MESURE INVARIANTE ET ÉQUIRÉPARTITION DANS LES GROUPES COMPACTS

BRUNO SÉVENNEC

Dans cet article, on donne un survol de résultats d'équirépartition dans les groupes compacts, et plus généralement dans les espaces homogènes de tels groupes. Dans le premier chapitre, on reproduit la belle preuve de von Neumann sur l'existence et l'unicité de la mesure de Haar des groupes compacts, où l'on voit qu'elle est obtenue comme limite de mesures à support fini. Dans le chapitre 2, on donne des exemples explicites d'équirépartition : le théorème de Weyl (1916) sur les rotations irrationnelles, celui d'Arnol'd et Krylov (1963) pour les rotations sur la sphère $\mathbb{S}^2$, et sa généralisation par Guivarc'h (1969). Le chapitre 3 concerne une mesure de la vitesse d'équirépartition des ensembles obtenus par composition d'un nombre fini d'isométries d'un espace métrique compact. C'est le "trou spectral" de l'opérateur de moyenne associé. Enfin le chapitre 4 passe d'abord en revue la construction, dûe à Lubotzky, Phillips et Sarnak (1986) de rotations de la sphère $\mathbb{S}^2$ avec trou spectral maximal. Après avoir évoqué l'application de ce résultat au problème de Ruziewicz, on discute d'une construction récente de familles de rotations ayant un trou spectral basée sur des arguments plus élémentaires (Gamburd, Jakobson, Sarnak 1999), et qui soulève des questions de type "approximation diophantienne" dans le groupe des rotations.

1. Mesure invariante

En 1933, A. Haar démontre l'existence d'une mesure invariante sur tout groupe localement compact métrisable [15]. L'année suivante paraît [44], dans lequel J. Von Neumann obtient l'existence *et l'unicité* (à un facteur près) pour les groupes compacts métrisables[1], et c'est sa très belle démonstration qui va d'abord nous occuper. Avant de commencer, signalons qu'il avait immédiatement appliqué le résultat de Haar dans le cas compact à la solution partielle du cinquième problème de Hilbert : un groupe compact est de Lie (analytique) si et seulement si il est localement homéomorphe à $\mathbb{R}^n$ [43] (voir aussi [31]).

Soit G un groupe topologique compact (métrisable), et $\mathcal{C}(G)_\mathbb{R}$ l'espace de Banach des fonctions continues réelles sur G. La loi de groupe fournit des opérateurs de translation sur $\mathcal{C}(G)_\mathbb{R}$

$$T_a f(g) = f(ga).$$

Ce sont des isométries. À toute suite finie $A = (a_1, \dots, a_n)$ d'éléments de G, on peut associer l'opérateur moyenne de translations

$$T_A = \frac{1}{n} \sum_1^n T_{a_i}.$$

Date: 19 Février 2004.

[1]Il faut attendre 1936 pour qu'il obtienne (en même temps que A. Weil) l'unicité en général.

Il est de norme ≤ 1. Plus précisément, pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$

$$\inf f \leq \inf T_A f \leq \sup T_A f \leq \sup f \ .$$

En posant $\operatorname{osc}(f) = \sup f - \inf f$, on a donc

$$\operatorname{osc}(T_A f) \leq \operatorname{osc}(f) \ .$$

Lemme 1.1. *Pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$,*

$$\inf_A \operatorname{osc}(T_A f) = 0$$

Démonstration. La fonction f étant uniformément continue et bornée, $\{T_A f\}_A \subset \mathcal{C}(G)_{\mathbb{R}}$ est équicontinu borné, donc d'adhérence compacte (Ascoli). Si $\operatorname{osc}(T_{A_n} f) \to \inf_A \operatorname{osc}(T_A f)$ pour $n \to \infty$, on peut donc supposer quitte à extraire une sous-suite que $T_{A_n} f$ converge uniformément, disons vers $\varphi \in \mathcal{C}(G)_{\mathbb{R}}$.

Pour toute famille finie B d'éléments de G,

$$\operatorname{osc}(T_B \varphi) = \lim \operatorname{osc}(T_B T_{A_n} f) \geq \operatorname{osc}(\varphi)$$

puisque $T_B T_{A_n} = T_{BA_n}$, avec la définition “évidente” de BA_n. D'où l'égalité

$$\operatorname{osc}(T_B \varphi) = \operatorname{osc}(\varphi) \, .$$

En particulier $\sup T_B \varphi = \sup \varphi$, et si $T_B \varphi$ atteint son maximum en $g \in G$, φ l'atteint en tout point de gB. Pour une suite $(b_i)_{i \geq 1}$ dense dans G, en prenant successivement $B = B_n = (b_1, \dots, b_n)$ on obtient des g_n tels que $\varphi = \sup \varphi$ sur $g_n B_n$.

En prenant une sous-suite convergente $g_{n_k} \to g$, on voit que $\varphi = \sup \varphi$ sur l'ensemble dense des gb_i. Donc φ est constante, et $\inf_A \operatorname{osc}(T_A f) = \operatorname{osc}(\varphi) = 0$. □

On voudrait pouvoir définir $\mu(f) = \int_G f \, d\mu = c$ dès que la constante c est limite d'une suite $T_{A_n} f$. Von Neumann appelle alors c une *moyenne à droite* de f. *A priori* elle n'est pas unique. L'astuce est de moyenner aussi à gauche, i.e. considérer les opérateurs $\check{T}_A = \frac{1}{n} \sum_1^n \check{T}_{a_i}$ sur $\mathcal{C}(G)_{\mathbb{R}}$, où

$$\check{T}_a f(g) = f(a^{-1} g) \ .$$

Lemme 1.2. *Si $T_{A_n} f \to c$ et $\check{T}_{A'_n} f \to c'$ avec c, c' constantes, on a $c = c'$. Autrement dit, toute moyenne à gauche coïncide avec toute moyenne à droite.*

Démonstration. Remarquer que les T_A commutent aux $\check{T}_B$, fixent les constantes et sont équicontinus (de norme ≤ 1), d'où

$$c = \lim \check{T}_{A'_n} T_{A_n} f = \lim T_{A_n} \check{T}_{A'_n} f = c'$$

□

Remarque 1.3. Notons $\mu(f)$ la valeur commune des moyennes à droite et à gauche de f. Par le même argument de commutation, on obtient aussi

$$\mu(T_A f) = \mu(f) = \mu(\check{T}_B f) \ .$$

Théorème 1.4. *Il existe sur $\mathcal{C}(G)_{\mathbb{R}}$ une unique forme linéaire μ continue invariante à droite (i.e. $\mu(T_a f) = \mu(f)$) prenant la valeur 1 sur la fonction constante 1. Elle est aussi invariante à gauche, positive, et définit la mesure de Haar (normalisée) sur G.*

Démonstration. L'unicité vient de ce que $\lambda(f) = \lim \lambda(T_{A_n} f) = \mu(f)$ pour toute forme linéaire candidate λ.

Inversement, $f \mapsto \mu(f)$ définit une application continue $\mu : \mathcal{C}(G)_{\mathbb{R}} \to \mathbb{R}$, homogène de degré 1, et ce qu'il reste à voir est qu'elle est additive.

$$\mu(f + f') \stackrel{?}{=} \mu(f) + \mu(f') .$$

Si $\mu(f) = \lim T_{A_n} f$, on a pour tout n

$$\mu(T_{A_n} f') = \mu(f')$$

d'où pour des A'_n convenables

$$\mu(f') = \lim T_{A'_n} T_{A_n} f' .$$

Comme $\mu(f) = \lim T_{A'_n} T_{A_n} f$ est aussi vérifiée, on peut écrire

$$\mu(f) + \mu(f') = \lim T_{A'_n A_n}(f + f') = \mu(f + f') .$$

□

1.1. **Equirépartition.** En itérant l'argument utilisé pour démontrer l'additivité de μ, on obtient au moyen d'un procédé diagonal[2] la

Proposition 1.5. *Il existe une suite (A_n) de familles finies dans G telle $T_{A_n} f \to \mu(f)$ pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$.*

En particulier (évaluer en $e \in G$)

$$\mu(f) = \lim \frac{1}{N_n} \sum_{i=1}^{N_n} f(a_{n,i})$$

pour $A_n = (a_{n,i})_{1 \leq i \leq N_n}$, i.e. μ est limite (faible) des mesures de comptage normalisées

$$\mu_n = \delta_{A_n} = \frac{1}{N_n} \sum_{i}^{N_n} \delta_{a_{n,i}} .$$

On peut donc dire que les suites finies A_n "s'équirépartissent selon μ". Pour donner plus de contenu à cette expression, rappelons comment, X désignant un espace compact (métrisable), on construit à partir d'une forme linéaire positive μ sur $\mathcal{C}(X)_{\mathbb{R}}$ une mesure "ensembliste" positive, σ-additive, encore notée μ. On pose d'abord

$$\begin{array}{rcll} \mu(U) & = & \sup\{\mu(\varphi) | \varphi \leq 1_U\} & U \text{ ouvert} \\ \mu(K) & = & \inf\{\mu(\varphi) | \varphi \geq 1_K\} & K \text{ compact} \end{array}$$

où $\varphi \in \mathcal{C}(X)_{\mathbb{R}}$ et 1_E désigne la fonction caractéristique d'une partie E.

