right| \geq T_j (\ln T_j)^{1-\varepsilon}$$

et, respectivement, l'existence d'un irrationnel γ' et d'une suite $T'_j \to \infty$, telle que pour tout $j \in \mathbb{N}$,

$$\left|V_{a,b}^{\widehat{q}_{\gamma'}}(\mathbb{Z}) \cap T'_j\Omega\right| \geq T'_j \left(\ln T'_j\right)^{1-\varepsilon}$$

Ceci montre que pour de telles formes, le résultat de 9.1. est en défaut.

15.2.2. *Résultat presque partout.* Le cas des basses signatures est à part, car lorsque $p = 2$, le résultat d'intégrabilité 11.1. n'est plus valable, par conséquent la preuve du §11 ne fonctionne plus. En fait, les auteurs de [EMM] ont montré que pour $p = 2$ et seulement $0 < s < 1$,

$$\sup_{t \geqslant 0} \int_K (\alpha(a_t k\Delta))^s \, dk < \infty$$

Et c'est même faux lorsque $s = 1$. Cependant, ils ont montré la borne supérieure suivante lorsque $p = 2$

$$\sup_{t \geqslant 1} \frac{1}{t} \int_K \alpha(a_t k\Delta) dk < \infty$$

Grâce à cette borne supérieure et en reprenant certains arguments de la preuve exposée au §11, les auteurs de [EMM] sont parvenus à démontrer deux résultats "positifs". D'une part, ils ont trouvé une borne supérieure valide pour ces signatures, et qui est l'analogue du théorème 13.1. D'autre part, le théorème 9.1., bien que ne s'appliquant pas aux cas des signatures (2,1) et (2,2), reste vrai presque partout. C'est-à-dire, en reprenant les notations du théorème 13.1.,

Proposition 15.1. *Soit $\mathcal{D}$ un compact quelconque de $\mathcal{O}_{p,n-p}$ avec $p = 2$ et $n = 3$ ou 4, Ω comme en 9.1. et $a < b$ quelconques. Alors il existe une constante $c > 0$, telle que pour tout $q \in \mathcal{D}$ et tout $T \geq 2$,*

$$\left|V_{a,b}^{q}(\mathbb{Z}) \cap T\Omega\right| \leq cT^{n-2} \ln T$$

Théorème 15.2. *Pour presque toutes les formes quadratiques q de signature (2,1) et (2,2), on a*

$$\left|V_{a,b}^{q}(\mathbb{Z}) \cap T\Omega\right| \sim c_{q,\Omega}(b-a)T^{n-2}$$

Bibliographie

[Ben] Y. Benoist, Notes de cours de DEA, Paris VII, 1994.

[Bil] P. Billingsley, *Ergodic Theory and Information*, John Wiley and Sons (1965).

[Bla] H. Blaney, *Indefinite quadratic forms in n variables*, J. London Math. Soc. 23 (1948), 153-160.

[Bor] A. Borel, *Introduction aux Groupes Arithmétiques*, Hermann, 1969.

[Bou1] N. Bourbaki, Topologie Générale, fascicule III, livre III, chap. 3, §3 Hermann, 1960

[Bou2] N. Bourbaki, Intégration, fascicule XXIX, livre VI, chap. 7, Hermann, 1963

[CaS] J.W.S. Cassels et Sir Swinnerton-Dyer, *On the product of three homogeneous linear forms and the indefinite ternary quadratic forms,* Philos. Trans. Roy. Soc. London Ser. A. **248** (1955), 73-96.

[DaM1] S.G. Dani et G. Margulis, *Values of quadratic forms at integral points : an elementary approach*, L'enseign. Math. t. **36**, (1990), p. 143-174.

[DaM2] S.G. Dani et G. Margulis, *Limit distribution of orbits of unipotent flows and values of quadratic forms*, Adv. in Soviet Math.**16** (1993), 143-180.

[DeM] Dellacherie & Meyer, *Probabilités et Potentiel*, chap. I-IV, Hermann, 1983.

[EMM] A. Eskin, G. Margulis, et S. Mozes, *Upper bounds and asymptotics in a quantitative version of the Oppenheim conjecture*, Ann. of Math. **147** (1998), 93-141.

