Marches aléatoires dans les groupes de Lie

Nicolas de Saxcé

24 mars 2023

Table des matières

Chapitre 1

Équidistribution dans les groupes compacts

Dans tout ce chapitre, on note G un groupe topologique compact. Étant donnée une mesure de probabilité μ borélienne sur G, on considère une suite de variables aléatoires $(g_i)_{i\in\mathbb{N}^*}$ indépendantes, identiquement distribuées suivant la loi μ, et on s'intéresse à la marche aléatoire associée, définie par

$$\begin{cases} x_0 = 1 \\ \forall n \geq 1,\ x_n = g_n x_{n-1} = g_n g_{n-1} \cdots g_1. \end{cases} \tag{1.1}$$

Nous montrerons dans un premier temps que, sous certaines hypothèses naturelles sur μ, la marche (x_n) converge en loi vers la probabilité de Haar, unique mesure de probabilité invariante par multiplication à gauche et à droite par les éléments de G, puis nous tâcherons de comprendre à quelle vitesse cette convergence a lieu.

1.1 Une construction de la mesure de Haar

Nous ferons dans la suite deux hypothèses sur la probabilité μ.

Définition 1.1. Une mesure borélienne μ sur un groupe topologique G est dite *adaptée* lorsque son support engendre un sous-groupe dense dans G. Elle est dite *apériodique* lorsque son support n'est pas contenu dans une classe à gauche d'un sous-groupe strict fermé et distingué.

Naturellement, nous dirons que la marche aléatoire définie en (1.1) ci-dessus est adaptée, ou apériodique, si la mesure μ l'est.

Exercice 1. Donner un exemple de mesure apériodique non adaptée, puis un exemple de mesure adaptée mais non apériodique.

Exercice 2. Soit μ une mesure adaptée sur un groupe G compact. Montrer que le semi-groupe engendré par le support de μ est dense dans G ; on dit que μ est *irréductible*. Cette propriété est-elle valable lorsque G n'est pas compact ?

Exercice 3. On dit qu'une mesure sur G est symétrique si elle est invariante par l'application $g \mapsto g^{-1}$. Montrer que toute mesure symétrique adaptée sur un groupe connexe est apériodique. Que peut-on dire si G n'est pas connexe ?

Le but de cette partie est de démontrer le théorème suivant, qui montre à la fois l'existence et l'unicité de la mesure de Haar sur un groupe compact G, et la convergence en loi des marches aléatoires adaptées apériodiques.

Théorème 1.2 (Existence et unicité de la mesure de Haar)**.** *Soit G un groupe compact. Il existe une unique probabilité m sur G telle que pour toute probabilité μ adaptée et apériodique sur G, la marche aléatoire (x_n) associée converge en loi vers m. Cette mesure m est invariante à gauche et à droite par G.*

Exercice 4. Soit G un groupe topologique compact. Vérifier que m est l'unique probabilité borélienne sur G invariante à gauche.

Étant données deux parties A et B d'un groupe G, nous noterons

$$AB = \{x = ab \ ; \ a \in A, \, b \in B\}.$$

De même, si S est une partie de G et $n \in \mathbb{N}^*$, nous noterons S^n l'ensemble des éléments de G qui peuvent s'écrire comme produit de n éléments de S :

$$S^n = \{x = s_1 s_2 \dots s_n \ ; \ s_i \in S\}.$$

Une partie S d'un groupe topologique est dite *topologiquement génératrice* si le sous-groupe engendré par S est dense dans G.

Proposition 1.3. *Soit G un groupe topologique compact, et S une partie topologiquement génératrice de G qui n'est pas incluse dans une classe à gauche d'un sous-groupe strict fermé distingué. Pour tout ouvert non vide $U \subset G$, il existe un entier n_0 tel que*

$$\forall n \geq n_0, \quad S^n U = G.$$

Démonstration. Fixons un élément $s \in S$. La suite de parties $(s^{-n} S^n)_{n \geq 1}$ est croissante. Notons

$$H = \overline{\bigcup_{n \geq 1} s^{-n} S^n}$$

et montrons que $H = G$.

Si $x, y \in H$, on veut voir que $xy \in H$, i.e. que pour tout voisinage U de l'identité dans G, xyU rencontre $s^{-n} S^n$ pour un certain n. Pour cela, on choisit un voisinage distingué symétrique V de l'identité tel que $V^6 \subset U$. Comme $x, y \in H$, pour tout n assez grand, $x, y \in s^{-n} S^n V$. On peut alors choisir n de sorte que $s^{-n} \in V$, ce qui donne $x, y \in V S^n V = S^n V^2$, et par suite,

$$xy \in S^n V^2 S^n V^2 = S^{2n} V^4 \subset s^{-2n} S^{2n} V^6 \subset s^{-2n} S^{2n} U.$$

Ainsi, H est un sous-semi-groupe compact de G, et donc un sous-groupe. De plus, H est normalisé par s, et donc par sH. Mais $S \subset sH$, donc le groupe H est normalisé par S, et comme S engendre un sous-groupe dense de G, H est distingué dans G. Comme $S \subset sH$, notre hypothèse sur S implique $H = G$.

Par conséquent, si U est un ouvert non vide, $G = \bigcup_{n \geq 1} s^{-n} S^n U$, et par compacité de G, il existe n_0 tel que pour tout $n \geq n_0$, $G = s^{-n} S^n U$, ce qui implique $G = S^n U$. □

Exercice 5. Soit G un groupe compact, et U un voisinage de l'identité dans G. Vérifier les points suivants, utilisés dans la démonstration ci-dessus.

1. Il existe un voisinage de l'identité distingué V inclus dans U.
2. Si $s \in G$, il existe n arbitrairement grand tel que $s^n \in U$.
3. Un sous-semi-groupe fermé d'un groupe compact est un groupe.
4. Donner un exemple d'un semi-groupe compact qui n'est pas un groupe.

Définition 1.4. Si μ et ν sont deux mesures boréliennes sur G, leur *produit de convolution* $\mu * \nu$ est l'image de la mesure produit $\mu \otimes \nu$ sur $G \times G$ par l'application $(x, y) \mapsto xy$. En d'autres termes, pour toute fonction $\phi \in C(G)$,

$$\int_G \phi(z)(\mu * \nu)(\mathrm{d}z) = \iint_{G\times G} \phi(xy)\mu(\mathrm{d}x)\nu(\mathrm{d}y).$$

Notons que pour $n \in \mathbb{N}^*$, la puissance de convolution $\mu^{*n} = \overbrace{\mu * \cdots * \mu}^{n \text{ fois}}$ est la loi au temps n de la marche aléatoire (x_n) associée à μ, de sorte que le théorème 1.2 est équivalent au fait que pour toute mesure μ apériodique et adaptée sur un groupe compact G, la suite des puissances de convolution $(\mu^{*n})_{n\geq 1}$ converge faiblement vers la mesure de probabilité m sur G.

Si μ est une mesure borélienne sur G et $f \in C(G)$, nous noterons $\mu * f$ et $f * \mu$ les convolutions de f par μ à gauche et à droite, respectivement, définies par

$$\mu * f(x) = \int_G f(g^{-1}x)\mu(\mathrm{d}g) \quad \text{et} \quad f * \mu(x) = \int_G f(xg)\mu(\mathrm{d}g).$$

Notre démonstration du théorème 1.2 s'inspire de la construction par Von Neumann de la mesure de Haar sur les groupes compacts, mais nous utiliserons des opérateurs de convolution sur $C(G)$ plutôt que des opérateurs de moyennes de translations.

Démonstration du théorème 1.2. Soit μ une probabilité adaptée et apériodique μ sur G et

$$\begin{array}{rccc} T_\mu : & C(G) & \to & C(G) \\ & f & \mapsto & \mu * f \end{array}$$

l'opérateur de convolution à gauche associé. Fixons aussi un élément f quelconque dans $C(G)$.

Observation 1 : Toute valeur d'adhérence de $(T_\mu^n f)$ est constante.
Supposons qu'une sous-suite $(T_\mu^{n_k} f)$ converge uniformément vers $\varphi \in C(G)$. Comme la suite $(\sup T_\mu^n f)$ est décroissante, elle converge, et

$$\sup \varphi = \inf_{n\geq 0} \sup T_\mu^n f.$$

Par conséquent, pour tout $r \geq 1$, $\sup T_\mu^r \varphi = \lim_{k\to\infty} \sup T_\mu^{n_k+r} f \geq \sup \varphi$ et donc $\sup T_\mu^r \varphi = \sup \varphi$. Soit maintenant x_0 tel que

$$T_\mu^r \varphi(x_0) = \int \varphi(g^{-1}x_0)\mu^{*r}(\mathrm{d}g) = \sup T_\mu^r \varphi.$$

Comme $\sup T_\mu^r \varphi = \sup \varphi$, cette égalité implique que pour presque tout g au sens de la mesure μ^{*r}, et donc pour tout g dans le support de μ^{*r}, $\varphi(g^{-1}x_0) = \sup \varphi$. Mais d'après la proposition 1.3, le support de μ^{*r} converge vers G lorsque r tend vers l'infini, et par continuité, φ est donc constante.

Observation 2 : La suite $(T_\mu^n f)$ n'admet qu'une seule valeur d'adhérence.
L'astuce consiste à étudier aussi un opérateur de convolution à droite. Soit ν une autre probabilité borélienne adaptée apériodique sur G, et $\check{T}_\nu : f \mapsto f * \nu$ l'opérateur de convolution *à droite* par ν. Si c et c' sont des valeurs d'adhérence (constantes) des suites $(T_\mu^n f)$ et $(\check{T}_\nu^n f)$, respectivement, alors $c = c'$. En effet, comme les opérateurs T_μ et $\check{T}_\nu$ sont de norme 1, commutent, et préservent les constantes,

$$c \leftarrow \check{T}_\nu^{n_k} T_\mu^{m_k} f = T_\mu^{m_k} \check{T}_\nu^{n_k} f \to c'.$$

Cet argument montre en outre que l'unique valeur d'adhérence de $(T_\mu^n f)$ ne dépend pas de la probabilité adaptée et apériodique μ, on la note $m(f)$.

La suite $(T_\mu^n f)$ est équicontinue et admet $m(f)$ comme unique valeur d'adhérence dans $C(G)$, donc, d'après le théorème d'Ascoli, elle converge uniformément vers cette valeur d'adhérence :

$$\lim T_\mu^n f = m(f).$$

D'après le théorème de Riesz, la forme linéaire positive $f \mapsto m(f)$ sur $C(G)$ correspond à une unique mesure de Radon. Bien sûr, $m(G) = \lim T_\mu^n 1 = 1$ donc m est une mesure de probabilité sur G. Enfin, pour tout $a \in G$, notant $(af)(x) = f(xa)$,

$$m(af) = m(\check{T}_{\delta_a} f) = \lim T_\mu^n \check{T}_{\delta_a} f = \lim \check{T}_{\delta_a} T_\mu^n f = \check{T}_{\delta_a} m(f) = m(f).$$

De même, en utilisant les opérateurs $\check{T}_\nu^n$ on montre que pour tout b dans G, $m(fb) = m(f)$, si $(fb)(x) = f(bx)$. Ainsi, la mesure m est bien invariante à gauche et à droite par G. □

Exercice 6. Soit G un groupe compact et μ une probabilité adaptée sur G, mais non nécessairement apériodique. À l'aide des méthodes utilisées dans la démonstration ci-dessus, montrer que la suite $(\frac{1}{n}\sum_{k=1}^n \mu^{*k})_{n\geq 1}$ converge faiblement vers m.

Exercice 7. Dans la démonstration ci-dessus, nous avons implicitement admis l'existence d'une mesure adaptée apériodique sur G, ce qui n'est pas un résultat évident a priori.

1. La *cellularité*[1] d'un espace topologique X, notée $c(X)$, est le cardinal maximal d'une famille d'ouverts disjoints de X.
   (a) Construire un espace X compact dont la cellularité est non dénombrable : $c(X) > \aleph_0$.
   (b) Si $c(X) > \aleph_0$, montrer que pour toute probabilité borélienne sur X, il existe un ouvert U non vide tel que $\mu(U) = 0$.
   (c) En déduire que si G est un groupe compact, alors $c(G) \leq \aleph_0$.
2. Montrer que si le groupe compact G est métrique, il existe une probabilité adaptée apériodique sur G.
3. On considère maintenant un groupe compact non nécessairement séparable.

1. Nous remercions Pierre Petit pour ses explications sur cette notion et les liens avec l'inexistence de mesures de probabilités à support total.

(a) Pour $f \in C(G)$, on note $\alpha_f = \inf\{\sup T_\mu f \ ; \ \mu \text{ probabilité borélienne sur } G\}$. Montrer que si (μ_n) est une suite de probabilités telle que $\alpha_f = \lim_n \sup T_{\mu_n} f$, alors toute valeur d'adhérence de $(T_{\mu_n} f)$ est constante, égale à α_f.

(b) Montrer qu'on a aussi $\alpha_f = \inf\{\sup \check{T}_\nu f \ ; \ \nu \text{ probabilité borélienne sur } G\}$. En déduire que l'application $m : f \mapsto \alpha_f$ définit une probabilité borélienne sur G invariante à droite et à gauche.

1.2 Analyse harmonique sur les groupes compacts

Nous rappelons dans cette partie les résultats fondamentaux de l'analyse harmonique sur les groupes compacts. Admettant l'existence de la mesure de Haar, cela nous donnera en particulier une deuxième démonstration de la convergence en loi des marches aléatoires sur G.

Définition 1.5. Une *représentation unitaire* d'un groupe topologique G est un morphisme continu $\rho : G \to U(V)$, où V est un espace de Hilbert, et $U(V)$ l'espace des opérateurs unitaires sur V, muni de la norme d'opérateur. La représentation ρ est dite *irréductible* si $\{0\}$ et V sont les seuls sous-espaces fermés invariants de V.

Notations. Dans ce cours, un espace de Hilbert V sera toujours muni d'un produit hermitien $\langle \cdot, \cdot \rangle$ linéaire par rapport à la seconde variable, et anti-linéaire par rapport à la première. En d'autres termes, pour $x, y \in V$ et $\lambda \in \mathbb{C}$, $\langle x, \lambda y \rangle = \lambda \langle x, y \rangle$ mais $\langle \lambda x, y \rangle = \bar{\lambda} \langle x, y \rangle$, où $\bar{\lambda}$ désigne le conjugué de λ dans $\mathbb{C}$. Si A est un endomorphisme de V, on note A^* l'adjoint de A, i.e. l'unique élément de $\operatorname{End} V$ qui satisfait, pour tous $x, y \in V$, $\langle x, Ay \rangle = \langle A^* x, y \rangle$.

Remarque. Pour insister sur le fait qu'on ne considère que les sous-espaces fermés, on parle parfois de représentation *topologiquement* irréductible. Par exemple, l'action de $SL_2(\mathbb{C})$ sur $L^2(\mathbb{C})$ est topologiquement irréductible (cf. Knapp, *Representation theory of semisimple Lie groups*, page 33), mais n'est pas algébriquement irréductible, puisque les fonctions C^∞ forment un sous-espace invariant dense.

Exercice 8. Donner un exemple de représentation unitaire d'un groupe topologique qui ne se décompose pas en somme directe hilbertienne de représentations irréductibles.

Définition 1.6. Si G est un groupe compact, nous noterons $\hat{G}$ le *dual unitaire* de G, c'est-à-dire l'ensemble des représentations irréductibles unitaires de G, à isomorphisme près.

Exercice 9. Soit $G = \mathbb{T} = \mathbb{R}/\mathbb{Z}$ le tore de dimension 1. Montrer que $\hat{G}$ s'identifie à $\mathbb{Z}$.

Comme dans le cas du tore $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, nous allons définir pour un groupe compact G quelconque la série de Fourier d'une fonction $f \in L^1(G)$. Cela nous permettra d'analyser ensuite la structure de l'algèbre $L^2(G)$ et de montrer des analogues des théorèmes classiques : Weierstrass trigonométrique, formule de Plancherel, ...etc.

Définition 1.7. Pour $\rho \in \hat{G}$, on définit le *sous-espace de coefficients* $\mathcal{H}_\rho < L^2(G)$ par

$$\mathcal{H}_\rho = \mathrm{Vect}\{g \mapsto \langle u, \rho(g)v\rangle;\ u, v \in V_\rho\}.$$

Notons que $\mathcal{H}_\rho$ est stable par l'action régulière de G à gauche et à droite sur $L^2(G)$, puisque l'on peut écrire $\langle u, \rho(h_1)\rho(g)\rho(h_2)v\rangle = \langle u', \rho(g)v'\rangle$ avec $u' = \rho(h_1)^* u$ et $v' = \rho(h_2)v$. Le théorème suivant est une généralisation du théorème de Weierstrass trigonométrique.

Théorème 1.8 (Péter-Weyl)**.** *Soit G un groupe compact. L'espace $L^2(G)$ se décompose en somme directe hilbertienne orthogonale*

$$L^2(G) = \bigoplus_{\rho \in \hat{G}} \mathcal{H}_\rho.$$

C'est à partir de ce résultat que nous montrerons les propriétés importantes de la transformée de Fourier sur les groupes compacts, dont nous rappelons maintenant la définition.

Définition 1.9 (Transformée de Fourier)**.** Pour $f \in L^1(G)$ et $\rho \in \hat{G}$, on note $\hat{f}(\rho) = \int_G f(g)\rho(g)^* \,\mathrm{d}g$. La *transformée de Fourier* sur le groupe compact G est l'application

$$\begin{array}{ccc} L^1(G) & \to & \bigoplus_{\rho\in\hat{G}} \mathrm{End}\, V_\rho \\ f & \mapsto & (\hat{f}(\rho))_{\rho\in\hat{G}} \end{array}$$

Le produit de convolution sur $L^1(G)$, défini par

$$f_1 * f_2(x) = \int_G f_1(g) f_2(g^{-1}x)\,\mathrm{d}g,$$

permet de munir les espaces $L^1(G)$, $L^2(G)$ et $C(G)$ de structures d'algèbres. On laisse au lecteur le soin de vérifier que la transformée de Fourier est un morphisme d'algèbres, i.e.

$$\forall f_1, f_2, \quad \widehat{f_1 * f_2}(\rho) = \widehat{f}_1(\rho)\widehat{f}_2(\rho).$$

Théorème 1.10 (Isomorphisme de Fourier)**.** *Si chaque $\mathrm{End}\, V_\rho$ est muni de la norme de Hilbert Schmidt définie par $\|A\|_{HS} = \mathrm{Tr}(A^*A)^{\frac{1}{2}}$, l'application*

$$f \mapsto \left((\dim V_\rho)^{\frac{1}{2}} \hat{f}(\rho)\right)_{\rho\in\hat{G}}$$

induit une isométrie $L^2(G) \simeq \bigoplus_{\rho\in\hat{G}} \mathrm{End}\, V_\rho$ (somme hilbertienne).

Comme corollaires de ce théorème, on obtient des généralisations des formules bien connues de l'analyse de Fourier sur le cercle.

Formule de Parseval

$$\forall f \in L^2(G), \quad \|f\|_2^2 = \sum_{\rho\in\hat{G}} (\dim V_\rho)\|\hat{f}(\rho)\|_{HS}^2$$

Formule de Plancherel

$$\forall f \in C^\infty(G), \forall x \in G, \quad f(x) = \sum_{\rho\in\hat{G}} (\dim V_\rho)\,\mathrm{Tr}(\hat{f}(\rho)\rho(x))$$

Le restant de cette partie est consacré à la démonstration de ces résultats fondamentaux, qui nous permettront de retrouver – en admettant l'existence de la mesure de Haar – l'équidistribution des marches aléatoires sur les groupes compacts.

Lemme 1.11 (Lemme de Schur)**.** *Soit G un groupe topologique et V_1, V_2 deux représentations unitaires irréductibles de G. Si $A : V_1 \to V_2$ est un opérateur linéaire tel que pour tout $g \in G$, $\rho_2(g)A = A\rho_1(g)$, alors*

1. *Si $V_1 \not\sim V_2$ (comme représentations de G), alors $A = 0$.*
2. *Si $V_1 = V_2$, alors il existe $\lambda \in \mathbb{C}$ tel que $A = \lambda \operatorname{Id}$.*

Démonstration. Les sous-espaces fermés $\ker A$ et $\overline{\operatorname{im} A}$ sont stables par l'action de G, donc égaux à $\{0\}$ ou à l'espace tout entier, par irréductibilité. Cela montre la première partie.

Pour la deuxième partie, on remarque que A commute à tous les opérateurs $\rho(g)$, $g \in G$, et comme ρ est unitaire, il en est de même pour l'opérateur adjoint A^*. Par suite, les opérateurs auto-adjoints $L = \frac{A+A^*}{2}$ et $M = \frac{A-A^*}{2i}$ commutent à l'action de G. D'après le théorème spectral, tout projecteur spectral $E : V \to V$ associé à L ou M commute à l'action de G, et son noyau est donc un sous-espace fermé stable par G, égal à $\{0\}$ ou V, par irréductibilité. Par conséquent L et M n'ont chacun qu'une unique valeur spectrale : pour certains $x, y \in C$, $L = x$, $M = y$, et donc $A = \lambda \operatorname{Id}$, avec $\lambda = x + iy$. □

Proposition 1.12. *Soit G un groupe compact. Toute représentation unitaire irréductible de G est de dimension finie.*

Démonstration. Soit v un vecteur unitaire dans V. L'opérateur

$$A_v \colon u \mapsto \int_G \langle gv, u\rangle gv \,\mathrm{d}g$$

commute à l'action de G donc $A_v = \lambda_v \operatorname{Id}$ d'après le lemme de Schur. De plus, pour u unitaire, $\lambda_v = \langle u, A_v u\rangle = \int_G |\langle gv, u\rangle|^2 \,\mathrm{d}g = \lambda_u$, donc il existe λ tel que $\forall v$, $\lambda_v = \lambda$. En outre, $\lambda = \langle v, A_v v\rangle = \int_G |\langle gv, v\rangle|^2 \,\mathrm{d}g > 0$.

Soit $u_1, \ldots, u_n$ une famille orthonormée dans V. Pour chaque k,

$$\int_G |\langle gu_1, u_k\rangle|^2 \,\mathrm{d}g = \lambda$$

et donc

$$\begin{aligned} n\lambda &= \sum_{k=1}^{n} \int_G |\langle gu_1, u_k\rangle|^2 \,\mathrm{d}g \\ &= \int_G \sum_{k=1}^{n} |\langle gu_1, u_k\rangle|^2 \,\mathrm{d}g \\ &\leq \int_G \|gu_1\|^2 \,\mathrm{d}g = \int_G \|u_1\|^2 \,\mathrm{d}g = 1. \end{aligned}$$

Cela montre que $n \leq \frac{1}{\lambda}$, et donc que V est de dimension finie. □

Exercice 10. Montrer que l'orbite d'un vecteur sous l'action d'un groupe compact peut engendrer un espace de dimension infinie.

Dans la suite, le groupe compact G est toujours muni de la probabilité de Haar, et l'espace $L^2(G)$ du produit scalaire associé.

Proposition 1.13 (Orthogonalité des coefficients)**.** *Soit G un groupe compact, et $\rho_1 : G \to \mathrm{GL}(V_1)$ et $\rho_2 : G \to \mathrm{GL}(V_2)$ deux représentations irréductibles de G. Pour $u_1, v_1 \in V_1$ et $u_2, v_2 \in V_2$,*

$$I_{u_1,v_1,u_2,v_2} = \int_G \langle u_1, \rho(g)v_1\rangle\overline{\langle u_2, \rho(g)v_2\rangle}\mathrm{d}g = \begin{cases} 0 & si\ \rho_1 \not\sim \rho_2 \\ \frac{\langle u_1,u_2\rangle\overline{\langle v_1,v_2\rangle}}{\dim V_1} & si\ \rho_1 = \rho_2. \end{cases}$$

Démonstration. Pour u dans un espace de Hilbert V, on note u^* la forme linéaire $v \mapsto (u, v)$. Cela permet de calculer les produits hermitiens avec la notation matricielle $(u, v) = u^*v$. Ensuite, calculons,

$$\begin{aligned}\int_G \langle u_1, \rho_1(g)v_1\rangle\overline{\langle u_2, \rho_2(g)v_2\rangle}\,\mathrm{d}g &= \int_G \langle u_1, \rho_1(g)v_1\rangle\langle \rho_2(g)v_2, u_2\rangle\mathrm{d}g \\ &= \int_G u_1^*\rho_1(g)v_1v_2^*\rho_2(g)^*u_2\mathrm{d}g \\ &= u_1^*\underbrace{\left(\int_G \rho_1(g)v_1v_2^*\rho_2(g)^{-1}\mathrm{d}g\right)}_{A}u_2\end{aligned}$$

L'opérateur $A \in \mathrm{Hom}(V_1, V_2)$ vérifie les hypothèses du lemme 1.11, donc

$$A = \begin{cases} 0 & \text{si } \rho_1 \not\sim \rho_2 \\ \frac{\mathrm{Tr}\,A}{\dim V_1}\,\mathrm{Id} & \text{si } \rho_1 = \rho_2. \end{cases}$$

Cela montre déjà le résultat si $\rho_1 \not\sim \rho_2$, et si $\rho_1 = \rho_2$, comme $\mathrm{Tr}(v_1v_2^*) = \overline{\langle v_1, v_2\rangle}$, on trouve bien

$$I_{u_1,v_1,u_2,v_2} = \langle u_1, u_2\rangle\frac{\mathrm{Tr}\,v_1v_2^*}{\dim V_1} = \frac{\langle u_1, u_2\rangle\overline{\langle v_1, v_2\rangle}}{\dim V_1}.$$

□

Exercice 11. Si V est un espace de Hilbert, on définit un produit hermitien sur $\mathrm{End}\,V$ par $\langle A, B\rangle = \mathrm{Tr}\,A^*B$.

1. Montrer que $\mathcal{H}_\rho = \{g \mapsto \langle A, \rho(g)\rangle\ ;\ A \in \mathrm{End}\,V_\rho\}$.
2. Montrer que sous les hypothèses de la proposition ci-dessus, pour tous $A_1 \in \mathrm{End}\,V_1$ et $A_2 \in \mathrm{End}\,V_2$,

$$I_{A_1,A_2} = \int_G \langle A_1, \rho(g)\rangle\overline{\langle A_2, \rho(g)\rangle}\mathrm{d}g = \begin{cases} 0 & \text{si } \rho_1 \not\sim \rho_2 \\ \frac{\langle A_1,A_2\rangle}{\dim V_1} & \text{si } \rho_1 = \rho_2. \end{cases}$$

Démonstration du théorème de Péter-Weyl. Par orthogonalité des coefficients, les sous-espaces $\mathcal{H}_\rho$ sont bien deux à deux orthogonaux. Reste à voir qu'ils engendrent un sous-espace dense. Pour cela, on remarque que $\mathcal{H} = \oplus_{\rho\in\hat{G}}\mathcal{H}_\rho$ est une algèbre. Cela découle de la formule

$$\langle u_1, \rho_1(g)v_1\rangle\langle u_2, \rho_2(g)v_2\rangle = \langle u_1 \otimes u_2, (\rho_1 \otimes \rho_2)(g)(v_1 \otimes v_2)\rangle$$

et du fait que $\rho_1 \otimes \rho_2$ se décompose en somme directe de représentations irréductibles, car G est compact. Si $\rho : G \to \mathrm{GL}(V)$ est une représentation de G, la représentation duale $\rho^* : G \to \mathrm{GL}(V^*)$ est définie par $\rho^*(g)f = f \circ \rho(g)^{-1}$ pour tout $f \in V^*$. Cette représentation duale montre que $\mathcal{H}$ est aussi stable par conjugaison complexe, et d'après le théorème de Stone-Weierstrass, $\mathcal{H}$ est dense dans $C(G)$ si $\mathcal{H}$ sépare les points, ce qui revient à dire que si $\rho(g) = 1$ pour tout $\rho \in \hat{G}$, alors $g = 1$. Cela est clair : si $\rho(g) = 1$ pour tout $g \in \hat{G}$, alors, comme $L^2(G)$ se décompose en somme d'irréductibles, g agit trivialement sur $L^2(G)$, donc $g = 1$. (Sinon, $g \cdot \mathbb{1}_U \neq \mathbb{1}_U$ dès que U est un voisinage compact de 1 ne contenant pas g.) □

Exercice 12. On propose une autre démonstration de la densité de $\mathcal{H}$ dans $L^2(G)$, qui n'utilise pas le théorème de Stone-Weierstrass, mais plutôt la convolution par des unités approchées.

1. Soit $\phi \in C(G)$ symétrique à valeurs réelles. Montrer que l'opérateur $T : f \mapsto f * \phi$ est un opérateur compact auto-adjoint sur $L^2(G)$.
2. En déduire que ses espaces propres pour les valeurs propres non nulles sont de dimension finie, et que
$$L^2(G) = \ker T \oplus \bigoplus_n (\ker T - \lambda_n).$$
3. En utilisant le fait que T commute à l'action de G régulière à gauche, montrer que les espaces propres sont stables par l'action régulière à gauche de G, puis que $\overline{\operatorname{im} T} = \oplus_n (\ker T - \lambda_n)$ est inclus dans le sous-espace $\mathcal{H}$ des coefficients de représentations de dimension finie.
4. Si f est un élément orthogonal à $\mathcal{H}$, montrer que pour tout ϕ, $f * \phi$ est orthogonal à f, et conclure.

