Le théorème de Freiman-Ruzsa

Weikun He - Joseph Thirouin

Sous la direction de Harald Helfgott
juin 2011

Remerciements

Nous voudrions remercier en premier lieu Harald Helfgott, qui s'est montré, pendant toute la préparation de ce mémoire, toujours disponible et enthousiaste, malgré toutes ses occupations.

Nos remerciements vont aussi à Nicolas Curien, qui nous a bien aidés à mettre au point l'argument de théorie de la mesure du lemme 4.2, avec patience et pédagogie, alors qu'il soutenait sa thèse le surlendemain. Nous remercions également Arthur-César Le Bras, qui a relu le texte de notre travail avec application ; son œil scrutateur nous a permis d'éviter bien des fautes.

Qu'il nous soit permis de remercier enfin Ben Green, que nous ne connaissons pas, mais dont les notes [5] nous ont été d'un immense secours. Elles constituent une excellente porte d'entrée pour ce sujet : elles sont parfaitement rédigées, et non dénuées d'une touche d'humour, qui en rend la lecture très plaisante.

Table des matières

Introduction

0.1 Notations

Sommes ensemblistes

Soit A un sous-ensemble quelconque d'un groupe G, dont $+$ est la loi de composition. On note $A+A$ l'ensemble des sommes de deux éléments de A :

$$A+A = \left\{a+a' \mid (a,a') \in A^2\right\}.$$

De façon plus générale, étant donnés k, l deux entiers, $kA-lA$ est l'ensemble des éléments du type

$$a_1 + a_2 + \cdots + a_k - a'_1 - a'_2 - \cdots - a'_l,$$

où $(a_1, \ldots, a_k, a'_1, \ldots, a'_l) \in A^k \times A^l$.

Si de plus $B \subseteq G$, on utilisera aussi les notations $A+B$, et $kA+lB$.

Le cardinal d'un ensemble fini E (*i.e.* le nombre d'éléments qu'il contient) est noté $|E|$. Nous n'aurons jamais recours aux cardinaux infinis.

Progressions arithmétiques

Supposons G abélien pour $+$. Soient $x, r \in G$ et m un entier positif. On peut considérer la progression arithmétique standard de raison r et de premier terme x :

$$P = \{x + jr \mid 0 \leq j < m\}.$$

Si on suppose que $|P| = m$, alors $|P+P| \leq 2m$, soit $|P+P| \leq 2|P|$. Les progressions arithmétiques standard ont donc un « petit » ensemble somme.

Le théorème de Freiman-Ruzsa donne, de façon spectaculaire, une réciproque : il affirme que les seuls ensembles à posséder un petit ensemble somme (au sens du théorème 0.2) sont en fait des progressions arithmétiques, à condition de généraliser la notion de progression arithmétique comme suit :

Définition. On dit que P est une progression arithmétique généralisée si c'est une somme (ensembliste) de progressions arithmétiques standard, autrement dit s'il existe $d \in \mathbb{N}^*$, ainsi que $x, r_1, \ldots, r_d \in G$ et $m_1, \ldots, m_d$ entiers positifs, tels que

$$P = \{x + j_1 r_1 + j_2 r_2 + \cdots + j_d r_d \mid 0 \leq j_i < m_i \text{ pour } 1 \leq i \leq d\}.$$

La *dimension* de P est l'entier d, la *taille* de P est le produit $m_1 m_2 \cdots m_d$.

On dit de plus que P est *propre* si $|P| = m_1 m_2 \cdots m_d$.

Remarquons que si P est une progression propre, avec les mêmes notations que dans la définition, alors

$$P+P \subseteq \{2x + j'_1 r_1 + j'_2 r_2 + \cdots + j'_d r_d \mid 0 \leq j'_i < 2m_i \text{ pour } 1 \leq i \leq d\},$$

de sorte que $|P+P| \leq (2m_1)(2m_2)\cdots(2m_d) \leq 2^d|P|$. Dans ce cas, P a donc un petit ensemble somme. On a également $|P-P| \leq 2^d|P|$.

Par un calcul semblable, on peut établir un lemme qui prouve la souplesse des progressions arithmétiques généralisées :

Lemme 0.1. *Soient P, Q deux progressions arithmétiques généralisées, de dimensions respectives d_P et d_Q, et de tailles respectives t_P et t_Q. Alors*

(i) $-P$ *est une progression arithmétique de dimension d_P et de taille t_P.*

(ii) $P + Q$ *est une progression arithmétique de dimension $\leq d_P + d_Q$ et de taille $\leq t_P t_Q$.*

0.2 Le théorème de Freiman-Ruzsa dans $\mathbb{Z}$

Nous pouvons déjà énoncer le résultat que nous allons nous attacher à prouver :

Théorème 0.2 (Freiman-Ruzsa)**.** *Soit $A \subseteq \mathbb{Z}$, tel que $|A + A| \leq C|A|$, avec C une constante réelle. Alors A est contenu dans une progression arithmétique généralisée,*

- *de dimension inférieure à $d(C)$,*
- *de taille inférieure à $f(C)|A|$,*

avec

$$d(C) = C \cdot \mathrm{e}^{K(\log C)^{\frac{1}{2}}}, \quad f(C) = \exp\left(C \cdot \mathrm{e}^{K(\log C)^{\frac{1}{2}}}\right),$$

où $K \in \mathbb{R}$ est une constante.

L'énoncé de ce théorème appelle quelques commentaires. Il s'agit d'un théorème qui donne un résultat de structure sur un ensemble à partir de la simple connaissance de la cardinalité de son ensemble somme. À mal le considérer, l'énoncé du théorème peut paraître oiseux, car il est clair que tout sous-ensemble fini $A \subseteq \mathbb{Z}$ est recouvert par une progression arithmétique, ne serait-ce que par la progression de raison 1 et de premier terme $\min A$. Ce serait négliger l'aspect quantitatif du théorème et l'importance des bornes qu'il fournit sur la taille et la dimension de la progression [*]. En effet, l'aspect non trivial du théorème est que ces bornes ont une certaine uniformité : elles ne dépendent que de $|A + A|/|A|$, autrement dit de la manière dont A grossit lorsqu'on le somme avec lui-même.

Donnons un exemple simple : l'ensemble $A_n = \{1, 2, n\}$ peut être recouvert par la progression P_n de raison 1 et de premier terme 1, mais la taille de P_n n'est pas bornée quand $n \to \infty$, alors que le théorème assure qu'il est possible de trouver une progression Q_n contenant A_n de taille uniformément bornée en n.

0.3 L'énergie

Nous définissons dès à présent une notion fort utile dans la suite :

Définition (Énergie)**.** Soient $X, Y \subseteq G$. On définit un ensemble

$$\mathcal{Q} = \left\{(x, x', y, y') \in X^2 \times Y^2 \mid x + y = x' + y'\right\}.$$

L'énergie de X et Y est $\mathsf{E}(X, Y) = |\mathcal{Q}|$.

∗. Celles du théorème 0.2 sont parmi les meilleures connues à ce jour : on a $d(C) = C^{1+\circ(1)}$ et $f(C) = \exp(C^{1+\circ(1)})$. Elles sont dues à T. Schoen, qui les établit dans [13]. T. Sanders, par d'autres méthodes, démontre aussi le théorème avec de très bonnes bornes dans [12], dans un groupe abélien général qui plus est.

Remarquons brièvement que si G est abélien, $\mathsf{E}(X,Y) = \mathsf{E}(Y,X)$.

On peut déjà pressentir que si $X+Y$ est petit, l'application $(x,y) \mapsto x+y$ aura un « grand défaut » d'injectivité, qu'alors chaque élément de $X+Y$ aura beaucoup d'écritures possibles, et donc que l'énergie de X et Y sera grande. C'est le résultat que formalise le lemme 0.4 ci-après.

Introduisons une notation : soient $A_1, \dots, A_m$ des sous-ensembles de G quelconques. Pour $x \in G$, on note $r_{A_1+\cdots+A_m}(x)$ le nombre de « représentations », *i.e.* le nombre d'écritures possibles de x comme une somme d'un élément de A_1, …, et d'un élément de A_m (éventuellement nul) :

$$r_{A_1+\cdots+A_m}(x) = |\{(a_1,\dots,a_m) \in A_1 \times \cdots \times A_m \mid x = a_1 + \cdots + a_m\}|.$$

En particulier, $x \in A_1 + \cdots + A_m$ si et seulement si $r_{A_1+\cdots+A_m}(x) > 0$.

