
GRAPHES EXPANSEURS ET PROPRIÉTÉ (T)

Amaury FRESLON¹

Le but de cet exposé est de présenter à un public de mathématiciens non-spécialistes la propriété (T) de Kazhdan, à travers son utilisation pour la construction de familles de graphes expandeurs. Il ne présuppose aucune connaissance de théorie des graphes ou de théorie géométrique des groupes. Le lecteur intéressé trouvera dans le livre [Lub94] un traitement détaillé de ce sujet, dont nous ne donnerons qu'un aperçu.

1 INTRODUCTION

Notre point de départ est un problème de théorie des graphes, celui de construire une famille de *graphes expandeurs*. Fixons tout d'abord quelques points de terminologie. Dans tout ce texte, un *graphe* sera un graphe fini, formé d'un ensemble de sommets V et d'un ensemble d'arêtes $E \subset V \times V$. En particulier, les graphes que nous considérerons seront simples (pas d'arêtes multiples) et non-orientés.

Les graphes permettent de modéliser de nombreuses situations. En voici une particulière : les réseaux de communications. On dispose d'un certains nombres de lieux qu'on veut relier par des canaux de communications. La construction d'un tel réseau repose sur deux contraintes concurrentes :

- Il faut que le réseau soit “bien connecté” de sorte que si l'un des canaux cesse de fonctionner, on puisse toujours joindre tout le monde.
- Il faut que le réseau comporte un nombre de canaux limité, parce que ça coûte cher.

C'est pour aborder ce problème que la notion de graphe expandeur a été introduite dans les années 70. L'exemple le plus notable est celui des réseaux téléphoniques, mais il s'avère que le premier travail sur le sujet, dû à Y. Barzdin et A. Kolmogorov dans [BK93] était motivé par les réseaux de neurones ! Ajoutons pour l'histoire que le résultat central de [BK93], qui montre par des arguments probabilistes l'existence de graphes expandeurs, a été retrouvé quelques années plus tard par M. Pinsker dans [Pin73], où il établit le terme *expandeur*. Notre premier objectif est maintenant de détailler et de motiver la définition de cette notion.

1.1 LA DÉFINITION

Commençons par la première contrainte ci-dessus. On cherche un moyen de mesurer la robustesse d'un graphe G par rapport aux déconnexions, c'est-à-dire de savoir si chaque ensemble de sommets est relié à suffisamment d'autres sommets. Pour ce faire, on introduit une notion de *frontière* de la façon suivante :

1. A. Freslon, Laboratoire de Mathématiques d'Orsay, Université Paris-Saclay, CNRS, Université Paris-Saclay, 91405 Orsay, France.

e-mail : amaury.freslon@universite-paris-saclay.fr

DEFINITION 1.1. Soit G un graphe et $S \subset V$ un ensemble de sommets. La *frontière* de S est l'ensemble

$$\partial S = E(S, V \setminus S)$$

des arêtes de G qui relient un sommet de S à un sommet qui n'est pas dans S .

Il nous faudrait donc caractériser le fait que chaque partie S possède une frontière assez importante, de sorte qu'il sera difficile de l'isoler. Comme par définition le bord de S est égal à celui de $V \setminus S$, il suffit de tester notre condition sur les parties contenant au plus la moitié des sommets. C'est ce qui mène à la notion suivante :

DEFINITION 1.2. Soit G un graphe. Sa *constante d'expansion* est la quantité

$$h(G) = \min_{1 \leq |S| \leq |V|/2} \frac{|\partial S|}{|S|}.$$

Remark 1.3. Si le graphe G n'est pas connexe, alors $h(G) = 0$. En effet, il admet alors une composante connexe contenant au plus la moitié des sommets, et la frontière de celle-ci est vide. Réciproquement, si $h(G) = 0$ c'est qu'il existe une partie stricte S de V dont la frontière est vide, donc que G n'est pas connexe. Ainsi, la constante d'expansion n'est intéressante que pour les graphes connexes, ce qui n'est pas un problème vu notre contexte.

Nous avons maintenant un critère pour la première condition : il faudra que la constante d'expansion soit suffisamment grande. Pour la seconde, l'idée est de limiter le nombre de voisins qu'un sommet donné peut avoir, en utilisant la notion de degré.

DEFINITION 1.4. Soit G un graphe et $v \in V$ un sommet. Le *degré* $d(v)$ de v est le nombre de sommets reliés à v . Le *degré maximal* de G est le plus grand degré d'un sommet de G :

$$d(G) = \max_{v \in V} d(v).$$

Nous cherchons donc des graphes de petit degré maximal mais de grande constante d'expansion. S'il s'agit d'un seul graphe, cela ne pose pas de problème. Par exemple, il est clair que pour tout graphe connexe, on a l'inégalité

$$h(G) \geq \frac{2}{|V(G)|}.$$

Ce qui va nous intéresser, c'est de trouver des familles de graphes de plus en plus grands pour lesquels on parvient à contrôler à la fois la constante d'expansion (par en-dessous) et le degré maximal (par au-dessus).

DEFINITION 1.5. Une famille $(G_n)_{n \in \mathbb{N}}$ de graphes est appelée *famille de graphes expandeurs* si

- Le nombre de sommets de G_n tend vers $+\infty$ quand n tend vers $+\infty$;
- Il existe un entier d tel que $d(G_n) \leq d$ pour tout $n \in \mathbb{N}$;
- Il existe $\epsilon > 0$ tel que pour tout $n \in \mathbb{N}$,

$$h(G_n) \geq \epsilon.$$

1.2 CAYLEY À LA RESCOUSSE

Il n'est pas du tout évident qu'une telle famille de graphes existe. De fait, la première construction *déterministe* d'une famille de graphes expandeurs fut un résultat très important, dû à G. Margulis [Mar73]. Le but de la suite de l'exposé est d'introduire un outil puissant pour la construction de familles d'expandeurs, la *propriété (T) de Kazhdan*, et d'expliquer son lien avec l'expansion.

Le point de départ de notre stratégie est de construire des graphes à partir de groupes. En effet, il existe un moyen très simple d'associer un graphe à un groupe fini, qui de plus donne un contrôle sur le degré maximal : les graphes de Cayley.