Maintenant que nous avons montré le théorème de Péter-Weyl, la formule d'inversion de Fourier découle d'un simple calcul d'intégrale.

Démonstration de l'isomorphisme de Fourier. Fixons $\rho \in \hat{G}$. Pour $f \in \mathcal{H}_\rho$, choisissons $A \in \operatorname{End} V_\rho$ tel que $f(g) = \langle A, \rho(g) \rangle$. Par orthogonalité des caractères,
$$\hat{f}(g) = \int_G \langle A, \rho(g) \rangle \rho^*(g) \, \mathrm{d}g = \frac{A}{\dim V_\rho}$$
tandis que
$$\|f\|^2_{L^2(G)} = \int_G |\langle A, \rho(g) \rangle|^2 \, \mathrm{d}g = \frac{\|A\|^2_{HS}}{\dim V_\rho}$$
et donc $f \mapsto (\dim V_\rho)^{\frac{1}{2}} \hat{f}(\rho)$ est une isométrie bijective de $\mathcal{H}_\rho$ sur $\operatorname{End} V_\rho$. Comme $L^2(G)$ est égal à la somme hilbertienne des $\mathcal{H}_\rho$, cela démontre l'isomorphisme annoncé. □

Exercice 13. On considère l'action de $G \times G$ sur l'espace $L^2(G)$ donnée par
$$[(g, h) \cdot f](x) = f(g^{-1} x h).$$
Montrer que les composantes irréductibles de cette représentation sont les sous-espaces $\mathcal{H}_\rho$ du théorème de Péter-Weyl.

Admettant l'existence de la mesure de Haar, l'analyse harmonique permet aussi de montrer la convergence des marches aléatoires apériodiques adaptées.

Convergence des marches aléatoires, deuxième démonstration. Soit μ une probabilité adaptée apériodique sur G. On veut voir que μ^{*n} converge faiblement vers la mesure de Haar sur G.

Rappelons que l'opérateur de convolution à droite T_μ associé à μ est défini par

$$T_\mu f = f * \mu.$$

Montrons tout d'abord que les opérateurs $T_{\mu^{*n}} = T_\mu^n$ convergent simplement vers 0 sur $L_0^2(G)$. Pour cela, notons, pour $\rho \in \hat{G}$,

$$\hat{\mu}(\rho) = \int_G \rho^*(g)\mu(\mathrm{d}g).$$

L'espace $L_0^2(G)$ se décompose en somme de représentations irréductibles non triviales, chacune de dimension finie et stable par T_μ. Comme $\|T_\mu\|_{op} \leq 1$ il suffit de vérifier que T_μ n'a pas de valeur propre de module 1. On raisonne par contraposée en supposant que $T_\mu f = \lambda f$ avec $|\lambda| = 1$. Cela implique $\check{\mu} * \mu * f = f$ et, par stricte convexité de $L^2(G)$, f est invariante par $S^{-1}S$, où $S = \operatorname{Supp}\mu$. Mais alors $S^{-1}S$ est inclus dans le sous-groupe fermé $\operatorname{Stab}_G f$, et μ n'est pas adaptée apériodique.

Soit maintenant $f \in C(G)$. La suite de fonctions $(T_\mu^n f)_{n\geq 1}$ est équicontinue et converge vers $\int_G f$ dans $L^2(G)$, donc elle converge vers $\int_G f$ dans $C(G)$. En particulier,

$$(T_\mu^n f)(1) = \int_G f(g)\mu^{*n}(\mathrm{d}g) \to_{n\to\infty} \int_G f,$$

et (μ^{*n}) converge faiblement vers la probabilité de Haar sur G. □

1.3 La propriété du trou spectral

Nous voulons maintenant étudier la vitesse de convergence de la suite $(\mu^{*n})_{n\geq 1}$ vers la mesure de Haar. Cela se fera par l'étude de la suite $(T_\mu^n)_{n\geq 1}$, où $T_\mu : f \mapsto \mu * f$ est l'opérateur de convolution associé à μ. Notons que l'analyse des marches aléatoires à l'aide de la théorie de Fourier nous a permis de montrer la proposition suivante.

Proposition 1.14. *Soit G un groupe compact et μ une probabilité adaptée et apériodique sur G. La suite d'opérateurs $(T_\mu^n)_{n\geq 1}$ converge simplement vers 0 sur l'espace $L_0^2(G) = \{f \in L^2(G) \mid \int_G f\mathrm{d}m = 0\}$.*

Exercice 14. Démontrer cette proposition directement à partir du théorème 1.2.

Définition 1.15 (Propriété du trou spectral)**.** Nous dirons que la mesure de probabilité μ sur G admet un *trou spectral* en 1 dans $L^2(G)$ si la suite $(T_\mu^n)_{n\geq 1}$ converge en norme vers 0 dans $L_0^2(G)$.

Rappelons que si A est une algèbre de Banach et $T \in A$, le spectre de T dans A est l'ensemble

$$\operatorname{Spec}_A(T) = \{\lambda \in \mathbb{C} \mid T - \lambda \text{ non inversible dans } A\}$$

et le rayon spectral de T

$$\mathrm{RS}_A(T) = \max\{|\lambda| \ ; \ \lambda \in \mathrm{Spec}_A(T)\}.$$

Proposition 1.16. *Soit A une algèbre de Banach et $T \in A$. Les assertions suivantes sont équivalentes.*

1. *La suite $(T^n)_{n\geq 1}$ converge en norme vers 0 dans A.*
2. *$\mathrm{RS}_A(T) < 1$.*

Démonstration. L'équivalence découle immédiatement de la formule pour le rayon spectral

$$\mathrm{RS}_A(T) = \inf_{n\geq 1} \|T^n\|^{\frac{1}{n}},$$

dont la démonstration est laissée en exercice. □

Exercice 15. Soit A une algèbre de Banach et $T \in A$. Montrer que $\mathrm{RS}_A(T) = \inf_{n\geq 1}\|T^n\|^{\frac{1}{n}}$.

Si μ admet un trou spectral dans $L^2(G)$, cette proposition montre que la valeur propre 1 est isolée dans $\mathrm{Spec}(T_\mu)$, ce qui justifie la terminologie utilisée.

Plus généralement, si μ est une mesure borélienne finie sur G, on pose

$$\hat{\mu}(\rho) = \int_G \rho(g)\mu(\mathrm{d}g).$$

Proposition 1.17. *Une probabilité borélienne μ sur G admet un trou spectral si, et seulement si, il existe une constante $\varepsilon > 0$ telle que pour toute représentation $\rho \in \hat{G}$ non triviale, $\mathrm{RS}(\hat{\mu}(\rho)) \leq 1 - \varepsilon$.*

Démonstration. L'isomorphisme de Fourier montre que $L^2_0(G)$ se décompose en somme de représentations irréductibles non triviales. Si $V \simeq V_\rho^*$ est l'une de ces composantes irréductibles, l'opérateur T_μ préserve V et agit sur V comme son coefficient de Fourier $\hat{\mu}(\rho)$. Par suite, $\mathrm{Spec}\, T_\mu = \bigcup_{\rho\in\hat{G}} \mathrm{Spec}\, \hat{\mu}(\rho)$ donc $\mathrm{RS}(T_\mu) = \sup_{\rho\in\hat{G}} \mathrm{RS}(\hat{\mu}(\rho))$ et le résultat est clair. □

Exercice 16. Soit μ une mesure apériodique adaptée sur G. Montrer que si μ est absolument continue par rapport à la mesure de Haar, alors μ admet un trou spectral.

Exercice 17. Soit $G = \mathbb{R}/\mathbb{Z}$ et $\mu = \frac{1}{2}(\delta_\alpha + \delta_{-\alpha})$, avec $\alpha \notin \mathbb{Q}$. Montrer que μ n'admet pas de trou spectral.

Chapitre 2

Mesures invariantes

Nous avons montré au chapitre précédent que sur un groupe compact G, il existe une unique probabilité borélienne m invariante. Si $\mathcal{B}(G)$ désigne la tribu borélienne de G, cette mesure m est l'unique application $m : \mathcal{B}(G) \to \mathbb{R}^+$ qui vérifie les conditions suivantes :

1. (normalisation) $m(G) = 1$;
2. (additivité) $\forall (A_n)_{n\in\mathbb{N}}$ disjoints, $\quad m(\bigcup_n A_n) = \sum_n m(A_n)$;
3. (invariance) $\forall g \in G,\ \forall A, \quad m(gA) = m(A)$.

Naturellement, on peut compléter la tribu $\mathcal{B}(G)$ en lui adjoignant les ensembles négligeables pour m, et obtenir ainsi la tribu de Lebesgue $\mathcal{L}(G)$, à laquelle m admet une unique extension. Mais dès que G est infini, il n'est pas possible de prolonger m à toutes les parties de G.

Exercice 18. Si G est infini, montrer qu'on ne peut pas prolonger m à $\mathcal{P}(G)$.

Pour pouvoir étendre le domaine de définition de la mesure de Haar, nous affaiblissons l'hypothèse d'additivité ci-dessus en la supposant seulement valable pour les familles finies de parties disjointes. On cherche donc à comprendre les applications $\lambda : \mathcal{L}(G) \to \mathbb{R}^+$ qui vérifient

1. (normalisation) $\lambda(G) = 1$;
2. (additivité) $\forall A, B$ disjoints, $\quad m(A \sqcup B) = m(A) + m(B)$;
3. (invariance) $\forall g \in G,\ \forall A, \quad m(gA) = m(A)$.

Nous nous intéresserons dans ce chapitre à deux problèmes étroitement reliés, posés par Hausdorff [10] et Ruziewicz [1] au début du XXème siècle :

1. (Hausdorff) Peut-on prolonger la mesure de Haar m à toutes les parties de G, tout en préservant les trois propriétés ci-dessus ?
2. (Ruziewicz) La mesure de Haar est-elle l'unique application $\mathcal{L}(G) \to \mathbb{R}^+$ vérifiant les trois propriétés ci-dessus ?

Dans le cas particulier où $G = \mathrm{SO}_n(\mathbb{R})$, ces problèmes on joué un rôle crucial dans la compréhension des sous-groupes de type fini du groupe des rotations, et ont mené en particulier à la conjecture du trou spectral que nous étudierons dans les chapitres suivants.

Remarque. En réalité, nous avons construit la mesure de Haar m comme une forme linéaire positive invariante sur $C(G)$, puis appliqué le théorème de représentation de Riesz pour justifier que cela donne lieu à une mesure borélienne sur la tribu des boréliens (puis la tribu complétée) de G. La théorie de l'intégration permet de prolonger naturellement m en une forme linéaire définie sur tout l'espace $L^\infty(G)$. Comme il apparaîtra ci-dessous, le problème de Hausdorff revient est celui de l'existence d'un prolongement de la forme linéaire m à l'espace $B(G)$ des fonctions bornées sur G, tandis que le problème de Ruziewicz est celui de l'unicité de m, vue comme forme linéaire sur $L^\infty(G)$.

2.1 Paradoxe de Banach-Tarski

Dans ce paragraphe, nous cherchons à répondre à la première des deux questions posées ci-dessus. Soit X un ensemble quelconque, et $B(X)$ l'ensemble des fonctions bornées à valeurs réelles sur X.

Définition 2.1. Une *moyenne* sur $B(X)$ est une forme linéaire $m' : B(X) \to \mathbb{R}$ telle que

(i) (positivité) $m'(f) \geq 0$ si $f \geq 0$;

(ii) (normalisation) $m'(\mathbb{1}_X) = 1$.

Si G est un groupe qui agit sur X, nous dirons que m' est *invariante* sous l'action de G si $\forall g \in G,\ \forall f \in B(X),\quad m'(gf) = m'(f)$, où G agit sur $B(X)$ suivant l'action régulière, i.e. $(gf)(x) = f(g^{-1}x)$.

Exercice 19. Montrer qu'une forme linéaire θ positive sur $B(X)$, i.e. vérifiant $\theta(f) \geq 0$ si $f \geq 0$, est nécessairement continue.

Lemme 2.2. *Soit G un groupe agissant sur un espace X. S'il existe une moyenne invariante sur $B(X)$, alors l'application $m : A \mapsto m'(\mathbb{1}_A)$ définie sur $\mathcal{P}(X)$ est à valeurs dans $[0, 1]$ et a les propriétés suivantes :*

1. *(normalisation) $m(X) = 1$;*
2. *(additivité) $\forall A, B$ disjoints, $\quad m(A \sqcup B) = m(A) + m(B)$;*
3. *(invariance) $\forall g \in G,\ \forall A,\quad m(gA) = m(A)$.*

Réciproquement, toute application qui vérifie ces conditions se prolonge uniquement en une moyenne invariante sur $B(X)$.

Démonstration. Par positivité de la forme linéaire m', pour tout $A \subset X$, $m(A) = m'(\mathbb{1}_A) \geq 0$, et de plus, comme $\mathbb{1}_X - \mathbb{1}_A \geq 0$, $1 - m(A) = m'(\mathbb{1}_X - \mathbb{1}_A) \geq 0$, donc $m(A) \in [0, 1]$. Les propriétés de normalisation, additivité et d'invariance de m découlent immédiatement de celles de m'. Réciproquement, si m est une application sur $\mathcal{P}(X)$ vérifiant les propriétés du lemme, elle se prolonge uniquement par linéarité à l'espace vectoriel des fonctions en escalier sur X, puis, par continuité et densité des fonctions en escalier, à $B(X)$ tout entier. Bien sûr, l'extension m' vérifie $m'(\mathbb{1}_X) = m(X) = 1$, et l'on vérifie sans peine que cette extension est positive et invariante. □

À cause de ce lemme, nous identifierons dans la suite une moyenne sur $B(X)$ à l'application qu'elle induit sur $\mathcal{P}(X)$, et parlerons donc souvent de « moyenne sur $\mathcal{P}(X)$ ». Le problème de Hausdorff énoncé ci-dessus est équivalent à celui de

l'existence d'une moyenne invariante sur $B(G)$. Pour déterminer si un groupe G admet une moyenne invariante, nous utiliserons les concepts d'*ensembles équi-décomposables* et de *décomposition paradoxale*.

Définition 2.3 (Ensembles équi-décomposables)**.** Deux parties A et B de X sont dites *équi-décomposables* sous l'action de G s'il existe deux partitions finies $A = \sqcup_{i=1}^{n} A_i$ et $B = \sqcup_{i=1}^{n} B_i$ et des éléments g_i, $i = 1, \ldots, n$ tels que pour chaque i, $B_i = g_i A_i$. Si A et B sont équi-décomposables, on note $A \sim B$. Si A est équi-décomposable à une partie de B, on note $A \lesssim B$.

Une réalisation de l'équivalence $A \sim B$ est une bijection $h : A \to B$ telle que pour certaines partitions $A = \sqcup_{i=1}^{n} A_i$ et $B = \sqcup_{i=1}^{n} B_i$ et certains éléments g_i, $i = 1, \ldots, n$, on ait $B_i = g_i A_i$ et $h(a_i) = g_i a_i$ pour tout $a_i \in A_i$. Alors, si S est une partie quelconque de A, $S \sim h(S)$.

Proposition 2.4. *Si $A \lesssim B$ et $B \lesssim A$, alors $A \sim B$.*

Démonstration. Soient $f : A \to B_1 \subset B$ et $g : B \to A_1 \subset A$ des réalisations des inégalités $A \lesssim B$ et $B \lesssim A$. Définissons par récurrence $C_0 = A \setminus A_1$ et $C_{n+1} = g \circ f(C_n)$ et posons $C = \cup_{n=0}^{\infty} C_n$.

On a $g^{-1}(A \setminus C) = B \setminus f(C)$. En effet, si $x = g^{-1}y$, avec $y \in A \setminus C$, alors $x \notin f(C)$ sans quoi $gx = gf(c) \in C$, car $gf(C) \subset C$. Et réciproquement, si $y \in B \setminus f(C)$, on peut écrire $y = g^{-1}x$, avec $x \in A_1$; alors $x \notin C$, sans quoi $x = (gf)^n a$, $a \in A \setminus A_1$, mais comme $x \in A_1$, on doit avoir $n \geq 1$, et donc $y = g^{-1}x = f(gf)^{n-1}a \in f(C)$.

Par conséquent, $A \setminus C \sim B \setminus f(C)$, et comme $C \sim f(C)$, on trouve bien $A \sim B$. □

Exercice 20. Faire un dessin qui explique la démonstration ci-dessus.

Corollaire 2.5. *Les assertions suivantes sont équivalentes :*
(i) Il existe deux parties disjointes A et B dans X telles que $A \sim X \sim B$.
(ii) Il existe une partition $X = A \sqcup B$ telle que $A \sim X \sim B$.

Démonstration. Il suffit de vérifier que *(i)* implique *(ii)*. Cela découle de la proposition, puisque $X \setminus A \lesssim X$ et $X \sim B \lesssim X \setminus A$. □

Définition 2.6 (Décomposition paradoxale)**.** Une *décomposition paradoxale* de X est une partition $X = A \sqcup B$ telle que $A \sim X \sim B$.

Exercice 21. Montrer que si X admet une décomposition paradoxale, il n'existe pas de moyenne invariante par G sur $B(X)$.

Exemple. Soit $F = \langle a, b \rangle$ un groupe libre engendré par deux générateurs. On note A^+ (resp. A^-) l'ensemble des mots réduits commençant par a (resp. a^{-1}), et on définit de même B^+ et B^-. Alors, $F = A^+ \sqcup A^- \sqcup B^+ \sqcup B^- \sqcup \{1\}$ et

$$F = A^+ \sqcup aA^- = B^+ \sqcup bB^-$$

d'où $F \sim A^+ \sqcup A^-$ et $F \sim B^+ \sqcup B^-$. Avec le corollaire 2.5 ci-dessus, cela montre que F admet une décomposition paradoxale.

Proposition 2.7. *Tout groupe G contenant un sous-groupe libre à deux générateurs admet une décomposition paradoxale. En particulier, un tel groupe n'admet pas de moyenne invariante sur $B(G)$.*

Démonstration. Soit F un sous-groupe libre de G, et $F = A \sqcup B$ une décomposition paradoxale de F. Soit $(x_\alpha)_\alpha$ un ensemble de représentants des classes à gauche de G modulo F. Notons $G_A = \sqcup_\alpha A x_\alpha$ et $G_B = \sqcup_\alpha B x_\alpha$. La partition $G = G_A \sqcup G_B$ est une décomposition paradoxale de G. □

Lemme 2.8. *Si $n \geq 2$, le groupe $\mathrm{SO}_{n+1}(\mathbb{R})$ contient un sous-groupe libre à deux générateurs.*

Démonstration. Montrons que les deux éléments

$$g = \frac{1}{3}\begin{pmatrix} 1 & -2\sqrt{2} & 0 \\ 2\sqrt{2} & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix} \quad \text{et} \quad h = \frac{1}{3}\begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & -2\sqrt{2} \\ 0 & 2\sqrt{2} & 1 \end{pmatrix}$$

engendrent un sous-groupe libre de $\mathrm{SO}_3(\mathbb{R})$. Notons que les matrices $3g$, $3g^{-1}$, $3h$ et $3h^{-1}$ sont à coefficients dans l'anneau $\mathbb{Z}[\sqrt{2}]$, et que par conséquent, pour tout mot w de longueur k en g et h, il existe des entiers $a, b, c \in \mathbb{Z}$ tels que

$$w \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 3^{-k} \begin{pmatrix} a \\ b\sqrt{2} \\ c \end{pmatrix}.$$

De plus, si w est irréductible de longueur $k \geq 1$ et se termine par g ou g^{-1}, alors $3 \nmid b$. Plus précisément, on montre par récurrence sur $k = \ell(w)$ que si $w = uw'g^{\pm 1}$, avec $u \in \{g^{\pm 1}, h^{\pm 1}\}$, alors

$$\begin{cases} 3 \nmid b \text{ et } 3 \mid a & \text{si } u = h^{\pm 1} \\ 3 \nmid b \text{ et } 3 \mid c & \text{si } u = g^{\pm 1} \end{cases}$$

Les détails de ce calcul sont laissés au lecteur. Cela implique que le groupe engendré par g et h est libre : si $w = w'g^{\pm 1}$, l'observation ci-dessus montre que $w \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, et donc $w \neq 1$; et dans le cas général, on peut toujours conjuguer w à un mot qui se termine par $g^{\pm 1}$. □

Remarque. Plus généralement, d'après l'*alternative de Tits*, tout sous-groupe de $\mathrm{GL}_d(\mathbb{R})$ dont l'adhérence de Zariski n'est pas virtuellement résoluble contient un groupe libre sur deux générateurs. La démonstration est là encore basée sur un argument de ping-pong.

Théorème 2.9 (Hausdorff)**.** *Si $n \geq 2$, il n'existe pas de moyenne invariante sur l'ensemble des parties de $\mathrm{SO}_{n+1}(\mathbb{R})$.*

Démonstration. Cela découle immédiatement de l'existence d'un sous-groupe libre à deux générateurs dans $\mathrm{SO}_{n+1}(\mathbb{R})$ et de la proposition 2.7. □

Exercice 22. Le but de cet exercice est de montrer qu'il n'existe pas de moyenne invariante par rotation sur l'ensemble des parties de $\mathbb{S}^2$, un résultat dû à Hausdorff.

1. Construire un sous-groupe libre $F \subset \mathrm{SO}_3(\mathbb{R})$ et une partie dénombrable $D \subset \mathbb{S}^2$ telle que F agisse librement sur $\mathbb{S}^2 \setminus D$.

2. En déduire que $\mathbb{S}^2 \setminus D$ admet une décomposition paradoxale.
3. Montrer que pour toute partie dénombrable $D' \subset \mathbb{S}^2$, les ensembles $\mathbb{S}^2$ et $\mathbb{S}^2 \setminus D'$ sont équi-décomposables.
4. Conclure.

Théorème 2.10 (Tarski)**.** *Un groupe G admet une moyenne invariante sur $\mathcal{P}(G)$ si, et seulement si, il n'admet pas de décomposition paradoxale.*

Remarque. Le théorème de Tarski est valable plus généralement dans le cadre d'une action de G sur un espace X : il existe une moyenne invariante sur $\mathcal{P}(X)$ si et seulement si X n'admet pas de décomposition paradoxale.

Pour montrer le théorème de Tarski, nous montrerons les caractérisations équivalentes suivantes des groupes G qui admettent une moyenne invariante sur $B(G)$. De tels groupes sont dits *moyennables* en tant que groupes discrets.

Théorème 2.11. *Soit G un groupe discret. Les conditions suivantes sont équivalentes :*

(i) (Følner) Pour tout $\varepsilon > 0$ et tout $K \subset G$ fini, il existe $U \subset G$ fini tel que pour tout $x \in K$, $\frac{|U \triangle xU|}{|U|} \leq \varepsilon$.

(ii) (moyennabilité) Il existe une moyenne invariante sur $B(G)$.

(iii) (Tarski) Il n'existe pas de décomposition paradoxale de G.

(iv) (application doublante) Quel que soit $K \subset G$ fini, il n'existe pas d'application $\psi : G \to G$ vérifiant, pour tout $g \in G$, $|\psi^{-1}(\{g\})| \geq 2$ et $\psi(g)g^{-1} \in K$.

Démonstration. $\underline{(i) \Rightarrow (ii)}$ Soit H le sous-espace de $B(G)$ engendré par les fonctions de la forme $g \cdot f - f$, où $g \in G$ et $f \in B(G)$. Montrons que pour tout $h \in H$, $\sup_{g \in G} h(g) \geq 0$. Pour cela, on écrit $h = \sum_{i=1}^{n} k_i f_i - f_i$, et on note $K = \{k_i\}_{1 \leq i \leq n}$. Soit $\varepsilon > 0$ arbitraire et U l'ensemble donné par la condition (i). Alors,

$$\begin{aligned}
\sup h &\geq \frac{1}{|U|} \sum_{u \in U} h(u) \\
&= \frac{1}{|U|} \sum_{i=1}^{n} \sum_{u \in U} f_i(k_i^{-1}u) - f_i(u) \\
&\geq -\frac{1}{|U|} \sum_{i=1}^{n} \|f_i\|_\infty \cdot |k_i U \triangle U| \\
&\geq -n\varepsilon \max_{1 \leq i \leq n} \|f_i\|_\infty.
\end{aligned}$$

Comme $\varepsilon > 0$ peut être pris arbitrairement petit, cela montre ce qu'on veut. Pour construire la moyenne invariante, on définit d'abord une forme linéaire m sur $H \oplus \mathbb{R}\mathbb{1}_G$ par $m(h + \lambda \mathbb{1}_G) = \lambda$. D'après le théorème de Hahn-Banach, on peut prolonger m à $B(G)$ tout entier de sorte que pour tout $f \in B(G)$, $m(f) \leq \sup f$. L'application m est une forme linéaire positive invariante sur $B(G)$; posant $m(A) = m(\mathbb{1}_A)$, on obtient la moyenne invariante souhaitée sur $B(G)$.
$\underline{(ii) \Rightarrow (iii)}$ Soit m une moyenne invariante sur $B(G)$. Si $G = A \sqcup B$ est une partition de G, alors $m(G) = 1 = m(A) + m(B)$, donc $m(A) \neq 1$ ou $m(B) \neq 1$, et A et B ne sauraient être tous deux équi-décomposables à G.

(iii) ⇒ (iv) On raisonne par contraposée. Soit $K \subset G$ un ensemble fini et $\psi : G \to G$ une application doublante telle que pour tout g, $\psi(g)g^{-1} \in K$. Pour chaque $g \in G$, choisissons a_g tel que $\psi(a_g) = g$, et posons

$$A = \{a_g\}_{g \in G} \quad \text{et} \quad B = G \setminus A,$$

de sorte que G s'écrit comme réunion disjointe $G = A \sqcup B$. Pour $k \in K$, posons

$$A_k = \{g \in A \mid \psi(g)g^{-1} = k\} \quad \text{et} \quad B_k = \{g \in B \mid \psi(g)g^{-1} = k\}.$$

Comme ψ envoie A surjectivement sur G, on doit avoir $G = \cup_{k \in K} kA_k$, et de même, $G = \cup_{k \in K} kB_k$. Donc $G = A \sqcup B$ est une décomposition paradoxale.
(iv) ⇒ (i) On raisonne par contraposée. Si G ne satisfait pas la condition de Følner, il existe $\varepsilon > 0$ et une partie finie $K \subset G$ telle que pour toute partie finie U non vide, $|KU \setminus U| \geq \varepsilon |U|$. On peut bien sûr supposer que K est symétrique et contient l'élément neutre. Et même, quitte à remplacer K par K^n, avec $n > \frac{2}{\varepsilon}$ on peut supposer que pour tout U fini non vide, $|KU \setminus U| \geq 2|U|$.

On considère alors le graphe biparti $G \sqcup G$, où deux éléments g et h sont reliés s'il existe $k \in K$ tel que $g = kh$. Pour tout $U \subset G$,

$$|\{h \in G \mid \exists g \in U : g \leftrightarrow h\}| \geq 2|U|.$$

D'après le lemme des mariages rappelé ci-dessous, il existe deux injections $\phi_1, \phi_2 : G \to G$ telles que :
— $\forall g \in G$, $\phi_1(g) \leftrightarrow g$ et $\phi_2(g) \leftrightarrow g$;
— $\forall g, g' \in G$, $\phi_1(g) \neq \phi_2(g')$.
On définit une application $\psi : G \to G$ en posant

$$\psi(h) = \begin{cases} g & \text{s'il existe } g \in G \text{ tel que } h \in \{\phi_1(g), \phi_2(g)\} \\ h & \text{sinon.} \end{cases}$$

Tout élément $g \in G$ admet au moins deux antécédents par ψ, à savoir $\phi_1(g)$ et $\phi_2(g)$, et on a toujours $\psi(g)g^{-1} \in K$. Donc ψ est l'application doublante recherchée. □

Lemme 2.12 (Lemme des mariages de Hall)**.** *Soit $X \sqcup Y$ un graphe biparti de valence bornée.*

1. *Si $\forall U \subset X$, $|\{b \in Y \mid \exists a \in U : \ a \leftrightarrow b\}| \geq |U|$, alors il existe $\phi : X \to Y$ injective telle que $\forall a, \ a \leftrightarrow \phi(a)$;*
2. *Si $\forall U \subset X$, $|\{b \in Y \mid \exists a \in U : \ a \leftrightarrow b\}| \geq 2|U|$, alors il existe $\phi_1, \phi_2 : X \to Y$ injectives telles que $\forall a, \ \phi_1(a) \leftrightarrow a$ et $\phi_2(a) \leftrightarrow a$ et $\forall a, a', \ \phi_1(a) \neq \phi_2(a')$.*

Démonstration. Commençons par montrer le premier point. Étant donnée une partie $U \subset X$, on note $\operatorname{Adj} U$ l'ensemble des voisins de U. Supposons d'abord $|X| < +\infty$. On raisonne par récurrence sur $|X|$. Si $|X| = 1$, alors $X = \{x\}$ et $|\operatorname{Adj} x| \geq 1$, donc le résultat est clair. Supposons donc $|X| \geq 2$. On distingue deux cas.
Premier cas : $\exists X' \subset X : \ \emptyset \neq X' \neq X$ et $|\operatorname{Adj} X'| = |X'|$.
Il suffit alors de construire ϕ sur X' à valeurs dans $\operatorname{Adj} X'$, puis sur $X \setminus X'$ à valeurs dans $\operatorname{Adj} X \setminus \operatorname{Adj} X'$.