Un sous-ensemble $E \subset G$ est dit μ-mesurable si sa mesure intérieure

$$\mu_*(E) = \sup_{K \subset E} \mu(K)$$

coïncide avec sa mesure extérieure

$$\mu^*(E) = \inf_{U \supset E} \mu(U) .$$

[2]noter que $\mathcal{C}(G)_{\mathbb{R}}$ est séparable, i.e. possède une partie dénombrable dense, à cause de la métrisabilité de G

Leur valeur commune est alors notée $\mu(E)$ (c'est cohérent, comme on le vérifie aisément). Les ensembles μ-mesurables forment une tribu (ou σ-algèbre), qui contient les boréliens et les parties μ-négligeables de X. Si par exemple μ est discrète, i.e. de la forme $\sum_i a_i \delta_{x_i}$ avec $a_i \geq 0$, $\sum a_i < \infty$, toute partie de X est μ-mesurable.

Lemme 1.6. *Soit X un espace compact et $(\mu_n)_{n\geq 1}$ une suite de mesures* positives *qui converge faiblement vers μ, i.e. $\mu_n(f) \to \mu(f)$ pour toute fonction continue f sur X. Si $E \subset X$ et si $\mu(\operatorname{Fr} E) = 0$, E est μ-mesurable et*

$$\mu(E) = \lim \mu_n^*(E) = \lim \mu_{n*}(E) \ .$$

Démonstration. Notons $U = \operatorname{Int} E$, $K = \operatorname{Adh} E$, de sorte que $K - U = \operatorname{Fr} E$. Au vu de leur définition, les fonctionnelles $\lambda \mapsto \lambda(K)$ et $\lambda \mapsto \lambda(U)$ sont semi-continues respectivement supérieurement et inférieurement sur le cône des mesures positives sur X, muni de la topologie faible. Or évidemment $\lambda(U) \leq \lambda(K)$ pour toute mesure positive λ, donc si μ vérifie $\mu(U) = \mu(K)$, c'est un point de continuité des deux fonctionnelles. Sous les hypothèses du lemme on peut donc écrire

$$\liminf \mu_{n*}(E) \geq \lim \mu_n(U) = \mu(U) = \mu(E) = \mu(K) = \lim \mu_n(K) \geq \limsup \mu_n^*(E)$$

d'où la conclusion résulte évidemment. □

Remarque 1.7. On peut montrer sans trop de peine que la conclusion du lemme est aussi une condition suffisante pour que μ_n converge faiblement vers μ. Il s'agit de voir que toute fonction continue est approchée uniformément par des combinaisons linéaires de fonctions de la forme 1_A avec $\mu(\operatorname{Fr} A) = 0$. Pour cela, on peut remarquer que si $f \in \mathcal{C}(X)_{\mathbb{R}}$, l'ensemble de t tels que $\mu(f^{-1}(t)) > 0$ est dénombrable.

Remarque 1.8. L'hypothèse de positivité des μ_n ne peut être supprimée, comme le montre l'exemple de la différence de deux masses de Dirac $\mu_n = \delta_{a_n} - \delta_a$ avec $a_n \to a$, $a_n \neq a$. On a alors $\mu_n \to 0$ et pour $E = \{a_n\}_{n\geq 0}$, $\mu_n(E) = 1$.

Remarque 1.9. Les parties bornées de $\mathbb{R}^n$ à frontière négligeable pour la mesure de Lebesgue sont parfois appelées "quarrables", ou mesurables au sens de Jordan. Ce sont aussi les parties dont la fonction caractéristique est intégrable au sens de Riemann (ou Jordan). Sur un espace compact X muni d'une mesure μ, elles forment une sous-algèbre de celle des parties μ-mesurables, qui est dense pour la distance $d(A, B) = \mu(A \Delta B) = \mu((A - B) \cup (B - A))$.

Lorsque comme ci-dessus on a

$$\mu_n = \lim \delta_{A_n} = \lim \frac{1}{N_n} \sum_1^{N_n} \delta_{a_{n,i}}$$

pour une suite de familles finies

$$A_n = (a_{n,i})_{1\leq i\leq N_n}$$

de points de G, on obtient

Corollaire 1.10. *Si les $A_n = (a_{n,i})_{1\leq i\leq N_n}$ s'équirépartissent selon la mesure de probabilité μ sur X, si $E \subset X$ a une frontière de mesure nulle pour μ, alors*

$$\mu(E) = \lim_n N_n(E)/N_n \ ,$$

où $N_n(E)$ désigne le nombre des i tels que $a_{n,i} \in E$.

Dans le cas où $a_{n,i} = a_i$ est indépendant de n, et où $N_n = n$, on dit aussi que la suite $(a_i)_{i\geq 1}$ est équirépartie selon μ.

1.2. **Espaces homogènes de groupes compacts.** Si $H \subset G$ est sous-groupe fermé du groupe compact (métrisable) G le quotient $X = G/H$ est naturellement un espace compact (métrisable) sur lequel G agit continûment et transitivement.

Théorème 1.11. *Il existe sur X une unique mesure de probabilité invariante par G. Elle est obtenue en projetant sur X la mesure de Haar normalisée de G.*

Démonstration. Noter qu'il suffit de prouver l'unicité. Elle suit le même schéma que la preuve d'unicité des moyennes à gauche ou à droite sur un groupe compact, à ceci près qu'on ne peut translater ici que d'un côté, le rôle des moyennes de l'autre côté étant tenu par la mesure invariante à gauche ν donnée.

Plus précisément, si $f \in \mathcal{C}(X)_{\mathbb{R}}$ l'ensemble des moyennes de translatées $\{T_A f\}_A$ est relativement compact dans $\mathcal{C}(X)_{\mathbb{R}}$, et on montre comme plus haut que $\inf_A \operatorname{osc}(T_A f) = 0$. Il suffit alors de remarquer que toute limite constante $c = \lim T_{A_n} f$ coïncide avec $\nu(f)$ pour toute mesure de probabilité invariante ν sur X. □

2. Exemples explicites d'équirépartition

Dans un groupe compact ou plus généralement un espace homogène d'un groupe compact (métrisable), on peut donner des exemples plus explicites de familles équiréparties selon la mesure de Haar, au moyen de sous-groupes (ou sous-monoïdes) dénombrables denses convenables.

2.1. **Sur le cercle.** (H. Weyl 1916)

Théorème 2.1. [45] *Si $\alpha \in \mathbb{R}$ est irrationnel, la suite $(n\alpha)_{n\geq 0}$ est équirépartie modulo 1 : pour toute $f \in \mathcal{C}(\mathbb{R}/\mathbb{Z})$*

$$\int_{\mathbb{R}/\mathbb{Z}} f(x)\,dx = \lim \frac{1}{n} \sum_{0\leq k<n} f(k\alpha).$$

C'est encore vrai pour toute fonction f intégrable au sens de Riemann, par exemple la fonction caractéristique d'un intervalle I.

Le groupe compact est ici $\mathbb{R}/\mathbb{Z}$, dont la mesure de Haar est la mesure de Lebesgue. Weyl utilise la densité des polynômes trigonométriques dans $\mathcal{C}(\mathbb{R}/\mathbb{Z})$, mais on peut aussi donner une preuve "à la von Neumann", qui s'adapte à tout groupe compact G (commutatif) ayant un sous-groupe dense à un seul générateur α (groupe "monothétique"). Par exemple $(\mathbb{R}/\mathbb{Z})^d$, ou $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n$, groupe additif des entiers p-adiques (p premier), ou encore $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Voici rapidement l'idée. On considère pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$ la suite des

$$S_n f = \frac{1}{n} \sum_{0\leq k<n} T_{k\alpha} f.$$

Selon un lemme classique, la suite de réels

$$u_n = n \operatorname{osc}(S_n f) = \operatorname{osc}(\sum_{0\leq k<n} T_{k\alpha} f)$$

étant visiblement sous-additive (i.e. $u_{m+n} \leq u_m + u_n$), la suite des $u_n/n = \operatorname{osc}(TS_nf)$ converge vers son infimum, donc il suffit de montrer que $\inf_n \operatorname{osc} S_nf = 0$.

Or, comme l'ensemble des S_nf est relativement compact, cet infimum est $\operatorname{osc} g$ pour une fonction $g = \lim S_{n_k}f$, avec $n_k \to \infty$. L'argument pour montrer que g est constante est ici plus direct : on a $T_\alpha g - g = \lim T_\alpha S_{n_k}f - S_{n_k}f$, et pour tout n on a

$$|T_\alpha S_nf - S_nf| \leq \operatorname{osc}(f)/n \ ,$$

d'où $T_\alpha g - g = 0$. Comme α engendre un sous-groupe dense, g est constante.

On en déduit que S_nf tend vers une constante, qui ne peut être que $\mu(f) = \int_G f \, d\mu$ pour la mesure de Haar normalisée μ de G.