Lemme 0.3. *Si $X, Y \subseteq G$ abélien, alors*

$$\mathsf{E}(X,Y) = \sum_{z \in G} r_{X+Y}(z)^2.$$

Preuve. En effet, on peut restreindre la somme à $X+Y$. Alors, si $z \in X+Y$, et si $(x,y), (x',y')$ sont deux représentations de z (non nécessairement distinctes), alors $(x,x',y,y') \in \mathcal{Q}$. Réciproquement, si $(x,x',y,y') \in \mathcal{Q}$, alors (x,y) et (x',y') sont deux représentations de $x+y$. □

Lemme 0.4. *Si $X, Y \subseteq G$ abélien, alors*

$$\mathsf{E}(X,Y) \geq \frac{|X|^2|Y|^2}{|X+Y|}.$$

Ce résultat corrobore la remarque intuitive que nous avons faite : plus $X+Y$ est petit, plus l'énergie est grande.

Preuve du lemme 0.4. La preuve repose simplement sur l'inégalité de Cauchy-Schwarz. Écrivons

$$|X||Y| = \sum_{z \in X+Y} r_{X+Y}(z) \leq \sqrt{\sum_{z \in X+Y} r_{X+Y}(z)^2} \sqrt{\sum_{z \in X+Y} 1^2}.$$

La première égalité provient de ce que chaque élément $(x,y) \in X \times Y$ est compté une et une seule fois dans la somme (à savoir dans $r_{X+Y}(x+y)$).

Élevons au carré pour trouver, grâce au lemme précédent,

$$\mathsf{E}(X,Y) \cdot |X+Y| \geq |X|^2|Y|^2$$

ce qui est le résultat cherché. □

1 Les inégalités de Plünnecke-Ruzsa

Ici, $(G,+)$ désigne un groupe abélien. Le but de cette partie est de prouver que si $B \subseteq G$ est tel que $B+B$ est petit, alors $kB-lB$ est petit pour tous k,l. Plus précisément, on prouve le théorème suivant :

Théorème 1.1 (Plünnecke-Ruzsa)**.** *Supposons que $B \subseteq G$ vérifie $|B+B| \leq C|B|$, avec C une constante réelle.*

Alors pour tous $k,l \in \mathbb{N}$ tels que $k+l>0$, on a l'inégalité

$$|kB-lB| \leq C^{k+l}|B|.$$

La preuve consiste en quelques résultats élémentaires.

1.1 L'inégalité triangulaire de Ruzsa

On commence par prouver un résultat très simple, qui joue cependant un rôle-clef par la suite.

Lemme 1.2. *Soient U,V,W des sous-ensembles quelconques de G. On a*

$$|U||V-W| \leq |U+V||U+W|.$$

Démonstration. Pour chaque $x \in V-W$, on fixe définitivement $(v(x),w(x)) \in V \times W$ tels que $x=v(x)-w(x)$. On considère l'application

$$\Phi : \begin{cases} U \times (V-W) \to & (U+V)\times(U+W) \\ (u,x) \mapsto & (u+v(x),u+w(x)) \end{cases}$$

Le lemme est prouvé si on montre que Φ est injective, ce qu'elle est en effet : si (a,b) est dans l'image de Φ, alors $x=a-b$ et u s'en déduit par $u=a-v(a-b)$. □

1.2 Le résultat principal

La proposition suivante est l'ingrédient principal de la preuve du théorème 1.1.

Proposition 1.3 (Petridis [9])**.** *Soient $A,B \subseteq G$ vérifiant pour un $K>0$:*

(i) $|A+B| = K|A|$.

(ii) $|Z+B| \geq K|Z|$ *pour tout sous-ensemble $Z \subseteq A$.*

Alors quel que soit $S \subseteq G$,

$$|A+B+S| \leq K|A+S|.$$

Démonstration. Ce résultat se démontre par récurrence sur la taille de l'ensemble S.

Si $S=\{s\}$, l'inégalité découle de *(i)*, car $|A+B+\{s\}| = |A+B|$ et $|A+\{s\}| = |A|$.

Supposons à présent le résultat démontré pour les ensembles de taille n. Soit S' un ensemble de taille $n+1$, que l'on écrit $S' = S \cup \{x\}$, avec $|S| = n$. Majorons d'abord grossièrement :

$$\begin{aligned} |A+B+S'| &= |(A+B+S) \cup (A+B+x)| \\ &\leq |A+B+S| + |A+B+x| \\ &\leq K(|A+S| + |A+x|), \end{aligned}$$

où la dernière inégalité provient de l'hypothèse de récurrence et de *(i)*. Malheureusement, l'inégalité $|A+S| + |A+x| \leq |A+S'|$ n'est vraie que si $A+x$ est disjoint de $A+S$. Cela donne cependant l'idée d'une majoration plus fine.

Posons W l'ensemble des éléments $a \in A$ tels que $a+x \in A+S$. Ainsi

$$|A+S'| = |(A+S) \cup ((A+x) \setminus (W+x))| = |A+S| + |A| - |W|.$$

D'autre part,

$$W+B+x \subseteq A+B+S, \qquad (\star)$$

et on a les majorations suivantes, en appliquant *(ii)* à W :

$$\begin{aligned} |A+B+S'| &= |(A+B+S) \cup ((A+B+x) \setminus (W+B+x))| \\ &\leq |A+B+S| + |A+B| - |W+B| \\ &\leq K(|A+S| + |A| - |W|) \\ &= K|A+S'|. \end{aligned}$$

□

1.3 Preuve des inégalités

Avec ce résultat, nous sommes armés pour prouver le théorème 1.1.

Preuve du théorème 1.1. Soit $B \subseteq G$ vérifiant $|B+B| \leq C|B|$ avec $C > 0$. Pour trouver K comme dans la proposition 1.3, l'idée est très simple : on choisit

$$K := \min_{\emptyset \subsetneq Z \subseteq B} \frac{|Z+B|}{|Z|}$$

et on appelle A le sous-ensemble de B qui réalise le minimum, de sorte qu'avec ce choix, les hypothèses *(i)* et *(ii)* de la proposition sont vérifiées.

Dès lors, pour tout $k > 1$, $|A+kB| = |A+B+(k-1)B| \leq K|A+(k-1)B|$, et par récurrence, on obtient que $|A+kB| \leq K^k|A|$.

Remarquons aussi que $K \leq C$ et que $|A| \leq |B|$.

Enfin, l'inégalité triangulaire de Ruzsa permet de se « débarrasser » de l'ensemble A :

$$\begin{aligned} |A||kB-lB| &\leq |A+kB||A+lB| \\ &\leq K^k|A|K^l|A| \\ &\leq C^{k+l}|A||B|, \end{aligned}$$

et il reste à simplifier par $|A| \neq 0$ pour conclure la preuve. □

2 Réduction du problème à $\mathbb{Z}/n\mathbb{Z}$

À partir de maintenant, nous nous limitons au cas où $G = \mathbb{Z}$, et où l'on se donne donc $A \subseteq \mathbb{Z}$, tel que $|A+A| \leq C|A|$, avec C une constante réelle. Il s'avère que toutes les propriétés que nous aimerions prouver à propos de notre ensemble A sont plus simples à démontrer pour des ensembles inclus dans un $\mathbb{Z}/n\mathbb{Z}$ (que nous noterons $\mathbb{Z}_n$, dans l'idée de se conformer aux usages qui prévalent dans la littérature). Par exemple, il est possible de faire de l'analyse de Fourier sur $\mathbb{Z}_p$, avec p premier. Nous commençons donc par montrer comment, dans une certaine mesure, on peut « passer » de $\mathbb{Z}$ à un $\mathbb{Z}_n$.

2.1 Les homomorphismes de Freiman

Pour que l'on puisse exploiter les propriétés des sous-ensembles de $\mathbb{Z}_n$, il faut néanmoins que ce passage préserve la structure additive des ensembles concernés, puisque c'est elle que nous étudions, ce qui justifie l'introduction des *homomorphismes de Freiman*.

Définition. Soit k un entier positif, A un sous-ensemble d'un groupe abélien G, et G' un autre groupe abélien.