[EMM2]A. Eskin, G. Margulis, et S. Mozes, *Quadratic forms of signature (2,2) and eigenvalue spacings on rectangular 2-tori*, (à paraître)

[EsM] A.Eskin, C. McMullen, *Mixing, counting, and equidistribution in Lie groups*, Duke Math. J., **71** n°1, 1993.

[Fus] H. Furstenberg, *A note on Borel density theorem*, Proc. Amer. Math. Soc. **55** n°1, Feb. 1976.

[Hal] P.R. Halmos, *Measure Theory*, Springer-Verlag, 1991.

[HeR] Hewitt et Ross, Abstract Harmonic Analysis, vol. I, chap. 2.

[HoY] Hocking et Young, *Topology*, Dover.

[Hum] J.E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, 1991.

[KlM] D. Kleinbock et G. Margulis, *Logarithm laws for flows on homogeneous spaces*, Invent. Math. **138** (1999), 451-494.

[Kna] A.W. Knapp, *Representation Theory of Semisimple Groups*, Princeton Math. Ser. **36**, Princeton Univ. Press., Princeton, 1986.

[Lan1] S.Lang, *Introduction to diophantine approximations*, Addison-Wesley, 1966.

[Lan2] S. Lang, *Analyse Réelle*, Interéditions, Paris, 1977.

[Mar1] G. Margulis, *Discrete subgroups and ergodic theory*, in Number Theory, Trace Formulas and Discrete Groups (symposium en l'honneur de A. Selberg), pp 377-398, Academic Press, 1989.

[Mar2] G. Margulis, *Indefinite quadratic forms and unipotent flows on homogeneous spaces*, in Dynamical Systems and Ergodic Theory, volume 23, pages 399-409, Banach Center Publ. PWN- Pol. Sci. Publ. Warsaw, 1989.

[Mar3] G. Margulis, *Oppenheim Conjecture*, in Fields Medalists Lectures, Eds. Atiyah, Iagolnitzer, 272-327, World Scientific, 1997.

[MaT1] G. Margulis et G. Tomanov, *Invariant measures for actions of unipotent groups over local fields on homogeneous spaces*, Invent. Math. **116** (1994), 347-392.

[MaT2] G. Margulis et G. Tomanov, *Measure rigidity for almost linear groups and its applications*, J. d'Anal. Math. **69** (1996), 25-54.

[MnT] Mneimné et Testard, *Introduction à la géométrie des groupes classiques*, Hermann.

[OnV] Onishchik et Vinberg, *Lie groups and algebraic groups*, Springer-Verlag, 1988.

[Opp1] Oppenheim, *The minima of indefinite quaternary quadratic forms*, Proc. Nat. Acad. Sci. USA **15** (1929) 724-727.

[Opp2] Oppenheim, *Values of quadratic forms* I et II, Quart. J. Math. Oxford Ser. (2) **4** (1953), 54-66.

[Pet] Petersen, *Ergodic Theory*, Cambridge University Press, 1983.

[Rag] M.S. Raghunathan, *Discrete subgroups of Lie groups*, Springer-Verlag, 1971.

[Rat] M. Ratner, *Interaction between Lie Groups, Ergodic Theory, and Number Theory*, in Proc. of ICM (Zurich, 1994).

[Rud] W. Rudin, *Real and Complex Analysis*, McGraw-Hill, 3d edition, 1987.

[Sam] P. Samuel, *Théorie algébrique des nombres*, Hermann, 1997.

[Sch1] W. Schmidt, *Asymptotic formulae for point lattices of bounded determinant and subspaces of bounded height*, Duke Math. J. 35 (1968), 327-339.

[Sch2] W. Schmidt, *Diophantine Approximation*, LNM Springer-Verlag, 1980.

[Ser] J.P. Serre, *Cours d'arithmétique*, PUF, 1995.

[Sie] C. Siegel, *A mean value theorem in the geometry of numbers*, Ann. of Math., Vol 46, n°2, April, 1945.

[Sik] J.C. Sikorav, *Valeurs des formes quadratiques indéfinies irrationnelles*, Séminaire de Théorie des Nombres, Paris (1987-1988).

[Wei] A. Weil, *L'intégration dans les groupes topologiques et ses applications*, Hermann 1940.