2.2. **Sur la sphère.** (V. I. Arnol'd, A. L. Krylov 1963)

On considère la sphère unité $\mathbb{S}^2 \subset \mathbb{R}^3$, espace homogène du goupe compact SO(3) des rotations. Deux rotations $a, b \in \mathrm{SO}(3)$, définissent un opérateur

$$T = T_{(a,b)} = \frac{1}{2}(T_a + T_b) : \mathcal{C}(\mathbb{S}^2) \to \mathcal{C}(\mathbb{S}^2).$$

On a alors $T^n = T_{M_n}$, où pour $n \geq 0$, M_n désigne la famille des 2^n mots (positifs) de longueur n en a, b. Enfin $M = \bigcup_{n\geq 0} M_n$ désigne le sous-monoïde de G engendré par a, b.

Théorème 2.2. [1] *Si pour un $x \in \mathbb{S}^2$, $M \cdot x$ est dense dans $\mathbb{S}^2$, on a pour toute $f \in \mathcal{C}(\mathbb{S}^2)$, $T^nf \to \int f \, d\nu$ (constante). Autrement dit, pout* tout *$x \in \mathbb{S}^2$ la suite des $M_n \cdot x$ s'équirépartit selon la probabilité uniforme ν sur $\mathbb{S}^2$.*

Une démonstration est donnée plus loin, qui simplifie et généralise celle d'Arnol'd et Krylov. On verra même qu'en fait les M_n s'équirépartissent selon la mesure de Haar de SO(3).

Remarque 2.3. On montre aisément qu'un sous-monoïde fermé d'un groupe compact est en fait un sous-groupe. Il revient donc au même de supposer que le sous-groupe Γ engendré par a, b a une orbite dense, ce qui est *a priori* plus faible.

Il est "facile" de vérifier l'hypothèse du théorème, en vertu du

Lemme 2.4. *Pour presque tout couple (a, b) de rotations dans* SO(3)*, le sous-monoïde engendré par a, b est dense dans* SO(3)*.*

Démonstration. Si a est d'angle irrationnel, $\overline{\{a^n\}}_{n\geq 0}$ est le sous-groupe des rotations de même axe que a. Deux tels sous-groupes d'axes distincts engendrent SO(3). □

Remarque 2.5. L'ensemble des couples $(a, b) \in \mathrm{SO}(3) \times \mathrm{SO}(3)$ qui n'engendrent pas un sous-groupe dense de SO(3) est non seulement de mesure nulle, mais est un fermé algébrique de codimension ≥ 2. C'est plus généralement le cas pour les groupes de Lie compacts à centre fini (i.e. semi-simples), mais pas pour les tores $(\mathbb{R}/\mathbb{Z})^n$, par exemple.

Remarque 2.6. Tout groupe de Lie compact connexe G admet un sous-groupe (ou sous-monoïde) dense à deux générateurs (Auerbach 1933 [2]). C'est encore vrai si G est un groupe compact connexe (Schreier-Ulam 1935 [40]). Un critère particulièrement élégant pour que des éléments proches de l'unité dans un groupe de Lie réel semi-simple connexe engendrent un sous-groupe dense figure dans [7] : il suffit que leurs "logarithmes" engengrent l'algèbre de Lie du groupe.

2.3. **Une généralisation.** (Y. Guivarc'h 1969, voir aussi [4, 5])

Soit X un espace métrique compact, a, b deux isométries de X, et $\Gamma \subset \mathrm{Isom}(X)$ le sous-groupe qu'elles engendrent.

On note $\Gamma_0 \subset \Gamma$ le sous-groupe des $\prod a^{m_i} b^{n_i}$ tels que $\sum(m_i + n_i) = 0$ (il est engendré par les $a^n b^{-n}$, $n \in \mathbb{Z}$).

Théorème 2.7. [14] *Supposons que Γ_0 a une orbite dense dans X. Alors*

- *X est un espace homogène du groupe compact $G = Isom(X)$.*
- *Pour tout $x \in X$, les $M_n \cdot x$ s'équirépartissent selon l'unique probabilité G-invariante ν sur X.*

Démonstration. Le premier point résulte aussitôt de la compacité du groupe des isométries de X, qui entraîne que ses orbites sont fermées.

Pour vérifier le second, il suffit de voir que $T^n f \to$ const pour toute $f \in \mathcal{C}(X)_\mathbb{R}$, avec $T = \frac{1}{2}(T_a + T_b)$. L'ensemble des $T^n f$ étant relativement compact dans $\mathcal{C}(X)_\mathbb{R}$, il s'agit de montrer que toute valeur d'adhérence de la suite $T^n f$ est constante.

Soit donc $\varphi = \lim_k T^{n_k} f$ une telle valeur d'adhérence, avec $n_{k+1} > n_k$. La remarque cruciale est alors que l'opérateur T est aussi continu de norme ≤ 1 sur $L^2(X, \nu)$, comme moyenne de T_a, T_b qui sont des isométries.

L'inclusion $\mathcal{C}(X) \hookrightarrow L^2(X, \nu)$ étant continue, on a pour les normes L^2

$$\|\varphi\| = \lim \|T^{n_{k+1}} f\| \leq \lim \|T T^{n_k} f\| = \|T\varphi\| \, .$$

Donc $\|T\varphi\| = \|\varphi\|$, c'est-à-dire

$$\|\tfrac{1}{2}(T_a\varphi + T_b\varphi)\| = \|T_a\varphi\| = \|T_b\varphi\| \, .$$

On en conclut que $T_a\varphi = T_b\varphi$ (par Pythagore !).

Le même argument montre que $T_s\varphi = T_{s'}\varphi$ si s, s' sont deux mots positifs de même longueur en a, b, i.e. appartiennent à un même M_n. Dans ce cas φ est donc invariante par tout $s^{-1}s' \in M_n^{-1}M_n$. On en déduit que φ est invariante par Γ_0 (et donc constante, comme annoncé) grâce au

Lemme 2.8. *Γ_0 est contenu dans l'adhérence de $\bigcup_n M_n^{-1}M_n$ et Γ dans celle de $M = \bigcup_n M_n$.*

Démonstration. Le groupe G étant compact, il existe des suites p_k, q_k tendant vers $+\infty$ telles que $a^{p_k} \to 1$, $b^{q_k} \to 1$. Soit

$$\gamma = a^{m_1} b^{n_1} a^{m_2} b^{n_2} \dots \, a^{m_r} b^{n_r}$$

un élément de Γ, avec $\sum(m_i + n_i) = 0$ si de plus $\gamma \in \Gamma_0$. Alors

$$\gamma = \lim_k \, a^{m_1+p_k} b^{n_1+q_k} \dots a^{m_r+p_k} b^{n_r+q_k} \, .$$

Il est clair que $a^{m_1+p_k} b^{n_1+q_k} \dots a^{m_r+p_k} b^{n_r+q_k}$ est un mot positif en a, b pour k assez grand, donc γ appartient bien à l'adhérence de $M = \bigcup_n M_n$.

De même si $\sum(m_i + n_i) = 0$ ($\gamma \in \Gamma_0$), l'écriture

$$\gamma = \lim_k \, (a^{p_k} b^{q_k})^{-r} a^{m_1+p_k} b^{n_1+q_k} \dots a^{m_r+p_k} b^{n_r+q_k}$$

jointe au fait que $a^{m_1+p_k} b^{n_1+q_k} \dots a^{m_r+p_k} b^{n_r+q_k}$ et $(a^{p_k} b^{q_k})^r$ sont des mots positifs et de même longueur pour k assez grand, montre que γ est adhérent à $\bigcup_n M_n^{-1}M_n$. $\square$

Remarque 2.9. Un résultat analogue reste vrai si on remplace a, b par k éléments $a_1, \ldots, a_k$ de G, Γ_0 par le sous-groupe des mots de somme d'exposants nulle en les $a_i^{\pm 1}$, et M_n la famille des k^n mots positifs de longueur n en les a_i. La preuve est essentiellement la même.

Pour déduire de ce théorème celui d'Arnol'd et Krylov énoncé plus haut (où $X = \mathbb{S}^2$), il suffit de montrer que si M a une orbite dense, Γ_0 en possède une aussi. Comme d'après le lemme précédent $\overline{M} = \overline{\Gamma}$, on voit qu'il revient au même de supposer que $\overline{\Gamma} \subset \mathrm{SO}(3)$ est transitif sur $\mathbb{S}^2$, i.e. que Γ a une orbite dense. Admettant provisoirement que le seul sous-groupe de $\mathrm{SO}(3)$ transitif sur $\mathbb{S}^2$ est $\mathrm{SO}(3)$ lui-même, on a dans ce cas $\overline{\Gamma} = \mathrm{SO}(3)$. Mais Γ_0 contient le sous-groupe dérivé $[\Gamma, \Gamma]$, dont l'adhérence contient $[\overline{\Gamma}, \overline{\Gamma}]$. Or ce dernier groupe est $\mathrm{SO}(3)$ car celui-ci est égal à son sous-groupe dérivé. Il reste à établir le

Lemme 2.10. [3] *Le seul sous-groupe (non nécessairement fermé) de* $\mathrm{SO}(3)$ *transitif sur* $\mathbb{S}^2$ *est* $\mathrm{SO}(3)$.