Second cas : $\forall X' \subset X,\ |\mathrm{Adj}\, X'| > |X'|$ si $X' \neq \emptyset$.
On choisit $x \in X$ quelconque puis $y \in Y$ tel que $y \leftrightarrow x$. Soit $X' = X \setminus \{x\}$ et $Y' = Y \setminus \{y\}$. Pour tout $U \subset X'$,

$$|\mathrm{Adj}_{Y'} U| \geq |\mathrm{Adj}_Y U| - 1 \geq |U|$$

et on peut donc appliquer l'hypothèse de récurrence à X' et Y' pour conclure.

Supposons maintenant X dénombrable. On écrit alors $X = \sqcup_{i=1}^{\infty} X_i$, avec $\forall i,\ |X_i| < +\infty$ et $X_1 \subset X_2 \subset \ldots$, et on note $Y_i = \mathrm{Adj}\, X_i$. Tous ces ensembles sont finis car le graphe $X \sqcup Y$ est de valence bornée. La première partie de la démonstration s'applique donc aux sous-graphes $X_i \sqcup Y_i$. Comme, pour chaque i, il n'y a qu'un nombre fini de possibilités pour ϕ_i, on peut supposer, quitte à extraire, que les ϕ_i sont compatibles avec l'inclusion, de sorte que la limite inductive $\phi = \mathrm{inj}\lim \phi_i$ est bien définie, injective, et vérifie $\forall x,\ \phi(x) \leftrightarrow x$.

Dans le cas général, on se ramène au cas dénombrable en construisant ϕ sur chaque composante connexe du graphe. Une telle composante connexe est dénombrable car le graphe est de valence bornée.

Enfin, pour montrer la seconde assertion du lemme, il suffit d'appliquer le premier point au graphe biparti $(X \sqcup X) \sqcup Y$. □

Exercice 23 (Rotations en dimension 2)**.** Montrer que $G = \mathrm{SO}_2(\mathbb{R})$ admet une moyenne invariante sur $B(G)$. (*Indication :* Utiliser le critère de Følner.)

Pour la suite, nous aurons aussi besoin de généraliser un peu la notion d'ensembles équi-décomposables. Étant donnés deux entiers $m, n \geq 1$ et deux parties $A, B \subset X$, nous dirons que mA et nB sont équi-décomposables si l'on peut décomposer m copies de A pour former avec les parties obtenues n copies de B grâce à l'action de G. Nous écrirons alors $mA \sim nB$. On laisse le soin au lecteur d'adapter la démonstration de la proposition 2.4 pour montrer que $mA \lesssim nB$ et $nB \lesssim mA$ implique $mA \sim nB$. La règle de simplification suivante est un peu plus subtile.

Proposition 2.13 (Règle de simplification)**.** *Si $nA \sim nB$ pour un certain $n \geq 1$, alors $A \sim B$.*

Démonstration. L'équivalence $A \sim B$ signifie qu'il existe un ensemble fini F d'éléments de G et une partition $A = \sqcup_{f \in F} A_f$ telle que B s'écrit comme réunion disjointe $B = \sqcup_{f \in F} fA_f$. On peut voir cela comme un graphe biparti $A \sqcup B$, où chaque point $a \in A$ est relié à fa, où $f \in F$ est choisi de sorte que $a \in A_f$. De la même manière, l'équivalence $nA \sim nB$ permet de construire un graphe biparti $A \sqcup B$ de valence n. En effet, pour chacune des n partitions $\mathcal{P}^{(i)}$, $i = 1, \ldots, n$ de A, un point a appartient à un unique atome $P_a^{(i)}$, envoyé sur une partie $g_i P_a^{(i)} \subset B$. Le point a est relié à chaque $g_i a$, $i = 1, \ldots, n$. D'après le théorème de Kőnig rappelé ci-dessous, il existe une application bijective $\phi : A \to B$ telle que pour tout $a \in A$, a est relié à $\phi(a)$. Cela montre que $A \sim B$. □

Théorème 2.14 (Kőnig)**.** *Soit $A \sqcup B$ un graphe biparti régulier de valence $k \in \mathbb{N}^*$. Il existe un couplage bijectif de A et B.*

Démonstration. On commence par le cas où le graphe est fini. Soit $X \subset A$ et $Y = \mathrm{Adj}\, X$. Le graphe est régulier, donc le nombre d'arêtes issues de X est égal à $k|X|$, tandis que le nombre d'arêtes issues de Y est égal à $k|Y|$. Comme ces

ensembles coïncident — ils sont simplement constitués des arêtes entre X et Y — cela montre que $|X| = |Y|$. D'après le lemme des mariages de Hall, il existe un couplage de A et B, qui est bijectif car $|A| = |B|$.

Dans le cas général, on remarque que toute composante connexe du graphe est dénombrable, puisque la valence est finie. Il suffit donc de montrer le résultat lorsque A et B sont dénombrables. Notons $(e_n)_{n\in\mathbb{N}}$ la suite des arêtes de $A \sqcup B$. Un couplage M de A et B peut être codé par une suite $s = (s_n)_{n\in\mathbb{N}}$, où

$$s_n = \begin{cases} 1 & \text{si } e_n \in M \\ 0 & \text{sinon.} \end{cases}$$

Le couplage est bijectif si pour chaque $a \in A$ (resp. $b \in B$), il existe un unique $n \in \mathbb{N}$ tel que $s_n = 1$ et a (resp. b) est une extrémité de e_n. Nous allons construire la suite (s_n) par induction. Une suite finie $s = (s_n)_{0\leq n\leq N}$ est dite *admissible* s'il existe un graphe biparti régulier $A' \sqcup B'$ fini contenant toutes les extrémités des arêtes e_n, $n = 0, \dots, N$ et admettant un couplage M' tel que pour $n = 0, \dots, N$, l'arête e_n appartient à M' si et seulement si $s_n = 1$. Pour tout N, il existe une suite finie admissible de longueur N. Cela permet de définir par récurrence la suite (s_n) recherchée : on choisit pour chaque N une suite admissible $(s_n)_{0\leq n\leq N}$ qui prolonge les termes $n < N$ déjà choisis et qui admet une infinité de prolongements. □

Remarque. Dans le théorème de Kőnig, comme dans la démonstration de la règle de simplification, le graphe peut avoir des arêtes multiples.

Théorème 2.15 (Paradoxe de Banach-Tarski)**.** *Soit G un groupe compact. On suppose que G n'est pas moyennable en tant que groupe discret. Alors G est équi-décomposable à toute partie d'intérieur non vide $U \subset G$.*

Démonstration. Comme G est compact et U d'intérieur non vide, G peut être recouvert par un nombre fini de translatés de U. Cela montre déjà que pour un certain n, $G \lesssim nU$. Mais G n'est pas moyennable comme groupe discret, et admet donc une décomposition paradoxale $G \sim 2G$, qui implique $G \sim nG$. Ainsi, $nG \lesssim nU$. Réciproquement, on a bien sûr $U \lesssim G$, et donc $nU \lesssim nG$, puis $nU \sim nG$. D'après la proposition 2.13, $U \sim G$, ce qu'il fallait démontrer. □

2.2 Problème de Ruziewicz

Dans le paragraphe précédent, le groupe G était vu comme un groupe discret, et nous avons ainsi donné un critère pour qu'il existe une moyenne invariante définie sur l'espace $B(G)$ des fonctions bornées sur G. Dorénavant, G sera muni d'une topologie localement compacte quelconque. Nous avons vu au chapitre 1 qu'il existe une unique mesure de Radon m sur G, appelée mesure de Haar, ce qui permet de définir l'espace $L^\infty(G) = L^\infty(G, m)$ constitué des classes d'équivalence modulo m de fonctions mesurables bornées.

Définition 2.16. Une *moyenne* sur $L^\infty(G)$ est une forme linéaire $\lambda : L^\infty(G) \to \mathbb{R}$ telle que

(i) (positivité) $\lambda(f) \geq 0$ si $f \geq 0$;

(ii) (normalisation) $\lambda(\mathbb{1}_G) = 1$.

Nous dirons que λ est *invariante* si $\forall g \in G,\ \forall f \in L^\infty(X), \quad \lambda(gf) = \lambda(f)$.

Remarque. Si G est muni de la topologie discrète, alors $L^\infty(G)$ coïncide avec l'espace $B(G)$ de toutes les fonctions bornées sur G. C'est ce cas que nous avons étudié au paragraphe précédent. En général, un groupe *topologique* G est dit moyennable s'il existe une moyenne invariante sur $L^\infty(G)$.

Exercice 24. Soit $\mathcal{L}(G)$ la tribu complétée pour la mesure de Haar. Montrer que la donnée d'une moyenne sur $L^\infty(G)$ est équivalente à celle d'une application $\lambda : \mathcal{L}(G) \to [0,1]$ telle que

1. (normalisation) $\lambda(G) = 1$;
2. (absolue continuité) $\forall A,\ m(A) = 0 \Rightarrow \lambda(A) = 0$;
3. (additivité) $\forall A, B$ disjoints, $\quad \lambda(A \sqcup B) = \lambda(A) + \lambda(B)$.

Vérifier que l'invariance est compatible avec cette équivalence.

Le problème de Ruziewicz concerne l'unicité de la mesure de Haar vue comme moyenne invariante sur $L^\infty(G)$. Dans le cas du groupe des rotations, nous y observerons la même distinction que pour le problème de Hausdorff : si $n \geq 2$ la mesure de Haar est l'unique moyenne invariante par rotation sur les parties mesurables de $\mathbb{S}^n$, tandis que sur $\mathbb{S}^1$, il existe de nombreuses autres moyennes invariantes, comme le montre l'exercice suivant.

Exercice 25. Le but de cet exercice est de démontrer que si G est un groupe compact métrique moyennable en tant que groupe discret, alors la mesure de Haar n'est pas l'unique moyenne invariante sur $L^\infty(G)$.

1. Soit A un G_δ dense de G. Reprendre la démonstration de $(i) \Rightarrow (ii)$ dans le théorème 2.11, et montrer qu'on peut prolonger la forme linéaire sur $H \oplus \mathbb{R}\mathbb{1}_G \oplus \mathbb{R}\mathbb{1}_A$ définie par $\lambda(h + \alpha\mathbb{1}_G + \beta\mathbb{1}_A) = \alpha + \beta$ en une moyenne invariante. (*Indication :* vérifier que pour tout $h \in H$, $\sup_{x\in A} h(x) \geq 0$).
2. Justifier qu'il existe un G_δ dense A dans G tel que $m(A) = 0$, et conclure.

Exercice 26. Pour montrer que la réciproque à l'énoncé de l'exercice précédent est fausse, construire un groupe compact G non moyennable en tant que groupe discret et sur lequel la mesure de Haar n'est pas l'unique moyenne invariante sur $L^\infty(G)$.

Les exercices ci-dessus montrent que la non moyennabilité est une condition nécessaire mais non suffisante pour que la mesure de Haar soit unique comme moyenne sur $L^\infty(G)$. C'est la propriété du trou spectral qui nous fournira un critère suffisant, grâce au théorème suivant.

Théorème 2.17. *Soit G un groupe compact. On suppose qu'il existe une probabilité μ à support fini sur G ayant un trou spectral dans $L^2(G)$. Alors la probabilité de Haar est l'unique moyenne invariante sur $L^\infty(G)$.*

Démonstration. Soit λ une moyenne invariante sur $L^\infty(G)$. Par densité de $L^1(G)$ dans son bi-dual [5, Lemme III.4], il existe une suite généralisée $(f_i)_{i\in I}$ d'éléments de $L^1(G)$ telle que pour tout i, $f_i \geq 0$, $\int_G f_i = 1$ et qui converge faiblement vers λ :

$$\forall \phi \in L^\infty(G), \quad \lim_i \int_G \phi(x) f_i(x) \mathrm{d}x = \lambda(\phi).$$

Par invariance de λ sous l'action de G, pour tout g dans G, $(gf_i)_i$ converge faiblement vers λ, et donc $\lim_i gf_i - f_i = 0$. D'après le théorème de Hahn-Banach, les adhérences d'une partie convexe sont les mêmes pour les topologies faible et forte [5, Théorème III.7], on peut obtenir par combinaisons convexes des f_i une suite généralisée $(g_i)_{i\in I}$ telle que pour tout $\gamma \in \operatorname{Supp}\mu$, $\lim_i \|\gamma g_i - g_i\|_1 = 0$; on a encore $g_i \geq 0$ et $\int_G g_i = 1$.

Posons $h_i = \sqrt{g_i}$, de sorte que $h_i \in L^2(G)$, $h_i \geq 0$ et $\|h_i\|_2 = 1$. Pour chaque γ dans $\operatorname{Supp}\mu$, on majore

$$\begin{aligned}\|\gamma h_i - h_i\|_2^2 &= \int_G \big((\gamma h_i)(x) - h_i(x)\big)^2 \mathrm{d}x \\ &\leq \int_G \big|(\gamma h_i)(x) - h_i(x)\big|\big(\gamma h_i)(x) + h_i(x)\big)\mathrm{d}x \\ &= \|\gamma g_i - g_i\|_1\end{aligned}$$

ce qui montre que $\lim_i \|\gamma h_i - h_i\|_2 = 0$, et donc $\lim_i \|T_\mu h_i - h_i\|_2 = 0$. Par la propriété du trou spectral, cela implique que (h_i) converge dans $L^2(G)$ vers $\mathbb{1}_G$. Mais $\|g_i - 1\|_1 \leq 2\|h_i - 1\|_1 \leq 2\|h_i - 1\|_2$, et donc

$$\lambda = \lim_i g_i = 1,$$

ce qu'il fallait démontrer. □

Remarque. On peut comprendre ce théorème et sa démonstration de la façon suivante. S'il existait une moyenne invariante λ sur $L^\infty(G)$, on aurait $T_\mu\lambda = \lambda$. Si μ est à support fini, en approchant λ par des fonctions, cela permet de construire des vecteurs presque invariants pour T_μ dans $L^2(G)$. Par la propriété du trou spectral, ces vecteurs doivent converger vers la fonction constante égale à 1, et λ est égale à la mesure de Haar.

Remarque. On peut adapter la démonstration pour montrer que le théorème est encore valable si l'on suppose qu'il existe $p \in]1, +\infty]$ et une mesure à support fini μ telle que l'opérateur T_μ ait un trou spectral dans $L^p(G)$. Il suffit de remarquer que pour $x, y \geq 0$, $|x - y|^p \leq x^p - y^p$, ce qui se ramène à $|1 - t|^p \leq |1 - t| \leq 1 - t^p$ pour $t \in [0, 1]$.

Par construction, la mesure de Haar est définie sur la tribu $\mathcal{B}(G)$ des boréliens de G, mais on peut l'étendre naturellement à la tribu $\mathcal{L}(G)$ des ensembles mesurables pour m, obtenue en adjoignant à $\mathcal{B}(G)$ les ensembles négligeables pour m :

$$\mathcal{L}(G) = \{A \in \mathcal{P}(G) \mid \exists B, B' \in \mathcal{B}(G) :\ B \subset A \subset B' \text{ et } m(B' \setminus B) = 0\}.$$

Le théorème ci-dessus permet de montrer le résultat d'unicité suivant.

Corollaire 2.18. *Soit G un groupe compact. On suppose qu'il existe une mesure μ à support fini sur G qui admet un trou spectral. Alors, la mesure de Haar est l'unique application définie sur $\mathcal{L}(G)$ vérifiant*

1. *(normalisation)* $\lambda(G) = 1$;
2. *(additivité)* $\forall A, B$ *disjoints*, $\quad \lambda(A \sqcup B) = \lambda(A) + \lambda(B)$;
3. *(invariance)* $\forall g \in G,\ \forall A, \quad \lambda(gA) = \lambda(A)$.

Démonstration. Vu le théorème 2.17 et la correspondance établie à l'exercice 24, il suffit de vérifier qu'une telle application vérifie $\lambda(A) = 0$ pour tout A tel que $m(A) = 0$. Si G est fini, m est la mesure de comptage, et le résultat est évident. Si G est infini, il existe une suite $(U_i)_{i\geq 1}$ de voisinages ouverts de l'identité telle que le nombre de translatés de U_i disjoints dans G tend vers l'infini. Par invariance, cela implique $\lim_i \lambda(U_i) = 0$. L'existence d'une probabilité à support fini ayant un trou spectral implique que G n'est pas moyennable en tant que groupe discret. D'après le paradoxe de Banach-Tarski, G est équi-décomposable au voisinage ouvert U_i, et A est donc équi-décomposable à une partie $A_i \subset U_i$. Mais A_i peut s'écrire comme réunion de translatés de parties de A, et chacun de ces translatés appartient à $\mathcal{L}(G)$, puisque il est inclus dans la partie négligeable A. Par conséquent, on peut écrire $\lambda(A) = \lambda(A_i) \leq \lambda(U_i)$, et en passant à la limite, $\lambda(A) = 0$. □

Comme pour le paradoxe de Banach-Tarski, le problème de Ruziewicz concerne à l'origine les mesures sur $\mathbb{S}^n$ invariantes par rotation. Dans ce cadre, il faut déterminer s'il existe une mesure à support fini dans $\mathrm{SO}_{n+1}(\mathbb{R})$ qui admet un trou spectral. La réponse a été apportée indépendamment par Margulis [12] et Sullivan [15] pour $n \geq 4$, puis par Drinfeld [6] pour $n = 2$ et $n = 3$.

Théorème 2.19 (Margulis, Sullivan, Drinfeld)**.** *Si $n \geq 2$, il existe une mesure à support fini dans $G = \mathrm{SO}_{n+1}(\mathbb{R})$ qui admet un trou spectral. En particulier, la mesure de Haar est l'unique application sur $\mathcal{L}(G)$ qui vérifie les conditions du corollaire 2.18.*

Exercice 27. Vérifier que les méthodes de ce paragraphe permettent de montrer que pour $n \geq 2$, la mesure de Haar est l'unique application définie sur $\mathcal{L}(\mathbb{S}^n)$ qui vérifie les conditions du corollaire 2.18.

2.3 La conjecture du trou spectral

Dans ce dernier paragraphe, on cherche à comprendre quelles mesures ont la propriété du trou spectral. Ce problème est difficile, et très largement ouvert aujourd'hui. Nous nous bornerons donc ici à quelques observations élémentaires, à l'énoncé de la conjecture du trou spectral, et des résultats récents de Bourgain et Gamburd dont la démonstration occupera une partie de la suite de ce cours. L'obstruction principale à la propriété du trou spectral est la donnée par la proposition suivante.

Proposition 2.20. *Soit G un groupe compact. On suppose qu'il existe un groupe abélien infini H et un morphisme de groupes surjectif et continu $\phi : G \to H$. Si μ est une probabilité à support fini sur G, alors μ n'admet pas de trou spectral dans $L^2(G)$.*

Démonstration. L'application $\begin{array}{ccc} L^2(H) & \to & L^2(G) \\ f & \mapsto & f \circ \phi \end{array}$ est une isométrie, car l'image de la mesure de Haar sur G par ϕ est égale à la mesure de Haar sur H. Cela permet d'identifier $L^2(H)$ à un sous-espace fermé de $L^2(G)$. En outre $L^2(H)$ est stable par l'action de G, et admet donc un supplémentaire fermé invariant. Par suite, le spectre de T_μ comme opérateur sur $L^2(G)$ contient le spectre de

T_μ comme opérateur sur $L^2(H)$, et il suffit de montrer la proposition dans le cas où $G = H$ est abélien, ce que nous supposons donc dans la suite.

Soit μ une probabilité à support fini dans G, et $S = \operatorname{Supp}\mu$. Tout d'abord, le groupe engendré par S est abélien, il existe donc une suite de parties U_n telles que

$$\lim_{n\to\infty} \frac{|SU_n \triangle U_n|}{|U_n|} = 0.$$

On peut choisir une suite de réels $\varepsilon_n > 0$ tels que pour chaque n, les boules $B(s, \varepsilon_n)$, pour $s \in U_n$ sont disjointes, et comme G est infini, on peut supposer de plus que $\lim_{n\to\infty} |U_n| m(B(1, \varepsilon_n)) = 0$. Posons alors $f_n = \sum_{s\in U_n} \mathbb{1}_{B(s,\varepsilon_n)}$ et notons que $\int_G f_n = \|f_n\|_2^2 = |U_n| m(B(1, \varepsilon_n))$. Par ailleurs, pour $t \in S$,

$$\|tf_n - f_n\|_2^2 \leq |tU_n \triangle U_n||B(1, \varepsilon_n)| \leq |SU_n \triangle U_n||B(1, \varepsilon_n)|$$

d'où

$$\lim_{n\to\infty} \frac{\|T_\mu f_n - f_n\|_2^2}{\|f_n\|_2^2} = 0.$$

Soit enfin $g_n = f_n - \int_G f_n$. Comme $T_\mu g_n - g_n = T_\mu f_n - f_n$ et $\int_G f_n = o(\|f_n\|_2)$, on a encore

$$\lim_{n\to\infty} \frac{\|T_\mu g_n - g_n\|_2}{\|g_n\|_2} = 0.$$

Donc (g_n) est une suite de vecteurs presque invariants pour T_μ dans $L^2_0(G)$, et μ n'a pas la propriété du trou spectral. □

Remarque. La proposition ci-dessus est encore valable si l'on suppose seulement que le groupe H est abstraitement moyennable. C'est tout ce que nous avons utilisé dans la démonstration.

La proposition ci-dessus assure que si G admet un quotient abélien, il existe des mesures adaptées apériodiques sur G qui n'admettent pas de trou spectral. La conjecture qui nous intéresse stipule une réciproque à cette observation, du moins si G est un groupe de Lie connexe. Dans ce cadre, la structure des groupes de Lie compacts montre que l'absence de quotient abélien infini équivaut à l'hypothèse que le centre de G est fini.

Conjecture (Conjecture du trou spectral)**.** *Toute mesure adaptée sur un groupe de Lie G compact connexe à centre fini admet un trou spectral dans $L^2(G)$.*

Remarque. Comme G est connexe, il n'est pas nécessaire de supposer que μ est apériodique. En effet, la connexité implique que G n'a pas de quotient fini, et comme G est semi-simple (par le théorème de structure des groupes de Lie compacts, cela est équivalent au fait que G est à centre fini) on en déduit que G n'admet pas de quotient abélien. Pour tout sous-groupe distingué H, l'image de μ dans G/H est adaptée, et ne saurait donc être supportée par un singleton.

Telle que nous l'avons énoncée, la conjecture du trou spectral est peut-être excessive, car à l'heure actuelle, on ne connaît même pas d'exemple de groupe compact infini sur lequel toute mesure apériodique adaptée admet un trou spectral. En fait, les seuls exemples de mesures μ à support fini ayant la propriété du trou spectral sont dans des cas où le groupe G admet une structure algébrique, et reposent sur les propriétés arithmétiques des éléments du support de μ. Le théorème le plus général, montré récemment grâce aux avancées remarquables de Bourgain et Gamburd [4, 3] sur le sujet, est énoncé ci-dessous.

Théorème 2.21. *Soit G un groupe de Lie compact connexe à centre fini et μ une probabilité adaptée sur G. On suppose que dans une certaine base de l'algèbre de Lie $\mathfrak{g}$ de G, tous les éléments $\operatorname{Ad} g$, $g \in \operatorname{Supp} \mu$ sont des matrices à coefficients algébriques. Alors μ admet un trou spectral.*

Exercice 28. Construire une mesure adaptée sur $\mathrm{SO}_3(\mathbb{R})$ à support fini dans $\mathrm{SO}_3(\mathbb{Q})$.

Exercice 29. Soit G un groupe topologique et $D(G)$ le sous-groupe fermé de G engendré par les commutateurs $xyx^{-1}y^{-1}$, $x, y \in G$.

1. Montrer que $D(G)$ est égal à l'intersection de tous les noyaux de morphismes continus $G \to H$, avec H abélien.
2. Nous dirons qu'un groupe compact G est *parfait* si le sous-groupe fermé $D(G)$ est d'indice fini dans G. Montrer que le groupe compact $G = \mathcal{A}_5^{\mathbb{N}}$ est parfait.
3. Construire une mesure adaptée sur G qui n'admet pas de trou spectral.
4. Vérifier que G est abstraitement moyennable.

Chapitre 3

Combinatoire additive

Dans ce chapitre, nous présentons quelques outils de combinatoire additive — distance de Ruzsa, inégalité de Plünnecke, etc. — dont nous aurons besoin dans la démonstration du théorème 2.21.

La combinatoire additive peut se définir comme l'étude des propriétés combinatoires des groupes. Typiquement, dans un groupe G, étant données deux parties finies A et B, on cherche à étudier les liens entre le cardinal de l'ensemble produit $AB = \{ab \ ; \ a \in A, b \in B\}$ et les propriétés algébriques des parties A et B. Mais commençons par un exemple élémentaire qui illustre bien les problèmes que nous aborderons.

Exercice 30. Soit A une partie finie d'un groupe G, et $AA = \{ab \ ; \ a, b \in A\}$.

1. Si $|AA| = |A|$, montrer qu'il existe un groupe fini H et un élément a normalisant H tel que $A = aH$.
2. On suppose maintenant $|AA| < \frac{3}{2}|A|$. On veut voir qu'il existe un sous-groupe fini H et a normalisant H tels que $A \subset aH$ et $|H| < \frac{3}{2}|A|$.
   (a) Vérifier que ces conditions donnent bien $|AA| < \frac{3}{2}|A|$.
   (b) Soit $H = A^{-1}A$. Montrer que tout $x \in H$ s'écrit de $k > |A|/2$ façons différentes $x = d_1 c_1^{-1} = \cdots = d_k c_k^{-1}$.
   (c) Montrer que H est un sous-groupe fini normalisé par A.
   (d) Montrer que si $a \in A$ et $B = a^{-1}A$, alors $a^{-1}BaB = H$, et conclure.

3.1 Calcul de Ruzsa

Dans ce paragraphe, on se place dans un groupe G quelconque.

Définition 3.1 (Distance de Ruzsa)**.** Étant données deux parties finies A et B de G, on pose

$$d(A, B) = \log \frac{|AB^{-1}|}{\sqrt{|A||B|}}.$$

Exercice 31. Montrer que $d(A, B) \geq 0$ avec égalité si et seulement si A et B sont des classes à gauche d'un même sous-groupe fini.

Lemme 3.2 (Inégalité triangulaire)**.** *Soient A, B et C des parties finies de G. Alors*

$$d(A,C) \leq d(A,B) + d(B,C).$$

Démonstration. Pour chaque x dans AC, fixons une décomposition $x = a_x c_x$, avec $a_x \in A$ et $c_x \in C$. L'application

$$\begin{array}{ccc} B \times AC^{-1} & \to & AB^{-1} \times BC^{-1} \\ (b,x) & \mapsto & (a_x b^{-1}, bc_x) \end{array}$$

est injective, donc $|B||AC^{-1}| \leq |AB^{-1}||BC^{-1}|$. □

Dans la suite, si A est une partie de G et $n \geq 1$, on note A^n l'ensemble produit $A^n = \{a_1 a_2 \dots a_n \ ; \ a_1, \dots, a_n \in A\}$. En ce qui nous concerne, la conséquence la plus importante de l'inégalité de Ruzsa est la suivante.

Proposition 3.3 (Ensembles à petit triplement)**.** *Soit $A \subset G$ tel que $|A^3| \leq K|A|$. Alors, pour tout $n \geq 3$, $|A^n| \leq K^{2n-5}|A|$. Plus généralement, si $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$, alors $|A^{\varepsilon_1} A^{\varepsilon_2} \dots A^{\varepsilon_n}| \leq K^{5n}|A|$.*

Démonstration. Soit $n \geq 3$. D'après l'inégalité de Ruzsa,

$$d(A^{n-1}, A^{-2}) \leq d(A^{n-1}, A^{-1}) + d(A^{-1}, A) + d(A, A^{-2})$$

et donc $|A^{n+1}| \leq |A^n| \frac{|A^2|}{|A|} \frac{|A^3|}{|A|}$. Par récurrence, cela montre déjà la première assertion.