- On dit que $\phi : A \to G'$ est un homomorphisme de Freiman d'ordre k (ou un k–homomorphisme) si pour tous $x_1, x_2, \ldots, x_{2k} \in A$ tels que $x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}$, on a aussi

$$\phi(x_1) + \cdots + \phi(x_k) = \phi(x_{k+1}) + \cdots + \phi(x_{2k}).$$

  Sans ambiguïté, ϕ définit donc une application sur kA.
- On dit que ϕ est un k–isomorphisme de Freiman si de plus ϕ est bijective, et si ϕ^{-1} est également un k–homomorphisme de Freiman.

Pour se convaincre de l'utilité de tels objets, et de leur adéquation aux problèmes sommatoires, nous prouvons un

Lemme 2.1. *Soient $A \subseteq G$ un groupe abélien, et G' un autre groupe abélien. Soit $\phi : A \to G'$ un homomorphisme de Freiman d'ordre 2. Si $P \subseteq A$ est une progression arithmétique (généralisée), alors $\phi(P)$ aussi.*

De plus, la dimension de $\phi(P)$ est inférieure à celle de P, et la taille de $\phi(P)$ est inférieure à celle de P.

Preuve. Soit $P = \{x + j_1 r_1 + j_2 r_2 + \cdots + j_d r_d \mid 0 \leq j_k < m_k \text{ pour } 1 \leq k \leq d\}$; notons aussi $P' := \phi(P)$. Si $0 \leq i_1 < m_1$, $0 \leq i_2 < m_2$, …, $0 \leq i_d < m_d$, on désigne par $P(i_1, i_2, \ldots, i_d)$ l'élément $x + i_1 r_1 + i_2 r_2 + \cdots + i_d r_d$ de P.

Comme pour tout $1 \leq k \leq d$, $r_k = (x+r_k) - x$, on introduit $s_k := \phi(x+r_k) - \phi(x)$. Dès lors, si on choisit $y \in P$, alors $y = P(i_1, i_2, \ldots, i_d)$, avec $0 \leq i_1 < m_1$, $0 \leq i_2 < m_2$, …, $0 \leq i_d < m_d$. Or $P(i_1, i_2, \ldots, i_d) - P(i_1 - 1, i_2, \ldots, i_d) = r_1$, donc $P(i_1, i_2, \ldots, i_d) + x = P(i_1 - 1, i_2, \ldots, i_d) + (x + r_1)$, et en appliquant la propriété d'homomorphisme d'ordre 2 de ϕ, on trouve $\phi(P(i_1, i_2, \ldots, i_d)) + \phi(x) = \phi(P(i_1 - 1, i_2, \ldots, i_d)) + \phi(x + r_1)$, soit enfin

$$\phi(P(i_1, i_2, \ldots, i_d)) - \phi(P(i_1 - 1, i_2, \ldots, i_d)) = s_1.$$

Comme le raisonnement que nous venons de faire ne dépend par de la valeur de i_1, on peut le réitérer, et on obtient ainsi

$$\begin{aligned}\phi(P(i_1,i_2,\dots,i_d)) - \phi(P(0,i_2,\dots,i_d)) \\ &= \sum_{l=0}^{i_1-1} \phi(P(i_1-l,i_2,\dots,i_d)) - \phi(P(i_1-(l+1),i_2,\dots,i_d)) \\ &= i_1 s_1.\end{aligned}$$

En recommençant le même travail avec la deuxième composante, et en poursuivant jusqu'à la d^{e}, on finit par trouver

$$\phi(P(i_1,i_2,\dots,i_d)) - \phi(P(0,0,\dots,0)) = i_1 s_1 + i_2 s_2 + \cdots + i_d s_d,$$

d'où $\phi(x + i_1 r_1 + i_2 r_2 + \cdots + i_d r_d) = \phi(x) + i_1 s_1 + i_2 s_2 + \cdots + i_d s_d$. Autrement dit, on peut écrire P' comme la progression arithmétique

$$P' = \{\phi(x) + j_1 s_1 + j_2 s_2 + \cdots + j_d s_d \mid 0 \leq j_k < m_k \text{ pour } 1 \leq k \leq d\}$$

dont la taille et la dimension sont bien inférieures à celles de P (en effet, rien n'interdit par exemple d'avoir $s_1 = s_2$). □

2.2 Le résultat de Ruzsa

Proposition 2.2 (Ruzsa)**.** *Soit $A \subseteq \mathbb{Z}$ tel que $|A+A| \leq C|A|$. Étant donnés $k \geq 2$ et $m > C^{2k}|A|$ des entiers, il existe un sous-ensemble $A' \subseteq A$ qui est k–isomorphe à un sous-ensemble de $\mathbb{Z}_m$.*

De plus, $|A'| \geq |A|/k$.

Démonstration. La preuve est constructive, de là un peu technique. Soit p un nombre premier à ajuster. On considère la suite

$$\mathbb{Z} \xrightarrow{\psi_1} \mathbb{Z}_p \xrightarrow{\psi_2(q)} \mathbb{Z}_p \xrightarrow{\psi_3} \mathbb{Z} \xrightarrow{\psi_4} \mathbb{Z}_m$$

où l'on a noté

- $\psi_1 : s \mapsto \bar{s}$ la réduction modulo p,
- $\psi_2(q)$ la multiplication par q à déterminer dans $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{\bar{0}\}$,
- ψ_3 l'injection qui à $\bar{s} \in \mathbb{Z}_p$ associe $s \in \{0,\dots,p-1\}$ tel que $\bar{s} \equiv_p s$,
- ψ_4 la réduction modulo m.

Les applications $\psi_1, \psi_2(q)$ et ψ_4 sont des homomorphismes de Freiman de tout ordre (car ce sont des morphismes de groupe). L'application ψ_3 est un k–homomorphisme quand elle est restreinte aux entiers modulo p compris dans l'intervalle $I_j = \left]\frac{j-1}{k}p, \frac{j}{k}p\right]$, avec $1 \leq j \leq k$. En effet, avec les notations précédentes, si $\bar{s}_1 + \cdots + \bar{s}_k = \bar{s}_{k+1} + \cdots + \bar{s}_{2k}$ dans $\mathbb{Z}_p$, on a dans $\mathbb{Z}$

$$s_1 + \cdots + s_k = s_{k+1} + \cdots + s_{2k} + n \cdot p,$$

avec un $n \in \mathbb{N}$ et $\frac{j-1}{k}p < s_i \leq \frac{j}{k}p$. De la sorte, $(j-1)\cdot p < s_1 + \cdots + s_k \leq j \cdot p$, et de même $(j-1)\cdot p < s_{k+1} + \cdots + s_{2k} \leq j \cdot p$, ce qui oblige $n = 0$ et prouve donc que ψ_3 est bien un k–homomorphisme lorsque restreint à un I_j.

Posons $A_j = \{x \in A \mid (\psi_2(q) \circ \psi_1)(x) \in I_j\}$. Il existe nécessairement $j(q) \in \{1, \ldots, k\}$ tel que $|A_{j(q)}| \geq |A|/k$. Restreinte à $A_{j(q)}$, l'application $\psi := \psi_4 \circ \psi_3 \circ \psi_2(q) \circ \psi_1$ est un k–homomorphisme de Freiman à valeurs dans $\mathbb{Z}_m$.

Il reste à choisir judicieusement q pour que ψ soit injective et que l'application inverse qu'elle induit sur son image soit également un k–homomorphisme de Freiman. En réalité, il suffit de déterminer une valeur de q telle que, lorsque

$$\psi(x_1) + \cdots + \psi(x_k) = \psi(x_{k+1}) + \cdots + \psi(x_{2k}),$$

on ait aussi

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k},$$

car cela prouverait de fait que ψ est injective : si $\psi(x) = \psi(y)$, alors en additionnant k fois puis en utilisant l'implication, on aurait $kx = ky$ dans $\mathbb{Z}$, d'où $x = y$ comme $k \neq 0$.