DEFINITION 1.6. Soit Γ un groupe fini et soit $S \subset \Gamma$ une partie finie ne contenant pas l'élément neutre qui engendre² Γ . Le *graphe de Cayley* de Γ associé à S est le graphe $\text{Cay}(\Gamma, S)$ dont l'ensemble des sommets est $V = \Gamma$ et l'ensemble des arêtes

$$E = \{(g, sg) \mid g \in \Gamma \ \& \ s \in S\}.$$

On le voit sur la définition, tous les sommets d'un graphe de Cayley sont de degré $|S|$. Comment utiliser cette idée pour construire une famille de graphes de degré maximal fixé? Il suffit de savoir produire une famille de groupes finis avec des parties génératrices de taille constante, et le plus simple pour cela serait qu'ils proviennent tous d'un même groupe. Nous allons donc chercher à construire un groupe Γ infini *de type fini*³ avec une partie génératrice S . Ensuite, nous prendrons des sous-groupes normaux $\Gamma_n \triangleleft \Gamma$ d'indice fini de sorte qu'en notant $\pi_n : \Gamma \rightarrow \Gamma/\Gamma_n$ le morphisme de groupes quotient, on n'aura plus qu'à considérer les graphes

$$\text{Cay}(\Gamma/\Gamma_n, \pi_n(S)).$$

Reste à trouver une condition sur Γ qui assure que la famille ainsi construite soit une famille d'expandeurs, c'est-à-dire que les constantes d'expansion soient uniformément minorées. C'est là qu'il faut faire un détour non-trivial par la théorie des groupes.

2 LA PROPRIÉTÉ (T) DE KAZHDAN

2.1 LA DÉFINITION

La propriété (T) est une propriété de rigidité des représentations unitaires d'un groupe topologique localement compact qui a été introduite par D. Kazhdan dans [Kaz67]. La motivation originelle était de montrer que les réseaux dans les groupes de Lie de rang supérieur sont de type fini et que leur abélianisation est finie. Néanmoins, la propriété (T) s'est avérée être un outil extrêmement puissant pour bien d'autres questions de théorie géométrique des groupes ou de théorie ergodique. L'imposant ouvrage [BdlHV08] donne un aperçu du sujet.

Nous allons ici nous restreindre au cas des groupes discrets, ce qui simplifie certains énoncés et suffit pour les applications que nous visons. L'idée de la propriété (T) est de donner une forme de rigidité pour les représentations unitaires. Pour expliquer cela, rappelons qu'une *représentation unitaire* d'un groupe discret Γ est un morphisme de groupes

$$\pi : \Gamma \rightarrow \mathcal{U}(H),$$

où H est un espace de Hilbert et $\mathcal{U}(H)$ est l'ensemble des opérateurs unitaires de H .

Un *vecteur invariant* pour π est un vecteur $\xi \in H$ tel que $\pi(g).\xi = \xi$ pour tout $g \in \Gamma$. Posséder un vecteur invariant est une propriété assez forte pour une représentation unitaire. La propriété (T) repose sur le lien entre cette propriété et une version plus faible.

2. Il est aisé de constater sur la définition que le graphe $\text{Cay}(\Gamma, S)$ est connexe si et seulement si S engendre Γ . Comme nous ne nous intéressons qu'aux graphes connexes, cette hypothèse est autant naturelle que nécessaire.

3. Un groupe discret est dit *de type fini* s'il coïncide avec le sous-groupe engendré par une partie finie $S \subset \Gamma$. Cette dernière est alors appelée *partie génératrice* de Γ .

DEFINITION 2.1. On dit qu'une représentation unitaire π d'un groupe discret Γ admet des vecteurs presque invariants si pour toute partie finie $F \subset \Gamma$ et pour tout $\delta > 0$, il existe un vecteur non nul $\xi \in H$ tel que

$$\sup_{g \in F} \|\pi(g).\xi - \xi\| \leq \delta \|\xi\|.$$

Un tel vecteur est dit $(\pi(F), \delta)$ -invariant.

Avant de poursuivre, donnons un exemple de représentation admettant des vecteurs presque invariants.

Exemple 2.2. Nous allons prendre $\Gamma = \mathbb{Z}$ et travailler avec la représentation régulière $\lambda : \mathbb{Z} \rightarrow \mathcal{U}(\ell^2(\mathbb{Z}))$ définie par

$$\lambda(g)\delta_h = \delta_{g+h}.$$

Pour un entier n , on définit une fonction $f_n : \mathbb{Z} \rightarrow \mathbb{C}$ suivante :

$$f_n = \frac{1}{\sqrt{2n+1}} \sum_{k=-n}^n \delta_k : x \mapsto \begin{cases} \frac{1}{\sqrt{2n+1}} & \text{si } |x| \leq n \\ 0 & \text{sinon} \end{cases}$$

On remarquera que $\|f_n\|_2 = 1$. Pour un entier positif $g \in \mathbb{N}$, on a alors

$$(\lambda(g).f_n - f_n)(x) = \frac{1}{\sqrt{2n+1}} \left(\sum_{k=g-n}^{g+n} \delta_k - \sum_{k=-n}^n \delta_k \right) = \begin{cases} \frac{1}{\sqrt{2n+1}} & \text{si } n < x \leq n+g \\ -\frac{1}{\sqrt{2n+1}} & \text{si } -n < x \leq -n+g \\ 0 & \text{sinon} \end{cases}$$

Ainsi, si $F \subset \mathbb{Z}$ est une partie finie et n_0 est tel que $F \subset [-n_0; n_0]$, alors pour tout $g \in F \cap \mathbb{N}$ et $n \geq n_0$

$$\begin{aligned} \|\lambda(g).f_n - f_n\|^2 &= \frac{2g}{2n+1} \\ &\leq \frac{2n_0}{2n+1} \\ &\xrightarrow{n \rightarrow +\infty} 0 \end{aligned}$$

De plus, si $g < 0$, alors

$$\begin{aligned} \|\lambda(g).f_n - f_n\|^2 &= \|\lambda(g).(f_n - \lambda(-g).f_n)\|^2 \\ &= \|f_n - \lambda(-g)f_n\|^2 \\ &= \frac{-2g}{2n+1} \\ &\leq \frac{2n_0}{2n+1} \\ &\xrightarrow{n \rightarrow +\infty} 0 \end{aligned}$$

Autrement dit, la représentation λ admet des vecteurs presque invariants.

La propriété (T) est précisément le fait de ne pouvoir admettre des vecteurs presque invariants que pour des raisons triviales, c'est-à-dire l'existence d'un vecteur invariant non nul.

DEFINITION 2.3. Un groupe discret Γ a la *propriété (T)*⁴ si toute représentation unitaire de Γ qui admet des vecteurs presque invariants admet un vecteur invariant non nul.

Notre premier et seul exemple sera élémentaire, même si la démonstration est astucieuse.