La démonstration de la seconde inégalité est analogue. Notons pour simplifier $A_n = A^{\varepsilon_1} A^{\varepsilon_2} \dots A^{\varepsilon_n}$. On commence par écrire,

$$d(A_{n-1}, A^{-\varepsilon_{n+1}} A^{-\varepsilon_n}) \leq d(A_{n-1}, A^{-\varepsilon_n}) + d(A^{-\varepsilon_n}, A) + d(A, A^{-\varepsilon_{n+1}} A^{-\varepsilon_n})$$

i.e.

$$|A_{n+1}| \leq |A_n| \frac{|AA^{\varepsilon_n}|}{|A|} \frac{|AA^{\varepsilon_n} A^{\varepsilon_{n+1}}|}{|A|}.$$

Pour majorer les deux derniers quotients indépendamment des valeurs de ε_n et ε_{n+1}, on utilise encore l'inégalité de Ruzsa. D'abord, $d(A, A^2) \leq d(A, A^{-1}) + d(A^{-1}, A^2)$ donne

$$\frac{|AA^{-2}|}{|A|} \leq \frac{|A^2|}{|A|} \frac{|A^3|}{|A|} \leq K^2,$$

et de même, échangeant les rôles de A et A^{-1}, $|A^{-1}A^2| \leq K^2|A|$. Enfin, écrivant $d(A, A^{-1}A) \leq d(A, A^{-1}) + d(A^{-1}, A^{-1}A)$, on trouve

$$\frac{|AA^{-1}A|}{|A|} \leq \frac{|A^2|}{|A|} \frac{|A^{-1}A^2|}{|A|} \leq K^3.$$

Ainsi, on a toujours $|A_{n+1}| \leq K^5 |A_n|$ et par récurrence, la proposition est démontrée.

□

Exercice 32. Montrer que l'énoncé analogue à la proposition 3.3 n'est pas valable si l'on suppose seulement $|A^2| \leq K|A|$.

Définition 3.4 (Sous-groupes approximatifs)**.** Soit $K \geq 1$. Un *sous-groupe K-approximatif* de G est une partie A qui vérifie les propriétés suivantes :
— $1 \in A$ et $A^{-1} = A$;
— il existe $X \subset G$ tel que $|X| \leq K$ et $AA \subset AX$.

Lemme 3.5 (Lemme de recouvrement de Ruzsa)**.** *Soient A et B deux parties finies de G et $K \geq 0$ tel que $|AB| \leq K|A|$. Alors, il existe $X \subset B$ tel que $|X| \leq K$ et $B \subset A^{-1}AX$.*

Démonstration. Soit $X = \{b_1, \ldots, b_n\}$ une famille maximale d'éléments de B telle que les ensembles $Ab_1, \ldots, Ab_n$ soient disjoints. Comme tous ces ensembles sont inclus dans AB, on doit avoir $n \leq K$. De plus, par maximalité de la famille, pour tout $b \in B$, il existe i tel que $Ab \cap Ab_i \neq \emptyset$, et par conséquent $b \in A^{-1}Ab_i$, puis $B \subset A^{-1}AX$. □

Avec la proposition 3.3, ce lemme permet de caractériser les ensembles à petit triplement en termes de sous-groupes approximatifs.

Proposition 3.6 (Caractérisation du petit triplement)**.** *Étant donné une partie finie $A \subset G$ et $K \geq 2$ les assertions suivantes sont équivalentes.*

(i) $|A^3| \leq K^{O(1)}|A|$

(ii) $\exists H$ *sous-groupe $K^{O(1)}$-approximatif tel que* $A \subset H$ *et* $|H| \leq K^{O(1)}|A|$.

Démonstration. Il est clair que la seconde assertion implique la première. En effet, $A^3 \subset H^3 \subset HX^2$, donc $|A^3| \leq |X|^2|H| \leq K^{O(1)}|H| \leq K^{O(1)}|A|$.

Réciproquement, montrons que si $|A^3| \leq K|A|$, alors $H = (A \cup A^{-1} \cup \{1\})^2$ est un sous-groupe $K^{O(1)}$-approximatif. Comme cet ensemble est symétrique, il suffit de voir que $H \subset HX$ pour un certain X tel que $|X| \leq K^{O(1)}$. Soit $A_1 = A \cup A^{-1} \cup \{1\}$. L'ensemble A_1^5 est inclus dans la réunion des parties de la forme $A^{\varepsilon_1}A^{\varepsilon_2}A^{\varepsilon_3}A^{\varepsilon_4}A^{\varepsilon_5}$, où $\varepsilon_i \in \{-1, 0, 1\}$, et d'après la proposition 3.3 chacune de ces parties vérifie $|A^{\varepsilon_1}A^{\varepsilon_2}A^{\varepsilon_3}A^{\varepsilon_4}A^{\varepsilon_5}| \leq K^{O(1)}|A|$. Donc $|A_1H^2| = |A_1^5| \leq K^{O(1)}|A_1|$. D'après le lemme de recouvrement de Ruzsa, il existe une partie $X \subset H$ telle que $|X| \leq K^{O(1)}$ et $H^2 \subset A_1^{-1}A_1X = HX$. □

Dans la suite, nous voudrons aussi comprendre les parties A et B qui satisfont l'inégalité $|AB| \leq K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$. La proposition suivante en donne une caractérisation en termes de sous-groupes approximatifs. La démonstration est sensiblement plus difficile que celle de la caractérisation des ensembles à petit triplement, et sera donnée au paragraphe 3.3, une fois que nous aurons introduits les outils nécessaires.

Proposition 3.7 (Caractérisation du petit doublement)**.** *Pour deux parties finies $A, B \subset G$ et $K \geq 2$, les assertions suivantes sont équivalentes.*

1. $|AB| \leq K^{O(1)}|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$;
2. *Il existe un sous-groupe $K^{O(1)}$-approximatif H et $X, Y \subset G$ tels que $|X|, |Y| \leq K^{O(1)}$ et $A \subset XH$ et $B \subset HY$.*

Remarque. Il est facile de voir que la seconde assertion implique la première : $AB \subset XHHY$ donc $|AB| \leq K^{O(1)}|HH| \leq K^{O(1)}|H|$. L'autre implication est plus difficile à démontrer.

3.2 Le lemme de Balog-Szemerédi-Gowers

Définition 3.8 (Énergie multiplicative)**.** L'*énergie multiplicative* de deux parties finies $A, B \subset G$ est

$$E(A,B) = |\{(a,b,a',b') \in A \times B \times A \times B \mid ab = a'b'\}|.$$

Commençons par noter quelques propriétés importantes de l'énergie multiplicative. Étant donnée une partie $S \subset A \times B$, nous noterons

$$A \cdot_S B = \{ab \ ; \ (a,b) \in S\}.$$

Proposition 3.9. *L'énergie multiplicative de deux ensembles A et B satisfait les propriétés suivantes.*

(i) $E(A,B) = \|\mathbb{1}_A * \mathbb{1}_B\|_2^2$.

(ii) *Pour tous* $g, h \in G$, $E(gA, Bh) = E(A,B)$.

(iii) $E(A, A^{-1}) = E(A^{-1}, A)$;

(iv) $|A||B| \leq E(A,B) \leq |A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$.

(v) *Si* $|AB| \leq K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$, *alors* $E(A,B) \geq \frac{|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}}{K}$.

(vi) *Si* $E(A,B) \geq \frac{1}{K}|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}$, *alors il existe une partie* $S \subset A \times B$ *telle que* $|S| \geq \frac{|A||B|}{2K^2}$ *et* $|A \cdot_S B| \leq 2K|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$.

Démonstration. (i) On calcule

$$\begin{aligned}
\sum_z (\mathbb{1}_A * \mathbb{1}_B(z))^2 &= \sum_z \Big(\sum_{xy=z} \mathbb{1}_A(x)\mathbb{1}_B(y)\Big)^2 \\
&= \sum_z \sum_{xy=z=x'y'} \mathbb{1}_A(x)\mathbb{1}_B(y)\mathbb{1}_A(x')\mathbb{1}_B(y') \\
&= \sum_{x,y,x',y' : xy=x'y'} \mathbb{1}_A(x)\mathbb{1}_B(y)\mathbb{1}_A(x')\mathbb{1}_B(y') \\
&= E(A,B)
\end{aligned}$$

(ii) évident

(iii) Le résultat découle d'un simple calcul :

$$\begin{aligned}
E(A, A^{-1}) &= |\{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid a_1 a_2^{-1} = a_3 a_4^{-1}\}| \\
&= |\{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid a_2^{-1} a_4 = a_1^{-1} a_3\}| \\
&= E(A^{-1}, A).
\end{aligned}$$

(iv) Le point (v) découle de l'exercice ci-dessous, en prenant $X = A \times B$ et $\phi : (a,b) \mapsto ab$.

(v) Pour faire voir (vi), on pose

$$S = \{(a,b) \mid ab \text{ a au moins } \frac{1}{2K}|A|^{1/2}|B|^{1/2} \text{ représentations sous la forme } a'b'\}.$$

Il est clair que $|A \cdot_S B| \leq 2K|A|^{1/2}|B|^{1/2}$. De plus,

$$\frac{|A|^{3/2}|B|^{3/2}}{K} \leq E(A,B) \leq |S||A|^{1/2}|B|^{1/2} + \frac{1}{2K}|A|^{1/2}|B|^{1/2}|A||B|$$

donc $|S| \geq \frac{|A||B|}{2K}$.

□

Exercice 33. Soient X et Y deux ensembles finis et $\varphi : X \to Y$. On note $E_\varphi = |\{(x_1, x_2) \in X \times X \mid \varphi(x_1) = \varphi(x_2)\}|$. Montrer que $|\varphi(X)| \geq \frac{|X|^2}{E_\varphi}$.

Exercice 34. Montrer que $E(B, A) \neq E(A, B)$ en général.

L'intérêt principal de l'énergie multiplicative provient du lemme ci-dessous, qui permet de construire des ensembles à petit doublement à partir d'ensembles A et B dont l'énergie multiplicative $E(A, B)$ est grande.

Lemme 3.10 (Balog-Szemerédi-Gowers, énergie multiplicative)**.** *Soit $K \geq 2$ un paramètre, et A, B deux parties finies d'un groupe G telles que*

$$E(A, B) \geq \frac{1}{K}|A|^{\frac{3}{2}}|B|^{\frac{3}{2}}.$$

Alors il existe $A' \subset A$ et $B' \subset B$ tels que

(i) $|A'| \geq K^{-O(1)}|A|$ *et* $|B'| \geq K^{-O(1)}|B|$ *;*

(ii) $|A'B'| \leq K^{O(1)}|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}$.

Ce lemme découle d'un résultat de théorie des graphes dû aux mêmes auteurs.

Lemme 3.11 (Balog-Szemerédi-Gowers, chemins de longueur 3)**.** *Soit $n \in \mathbb{N}$, $K \geq 2$, et $A \sqcup B$ un graphe biparti, avec $|A|, |B| \leq n$. On note E l'ensemble des arêtes, et on suppose que $|E| \geq \frac{n^2}{K}$. Alors, il existe des ensembles $A' \subset A$ et $B' \subset B$ tels que*

(i) $|A'| \geq K^{-O(1)}|A|$ *et* $|B'| \geq K^{-O(1)}|B|$ *;*

(ii) pour tout $(a, b) \in A' \times B'$, il existe au moins $K^{-O(1)}n^2$ chemins de longueur 3 entre a et b.

Remarque. Attention ! Les chemins qui relient $(a, b) \in A' \times B'$ peuvent passer par des points hors de $A' \sqcup B'$.

Notations. Pour $x \in A \sqcup B$, on note $V(x)$ l'ensemble des voisins de x. Pour $X \subset A \sqcup B$ on note $V(X) = \cap_{x \in X} V(x)$ l'ensemble des voisins communs à tous les points de X.

Exercice 35. Nous dirons qu'un sous-graphe $A' \sqcup B'$ dans $A \sqcup B$ est *totalement connecté* si toute paire de points $(a, b) \in A' \times B'$ est reliée par une arête.

1. Montrer que s'il existe A', B' satisfaisant le point (i) et tels que le sous-graphe $A' \sqcup B'$ soit totalement connecté, alors on a bien le point (ii) ci-dessus.
2. Sous les hypothèses du lemme, construire $A' \sqcup B'$ totalement connecté tel que $|A'||B'| \geq \frac{n}{K}$.
3. Sous les hypothèses du lemme, construire $A' \sqcup B'$ totalement connecté tel que $|A'| \geq 2$ et $|B'| \geq \frac{n}{K^3}$.
4. Sous les hypothèses du lemme, construire $A' \sqcup B'$ totalement connecté tel que $\min(|A'|, |B'|) \geq \frac{\log n}{2 \log K}$.

5. Montrer que sous les hypothèses du lemme, il n'existe pas nécessairement $A' \sqcup B'$ totalement connecté satisfaisant (i). (*Indication :* Considérer un graphe aléatoire.)
6. Le lemme ci-dessus implique qu'il existe un sous-graphe $A' \sqcup B'$ qui vérifie (i) et qui est totalement connecté pour les chemins de longueur 3. Vérifier ce résultat directement.

Démonstration du lemme 3.11. Pour $x \in A \sqcup B$, nous noterons $V(x)$ l'ensemble des voisins de x. Pour que tous les éléments de B aient beaucoup d'arêtes, on commence par restreindre le graphe à $A \sqcup B_0$, où

$$B_0 = \{b \in B \mid |V(b)| \geq \frac{n}{2K}\}.$$

Le nombre total d'arêtes vérifie encore $|E| \geq \frac{n^2}{2K}$.

On considère maintenant un point x choisi aléatoirement uniformément dans A. Alors,

$$\mathbb{E}[|V(x)|] = \frac{1}{|A|}|E| \geq \frac{1}{n}|E| \geq \frac{n}{2K}.$$

Nous dirons que deux éléments b, b' dans B sont *mal connectés* si l'ensemble $V(b, b')$ de leurs voisins communs vérifie $|V(b, b')| \leq \frac{n}{128K^3}$. Notons $N(x)$ le nombre de couples (b, b') d'éléments de $V(x)$ mal connectés. Si (b, b') est un tel couple, on a évidemment $x \in V(b, b')$, et la probabilité de cet événement est donc majorée par $\frac{1}{128K^3}$. Par conséquent,

$$\mathbb{E}[N(x)] \leq \frac{n^2}{128K^3}.$$

Soit $Z(x) \subset V(x)$ l'ensemble des éléments b mal connectés à au moins $\frac{n}{32K^2}$ éléments de $V(x)$. Naturellement, $N(x) \geq |Z(x)|\frac{n}{32K^2}$, et donc

$$\mathbb{E}[|Z(x)|] \leq \frac{n}{4K}.$$

Cela permet de choisir un point $x \in A$ tel que $B' = V(x) \backslash Z(x)$ vérifie $|B'| \geq \frac{n}{4K}$. Ensuite, on pose

$$A' = \{a \in A \mid |V(a) \cap B'| \geq \frac{n}{16K^2}\}.$$

Soit R le nombre d'arêtes partant de B'. Alors,

$$\frac{n^2}{8K^2} = \frac{n}{2K}\frac{n}{4K} \leq R \leq |A'|n + \frac{n^2}{16K^2},$$

et donc $|A'| \geq \frac{n^2}{16K^2}$.

Reste à minorer le nombre de chemins de longueur 3 entre deux points $a \in A'$ et $b \in B'$. Pour cela, on remarque que l'ensemble

$$M = \{b' \in B' \mid (b, b') \text{ est mal connecté}\}$$

vérifie $|M| \leq \frac{n}{32K^2}$, tandis que $|V(a) \cap B'| \geq \frac{n}{16K^2}$, et donc il existe au moins $\frac{n}{16K^2}$ éléments b' dans $V(a)$ bien connectés à b. Pour chaque tel b', il existe au moins $\frac{n}{256K^3}$ chemins de longueur 2 entre b et b', donc le nombre de chemins de longueur 3 entre a et b est minoré par $\frac{n^2}{2^{12}K^5}$, ce qu'il fallait démontrer. □

Démonstration du lemme 3.10. D'après le dernier point de la proposition 3.9, il existe $S \subset A \times B$ tel que, notant $\pi : (a,b) \mapsto ab$ l'application produit,

$$|S| \geq \frac{|A||B|}{K^{O(1)}} \quad \text{et} \quad |\pi(S)| \leq K^{O(1)}|A|^{\frac{1}{2}}|B|^{\frac{1}{2}}.$$

Comme $|S| \geq \frac{|A||B|}{K^{O(1)}}$, il existe $b \in B$ tel que $|\{a \in A \mid (a,b) \in S\}| \geq \frac{|A|}{K^{O(1)}}$. Mais l'application π est injective en restriction à cette fibre, et donc $|A| \leq K^{O(1)}|B|$. Échangeant les rôles de A et B, on a aussi $|B| \leq K^{O(1)}|A|$. Posant alors $n = \max(|A|,|B|)$, on observe que les hypothèses du lemme sont satisfaites pour le graphe biparti $A \sqcup B$ défini par la partie S, avec la constante $K^{O(1)}$.

Soient A' et B' les ensembles qui résultent de l'application du lemme. On a bien sûr $|A'| \geq K^{-O(1)}|A|$ et $|B'| \geq K^{-O(1)}|B|$. Notons que $A'B' \subset (A \cdot_S B)(A \cdot_S B)^{-1}(A \cdot_S B)$. En effet, si $(a,b) \in A' \times B'$, il existe un chemin $a \leftrightarrow b' \leftrightarrow a' \leftrightarrow b$ et donc

$$ab = ab'(a'b')^{-1}a'b \in (A \cdot_S B)(A \cdot_S B)^{-1}(A \cdot_S B).$$

De plus, tout produit ab dans $A'B'$ admet $K^{-O(1)}n^2$ représentations de cette forme. Donc

$$|A'B'| \leq K^{O(1)}n^{-2}|A \cdot_S B|^3 \leq K^{O(1)}n = K^{O(1)}|A|^{1/2}|B|^{1/2}.$$

□

3.3 Le lemme de Petridis et ses applications

Pour conclure la démonstration de la proposition 3.7, nous utiliserons aussi le lemme suivant, dû à Petridis.

Lemme 3.12 (Petridis)**.** *Soit A et B deux parties finies de G et $B_0 \subset B$ tel que le rapport $\frac{|AB_0|}{|B_0|}$ soit minimal ; on note K_0 ce rapport. Alors, pour toute partie X de G,*

$$|AB_0X| \leq K_0|B_0X|.$$

Démonstration. On procède par récurrence sur le cardinal de X.
Si $|X| = 1$, alors $|AB_0X| = |AB_0| = K_0|B_0| = K_0|B_0X|$.
Supposons le résultat connu pour $|X| = n \geq 1$. Soit X une partie de cardinal $n+1$ et x un élément de X. Notons $X' = X \backslash \{x\}$. Alors,

$$\begin{aligned} |AB_0X| &= |AB_0X'| + |AB_0x| - |(AB_0X') \cap (AB_0x)| \\ &\leq K_0|B_0X'| + K_0|B_0x| - |(AB_0X') \cap (AB_0x)| \\ &\leq K_0|B_0X'| + K_0|B_0x| - |AZx|, \end{aligned}$$

où $Z = \{z \in B_0 | Azx \subset AB_0X'\}$. On remarque que $Z \supset B_0 \cap B_0X'x^{-1}$ et que par conséquent $|Z| \geq |B_0x \cap (B_0X')|$. De plus, comme $Z \subset B$, par définition de K_0, $|AZ| \geq K_0|Z|$. L'inégalité ci-dessus donne alors ce qu'on veut :

$$\begin{aligned} |AB_0X| &\leq K_0|B_0X'| + K_0|B_0x| - K_0|(B_0x) \cap (B_0X')| \\ &= K_0|B_0X|. \end{aligned}$$

Ceci achève la récurrence. □

Nous pouvons maintenant démontrer la caractérisation des ensembles à petit doublement à partir des sous-groupes approximatifs.

Démonstration de la proposition 3.7. Par l'inégalité de Ruzsa $d(A,A) \leq d(A,B)+d(B,A) \leq 2\log K$ i.e. $|AA^{-1}| \leq K^2|A|$. Par conséquent, $E(A,A^{-1}) = E(A^{-1},A) \geq K^{-C}|A|^3$. D'après le lemme 3.10 appliqué à $A = A^{-1}$ et $B = A$, il existe une partie $A_1 \subset A$ telle que $|A_1| \geq K^{-C}|A|$ et $|A_1^{-1}A_1| \leq K^{-C}|A|$. Comme $A_1 \subset A$, on a aussi $|A_1A_1^{-1}| \leq K^{-C}|A|$.

Soit $A_2 \subset A_1$ tel que le rapport $\frac{|A_1A_2^{-1}|}{|A_2|}$ soit minimal. D'après le lemme de Petridis, pour toute partie X finie

$$|A_1A_2^{-1}X| \leq K^{O(1)}|A_2^{-1}X|. \tag{3.1}$$

Cela implique en particulier que $|A_1| \leq K^{O(1)}|A_2|$. De plus, $A_2 \subset A_1$ donc $|A_2^{-1}A_2| \leq K^{O(1)}|A_2|$. Soit alors $A_3 \subset A_2$ tel que le rapport $\frac{|A_2^{-1}A_3|}{|A_3|}$ soit minimal. D'après le lemme de Petridis, pour tout X fini,

$$|A_2^{-1}A_3X| \leq K^{O(1)}|A_3X| \leq K^{O(1)}|A_2X|. \tag{3.2}$$

Cela implique $|A_2| \leq K^{O(1)}|A_3|$. De plus, appliquant successivement les inégalités (3.2), (3.1) et (3.2) ci-dessus,

$$\begin{aligned}
|(A_3^{-1}A_3)^2A_3^{-1}| &\leq |A_2^{-1}A_3(A_3^{-1}A_3A_3^{-1})| \\
&\leq K^{O(1)}|A_3A_3^{-1}A_3A_3^{-1}| \\
&\leq K^{O(1)}|A_1A_2^{-1}A_3A_3^{-1}| \\
&\leq K^{O(1)}|A_2^{-1}A_3A_3^{-1}| \\
&\leq K^{O(1)}|A_3A_3^{-1}| \\
&\leq K^{O(1)}|A_3^{-1}|.
\end{aligned}$$

Le lemme de recouvrement de Ruzsa montre donc que $(A_3^{-1}A_3)^2 \subset (A_3^{-1}A_3)T$, avec $|T| \leq K^{O(1)}$ et $H = A_3^{-1}A_3$ est donc un sous-groupe $K^{O(1)}$-approximatif. Comme $|AA_3^{-1}| \leq |AA^{-1}| \leq K^{O(1)}|A_3|$, on a aussi, par recouvrement de Ruzsa, $A \subset XH$, avec $|X| \leq K^{O(1)}$. Enfin, $|A_3B| \leq |AB| \leq K^{O(1)}|A_3|$ donc $B \subset HY$, avec $|Y| \leq K^{O(1)}$. □

Une autre application du lemme de Petridis est une variante de la proposition 3.3 pour les groupes abéliens, dans laquelle il suffit de supposer que l'ensemble considéré est à petit doublement. Ce résultat est connu sous le nom d'inégalité de Plünnecke. Si $(G,+)$ est un groupe abélien, et $A, B \subset G$, on note

$$A+B = \{a+b\ ;\ a \in A,\ b \in B\}$$

et pour $n \in \mathbb{N}^*$,

$$nA = \{a_1 + \cdots + a_n\ ;\ a_i \in A\}.$$

Théorème 3.13 (Inégalité de Plünnecke)**.** *Si A et B sont deux parties d'un groupe abélien $(G,+)$ vérifiant $|A+B| \leq K|B|$, alors, pour tous entiers naturels m et n,*

$$|mA - nA| \leq K^{m+n}|B|.$$

Démonstration. Choisissons $B_0 \subset A$ tel que $\frac{|A+B_0|}{|B_0|} = K_0$ soit minimal ; en particulier $K_0 \leq K$. Grâce au lemme de Petridis appliqué successivement, on obtient

$$|B_0 + mA| = |A + B_0 + (m-1)A| \leq K_0|B_0 + (m-1)A| \leq \cdots \leq K_0^m|B_0|,$$

et de même,

$$|B_0 + nA| \leq K_0^n|B_0|.$$

On utilise alors l'inégalité triangulaire de Ruzsa pour conclure :

$$|mA - nA||B_0| \leq |B_0 + mA||B_0 + nA| \leq K_0^{m+n}|B_0|^2$$

d'où

$$|mA - nA| \leq K^{m+n}|B|.$$

□

Exercice 36. Soit G un groupe abélien et $X, Y_1, \ldots, Y_k$ des parties finies de G. On suppose que $|X + Y_i| \leq K_i|X|$, $i = 1, \ldots, k$.

1. Montrer qu'il existe $Z_0 \subset X$ tel que $|Z_0| \geq \frac{|Z_0|}{2}$ et $|Z_0 + Y_1 + Y_2| \leq 4K_1K_2|Z_0|$. (*Indication :* Utiliser le lemme de Petridis, et si $|X_0| < \frac{|X|}{2}$, appliquer une nouvelle fois le lemme à l'ensemble $X \setminus X_0$, et ainsi de suite.)
2. Montrer par récurrence qu'il existe $Z \subset X$ tel que $|Z + Y_1 + \cdots + Y_k| \ll_k (\prod_{i=1}^k K_i)|Z|$.
3. Montrer qu'on peut en outre imposer $|Z| \geq \frac{|X|}{2}$ à la question précédente.

3.4 Somme-produit dans les corps finis

Étant donné un groupe ambiant G, nous avons commencé à étudié au paragraphe précédent les parties A telles que $|A^2| \leq K|A|$. Dans ce paragraphe, nous nous placerons dans un cadre un peu plus riche, en supposant que la partie A est incluse dans un anneau. On dispose alors de deux opérations, somme et produit, et l'on cherche donc à comprendre quelles parties A peuvent satisfaire simultanément $|A^2| \leq K|A|$ et $|A+A| \leq K|A|$. Le premier résultat remarquable sur le sujet est sans doute le théorème suivant, montré par Erdős et Szemerédi [8] en 1983.

Théorème 3.14 (Somme-produit dans $\mathbb{Z}$)**.** *Il existe $\tau > 0$ tel que pour toute partie finie $A \subset \mathbb{Z}$,*

$$|A + A| + |A \cdot A| \geq |A|^{1+\tau}.$$

Solymosi [14] à démontré que le théorème était valable pour $\tau = \frac{1}{3}$. Le meilleur exposant, égal à $\frac{1}{3} + \frac{2}{1167}$ a été obtenu récemment par Rudnev et Stevens [13]. La conjecture ci-dessous sur la valeur optimale de l'exposant τ, due à Erdős et Szemerédi, n'a pas encore été résolue.

Conjecture (Erdős et Szemerédi)**.** *Pour tout $\varepsilon > 0$, il existe n_0 tel que si $|A| \geq n_0$, on peut prendre $\tau = 1 - \varepsilon$ dans l'inégalité ci-dessus.*

Nous allons montrer une généralisation du résultat ci-dessus valable dans un corps quelconque.

Théorème 3.15 (Somme-produit dans un corps quelconque)**.** *Il existe $\tau > 0$ tel que l'énoncé suivant soit vérifié.*
Soit A une partie finie d'un corps F quelconque. Si $|A+A| + |A \cdot A| \leq K|A|$, alors on a l'alternative suivante :

- *soit $|A| \leq K^{O(1)}$;*
- *soit il existe un sous-corps fini F_A tel que $|F_A| \leq K^{O(1)}|A|$ et $A \subset xF_A \cup X$ pour $x \in A$ et $|X| \leq K^{O(1)}$.*

Exercice 37. Vérifier que cet énoncé est optimal, au sens où tout ensemble qui vérifie l'une des deux conditions du théorème vérifie $|A+A|+|A\cdot A| \leq K^{O(1)}|A|$.

Exercice 38 (Somme-produit en caractéristique nulle)**.** Montrer qu'il existe $\tau > 0$ tel que si F est un corps de caractéristique nulle et $A \subset F$, alors $|A + A| + |A \cdot A| \geq |A|^{1+\tau}$. En déduire le résultat d'Erdős et Szemerédi cité ci-dessus.

Exercice 39 (Somme-produit dans les corps finis)**.** On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Montrer qu'il existe $\tau > 0$ tel que pour tout $\mathbb{F}_p$ et tout $A \subset \mathbb{F}_p$,

$$|A + A| + |A \cdot A| \geq |A|(\min\{|A|, \frac{p}{|A|}\})^{\tau}.$$

Que peut-on dire dans un corps fini $\mathbb{F}_q$, $q = p^n$ quelconque ?

Avant de chercher à démontrer le théorème 3.15, il est plus facile d'étudier les parties qui ne croissent pas sous l'action simultanée de l'addition et de la multiplication. La démonstration du théorème 3.15 se ramènera à ce cas particulier, qui d'ailleurs est souvent suffisant dans les applications.