Démonstration. Si $G \subset \mathrm{SO}(3)$ est transitif sur $\mathbb{S}^2$, le groupe $A \subset \mathbb{R}/2\pi\mathbb{Z}$ des angles des rotations fixant $x \in \mathbb{S}^2$ ne dépend pas de x. Or si a, b sont des rotations d'angles (non nuls) α, β fixant x, y respectivement, l'angle γ de la rotation composée ab dépend effectivement (et continûment) de la distance de x à y [4]. Il en résulte que le sous-groupe A contient un intervalle ouvert non vide de $\mathbb{R}/2\pi\mathbb{Z}$, d'où $A = \mathbb{R}/2\pi\mathbb{Z}$ et $G = \mathrm{SO}(3)$. □

Remarque 2.11. Si le sous-groupe est supposé fermé (c'est tout ce dont on a besoin ici), c'est un sous-groupe de Lie de dimension au moins 2, et il en résulte aussitôt qu'il est de dimension 3, donc égal à $\mathrm{SO}(3)$. Plus généralement d'après Borel [6], un sous-groupe fermé strict de $\mathrm{SO}(2n+1)$ transitif sur $\mathbb{S}^{2n}$ n'existe que pour $n = 3$, et est alors isomorphe à $G_2 = \mathrm{Aut}(\mathbb{O})$, groupe des automorphismes de l'algèbre des octaves de Cayley, qui opère transitivement sur $\mathbb{S}^6 \subset \mathrm{Im}\,\mathbb{O} \simeq \mathbb{R}^7$.

Remarque 2.12. Dans le théorème d'Arnold et Krylov, puisque Γ_0 est dense dans $\mathrm{SO}(3)$, on peut en fait conclure que les M_n s'équirépartissent selon la mesure de Haar de $\mathrm{SO}(3)$. En général, si X désigne un espace métrique compact, on voit de même que si $\overline{\Gamma} = H$ est un sous-groupe parfait de $\mathrm{Isom}(X)$, les M_n séquirépartissent selon la mesure de Haar de H.

2.4. **Un autre résultat d'équirépartition.** On considère à nouveau un espace métrique compact X, deux isométries a, b de X, et $\Gamma \subset \mathrm{Isom}(X)$ le sous-groupe qu'elles engendrent. On notera $\Gamma^{(2)} \subset \Gamma$ le sous-groupe (d'indice au plus 2) constitué des mots de somme d'exposants paire en $a^{\pm 1}, b^{\pm 1}$. Il contient le sous-groupe dérivé $[\Gamma, \Gamma]$.

Enfin, Σ_n désigne la famille des mots réduits (i.e. sans lettres inverses consécutives) de longueur n en $a^{\pm 1}$, $b^{\pm 1}$. Ils sont au nombre de 4.3^{n-1} pour $n \geq 1$.

Théorème 2.13. [1, 14] *Si* $\Gamma^{(2)}$ *a une orbite dense dans* X, X *est homogène, et pour tout* $x \in X$ *les* $\Sigma_n \cdot x$ *s'équirépartissent selon l'unique probabilité* ν *invariante par isométries sur* X.

Démonstration. Il s'agit de montrer que les opérateurs

$$S_n = \frac{1}{4.3^{n-1}} \sum_{s \in \Sigma_n} T_{s(a,b)} \qquad (n \geq 1)$$

[3] Je tiens à remercier Pierre de la Harpe de m'avoir signalé ce résultat, qu'il attribue à Élie Cartan.

[4] plus précisément $\gamma \neq \alpha + \beta$ quand y est voisin de x et $y \neq x$.

(et $S_0 = \mathrm{Id}$) de $\mathcal{C}(X)_{\mathbb{R}}$ dans lui-même vérifient $S_n f \to \mathrm{const} = \int f\, d\nu$ pour toute $f \in \mathcal{C}(X)_{\mathbb{R}}$. Mais les S_n sont aussi des opérateurs continus (de norme 1) de $L^2(X,\nu)$ dans lui-même, et ils sont *auto-adjoints*. Leurs spectres sont donc contenus dans $[-1,1]$.

Une remarque simple, mais cruciale pour la suite, est qu'ils satisfont à la relation de récurrence

$$S_1 S_n = 3/4\, S_{n+1} + 1/4\, S_{n-1} \qquad (n \geq 1)\ .$$

On a donc $S_n = P_n(S_1)$ pour des polynômes réels $P_n(t)$: $P_0 = 1$, $P_1 = t$, $P_2 = (4t^2-1)/3$, ...

Les mêmes polynômes P_n interviennent dans la situation "abstraite" suivante : on se donne deux opérateurs unitaires A, B d'un espace de Hilbert complexe H, et on pose

$$S_n(A,B) = \frac{1}{4.3^{n-1}} \sum_{s \in \Sigma_n} s(A,B)\ .$$

Alors $S_n(A,B) = P_n(S_1(A,B))$. Prenant en particulier $A = B = \exp(i\theta)$ opérant sur $H = \mathbb{C}$, on a $S_1 = \cos(\theta)$ et $|P_n(\cos(\theta))| = |S_n| \leq 1$. Il en résulte que

$$|P_n(t)| \leq 1 \text{ si } |t| \leq 1\ .$$

Par ailleurs, si on désigne par λ, λ' les racines de $4t\lambda = 3\lambda^2 + 1$ (équation caractéristique de la récurrence), on a $P_n(t) = c\lambda^n + c'\lambda'^n$ (ou $c\lambda^n + c'n\lambda^{n-1}$ si $\lambda = \lambda'$). Comme l'équation caractéristique $\lambda^2 - 4/3\, t\lambda + 1/3 = 0$ n'a visiblement pas de solution de module 1 quand $|t| < 1$, on obtient (puisque $P_n(t)$ reste borné pour $n \to \infty$)

$$\lim_n P_n(t) = 0, \qquad |t| < 1$$

et la convergence est même exponentielle pour chaque t fixé dans $]-1,1[$.

Or le théorème de décomposition spectrale des opérateurs auto-adjoints bornés (voir [21], [47] par exemple) permet essentiellement[5] d'identifier S_1 opérant sur $L^2(X,\nu)$ à l'opérateur de multiplication par t sur $L^2(\mathbb{R}, \sigma(dt))$ où σ est une mesure positive supportée par le spectre de S_1 (et donc par $[-1,1]$). On notera $\varphi \leftrightarrow \hat{\varphi}$ l'isométrie $L^2(X,\nu) \leftrightarrow L^2(\mathbb{R}, \sigma(dt))$ réalisant cette identification. L'orthogonal de $\ker(S_1 \pm 1)$ correspond alors à l'espace des (classes de) fonctions $\hat{\varphi}$ nulles en ∓ 1.

On en déduit que $S_n\varphi = P_n(S_1)\varphi \to 0$ dans $L^2(X,\nu)$ pour toute $\varphi \in L^2(X,\nu)$ orthogonale à $\ker(S_1 \pm 1)$. En effet $P_n(t)\hat{\varphi}(t)$ est dominée par $|\hat{\varphi}(t)|$ et converge vers 0 pour tout $t \in [-1,1]$ (donc σ-presque partout) lorsque $\hat{\varphi}(\pm 1) = 0$, et on conclut grâce au théorème de convergence dominée de Lebesgue.

Enfin, l'hypothèse sur $\Gamma^{(2)}$ entraîne $\ker(S_1 + 1) = 0$ et $\ker(S_1 - 1) = \{\mathrm{const}\}$, car pour $\varphi \in L^2(X,\nu)$, $S_1\varphi = \pm\varphi$ impose $T_a\varphi = T_b\varphi = \pm\varphi$ et donc $T_g\varphi = \varphi$ pour tout $g \in \Gamma^{(2)}$. Or $g \mapsto T_g\varphi$ est continue de G dans $L^2(X,\nu)$, et $\overline{\Gamma^{(2)}}$ agit transitivement sur X, d'où l'assertion.

On en conclut que $S_n f \to \nu(f)$ pour toute $f \in \mathcal{C}(X)$, où la convergence, *a priori* dans $L^2(X,\nu)$, a en fait lieu dans $\mathcal{C}(X)$ puisque l'ensemble des $S_n f$ est relativement compact dans $\mathcal{C}(X)$. □

Remarque 2.14. Les polynômes P_n vérifient en fait

$$|P_n(t)| < 1 \text{ si } |t| < 1 \ (n \geq 1).$$

[5] quitte à restreindre S_1 au sous-espace fermé invariant engendré par un vecteur quelconque. Ce n'est pas gênant ici, et évite les problèmes liés à la possible multiplicité du spectre.

En effet, avec $A = B = \exp(i\theta)$ opérant dans $H = \mathbb{C}$ comme ci-dessus, $|P_n(\cos(\theta))| = |S_n| = 1$ n'est possible que si tous les $s(A, B) \in \mathbb{S}^1$, $s \in \Sigma_n$ sont égaux, ce qui nécessite $A^2 = 1$ et donc $\cos(\theta) = \pm 1$. De plus, on vérifie sans trop de peine que l'on a $|P_n(t)| \leq (2n-1)|\lambda|^{n-1}$ pour $n \geq 1$ et λ racine de plus grand module de l'équation caractéristique. Il en résulte que

$$\sup_{|t|\leq\delta, n\geq 1} |P_n(t)|^{1/n} < 1 \text{ pour tout } \delta < 1$$

i.e.

$$|P_n(t)| \leq (1 - \epsilon(|t|))^n$$

pour une fonction ϵ décroissante strictement positive sur $[0, 1[$.