Proposition 2.4. *Tout groupe fini a la propriété (T).*

Démonstration. Soit Γ un groupe fini et soit $\pi : \Gamma \rightarrow \mathcal{U}(H)$ une représentation unitaire admettant des vecteurs presque invariants. En particulier, il existe un vecteur ξ de norme 1 qui est $(\pi(\Gamma), 1)$ -invariant. On considère alors l'enveloppe convexe fermée \mathcal{C} de l'ensemble

$$\pi(\Gamma).\xi = \{\pi(g).\xi \mid g \in \Gamma\}$$

et l'unique élément $\eta \in \mathcal{C}$ de norme minimale⁵. Comme \mathcal{C} est $\pi(\Gamma)$ -invariant par définition, η est $\pi(\Gamma)$ -invariant. Il reste donc à montrer qu'il est non nul. Pour ce faire, observons que pour tout $g \in \Gamma$,

$$2 - 2\operatorname{Re}\langle \pi(g).\xi, \xi \rangle = \|\pi(g).\xi - \xi\|^2 \leq 1,$$

de sorte que

$$\operatorname{Re}\langle \pi(g).\xi, \xi \rangle \geq \frac{1}{2}.$$

Cette inégalité définit un demi-espace affine fermé qui contient $\{\pi(g).\xi \mid g \in \Gamma\}$, donc qui contient \mathcal{C} . Par conséquent,

$$\operatorname{Re}\langle \eta, \xi \rangle \geq \frac{1}{2},$$

ce qui implique $\eta \neq 0$. ■

Il est difficile de donner plus d'exemples, car démontrer la propriété (T) n'est jamais simple. Il est en fait plus facile de montrer que certains groupes n'ont pas la propriété (T), mais nous ne donnerons qu'un exemple qui nous évite d'introduire trop de concepts supplémentaires⁶

Proposition 2.5. *Le groupe \mathbb{Z} n'a pas la propriété (T).*

Démonstration. Considérons la représentation régulière λ de l'Exemple 2.2. Elle admet des vecteurs presque invariants, mais elle n'a pas de vecteur invariant non nul. En effet, si $f \in \ell^2(\mathbb{Z})$ est invariante, alors on a pour tout $x \in \mathbb{Z}$

$$f(x+1) = \lambda(1).f(x) = f(x)$$

Ainsi, f est constante et pour être de carré sommable, il faut alors qu'elle soit nulle, ce qui conclut la preuve. ■

Ce résultat peut ensuite être étendu en exploitant la structure des groupes abéliens de type fini.

Corollaire 2.6. *Soit Γ un groupe discret abélien de type fini qui possède la propriété (T). Alors, Γ est fini.*

4. On dit aussi parfois que Γ est un *groupe de Kazhdan*.

5. La fonction $x \mapsto \|x\|^2$ est strictement convexe sur le convexe compact \mathcal{C} , donc elle admet un unique minimum.

6. Aucun groupe discret *moyennable* infini n'a la propriété (T), et les résultats de la Proposition 2.5, du Corollaire 2.6 et du Corollaire 2.10 découlent immédiatement de cet énoncé plus général.

Démonstration. Tout groupe discret abélien de type fini est un produit fini de groupes cycliques ⁷ :

$$\Gamma = \prod_{i=1}^N \Gamma_i.$$

S'il est infini, alors l'un au moins de ses facteurs est isomorphe à \mathbb{Z} , disons Γ_1 . Considérons alors la représentation unitaire π égale à la représentation régulière λ_1 de Γ_1 sur la première composante et à la représentation triviale (qui envoie tout élément sur l'opérateur identité) sur toutes les autres composantes. Alors π admet des vecteurs presque invariants par l'Exemple 2.2, mais n'admet pas de vecteur invariant non-trivial, donc Γ n'a pas la propriété (T). ■

Nous allons tout de même donner des exemples, mais sans démonstration. Précisons tout de même que nous donnerons quelques indications concernant $\mathrm{SL}_3(\mathbb{Z})$ plus loin (voir le Théorème 3.2) puisqu'il jouera un rôle crucial pour la construction d'expansions.

Exemple 2.7. Les groupes suivants ont la propriété (T) :

- $\mathrm{SL}_n(\mathbb{Z})$ pour tout $n \geq 3$ [Kaz67];
- Les réseaux dans $\mathrm{Sp}(n, 1)$, qui sont des groupes hyperboliques (voir [BdlHV08]);
- $\mathrm{Aut}(\mathbb{F}_n)$ pour $n \geq 5$ [KNO19, KKN21].

2.2 CONSÉQUENCES

Avant d'expliquer comment la propriété (T) permet de construire des familles d'expansions, nous allons donner en donner deux conséquences qui permettront de voir comment on peut exploiter les représentations unitaires d'un groupe discret pour donner des informations sur sa structure algébrique. Le principal outil pour cela sera la somme directe hilbertienne de représentations, que nous allons définir

Soit Γ un groupe discret et soit pour tout $n \in \mathbb{N}$ une représentation unitaire $\pi_n : \Gamma \rightarrow \mathcal{U}(H_n)$. On définit la somme directe hilbertienne des espaces de Hilbert comme

$$\overline{\bigoplus_{n \in \mathbb{N}} H_n} = \left\{ (\eta_n)_{n \in \mathbb{N}} \in \prod_{n \in \mathbb{N}} H_n \mid \sum_{n \in \mathbb{N}} \|\eta_n\|^2 < +\infty \right\}.$$

La barre au-dessus de la somme directe est parfois omise quand le contexte n'est pas ambiguë, mais nous la garderons pour plus de clarté. On définit sur cet espace un produit scalaire en posant

$$\langle (\eta_n)_{n \in \mathbb{N}}, (\zeta_n)_{n \in \mathbb{N}} \rangle = \sum_{n \in \mathbb{N}} \langle \eta_n, \zeta_n \rangle. \quad (1)$$

Il suit de la définition que la somme de droite converge absolument. On vérifie par des arguments standard que ceci muni la somme hilbertienne d'une structure d'espace de Hilbert.

Il est maintenant aisé de produire une représentation unitaire sur cet espace de Hilbert. En effet, il suit directement de la définition du produit scalaire que pour tout $g \in \Gamma$, l'opérateur

$$\pi(g) : (\eta_n)_{n \in \mathbb{N}} \rightarrow (\pi(g)\eta_n)_{n \in \mathbb{N}}$$

est bien défini et unitaire. Il définit une représentation unitaire qu'on note

$$\pi = \bigoplus_{n \in \mathbb{N}} \pi_n.$$

La premier énoncé est une reformulation de la propriété (T) qui permet de se restreindre à trouver des vecteurs presque invariants pour une seule partie finie de Γ , pourvue qu'elle soit génératrice. C'est la forme qui nous servira plus tard pour les graphes.

7. Une preuve élémentaire de ce résultat est donnée en appendice.

Proposition 2.8. Soit Γ un groupe discret de type fini⁸ ayant la propriété (T) et soit $S \subset \Gamma$ une partie génératrice finie. Alors, il existe $\delta > 0$ tel que toute représentation unitaire π possédant des vecteurs $(\pi(S), \delta)$ -invariants possède un vecteur invariant non nul.