Théorème 3.16 (Somme-produit, deuxième version)**.** *Soit F un corps quelconque. Si $A \subset F$ est une partie finie telle que $|A + AA| \leq K|A|$, alors $|A| \leq K^{O(1)}$ ou il existe un sous-corps fini $B \supset A$ tel que $|B| \leq K^{O(1)}|A|$.*

Démonstration. Quitte à remplacer A par $A \cup \{0, 1\}$, on peut supposer que $0, 1 \in A$. On considère alors

$$B = \{\frac{a_1 - a_2}{a_3 - a_4} \mid a_i \in A,\ a_3 - a_4 \in F \setminus \{0\}\}.$$

Premier cas : B est stable par $\cdot$ et $+$.
Comme B est fini, et contient 0 et 1, c'est un sous-corps de F, et $B \supset A$. Pour chaque $x \in B$, fixons une représentation $x = \frac{a_x}{b_x}$, avec $a_x \in A - A$ et $b_x \in (A - A) \setminus \{0\}$. Notons aussi $A^* = A \setminus \{0\}$. L'application

$$\begin{array}{ccc} A^* \times B & \to & A(A-A) \times (A-A)A \\ (a, x) & \mapsto & (aa_x, b_x a) \end{array}$$

est injective, donc

$$|B| \leq \frac{|AA - AA|^2}{|A^*|} \leq K^{O(1)}|A|.$$

Second cas : $\exists x, y \in B :\ x + y \notin B$ ou $xy \notin B$.
Selon le cas, écrivons $x + y = \frac{e_1}{e_2}$ ou $xy = \frac{e_1}{e_2}$, avec $e_1 \in [(A - A)(A - A) + (A - A)(A - A)] \cup (A - A)(A - A)$ et $e_2 \in (A - A)(A - A) \setminus 0$, et considérons l'application

$$\begin{array}{rccc} \phi : & A \times A & \to & e_1 A + e_2 A \\ & (a, b) & \mapsto & e_1 a + e_2 b. \end{array}$$

Si $a - a' \neq 0$, l'égalité $e_1 a + e_2 b = e_1 a' + e_2 b'$ implique $\frac{e_1}{e_2} = \frac{b'-b}{a-a'} \in B$. Par contraposée, $\phi(a,b) = \phi(a',b')$ implique $a = a'$, puis $b = b'$. Donc cette application est injective,

$$|e_1 A + e_2 A| = |\phi(A \times A)| = |A|^2.$$

Pour conclure, reste à voir que $|e_1 A + e_2 A| \leq K^{O(1)}|A|$. Cela découle de la proposition 3.17 ci-dessous. □

Proposition 3.17. *Soit A une partie finie d'un anneau telle que $|A + AA| \leq K|A|$. Pour $s \in \mathbb{N}^*$, on note $\langle A \rangle_s$ l'ensemble des sommes ou différences d'au plus s produits d'au plus s éléments de A. Alors $|\langle A \rangle_s| \leq K^{O_s(1)}|A|$.*

Démonstration. Par l'inégalité de Plünnecke et le lemme de recouvrement de Ruzsa, la condition $|A + AA| \leq K|A|$ implique que $A - A$ est un sous-groupe $K^{O(1)}$-approximatif.

Montrons d'abord que pour tout $x \in \langle A \rangle_s$, il existe $X_{x,s}$ tel que $|X_{x,s}| \leq K^{O_s(1)}$ et $xA \subset A - A + X_{x,s}$. Cela se voit par récurrence sur s. Pour $s = 1$, par recouvrement de Ruzsa, $AA \subset A - A + X$, pour $|X| \leq K^{O(1)}$, donc le résultat est clair. Ensuite, on remarque que si $xA \subset A - A + X_{x,s}$ et $yA \subset A - A + X_{y,s}$, alors $(x+y)A \subset xA + yA \subset A - A + A - A + X_{x,s} + X_{y,s} \subset A - A + X_{x+y,s+1}$ et de même, $(x-y)A \subset A - A + X_{x-y,s+1}$. Enfin, $xyA \subset xA - xA + xX_{y,s} \subset A - A + A - A + X_{x,s} - X_{x,s} + xX_{y,s} \subset A - A + X_{xy,s+1}$.

Montrons maintenant par récurrence qu'il existe $X_s \subset \langle A \rangle_s$ tel que $|X_s| \leq K^{O_s(1)}$ et $A^s \subset A - A + X_s$. Cela a déjà été vu pour $s = 2$. Supposons donc le résultat démontré pour $s \geq 2$. Alors,

$$A + A^{s+1} \subset A + A(A - A + X_s) \subset A + AA - AA + AX_s.$$

Par la première partie de la démonstration, $AX_s \subset A - A + X'$, où $X' = \cup_{x \in X_s} X_{x,s}$, donc $|A + A^{s+1}| \leq |A + AA - AA + A - A + X'| \leq K^{O_s(1)}|A|$ puis $A^{s+1} \subset A - A + X_{s+1}$, par inégalité de Ruzsa.

Pour conclure, notons que $\langle A \rangle_{s+1} = A^{s+1} \pm \cdots \pm A^{s+1} \subset A - A + \cdots + A - A + X_s \pm \cdots \pm X_s$ et donc $|\langle A \rangle_{s+1}| \leq K^{O_s(1)}|A|$. □

L'exercice suivant donne une version de l'énoncé valable dans un anneau quelconque. On s'aperçoit qu'en général, il faut comprendre la position de A par rapport aux éléments non inversibles de l'anneau.

Exercice 40 (Somme-produit dans un anneau)**.** Soit R un anneau quelconque, dont on note $R^\times$ les éléments inversibles et $R_0 = R \setminus R^\times$. Si $A \subset R$ est une partie finie telle que $|A + AA| \leq K|A|$, montrer que l'une des deux assertions suivantes est vérifiée :

— $|(A - A) \cap R_0| \geq K^{-O(1)}|A|$;

— il existe un sous-anneau fini $B \supset A$ tel que $|B| \leq K^{O(1)}|A|$.

Pour démontrer le théorème 3.15, nous aurons besoin du lemme suivant, qui est en quelque sorte analogue à la classification des ensembles à petit doublement par les sous-groupes approximatifs.

Lemme 3.18 (Katz-Tao)**.** *Soit A une partie finie d'un corps quelconque F telle que $|A + A| + |A \cdot A| \leq K|A|$. Il existe une partie $A' \subset A$ telle que*

1. $|A'| \geq K^{-O(1)}|A|$;

2. $|A'+A'| \leq K^{O(1)}|A|$ *et* $|A'A'+A'A'| \leq K^{O(1)}|A|$.

Démonstration. Soit $A \subset \mathbb{F}$ et $K \geq 2$ tel que $|A+A|+|AA| \leq K|A|$. Par l'inégalité de Schwarz,

$$|AA|\left(\sum_{z\in AA}(\sum_{x\in A}\mathbb{1}_{xA}(z))^2\right) \geq \left(\sum_{z\in AA}\sum_{x\in A}\mathbb{1}_{xA}(z)\right)^2 = (\sum_{x\in A}|xA|)^2 = |A|^4$$

et comme $|AA| \leq K|A|$,

$$\sum_{x,y\in A}|xA\cap yA| \geq \frac{|A|^3}{K}.$$

Fixons $b \in A$ tel que $\sum_{x\in A}|xA\cap bA| \geq \frac{|A|^2}{K}$, puis

$$A' = \{a \in A \mid |aA\cap bA| \geq \frac{|A|}{2K}\}.$$

Notons que $|A'| \geq \frac{|A|}{2K}$. De plus, pour $a \in A'$, si $X = |aA\cap bA|$, alors $|X| \geq \frac{|A|}{2K}$ et

$$\begin{cases} |X+aA| \leq K|A| \leq 2K^2|X| \\ |X+bA| \leq K|A| \leq 2K^2|X|. \end{cases}$$

Soit $a_1,a_2,a_3,a_4 \in A'$. Par recouvrement de Ruzsa, $a_iA \subset b(A-A)+X$ pour un certain X tel que $|X| \leq K^{O(1)}$, et donc $(a_1a_2-a_3a_4)A \subset b^2(A-A)+Y$ avec $|Y| \leq K^{O(1)}$. Par conséquent, pour chaque $c \in A'A'-A'A'$, il existe $y \in Y$ tel que pour au moins $K^{-O(1)}|A|$ éléments $a \in A$, $ca \in b^2(A-A)+y$. Donc il existe au moins $K^{-O(1)}|A|$ différences $cu = c(a-a')$ telles que $cu \in b^2(A-A+A-A)$. En d'autres termes, l'élément c admet au moins $K^{-O(1)}|A|$ représentations de la forme $\frac{v}{u}$, avec $v \in A-A$ et $u \in b^2(A-A+A-A)$. Comme $|A| \leq |A-A| \leq |b^2(A-A+A-A)| \leq K^{O(1)}|A|$, cela implique $|A'A'-A'A'| \leq K^{O(1)}|A|$. □

Nous pouvons enfin démontrer le théorème 3.15.

Démonstration du théorème 3.15. Soit $A \subset F$ tel que $|A+A|+|A\cdot A| \leq K|A|$. D'après le lemme 3.18, il existe une partie $A' \subset A$ telle que $|A'| \geq K^{-O(1)}|A|$, $|A'-A'| \leq K^{O(1)}|A|$ et $|A'A'-A'A'| \leq K^{O(1)}|A|$. Fixons $a \in A' \setminus \{0\}$ et notons $\bar{A} = a^{-1}A'$. Si $|\bar{A}| \leq K^{O(1)}$ on a aussi $|A| \leq K^{O(1)}$. Sinon, comme $\bar{A}$ vérifie les hypothèses du théorème 3.16 pour $K^{O(1)}$, le corps F_A engendré par $\bar{A}$ vérifie $|F_A| \leq K^{O(1)}|A|$. De plus, par recouvrement de Ruzsa, $A \subset aF_A+X$ et $A \subset F_AY$, avec $|X|,|Y| \leq K^{O(1)}$. Donc A est inclus dans une réunion d'au plus $K^{O(1)}$ ensembles de la forme $a[(F_A+x)\cap F_Ay]$. Or, si $f+x=gy$ et $f'+x=g'y$, on trouve $f-f'=(g-g')y$ puis $f-f'=g-g'=0$ ou $y=\frac{f-f'}{g-g'} \in F_A$. Cela montre que l'intersection $(F_A+x)\cap F_Ay$ est égale à F_A, vide, ou réduite à un singleton, et le théorème est démontré. □

Exercice 41. Soit p un nombre premier, et soit $A \subset \mathbb{F}_p$ tel que $|A| > \sqrt{p}$.

1. Montrer que tout élément $x \in \mathbb{F}_p$ peut s'écrire $x = \frac{a_1-a_2}{a_3-a_4}$.
2. En déduire qu'il existe $b = \frac{b_1-b_2}{b_3-b_4}$ tel que $|\{(a_1,a_2,a_3,a_4) \in A^{\times 4} \mid b = \frac{a_1-a_2}{a_3-a_4}\}| \leq \frac{|A|^4}{p}$.
3. Conclure que $A(A-A)+A(A-A) = \mathbb{F}_p$.

Chapitre 4

Combinatoire discrétisée

Le théorème somme-produit démontré au chapitre précédent illustre bien les méthodes de la combinatoire additive, mais pour montrer la propriété du trou spectral dans les groupes compacts, nous aurons besoin de résultats analogues où le cardinal est remplacé par le nombres de recouvrement à une certaine échelle δ. À l'origine, ces énoncés ont été introduits par Katz et Tao [11] pour résoudre la conjecture suivante :

Conjecture (Erdős-Volkmann, résolue par Edgar-Miller [7])**.** *Tout sous-anneau borélien strict dans $\mathbb{R}$ est de dimension de Hausdorff nulle.*

Exercice 42. Le but de cet exercice est de démontrer le théorème d'Edgar et Miller.

1. (Théorème de Marstrand) Soit $A \subset \mathbb{R}^n$ borélien tel que $\dim_H A > 1$. Montrer que pour presque toute forme linéaire $\phi : \mathbb{R}^n \to \mathbb{R}$, $\phi(A)$ est de mesure de Lebesgue positive.
2. Soit A un sous-anneau mesurable de $\mathbb{R}$ tel que $\dim_H A > 0$. Justifier qu'il existe $n \in \mathbb{N}^*$ et $\phi \in (\mathbb{R}^n)^*$ tels que $\phi(A^n) = \mathbb{R}$.
3. Montrer que si n est l'entier minimal tel qu'il existe $\phi \in (\mathbb{R}^n)^*$ tel que $\phi(A^n) = \mathbb{R}$, alors $\phi : A^n \to \mathbb{R}$ est injective. En déduire que $n = 1$ puis $A = \mathbb{R}$.

Peu après la publication de la solution d'Edgar et Miller, Jean Bourgain [2] est parvenu à mettre en œuvre la méthode suggérée par Katz et Tao [11] et a donné une autre démonstration de la conjecture, beaucoup plus technique, mais avec l'avantage de montrer au passage la proposition suivante.

Proposition 4.1 (Bourgain)**.** *Pour tout $\sigma > 0$, il existe $\tau > 0$ tel que l'énoncé suivant soit vérifié. Soit $A \subset \mathbb{R}$ une partie borélienne de dimension de Hausdorff $\dim_H A \in [\sigma, 1-\sigma]$. Alors $\dim_H A + AA \geq \varepsilon + \dim_H A$.*

La démonstration de cette proposition passe par celle d'un énoncé analogue « discrétisé », conjecturé par Katz et Tao [11], qui a trouvé depuis de nombreuses autres applications. Pour $A \subset \mathbb{R}$ et $\delta > 0$, on note $N(A, \delta)$ le cardinal minimal d'un recouvrement de A par des boules de rayons δ.

Théorème 4.2 (Somme-produit discrétisé dans $\mathbb{R}$)**.** *Pour tout $\sigma \in]0, 1[$, il existe $\varepsilon > 0$ tel que l'énoncé suivant soit vérifié pour tout $\delta > 0$ suffisamment petit.*

Soit $A \subset [0, 1]$ tel que

(i) $N(A,\delta) \leq \delta^{-\sigma-\varepsilon}$;
(ii) pour tout $\rho \geq \delta$ *et tout* $x \in [0,1]$, $N(A \cap B(x,\rho),\delta) \leq \delta^{-\varepsilon}\rho^{\sigma}N(A,\delta)$.
Alors

$$N(A+AA,\delta) \geq \delta^{-\varepsilon}N(A,\delta).$$

En termes de dimension de Hausdorff, la première condition sur l'ensemble A correspond à l'inégalité $\dim_H A \leq \sigma+\varepsilon$, et la deuxième à $\dim_H A \geq \sigma-\varepsilon$. Il est toutefois important de noter qu'il ne suffit pas de supposer $N(A,\delta) \geq \delta^{-\sigma+\varepsilon}$, il faut aussi éviter que l'ensemble A soit concentré dans une boule $B(x,\rho)$, avec $\rho \in [\delta, \delta^{\varepsilon}]$.

Exercice 43. Montrer que pour $A = B(\frac{1}{2}, \delta^{1-\sigma})$, on a $N(A,\delta) = \delta^{-\sigma}$ et pourtant $N(A+AA,\delta) \leq 2N(A,\delta)$.

À l'aide d'un analogue discrétisé du lemme 3.18, on peut montrer que sous les hypothèses du théorème 4.2, on a même

$$\max(N(A+A,\delta), N(AA,\delta)) \geq \delta^{-\varepsilon}N(A,\delta).$$

Cependant, l'exercice suivant montre que l'énoncé analogue pour la dimension de Hausdorff n'est pas valable. À une échelle δ fixée, l'un des deux ensembles $A+A$ ou AA croît, mais on peut construire A de sorte qu'à certaines échelles arbitrairement petites, $A+A$ ne croît pas et à d'autres, AA ne croît pas ; cela permet de majorer la dimension de Hausdorff de chaque ensemble.

Exercice 44. Soit $\alpha \in]0,1[$ fixé.

1. Construire une partie $A \subset \mathbb{R}$ telle que $\dim_H A = \dim_H A+A = \alpha$. Montrer qu'on peut même imposer que A soit un sous-groupe.
2. Montrer qu'il existe une partie $A \subset \mathbb{R}$ telle que $\dim_H A = \dim_H AA = \alpha$.
3. Construire $A \subset [1,2]$ tel que $\dim_H A = \dim_H A+A = \dim_H AA = \alpha$.

Le premier but de ce chapitre est de donner une démonstration simple du théorème 4.2, basée sur un article récent de Guth, Katz et Zahl [9]. Nous étudierons ensuite les généralisations de ce résultat à $\mathbb{C}$ ou à d'autres algèbres matricielles de dimension supérieures. Mais pour commencer, nous expliquons brièvement comment les résultats du chapitre précédent s'adaptent à notre nouveau cadre de travail.

4.1 Nombres de recouvrement

Définition 4.3. Soit E un espace métrique, $X \subset E$ et $\delta > 0$. Le *nombre de recouvrement* de X à l'échelle δ — ou *entropie de* X à l'échelle δ — noté $N(X,\delta)$ est le cardinal minimal d'un recouvrement de X par des boules de rayon δ :

$$N(X,\delta) = \min\{N \in \mathbb{N} \mid \exists (x_i)_{1\leq i\leq N} : X \subset \bigcup_{i=1}^{N} B(x_i,\delta)\}.$$

Dans la suite, nous considérons seulement le cas où E est un espace vectoriel réel de dimension finie, isométrique à $\mathbb{R}^d$ muni de sa norme euclidienne. L'espace métrique E est donc doublant : il existe une constante C_E, telle que pour tout $x \in E$ et tout $r > 0$, la boule $B(x,r)$ peut être recouverte par C_E boules de rayon $\frac{r}{2}$. En d'autres termes, $N(B(x,r), \frac{r}{2}) = O(1)$. Cela implique en particulier la proposition suivante, dont nous ferons souvent usage implicitement.

Proposition 4.4. *Soit E un espace métrique doublant. À certaines constantes multiplicatives près ne dépendant que que E, si $X \subset E$ et X' est une partie δ-séparée maximale dans X, alors $N(X,\delta) \asymp |X'|$.*

Démonstration. Par la propriété de doublement, $N(X, \frac{\delta}{2}) \ll N(X,\delta)$. Or, si $X \subset \bigcup_{i=1}^{N} B(x_i, \frac{\delta}{2})$, chaque boule $B(x_i, \frac{\delta}{2})$ contient au plus un élément de X', car X' est δ-séparé. Cela montre déjà que $|X'| \ll N(X,\delta)$. Réciproquement, par maximalité de X', on a $X \subset \bigcup_{x\in X'} B(x, 2\delta)$, donc $|X'| \geq N(X, 2\delta) \gg N(X,\delta)$. □

Exercice 45. Vérifier que tout espace vectoriel normé de dimension finie est un espace métrique doublant. Donner un exemple d'espace métrique non doublant.

Les propriétés de combinatoire additive démontrées au paragraphe 3.1 ci-dessus pour le cardinal admettent toutes des analogues pour le nombre de recouvrement à l'échelle δ. Nous utiliserons en particulier le résultat suivant.

Théorème 4.5 (Inégalités de Plünnecke)**.** *Soient $X, Y_1, \dots, Y_k$ des parties bornées de $\mathbb{R}^d$. On suppose que $N(X + Y_i, \delta) \leq K_i N(X,\delta)$, $i = 1, \dots, k$. Il existe alors $X_0 \subset X$ tel que $N(X_0 + Y_1 + \cdots + Y_k, \delta) \ll_k (\prod_{i=1}^{k} K_i) N(X_0,\delta)$. On peut de plus supposer que $N(X_0,\delta) \gg N(X,\delta)$.*

Démonstration. Nous allons nous ramener à l'inégalité de Plünnecke usuelle en approchant chaque partie par une partie finie de $G = \delta\mathbb{Z}^d$. Pour $Z \subset \mathbb{R}^d$, on pose $Z' = G \cap Z^{(2\delta)}$, de sorte que $N(Z,\delta) \asymp |Z'|$. Par conséquent, pour chaque i, $|X' + Y_i'| \ll K_i |X'|$. D'après l'exercice 36, il existe $X_0' \subset X'$ tel que $|X_0'| \geq \frac{X'}{2}$ et $|X_0' + Y_1' + \cdots + Y_k'| \ll_k (\prod_{i=1}^{k} K_i)|X_0'|$. Par suite, posant $X_0 = X \cap (X_0')^{(2\delta)}$, on a bien $N(X_0,\delta) \geq |X_0'| \gg N(X,\delta)$ et

$$N(X_0 + Y_1 + \cdots + Y_k, \delta) \ll_k (\prod_{i=1}^{k} K_i) N(X_0,\delta).$$

□

On laisse au lecteur le soin de vérifier que l'inégalité et de lemme de recouvrement de Ruzsa peuvent aussi s'adapter pour les nombres de recouvrement, ainsi que la proposition suivante.

Proposition 4.6. *Soit E une algèbre réelle de dimension finie et A une partie de E telle que $N(A+AA,\delta) \leq K N(A,\delta)$. Pour $s \in \mathbb{N}^*$, on note $\langle A\rangle_s$ l'ensemble des sommes ou différences d'au plus s produits d'au plus s éléments de A. Alors $N(\langle A\rangle_s,\delta) \leq K^{O_s(1)} N(A,\delta)$.*

4.2 Somme-produit discrétisé dans $\mathbb{R}$

Comme ce cas est un peu plus facile, nous commencerons par l'étude du phénomène somme-produit discrétisé dans $\mathbb{R}$. Notre but est de démontrer le théorème 4.2 énoncé ci-dessus. La démonstration est analogue à celle du théorème somme-produit démontré au chapitre précédent, mais un nouveau paramètre intervient, qui sert à contrôler les éléments mal inversibles, i.e. trop proches de zéro, dans $A - A$.

Démonstration du théorème 4.2. Soit $A \subset [0,1]$ une partie satisfaisant les conditions suivantes :

(i) $N(A,\delta) \leq \delta^{-\sigma+\varepsilon}$;

(ii) pour tout $\rho \geq \delta$ et tout $x \in [0,1]$, $N(A \cap B(x,\rho),\delta) \leq \delta^{-\varepsilon}\rho^{\sigma}N(A,\delta)$;

(iii) $N(A+AA,\delta) \leq \delta^{-\varepsilon}N(A,\delta)$.

On veut en déduire une inégalité $\varepsilon \geq \varepsilon(\sigma) > 0$. Fixons un paramètre $\gamma \in]0, \frac{1}{2}[$ dont la valeur exacte sera choisie plus tard, et posons $A_0 = A - A$, $A_1 = A_0 \setminus B(0,\delta^{\gamma})$ et $B = A_0 A_1^{-1}$. En d'autres termes,

$$B = \left\{ \frac{a_1 - a_2}{a_3 - a_4} \ ; \ a_i \in A, \ |a_3 - a_4| > \delta^{\gamma} \right\}.$$

Notons que par l'inégalité de Ruzsa $N(A_0,\delta) \ll \delta^{3\varepsilon}N(A,\delta)$ tandis que l'hypothèse de non concentration implique $N(A_1,\delta) \geq N(A,\delta)(1-\delta^{\sigma\gamma}) \gg N(A,\delta)$.

Posons $\delta_1 = \delta^{1-2\gamma}$. L'ensemble B doit vérifier l'une des deux assertions suivantes :

(A) $B^{(2\delta_1)} \supset [0,1]$.

(B) Il existe $b \in B \cap [0,1]$ tel que $d(\frac{b}{2}, B) \geq \delta_1$ ou $d(\frac{b+1}{2}, B) \geq \delta_1$.

Supposons en effet que la seconde assertion ne soit pas vérifiée. Alors, l'ensemble $B^{(2\delta_1)}$ est stable par les opérations $b \mapsto \frac{b}{2}$ et $b \mapsto \frac{b+1}{2}$. Comme $0, 1 \in B^{(2\delta_1)}$, cela implique que $B^{(2\delta_1)}$ contient tous les rationnels dyadiques, puis que $B^{(2\delta_1)} = [0,1]$.

Premier cas : (A)
Soit B' une partie δ_1-séparée dans B, et pour chaque $x \in B'$ fixons une représentation $x = \frac{a_x}{b_x}$, avec $a_x \in A_0$ et $b_x \in A_1$. Soit aussi A' une partie δ_1-séparée dans $\tilde{A} = A \setminus B(0,\delta^{\gamma})$. L'application

$$\begin{array}{ccc} A' \times B' & \to & AA_0 \times A_1 A \\ (a,x) & \mapsto & (aa_x, b_x a) \end{array}$$

est injective à échelle δ. En effet, si

$$\left\{ \begin{array}{l} aa_x = u + O(\delta) \\ b_x a = v + O(\delta) \end{array} \right.$$

alors $x = \frac{a_x}{b_x} = \frac{u}{v} + O(\frac{\delta}{ab_x}) = \frac{u}{v} + O(\delta_1)$ donc $x \in B'$ est uniquement déterminé, puis $a = \frac{v}{b_x} + O(\frac{\delta}{b_x}) = \frac{v}{b_x} + O(\delta_1)$ est aussi déterminé dans A'. Par conséquent,

$$N(B,\delta_1) \leq \frac{N(AA-AA,\delta)^2}{|A'|}.$$

Or, d'après l'inégalité de Ruzsa, $N(AA-AA,\delta) \leq \delta^{2\varepsilon}N(A,\delta)$, et par ailleurs, $|A'| \asymp N(\tilde{A},\delta_1) \geq \delta^{2\gamma}N(\tilde{A},\delta) \gg \delta^{2\gamma}N(A,\delta)$, donc

$$N(B,\delta_1) \ll \delta^{-2\gamma-4\varepsilon}N(A,\delta).$$

Mais comme $B^{(2\delta_1)} \supset [0,1]$, on a aussi $N(B,\delta_1) \gg \delta_1^{-1} = \delta^{-1+2\gamma}$ et donc

$$\delta^{-\sigma-\varepsilon} \geq N(A,\delta) \geq \delta^{-1+4\gamma+4\varepsilon},$$

d'où $\varepsilon \geq \frac{1-\sigma-4\gamma}{5}$.

Second cas : (B)

Si $d(\frac{b}{2}, B) \geq \delta_1$, on écrit $\frac{b}{2} = \frac{e_1}{e_2}$, avec $e_1 \in A_0$ et $e_2 \in 2A_1$, tandis que si $d(\frac{b+1}{2}, B) \geq \delta_1$, on écrit $\frac{b+1}{2} = \frac{e_1}{e_2}$, avec $e_1 \in A_0 + A_1$ et $e_2 \in 2A_1$.

Nous voulons d'abord minorer $N(e_1A + e_2A, \delta)$. Soit

$$Q = \{(a_1, a_2, a_3, a_4) \in A^{\times 4} \mid e_2a_1 + e_1a_4 = e_2a_2 + e_1a_3 + O(\delta)\}.$$

L'inégalité qui définit Q implique

$$\left|\frac{a_1 - a_2}{a_3 - a_4} - \frac{e_1}{e_2}\right| \ll \delta|e_2|^{-1}|a_3 - a_4|^{-1} \leq \delta^{1-\gamma}|a_3 - a_4|^{-1}.$$

Comme $d(\frac{e_1}{e_2}, B) \geq \delta^{1-2\gamma}$, on doit avoir $|a_3 - a_4| \leq \delta^\gamma$. Si a_4 est connu à δ près, par non concentration, il y a au plus $\delta^{\gamma\sigma-\varepsilon}N(A, \delta)$ possibilités pour a_3. Ensuite, si a_1, a_3, a_4 sont connus à δ près, comme

$$a_2 + \frac{e_1}{e_2}a_3 = a_1 + \frac{e_1}{e_2}a_4 + O(|e_2|^{-1}\delta)$$

l'hypothèse de non concentration montre qu'il y a au plus $|e_2|^{-\sigma}\delta^{\sigma-\varepsilon}N(A, \delta)$ possibilités pour a_2, et ainsi

$$N(Q, \delta) \leq |e_2|^{-\sigma}\delta^{\sigma(1+\gamma)-2\varepsilon}N(A, \delta)^4.$$

Avec l'inégalité de Schwarz cela donne

$$N(e_1A_1 + e_2A_1, \delta) \geq \frac{N(A, \delta)^4}{N(Q, \delta)} \geq |e_2|^\sigma\delta^{-\sigma(1+\gamma)+2\varepsilon}.$$

D'autre part, on peut aussi majorer

$$\begin{aligned} N(e_1A + e_2A, \delta) &\leq \frac{1}{N(A, |e_2|)}N(A + e_1A + e_2A, \delta) \\ &\leq \delta^{-\varepsilon}|e_2|^\sigma N(A + AA - AA + AA - AA + AA - AA, \delta) \\ &\leq |e_2|^\sigma\delta^{-10\varepsilon}N(A, \delta). \end{aligned}$$

Ainsi, $N(A, \delta) \geq \delta^{-\sigma(1+\gamma)+12\varepsilon}$ et donc $\varepsilon \geq \frac{\sigma\gamma}{10}$.

Dans les deux cas, $\varepsilon \geq \min(\frac{1-\sigma-4\gamma}{5}, \frac{\sigma\gamma}{12})$, et choisissant $\gamma = \frac{1-\sigma}{4+\frac{5\sigma}{12}}$, on obtient $\varepsilon \geq \frac{\sigma(1-\sigma)}{53}$. □

Exercice 46. Vérifier que le théorème ci-dessus n'est pas valable pour les ensembles $A \subset B_{\mathbb{C}}(0, 1)$. Quelle hypothèse faudrait-il ajouter ?

Nous aurons même besoin d'une version du théorème somme-produit valable dans le corps $\mathbb{C}$ des complexes. La démonstration est quasiment identique à celle présentée dans dans le cas réel, mais évidemment, il faut ajouter comme hypothèse que l'ensemble A n'est pas inclus dans un δ^ε-voisinage de $\mathbb{R}$.