Choisissons $s = x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{2k} \in kA - kA$, non nul, et cherchons, pour les exclure, des valeurs de q pour lesquelles $\psi(x_1)+\cdots+\psi(x_k)-\psi(x_{k+1})-\cdots-\psi(x_{2k}) = 0$ tout de même. On va chercher $q \in \mathbb{Z}_p^*$ tel que m divise $\psi_3(q\bar{s})$, c'est-à-dire le résidu modulo p de $q\bar{s}$. On aimerait savoir l'ensemble que décrit $q\bar{s}$ quand q décrit $\mathbb{Z}_p^*$, c'est pour cela que nous sommes amenés à supposer que $\bar{s} \neq 0$. Dans ce but, choisissons p vérifiant

$$p > \max_{s \in kA-kA} |s|.$$

Cela garantit que si $s \neq 0$, alors $\bar{s} \neq 0$. Ainsi $q \mapsto q\bar{s}$ est bijective, puisque $\mathbb{Z}_p$ est un corps. Donc $q\bar{s}$ décrit $\{1, \cdots, p-1\}$, chaque valeur n'étant prise qu'une fois, et parmi ces valeurs, au plus $(p-1)/m$ sont divisibles par m, *i.e.* valent 0 modulo m, ce qui correspond à au plus $(p-1)/m$ valeurs de q.

On a montré ainsi que pour chaque $s \in kA - kA \backslash \{0\}$, il existe au plus $(p-1)/m$ valeurs de q telles que m divise $\psi_3(q\bar{s})$. D'après les inégalités de Plünnecke, $|kA - kA| \leq C^{2k}|A|$, donc le nombre de valeurs de q à exclure, c'est-à-dire telles qu'il existe $s \in kA - kA \backslash \{0\}$ avec $m \mid \psi_3(q\bar{s})$, et *a fortiori* le nombre de valeurs de q telles que ψ ne vérifie pas la condition ci-dessus, n'excède pas

$$|kA - kA\backslash\{0\}| \cdot \frac{p-1}{m} \leq C^{2k}|A|\frac{p-1}{m} < p - 1,$$

car on a choisi $m > C^{2k}|A|$. En définitive, puisque $|\mathbb{Z}_p^*| = p-1$, cela prouve qu'il existe au moins un $q \in \mathbb{Z}_p^*$ tel que, pour tout $s \in kA - kA$ vérifiant $m \mid \psi_3(q\bar{s})$, on a $s = 0$. Pour cette valeur de q, posons $A' := A_{j(q)}$. Grâce aux remarques précédents, ψ restreint à A' est un k–isomorphisme de Freiman sur son image, et $|A'| \geq |A|/k$, ce qui conclut la preuve. □

Remarque. Pour justifier à grands traits les manipulations de cette preuve, remarquons que la réduction modulo m n'a en général aucune raison d'être un isomorphisme de Freiman, car il se peut même qu'elle ne soit pas injective. On a donc commencé par « contrôler » la taille de l'ensemble A en le réduisant modulo p, où p est très grand, puis on redispose les éléments de A en les multipliant par un q bien choisi. Dans ces conditions (quitte à se restreindre à un grand sous-ensemble de A), la réduction modulo m est bien un k–isomorphisme.

L'intérêt majeur du théorème est de permettre de choisir m le plus petit possible, de façon qu'on puisse réduire au maximum la taille du groupe ambiant, et étudier des ensembles de « grande densité » (ce sera très utile pour le lemme 3.13 par exemple).

3 Analyse de Fourier dans le groupe $\mathbb{Z}_N$

Le but de cette partie est de présenter toutes sortes d'outils d'analyse qui, maintenant que nous nous sommes ramenés à un problème dans un $\mathbb{Z}_N$, nous permettront de progresser.

3.1 Transformée de Fourier

Ici, N désigne un entier premier impair. On pose $\omega = e^{2\pi i/N}$. C'est une racine N-ième de l'unité.

Définition. Soit $f : \mathbb{Z}_N \to \mathbb{C}$ une application. La norme 2 de f est le nombre $\|f\|_2 = \sqrt{\sum_{x\in\mathbb{Z}_N} |f(x)|^2}$.

On définit la *transformée de Fourier* de f par

$$\hat{f}(\xi) = \sum_{x\in\mathbb{Z}_N} f(x)\omega^{\xi x}$$

pour tout $\xi \in \mathbb{Z}_N$. Remarquons que la notation $\omega^{\xi x}$ a bien un sens, car la valeur de $\omega^{\xi x}$ ne dépend pas du choix du représentant de ξ dans $\mathbb{Z}$.

Soit $g : \mathbb{Z}_N \to \mathbb{C}$ une autre application. On définit le *produit de convolution* de f et de g par

$$f * g(x) = \sum_{y\in\mathbb{Z}_N} f(x-y)g(y).$$

Recensons quelques propriétés classiques et utiles, qu'un calcul direct permet d'obtenir.

Proposition 3.1. *Soient $f, g : \mathbb{Z}_N \to \mathbb{C}$.*

1. *(Formule d'inversion de Fourier). $\forall x \in \mathbb{Z}_N$, $f(x) = \frac{1}{N}\sum_\xi \hat{f}(\xi)\omega^{-\xi x}$.*
2. *(Formule de Parseval). $\sum_\xi \hat{f}(\xi)\overline{\hat{g}(\xi)} = N\sum_x f(x)\overline{g(x)}$. En particulier, $\sum_\xi |\hat{f}(\xi)|^2 = N\sum_x |f(x)|^2 = N\|f\|_2^2$.*
3. *$\forall \xi \in \mathbb{Z}_N$, $\hat{\hat{f}}(\xi) = \overline{\hat{f}(-\xi)}$.*
4. *Le produit de convolution est associatif, et respecte la conjugaison complexe : $\overline{f * g} = \bar{f} * \bar{g}$.*
5. *$\widehat{f * g} = \hat{f} \cdot \hat{g}$.*

Dans la suite, on identifie un sous-ensemble A de $\mathbb{Z}_N$ avec sa fonction indicatrice : $A = \mathbf{1}_A$. La proposition suivante montre que les notions introduites sont tout à fait adaptées à l'étude des propriétés additives de A.

Proposition 3.2. *Soient $A, B, \cdots \subseteq \mathbb{Z}_N$. Soit $x \in \mathbb{Z}_N$. On peut exprimer à l'aide des transformées de Fourier*

1. *le cardinal d'un ensemble :*

$$N|A| = \sum_\xi |\hat{A}(\xi)|^2.$$

2. le nombre de représentations de x dans une somme :

$$\frac{1}{N}\sum_{\xi}\hat{A_1}(\xi)\cdots\hat{A_n}(\xi)\omega^{-\xi x} = A_1 * \cdots * A_n(x) = r_{A_1+\cdots+A_n}(x).$$

3. l'énergie de deux ensembles :

$$\mathsf{E}(A,B) = \sum_x (A*B(x))^2 = \|A*B\|_2^2 = \frac{1}{N}\sum_{\xi}|\hat{A}(\xi)|^2|\hat{B}(\xi)|^2.$$

Démonstration. Le premier résultat est une application littérale de la formule de Parseval à la fonction A.

Dans le deuxième point, la première égalité est une conséquence de la formule d'inversion :

$$\begin{aligned} A_1 * \cdots * A_n(x) &= \frac{1}{N}\sum_{\xi} \widehat{A_1 * \cdots * A_n}(\xi)\omega^{-\xi x} \\ &= \frac{1}{N}\sum_{\xi}\hat{A_1}(\xi)\cdots\hat{A_n}(\xi)\omega^{-\xi x}. \end{aligned}$$

Pour la deuxième égalité, écrivons que

$$\begin{aligned} A_1 * \cdots * A_n(x) &= \sum_{y_1+\cdots+y_n=x} A_1(y_1)\cdots A_n(y_n) \\ &= |\{(y_1,\cdots,y_n)\in A_1\times\cdots\times A_n \mid y_1+\cdots+y_n = x\}| \\ &= r_{A_1+\cdots+A_n}(x). \end{aligned}$$

Enfin, le lemme 0.3 nous dit que $\mathsf{E}(A,B) = \sum_x r_{A+B}(x)^2$. D'après le point que l'on vient de montrer, $r_{A+B}(x)^2 = (A*B(x))^2$. De la sorte, $\mathsf{E}(A,B) = \sum_x (A*B(x))^2 = \|A*B\|_2^2$. La formule de Parseval et (3.1.5) permettent de voir que $\sum_x (A*B(x))^2 = \frac{1}{N}\sum_\xi |\widehat{A*B}(\xi)|^2 = \frac{1}{N}\sum_\xi |\hat{A}(\xi)|^2|\hat{B}(\xi)|^2$. □

3.2 Ensembles de Bohr

À présent, nous portons notre attention sur des sous-ensembles très particuliers de $\mathbb{Z}_N$, dont on verra plus loin que ce sont eux qui nous fourniront les progressions arithmétiques que nous cherchons.