Démonstration. Nous allons procéder par l'absurde, en supposant que pour tout $\delta > 0$, il existe une représentation unitaire π possédant des vecteurs $(\pi(S), \delta)$ -invariants mais pas de vecteur invariant non nul. En particulier, une telle représentation existe pour $\delta = n^{-2}$, que nous noterons π_n .

La première étape est d'observer qu'en posant

$$S^n = \{g_1 \cdots g_n \mid g_i \in S \text{ pour tout } 1 \leq i \leq n\} \subset \Gamma.$$

la représentation π_n possède des vecteurs $(\pi_n(S^n), n^{-1})$ -invariants. En effet, si ξ_n est $(\pi_n(S), n^{-2})$ -invariant et $g_1, \dots, g_n \in S$, alors

$$\begin{aligned} \|\pi_n(g_1 \cdots g_n) \cdot \xi_n - \xi_n\| &\leq \sum_{i=1}^{n-1} \|\pi_n(g_1 \cdots g_{i+1}) \cdot \xi_n - \pi_n(g_1 \cdots g_i) \cdot \xi_n\| + \|\pi_n(g_1) \cdot \xi_n - \xi_n\| \\ &= \|\pi_n(g_1) \cdot \xi_n - \xi_n\| + \sum_{i=1}^{n-1} \|\pi_n(g_1 \cdots g_i) \cdot (\pi_n(g_{i+1}) \cdot \xi_n - \xi_n)\| \\ &\leq \|\pi_n(g_1) \cdot \xi_n - \xi_n\| + \sum_{i=1}^{n-1} \|\pi_n(g_{i+1}) \cdot \xi_n - \xi_n\| \\ &= \sum_{i=1}^n \|\pi_n(g_i) \cdot \xi_n - \xi_n\| \\ &\leq \sum_{i=1}^n \frac{1}{n^2} \\ &= \frac{1}{n}. \end{aligned}$$

Considérons maintenant la représentation unitaire

$$\pi = \bigoplus_{n \in \mathbb{N}} \pi_n : \Gamma \rightarrow \mathcal{U} \left(\overline{\bigoplus_{n \in \mathbb{N}} H_n} \right).$$

Nous allons montrer qu'elle possède des vecteurs presque invariants. Pour ce faire, prenons une partie finie $F \subset \Gamma$ et $\epsilon > 0$. Comme S est une partie génératrice, il existe $n_1 \in \mathbb{N}$ tel que pour tout $n \geq n_1$, $F \subset S^n$. De même, il existe $n_2 \in \mathbb{N}$ tel que $n^{-1} < \epsilon$ pour tout $n \geq n_2$. Alors, $\xi_{n_1+n_2}$ étant $(\pi_{n_1+n_2}(S^{n_1+n_2}), (n_1+n_2)^{-1})$ -invariant par définition, il est en particulier $(\pi_n(F), \epsilon)$ -invariant. Autrement dit, π admet des vecteurs presque invariants, ce qui implique par définition de la propriété (T) que π a un vecteur invariant

$$\eta \in \bigoplus_{n \in \mathbb{N}} H_n.$$

Mais alors, il existe $n_0 \in \mathbb{N}$ tel que $\eta_{n_0} \neq 0$, et comme H_{n_0} est fixé par π , on en déduit que η_{n_0} est un vecteur invariant pour π_{n_0} , ce qui est une contradiction. ■

Le second énoncé – qui ne nous sera pas utile pour la suite – est l'un des résultats originaux de D. Kazhdan qui ont motivé l'introduction de la propriété (T).

8. Comme nous le verrons bientôt (Théorème 2.9), cette hypothèse est en fait inutile.

THÉORÈME 2.9 (Kazhdan) Soit Γ un groupe discret dénombrable possédant la propriété (T). Alors Γ est de type fini.

Démonstration. Si Γ est fini, alors le résultat est évident. Nous supposons donc désormais Γ infini et commencerons par remarquer que comme Γ est dénombrable, il admet une partie génératrice dénombrable. On dispose donc d'une suite $(s_n)_{n \in \mathbb{N}}$ d'éléments de Γ qui engendrent le groupe, et on note Γ_n le sous-groupe engendré par $\{s_1, \dots, s_n\}$. Afin d'exploiter la propriété (T), nous allons construire une représentation unitaire à partir de ces groupes. La façon la plus simple est de poser $H_n = \ell^2(\Gamma/\Gamma_n)$, muni de la représentation dite *quasi-régulière (gauche)* :

$$\pi_n(g) : \delta_{h.\Gamma_n} \mapsto \delta_{gh.\Gamma_n}.$$

On peut ensuite regrouper ces représentations en posant

$$H = \overline{\bigoplus_{n \in \mathbb{N}} H_n}$$

et

$$\pi = \bigoplus_{n \in \mathbb{N}} \pi_n : \Gamma \rightarrow \mathcal{U}(H).$$

L'étape suivante est de montrer que π admet des vecteurs presque invariants. Soient donc $F \subset \Gamma$ une partie finie et $\delta > 0$. Comme par construction Γ est la réunion des Γ_n , il existe n_0 tel que $F \subset \Gamma_{n_0}$. Considérons alors le vecteur $\xi \in H$ dont la composante selon H_{n_0} est $\delta_{\Gamma_{n_0}}$ et toutes les autres composantes sont nulles. Par définition, on a pour tout $g \in \Gamma_{n_0}$

$$\pi(g).\xi = \xi.$$

Ceci étant en particulier vrai pour tout $g \in F$, on a bien montré que π a des vecteurs presque invariants⁹.

Comme Γ a la propriété (T), π doit avoir un vecteur invariant non nul, qu'on notera ξ . Soit n_1 tel que la composante ξ_{n_1} de ξ sur n_1 soit non nulle. Alors, ξ_{n_1} est un vecteur invariant non nul pour π_{n_1} . Ce vecteur est une fonction de carré sommable sur les classes modulo Γ_{n_1} . Or, comme Γ agit transitivement sur ces classes, toute fonction invariante est constante. Ainsi, il existe une fonction constante non nulle dans $\ell^2(\Gamma/\Gamma_{n_1})$, ce qui implique que l'ensemble Γ/Γ_{n_1} est fini. Alors, l'ensemble S formé par les générateurs de Γ_{n_1} ainsi qu'un représentant de chaque classe modulo Γ_{n_1} est une partie génératrice finie de Γ , ce qui conclut. ■

De ce résultat, on peut aisément tirer deux corollaires intéressants. Le premier généralise le Corollaire 2.6.

Corollaire 2.10. Soit Γ un groupe abélien discret qui possède la propriété (T). Alors, Γ est fini.

Démonstration. Par le Théorème 2.9, Γ est de type fini et on conclut par la proposition 2.5. ■

Le second donne une propriété de finitude remarquable.

Corollaire 2.11. Soit Γ un groupe dénombrable avec la propriété (T), alors son abélianisé $\Gamma/[\Gamma, \Gamma]$ est fini.

