J. Von Neumann (Annals of Math. 1933)
"Zum Haarschen Maß in topologischen Gruppen"

G: groupe topologique compact (métrisable)

$\mathcal{C}(G)_{\mathbb{R}}$: fonctions continues réelles sur G

Opérateurs de translation sur $\mathcal{C}(G)_{\mathbb{R}}$

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

$A = (a_1, \ldots, a_k)$ famille finie dans G

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

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

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

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

Lemme 1. Pour toute $f \in \mathcal{C}(G)_{\mathbb{R}}$, il existe des A_n tels que $T_{A_n} f \to$ constante.

Démonstration.

- $\{T_A f\}_A \subset \mathcal{C}(G)_{\mathbb{R}}$ est équicontinu borné, donc d'adhérence compacte (Ascoli), car f est uniformément continue (et bornée).

- Soit (A_n) telle que

$$\operatorname{osc}(T_{A_n} f) \xrightarrow{n \to \infty} \inf_A \operatorname{osc}(T_A f)$$

Quitte à extraire, $T_{A_n} f \to \varphi$ uniformément.

- Pour toute suite 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 $T_B T_{A_n} = T_{BA_n}$. 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_nB_n.

• Quitte à extraire on peut supposer que $g_n \to g$, et alors $\varphi = \sup\varphi$ sur l'ensemble dense des gb_i, donc φ est constante. cqfd.

Toute constante c limite d'une suite $T_{A_n}f$ est appellée par Von Neumann une *moyenne à droite* de f.

A priori elle n'est pas unique...

Unicité de la moyenne

Astuce : moyenner aussi à gauche.

Opérateurs $\check{T}_A = \frac{1}{k}\sum_1^k \check{T}_{a_i}$ sur $\mathcal{C}(G)_{\mathbb{R}}$, où

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

Lemme 2. Si $T_{A_n} f \to c$ et $\check{T}_{A'_n} f \to c'$ avec c, c' constantes, on a $c = c'$: toute moyenne à gauche coïncide avec toute moyenne à droite.

Démonstration.

Les T_A commutent aux $\check{T}_B$, d'où

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

cqfd.

Théorème. Il existe sur $\mathcal{C}(G)_{\mathbb{R}}$ une unique forme linéaire μ continue invariante à droite ($\mu = \mu \circ T_a$) telle que $\mu(1_G) = 1$.

Elle est aussi invariante à gauche, positive. C'est la *mesure de Haar* (normalisée) de G.

Démonstration.

$\mu(f)$ = moyenne à droite ou à gauche de f.

Il suffit de voir que $\mu(f+f') = \mu(f) + \mu(f')$.

Si $T_{A_n} f \to \mu(f)$, on a $\mu(T_{A_n} f') = \mu(f')$ en voyant $\mu(f')$ comme moyenne à gauche.

Donc il existe des A'_n tels que

$$T_{A'_n} T_{A_n} f' \to \mu(f')$$

Comme $T_{A'_n} T_{A_n} f \to \mu(f)$ aussi,

$$T_{A'_n} T_{A_n} (f + f') \to \mu(f) + \mu(f')$$

cqfd.

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

(séparabilité de $\mathcal{C}(G)_{\mathbb{R}}$ et procédé diagonal)

En particulier

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

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

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

"Les A_n s'équirépartissent selon μ"

Espaces homogènes compacts

G groupe compact (métrisable)
$H \subset G$ sous-groupe fermé
$X = G/H$ espace homogène de G

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

Démonstration (de l'unicité).

- $\{T_A f\}_A$ est relativement compact dans $\mathcal{C}(X)_{\mathbb{R}}$.
- Si $f \in \mathcal{C}(X)_{\mathbb{R}}$, $\inf_A \operatorname{osc}(T_A f) = 0$.
- Toute limite constante $c = \lim T_{A_n} f$ coïncide avec $\nu(f)$ pour toute mesure de probabilité invariante ν sur X. cqfd.

H. Weyl (Math. Ann. 1916) *"Über die Gleichverteilung von Zahlen mod Eins."*

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

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

Le groupe compact est $G = \mathbb{R}/\mathbb{Z}$.
La mesure de Haar est la mesure de Lebesgue.

Weyl utilise la densité des polynômes trigonométriques dans $\mathcal{C}(\mathbb{R}/\mathbb{Z})$.

On peut aussi donner une preuve "à la Von Neumann", qui s'adapte à tout groupe compact (commutatif) ayant un sous-groupe dense à un seul générateur (groupe "monothétique").

V. I. Arnol'd, A. L. Krylov (Doklady 1963)
"Uniform distribution of points on a sphere..."

Deux rotations $a, b \in \mathrm{SO}(3)$

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

$T^n = T_{M_n}$

M_n famille des mots de longueur n en a, b

Théorème. Si pour un $x \in \mathbb{S}^2$, $\bigcup_n M_n \cdot x$ est dense dans $\mathbb{S}^2$, on a $T^n f \to \int f \, d\nu$ pour toute $f \in \mathcal{C}(\mathbb{S}^2)$.