Théorème 4.7 (Somme-produit discrétisé dans $\mathbb{C}$)**.** *Pour tout $\sigma \in]0, 2[$, il existe $\varepsilon > 0$ tel que l'énoncé suivant soit vérifié pour tout $\delta > 0$ suffisamment petit.*

Soit $A \subset B_{\mathbb{C}}(0, 1)$ tel que

(i) $N(A,\delta) \leq \delta^{-\sigma-\varepsilon}$;

(ii) pour tout $\rho \geq \delta$ *et tout* $x \in [0,1]$, $N(A \cap B(x,\rho),\delta) \leq \delta^{-\varepsilon}\rho^{\sigma}N(A,\delta)$;

(iii) il existe $a \in A$ *tel que* $d(a,\mathbb{R}) \geq \delta^{\varepsilon}$.

Alors

$$N(A+AA,\delta) \geq \delta^{-\varepsilon}N(A,\delta).$$

Démonstration. Soit $A \subset B_{\mathbb{C}}(0,1)$ une partie satisfaisant les conditions suivantes :

(i) $N(A,\delta) \leq \delta^{-\sigma+\varepsilon}$;

(ii) pour tout $\rho \geq \delta$ et tout $x \in [0,1]$, $N(A \cap B(x,\rho),\delta) \leq \delta^{-\varepsilon}\rho^{\sigma}N(A,\delta)$;

(iii) il existe $a \in A$ tel que $d(a,\mathbb{R}) \geq \delta^{\varepsilon}$;

(iv) $N(A+AA,\delta) \leq \delta^{-\varepsilon}N(A,\delta)$.

On veut en déduire une inégalité $\varepsilon \geq \varepsilon(\sigma) > 0$. Fixons un paramètre $\gamma \in]0,\frac{1}{2}[$ dont la valeur exacte sera choisie plus tard, et posons $A_0 = A - A$, $A_1 = A_0 \setminus B(0,\delta^{\gamma})$ et $B = A_0A_1^{-1}$. En d'autres termes,

$$B = \left\{ \frac{a_1-a_2}{a_3-a_4} \ ; \ a_i \in A, \ |a_3-a_4| > \delta^{\gamma} \right\}.$$

Notons que par l'inégalité de Ruzsa $N(A_0,\delta) \ll \delta^{2\varepsilon}N(A,\delta)$ tandis que l'hypothèse de non concentration implique $N(A_1,\delta) \geq N(A,\delta)(1-\delta^{\sigma\gamma}) \gg N(A,\delta)$.

Posons $\delta_1 = \delta^{1-2\gamma}$. L'ensemble B doit vérifier l'une des deux assertions suivantes :

(A) $B^{(2\delta_1)} \supset [0,1]$.

(B) Il existe $b \in B \cap [0,1]$ tel que $d(\frac{b}{2},B) \geq \delta_1$ ou $d(\frac{b+1}{2},B) \geq \delta_1$.

Supposons en effet que la seconde assertion ne soit pas vérifiée. Alors, l'ensemble $B^{(2\delta_1)}$ est stable par les opérations $b \mapsto \frac{b}{2}$ et $b \mapsto \frac{b+1}{2}$. Comme $0,1 \in B^{(2\delta_1)}$, cela implique que $B^{(2\delta_1)}$ contient tous les rationnels dyadiques, d'où $B^{(2\delta_1)} \supset [0,1]$.

Premier cas : (A)

Soit $a \in A$ tel que $d(a,\mathbb{R}) \geq \delta^{\varepsilon}$. Comme $[0,1] \subset B^{(2\delta_1)}$, on a

$$N(aB+B,\delta_1) \gg \delta^{\varepsilon}\delta_1^{-2} = \delta^{-2+4\gamma+\varepsilon}.$$

D'autre part, notant $A_2 = A(A-A)(A-A) + (A-A)(A-A)$ et $A_3 = (A-A)(A-A) \setminus B(0,\delta^{2\gamma})$,

$$aB + B \subset A_2A_3^{-1} = C$$

Soit C' une partie δ_1-séparée dans C, et pour chaque $x \in C'$ fixons une représentation $x = \frac{a_x}{b_x}$, avec $a_x \in A_2$ et $b_x \in A_3$. Soit aussi A' une partie δ_1-séparée dans $\tilde{A} = A \setminus B(0,\delta^{\gamma})$. Soit enfin $A_4 = AA_2$ et $A_5 = AA_3$. L'application

$$\begin{array}{ccc} A' \times C' & \to & A_4 \times A_5 \\ (a,x) & \mapsto & (aa_x, b_xa) \end{array}$$

est injective à échelle δ. En effet, si

$$\left\{ \begin{array}{l} aa_x = u + O(\delta) \\ b_xa = v + O(\delta) \end{array} \right.$$

alors $x = \frac{a_x}{b_x} = \frac{u}{v} + O(\frac{\delta}{ab_x}) = \frac{u}{v} + O(\delta_1)$ donc $x \in C'$ est uniquement déterminé, puis $a = \frac{u}{a_x} + O(\frac{\delta}{a_x}) = \frac{u}{a_x} + O(\delta_1)$ est aussi déterminé. Par conséquent,

$$N(C, \delta_1) \leq \frac{N(A_4, \delta)N(A_5, \delta)}{|A'|} \ll \delta^{-4\gamma-98\varepsilon} N(A, \delta) \ll \delta^{-\sigma-4\gamma-99\varepsilon}.$$

Ainsi

$$\delta^{-\sigma-4\gamma-99\varepsilon} \geq \delta^{-2+4\gamma+\varepsilon},$$

et donc $\varepsilon \geq \frac{2-\sigma-8\gamma}{100}$.

Second cas : (B)

Si $d(\frac{b}{2}, B) \geq \delta_1$, on écrit $\frac{b}{2} = \frac{e_1}{e_2}$, avec $e_1 \in A_0$ et $e_2 \in 2A_1$, tandis que si $d(\frac{b+1}{2}, B) \geq \delta_1$, on écrit $\frac{b+1}{2} = \frac{e_1}{e_2}$, avec $e_1 \in A_0 + A_1$ et $e_2 \in 2A_1$.

Nous voulons d'abord minorer $N(e_1A + e_2A, \delta)$. Soit

$$Q = \{(a_1, a_2, a_3, a_4) \in A_1^{\times 4} \mid e_2a_1 + e_1a_4 = e_2a_2 + e_1a_3 + O(\delta)\}.$$

L'inégalité qui définit Q implique

$$\left|\frac{a_1 - a_2}{a_3 - a_4} - \frac{e_1}{e_2}\right| \ll \delta |e_2|^{-1} |a_3 - a_4|^{-1} \leq \delta^{1-\gamma} |a_3 - a_4|^{-1}.$$

Comme $d(\frac{e_1}{e_2}, B) \geq \delta^{1-2\gamma}$, on doit avoir $|a_3 - a_4| \leq \delta^\gamma$. Si a_4 est connu à δ près, par non concentration, il y a au plus $\delta^{\gamma\sigma-\varepsilon} N(A, \delta)$ possibilités pour a_3. Ensuite, si a_1, a_3, a_4 sont connus à δ près, comme

$$a_2 + \frac{e_1}{e_2} a_3 = a_1 + \frac{e_1}{e_2} a_4 + O(|e_2|^{-1}\delta)$$

l'hypothèse de non concentration montre qu'il y a au plus $|e_2|^{-\sigma}\delta^{\sigma-\varepsilon} N(A, \delta)$ possibilités pour a_2, et ainsi

$$N(Q, \delta) \leq |e_2|^{-\sigma} \delta^{\sigma(1+\gamma)-2\varepsilon} N(A, \delta)^4.$$

Avec l'inégalité de Schwarz cela donne

$$N(e_1A_1 + e_2A_1, \delta) \geq \frac{N(A, \delta)^4}{N(Q, \delta)} \geq |e_2|^\sigma \delta^{-\sigma(1+\gamma)+2\varepsilon}.$$

D'autre part, on peut aussi majorer

$$\begin{aligned} N(e_1A + e_2A, \delta) &\leq \frac{1}{N(A, |e_2|)} N(A + e_1A + e_2A, \delta) \\ &\leq \delta^{-\varepsilon} |e_2|^\sigma N(A + 4AA - 4AA, \delta) \\ &\leq |e_2|^\sigma \delta^{-10\varepsilon} N(A, \delta). \end{aligned}$$

Ainsi, $N(A, \delta) \geq \delta^{-\sigma(1+\gamma)+12\varepsilon}$ et donc $\varepsilon \geq \frac{\sigma\gamma}{12}$.

Dans tous les cas, $\varepsilon \geq \min(\frac{2-\sigma-8\gamma}{100}, \frac{\sigma\gamma}{12})$, et choisissant γ convenablement, on obtient $\varepsilon \geq \frac{\sigma(2-\sigma)}{300}$. □

Remarque. Le théorème 4.7 est encore valable si l'on remplace l'hypothèse de non concentration par l'hypothèse un peu plus faible

$$\forall \rho \geq \delta, \quad N(A,\rho) \geq \delta^{\varepsilon}\rho^{-\sigma}.$$

Cela découle simplement de l'observation suivante : si A vérifie cette hypothèse et est concentré à une certaine échelle ρ, i.e. vérifie $N(A \cap B(x,\rho),\delta) \geq \delta^{-2\varepsilon}\rho^{\sigma}N(A,\delta)$ pour une certaine boule $B(x,\rho)$, alors

$$N(A+A,\delta) \gg N(A,\rho)N(A\cap B(x,\rho),\delta) \geq \delta^{-\varepsilon}N(A,\delta),$$

et la conclusion du théorème somme-produit est vérifiée.

Un argument formel permet même d'affaiblir encore l'hypothèse de non concentration, ce qui nous sera utile plus tard.

Théorème 4.8 (Somme-produit discrétisé dans $\mathbb{C}$)**.** *Pour tout $\sigma \in]0,2[$ et tout $\kappa > 0$, il existe $\varepsilon > 0$ tel que l'énoncé suivant soit vérifié pour tout $\delta > 0$ suffisamment petit.*

Soit $A \subset B_{\mathbb{C}}(0,1)$ tel que

(i) $N(A,\delta) \leq \delta^{-\sigma-\varepsilon}$;

(ii) pour tout $\rho \geq \delta$, $N(A,\rho) \geq \delta^{\varepsilon}\rho^{-\kappa}$;

(iii) il existe $a \in A$ *tel que* $d(a,\mathbb{R}) \geq \delta^{\varepsilon}$.

Alors

$$N(A+AA,\delta) \geq \delta^{-\varepsilon}N(A,\delta).$$

Démonstration. Le théorème 4.7 et la remarque ci-dessus montrent qu'il existe $\varepsilon > 0$ tel que pour tout $\sigma' \in [\kappa,\sigma]$, pour tout δ suffisamment petit, si un ensemble A vérifie les conditions

(i) $N(A,\delta) \leq \delta^{-\sigma'-\varepsilon_0}$;

(ii) il existe $a \in A$ tel que $d(a,\mathbb{R}) \geq \delta^{\varepsilon_0}$;

(iii) $N(A+AA,\delta) \leq \delta^{-\varepsilon_0}N(A,\delta)$;

alors il existe $\rho \geq \delta$ tel que $N(A,\rho) \leq \delta^{\varepsilon_0}\rho^{-\sigma'}$. Par conséquent, si $N(A+AA,\delta) \leq \delta^{-\varepsilon_0}N(A,\delta)$, il existe $\delta_1 \geq \delta$ tel que

$$N(A,\delta_1) \leq \delta^{\varepsilon_0}\delta_1^{-\sigma} \leq \delta_1^{-\sigma+\varepsilon_0}.$$

Si $N(A+AA,\delta_1) \leq \delta_1^{-\varepsilon_0}N(A,\delta_1)$, on obtient de même $\delta_2 \geq \delta_1$ tel que

$$N(A,\delta_2) \leq \delta_1^{\varepsilon_0}\delta_2^{-\sigma+\varepsilon_0} \leq \delta_2^{-\sigma+2\varepsilon_0}.$$

Et ainsi de suite, tant que $N(A+AA,\delta_{k-1}) \leq \delta_{k-1}^{-\varepsilon_0}N(A,\delta_{k-1})$, il existe $\delta_k \geq \delta_{k-1}$ tel que

$$N(A,\delta_k) \leq \delta_{k-1}^{\varepsilon_0}\delta_k^{-\sigma+(k-1)\varepsilon_0} \leq \delta_k^{-\sigma+k\varepsilon_0}.$$

Par conséquent, pour $k \leq \lfloor \frac{\sigma}{\varepsilon_0} \rfloor$, on doit avoir

$$N(A+AA,\delta_k) \geq \delta_k^{-\varepsilon_0}N(A,\delta_k).$$

Notons que $\delta^{\varepsilon}\delta_1^{-\kappa} \leq N(A,\delta_1) \leq \delta^{\varepsilon_0}\delta_1^{-\sigma}$ et donc $\delta_1 \leq \delta^{\frac{\varepsilon_0}{2(\sigma-\kappa)}}$ si $\varepsilon > 0$ est suffisamment petit. De même, $\delta_k \leq \delta_{k-1}^{\frac{\varepsilon_0}{2(\sigma-\kappa)}}$, et par conséquent

$$\delta_k \leq \delta_{k-1}^{\frac{\varepsilon_0}{2(\sigma-\kappa)}} \leq \cdots \leq \delta^{\left(\frac{\varepsilon_0}{2(\sigma-\kappa)}\right)^k}$$

et donc $\delta_k^{-\varepsilon_0} \geq \delta^{-2\varepsilon}$ si $\varepsilon > 0$ est choisi de sorte que $2\varepsilon < \varepsilon_0 \left(\frac{\varepsilon_0}{\kappa}\right)^k$. Soit alors $B_{\delta_k} = B(x, \delta_k)$ une boule de A tel que $N(A \cap B_{\delta_k}, \delta)$ soit maximal. Cela implique en particulier $N(A \cap B_{\delta_k}, \delta) \geq \frac{N(A,\delta)}{N(A,\delta_k)}$ et par conséquent

$$\begin{aligned} N(A+A+AA,\delta) &\geq N(A \cap B_{\delta_k}, \delta) N(A + AA, \delta_k) \\ &\geq \frac{N(A,\delta)}{N(A,\delta_k)} N(A + AA, \delta_k) \\ &\geq \delta_k^{-\varepsilon_0} N(A, \delta). \end{aligned}$$

Pour conclure, on utilise l'inégalité de Ruzsa

$$N(A+A+AA,\delta) \leq \left(\frac{N(A+AA,\delta)}{N(A,\delta)}\right)^2 N(A,\delta).$$

□

Enfin remarquons que si $A \subset B_{\mathbb{C}}(0,1)$ est une partie non concentrée, une application itérée du théorème 4.8 montre qu'à l'aide d'un nombre borné de sommes et de produits d'éléments de A, on peut obtenir tout élément dans une boule $B(0, \delta^{\varepsilon_0})$, où $\varepsilon_0 > 0$ est arbitrairement petit.

Proposition 4.9. *Étant donnés $\kappa, \varepsilon_0 > 0$, il existe $s \in \mathbb{N}^*$ tel que l'énoncé suivant soit vérifié pour tout $\delta > 0$ suffisamment petit.*

Soit $A \subset B_{\mathbb{C}}(0,1)$ vérifiant :

1. *il existe $a \in A$ tel que $d(a, \mathbb{R}) \geq \delta^{\varepsilon}$;*
2. *pour tout $\rho \geq \delta$, $N(A, \rho) \geq \delta^{\varepsilon} \rho^{-\kappa}$.*

Alors, notant $\langle A \rangle_s$ l'ensemble des éléments qui s'écrivent comme somme d'au plus s produits de longueur au plus s d'éléments de A,

$$N(\langle A \rangle_s, \delta) \geq \delta^{-2+\varepsilon_0}.$$

Démonstration. Il suffit de choisir un entier ℓ tel que $\kappa + (\ell - 1)\varepsilon > 2 - \varepsilon_0$ et d'appliquer le théorème 4.8 successivement aux parties A_k définies par

$$\begin{cases} A_0 = A \\ \forall k \geq 1, \quad A_k = A_{k-1} + A_{k-1} A_{k-1}. \end{cases}$$

Comme $N(A_0, \delta) \geq \delta^{-\kappa-\varepsilon}$, on obtient $N(A_\ell, \delta) \geq \delta^{-2+\varepsilon_0}$, et comme $A_\ell \subset \langle A \rangle_s$ pour $s = 2^{2^\ell}$, le résultat est démontré. □

Chapitre 5

Analyse dans les groupes de Lie

Soit G un groupe de Lie compact à centre fini. On munit G de la distance associée à une métrique riemmanienne invariante à gauche et à droite. Si X est une partie de G et $\delta > 0$ une échelle, on note $N(X, \delta)$ le cardinal minimal d'un recouvrement de X par des boules de rayon δ. On note aussi $X^{(\delta)}$ le δ-voisinage de X dans G. La démonstration du théorème 2.21 se fonde sur l'énoncé combinatoire suivant.

Théorème 5.1 (Théorème produit discrétisé)**.** *Soit G un groupe de Lie compact à centre fini. Il existe un voisinage de l'identité U dans G tel que pour tout $\kappa > 0$, il existe $\varepsilon > 0$ tel que l'énoncé suivant soit vérifié.*

Soit $A \subset U$ une partie vérifiant

(i) $N(A, \delta) \leq \delta^{-\dim G + \sigma}$;

(ii) pour tout sous-groupe fermé distingué connexe $N \lhd G$,

$$\forall \rho \geq \delta, \quad N(\pi_{G/N}(A), \rho) \geq \delta^{\varepsilon} \rho^{-\kappa};$$

(iii) pour tout sous-groupe fermé connexe $H < G$, il existe $x \in A$ tel que $d(x, H) \geq \delta^{\varepsilon}$.

Alors,

$$N(AAA, \delta) \geq \delta^{-\varepsilon} N(A, \delta).$$

Remarque. L'hypothèse de compacité n'est pas essentielle, l'important est que l'algèbre de Lie $\mathfrak{g}$ du groupe soit parfaite, i.e. vérifie $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$.

Comme la démonstration de ce résultat général est trop longue pour être incluse dans ce cours, nous la présenterons seulement pour le groupe $G = \mathrm{SO}_3(\mathbb{R})$ des rotations en dimension 3. Ce cas particulier nécessitera déjà une grande partie des outils d'analyse et de combinatoire nécessaires à la démonstration dans le cas général. Notons que $\mathrm{SO}_3(\mathbb{R})$ est localement isomorphe à $\mathrm{SU}_2(\mathbb{R}) = \{g \in \mathrm{SL}_2(\mathbb{C}) \mid gg^* = 1\}$, le théorème produit est donc le même pour chacun de ces deux groupes, et comme les calculs sont un peu plus simples dans $\mathrm{SU}_2(\mathbb{R})$, nous nous placerons dans ce cadre pour le restant du chapitre. Les seuls sous-groupes connexes de $G = \mathrm{SU}_2(\mathbb{R})$ sont des tores de dimension 1, qui ne sont pas distingués ; dans ce cadre, le résultat que nous voulons démontrer s'énonce donc comme suit.

Théorème 5.2 (Théorème produit discrétisé dans $\mathrm{SU}_2(\mathbb{R})$)**.** *Soit $G = \mathrm{SU}_2(\mathbb{R})$ et $\sigma, \kappa > 0$ des paramètres fixés. Il existe $\varepsilon > 0$ tel que l'énoncé suivant soit vérifié.*

Soit $A \subset G$ une partie vérifiant

(i) $N(A, \delta) \leq \delta^{-3+\sigma}$;

(ii) pour tout $\rho \geq \delta$, $N(A, \rho) \geq \delta^{\varepsilon} \rho^{-\kappa}$;

(iii) pour tout sous-groupe fermé connexe $H < G$, *il existe* $x \in A$ *tel que* $d(x, H) \geq \delta^{\varepsilon}$.

Alors,

$$N(AAA, \delta) \geq \delta^{-\varepsilon} N(A, \delta).$$

5.1 Construction d'un tore riche

L'idée de la démonstration du théorème 5.1 est de se ramener au phénomène somme-produit discrétisé dans $\mathbb{C}$. Le cas de $G = \mathrm{SU}_2(\mathbb{R})$ est un peu plus simple, car les tores maximaux sont de dimension 1, isomorphes au groupe des complexes de module 1. C'est la proposition suivante qui nous permettra construire, à partir d'un sous-groupe approximatif dans G, les parties non concentrées de $\mathbb{C}$ auxquelles nous appliquerons le théorème somme-produit.

Proposition 5.3 (Existence d'un tore riche)**.** *Soit $A \subset G$ tel que*

1. $\forall H < G,\ \exists a \in A : \quad d(a, H) \geq \delta^{\varepsilon}$;
2. $N(AAA, \delta) \leq \delta^{\varepsilon} N(A, \delta)$.

Il existe un tore T dans G tel que $N(A^6 \cap T^{(\delta^{1-O(\varepsilon)})}, \delta) \geq \delta^{O(\varepsilon)} N(A, \delta)^{\frac{1}{3}}$.

Commençons par un lemme sur les éléments qui stabilisent presque un vecteur dans une représentation linéaire.

Lemme 5.4. *Soit G un groupe de Lie compact et V une représentation linéaire de G.*

1. *Pour tout $v \in V$, il existe une constante $c > 0$ telle que pour tout $g \in G$, $d(gv, v) \geq c \cdot d(g, H_v)$, où $H_v = \operatorname{Stab} v$.*
2. *Si V ne contient pas de vecteur invariant, il existe une constante $C > 0$ telle que pour tout $v \in V$ unitaire, il existe un sous-groupe fermé strict H tel que pour tout $g \in G$, si $d(gv, v) \leq \varepsilon$, alors $d(g, H) \leq C\varepsilon$.*

Démonstration. Soit W un supplémentaire de $\mathfrak{h}$ dans $\mathfrak{g}$ et U un voisinage de 0 dans W tel que $Y \mapsto e^Y \cdot v$ soit un difféomorphisme de U sur son image. Il existe $c_0 > 0$ tel que si $d(g, H_v) < c_0$, on peut écrire $g = e^Y h$, avec $h \in H_v$ et $Y \in U$, d'où

$$d(gv, v) = d(e^Y v, v) \asymp \|Y\| \asymp d(g, H_v).$$

Comme par ailleurs, la fonction continue $g \mapsto \frac{d(gv,v)}{d(g,H_v)}$ est strictement positive sur le compact $d(g, H_v) \geq c_0$, on trouve bien qu'il existe $c > 0$ tel que pour tout $g \in G$, $d(gv, v) \geq c d(g, H_v)$. Cela montre la première partie du lemme.

Pour la seconde partie, fixons v_0 un vecteur unitaire dans V, D'après le premier point du lemme, pour tout x dans G, l'inégalité $d(gxv_0, xv_0) \leq \varepsilon$ implique $d(g, H_{xv_0}) \leq C_0\varepsilon$, pour une constante C_0 qui ne dépend que de v_0. Notons $\mathfrak{h}_0$

l'algèbre de Lie de $H_{v_0} = \operatorname{Stab} v_0$, et W_0 tel que $\mathfrak{g} = \mathfrak{h}_0 \oplus W_0$. Dans un voisinage U_{v_0} de v_0, tout vecteur v peut s'écrire $v = e^Y(v_0 + u)$, avec $Y \in W_0$ et $u \in (W_0 v_0)^\perp$, et cette écriture est unique. Supposons $d(gv, v) \leq \varepsilon$. On a alors $gv = ge^Y(v_0 + u)$ donc $\varepsilon \geq d(gv, v) \geq d(ge^Y v_0, e^Y v_0)$. Par conséquent, $d(g, H_{e^Y v_0}) \leq C_0\varepsilon$. Pour conclure, il suffit de prendre un recouvrement fini de la sphère unité dans V par des petits ouverts U_{v_0}. □

Exercice 47. Montrer que le sous-groupe H dans le deuxième point du lemme n'est pas nécessairement égal à $\operatorname{Stab} v$.

Lemme 5.5. *Soit $A \subset G$ à distance au moins ρ de tout sous-groupe. Il existe des éléments $g_1, g_2, g_3 \in A^2$ tels que le jacobien de l'application $\phi : g \mapsto (\operatorname{Tr} g_1 g, \operatorname{Tr} g_2 g, \operatorname{Tr} g_3 g)$ vérifie*

$$|J_\phi(1)| \geq \rho^{O(1)}.$$

Démonstration. Le jacobien $J_\phi(1)$ est égal au déterminant de l'application

$$\begin{array}{rccc} \phi\colon & M_2(\mathbb{C}) & \to & \mathbb{C}^4 \\ & X & \mapsto & (\operatorname{Tr} X, \operatorname{Tr} g_1 X, \operatorname{Tr} g_2 X, \operatorname{Tr} g_3 X) \end{array}$$

. Notons $g_0 = 1$ et commençons par fixer g_1 tel que $d(g_1, g_0) \geq \rho$. Ensuite, soit $V_1 = \mathbb{C}g_0 \oplus \mathbb{C}g_1 \leq M_2(\mathbb{C})$. Comme $V_1 \cap G = Z(g_1)$, il existe $g_2 \in A$ tel que $d(g_2, V_1) \geq \rho$. Soit alors $V_2 = \mathbb{C}g_0 \oplus \mathbb{C}g_1 \oplus \mathbb{C}g_2 \leq M_2(\mathbb{C})$. Cet espace n'est pas un idéal à gauche de $M_2(\mathbb{C})$ car il contient $g_0 = 1$ donc il existe $u \in A$ tel que $d(u, \operatorname{Stab}_G V_2) \geq \rho$. D'après le lemme 5.4, cela implique $d(uV_2, V_2) \gg \rho$ et donc, pour un certain $i \in \{0, 1, 2\}$, $d(ug_i, V_2) \gg \rho^{O(1)}$. Posant $g_3 = ug_i$ on obtient la famille souhaitée, car $\det \phi = \det(g_0, g_1, g_2, g_3)$. □

Démonstration de la proposition 5.3. D'après le lemme 5.5,

$$N(\operatorname{Tr}(AAA), \delta)^3 \geq \prod_{i=1}^{3} N(\operatorname{Tr}(g_i A), \delta) \geq \delta^{O(\varepsilon)} N(A, \delta)$$

i.e. $N(\operatorname{Tr}(AAA), \delta) \geq \delta^{O(\varepsilon)} N(A, \delta)^{\frac{1}{3}}$. Par le principe des tiroirs, il existe donc $a \in A^3$ tel que l'ensemble $C_a(\delta) = \{g \in G \mid |\operatorname{Tr}(g) - \operatorname{Tr}(a)| \leq \delta\}$ vérifie

$$N(A^9 \cap C_a(\delta), \delta) \leq \frac{N(A^9, \delta)}{N(\operatorname{Tr}(AAA), \delta)} \leq \delta^{-O(\varepsilon)} N(A, \delta)^{\frac{2}{3}}.$$

Mais $A^9 \cap C_a(\delta)$ contient tous les éléments gag^{-1}, $g \in A$, et il doit donc exister $g_0 \in A$ tel que

$$N(\{g \in A \mid gag^{-1} = g_0 a g_0^{-1} + O(\delta)\}, \delta) \geq \delta^{O(\varepsilon)} N(A, \delta)^{\frac{1}{3}}.$$

Comme $d(a, 1) \geq \delta^\varepsilon$, le lemme 5.4 montre que $gag^{-1} = g_0 a g_0^{-1} + O(\delta)$ implique $d(g_0^{-1} g, Z_a) = O(\delta^{1-\varepsilon})$, et donc

$$N(A^6 \cap T^{(O(\delta^{1-\varepsilon}))}, \delta) \geq \delta^{O(\varepsilon)} N(A, \delta)^{\frac{1}{3}}.$$

□

5.2 Croissance dans la représentation adjointe

Pour montrer l'expansion dans G, on commence par démontrer l'expansion via somme et produit dans la représentation adjointe. On rappelle que si $\mathfrak{g} = \mathrm{Lie}\, G$, la représentation adjointe $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$ est définie par

$$(\mathrm{Ad}\, g)X = gXg^{-1}.$$

Comme $G = \mathrm{SU}_2(\mathbb{R})$ est simple, la représentation adjointe est irréductible, et l'algèbre engendrée par $\mathrm{Ad}\, G$ dans $\mathrm{End}\, \mathfrak{g}$ est égale à $\mathrm{End}\, \mathfrak{g} \simeq M_3(\mathbb{R})$.