9. On remarquera que le δ ne joue aucun rôle, nous avons en fait montré que pour toute partie finie, il existe un vecteur invariant par l'image de cette partie!

Démonstration. L'abélianisé d'un groupe discret étant un groupe abélien discret, il suffit de prouver que la propriété (T) passe au quotient. Soit donc $\phi : \Gamma \rightarrow \Lambda$ un morphisme de groupes surjectifs et soit $\pi : \Lambda \rightarrow \mathcal{U}(H)$ une représentation unitaire admettant des vecteurs presque invariants. Nous allons considérer la représentation

$$\tilde{\pi} = \pi \circ \phi : \Gamma \rightarrow \mathcal{U}(H).$$

Soit $F \subset \Gamma$ finie et $\delta > 0$. Alors, $\phi(F)$ étant finie, il existe un vecteur non nul $\xi \in H$ tel que

$$\sup_{h \in \phi(F)} \|\pi(h).\xi - \xi\| \leq \delta \|\xi\|.$$

Mais alors,

$$\sup_{g \in F} \|\tilde{\pi}(g).\xi - \xi\| = \sup_{h \in \phi(F)} \|\pi(h).\xi - \xi\| \leq \delta \|\xi\|.$$

Autrement dit, ξ est $(\tilde{\pi}(F), \delta)$ -invariant. Comme Γ a la propriété (T), il existe donc un vecteur non nul $\eta \in H$ tel que $\tilde{\pi}(g).\eta = \eta$ pour tout $g \in \Gamma$. Comme ϕ est surjective, ceci implique que $\pi(h).\eta = \eta$ pour tout $h \in \Lambda$, donc que π a un point fixe. Ainsi, Λ a bien la propriété (T). ■

Ce résultat peut se voir comme une propriété cohomologique : en effet, l'abélianisé de Γ est le premier groupe de cohomologie à coefficients entiers $H^1(\Gamma, \mathbb{Z})$. Ce résultat permet également de montrer facilement que des groupes n'ont pas la propriété (T), comme par exemple les groupes libres puisque leurs abélianisés sont des groupes abéliens libres, donc infinis.

2.3 UN MOT D'HISTOIRE

Avant d'appliquer la propriété (T) aux familles de graphes expanseurs, nous voudrions ouvrir une petite parenthèse pour expliquer l'étrange notation (T) de la Définition 2.3. Pour ce faire, il faut considérer l'ensemble des représentations unitaires d'un groupe discret donné Γ d'un point de vue topologique. Plus précisément, étant donné une représentation unitaire π de Γ sur un espace de Hilbert H , $F \subset \Gamma$ finie, $\delta > 0$ et $\xi \in H$ un vecteur de norme 1, on voudrait poser

$$V(\pi, F, \delta, \xi) = \{(\rho, K) \mid \exists \eta \in H, \|\eta\| = 1, |\langle \pi(g).\xi, \xi \rangle - \langle \rho(g).\eta, \eta \rangle| < \delta \text{ pour tout } g \in F\}.$$

Telle qu'elle est écrite, cette définition n'a pas de sens puisque les représentations unitaires ne forment pas un ensemble. Pour lever cette difficulté, on peut commencer par travailler à équivalence près. Deux représentations unitaires (π, H) et (ρ, K) d'un groupe Γ sont dites (*unitairement*) *équivalentes* s'il existe un opérateur unitaire $U : H \rightarrow K$ tel que pour tout $g \in \Gamma$, $U\pi(g) = \rho(g)U$. On note alors $\pi \sim \rho$. On voit immédiatement que si $\pi' \sim \pi$ et $\rho' \sim \rho$, alors $\rho \in V(\pi, F, \delta, \xi)$ si et seulement si $\rho' \in V(\pi', F, \delta, \xi)$. On peut donc considérer des classes d'équivalences de représentations. Il n'est toujours pas clair que celles-ci forment un ensemble, mais on peut s'y ramener.

DEFINITION 2.12. Soit \mathcal{R} un ensemble de classes d'équivalences de représentations unitaires d'un groupe discret Γ . Les ensembles

$$V(\pi, F, \delta, \xi) \cap \mathcal{R}$$

forment une base de voisinages pour une topologie sur \mathcal{R} , appelée *topologie de Fell*.

On a alors la caractérisation suivante de la propriété (T), qui est en fait la définition originelle de [Kaz67]. Rappelons que la *représentation triviale* de Γ est la représentation unitaire $\pi_T : \Gamma \rightarrow \mathbb{C} \simeq \mathcal{U}(\mathbb{C})$ telle que $\pi_T(g) = 1$ for all $g \in \Gamma$.

Proposition 2.13. *Un groupe discret Γ a la propriété (T) si et seulement si pour tout ensemble \mathcal{R} de classes d'équivalence de représentations irréductibles sans vecteur invariant non nul, la représentation triviale est isolée pour la topologie de Fell sur l'ensemble $\mathcal{R} \cup \{\pi_T\}$.*

Avant de démontrer ce résultat, expliquons l'origine de la terminologie : la lettre T désigne la représentation triviale du groupe Γ , et les parenthèses qui l'entourent signifient son isolement ... dans la topologie de Fell.

Démonstration. L'idée principale de la démonstration est de remarquer qu'une suite¹⁰ $(\pi_n)_{n \in \mathbb{N}}$ de représentation unitaire converge vers π_T pour la topologie de Fell si et seulement si $\bigoplus_{n \in \mathbb{N}} \pi_n$ admet des vecteurs presque invariants. En observant en outre qu'une telle somme hilbertienne a un vecteur invariant non nul si et seulement si l'un de ses facteurs a un vecteur invariant non nul, on obtient le résultat. Nous renvoyons à [BdlHV08] pour de plus amples détails. ■

3 RETOUR À L'EXPANSION

3.1 DE LA PROPRIÉTÉ (T) AUX FAMILLES D'EXPANSEURS

Nous avons maintenant tous les outils en main pour montrer l'existence de familles de graphes expandeurs. Comme on va le voir, la propriété (T) suffit à obtenir le résultat, et la preuve issue de [Mar73] est de plus très élémentaire. Rappelons qu'une partie S d'un groupe Γ est dite *symétrique* si $S = S^{-1}$.

THÉORÈME 3.1 (Margulis) Soit Γ un groupe discret avec la propriété (T) possédant des sous-groupes normaux $(\Gamma_n)_{n \in \mathbb{N}}$ d'indice fini tels que

$$[\Gamma : \Gamma_n] \rightarrow \infty.$$

Soit $S \subset \Gamma$ une partie génératrice symétrique finie et, pour $n \in \mathbb{N}$, S_n son image dans le quotient Γ/Γ_n . Alors, la famille de graphes

$$G_n = \text{Cay}(\Gamma/\Gamma_n, S_n)$$

est une famille d'expandeurs.