Autrement dit, pout tout $x \in \mathbb{S}^2$, la suite des $M_n \cdot x$ s'équirépartit selon la probabilité uniforme ν sur $\mathbb{S}^2$.

Y. Guivarc'h (C. R. Acad. Sc. Paris 1969)
"Généralisation d'un théorème de Von Neumann"

Un espace métrique compact X.

Deux isométries a, b de X, et $\Gamma \subset \mathrm{Isom}(X)$ le sous-groupe qu'elles engendrent.

Le sous-groupe $\Gamma_0 \subset \Gamma$ des $\prod a^{m_i} b^{n_i}$ tels que $\sum (m_i + n_i) = 0$.

Théorème. Si Γ_0 a une orbite dense dans X

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

Démonstration.

Il suffit de voir que $T^n f \to \text{const}$ pour toute $f \in \mathcal{C}(X)_{\mathbb{R}}$, avec $T = 1/2(T_a + T_b)$.

L'ensemble des $T^n f$ est relativement compact dans $\mathcal{C}(X)_{\mathbb{R}}$.

Soit $\varphi = \lim_k T^{n_k} f$ une valeur d'adhérence, $n_{k+1} > n_k$.

$T : L^2(X, \nu) \to L^2(X, \nu)$ est continu, de norme ≤ 1 (T_a, T_b sont des isométries).

Comme l'inclusion $\mathcal{C}(X) \hookrightarrow L^2(X, \nu)$ est 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-à-d

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

Conclusion : $T_a\varphi = T_b\varphi$.

De même $T_s\varphi = T_{s'}\varphi$ si $s, s' \in M_n$, donc φ est invariante par $s's^{-1}$.

On en déduit que φ est invariante par Γ_0 (donc constante) grâce au

Lemme. Γ_0 est contenu dans l'adhérence de $\bigcup_n M_n M_n^{-1}$ (et Γ dans celle de $\bigcup_n M_n$).

Il existe des suites p_k, q_k tendant vers $+\infty$ telles que $a^{p_k} \to 1$, $b^{q_k} \to 1$. Soit $\gamma \in \Gamma$

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

avec $\sum(m_i + n_i) = 0$ si $\gamma \in \Gamma_0$. Alors

$$\gamma = \lim_k a^{m_1 + p_k} b^{n_1 + q_k} \ldots (a^{p_k} b^{q_k} \ldots)^{-1}$$

où $a^{m_1+p_k} b^{n_1+q_k} \ldots$, $a^{p_k} b^{q_k} \ldots$ sont des mots positifs pour k assez grand, et de même longueur si $\sum(m_i + n_i) = 0$. cqfd.

Pour en déduire le résultat d'Arnol'd et Krylov, on peut remarquer l'équivalence de

- $M = \bigcup M_n$ a une orbite dense dans X
- $\overline{M} = \overline{\Gamma}$ est transitif sur X

Or

- Le seul sous-groupe fermé de $\mathrm{SO}(3)$ transitif sur $X = \mathbb{S}^2$ est $\mathrm{SO}(3)$ donc $\overline{\Gamma} = \mathrm{SO}(3)$.

- $[\Gamma, \Gamma] \subset \Gamma_0$.
- $[\overline{\Gamma}, \overline{\Gamma}] \subset \overline{[\Gamma, \Gamma]}$.

On conclut car $\overline{\Gamma} = \mathrm{SO}(3)$ est égal à son sous-groupe dérivé.

Un autre résultat d'équirépartition

Un espace métrique compact homogène X.

Deux isométries a, b de X, et $\Gamma \subset \mathrm{Isom}(X)$ le sous-groupe qu'elles engendrent.

Le sous-groupe $\Gamma^2 \subset \Gamma$ engendré par les carrés.

Σ_n la famille des mots réduits de longueur n en $a^{\pm 1}$, $b^{\pm 1}$ (4.3^{n-1} mots).

Théorème. (Arnol'd-Krylov, Guivarc'h)
Si Γ^2 a une orbite dense dans X, pour tout $x \in X$ les $\Sigma_n \cdot x$ s'équirépartissent selon l'unique probabilité invariante par isométries sur X.

Remarque : $\Gamma^2 \supset [\Gamma, \Gamma]$.

Esquisse de démonstration.

Étude des opérateurs auto-adjoints

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

Ils vérifient $S_1 S_n = 3/4\, S_{n+1} + 1/4\, S_{n-1}$, donc

$$S_n = P_n(S_1)$$

avec $P_n(t)$ des polynômes vérifiant

$|P_n(t)| \leq 1$ si $|t| \leq 1$, $|P_n(t)| < 1$ si $|t| < 1$.

On en déduit $S_n \varphi \to 0$ dans $L^2(X, \nu)$ pour toute φ orthogonale à $\ker(S_1 \pm 1)$, grâce au théorème de décomposition spectrale et à la convergence dominée.