Définition. Soient $S \subseteq \mathbb{Z}_N$ et $\delta \in \mathbb{R}_+^*$. On appelle *ensemble de Bohr* (ou *voisinage de Bohr*) de base S, et on note $B(S,\delta)$, l'ensemble

$$\left\{x\in\mathbb{Z}_N \mid \forall \xi\in S, \left\|\frac{\xi x}{N}\right\| \leq \delta\right\}$$

où $\|t\|$ est la distance de t à l'ensemble $\mathbb{Z}$.

Ici encore, la notion est bien définie, car la valeur de $\|\frac{\xi x}{N}\|$ est toujours la même, quels que soient les choix des représentants de ξ et x dans $\mathbb{Z}$.

Définition. Soit $\rho \in]0,1]$. Soit $f : \mathbb{Z}_N \to \mathbb{C}$. On appelle *$\rho$-spectre* de f l'ensemble suivant

$$\mathrm{Spec}(f,\rho) = \left\{ \xi \in \mathbb{Z}_N \mid |\hat{f}(\xi)| \geq \rho \|f\|_1 \right\}.$$

En particulier, le ρ-spectre $\mathrm{Spec}(A,\rho)$ d'un ensemble $A \subseteq \mathbb{Z}_N$ est l'ensemble des ξ tel que $|\hat{A}(\xi)| \geq \rho|A|$.

La proposition suivante montre que si $\mathsf{E}(X,Y)$ est de l'ordre de $|X|^2|Y|$, alors $X+Y-X-Y$ contient un ensemble de Bohr de base un spectre de X.

Proposition 3.3. *Soient $X, Y \subseteq \mathbb{Z}_N$. Supposons qu'il existe $\alpha \in]0,1]$ tel que $\mathsf{E}(X,Y) \geq \alpha|X|^2|Y|$. Alors $B(S,\frac{1}{6}) \subseteq X+Y-X-Y$, où $S = \mathrm{Spec}(X, \frac{1}{2}\alpha^{1/2})$.*

Remarque. Plus α est petit, plus le spectre S est de grande taille, mais alors plus l'ensemble de Bohr $B(S,\frac{1}{6})$ est petit (car la condition sur $x \in B(S,\frac{1}{6})$ est d'autant plus restrictive que S est grand). Dans l'idée d'exploiter au mieux la proposition, il semble plus judicieux de choisir un α qui soit maximal pour la propriété $\mathsf{E}(X,Y) \geq \alpha|X|^2|Y|$, de façon à obtenir un grand ensemble de Bohr inclus dans $X+Y-X-Y$.

Démonstration de la proposition 3.3. Soient X, Y, α comme dans l'énoncé. Grâce à la proposition précédente, on peut reformuler l'hypothèse :

$$\frac{1}{N}\sum_{\xi} |\widehat{X}(\xi)|^2 |\widehat{Y}(\xi)|^2 = \mathsf{E}(X,Y) \geq \alpha|X|^2|Y|.$$

Le choix de $\frac{1}{2}\alpha^{1/2}$ peut paraître obscur. Posons donc dans un premier temps $S = \mathrm{Spec}(X,\rho)$, avec $\rho \in]0,1]$ un réel que l'on déterminera dans la suite.

Soit $x \in B(S,\frac{1}{6})$. Toujours d'après la proposition précédente, $x \in X+Y-X-Y$ si et seulement si

$$r_{X+Y-X-Y}(x) = \frac{1}{N}\sum_{\xi} \widehat{X}(\xi)\widehat{Y}(\xi)\widehat{-X}(\xi)\widehat{-Y}(\xi)\omega^{-\xi x} > 0.$$

Mais on a $\widehat{-X}(\xi) = \widehat{X}(-\xi) = \overline{\widehat{X}(\xi)}$ (car $(-X)(x) = X(-x)$), et de même pour Y, donc

$$r_{X+Y-X-Y}(x) = \frac{1}{N}\sum_{\xi} |\widehat{X}(\xi)|^2 |\widehat{Y}(\xi)|^2 \omega^{-\xi x}.$$

Comme $r_{X+Y-X-Y}(x)$ est réel, il s'agit en fait d'une égalité entre parties réelles :

$$r_{X+Y-X-Y}(x) = \frac{1}{N}\sum_{\xi} |\widehat{X}(\xi)|^2 |\widehat{Y}(\xi)|^2 \cos\frac{2\pi\xi x}{N}.$$

Pour tout $\xi \in S$, par définition de $B(S,\frac{1}{6})$, on a $\|\frac{\xi x}{N}\| \leq \frac{1}{6}$, et donc $\frac{2\pi\xi x}{N} \in [-\frac{\pi}{3}, \frac{\pi}{3}]$, d'où $\cos\frac{2\pi\xi x}{N} \geq \frac{1}{2}$. Cela suggère de séparer la somme en deux pour

minorer ainsi les cosinus.

$$\begin{aligned} r_{X+Y-X-Y}(x) &= \frac{1}{N}\sum_{\xi\in S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2\cos\frac{2\pi\xi x}{N} + \frac{1}{N}\sum_{\xi\notin S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2\cos\frac{2\pi\xi x}{N} \\ &\geq \frac{1}{2N}\sum_{\xi\in S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2 - \frac{1}{N}\sum_{\xi\notin S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2 \\ &= \frac{1}{2N}\sum_{\xi\in\mathbb{Z}_N}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2 - \frac{3}{2N}\sum_{\xi\notin S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2 \\ &= \frac{1}{2}\,\mathsf{E}(X,Y) - \frac{3}{2N}\sum_{\xi\notin S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2. \end{aligned}$$

On peut encore majorer le dernier terme, en utilisant d'une part la définition de $\mathrm{Spec}(X,\rho)$, et de l'autre l'expression du cardinal de Y à partir de sa transformée de Fourier :

$$\frac{1}{N}\sum_{\xi\notin S}|\widehat{X}(\xi)|^2|\widehat{Y}(\xi)|^2 \leq \sup_{\xi\notin S}|\widehat{X}(\xi)|^2\cdot\frac{1}{N}\sum_{\xi}|\widehat{Y}(\xi)|^2 \leq (\rho|X|)^2|Y|.$$

On en déduit que

$$r_{X+Y-X-Y}(x) \geq \frac{1}{2}\,\mathsf{E}(X,Y) - \frac{3}{2}\rho^2|X|^2|Y| \geq \frac{|X|^2|Y|}{2}(\alpha - 3\rho^2).$$

On voit qu'il suffit de prendre $\rho = \frac{1}{2}\alpha^{1/2}$ pour avoir $r_{X+Y-X-Y}(x) > 0$, et donc $x \in X+Y-X-Y$. Par conséquent, avec ce choix, $B(S,\frac{1}{6}) \subseteq X+Y-X-Y$. □

Établissons un corollaire de cette proposition, dans le cas particulier des hypothèses du théorème de Freiman.

Corollaire 3.4. *Soit $A \subseteq \mathbb{Z}_N$ tel que $|A+A| \leq C|A|$. Posons $S = \mathrm{Spec}(A, \frac{1}{2\sqrt{C}})$. Alors $B(S,\frac{1}{6}) \subseteq 2A - 2A$.*

Démonstration. Par le lemme (0.4), on a

$$\mathsf{E}(A,A) \geq \frac{|A|^2|A|^2}{|A+A|} \geq \frac{1}{C}|A|^2|A|.$$

On applique ensuite la proposition précédente à $X = Y = A$ et $\alpha = C^{-1}$. □

3.3 Maximisation de l'énergie : le lemme central

Pour aller dans le sens de notre remarque sur le choix de α dans la proposition 3.3, observons que dans le corollaire précédent, le paramètre du spectre est fixé (à $\frac{1}{2}C^{-1/2}$). Nous allons à présent assouplir cette constante (pour la faire s'approcher de 1), en considérant des sous-ensembles de A.