Démonstration. Remarquons tout d'abord que, conformément à notre stratégie initiale, les graphes G_n sont tous $|S|$ -réguliers, et que cette partie de la définition d'une famille d'expandeurs est donc vérifiée par construction. De même, le nombre d'arêtes de G_n , étant égal à l'indice de Γ_n , tend vers $+\infty$. Il reste donc à minorer uniformément la constante d'expansion.

On sait par la Proposition 2.8 qu'il existe $\delta > 0$ tel que toute représentation unitaire possédant un vecteur (S, δ) -invariant possède un vecteur invariant non nul. Par contraposée, pour toute représentation unitaire $\pi : \Gamma \rightarrow \mathcal{U}(H)$ ne possédant pas de vecteur invariant non nul, on a pour tout $\xi \in H$ que

$$\sup_{s \in S} \frac{\|\pi(s) \cdot \xi - \xi\|}{\|\xi\|} \geq \delta.$$

10. La topologie de Fell n'étant pas métrisable en général, il faudrait travailler plus généralement avec des filtres, mais cela ne change pas le raisonnement.

Comme S est finie, cette borne supérieure est atteinte et il existe donc $s \in S$ tel que

$$\|\pi(s).\xi - \xi\| \geq \delta \|\xi\|.$$

Nous allons maintenant construire une représentation unitaire sans point fixe pour chaque entier $n \in \mathbb{N}$ en utilisant Γ_n . Plus précisément, on considère l'espace de Hilbert $\ell^2(V_n)$, où V_n est l'espace fini des arêtes du graphe $\text{Cay}(\Gamma/\Gamma_n, S_n)$, c'est-à-dire l'ensemble Γ/Γ_n des classes modulo Γ_n . On note $\pi_n : \Gamma \rightarrow \mathcal{U}(\ell^2(V_n))$ la représentation quasi-régulière déjà utilisée dans la démonstration du Théorème 2.9 qui est définie pour $g \in \Gamma$ et $f \in \ell^2(V_n)$ par ¹¹

$$\pi_n(g)f : h.\Gamma_n \mapsto f(g^{-1}h.\Gamma_n).$$

Comme l'action de Γ sur les classes à gauches modulo Γ_n est transitive, les seules fonctions invariantes pour cette représentation sont les fonctions constantes. Afin de n'avoir plus de vecteur invariant non nul, on peut donc se restreindre au sous-espace

$$H_n = \left\{ f \in \ell^2(V_n) \mid \sum_{x \in V_n} f(x) = 0 \right\}.$$

On vérifie alors aisément que cet espace est stable par $\pi_n(\Gamma)$: c'est l'orthogonal de l'espace des fonctions constantes. On a donc par restriction une représentation unitaire de Γ sur H_n , que nous noterons à nouveau π_n .

Pour estimer la constante d'expansion de G_n , prenons une partie $A \subset V_n$ telle que $|A| \leq |V_n|/2$. Pour alléger les notations, nous poserons

$$a = |A| \quad \& \quad b = |V_n| - a \geq a.$$

On définit la fonction suivante :

$$f_A : x \in V_n \mapsto \begin{cases} a & \text{si } x \in A \\ -b & \text{si } x \notin A \end{cases}$$

Par définition, $f \in H_n$ donc il existe $s \in S$ tel que

$$\|\pi_n(s).f_A - f_A\| \geq \delta \|f_A\|.$$

Nous allons maintenant calculer le membre de gauche de cette inégalité : on a

$$\pi_n(s).f_A : x \in V_n \mapsto \begin{cases} a & \text{si } x \in s.A \\ -b & \text{si } x \notin s.A \end{cases}$$

et donc

$$\pi_n(s).f_A - f_A : x \in V_n \mapsto \begin{cases} a+b & \text{si } x \notin A \quad \& \quad x \in s.A \\ -a-b & \text{si } x \in A \quad \& \quad x \notin s.A \\ 0 & \text{sinon} \end{cases}$$

Pour interpréter géométriquement ces quantités, notons $\partial_s A$ l'ensemble des arêtes de ∂A qui sont indexées par s , c'est-à-dire

$$\partial_s A = \{x \in A \mid s.x \notin A\} \cup \{x \notin A \mid s.x \in A\}.$$

Les deux ensembles ci-dessus ne sont pas nécessairement disjoints : ils le sont si $s \neq s^{-1}$, mais si $s^2 = 1$ ils sont égaux. Cela dit, dans tous les cas, on peut minorer $|\partial_s A|$ par la

11. Cette définition utilisant g^{-1} est compatible avec notre précédente définition $\pi(g)\delta_{h.\Gamma_n} = \delta_{gh.\Gamma_n}$.

moyenne des cardinaux des deux ensembles :

$$\begin{aligned}
|\partial_s A| &\geq \frac{1}{2} |\{x \in A \mid s.x \notin A\} \cup \{x \notin A \mid s.x \in A\}| \\
&= \frac{1}{2} \left\| \frac{\pi_n(s) \cdot f_A - f_A}{a+b} \right\|^2 \\
&= \frac{1}{2(a+b)^2} \delta^2 \|f_A\|^2 \\
&\geq \frac{\delta^2 ab^2 + ba^2}{2(a+b)} \\
&= \frac{\delta^2 ab}{2(a+b)}.
\end{aligned}$$

En observant que l'inégalité $b \geq a$ implique

$$\frac{b}{a+b} \geq \frac{1}{2},$$

on peut conclure que

$$\begin{aligned}
\frac{|\partial A|}{|A|} &= \frac{|\partial A|}{a} \\
&\geq \frac{|\partial_s A|}{a} \\
&\geq \frac{\delta^2 ab}{2(a+b)a} \\
&= \frac{\delta^2 b}{2(a+b)} \\
&\geq \frac{\delta^2}{4}.
\end{aligned}$$

Comme A était arbitraire, nous avons montré que $h(G_n) \geq \delta^2/4$, ce qui conclut la preuve. ■

Avant d'appliquer ce théorème, nous voudrions faire quelques commentaires.

- Nous n'avons pas vraiment utilisé le fait que les sous-groupes Γ_n étaient distingués, si ce n'est pour construire le graphe de Cayley. Or, cette dernière construction se généralise sans peine au cas de sous-groupes arbitraires sous le nom de *graphe de Schreier*, et cela suffit à faire fonctionner la preuve. Ainsi, l'hypothèse Γ_n distingué peut être retirée.
- Les représentations π_n sont en fait la composition du morphisme quotient $\phi_n : \Gamma \rightarrow \Gamma/\Gamma_n$ avec la représentation régulière de Γ/Γ_n . Ainsi, nous n'avons utilisé la propriété (T) que pour des représentations se factorisant par un quotient fini. On dit qu'un groupe a la *propriété* (τ) si toute représentation unitaire se factorisant par un quotient fini qui admet des vecteurs presque invariants admet un vecteur invariant non nul. On le voit, cette propriété est suffisante pour faire fonctionner la preuve, et est satisfaite par beaucoup plus de groupes. Nous renvoyons à [Lub94] pour plus de détails à ce sujet.