Remarque 2.15. Comme plus haut, il suffit pour $X = \mathbb{S}^2$ et $\Gamma \subset \mathrm{SO}(3)$ de supposer que Γ a une orbite dense sur $\mathbb{S}^2$, puisque $\Gamma^{(2)} \supset [\Gamma, \Gamma]$.

Remarque 2.16. Ici encore, la preuve s'adapte aisément à $k \geq 2$ générateurs $a_1, \ldots, a_k$, où $\Gamma^{(2)}$ est le sous-groupe des mots de somme d'exposants paire en les $a_i^{\pm 1}$, et Σ_n la famille des mots réduits de longueur n en les $a_i^{\mp 1}$ (au nombre de $2k(2k-1)^{n-1}$ pour $n \geq 1$).

3. Vitesse d'équirépartition et trou spectral

Soit $A = (a_1, ..., a_k)$ une famille finie d'isométries d'un espace métrique compact X homogène (par exemple une famille d'éléments de $\mathrm{O}(3) = \mathrm{Isom}(\mathbb{S}^2)$). On note ν la mesure de probabilité invariante par isométries sur X, et

$$T = \frac{1}{2}(T_A + T_A^*) = \frac{1}{2k}\sum_{i=1}^{k}(T_{a_i} + T_{a_i}^{-1})$$

opérant sur l'espace de Hilbert $L^2(X, \nu)$. C'est un opérateur auto-adjoint de norme ≤ 1, et il agit trivialement sur les constantes.

Désignons par $L_0^2 = L_0^2(X, \nu)$ le sous-espace des fonctions L^2 de moyenne nulle sur X (i.e. l'orthogonal des constantes); il est invariant par T. On note

$$\delta(A) = \delta(a_1, ..., a_k) = \|T\|_{L_0^2} \leq 1 \ .$$

la norme de T sur ce sous-espace.

Alors la propriété de "trou spectral" $\delta(A) < 1$ entraîne non seulement la convergence $T^n f \to \int_X f\, d\nu$, pour toute $f \in L^2(X, \nu)$, mais aussi que cette convergence est exponentiellement rapide (en norme L^2).

Mieux, en désignant par Σ_n la famille des mots réduits de longueur n en les $a_i^{\pm 1}$, et $S_n = T_{\Sigma_n}$ l'opérateur moyenne de translations correspondant, on a la

Proposition 3.1. *La propriété de trou spectral $\delta(A) < 1$ entraîne $S_n f \to \int_X f\, d\nu$ exponentiellement rapidement en norme L^2 pour toute $f \in L^2(X, \nu)$. Plus précisément, on a $\|S_n\|_{L_0^2} \leq (1 - \epsilon)^n$ pour un $\epsilon = \epsilon(\delta(A)) > 0$.*

Démonstration. Les opérateurs S_n vérifient une relation de récurrence analogue à celle vue plus haut pour $k = 2$, à savoir

$$TS_n = \frac{2k-1}{2k} S_{n+1} + \frac{1}{2k} S_{n-1} \ .$$

On en déduit que $S_n = P_n(S_1) = P_n(T)$, où les polynômes réels P_n vérifient encore $|P_n(t)| \leq 1$ pour $|t| \leq 1$. Comme dans la remarque 2.14 ci-dessus, on a même $|P_n(t)| \leq (1-\varepsilon(|t|))^n$ pour une fonction décroissante $\varepsilon : [0,1] \to [0,1]$, strictement positive sur $[0,1[$.

La conclusion résulte alors du théorème de décomposition spectrale, puisque par hypothèse le spectre de T sur L^2_0 est contenu dans $[-\delta(A), \delta(A)] \subset \,]-1,1[$. □

On pourrait montrer le même type de résultat pour la famille des mots réduits de longueur au plus n en les $a_i^{\pm 1}$.

Remarque 3.2. Lorsque $X = \mathbb{S}^2$, si f est assez régulière (par exemple $f \in \mathcal{C}^2$), la convergence de $T^n f$ et $S_n f$ est aussi exponentiellement rapide en norme uniforme. Cela tient au fait que, le laplacien $\Delta_{\mathbb{S}^2}$ sur $\mathbb{S}^2$ commutant aux T_g ($g \in \mathrm{SO}(3)$), il commute avec T et les S_n. En particulier pour $f \in \mathcal{C}^2$, ou même seulement $\Delta_{\mathbb{S}^2} f \in L^2$,

$$\|\Delta_{\mathbb{S}^2} S_n f\|_{L^2} = \|S_n \Delta_{\mathbb{S}^2} f\|_{L^2} \leq (1-\epsilon)^n \|\Delta_{\mathbb{S}^2} f\|_{L^2}.$$

Le résultat découle alors de l'inclusion de Sobolev $\Delta_{\mathbb{S}^2} u \in L^2(\mathbb{S}^2) \Rightarrow u \in C^0(\mathbb{S}^2)$.

Par contre, la norme de chaque S_n sur l'espace $\mathcal{C}_0(X)$ des fonctions continues de moyenne nulle (muni de la norme uniforme) est égale à 1 dès que X est infini. Par application de Banach-Steinhaus, on en déduit l'existence de fonctions continues f pour lesquelles la convergence de $S_n f$ vers la moyenne de f est arbitrairement lente.

Il existe une borne à la vitesse d'équirépartition mesurée par le trou spectral :

Théorème 3.3. *Soit X un espace métrique compact homogène infini, ν sa mesure de probabilité invariante par isométries, et S un ensemble fini d'isométries de X, invariant par $s \mapsto s^{-1}$. Alors la norme de l'opérateur $T_S = \frac{1}{|S|}\sum_{s \in S} T_s$ sur $L^2_0(X,\nu)$ est minorée par $\frac{2}{|S|}\sqrt{|S|-1}$.*

Démonstration. Soit p un entier positif. Alors si ϕ est une fonction de norme 1 dans $L^2_0(X)$, on a

$$\langle T^{2p}\phi, \phi \rangle = \|T^p \phi\|^2 \leq \|T^p\|^2 \leq \|T\|^{2p}$$

où $T = T_S$ et les normes sont sur $L^2_0(X)$ (T est autoadjoint à cause de la symétrie de S). On va d'abord trouver ϕ permettant de minorer commodément le produit scalaire ci-dessus. On a aussi

$$T^{2p} = \frac{1}{|S|^{2p}} \sum_{(s_1,\ldots,s_{2p}) \in S^{2p}} T_{s_1 \ldots s_{2p}}.$$

Or on peut trouver un point $x \in X$ tel que pour tout produit $g = s_1 \ldots s_{2p}$ de $2p$ éléments de S, ont ait soit $gx \neq x$, soit $g = \mathrm{Id}$ au voisinage de x. En effet, l'ensemble des x ayant cette propriété n'est autre que le complémentaire de la réunion (finie) des frontières des fermés $\mathrm{Fix}(g)$; or la frontière d'un fermé est un fermé d'intérieur vide, et l'union d'un nombre fini (ou même dénombrable) de tels ensembles ne peut recouvrir X.

Soit maintenant ε l'infimum des distances non nulles $d(x, gx)$ et des distances $d(x, X - \mathrm{Fix}(g))$ lorsque $gx = x$, pour g produit de $2p$ éléments de S. Puisque X est compact homogène et infini, x n'est pas isolé dans X et on peut trouver dans la boule ouverte $B(x,\varepsilon)$ deux boules ouvertes isométriques disjointes (et non vides !), B_1, B_2. On pose maintenant

$$\phi = (1_{B_1} - 1_{B_2}) / \|1_{B_1} - 1_{B_2}\|_{L^2} \in L^2_0(X,\nu).$$

Il est alors clair que pour tout produit g de $2p$ éléments de S, on a $\langle T_g\phi, \phi\rangle = 0$ ou 1, et c'est bien sûr 1 si $g = \mathrm{Id}$. Avec ce choix de ϕ, on a donc

$$\langle T^{2p}\phi, \phi\rangle \geq \frac{1}{|S|^{2p}} m_{2p},$$

où m_{2p} est le nombre de suites $(s_1, \ldots, s_{2p}) \in S^{2p}$ telles que $s_1 \ldots s_{2p} = \mathrm{Id}$. Il reste à établir l'inégalité $\sup_p m_{2p}^{1/2p} \geq 2\sqrt{|S|-1}$.

Or le nombre m_{2p} est minoré par le nombre r_{2p} de chemins de longueur $2p$ dans l'arbre régulier $\mathcal{A}$ de valence $|S|$ qui commencent et finissent en un sommet fixé (origine). En effet, $\mathcal{A}$ s'envoie naturellement sur le graphe de Cayley[6] du groupe Γ engendré par S. Le fait que $\lim_p r_{2p}^{1/2p} = 2\sqrt{|S|-1}$ est connu au moins depuis [23], mais, pour la commodité du lecteur, on va donner ici une preuve de la minoration de la limite (voir aussi l'exercice 9, p. 13 dans [17]).