Lemme 3.5 (Schoen [13])**.** *Soit $A \subseteq G$ un groupe abélien. Supposons que $|A+A| \leq C|A|$, avec C une constante réelle. Pour tout $\varepsilon > 0$, il existe deux ensembles $X \subseteq A$ et $Y \subseteq A+A$ tels que*

- $|X| \geq (2C^2)^{-2^{1/\varepsilon}}|A|$ *et* $|Y| \geq |A|$,

- *l'énergie* $\mathsf{E}(X,Y) \geq C^{-2\varepsilon}|X|^2|Y|$.

Remarque. La borne sur l'énergie est bien celle qu'exige la proposition 3.3. Qui plus est, on peut ici choisir α arbitrairement proche de 1 (la seule restriction étant que les ensembles X et Y dépendent du choix de ε).

Démonstration. La preuve est tout à la fois technique et très élémentaire. Commençons par introduire une notation : pour un ensemble $B \subseteq A$, on note

$$\tau(B) = \left\{ t \in B - B \;\middle|\; r_{B-B}(t) \geq \frac{|B|^2}{2|B-B|} \right\}.$$

Il est important de remarquer que, si B est non-vide, $\tau(B)$ n'est jamais vide. Supposons le contraire. Par un calcul déjà effectué dans la preuve du lemme 0.4,

$$|B|^2 = \sum_{t \in B-B} r_{B-B}(t) < \sum_{t \in B-B} \frac{|B|^2}{2|B-B|} < \frac{|B|^2}{2}.$$

C'est absurde.

Nous procédons en plusieurs étapes. Fixons $\varepsilon > 0$.

Étape 1. Montrons qu'il existe un ensemble $B \subseteq A$ dont le cardinal $|B| \geq (2C^2)^{-2^{1/\varepsilon}+1}|A|$ et qui vérifie

$$\text{pour tout } t \in \tau(B), \quad |A + B_t| \geq C^{-\varepsilon}|A+B|, \tag{1}$$

où l'on a noté $B_t = B \cap (t+B)$. Pour prouver cela, nous proposons un algorithme. Posons $A^0 = A$. Nous définissons récursivement des ensembles $A^l \subseteq A$, $l \geq 0$, tels que $|A^l| \geq (2C^2)^{-2^l+1}|A|$. Supposons donc défini A^l.

- S'il existe $t_0 \in \tau(A^l)$ tel que $|A + A^l_{t_0}| < C^{-\varepsilon}|A + A^l|$, on pose $A^{l+1} := A^l_{t_0} \subseteq A$. Vérifions la condition sur le cardinal de A^{l+1}. Si $x - a$ est une représentation de t_0 dans $A^l - A^l$, alors $x \in A^l$ et $x = a + t_0 \in t_0 + A^l$, et donc $x \in A^l_{t_0}$. De la sorte, à chaque représentation de t_0, on peut associer un x (différent) dans $A^l_{t_0}$, et en utilisant l'inégalité de Plünnecke,

$$\begin{aligned} |A^{l+1}| = |A^l_{t_0}| &\geq r_{A^l - A^l}(t_0) \\ &\geq \frac{|A^l|^2}{2|A^l - A^l|} \\ &\geq \frac{|A^l|^2}{2|A-A|} \\ &\geq \frac{(2C^2)^{-2^{l+1}+2}|A|^2}{2C^2|A|} = (2C^2)^{-2^{l+1}+1}|A|. \end{aligned}$$

- Si un tel t_0 n'existe pas, alors (1) est vérifié pour $B := A^l$.

Il reste à s'assurer que l'algorithme se termine à temps pour que l'inégalité sur le cardinal de B soit vraie. En effet, après m étapes, un raisonnement par récurrence montre que l'ensemble A^m vérifie

$$|A + A^m| < C^{-\varepsilon}|A + A^{m-1}| < \cdots < C^{-m\varepsilon}|A + A^0| \leq C^{1-m\varepsilon}|A|,$$

alors que d'autre part $|A + A^m| \geq |A|$ (car l'application $g \mapsto g + x$ est une bijection de G). Cela prouve que $C^{1-m\varepsilon} > 1$, et comme $C \geq 1$, que $1 - m\varepsilon > 0$,

ou encore que $m < 1/\varepsilon$. Ainsi, m ne peut excéder $\lceil 1/\varepsilon \rceil - 1$. Donc l'algorithme se termine; de plus, $B = A^l$ pour un $l < 1/\varepsilon$, d'où $|B| \geq (2C^2)^{-2^l+1}|A| \geq (2C^2)^{-2^{1/\varepsilon}+1}|A|$.

Étape 2. On choisit un B tel que décrit dans l'étape 1, et on construit l'ensemble X. Calculons d'abord le nombre de couples (b, b') tels que $b - b' \in \tau(B)$. Ce nombre vaut

$$\begin{aligned}
\sum_{\substack{t \in B-B \\ t \in \tau(B)}} r_{B-B}(t) &= \sum_{t \in B-B} r_{B-B}(t) - \sum_{\substack{t \in B-B \\ t \notin \tau(B)}} r_{B-B}(t) \\
&= |B|^2 - \sum_{\substack{t \in B-B \\ t \notin \tau(B)}} r_{B-B}(t) \\
&\geq |B|^2 - \sum_{\substack{t \in B-B \\ t \notin \tau(B)}} \frac{|B|^2}{2|B-B|} \\
&\geq |B|^2 - |B-B|\frac{|B|^2}{2|B-B|} = \frac{|B|^2}{2}.
\end{aligned}$$

Cette minoration prouve qu'il existe $b_0 \in B$ tel que $|(B - b_0) \cap \tau(B)| \geq |B|/2$, car sinon, pour chaque $b' \in B$, il existe strictement moins de $|B|/2$ éléments de B tels que $b - b' \in \tau(B)$, donc strictement moins de $|B|^2/2$ couples (b, b') tels que $b - b' \in \tau(B)$, ce qui est contraire à la minoration que l'on vient d'établir.

Posons alors $X := B \cap (\tau(B) + b_0)$. La condition $X \subseteq A$ est bien remplie, puisque $B \subseteq A$. De plus $|X| = |B \cap (\tau(B) + b_0)| = |(B - b_0) \cap \tau(B)|$, les deux derniers ensembles étant en bijection par $x \mapsto x - b_0$. Donc

$$|X| \geq \frac{|B|}{2} \geq \frac{1}{2}(2C^2)^{-2^{1/\varepsilon}+1}|A| \geq (2C^2)^{-2^{1/\varepsilon}}|A|.$$

Ainsi, X répond aux critères de la proposition [†].

Étape 3 (Calcul de l'énergie). Commençons par une remarque : pour tout $t \in \tau(B)$, $A + B_t \subseteq A + B$ et $A + B_t \subseteq A + B + t$, donc $A + B_t$ est inclus dans l'intersection de ces deux ensembles, et on peut minorer

$$|(A + B) \cap (A + B + t)| \geq |A + B_t| \geq C^{-\varepsilon}|A + B|$$

grâce à la propriété de l'ensemble B.

Posons $Y := A + B$ (il s'agit bien d'un sous-ensemble de $A + A$ de cardinal $\geq |A|$), et calculons, à partir du lemme 0.3, et à l'aide de l'inégalité de Cauchy-Schwarz :

$$\begin{aligned}
\mathsf{E}(X, Y) = \sum_{z \in G} r_{X+Y}(z)^2 &= \sum_{z \in G} |\{t \in X \mid z \in Y + t\}|^2 \\
&\geq \sum_{z \in A+B+b_0} |\{t \in X \mid z \in Y + t\}|^2 \\
&\geq |A + B + b_0|^{-1} \left(\sum_{z \in A+B+b_0} |\{t \in X \mid z \in Y + t\}| \right)^2.
\end{aligned}$$

†. On peut voir par le même raisonnement que celui qui précède (sur le nombre de couples (b, b')) que $|\tau(B)| \geq |B|/2$, et aurait donc pu convenir, si ce n'est que $\tau(B)$ est un sous-ensemble de $A - A$ et non de A. Tout le but de l'étape 2 a donc été de trouver un ensemble ressemblant, dans A.