3.2 UN EXEMPLE (PRESQUE) EXPLICITE

Rappelons que notre objectif était de prouver l'existence d'une famille de graphes *expanseurs*, voire d'être capable d'en construire une explicitement. Pour ce faire, il nous reste à trouver un groupe satisfaisant les hypothèses du Théorème 3.1. Le plus dur pour cela est de trouver un groupe infini avec la propriété (T). Nous utiliserons le suivant :

THÉORÈME 3.2 Le groupe $\mathrm{SL}_3(\mathbb{Z})$ a la propriété (T).

Nous donnerons plus loin une idée de la démonstration, mais avant cela nous allons montrer comment appliquer le Théorème 3.1 à cet exemple. Pour tout entier n , le morphisme d'anneaux surjectifs $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ induit un morphisme de groupes surjectifs

$$\phi_n : \mathrm{SL}_3(\mathbb{Z}) \rightarrow \mathrm{SL}_3(\mathbb{Z}/n\mathbb{Z}).$$

On pose $\Gamma = \mathrm{SL}_3(\mathbb{Z})$ et $\Gamma_n = \ker(\phi_n)$. Par construction, il s'agit de sous-groupes d'indice fini et comme le cardinal des quotients tend vers $+\infty$ quand n tend vers $+\infty$, il en va de même pour les indices des noyaux. On peut ainsi appliquer le Théorème 3.1. Pour conclure, il nous reste à trouver une partie génératrice finie de $\mathrm{SL}_3(\mathbb{Z})$, ce qui n'est pas très difficile : nous avons tous appris dans notre jeunesse que $\mathrm{SL}_n(\mathbb{Z})$ est engendré par les matrices de transvections ! Nous pouvons ainsi conclure qu'en notant S l'ensemble des matrices de transvections et de leurs inverses, les graphes

$$\mathrm{Cay}(\mathrm{SL}_3(\mathbb{Z}/n\mathbb{Z}), \phi_n(S))$$

forment une famille d'expandeurs.

Pour conclure, nous allons donner les grandes étapes de la preuve de la propriété (T) pour $\mathrm{SL}_3(\mathbb{Z})$. L'argument originel de D. Kazhdan dans [Kaz67] repose sur le fait que $\mathrm{SL}_3(\mathbb{Z})$ est un réseau dans $\mathrm{SL}_3(\mathbb{R})$, et qu'il suffit donc ¹² de démontrer la propriété (T) pour ce dernier. Comme nous n'avons pas introduit le cadre général des groupes localement compacts, nous allons donner une autre preuve, moins directe mais tout aussi élégante, due à Y. Shalom [Sha99].

Démonstration du Théorème 3.2. Commençons par considérer les trois sous-groupes suivants dans $\mathrm{SL}_3(\mathbb{Z})$:

$$\begin{aligned} \Gamma &= \left\{ \left(\begin{array}{ccc} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{array} \right) \middle| a, b, c, d, \in \mathbb{Z}, ad - bc = 1 \right\} \\ \Lambda_1 &= \left\{ \left(\begin{array}{ccc} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{array} \right) \middle| a, b \in \mathbb{Z} \right\} \\ \Lambda_2 &= \left\{ \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & b & 1 \end{array} \right) \middle| a, b \in \mathbb{Z} \right\} \end{aligned}$$

Il est clair sur la définition que $\Gamma \cong \mathrm{SL}_2(\mathbb{Z})$ et que $\Lambda_i \cong \mathbb{Z}^2$. De plus, l'action par conjugaison de Γ sur Λ_i coïncide avec l'action matricielle de $\mathrm{SL}_2(\mathbb{Z})$ sur \mathbb{Z}^2 . En particulier, Γ normalise Λ_i et ils engendrent à eux deux le groupe $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$.

Les groupes que nous venons de construire ont deux propriétés remarquables. La première c'est qu'ils engendrent le groupe $\mathrm{SL}_3(\mathbb{Z})$ de façon bornée : pour tout $M \in \mathrm{SL}_3(\mathbb{Z})$, il existe $A_1, B_1 \in \Lambda_1$, $A_2, B_2 \in \Lambda_2$ et $C \in \Gamma$ tels que

$$M = A_1 A_2 B_1 B_2 C.$$

Ceci se démontre facilement avec un peu d'algèbre linéaire et d'arithmétique modulaire. La seconde, c'est que l'inclusions $\mathbb{Z}^2 \subset \mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ satisfait la propriété (T) relative : toute

¹². C'est l'un des résultats importants de [Kaz67] qu'un groupe localement compact a la propriété (T) si et seulement si tous ses réseaux l'ont.

représentation unitaire π de $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ qui admet des vecteurs presque invariants admet un vecteur $\pi(\mathbb{Z}^2)$ -invariant non nul. Il s'agit d'un résultat hautement non-trivial et fondamental dû à G. Margulis. Nous renvoyons par exemple à [BO08, Théorème 12.1.10] pour une démonstration.

Si maintenant π est une représentation unitaire admettant des vecteurs presque invariants, la restriction de π au sous-groupe engendré par Γ et Λ_i admet également des vecteurs presque invariants, donc elle admet des vecteurs $\pi(\Lambda_i)$ -invariants non nuls. C'est ici que les choses se corsent. En effet, il n'est pas difficile de voir que Λ_1 et Λ_2 engendrent¹³ à eux deux tout le groupe $\mathrm{SL}_3(\mathbb{Z})$. Le problème, c'est qu'ils n'ont pas de raison d'avoir un vecteur fixe non nul en commun. La démonstration procède donc par l'absurde, en supposant qu'il n'y en a pas, selon le schéma suivant :

1. Si P_i désigne la projection orthogonale sur l'espace des vecteurs $\pi(\Lambda_i)$ invariants, alors l'absence de vecteur invariant non nul se traduit par le fait que 1 n'est pas dans le spectre de

$$T = \frac{P_1 + P_2}{2}.$$

2. D'autre part, l'existence de vecteurs presque invariants permet de montrer qu'il existe $\epsilon > 0$ tel que $[1 - \epsilon; 1] \cap \mathrm{Sp}(T) \neq \emptyset$. Par le premier point, il existe également $\delta > 0$ tel que $[1 - \epsilon; 1 - \delta] \cap \mathrm{Sp}(T) \neq \emptyset$.
3. On définit par calcul fonctionnel borélien l'opérateur $Q = \mathbf{1}_{[1 - \epsilon; 1 - \delta]}(T)$ et on montre qu'il commute "presque" à $\pi(\Lambda_1)$ et $\pi(\Lambda_2)$, et qu'il commute *exactement* à $\pi(\Gamma)$.
4. La propriété de génération bornée permet d'en déduire que T commute également "presque" à $\pi(\mathrm{SL}_3(\mathbb{Z}))$ avec un contrôle précis sur le défaut.
5. On utilise ce dernier résultat quantitatif pour obtenir une inégalité sur Q qui contredit sa définition.