Soit $l^2(\mathcal{A})$ l'espace des fonctions de carré sommable sur l'ensemble des sommets de $\mathcal{A}$. Il admet pour base hilbertienne la famille des fonctions caractéristiques δ_x des sommets de $\mathcal{A}$. Désignons par $\widehat{T}$ l'opérateur "moyenne sur les sommets voisins" de $l^2(\mathcal{A})$ dans lui-même. On a alors clairement

$$\|\widehat{T}^p\delta_o\|^2 = \langle \widehat{T}^{2p}\delta_o, \delta_o\rangle = \frac{1}{|S|^{2p}} r_{2p}$$

où o est l'origine fixée dans $\mathcal{A}$.

Remarquons tout d'abord que pour tout ouvert $I \subset \mathbb{R}$, le projecteur spectral P_I de l'opérateur autoadjoint $\widehat{T}$ commute avec tout opérateur qui commute avec $\widehat{T}$, et donc avec les opérateurs unitaires induits par les automorphismes du graphe $\mathcal{A}$. En particulier si $P_I\delta_o = 0$, on a aussi $P_I\delta_x = 0$ pour tout sommet x, donc $P_I = 0$ et I est disjoint du spectre de $\widehat{T}$. En prenant $I =]-\infty, -\|\widehat{T}\| + \varepsilon[\cup]\|\widehat{T}\| - \varepsilon, +\infty[$, $(\varepsilon > 0)$ on en conclut que $P_I\delta_o \neq 0$, et donc que $\liminf_p \|\widehat{T}^p\delta_o\|^{1/p} \geq \|\widehat{T}\| - \varepsilon$. Comme ceci est vrai pour tout $\varepsilon > 0$, on a

$$\frac{1}{|S|} \lim_p r_{2p}^{1/2p} = \lim_p \|\widehat{T}^p\delta_o\|^{1/p} = \|\widehat{T}\| \quad .$$

Reste à minorer la norme de $\widehat{T}$. Pour cela, on va montrer que tout λ réel inférieur à $\frac{2}{|S|}\sqrt{|S|-1}$ en valeur absolue appartient au spectre de $\widehat{T}$. Sinon, par définition du spectre, il existerait une *unique* fonction $u = (u_x)_x \in l^2(\mathcal{A})$ telle que $\widehat{T}u - \lambda u = \delta_o$. Comme u est unique et que $\widehat{T}$ commute avec les automorphismes de $\mathcal{A}$, u_x ne dépend que de la distance de x à o dans l'arbre $\mathcal{A}$). En effet les automorphismes de $\mathcal{A}$ qui fixent o agissent transitivement sur les sommets à distance n de o, pour tout n. Notons $u_n = u_x$ si x est à distance n de o.

Maintenant, l'équation définissant u fournit immédiatement

$$u_1 - \lambda u_0 = 1, \quad \text{et}$$

$$(|S|-1)u_{n+1} + u_{n-1} = \lambda|S|u_n \quad \text{si } n \geq 1.$$

L'équation caractéristique de la récurrence ci-dessus est

$$(|S|-1)X^2 - \lambda|S|X + 1 = 0,$$

[6]Ici, il s'agit du graphe dont l'ensemble des sommets est Γ, et dont deux sommets x, y sont joints par une arête s'il existe $s \in S$ tel que $y = xs$.

donc si $(\lambda|S|)^2 < 4(|S|-1)$, les deux racines sont complexes de module $(|S|-1)^{-1/2}$, et

$$|u_n| \geq c/(|S|-1)^{n/2}$$

pour une infinité de n et un $c > 0$. Mais la norme de u est donnée par

$$\|u\|^2 = |u_0|^2 + \sum_{n\geq 1} |S|(|S|-1)^{n-1}|u_n|^2,$$

et l'inégalité ci-dessus montre que cette série diverge. Donc le spectre de $\widehat{T}$ contient l'intervalle $|\lambda| < \frac{2}{|S|}\sqrt{|S|-1}$, et on a bien $\|\widehat{T}\| \geq \frac{2}{|S|}\sqrt{|S|-1}$. □

Remarque 3.4. Ce théorème est démontré pour $X = \mathbb{S}^2$ dans [26] (voir aussi [8]) par une méthode différente, qui donne des renseignements supplémentaires sur le spectre de T : elle consiste à restreindre T aux espaces propres V_n du laplacien sur $\mathbb{S}^2$ et à montrer que les traces normalisées $\mathrm{tr}(T^k|_{V_n})/\dim(V_n)$ convergent pour $n \to \infty$ vers $m_k/|S|^k$, où m_k est le nombre de mots de longueur k en S dont le produit est l'identité. En particulier les valeurs propres de T sur V_n s'équirépartissent pour $n \to \infty$ selon la mesure μ de moments $\int t^k \mu(dt) = m_k/|S|^k$, $k \geq 0$. Noter que μ ne dépend que du groupe "abstrait" Γ engendré par S et de son système de générateurs S. Un énoncé du même type valable pour X riemannienne compacte est donné dans [36] (sans démonstration). Enfin, la minoration de $\|\widehat{T}\|$ se trouve dans [23], lorsque $s \neq s^{-1}$ pour tout $s \in S$, ainsi que le fait que Γ est libre en cas d'égalité (voir aussi [30, 32]).

4. Trou spectral sur $\mathbb{S}^2$

On connaît pour $X = \mathbb{S}^2$ une infinité (dénombrable) d'exemples de $S \subset \mathrm{SO}(3)$ qui atteignent la borne donnée par le théorème ci-dessus, et en particulier possèdent.

Théorème 4.1. [26] *Si p est premier avec $p \equiv 1(\mathrm{mod}\ 4)$, il existe un ensemble symétrique $S_p = S_p^{-1} \subset \mathrm{SO}(3)$ formé de $p+1 = 2k$ rotations et tel que $\|T_{S_p}\|_{L_0^2(\mathbb{S}^2)} = \sqrt{2k-1}/k$.*

Les rotations du théorème sont celles associées aux quaternions entiers $x_0 + x_1e_1 + x_2e_2 + x_3e_3$ à partie réelle x_0 positive et impaire situés sur la sphère de rayon $\sqrt{p}$, i.e. les solutions entières de $x_0^2 + x_1^2 + x_2^2 + x_3^2 = p$ avec x_0 positif impair.

Rappelons que tout quaternion non nul $q \in \mathbb{H} \simeq \mathbb{R} \oplus \mathbb{R}^3$ définit une rotation $R_q \in \mathrm{SO}(3)$ par $v \in \mathbb{R}^3 = \mathrm{Im}\mathbb{H}$, $v \mapsto R_q(v) = qvq^{-1} = qv\overline{q}/|q|^2$. Explicitement, si $q = x + u \in \mathbb{R}_+ \oplus \mathbb{R}^3$, R_q est la rotation d'axe $\mathbb{R}u$ et d'angle $2\tan^{-1}(|u|/x) = \cos^{-1}((x^2-|u|^2)/(x^2+|u|^2))$.

On sait depuis Jacobi que pour tout entier $n \geq 1$, l'équation $x_0^2 + x_1^2 + x_2^2 + x_3^2 = n$ possède au total $8N$ solutions entières, où N est la somme des diviseurs de n non divisibles par 4 (voir [16],[25] ou [9]). En particulier pour $n = p$ premier, il y a $8(p+1)$ solutions, et lorsque $p \equiv 1(\mathrm{mod}\ 4)$, on voit facilement que $p+1$ d'entre elles vérifient x_0 impair et positif. Par exemple pour $k = 3$, on trouve les rotations d'angle $\cos^{-1}(-3/5)$ autour des trois axes de coordonnées, associées aux quaternions $1 + 2e_i$, $i = 1, 2, 3$.

Très brièvement, la preuve du théorème 4.1 procède ainsi (voir [26],[8],[37] ou [25] pour plus de détails). Les opérateurs autoadjoints $\Delta_{\mathbb{S}^2}$ et $T_p = T_{S_p}$ commutant sur $L_0^2(\mathbb{S}^2)$, ils possèdent une base hilbertienne de fonctions propres communes. Si u est une telle fonction propre c'est une "harmonique sphérique", restriction à $\mathbb{S}^2$ d'un polynôme homogène harmonique de degré m sur $\mathbb{R}^3$, et elle vérifie $T_pu = \lambda u$. Suivant Schoeneberg [38] (voir aussi [29],[39] pour un historique), on construit à l'aide de u une forme holomorphe $\theta_u(z)\,(dz)^{m+1}$ sur le demi-plan $\mathrm{Im}\, z > 0$, invariante par un sous-groupe de congruence Γ de $\mathrm{PSL}_2(\mathbb{Z})$, et nulle aux "pointes" de Γ (autrement dit une forme modulaire de poids $2m+2$ "parabolique", ou "cuspidale"). Alors le théorème de Deligne [11] (*ex* conjecture de Weil, *alias* hypothèse de Riemann pour les variétés algébriques sur un corps fini), joint à ses résultats antérieurs [10] (ramenant à la conjecture de Weil la conjecture de Ramanujan-Petersson sur l'estimation des coefficients de Fourier des formes modulaires paraboliques de poids entier ≥ 2), fournit l'estimation $|\lambda| \leq 2\sqrt{p}/(p+1)$, et donc $\|T_p\|_{L^2_0(\mathbb{S}^2)} = 2\sqrt{p}/(p+1)$, comme annoncé.