Proposition 5.6. *Soit $A \subset G$ tel que*

1. $\forall H < G,\ \exists a \in A : \quad d(a, H) \geq \delta^{\varepsilon}$;
2. $N(AAA, \delta) \leq \delta^{-\varepsilon} N(A, \delta)$.
3. $\forall \rho \geq \delta, \quad N(A, \rho) \geq \delta^{\varepsilon} \rho^{-\kappa}$;

On note $A_1 = \mathrm{Ad}\, A \subset \mathrm{End}\, \mathfrak{g}$ l'image de A par la représentation adjointe. Pour tout $\varepsilon_0 > 0$, il existe $s \in \mathbb{N}^*$ tel que

$$N(\langle A_1 \rangle_s, \delta) \geq \delta^{-9(1-\varepsilon_0)}.$$

Démonstration. D'après la proposition 5.3, les deux premières conditions sur A impliquent qu'il existe un tore T tel que

$$N(A^6 \cap T^{(\delta^{1-O(\varepsilon)})}, \delta) \geq \delta^{O(\varepsilon)} N(A, \delta)^{\frac{1}{3}}.$$

En outre, on peut supposer que l'ensemble $A' = T \cap (A^6)^{(\delta^{1-O(\varepsilon)})}$ vérifie, pour tout $\rho \geq \delta$,

$$N(A' \cap B_\rho, \delta) \leq \delta^{-O(\varepsilon)} \rho^{\frac{\kappa}{3}} N(A', \delta).$$

En effet, si ce n'est pas le cas, en conjugant par des éléments de A en bonne position, on obtient $N(A^C \cap B_\rho, \delta) \geq \delta^{-O(\varepsilon)} \rho^{\kappa} N(A', \delta)^3 \geq \delta^{-O(\varepsilon)} \rho^{\kappa} N(A, \delta)$, ce qui implique $N(A^{C+1}, \delta) \geq N(A, \rho) N(A^C \cap B_\rho, \delta) \geq \delta^{-O(\varepsilon)} N(A, \delta)$, et par l'inégalité de Ruzsa, cela contredit $N(AAA, \delta) \leq \delta^{-\varepsilon} N(A, \delta)$.

On considère maintenant l'image $T_1 = (\mathrm{Ad}\, T)$ du tore T dans la représentation adjointe $G \to \mathrm{GL}(\mathfrak{g}) \simeq \mathrm{GL}_3(\mathbb{R})$. La sous-algèbre engendrée par T_1 dans $M_3(\mathbb{R})$ s'identifie à $\mathbb{C}$, et dans cette identification, l'ensemble $A_1' = \mathrm{Ad}\, A'$ vérifie les hypothèses de la proposition 4.9 et donc, pour un certain s_0,

$$N(\langle A_1' \rangle_{s_0}, \delta) \geq \delta^{-2+\varepsilon_0}.$$

En particulier, il existe un vecteur unitaire $\eta \in M_3(\mathbb{R})$ tel que

$$N(\langle A_1' \rangle_{s_0} \cap \eta[0,1], \delta) \geq \delta^{-1+\varepsilon_0}.$$

Comme $G \times G$ agit irréductiblement sur $M_3(\mathbb{R})$ par $X \mapsto aXb^{-1}$ et A est à distance au moins δ^{ε} de tout sous-groupe dans G, le lemme 5.4 montre qu'il existe des éléments $a_i, b_i \in A^9$, $i = 1, \ldots, 9$ tels que, notant $V_i = \mathrm{Vect}\{a_j \eta b_j \ ;\ j \leq i\}$,

$$\forall i = 1, \ldots, 9, \quad d(a_i \eta b_i, V_{i-1}) \geq \delta^{O(\varepsilon)}.$$

Par suite, posant $s = 9(s_0 + 18)$,

$$\begin{aligned} N(\langle A_1 \rangle_s, \delta) &\geq \delta^{O(\varepsilon)} \prod_{i=1}^{9} N(a_i \langle A_1' \rangle_{s_0} b_i \cap a_i \eta b_i [0,1], \delta) \\ &\geq \delta^{O(\varepsilon)} \delta^{-9(1-\varepsilon_0)}. \end{aligned}$$

□

5.3 Application exponentielle

Commençons par une observation élémentaire sur l'application exponentielle au voisinage de 0. Soit $\rho \in]0, \frac{1}{2}[$ et $X, Y \in B_{\mathfrak{g}}(0, \rho)$. Alors, à l'ordre 1, $e^{X+Y} = e^X e^Y$ et donc

$$d(e^{X+Y}, e^X e^Y) = O(\rho^2).$$

Si l'on ajoute un terme correctif à $e^X e^Y$, on peut améliorer la précision de l'approximation. En effet, un calcul élémentaire montre que

$$\begin{aligned} e^{-2Y} e^{-2X} e^{2X+2Y} &= 1 + 2[X, Y] + O(\rho^3) \\ &= (e^X e^Y e^{-X} e^{-Y})^2 + O(\rho^3) \end{aligned}$$

et donc, notant $(g, h) = ghg^{-1}h^{-1}$,

$$d(e^{2X+2Y}, e^{2X} e^{2Y} (e^X, e^Y)^2) = O(\rho^3).$$

En poursuivant cette analyse grâce à la formule de Campbell-Hausdorff, on peut montrer par récurrence que pour tout $k \in \mathbb{N}^*$, il existe un entier m_k tel que $e^{m_k(X+Y)}$ soit approchable à l'ordre k par un mot en e^X et e^Y. C'est le contenu du lemme suivant.

Lemme 5.7. *Fixons $s \in \mathbb{N}^*$. Pour chaque $k \in \mathbb{N}^*$, il existe $m_k \in \mathbb{N}^*$ et un mot $w_k \in F_s$, le groupe libre sur s générateurs, tel que*

$$\forall X_1, \dots, X_s \in B_{\mathfrak{g}}(0, \rho), \quad d(\exp(m_k(X_1 + \cdots + X_s)), w(e^{X_1}, \dots, e^{X_s})) \leq \rho^{k+1}.$$

Démonstration. On construit le mot w_k et l'entier m_k par récurrence sur k. Pour $k = 1$, $w_1(x_1, \dots, x_s) = x_1 \dots x_s$ car $e^{X_1 + \cdots + X_s} = e^{X_1} \dots e^{X_s} + O(\rho^2)$. Supposons construits $m_{k-1} \in \mathbb{N}^*$ et w_{k-1} tels que

$$e^{m_{k-1}(X_1 + \cdots + X_s)} = w_{k-1}(e^{X_1}, \dots, e^{X_s}) + O(\rho^k).$$

D'après la formule de Campbell-Hausdorff, l'expression $\log w_{k-1}(e^{X_1}, \dots, e^{X_s})$ admet un développement à tout ordre en somme de crochets de Lie des éléments $X_1, \dots, X_s$; en particulier, on peut écrire à l'ordre k, pour certains rationnels r_i, $i \in [\![1, s]\!]^k$,

$$\begin{aligned} m_{k-1}(X_1 + \cdots + X_s) = \log w_{k-1}(e^{X_1}, \dots, e^{X_s}) \\ + \sum_{(i_1, \dots, i_k) \in [\![1,s]\!]^k} r_i [X_{i_1}, [X_{i_2}, [\dots, [X_{i_{k-1}}, X_{i_k}] \dots]]] + O(\rho^{k+1}). \end{aligned}$$

En multipliant par un dénominateur n_k commun à tous les r_i, on obtient $m_k, n_k \in \mathbb{N}^*$ et des entiers a_i tels que

$$\begin{aligned} m_k(X_1 + \cdots + X_s) = \log w_{k-1}(e^{X_1}, \dots, e^{X_s})^{n_k} \\ + \sum_{(i_1, \dots, i_k) \in [\![1,s]\!]^k} a_i [X_{i_1}, [X_{i_2}, [\dots, [X_{i_{k-1}}, X_{i_k}] \dots]]] + O(\rho^{k+1}). \end{aligned}$$

Notons que si $(x, y) = xyx^{-1}y^{-1}$, alors

$$[X_{i_1}, [X_{i_2}, [\dots, [X_{i_{k-1}}, X_{i_k}] \dots]]] = \log(e^{X_{i_1}}, (e^{X_{i_2}}, (\dots, (e^{X_{i_{k-1}}}, e^{X_{i_k}}) \dots))) + O(\rho^{k+1}).$$

On peut donc poser

$$w_k(x_1,\dots,x_s) = w_{k-1}(x_1,\dots,x_s)\prod_i (x_{i_1},(x_{i_2},(\dots,(x_{i_{k-1}},x_{i_k})\dots)))^{-a_i}$$

pour avoir le développement à l'ordre k souhaité. □

Partant du tore riche construit au paragraphe précédent, et grâce à l'action adjointe, ce lemme va nous permettre de transformer une expression somme-produit dans la représentation adjointe en un produit dans G, et ainsi, de démontrer le théorème 5.1.

Démonstration du théorème 5.1 pour $G = \mathrm{SU}_2(\mathbb{R})$. L'hypothèse de non concentration sur A permet d'obtenir $x = e^X \in AA^{-1}$ tel que $d(x,1) \asymp \delta^{\varepsilon_0}$. Si s est l'entier donné par la proposition 5.6, on a

$$N(\langle A_1\rangle_s \cdot X, \delta) \geq \|X\|\delta^6 N(\langle A_1\rangle_s, \delta) \geq \|X\|\delta^{-3+9\varepsilon_0} \geq \delta^{-3+10\varepsilon_0},$$

et comme l'application exponentielle est un difféomorphisme local au voisinage de l'identité

$$N(\exp(\langle A_1\rangle_s \cdot X), \delta) \gg \delta^{-3+10\varepsilon_0},$$

Posons $k = \frac{1}{\varepsilon_0}$ et notons $m = m_k \in \mathbb{N}^*$ et $w = w_k \in F_k$ les éléments donnés par le lemme 5.7. Pour $a_1,\dots,a_s \in A^s$, notons $X_i = (\mathrm{Ad}\, a_i)X$ et $x_i = e^{(\mathrm{Ad}\, a_i)X} = a_i x a_i^{-1} \in A^{s+2}$. Alors, le lemme 5.7 appliqué avec $\rho = \delta^{\varepsilon_0}$ donne

$$\exp[m_s(X_1+\dots+X_s)] = w(e^{X_1},\dots,e^{X_s}) + O(\delta).$$

Par conséquent, si $\ell = \ell(w)$ est la longueur du mot w,

$$\exp[m_s(X_1+\dots+X_s)] \subset A^{(s+2)\ell}\cdot B(1,O(\delta)),$$

d'où

$$N(A^{(s+2)\ell},\delta) \gg N(\exp(m_s\langle A_1\rangle_s \cdot X)),\delta) \gg \delta^{-3+10\varepsilon_0}.$$

Prenant ε_0 tel que $3-10\varepsilon_0 = \frac{3+\sigma}{2}$ et $\varepsilon > 0$ tel que $2(s+2)\ell\varepsilon < \frac{3-\sigma}{2}$, cela implique $N(A^{(s+2)\ell},\delta) \geq \delta^{-2(s+2)\ell\varepsilon} N(A,\delta)$ et donc, par l'inégalité de Ruzsa

$$N(A^3,\delta) \geq \delta^{-\varepsilon} N(A,\delta).$$

□

Chapitre 6

Aplanissement et trou spectral

Dans ce chapitre, nous achevons la démonstration du théorème 2.21, suivant la méthode développée par Bourgain et Gamburd [4, 3]. Le théorème produit 5.1 et les méthodes de combinatoire additive des chapitres 3 et **??** vont nous permettre de montrer que la propriété du trou spectral pour une mesure symétrique μ est équivalente à une certaine propriété de non concentration de la marche aléatoire au voisinage des sous-groupes.

Définition 6.1 (Mesures presque diophantiennes)**.** Une probabilité symétrique μ sur G est dite *presque diophantienne* s'il existe des constantes $C, c > 0$ et $n_0 \in \mathbb{N}$ telles que pour tout $n \geq n_0$ et tout sous-groupe fermé H tel que $\dim H < \dim G$,

$$\mu^{*n}(\{g \in G \mid d(g, H) \leq e^{-Cn}\}) \leq e^{-cn}.$$

Le résultat que nous montrerons dans ce chapitre est le suivant.

Théorème 6.2. *Une probabilité symétrique μ sur G admet un trou spectral si et seulement si elle est presque diophantienne.*

Commençons par vérifier le sens facile de cette équivalence : si μ admet un trou spectral, alors μ est presque diophantienne.

Trou spectral $\Rightarrow$ Condition presque diophantienne. Pour $\rho > 0$, on définit un élément de $L^2_0(G)$ en posant $f = \mathbb{1}_{H^{(\rho)}} - m(H^{(\rho)})$. Notons que $\|f\|_2 \asymp \|\mathbb{1}_{H^{(\rho)}}\| \asymp m(H^{(\rho)})^{1/2} \leq \rho^{1/2}$. Donc pour $n = C_\mu \log 1/\rho$, notant $p = \dim H$,

$$\|T^n_\mu \mathbb{1}_{H^{(2\rho)}}\|_2 \ll \rho^{d-p}.$$

Or,

$$\begin{aligned}
\|T^n_\mu \mathbb{1}_{H^{(2\rho)}}\|_2 &= \left(\int (\int \mathbb{1}_{H^{(2\rho)}}(xy)\mu^{*n}(\mathrm{d}x))^2 \mathrm{d}y\right)^{1/2} \\
&= \left(\int (\mu^{*n}(H^{(2\rho)}y)^2 \mathrm{d}y\right)^{1/2} \\
&\geq |H^{(\rho)}|^{1/2} \mu^{*n}(H^{(\rho)})
\end{aligned}$$

et donc

$$\mu^{*n}(H^{(\rho)}) \ll \rho^{\frac{d-p}{2}}.$$

□

La suite du chapitre a pour but de démontrer l'implication réciproque.

6.1 Aplanissement

Nous utiliserons la famille d'unités approchées $(P_\delta)_{\delta>0}$ définie par

$$P_\delta(x) = \frac{\mathbb{1}_{B(1,\delta)}(x)}{|B(1,\delta)|}.$$

Si ν est une probabilité sur G et $\delta > 0$, on note $\nu_\delta = \nu * P_\delta$ la régularisée de ν à l'échelle δ, et

$$\|\nu\|_{2,\delta} = \|\nu * P_\delta\|_2.$$

Le lemme central dans la démonstration du théorème 6.2 est le suivant. C'est l'analogue pour les mesures de probabilité du théorème produit discrétisé, et il s'en déduit à l'aide du lemme de Balog-Szemerédi-Gowers.

Lemme 6.3 (Aplanissement L^2)**.** *Étant donné $\sigma, \kappa > 0$, il existe $\varepsilon > 0$ tel que l'énoncé suivant soit vérifié pour tout $\delta > 0$ suffisamment petit.*
Soit ν une probabilité sur G telle que

(i) $\|\nu\|_{2,\delta} \geq \delta^{-\sigma}$;

(ii) $\forall H < G,\ \forall \rho \geq \delta, \quad (\nu * \check{\nu})(H^{(\rho)}) \leq \rho^\kappa$.

Alors,

$$\|\nu * \nu\|_{2,\delta} \leq \delta^\varepsilon \|\nu\|_{2,\delta}.$$

Démonstration. Supposons que ν vérifie

(i) $\|\nu\|_{2,\delta} \geq \delta^{-\sigma}$;

(ii) $\forall H < G,\ \forall \rho \geq \delta, \quad (\nu * \check{\nu})(H^{(\rho)}) \leq \rho^\kappa$.

(iii) $\|\nu * \nu\|_{2,\delta} \geq \delta^\varepsilon \|\nu\|_{2,\delta}$.

Nous approcherons la densité $\nu_\delta = \nu * P_\delta$ de ν à l'échelle δ par des ensembles de niveau dyadiques. Posant

$$\forall i \geq 1,\ A_i = \{x \mid 2^i \leq \nu_\delta(x) \leq 2^{i+1}\},$$

on a

$$\sum_{1 \leq i \leq d \log \frac{1}{\delta}} 2^i \mathbb{1}_{A_i}(x) \leq \nu_\delta(x) \leq 1 + 2 \sum_{1 \leq i \leq d \log \frac{1}{\delta}} \mathbb{1}_{A_i}(x).$$

La troisième condition sur ν implique

$$\left\| \sum_{1 \leq i,j \ll \log \frac{1}{\delta}} 2^{i+j} \mathbb{1}_{A_i} * \mathbb{1}_{A_j} \right\|_2 \geq \delta^\varepsilon \|\nu\|_{2,\delta}$$

et donc il existe i, j tels que

$$2^{i+j} \| \mathbb{1}_{A_i} * \mathbb{1}_{A_j} \|_2 \geq \delta^{2\varepsilon} \|\nu\|_{2,\delta}.$$

Comme $\|2^i \mathbb{1}_{A_i}\|_1 \leq 1$ et $\|2^i \mathbb{1}_{A_i}\|_2 \leq \|\nu\|_{2,\delta}$, cela implique

$$\|\nu\|_{2,\delta} \geq \|2^i \mathbb{1}_{A_i}\|_1 \|2^j \mathbb{1}_{A_j}\|_2 \geq 2^{i+j} \|\mathbb{1}_{A_i}\|_1 \|\mathbb{1}_{A_j}\|_2 \geq \delta^{2\varepsilon} \|\nu\|_{2,\delta}$$

et donc

$$1 \geq 2^i |A_i| \geq \delta^{2\varepsilon} \quad \text{et} \quad \|\nu\|_{2,\delta} \geq 2^j |A_j|^{\frac{1}{2}} \geq \delta^{2\varepsilon} \|\nu\|_{2,\delta}.$$

Les mêmes encadrements sont encore valables si l'on échange i et j, d'où, à un facteur $\delta^{O(\varepsilon)}$ près,

$$\|\nu\|_{2,\delta} \asymp 2^{\frac{i}{2}} \asymp 2^{\frac{j}{2}}$$

et

$$|A_i| \asymp |A_j| \asymp 2^{-i} \asymp 2^{-j}.$$

Par suite, l'énergie multiplicative de A_i et A_j est minorée :

$$E(A_i, A_j) = \|\mathbb{1}_{A_i} * \mathbb{1}_{A_j}\|_2^2 \geq \delta^{O(\varepsilon)} |A_i|^{\frac{3}{2}} |A_j|^{\frac{3}{2}}.$$

D'après le lemme de Balog-Szemerédi-Gowers (lemme 3.10), et la classification des ensembles à petit doublement (proposition 3.7), il existe un sous-groupe $\delta^{O(\varepsilon)}$-approximatif H et deux éléments $x, y \in G$ tels que

— $|H| \leq \delta^{-O(\varepsilon)} |A_i|^{\frac{1}{2}} |A_j|^{\frac{1}{2}}$;

— $|A_i \cap xH| \geq \delta^{O(\varepsilon)} |A_i|$ et $|A_j \cap Hy| \geq \delta^{O(\varepsilon)} |A_j|$.

Notons que $\nu_\delta(xH) \geq \delta^{O(\varepsilon)}$ et vu l'hypothèse de non concentration sur ν, cela implique que xH n'est pas inclus dans un $\delta^{O(\varepsilon)}$-voisinage d'un sous-groupe fermé strict. Cela implique aussi $N(H, \rho) = N(xH, \rho) \geq \delta^{O(\varepsilon)} \frac{1}{\max_x \nu_\delta(B(x,\rho))} \geq \rho^{-\kappa/2} \delta^{O(\varepsilon)}$. (En effet, pour tout x dans G, on peut majorer $\nu_\delta(B(x,\rho))^2 \leq \nu * \check{\nu}(B(1, 2\rho)) \ell\ell \delta^{-\varepsilon} \rho^\kappa$.)

D'après le théorème produit, il existe $\tau > 0$ tel que si $\varepsilon > 0$ est suffisamment petit, on doit avoir $N(H^3, \delta) \geq \delta^{-\tau} N(H, \delta)$. Par conséquent, $\tau \leq O(\varepsilon)$, et $\varepsilon > 0$ est minoré, ce qu'il fallait démontrer. □

Grâce à une application itérée du lemme d'aplanissement, nous allons montrer la proposition suivante.

Proposition 6.4. *Soit μ une probabilité symétrique presque diophantienne sur G. Pour tout $\sigma > 0$, il existe une constante $c_0 > 0$ telle que pour tout n suffisamment grand, si $\delta = e^{-c_0 n}$, alors*

$$\|\mu_n\|_{2,\delta} \leq \delta^{-\sigma}.$$

Démonstration. Rappelons que pour tout n suffisamment grand,

$$\forall H < G, \quad \mu_n(H^{(e^{-Cn})}) \leq e^{-cn}.$$

Posant $\kappa = \frac{c}{C}$, cela implique que pour tout $n \geq n_0$,

$$\forall H < G, \ \forall \rho \geq e^{-Cn}, \quad \mu_n(H^{(\rho)}) \leq \rho^\kappa.$$

Comme μ est symétrique, cela montre que pour tout $N \geq n_0$, la mesure $\nu = \mu_N$ vérifie les hypothèses du lemme 6.3 pour tout $\delta \geq e^{-CN}$. Définissons par récurrence

$$\begin{cases} \nu_0 = \mu_N \\ \forall k \geq 1, \ \nu_k = \nu_{k-1} * \nu_{k-1}. \end{cases}$$

Tant que $\|\nu_k\|_{2,\delta} \geq \delta^{-\sigma}$, le lemme 6.3 montre que $\|\nu_{k+1}\|_{2,\delta} \leq \delta^{-\tau}\|\nu_k\|_{2,\delta}$. Par conséquent, il existe $k \leq \frac{\dim G}{2\tau}$ tel que $\|\nu_k\|_{2,\delta} \leq \delta^{-\sigma}$. Si $n = 2^k N$ et $c_0 = \frac{C}{2^k}$, comme $\nu_k = \mu_{2^k N} = \mu_n$ et $\delta = e^{-CN} = e^{-c_0 n}$, on obtient

$$\|\mu_n\|_{2,\delta} \leq \delta^{-\sigma}.$$

Cela montre la propriété souhaitée lorsque $n = 2^k N$ pour N assez grand. Le cas général en découle, quitte à diminuer un peu la valeur de c_0, car on peut toujours écrire $n = 2^k N + p$, $p \in [\![0, 2^k - 1]\!]$ et donc

$$\|\mu_n\|_{2,\delta} \leq \|\mu_{2^k N}\|_{2,\delta} \leq \delta^{-\sigma}.$$

□

6.2 Analyse de Fourier

Rappelons la classification des représentations unitaires irréductibles de $G = \mathrm{SU}_2(\mathbb{R})$.

Théorème 6.5. *Pour chaque $m \geq 1$, il existe à équivalence près une unique représentation irréductible de $G = \mathrm{SU}_2(\mathbb{R})$ sur un espace de dimension m. Cette représentation est donnée par l'action régulière de G sur l'espace $V_n = \mathbb{C}_n[X, Y]$ des polynômes homogènes de degré m en deux variables X, Y :*

$$(g \cdot P)\begin{pmatrix} X \\ Y \end{pmatrix} = P\left(g^{-1}\begin{pmatrix} X \\ Y \end{pmatrix}\right).$$

Démonstration. Une représentation de $\mathrm{SU}_2(\mathbb{R})$ est un morphisme $\mathrm{SU}_2(\mathbb{R}) \to \mathrm{GL}_d(\mathbb{C})$. Comme $\mathrm{SU}_2(\mathbb{R})$ est simplement connexe, ces représentations sont en bijection avec les représentations de l'algèbre de Lie

$$\mathfrak{su}_2 = \{X \in \mathfrak{sl}_2(\mathbb{C}) \mid X^* + X = 0\}.$$

Et comme $\mathfrak{su}_2 \oplus i\mathfrak{su}_2 = \mathfrak{sl}_2(\mathbb{C})$, une telle représentation se prolonge uniquement en une représentation $\mathbb{C}$-linéaire $\mathfrak{sl}_2(\mathbb{C}) \to \mathfrak{gl}_d(\mathbb{C})$. Il s'agit donc de classifier les représentations de l'algèbre de Lie complexe $\mathfrak{sl}_2(\mathbb{C})$. On utilise pour cela la base

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

qui vérifie $[h, e] = 2e$, $[h, f] = -2f$ et $[e, f] = h$. Soit $\pi : \mathfrak{sl}_2(\mathbb{C}) \to \mathfrak{gl}(V)$ une représentation de dimension finie de $\mathfrak{sl}_2(\mathbb{C})$. Comme $\mathbb{C}$ est algébriquement clos, l'endomorphisme $\pi(h)$ admet une valeur propre :

$$\exists v \in V \setminus \{0\}, \lambda \in \mathbb{C} : \ \pi(h)v = \lambda v.$$

On écrit alors

$$\pi(h)\pi(e)v = \pi(e)\pi(h)v + [\pi(h), \pi(e)]v = (\lambda + 2)\pi(e)v$$

et par récurrence

$$\pi(h)\pi(e)^k v = (\lambda + 2k)\pi(e)^k v.$$

Les vecteurs $\pi(e)^k v$, $k \geq 0$ sont linéairement indépendants s'ils sont non nuls, car ils sont associés à des valeurs propres distinctes de $\pi(h)$. Comme $\dim V < +\infty$, il existe k tel que $\pi(e)^k v = 0$, et par conséquent, quitte à changer λ,

$$\exists v_0 \neq 0 : \ \pi(e)v_0 = 0 \quad \text{et} \quad \pi(h)v_0 = \lambda v_0.$$

Pour $i \geq 0$, notons $v_i = \pi(f)^i v_0$. On vérifie facilement par récurrence sur i que $\pi(h)v_i = (\lambda - 2i)v_i$ et donc il existe n tel que $\pi(f)^{n+1}v_0 = 0$. Si $n \in \mathbb{N}^*$ est l'entier minimal qui satisfait cette égalité, les vecteurs $v_0, \ldots, v_n$ sont linéairement indépendants. Montrons que $V = \mathrm{Vect}(v_0, \ldots, v_n)$. Pour cela, il suffit de vérifier que $W = \mathrm{Vect}(v_0, \ldots, v_n)$ est stable par l'action de $\mathfrak{sl}_2(\mathbb{C})$. Comme W est clairement stable par $\pi(f)$ et $\pi(h)$, il reste à montrer la stabilité par $\pi(e)$. On montre par récurrence que $\pi(v_i) \in \mathrm{Vect}(v_0, \ldots, v_{i-1})$. Tout d'abord, $\pi(e)v_0 = 0$, puis $\pi(e)v_1 = \pi(e)\pi(f)v_0 = [\pi(e), \pi(f)]v_0 = \lambda v_0$ et ensuite

$$\begin{aligned}\pi(e)v_{i+1} &= \pi(e)\pi(f)v_i = \pi(h)v_i + \pi(f)\pi(e)v_i \\ &= (\lambda - 2i)v_i + \pi(f)\pi(e)v_i\end{aligned}$$

et comme $\pi(e)v_i \in \mathrm{Vect}(v_0, \ldots, v_{i-1})$, on trouve bien $\pi(e)v_{i+1} \in \mathrm{Vect}(v_0, \ldots, v_i)$. Pour conclure, on remarque que $\lambda = n$ car

$$\mathrm{Tr}\, \pi(h) = \mathrm{Tr}(\pi(e)\pi(f) - \pi(f)\pi(e)) = 0$$

i.e.

$$0 = \sum_{i=0}^{n} (\lambda - 2i) = (n+1)\lambda - n(n+1).$$

Cela permet d'exprimer les matrices de $\pi(e)$, $\pi(f)$ et $\pi(h)$ dans la base $v_0, \ldots, v_n$ et de vérifier qu'elles correspondent bien à la représentation de $\mathfrak{sl}_2(\mathbb{C})$ sur $\mathbb{C}_n[X, Y]$, dans la base canonique. □

Cette description du dual unitaire de G permet d'expliciter la formule de Parseval. Pour $m \in \mathbb{N}^*$, et $f \in L^1(G)$, on note

$$\hat{f}(m) = \int_G f(g)\rho_n(g)^* \, \mathrm{d}g,$$

où $\rho_n : G \to \mathrm{GL}(V_n)$ est l'unique représentation irréductible de G de dimension m. Alors,

$$\forall f \in L^2(G), \quad \|f\|_2^2 = \sum_{m \geq 1} m \|\hat{f}(m)\|_{HS}^2.$$

C'est la croissance linéaire en m de la dimension des représentations irréductibles de G qui va nous permettre de déduire de la proposition 6.4 que toute mesure presque diophantienne admet un trou spectral.

Démonstration du théorème 6.2. D'après la proposition 6.4 appliquée avec $\sigma = \frac{1}{4}$, pour tout n assez grand, si $\delta = e^{-c_0 n}$,

$$\|\mu_n\|_{2,\delta}^2 \leq \delta^{-\frac{1}{2}}.$$

Or, par la formule de Parseval appliquée à $f = \mu_n * P_\delta$,

$$\begin{aligned}\|\mu_n\|_{2,\delta}^2 &= \sum_{m\geq 1} m\|\hat{\mu}(m)^n \hat{P}_\delta(m)\|_{HS}^2 \\ &\geq m\|\hat{\mu}(m)^n \hat{P}_\delta(m)\|_{HS}^2 \\ &\geq m\|\hat{\mu}(m)^n \hat{P}_\delta(m)\|_{op}^2.\end{aligned}$$

Choisissons $m = \lfloor \frac{1}{10\delta} \rfloor$, de sorte que $\|\hat{P}_\delta(m) - 1\|_{op} \leq \frac{1}{2}$. On a alors

$$\|\hat{\mu}(m)^n\|_{op}^2 \leq 2\|\hat{\mu}(m)^n \hat{P}_\delta(m)\|_{op}^2 \leq m^{-1}\delta^{\frac{1}{2}} \leq 100 m^{-\frac{1}{2}}$$

et par conséquent, comme $m \asymp \delta^{-1} = e^{c_0 n}$,

$$\|\hat{\mu}(m)^n\|_{op}^{\frac{1}{n}} \leq 10^{\frac{1}{n}} e^{-\frac{c_0}{4}} \leq 1 - \varepsilon,$$

pour un certain $\varepsilon > 0$ indépendant de m, suffisamment grand. Comme μ est adaptée apériodique, on a aussi pour tout $m \neq 1$, $\|\hat{\mu}(m)\| < 1$, et par conséquent la mesure μ admet un trou spectral en 1, ce qu'il fallait démontrer. □

Chapitre 7

Non concentration des marches aléatoires

Le but de ce chapitre est de conclure la démonstration du théorème 2.21. Nous commençons par en rappeler l'énoncé.