L'hypothèse sur Γ^2 force $\ker(S_1 + 1) = 0$, et on conclut que $S_n f \to \nu(f)$ pour toute $f \in \mathcal{C}(X)$.

Sous-groupes denses à deux générateurs dans $\mathbf{SO}(3)$

Proposition. Pour presque tout couple (a, b) de rotations, le sous-groupe engendré par a, b est dense dans $\mathrm{SO}(3)$.

Démonstration.

- Si a est d'angle irrationnel, $\overline{\{a^n\}}$ est le sous-groupe des rotations de même axe que a.

- Deux tels sous-groupes d'axes distincts engendrent $\mathrm{SO}(3)$.

Remarque : Tout groupe de Lie compact connexe G admet un sous-groupe dense à deux générateurs (Auerbach 1935).

Vitesse d'équirépartition

$A = (a_1, ..., a_k)$ famille finie dans SO(3)

$T = \frac{1}{2k}\sum_{i=1}^{k}(T_{a_i} + T_{a_i}^{-1})$ opérant sur $L^2(\mathbb{S}^2)$

$L_0^2(\mathbb{S}^2) =$ fonctions L^2 de moyenne nulle

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

- La "propriété de trou spectral" $\delta(A) < 1$ entraîne $T^n f \to \int_{\mathbb{S}^2} f$ et $S_n f \to \int_{\mathbb{S}^2} f$ exponentiellement vite en norme L^2 pour toute $f \in L^2(\mathbb{S}^2)$, avec $S_n f =$ moyenne des $T_s f$, s mot réduit de longueur n en les $a_i^{\pm 1}$.

- Si f est assez régulière (par ex. $f \in \mathcal{C}^2$) la même chose est vraie en norme uniforme.

Nombreuses autres "discrépances"...

V. Drinfel'd (Funct. Anal. Appl. 1984)
A. Lubotzky, R. Phillips, P. Sarnak (CPAM 1986,1987)

Théorème. Si k est impair et $p = 2k - 1$ premier, il existe k rotations $a_1, ..., a_k$ telles que $\delta(a_1, ..., a_k) = \sqrt{2k-1}/k < 1$.

Les a_i construites sont les rotations associées aux quaternions entiers à partie réelle > 0 impaire sur la sphère de rayon $\sqrt{p}$.

$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p$ possède $p+1$ solutions entières avec $x_0 > 0$ impair (Jacobi 19^e s).

Si $k = 3$, on trouve les rotations d'angle $\cos^{-1}(-3/5)$ autour des trois axes de coordonnées, associées aux quaternions $1 + 2e_i$, $i = 1, 2, 3$.

Remarques

- Arithmétique, géométrie algébrique et analyse difficiles... (Conjectures de Weil, Deligne 1974).

- La borne est optimale : $\delta \geq \sqrt{2k-1}/k$ dans tous les cas, et l'égalité entraîne que le groupe engendré est libre (Kesten 1959).

- $\delta(a_1, ..., a_k) < 1$ plus accessible (Drinfeld, Sarnak).

- Résolution du problème de Ruziewicz (1916) pour $\mathbb{S}^2$ (et $\mathbb{S}^3$) : la mesure de Lebesgue est la seule mesure *finiment additive* invariante par rotations sur la tribu de Lebesgue de $\mathbb{S}^2$. Le cas de $\mathbb{S}^d$, $d \geq 4$ avait été résolu par G. Margulis et D. Sullivan (1980).

- Nombre dénombrable d'exemples de $\delta < 1$ ("arithmétiques").

A. Gamburd, D. Jakobson, P. Sarnak
(J. Eur. Math. Soc. 1999)
Spectra of elements in the group ring of $SU(2)$

• Méthode "élémentaire" pour obtenir des familles de rotations avec $\delta < 1$, dont certaines nouvelles.

Exemple : rotations d'angle $\cos^{-1}(1/7)$ autour de trois des quatre grandes diagonales d'un cube.

• Les exemples obtenus forment encore une famille dénombrable.

Problème (GJS) : montrer que presque tout $(a_1, ..., a_k) \in \mathrm{SO}(3)^k$ a un trou spectral.

Approximation diophantienne dans $\mathbf{SO}(3)$

$(a_1, ..., a_k) \in \mathrm{SO}(3)^k$ *diophantien* si

$$|R_n(a_1, ..., a_k) - 1| \geq D^{-n}$$

pour un $D = D(a_1, ..., a_k) > 0$ et tout mot réduit R_n de longueur n en les $a_i^{\pm 1}$ tel que $R_n(a_1, ..., a_k) \neq 1$.

- C'est vrai si les a_i sont à coefficients algébriques.

- Les k-uplets non-diophantiens forment un G_δ dense.

Problème (GJS) : montrer que presque tout $(a_1, ..., a_k) \in \mathrm{SO}(3)^k$ est diophantien ($k \geq 2$).

V. Kaloshin, I. Rodnianski (preprint 2000) obtiennent $|R_n(a_1, a_2) - 1| \geq D^{-n^2}$ pour presque tout (a_1, a_2).