Remarque 4.2. Pour démontrer "seulement" que $\delta(S_p) = \|T_p\|_{L^2_0(\mathbb{S}^2)} < 1$, on n'a pas besoin d'invoquer le résultat monumental de Deligne. Il suffit d'utiliser par exemple les estimations de Rankin [33] pour les coefficients des formes modulaires paraboliques (voir [41],[34]). On obtient alors $\delta(S_p) \leq (p^{4/5} + p^{1/5})/(p+1) < 1$.

4.1. **Le problème de Ruziewicz.** Une conséquence de l'existence de $S \subset \mathrm{SO}(3)$ avec un trou spectral (i.e. $\delta(S) < 1$), est la solution du problème de Ruziewicz (1916) sur la sphère $\mathbb{S}^2$ (voir [37] ou [25] pour une démonstration) :

Corollaire 4.3. *La mesure de Lebesgue est la seule mesure de probabilité finiment additive invariante par rotations sur la tribu de Lebesgue de* $\mathbb{S}^2$.

En fait, ce résultat (ainsi que le cas de $\mathbb{S}^3$) avait déjà été obtenu par Drinfel'd [12], avec une preuve moins "explicite". Le cas de $\mathbb{S}^d$, $d \geq 4$ avait été résolu antérieurement par Margulis et Sullivan [27, 42], au moyen de la propriété (T) de Kazhdan, mais on peut montrer (voir [37]) que l'existence de $S \subset \mathrm{SO}(d+1)$, $d > 2$, possédant un trou spectral se déduit du cas $d = 2$.

La démonstration du corollaire ci-dessus utilise deux ingrédients. Le premier est l'unicité d'une "moyenne invariante" en présence d'un trou spectral :

Théorème 4.4. [35],[24] *Soit* (X,ν) *un espace probabilisé, et* S *un ensemble fini d'automorphismes de* (X,ν)*, invariant par* $s \mapsto s^{-1}$*. Si* $\delta(S) = \|T_S\|_{L^2_0(X,\nu)} < 1$*, si* $M : L^\infty(X,\nu) \to \mathbb{R}$ *est une forme linéaire positive (sur le cône positif) telle que* $M(1) = 1$*, et si* M *est invariante par* S*, alors* M *est l'intégration contre* ν *("*$M = \nu$*").*

(voir aussi [25] pour une démonstration) Le second ingrédient est l'observation (dûe à Tarski) qu'une probabilité P finiment additive invariante par rotations sur la tribu de Lebesgue $\mathcal{L}$ de $\mathbb{S}^2$ (ou $\mathbb{S}^d$, $d \geq 2$), est nécessairement nulle sur les ensembles de mesure de Lebesgue nulle. En effet, l'existence de décompositions paradoxales de $\mathbb{S}^2$ sous $\mathrm{SO}(3)$ (voir [18]) entraîne que toute partie E de $\mathbb{S}^2$ est équivalente (par partition finie et rotations) à une partie E' de diamètre arbitrairement petit. Mais si E est de mesure nulle, toutes ses parties sont mesurables, et donc E' l'est aussi. Or si E' est de diamètre assez petit, elle possède N images deux à deux disjointes par des rotations, donc $P(E) = P(E') \leq 1/N$, et comme N est quelconque $P(E) = 0$.

Pour terminer, on remarque qu'une probabilité finiment additive P sur la tribu des ensembles mesurables d'un espace probabilisé (X,ν), nulle sur les ensembles de ν-mesure nulle, équivaut à la donnée d'une "moyenne" $M : L^\infty(X,\nu) \to \mathbb{R}$. Il suffit de construire (en suivant Lebesgue !) l'intégrale associée à P sur l'espace $\mathcal{L}^\infty(X,\nu)$ des fonctions ν-mesurables bornées, et d'observer que l'hypothèse $\nu(E) = 0 \Rightarrow P(E) = 0$ fait que cette intégrale passe au quotient à l'espace $L^\infty(X,\nu)$ des *classes* de fonctions ν-mesurables bornées.

4.2. **Autres exemples.** Dans [13] est exposée une méthode “élémentaire” pour obtenir dans SU(2) (opérant sur $\mathbb{S}^3$ ou $\mathbb{S}^2 \simeq \mathbb{C}P^1$) des familles avec un trou spectral, dont une infinité (dénombrable) de nouvelles. En particulier la preuve ne fait plus intervenir les formes modulaires.

Soit $p \geq 3$ un nombre premier, et H_p l'ensemble des quaternions entiers sur la sphère de rayon $\sqrt{p}$

$$H_p = \{x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 \mid x_i \in \mathbb{Z}, x_0^2 + x_1^2 + x_2^2 + x_3^2 = p\}.$$

Théorème 4.5. [13] *Soit $\widetilde{S} \subset H_p$ un sous-ensemble de cardinal $|\widetilde{S}| = 2k > 1+p^{4/5}$ invariant par conjugaison, tel que pour tous q, q' distincts dans $\widetilde{S}$, $q'q^{-1}$ n'est aucune des unités $\pm 1, \pm e_i$, $i = 1, 2, 3$. Alors si $S = \{x/|x|, x \in \widetilde{S}\} \subset \mathbb{S}^3 \simeq \mathrm{SU}(2)$, on a $\delta(S) < 1$.*

Le cardinal de H_p étant $8(p+1)$, on voit facilement que S (ou $\widetilde{S}$) est au plus de cardinal $p+1$, et correspond alors aux rotations du théorème 4.1 si $p \equiv 1 (\mathrm{mod}\ 4)$, via le revêtement double $\mathrm{SU}(2) \to \mathrm{SO}(3)$. Le premier cas pour lequel on peut prendre $2k < p+1$ est $p = 7$, pour lequel conviennent les rotations d'angle $\pm \cos^{-1}(1/7)$ autour de trois quelconques des quatre grandes diagonales d'un cube.

Pour démontrer ce théorème, les auteurs étudient le spectre des opérateurs $T_S|_{V_N}$, $N \geq 0$, où V_N est l'espace des polynômes complexes homogènes de degré N en deux variables[7], muni de la norme hilbertienne induite par $L^2(\mathbb{S}^3)$. Ils montrent en fait que

$$(*) \qquad \limsup_{N \to \infty} \|T_S|_{V_N}\| < 1$$

ce qui entraîne $\sup_{N \geq 1} \|T_S|_{V_N}\| < 1$ car aucun V_N, $N \geq 1$ ne contient de vecteur fixe par T_S (ce dernier point résulte de ce que le groupe engendré par S étant libre et non-abélien [9, chap. 2], il est nécessairement dense dans SU(2)). Mais ceci implique que la norme $\delta(S)$ de T_S sur $L_0^2(\mathbb{S}^3)$ est < 1, car cet espace est la somme hilbertienne de copies des représentations V_N, $N \geq 1$. Noter que l'ensemble des rotations dans SO(3) associées aux éléments de S possède *a fortiori* un trou spectral sur $L_0^2(\mathbb{S}^2)$, car cet espace est contenu (comme sous-représentation) dans $L_0^2(\mathbb{S}^3)$: c'est simplement l'espace des fonctions invariantes par l'action scalaire de $U(1) \subset \mathbb{C}^*$, qui commute à celle de SU(2).

Un point important dans la preuve de l'inégalité $(*)$ est une condition “diophantienne” sur les éléments S. Plus précisément, si $S = \{g_1^{\pm 1}, \ldots, g_k^{\pm 1}\}$, on a besoin de savoir que

$$(*_1) \qquad \mathrm{dist}_{\mathrm{SU}(2)}(\omega(g_1, \ldots, g_k), \{\pm 1\}) \geq D^{-n}, \text{ avec } D > 1$$

pour tout n et tout mot réduit $\omega = \omega(X_1, \ldots, X_k)$ de longueur n en les $X_i^{\pm 1}$ tel que $\omega(g_1, \ldots, g_k) \neq \pm 1$. D'après [13], les $(g_1, \ldots, g_k) \in \mathrm{SU}(2)^k$ dont les coordonnées dans $M_2(\mathbb{C}) \simeq \mathbb{C}^4$ sont *algébriques* sont diophantiens, i.e. vérifient cette condition. Cependant ces exemples algébriques ne forment qu'une partie dénombrable dans $\mathrm{SU}(2)^k$, alors que les auteurs posent le

Problème 4.6. [13] Montrer que presque tout $(g_1, \ldots, g_k) \in \mathrm{SU}(2)^k$ est diophantien.

Un premier résultat dans cette direction fait l'objet de [20], dans lequel les auteurs établissent une minoration en D^{-n^2} pour presque tout couple de rotations $(g_1, g_2) \in \mathrm{SO}(3)^2$.