Or on peut écrire autrement la somme entres parenthèses :

$$\begin{aligned}\sum_{z\in A+B+b_0} |\{t\in X \mid z\in Y+t\}| &= \sum_{z\in A+B+b_0}\left(\sum_{t\in X}\mathbf{1}_{Y+t}(z)\right)\\ &= \sum_{t\in X}\sum_{z\in A+B+b_0}\mathbf{1}_{A+B+t}(z)\\ &= \sum_{t\in X}|(A+B+t)\cap(A+B+b_0)|.\end{aligned}$$

Utilisons la définition de X : pour tout $t\in X$, il existe $t'\in\tau(B)$ tel que $t=t'+b_0$, et alors $|(A+B+t)\cap(A+B+b_0)| = |(A+B+t')\cap(A+B)| \geq C^{-\varepsilon}|A+B|$. En conclusion,

$$\begin{aligned}\mathsf{E}(X,Y) &\geq |A+B+b_0|^{-1}\left(\sum_{t\in X}|(A+B+t)\cap(A+B+b_0)|\right)^2\\ &\geq |A+B|^{-1}\left(|X|C^{-\varepsilon}|A+B|\right)^2 = C^{-2\varepsilon}|X|^2|Y|.\end{aligned}$$

□

Muni de cet élément, reformulons la proposition 3.3 :

Corollaire 3.6. *Soient $\varepsilon>0$ et $K>1$. Soient X,Y deux sous-ensembles finis de $\mathbb{Z}_N$. Supposons que $\mathsf{E}(X,Y)\geq C^{-2\varepsilon}|X|^2|Y|$, alors $B(S,\frac{1}{6})\subseteq X+Y-X-Y$, avec $S=\mathrm{Spec}(X,\frac{1}{2}C^{-\varepsilon})$.*

3.4 Théorème spectral de Chang

Nous allons améliorer l'ensemble de Bohr trouvé dans le corollaire 3.6, grâce à un nouveau résultat : le théorème spectral de Chang. Il explicite la structure du spectre d'un ensemble, et dit plus précisément que l'ensemble des points où $\widehat{X}$ est grand est très structuré, à savoir inclus dans un petit *cube*.

Définition. Soit $Z=\{z_1,\dots,z_k\}$ un sous-ensemble d'un groupe abélien G. On définit le *cube* engendré par Z, et on note $\mathrm{Span}(Z)$, l'ensemble des éléments de la forme $\sum_{i=1}^k \epsilon_i z_i$, où $\epsilon_i\in\{-1,0,1\}$.

Le résultat de Chang est le suivant :

Théorème 3.7 (Chang [1])**.** *Soient $\rho\in]0,1]$. Soit $X\subseteq\mathbb{Z}_N$. Alors il existe $\Gamma\subseteq\mathrm{Spec}(X,\rho)$ tel que $\mathrm{Spec}(X,\rho)\subseteq\mathrm{Span}(\Gamma)$.*
De plus, $|\Gamma| = \mathcal{O}(\frac{1}{\rho^2}\log\frac{N}{|X|})$.

L'idée est de montrer que le spectre $\mathrm{Spec}(X,\rho)$ ne contient pas de grand sous-ensemble peu structuré. La notion de *dissociativité* traduit le fait que certains éléments sont très peu corrélés, et donc est bien adaptée pour mettre en évidence un manque de structure dans un ensemble.

Définition. On dit qu'un ensemble $\Gamma\subseteq\mathbb{Z}_N$ ensemble est *dissocié* si toute application $\epsilon:\Gamma\to\{-1,0,1\}$ telle que $\sum_{\xi\in\Gamma}\epsilon(\xi)\xi=0$ est identiquement nulle.

3.4.1 Une inégalité de Rudin

Le but de ce paragraphe est de démontrer l'inégalité de Rudin qui servira à la preuve du théorème spectral de Chang.

Soit $\Gamma \subseteq \mathbb{Z}_N$. On considère l'opérateur T qui à $c \in \mathbb{C}^\Gamma$, une suite de nombres complexes indexée par Γ, associe l'application $x \mapsto \sum_{\xi\in\Gamma} c(\xi)\omega^{-\xi x}$. Soit $p > 1$. On munit l'ensemble $\mathbb{C}^\Gamma$ la norme l^2 et l'ensemble $\mathbb{C}^{\mathbb{Z}_N}$ la norme L^p pour $\mu_{\mathbb{Z}_N}$, la mesure de probabilité uniforme sur $\mathbb{Z}_N$:

$$\|c\|_2 = \sqrt{\sum_{\xi\in\Gamma} |c(\xi)|^2},$$
$$\|f\|_{L^p} = \sqrt[p]{\frac{1}{N}\sum_{x\in\mathbb{Z}_N} |f(x)|^p}.$$

T est donc une application linéaire de l'espace $l^2_{\mathbb{C}}(\Gamma)$ à l'espace $L^p_{\mathbb{C}}(\mathbb{Z}_N, \mu_{\mathbb{Z}_N})$. L'inégalité de Rudin permet de contrôler la norme subordonnée $\|T\|_{2\to p}$ de cet opérateur T pour les ensembles Γ dissociés.

Proposition 3.8 (Rudin)**.** *Si $\Gamma \subseteq \mathbb{Z}_N$ est dissocié, alors pour tout $p \geq 1$, $\|T\|_{2\to p} \leq K\sqrt{p}$, avec K une constante absolue.*

Démonstration. Le formalisme probabiliste rend agréable la preuve qui suit. Commençons par traduire les hypothèses en langage probabiliste. $\mathbb{Z}_N$ est un espace de probabilité muni de la tribu discrète et de la mesure de probabilité uniforme sur $\mathbb{Z}_N$. Les applications de $\mathbb{Z}_N$ dans $\mathbb{C}$ sont donc des variables aléatoires complexes. Posons $X_\xi : x \mapsto c(\xi)\omega^{-\xi x}$ des variables aléatoires. Notons $S = \sum_{\xi\in\Gamma} X_\xi$. Prouver l'inégalité de Rudin revient à majorer la norme p de S par $\|c\|_2$. On constate que chaque X_ξ est borné par $|c(\xi)|$.

L'hypothèse de dissociativité traduit une certaine indépendance des X_ξ. En fait, on a

$$\mathbb{E}\left[X_{\xi_1}\cdots X_{\xi_k}\overline{X_{\xi'_1}}\cdots\overline{X_{\xi'_l}}\right] = 0 \tag{2}$$

pour tous $k + l \geq 1$ et $\xi_1, \ldots, \xi_k, \xi'_1, \ldots, \xi'_l \in \Gamma$ deux à deux distincts. En effet,

$$\mathbb{E}\left[X_{\xi_1}\cdots X_{\xi_k}\overline{X_{\xi'_1}}\cdots\overline{X_{\xi'_l}}\right] = \frac{z}{N}\sum_{x\in\mathbb{Z}_N} \omega^{(-\xi_1-\cdots-\xi_k+\xi'_1+\cdots+\xi'_l)x},$$

avec un $z \in \mathbb{C}$, et comme $-\xi_1 - \cdots - \xi_k + \xi'_1 + \cdots + \xi'_l \neq 0$ par dissociativité, la somme (géométrique) est nulle.

On voit alors que les parties réelles et imaginaire de X_ξ, $\xi \in \Gamma$ vérifient

$$\mathbb{E}\left[\Re X_{\xi_1}\cdots\Re X_{\xi_k}\right] = \mathbb{E}\left[\Im X_{\xi_1}\cdots\Im X_{\xi_k}\right] = 0$$

pour tous $k \geq 1$ et $\xi_1, \ldots, \xi_k \in \Gamma$ deux à deux distincts. En effet si l'on développe le produit en polynôme de X_ξ et $\overline{X_\xi}, \xi \in \Gamma$, chaque monôme est de la forme du membre gauche de (2) donc nulle.

Démontrons ensuite quelques lemmes en utilisant la méthode du moment exponentiel.