■

RÉFÉRENCES

- [BdlHV08] B. BEKKA, P. DE LA HARPE & A. VALETTE – *Kazhdan's property (T)*, New Mathematical Monographs, vol. 11, Cambridge university press, 2008.
- [BK93] Y. BARZDIN & A. KOLMOGOROV – « On the realization of networks in three-dimensional space », *Selected Works of A.N. Kolmogorov : Volume III : Information Theory and the Theory of Algorithms* (1993), p. 194–202.
- [BO08] N. P. BROWN & N. OZAWA – *C*-algebras and finite-dimensional approximation*, Graduate Studies in Mathematics, vol. 88, American Mathematical Society, 2008.
- [Kaz67] D. KAZHDAN – « Connection of the dual space of a group with the structure of its subgroups », *Funct. Anal. Appl.* **1** (1967), p. 63–65.
- [KKN21] M. KALUBA, D. KIELAK & P. NOWAK – « On property (T) for $\mathrm{Aut}(\mathbb{F}_n)$ and $\mathrm{SL}_n(\mathbb{Z})$ », *Ann. Math.* **193** (2021), no. 2, p. 539–562.
- [KNO19] M. KALUBA, P. NOWAK & N. OZAWA – « $\mathrm{Aut}(\mathbb{F}_5)$ has property (T) », *Math. Annalen* **375** (2019), p. 1169–1191.
- [Lub94] A. LUBOTZKY – *Discrete groups, expanding graphs and invariant measures*, Progress in Mathematics, vol. 125, Birkhäuser Verlag, Basel, 1994, with an appendix by J. D. Rogawski.

13. Mais cette fois-ci pas de façon bornée.

-
- [Mar73] G. A. MARGULIS – « Explicit constructions of expanders », *Problemy Peredači Informacii* **9** (1973), no. 4, p. 71–80.
- [Mil21] J. MILNE – « Group theory (v4.00) », 2021, Available at www.jmilne.org/math/, p. 139.
- [Pin73] M. PINSKER – « On the complexity of a concentrator », in *7th International Teletraffic Conference*, vol. 4, 1973, p. 1–318.
- [Sha99] Y. SHALOM – « Bounded generation and Kazhdan’s property (T) », *Publications Mathématiques de L’IHÉS* **90** (1999), no. 1, p. 145–168.

A LA STRUCTURE DES GROUPES ABÉLIENS DE TYPE FINI

Nous avons utilisé plus haut un résultat de structure sur les groupes abéliens de type fini : ce sont des produits de groupes cycliques. Par soucis de donner un exposé complet, nous allons en donner une démonstration élémentaire tirée de [Mil21]. La démonstration repose sur l'analyse des relations possibles entre générateurs d'un tel groupe, aussi aurons-nous besoin du résultat suivant.

Lemme A.1. *Soit Γ un groupe abélien engendré par des éléments x_1, \dots, x_n . Pour tous $c_1, \dots, c_n \in \mathbb{N}$ tels que $\text{pgcd}(c_1, \dots, c_n) = 1$, il existe des générateurs y_1, \dots, y_n de Γ tels que*

$$y_1 = \sum_{i=1}^n c_i x_i.$$

Démonstration. La démonstration se fait par récurrence sur l'entier

$$s = \sum_{i=1}^n c_i.$$

Si $s = 1$, alors il existe i_0 tel que $c_{i_0} = 1$ et tous les autres coefficients sont nuls. On pose alors $y_1 = x_{i_0}$, $y_{i_0} = x_1$ et $y_j = x_j$ pour tout $j \notin \{1, i_0\}$.

Si le résultat est vrai jusqu'à un certain $s - 1 \geq 0$, et si la somme des coefficients vaut s , alors il y a au moins deux coefficients non nuls. Quitte à changer les indices, nous supposons que $c_1 \geq c_2 > 0$. Alors,

- $\{x_1, x_2 + x_1, x_3, \dots, x_n\}$ engendrent Γ ;
- $\text{pgcd}(c_1 - c_2, c_2, \dots, c_n) = 1$;
- $(c_1 - c_2) + c_2 + \dots + c_n < s$;

on peut donc appliquer l'hypothèse de récurrence pour trouver des générateurs y_1, \dots, y_n tels que

$$y_1 = (c_1 - c_2)x_1 + c_2x_2 + \sum_{i=3}^n c_i x_i = \sum_{i=1}^n c_i x_i,$$

ce qui conclut. ■

THÉORÈME A.2 Soit Γ un groupe abélien de type fini, alors Γ est un produit de groupes cycliques.

Démonstration. Nous allons procéder par récurrence sur le nombre n de générateurs de Γ . Si $n = 1$, Γ est cyclique, ce qui conclut. Supposons le résultat vrai pour un certain n et soit Γ un groupe abélien qui ne peut être engendré par moins de $n + 1$ éléments. Parmi toutes les parties génératrices (x_1, \dots, x_{n+1}) de Γ , on en choisit une pour laquelle l'ordre de x_1 est minimal. Supposons maintenant qu'il existe une relation

$$a_1x_1 + \dots + a_{n+1}x_{n+1} = 0$$

dans Γ avec $a_1x_1 \neq 0$. Quitte à remplacer x_i par son inverse, on peut supposer que $a_i \geq 0$ pour tout $1 \leq i \leq n + 1$. On peut de plus aussi supposer $0 < a_1 < o(x_1)$. Posons alors

$$d = \text{pgcd}(a_1, \dots, a_{n+1})$$

et $c_i = a_i/d$. D'après le Lemme A.1, il existe une partie génératrice y_1, \dots, y_{n+1} telle que

$$y_1 = c_1x_1 + \dots + c_{n+1}x_{n+1}.$$

Mais alors, l'ordre de y_1 divise d , puisque

$$dy_1 = \sum_{i=1}^{n+1} dc_i x_i = \sum_{i=1}^{n+1} a_i x_i = 0.$$

Or, $0 < d < a_1$, donc ceci contredit la minimalité de l'ordre de x_1 .

Ainsi, il n'existe aucune relation entre x_1 et les autres générateurs, ce qui signifie que Γ est le produit du sous-groupe engendré par x_1 et de celui engendré par x_2, \dots, x_{n+1} . On conclut alors par l'hypothèse de récurrence. ■