[7] Les V_N constituent la liste des représentations unitaires irréductibles du groupe SU(2), tout comme les espaces propres du laplacien sur $\mathbb{S}^2$ fournissent celles de $\mathrm{SO}(3) = \mathrm{SU}(2)/\{\pm 1\}$, qui ne sont autres que les V_{2N} (cf [21]).

L'autre point crucial dans la preuve de l'inégalité $(*)$ est l'obtention d'une majoration du nombre $M_{n,\alpha}$ de mots réduits ω de longueur $\leq n$ en les $g_i^{\pm 1}$ tels que $\omega(g_1, \ldots, g_k)$ soit dans la boule de rayon $\alpha > 0$ de SU(2) autour de l'élément neutre. Plus précisément, une majoration du type

$$(*_2) \qquad M_{n,\alpha} \leq C_\varepsilon (2k-1)^{n\varepsilon}(1 + (2k-1)^{n\sigma}\alpha^3)$$

pour tout $\varepsilon > 0$, et un $\sigma < 5/4$. Noter que l'ordre de grandeur de $M_{n,\alpha}$ si les $\omega(g_1, \ldots, g_k)$ étaient "idéalement équirépartis" dans SU(2) serait $(2k-1)^n\alpha^3$, et donc l'estimation ci-dessus est raisonnable. Les auteurs l'obtiennent pour les exemples du théorème en se ramenant à une majoration élémentaire du nombre de représentations d'un entier m comme somme de trois carrés, à savoir $r_3(m) \leq A_\varepsilon m^{1/2+\varepsilon}$.

L'obtention d'une inégalité du type $(*_2)$ pour une quantité non dénombrable de $(g_i) \in \mathrm{SU}(2)^k$ reste un problème ouvert et les auteurs posent le

Problème 4.7. [13] Montrer que presque tout $(g_1, ..., g_k) \in \mathrm{SU}(2)^k$ (au sens de la mesure) a un trou spectral.

Références

[1] V. I. Arnol'd, A. L. Krylov, *Uniform distribution of points on a sphere and certain ergodic properties of solutions of linear ordinary differential equations in a complex domain*, Dokl. Akad. Nauk SSSR 148 (1963) 9–12.

[2] H. Auerbach, *Sur le nombre de générateurs d'un groupe linéaire borné*, C. R. Acad. Sci. Paris 197 (1933) 1385–1386.

[3] H. Auerbach, *Sur les groupes linéaires bornés. III.*, Stud. Math. 5 (1935) 43–49.

[4] A. Avez, *Une gnralisation du thorme d'quipartition de Weyl*, Acad. Roy. Belg. Bull. Cl. Sci. (sér. 5) 53 (1967) 1000–1006.

[5] A. Avez, *A generalization of a theorem of Arnold and Krylov,* Notas Ci. Ser. M Mat. 7 (1969), no. 2, 80–87.

[6] A. Borel, *Some remarks about Lie groups transitive on spheres and tori*, Bull. Amer. Math. Soc. 55, (1949) 580–587.

[7] E. Breuillard, T. Gelander, *On dense free subgroups of Lie groups*, J. Algebra 261 (2003), no. 2, 448–467.

[8] Y. Colin de Verdière, *Distribution de points sur une sphère (d'après Lubotzky, Phillips et Sarnak)*, Séminaire Boubaki, Astérisque 177/178, 83–93 (1989)

[9] G. Davidoff, P. Sarnak, A. Valette, " Elementary number theory, group theory, and Ramanujan graphs", London Mathematical Society Student Texts, 55. Cambridge University Press, Cambridge, 2003.

[10] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, Sémin. Bourbaki 1968/69, No.355, Lect. Notes in Math. 179, (1971) 139–172.

[11] P. Deligne, *La conjecture de Weil. I*, Publ. Math. Inst. Hautes Études Sci. No. 43 (1974), 273–307.

[12] V. G. Drinfel'd, *Finitely-additive measures on S^2 and S^3, invariant with respect to rotations.* Functional Anal. Appl. 18 (1984), no. 3, 245–246.

[13] A. Gamburd, D. Jakobson, P. Sarnak, *Spectra of elements in the group ring of* SU(2), J. Eur. Math. Soc. 1 (1999), no. 1, 51–85.

[14] Y. Guivarc'h , *Généralisation d'un théorème de Von Neumann*, C. R. Acad. Sci. Paris Sér. A-B, 268 (1969) A1020–A1023.

[15] A. Haar, *Der Maß begriff in der Theorie der kontinuierlichen Gruppen*, Ann. of Math., 34 (1933) 147–160.

[16] G. H. Hardy, E. M. Wright, "An introduction to the theory of numbers", Oxford University Press, 1979.

[17] P. de la Harpe, "Topics in geometric group theory", Chicago Univ. Press, 2000.

[18] P. de la Harpe, *Mesures finiment additives et paradoxes*, ce volume.
[19] G. Hochschild, "The structure of Lie groups". Holden-Day, 1965.
[20] V. Kaloshin, I. Rodnianski, *Diophantine properties of elements of* SO(3). Geom. Funct. Anal. 11 (2001), no. 5, 953–970.
[21] A. Kirillov, "Éléments de la théorie des représentations", Mir, 1974.
[22] L. Kuipers, H. Niederreiter, "Uniform distribution of sequences". Pure and Applied Mathematics. Wiley-Interscience 1974.
[23] H. Kesten, *Symmetric random walks on groups,* Trans. AMS 92, 336–354 (1959)
[24] V. Losert, H. Rindler, *Almost invariant sets,* Bull. London Math. Soc. 13 (1981), no. 2, 145–148.
[25] A. Lubotzky, "Discrete groups, expanding graphs and invariant measures", Progress in Mathematics 125, Birkhäuser, 1994.
[26] A. Lubotzky, R. Phillips, P. Sarnak, *Hecke operators and distributing points on S^2,* I. Comm. Pure Appl. Math. 39(S), S149–S186 (1986) II. Comm. Pure Appl. Math. 40(4), 401–420 (1987)
[27] G. A. Margulis, *Some remarks on invariant means,* Monatsh. Math. 90 (1980), no. 3, 233–235.
[28] G. A. Margulis, *Finitely-additive invariant measures on Euclidean spaces,* Ergodic Theory Dynam. Systems 2 (1982), no. 3-4, 383–396.
[29] A. Ogg, "Modular forms and Dirichlet series", W. A. Benjamin, 1969.
[30] G. Pisier, *Quadratic forms in unitary operators,* Linear Algebra Appl. 267 (1997), 125–137.
[31] L. Pontrjagin, "Topological Groups". Princeton Mathematical Series v. 2. Princeton University Press, 1939.
[32] U. Porod, S. Zelditch, *Semi-classical limit for random walks.* Trans. Amer. Math. Soc. 352 (2000), no. 11, 5317–5355.
[33] R.A. Rankin, *Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions. II. The order of the Fourier coefficients of integral modular forms.* Proc. Camb. Philos. Soc. 35, (1939) 357–372.
[34] R.A. Rankin, *Fourier coefficients of cusp forms,* Math. Proc. Cambridge Philos. Soc. 100 (1986), no. 1, 5–29.
[35] J. Rosenblatt, *Uniqueness of invariant means for measure-preserving transformations.* Trans. Amer. Math. Soc. 265 (1981), no. 2, 623–636.
[36] P. Sarnak, *Statistical properties of eigenvalues of the Hecke operators*, Analytic number theory and diophantine problems, Proc. Conf., Stillwater/Okla. 1984, Prog. Math. 70, (1987) 321–331.
[37] P. Sarnak, "Some applications of modular forms", Cambridge Univ. Press, 1990.
[38] B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen,* Math. Ann. 116, (1939) 511–523.
[39] B. Schoeneberg, "Elliptic modular functions: an introduction", Grundlehren 203. Springer-Verlag, 1974.
[40] J. Schreier, S. Ulam, *Sur le nombre des générateurs d'un groupe topologique compact et connexe,* Fundam. Math. 24 (1935) 302–304.
[41] A. Selberg, *On the estimation of Fourier coefficients of modular forms.* 1965 Proc. Sympos. Pure Math., Vol. VIII, Amer. Math. Soc. (1965) 1–15.
[42] D. Sullivan, *For $n > 3$ there is only one finitely additive rotationally invariant measure on the n-sphere defined on all Lebesgue measurable subsets.* Bull. Amer. Math. Soc. (N.S.) 4 (1981), no. 1, 121–123.
[43] J. Von Neumann, *Die Einführung analytischer Parameter in topologischen Gruppen*, Ann. of Math. 34 (1933) 170–190.
[44] J. Von Neumann, *Zum Haarschen Maß in topologischen Gruppen*, Compositio Mathematica, 1 (1934) 106–114.
[45] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Ann. 77 (1916) 313–352.
[46] D. Zagier, *Introduction to modular forms,* dans "From number theory to physics", Waldschmidt et al ed., Springer Verlag, 1992.
[47] R. J. Zimmer, "Essential results of functional analysis", Univ. Chicago Press, 1990.