Théorème 7.1. *Soit μ une mesure adaptée sur $G = \mathrm{SU}_2(\mathbb{R})$ dont le support est constitué de matrices à coefficients algébriques. Alors μ admet un trou spectral.*

Vu le théorème 6.2 démontré au chapitre précédent, il suffit de faire voir que toute mesure adaptée sur G dont le support est constitué de matrices à coefficients algébriques vérifie la condition presque diophantienne :

$$\exists n_0, C, c > 0 : \ \forall H < G, \ \forall n \geq n_0, \quad \mu^{*n}(H^{(e^{-Cn})}) \leq e^{-cn}.$$

Nous procéderons pour cela en deux étapes. Dans un premier lieu, nous montrerons que pour toute mesure μ adaptée, on peut majorer uniformément $\mu^{*n}(H) \leq e^{-cn}$ pour tout n suffisamment grand et tout sous-groupe fermé strict $H < G$. Ensuite, nous vérifierons que si μ est supportée par un ensemble S fini constitué d'éléments à coefficients algébriques, il existe une constante $C > 0$ telle que pour tout sous-groupe fermé $H < G$ et tout $n \geq n_0$, il existe $H' < G$ tel que

$$S^n \cap H^{(e^{-Cn})} \subset H'.$$

Avec ce qui précède, cette inclusion permet alors de majorer $\mu^{*n}(H^{(e^{-Cn})}) \leq \mu^{*n}(H') \leq e^{-cn}$.

7.1 Moyennabilité et probabilité de retour

Avant d'étudier la propriété presque diophantienne d'une marche aléatoire, il convient d'abord de comprendre à quelle condition la probabilité de retour en l'identité décroit exponentiellement. C'est ce que nous faisons dans cette partie, en présentant le critère de moyennabilité de Kesten.

Nous avons vu au chapitre 2 qu'un groupe discret Γ est dit *moyennable* si pour toute partie finie $K \subset \Gamma$ et tout $\varepsilon > 0$, il existe une partie finie $U \subset \Gamma$

telle que $\frac{|KU\triangle U|}{|U|} \leq \varepsilon$. Lorsque Γ est de type fini, cette propriété est équivalente à une décroissance sous-exponentielle de la probabilité de retour en l'identité pour une marche aléatoire symétrique.

Théorème 7.2 (Critère de Kesten)**.** *Un groupe de type fini est moyennable si et seulement si, pour toute probabilité symétrique μ adaptée,*

$$\lim \mu^{*2n}(\{1\})^{\frac{1}{2n}} = 1.$$

Pour démontrer ce critère, il est commode d'interpréter la moyennabilité d'un groupe de type fini Γ comme une propriété géométrique de son graphe de Cayley.

Notations. Soit $\mathcal{G} = (V, E)$ un graphe, i.e. un ensemble de sommets V et un ensemble d'arêtes $E \subset V \times V$. Étant donné une partie A quelconque d'un graphe $\mathcal{G}$, nous noterons la frontière de A

$$\partial A = \{e \in E \mid e = (a, b)\, a \in A,\ b \notin A\} = E \cap (A \times (V \setminus A))\,.$$

Définition 7.3. Un graphe $\mathcal{G}$ est dit *non moyennable* s'il existe $c > 0$ tel que pour toute partie finie $A \subset V$, $|\partial A| \geq c|A|$.

Exercice 48. Vérifier qu'un arbre régulier de valence $v \geq 3$ est non moyennable.

Donnons tout de suite quelques caractérisations des graphes non moyennables. Ci-dessous, étant donnée une fonction $f : V \to \mathbb{R}$ sur l'ensemble des sommets d'un graphe $\mathcal{G} = (V, E)$, on note $\nabla f : E \to \mathbb{R}$ l'application définie par $\nabla f(e) = f(e^+) - f(e^-)$, où $e = (e^+, e^-)$. (Si le graphe n'est pas orienté, cette application n'est définie qu'au signe près, mais cela n'a pas d'importance, car nous considérerons seulement $|\nabla f|$.)

Proposition 7.4. *Soit $\mathcal{G}$ un graphe quelconque. On note $C_c(\mathcal{G})$ l'ensemble des fonctions à support fini dans $\mathcal{G}$. Les assertions suivantes sont équivalentes.*

(i) $\mathcal{G}$ est non moyennable ;

(ii) $\exists C \geq 0 :\ \forall f \in C_c(\mathcal{G}),\ \|f\|_1 \leq C\|\nabla f\|_1$ *;*

(iii) $\exists C \geq 0 :\ \forall f \in C_c(\mathcal{G}),\ \|f\|_2 \leq C\|\nabla f\|_2$ *;*

Démonstration. $\underline{(i) \Rightarrow (ii)}$ Comme $\|\nabla f\|_1 \geq \|\nabla |f|\|_1$, on peut supposer $f \geq 0$. Soit alors, pour $t \geq 0$, $A_t = \{f \geq t\}$. On utilise alors la formule de la coaire $\|\nabla f\|_1 = \int_0^\infty |\partial A_t| \mathrm{d}t$ pour minorer

$$\|\nabla f\|_1 \geq c \int_0^\infty |A_t| \mathrm{d}t = c \int_0^\infty |\{f \geq t\}| \mathrm{d}t = c\|f\|_1.$$

$\underline{(ii) \Rightarrow (iii)}$

$$\begin{aligned}
\|f\|_2^2 = \|f^2\|_1 \leq C\|\nabla f^2\|_1 &= C \sum |f(e^+)^2 - f(e^-)^2| \\
&= C \sum |f(e^+) - f(e^-)||f(e^+) + f(e^-)| \\
&\leq C\|\nabla f\|_2 \sqrt{\sum |f(e^+) + f(e^-)|^2} \\
&\leq 2C\|\nabla f\|_2 \|f\|_2.
\end{aligned}$$

$\underline{(iii) \Rightarrow (i)}$ Il suffit de prendre $f = \mathbb{1}_A$ pour obtenir la définition de la non moyennabilité. □

Exercice 49. Démontrer la formule de la coaire sur un graphe quelconque : pour $f \in C_c(\mathcal{G})$ à valeurs positives, si $A_t = \{f \geq t\}$, alors $\|\nabla f\|_1 = \int_0^\infty |\partial A_t| \mathrm{d}t$.

Définition 7.5 (Graphe de Cayley)**.** Soit $\Gamma = \langle S \rangle$ un groupe de type fini engendré par un ensemble fini symétrique S de générateurs. Le graphe de Cayley $G(\Gamma, S)$ de Γ pour S est le graphe sur l'ensemble de sommets Γ dans lequel deux éléments sont reliés s'ils diffèrent par un élément de s :

$$a \leftrightarrow b \quad \Leftrightarrow \quad \exists s \in S : b = sa.$$

Proposition 7.6. *Un groupe de type fini $\Gamma = \langle S \rangle$ est non moyennable si et seulement si son graphe de Cayley $G(\Gamma, S)$ est non moyennable. Cette propriété ne dépend pas du système (symétrique) de générateurs S.*

Démonstration. Si le graphe de Cayley $G(\Gamma, S)$ est non moyennable, il est clair que Γ est non moyennable, puisque en prenant $K = S$, pour toute partie finie non vide U, on aura $\frac{|SU \triangle U|}{|U|} \geq c$.

Réciproquement, supposons Γ non moyennable. Il existe donc une partie finie $K \subset \Gamma$ telle que pour toute partie finie non vide U, $\frac{|KU \triangle U|}{|U|} \geq c$. Si S est une partie génératrice finie symétrique de Γ quelconque, il existe $n \in \mathbb{N}^*$ tel que $S^n \supset K$. Par conséquent, pour toute partie finie, $|S^n U \setminus U| \geq c|U|$. Posant $c' = n^{-1}|S^n|^{-1}c$, on obtient donc qu'il existe $s_1 \dots s_n \in S^n$ tel que $|s_1 \dots s_n U \setminus U| \geq nc'|U|$. Or

$$|s_1 \dots s_n U \setminus U| \leq \sum_k |s_1 \dots s_k U \setminus s_1 \dots s_{k-1} U| = \sum_k |s_k U \setminus U|$$

et par suite, pour un certain k

$$|s_k U \setminus U| \geq c'|U|.$$

Cela montre que $G(\Gamma, S)$ est non moyennable. □

Dans le cas des graphes de Cayley, la moyennabilité s'intérprète naturellement à l'aide d'opérateurs de convolution. Étant donnée une mesure sur Γ, on note $P_\mu : L^2(\Gamma) \to L^2(\Gamma)$ l'opérateur de convolution défini par

$$P_\mu f(x) = \sum_{x \in \Gamma} \mu(g) f(xg).$$

Proposition 7.7. *Soit Γ un groupe de type fini et S une partie finie génératrice. Les assertions suivantes sont équivalentes.*

(i) Γ *est moyennable ;*

(ii) $\forall \varepsilon > 0 : \ \exists f \in L^2(\Gamma), \ \forall s \in S : \ \|f - sf\|_2 \geq \varepsilon \|f\|_2$ *;*

(iii) pour toute probabilité μ sur Γ, $\|P_\mu\| = 1$;

(iv) il existe une probabilité adaptée μ sur Γ telle que $\|P_\mu\| = 1$.

Démonstration. Remarquons que $\|\nabla f\|_2^2 = \sum_{x \in \Gamma} \sum_{s \in S} |f(x) - f(sx)|^2 = \sum_{s \in S} \|f - sf\|_2^2$. L'équivalence $(i) \Leftrightarrow (ii)$ découle donc du troisième point de la proposition 7.4.

$\underline{(ii) \Rightarrow (iii)}$

Soit μ une probabilité adaptée sur Γ moyennable. Étant donné $\varepsilon > 0$ on peut

choisir S fini tel que $\mu(S) \geq 1-\varepsilon$. D'après ce qui précède, il existe $f \in L^2(\Gamma)$ tel que $\forall s \in S,\ \|f - sf\|_2 \leq \varepsilon \|f\|_2$. Cela implique

$$\begin{aligned}\|f - P_\mu f\|_2 &\leq \sum_{s\in S} \mu(s)\|f - sf\|_2 + \sum_{s\notin S} \mu(s)\|f - sf\|_2 \\ &\leq \varepsilon\|f\|_2 + 2\varepsilon\|f\|_2.\end{aligned}$$

Par conséquent, $\|P_\mu\| \geq 1$ et donc $\|P_\mu\| = 1$ pour toute probabilité μ sur Γ.
$\underline{(iii) \Rightarrow (iv)}$
Évident.
$\underline{(iv) \Rightarrow (i)}$
Supposons qu'il existe une probabilité adaptée μ vérifiant $\|P_\mu\| = 1$. Sans perte de généralité, on peut supposer que $1 \in S = \operatorname{Supp}\mu$. Soit (f_n) une suite de vecteurs unitaires dans $L^2(\Gamma)$ tels que $\lim\|P_\mu f\|_2 = 1$. Comme

$$\|P_\mu f_n\|_2^2 = \int \langle s^{-1}tf_n, f_n\rangle \mu(\mathrm{d}s)\mu(\mathrm{d}t)$$

et pour tout s,t, $|\langle s^{-1}tf_n, f_n\rangle| \leq \|f_n\|_2^2 = 1$, la convergence $\|P_\mu f_n\|_2^2 \to 1$ implique que pour presque tout s,t, $\langle s^{-1}tf_n, f_n\rangle \to 1$, i.e. $\|f_n - s^{-1}tf_n\|_2^2 = 2 - 2\langle s^{-1}tf_n, f_n\rangle \to 0$. Ainsi, la suite de vecteurs (f_n) est presque invariante par l'ensemble symétrique $SS^{-1} \supset S$ qui engendre Γ. Cela montre que Γ est moyennable. □

Pour conclure la démonstration du théorème 7.2, il reste seulement à démontrer le théorème suivant.

Théorème 7.8 (Kesten)**.** *Soit Γ un groupe de type fini et μ une probabilité symétrique sur Γ. La norme de l'opérateur de convolution $P_\mu : L^2(\Gamma) \to L^2(\Gamma)$ est donnée par la formule*

$$\|P_\mu\| = \lim_{n\to\infty} \left(\mu^{*2n}(\{1\})\right)^{\frac{1}{2n}}.$$

Démonstration. Une inégalité est facile à vérifier :

$$\mu^{*2n}(1) = \langle P_\mu^{2n}\mathbb{1}_e, \mathbb{1}_e\rangle = \|P_\mu^n \mathbb{1}_e\|_2^2 \leq \|P_\mu\|^{2n}.$$

Pour la réciproque, on applique le théorème spectral à l'opérateur symétrique $P_\mu : L^2(\Gamma) \to L^2(\Gamma)$. En restriction au sous-espace cyclique H_e engendré par $\mathbb{1}_e$, P_μ est conjugué à l'opérateur de multiplication $f \mapsto (t \mapsto tf(t))$ sur $L^2(\operatorname{Spec} P_\mu, m_e)$, où m_e est la mesure spectrale donnée par $m_e(f) = \langle f(P_\mu)\mathbb{1}_e, \mathbb{1}_e\rangle$. Par conséquent, en restriction à H_e, on a

$$\begin{aligned}\|P_\mu|_{H_e}\| = \max\operatorname{Supp} m_e &= \lim_{n\to\infty} \left(\int_{\operatorname{Spec} P_\mu} t^{2n} m_e(\mathrm{d}t)\right)^{\frac{1}{2n}} \\ &= \lim_{n\to\infty} \langle P_\mu^{2n}\mathbb{1}_e, \mathbb{1}_e\rangle^{\frac{1}{2n}} \\ &= \lim_{n\to\infty} \mu^{*2n}(e)^{\frac{1}{2n}}.\end{aligned}$$

Plus généralement, en restriction au sous-espace cyclique H_v engendré par $v \in L^2(\Gamma)$, P_μ est conjugué à la multiplication par t dans $L^2(\operatorname{Spec} P_\mu, m_v)$, avec $m_v(f) = \langle f(P_\mu)v, v\rangle$. Or, écrivant $v = \sum_x v(x)\mathbb{1}_x$, on observe que

$$\langle f(P_\mu)v, v\rangle = \sum_{x,y} v(x)v(y)\langle f(P_\mu)\mathbb{1}_x, \mathbb{1}_y\rangle,$$

et comme pour tous x, y, et $A \subset \operatorname{Spec} P_\mu$,

$$\langle \mathbb{1}_A(P_\mu)\mathbb{1}_x, \mathbb{1}_y\rangle \leq \|\mathbb{1}_A(P_\mu)\mathbb{1}_x\|^2 = \|\mathbb{1}_A(P_\mu)\mathbb{1}_e\|^2$$

la mesure m_v est absolument continue par rapport à m_e. En particulier, $\max \operatorname{Supp} m_v \leq \max \operatorname{Supp} m_e$. Pour conclure, on décompose $L^2(\Gamma)$ en somme orthogonale de sous-espaces cycliques de la forme H_v, ce qui montre que $\|P_\mu\| \leq \sup_v \|P_\mu|_{H_v}\| = \|P_\mu|_{H_e}\| = \lim_{n\to\infty} \mu^{*2n}(e)^{\frac{1}{2n}}$. □

Exercice 50. Cet exercice a pour but de démontrer la version du théorème spectral utilisée dans la démonstration ci-dessus. On considère donc un espace de Hilbert réel H et un opérateur symétrique $T : H \to H$. On suppose en outre qu'il existe $v \in H$ tel que l'espace engendré par la suite $(T^n v)_{n\geq 0}$ est dense dans H ; on dit que H est *cyclique*. Notons $S = \operatorname{Spec} T$ le spectre de T, i.e. l'ensemble des éléments $\lambda \in \mathbb{C}$ tel que T n'est pas inversible dans l'algèbre des opérateurs bornés sur H. Nous voulons démontrer qu'il existe une mesure borélienne m_T sur S et un isomorphisme $U : L^2(S, m_T) \to H$ tel que $T = UMU^{-1}$, où $M : L^2(S) \to L^2(S)$ est l'opérateur $f \mapsto (t \mapsto tf(t))$ de multiplication par t.

1. On note $\mathbb{R}_S[t]$ l'ensemble des applications polynomiales restreintes à S. Montrer que l'application $\mathbb{R}_S[t] \to H;\ f \mapsto f(T)v$ est bien définie.
2. Montrer que l'expression $m_T(f) = \langle v, f(T)v)\rangle$ définit une forme linéaire sur $\mathbb{R}_S[t]$ qui induit une mesure borélienne finie sur S. Justifier que cette mesure est positive.
3. Montrer que l'application définie à la première question induit une isométrie bijective $U : L^2(S, m_T) \to H$ qui a les propriétés souhaitées.
4. Expliquer la notation $f(T)$ pour $f \in L^\infty(S)$.

7.2 Alternative de Tits

Théorème 7.9 (Alternative de Tits)**.** *En caractéristique zéro, un groupe linéaire contient soit un sous-groupe résoluble d'indice fini, soit un groupe libre à deux générateurs.*

Démonstration. □

Corollaire 7.10. *Si la composante neutre de l'adhérence de Zariski de Γ n'est pas résoluble, alors Γ contient un sous-groupe libre à deux générateurs.*

Démonstration. On raisonne par contraposée. Si Γ ne contient pas de sous-groupe libre, d'après l'alternative de Tits, il existe $\Gamma_0 < \Gamma$ résoluble tel que $[\Gamma : \Gamma_0] < +\infty$. Alors, l'adhérence de Zariski de Γ_0 est résoluble, et comme celle-ci est d'indice fini dans l'adhérence de Zariski de Γ, elle en contient la composante neutre, qui doit aussi être résoluble. □

Corollaire 7.11. *Soit G un groupe semi-simple et μ une mesure adaptée sur G. Il existe une constante $c > 0$ telle que pour tout $n \geq 1$, $\mu^{*n}(\{1\}) \leq e^{-cn}$.*

Dans le cas où $G = \mathrm{SU}_2(\mathbb{R})$ et le sous-groupe engendré par le support de μ est libre, on peut même montrer la proposition suivante, qui permet de majorer la mesure d'un sous-groupe fermé pour la loi de la marche aléatoire au temps n.

Proposition 7.12. *Soit μ une mesure adaptée sur $G = \mathrm{SU}_2(\mathbb{R})$ tel que $S = \mathrm{Supp}\,\mu$ est fini et engendre un groupe libre. Il existe $c > 0$ tel que pour tout n suffisamment grand et tout sous-groupe fermé $H < G$,*

$$\mu^{*n}(H) \leq e^{-cn}.$$

Cette proposition est valable plus généralement dans tout groupe semi-simple G, et même si le sous-groupe engendré par μ n'est pas libre, mais la démonstration est plus délicate. En effet, dans $\mathrm{SU}_2(\mathbb{R})$, tous les sous-groupes fermés stricts sont abéliens à indice fini près, et cela va nous permettre de majorer leur mesure en utilisant simplement la borne de Kesten sur la probabilité de retour en l'identité. Nous utiliserons le lemme suivant.

Lemme 7.13. *Soit F un groupe libre et $u, v \in F$ deux éléments quelconques. Si $uv = vu$, alors il existe $w \in F$ et $m, n \in \mathbb{Z}$ tels que $u = w^m$ et $v = w^n$. En d'autres termes, tout sous-groupe abélien de F est cyclique.*

Démonstration. On procède par récurrence sur $\ell(u) + \ell(v)$. Le résultat est clair si $\ell(u) + \ell(v) \leq 1$.

Quitte à échanger u et v, on peut supposer que $\ell(u) \leq \ell(v)$. On distingue alors plusieurs cas :

- Si le mot uv est réduit, alors vu aussi, car ces deux mots ont la même longueur. Par conséquent, u est un segment initial de v, i.e. $v = uv'$. On a alors $uv' = v'u$, et par récurrence, pour un certain w, $u = w^m$, $v' = w^{n'}$. Posant $n = n' + m$, cela montre ce qu'on veut.
- Si u^{-1} est un segment initial de v, on conclut aussi facilement par récurrence.
- Si uv n'est pas réduit et u^{-1} ne divise pas v, on écrit $u = u't$ et $v = t^{-1}v'$ de sorte que $uv = u'v'$ soit réduit. Alors, $u'v' = t^{-1}v'u't$.
  - si u'^{-1} est un segment final de v', on écrit $v'' = v'u'^{-1}$ puis $u'v''u'^{-1} = t^{-1}v''t$. Cela donne $tu'v'' = v''tu'$ et par récurrence $tu' = w_0^k$ et $v'' = w_0^\ell$. Posant $w = t^{-1}w_0t$, on vérifie facilement que $u = w^m$ et $v = w^n$ pour certains entiers m, n.
  - sinon, on écrit $v' = v''s$ et $u' = s^{-1}u''$ de sorte que $v'u' = v''u''$ soit réduit. Cela donne $s^{-1}u''v''s = t^{-1}v''u''t$. Comme par construction, ces mots sont réduits, on doit avoir $\ell(s) = \ell(t)$, puis, comme s est un segment final de t, nécessairement $t = s$. Par suite, $u''v'' = v''u''$, et par récurrence $u'' = w_0^m$ et $v'' = w_0^n$. Posant $w = t^{-1}w_0t$, et nous souvenant que $t = s$, on trouve bien $u = t^{-1}u''t = w^m$ et $v = t^{-1}v''t = w^n$.

□

Nous pouvons maintenant démontrer la proposition 7.12.

Démonstration de la proposition 7.12. D'après le théorème de Jordan, il existe une constante $C \geq 0$ telle que tout sous-groupe fini de $\mathrm{SU}_2(\mathbb{R})$ contient un sous-groupe abélien d'indice au plus C. Par ailleurs, les seules sous-algèbres de Lie propres de $\mathfrak{su}_2$ sont les sous-algèbres de dimension 1. Par conséquent, si H est un sous-groupe fermé infini strict de $\mathrm{SU}_2(\mathbb{R})$, son algèbre de Lie est abélienne, donc sa composante neutre est un tore T, pour lequel $[H : H \cap T] \leq 2$. Ainsi, dans tous les cas, si H est un sous-groupe fermé strict de G, il existe un sous-groupe abélien $H_0 \leq H$ tel que $[H : H_0] \leq C$.

Soit $\Gamma = \langle S \rangle$ le sous-groupe engendré par μ. Comme Γ est non moyennable, il existe une constante $c > 0$ telle que pour tout $x \in \Gamma$ et tout $n \geq 0$,

$$\mu^{*2n}(x) \leq \mu^{*2n}(1) \leq e^{-cn}.$$

Par ailleurs, comme H_0 est abélien, d'après le lemme 7.13, le sous-groupe $H_0 \cap \Gamma$ est cyclique. Cela permet de majorer, pour tout $2n \in \mathbb{N}$,

$$|H_0 \cap S^{2n}| \leq 2n,$$

et comme μ^{*2n} est supportée par S^{2n},

$$\mu^{*2n}(H_0) = \sum_{x \in S^{2n} \cap H_0} \mu^{*2n}(x) \leq n e^{-cn}.$$

Pour conclure, on remarque que, par symétrie de μ, pour tout $x \in G$, $\mu^{*n}(H_0 x)^2 \leq \mu^{*2n}(H_0)$, et donc

$$\mu^{*n}(H) = \sum_{x \in H/H_0} \mu^{*n}(H_0 x) \leq C\sqrt{n} e^{-\frac{cn}{2}} \leq e^{-cn}$$

pour tout n suffisamment grand. □

7.3 Une propriété diophantienne

Si on ajoute une hypothèse d'algébricité sur les coefficients des éléments de $\operatorname{Supp} \mu$, on peut déduire facilement de la borne de Kesten que la mesure est presque diophantienne.

Proposition 7.14. *Soit μ une mesure adaptée sur $G = \mathrm{SU}_2(\mathbb{R})$, à support fini constitué de matrices à coefficients algébriques qui engendrent un groupe libre. Alors μ est presque diophantienne.*

La démonstration de cette proposition se fonde sur l'observation suivante.

Lemme 7.15. *Soit S un ensemble fini d'éléments de $\overline{\mathbb{Q}}$. Il existe une constante $C > 0$ telle que pour tout $n \in \mathbb{N}^*$, pour toute somme $x = s_{11} \dots s_{1n} + \dots + s_{k1} \dots s_{kn}$ de produits de longueur au plus n d'éléments de S, si $x \neq 0$, alors $|x| \geq k^{-C} e^{-Cn}$.*

Démonstration. Soit K le corps de nombres engendré par S, $d = [K : \mathbb{Q}]$, et $\mathcal{O}_K$ l'anneau des entiers de K. Soit $q \in \mathbb{N}^*$ tel que pour tout $s \in S$, $qs \in \mathcal{O}_K$. Alors, $q^n x \in \mathcal{O}_K$ et par conséquent $q^{dn} N(x) = N(qx) \in \mathbb{Z}$. Si $x \neq 0$, on a donc

$$q^{-dn} \leq |N(x)| = \prod_{i=1}^{d} |\sigma_i(x)|$$

d'où

$$|x| \geq \frac{q^{-dn}}{\prod_{i=2}^{d} |\sigma_i(x)|}.$$

Il existe une constante $C_0 = C_0(S)$ telle que pour tout i, $|\sigma_i(x)| \leq k e^{C_0 n}$ et donc

$$|x| \geq k^{-d} e^{-Cn},$$

où C est choisi tel que $e^C = q^d e^{dC_0 n}$. □

Démonstration de la proposition 7.14. Soit U un voisinage ouvert de l'identité dans $\mathrm{SU}_2(\mathbb{R})$ tel que pour tout sous-groupe fermé H, le sous-groupe engendré par $U \cap H$ soit abélien. Notons $S = \operatorname{Supp} \mu$ et S' l'ensemble des coefficients des éléments de S. Les coefficients d'un mot w de longueur n en les éléments de S sont des sommes d'au plus n produits de longueur au plus n d'éléments de S'. D'après le lemme ci-dessus appliqué à S', on a donc, pour une constante C dépendant de S,

$$d(w, 1) \geq e^{-Cn}.$$

Si $w_1, w_2 \in U \cap H^{(e^{-5Cn})}$, alors $d([w_1, w_2], 1) \leq e^{-5Cn}$ et comme $\ell([w_1, w_2]) \leq 4n$, la condition diophantienne implique $[w_1, w_2] = 1$. Ainsi, $U \cap H^{(e^{-5Cn})} \cap S^n$ est une partie commutative de $\mathrm{SU}_2(\mathbb{R})$, elle est donc incluse dans un tore H', et d'après la proposition 7.12,

$$\mu^{*n}(U \cap H^{(e^{-5Cn})}) \leq \mu^{*n}(H') \leq e^{-cn}.$$

□

Bibliographie

[1] S. Banach. Sur le problème de la mesure. *Fundam. Math.*, 4 :7-33, 1923.

[2] Bourgain. On the erdös-volkmann and katz-tao ring conjectures.

[3] Jean Bourgain et Alex Gamburd. A spectral gap theorem in SU(d). *J. Eur. Math. Soc. (JEMS)*, 14(5) :1455-1511, 2012.

[4] Jean Bourgain et Alex Gamburd. On the spectral gap for finitely-generated subgroups of SU(2). *Invent. Math.*, 171(1) :83-121, 2008.

[5] Haïm Brézis. *Analyse fonctionnelle. Théorie et applications.* Paris : Masson, 1994, page 248.

[6] V. G. Drinfel'd. Finitely additive measures on S^2 and S^3, invariant with respect to rotations. *Funct. Anal. Appl.*, 18 :245-246, 1984.

[7] Edgar et Miller. Borel subrings on the reals.

[8] Erdös et Szemeredi. On sums and products of integers.

[9] Guth, Katz et Zahl. On the discretized sum-product problem.

[10] Felix Hausdorff. Grundzüge der Mengenlehre. Mit 53 Figuren im Text. Leipzig : Veit & Comp. VIII u. 476 S. gr. 8° (1914). 1914.

[11] Katz et Tao. Some connections between falconer's distance set conjecture and sets of furstenburg type.

[12] G. A. Margulis. Some remarks on invariant means. *Monatsh. Math.*, 90 :233-236, 1980.

[13] Rudnev et Stevens. An update on the sum-product problem, 2020.

[14] Solymosi. Bounding multiplicative energy by the sumset.

[15] Dennis Sullivan. For $n > 3$ there is only one finitely additive rotationally invariant measure on the n-sphere defined on all Lebesgue measurable subsets. *Bull. Am. Math. Soc., New Ser.*, 4 :121-123, 1981.