Lemme 3.9. *Soient $X_1, \ldots, X_n$ des variables aléatoires réelles bornées respectivement par $c_i > 0$ et vérifiant*

$$\mathbb{E}\left[X_{i_1}\cdots X_{i_k}\right] = 0 \text{ pour tout } i_1 < i_2 < \cdots < i_k. \tag{3}$$

Alors $\forall t \geq 0$,

$$\mathbb{E}\left[e^{t(X_1+\cdots+X_n)}\right] \leq e^{\frac{t^2\|c\|_2^2}{2}}.$$

Démonstration. Établissons d'abord deux inégalités élémentaires

$$\forall t \geq 0,\ \forall y \in [-1,1], \quad e^{ty} \leq \cosh t + y \sinh t, \tag{4}$$

$$\forall t \geq 0, \quad \cosh t \leq e^{\frac{t^2}{2}}. \tag{5}$$

La première provient de la convexité de $y \mapsto e^{ty}$, et la deuxième, de la comparaison des développements en série entière de chacune des fonctions. Appliquons (4) à $c_i t$ et $y = \frac{X_i}{c_i}$ et faisons le produit. On obtient

$$e^{t(X_1+\cdots+X_n)} \leq \prod_{i=1}^{n} \left(\cosh(c_i t) + \frac{X_i}{c_i}\sinh(c_i t)\right).$$

On développe le membre de droite, on obtient un premier terme $\prod_{i=1}^n \cosh(c_i t)$, puis suit une combinaison linéaire de $X_{i_1}\cdots X_{i_k}$, $k \geq 1$ et $i_1 < i_2 < \cdots < i_k$. Prenons l'espérance ; l'hypothèse (3) permet d'annuler tous les termes, sauf le premier :

$$\mathbb{E}\left[e^{t(X_1+\cdots+X_n)}\right] \leq \mathbb{E}\left[\prod_{i=1}^{n} \cosh(c_i t)\right].$$

On conclut grâce à la remarque (5). □

Le résultat suivant est une inégalité « à la Chernoff » :

Lemme 3.10. *Sous les mêmes hypothèses que le lemme précédent, on a*

$$\forall a \geq 0, \quad \mathbb{P}\left[|X_1 + \cdots + X_n| \geq a\right] \leq 2e^{-\frac{a^2}{2\|c\|_2^2}}.$$

Démonstration. Pour tout $a \leq 0$,

$$\begin{aligned}
\mathbb{P}\left[X_1 + \cdots + X_n \geq a\right] =& \mathbb{P}\left[e^{t(X_1+\cdots+X_n)} \geq e^{ta}\right] && \text{pour tout } t \geq 0\\
\leq& e^{-ta}\mathbb{E}\left[e^{t(X_1+\cdots+X_n)}\right] && \text{par l'inégalité de Markov}\\
\leq& e^{-ta+\frac{t^2\|c\|_2^2}{2}}. && \text{par le lemme précédent}
\end{aligned}$$

On prend $t = \frac{a}{\|c\|_2^2}$ pour optimiser :

$$\mathbb{P}\left[X_1 + \cdots + X_n \geq a\right] \leq e^{-\frac{a^2}{2\|c\|_2^2}}.$$

De même, comme les variables aléatoires $-X_1, \ldots, -X_n$ vérifient les hypothèses du lemme, on a

$$\mathbb{P}\left[X_1 + \cdots + X_n \leq -a\right] \leq e^{-\frac{a^2}{2\|c\|_2^2}},$$

d'où la majoration finale. □

Tout cela reste vrai dans le cas complexe :

Lemme 3.11. *Si $X_1, \dots, X_n$ sont des variables aléatoires complexes bornées respectivement par c_i et dont les parties réelles et imaginaires vérifient* (3)*, alors*

$$\mathbb{P}\left[|X_1 + \cdots + X_n| \geq a\right] \leq 4e^{-\frac{a^2}{4\|c\|_2^2}}.$$

Démonstration. Le lemme précédent appliqué à la suite $\Re X_1, \dots, \Re X_n$ et la suite $\Im X_1, \dots, \Im X_n$ donne pour tout $a \leq 0$,

$$\mathbb{P}\left[|\Re(X_1 + \cdots + X_n)| \geq a\right] \leq 2e^{-\frac{a^2}{2\|c\|_2^2}},$$
$$\mathbb{P}\left[|\Im(X_1 + \cdots + X_n)| \geq a\right] \leq 2e^{-\frac{a^2}{2\|c\|_2^2}}.$$

On remarque ensuite que pour un nombre complexe z, si $|z| \leq a$, alors ou bien $\Re z \geq \frac{a}{\sqrt{2}}$, ou bien $\Im z \geq \frac{a}{\sqrt{2}}$. Donc,

$$\begin{aligned}
&\mathbb{P}\left[|(X_1 + \cdots + X_n)| \geq a\right] \\
&\leq \mathbb{P}\left[|\Re(X_1 + \cdots + X_n)| \geq \frac{a}{\sqrt{2}}\right] + \mathbb{P}\left[|\Im(X_1 + \cdots + X_n)| \geq \frac{a}{\sqrt{2}}\right] \\
&\leq 2 \cdot 2e^{-\frac{a^2}{2\cdot 2\|c\|_2^2}}.
\end{aligned}$$

□

La connaissance de la queue de la distribution permet de majorer le moment d'ordre p :

Lemme 3.12. *Sous les mêmes hypothèses que le lemme précédent, on a*

$$\mathbb{E}\left[|X_1 + \cdots + X_n|^p\right]^{\frac{1}{p}} = \mathcal{O}(\sqrt{p}\|c\|_2).$$

Démonstration. On utilise la formule de Fubini-Tonelli :

$$\begin{aligned}
\mathbb{E}\left[|X_1 + \cdots + X_n|^p\right] &= \mathbb{E}\left[\int_0^\infty \mathbf{1}_{t \leq |X_1 + \cdots + X_n|^p}\, dt\right] \\
&= \int_0^\infty \mathbb{E}\left[\mathbf{1}_{t \leq |X_1 + \cdots + X_n|^p}\right] dt \\
&= \int_0^\infty \mathbb{P}\left[|X_1 + \cdots + X_n| \geq t^{\frac{1}{p}}\right] dt.
\end{aligned}$$

Donc par le lemme précédent,

$$\mathbb{E}\left[|X_1 + \cdots + X_n|^p\right] \leq 4\int_0^\infty e^{-\frac{t^{\frac{2}{p}}}{4\|c\|_2^2}} dt.$$

On fait le changement de variable : $u = \frac{t^{\frac{2}{p}}}{4\|c\|_2^2}$.

$$\begin{aligned}
\mathbb{E}\left[|X_1 + \cdots + X_n|^p\right] &\leq 4 \cdot (2\|c\|_2)^p \frac{p}{2} \int_0^\infty e^{-u} u^{\frac{p}{2}-1} du \\
&= 4 \cdot (2\|c\|_2)^p \frac{p}{2} \cdot \Gamma\left(\frac{p}{2}\right) \\
&= 4 \cdot (2\|c\|_2)^p \cdot \Gamma\left(\frac{p}{2} + 1\right),
\end{aligned}$$

d'où

$$\mathbb{E}\left[|X_1+\cdots+X_n|^p\right]^{\frac{1}{p}} \leq 2\|c\|_2\left(4\Gamma\left(\frac{p}{2}+1\right)\right)^{\frac{1}{p}} = \mathcal{O}(\sqrt{p}\|c\|_2)$$

par la formule de Stirling. □

On a vu que les variables aléatoires $x \mapsto c(\xi)\omega^{-\xi x}$ vérifient l'hypothèse de ce lemme. Donc cela termine la preuve de l'inégalité de Rudin. □

3.4.2 Preuve du théorème spectral de Chang

Attachons-nous maintenant à démontrer le théorème spectral de Chang. Il s'avère que c'est l'adjoint de T qui va nous être utile. On note p' l'exposant conjugué de p. On rappelle que l'adjoint de T est l'unique application T^* tel que pour tout $c \in \mathbb{C}^\Gamma$ et pour tout $f \in \mathbb{C}^{\mathbb{Z}_N}$

$$\langle T(c), f\rangle_{\mathbb{Z}_N} = \langle c, T^*(f)\rangle\,,$$

où $\langle f, g\rangle_{\mathbb{Z}_N} = \frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x)\overline{g(x)}$ et $\langle c, d\rangle = \sum_{\xi\in\Gamma} c(\xi)\overline{d(\xi)}$ sont des produits scalaires hermitiens dans les espaces respectifs.

La première chose à remarquer est que la norme subordonnée de T^* : $L^{p'}(\mathbb{Z}_N, \mu_{\mathbb{Z}_N}) \to l^2(\Gamma)$ est inférieure à $\|T\|_{2\to p}$. Pour le montrer, on prend $c = T^*(f)$ dans la définition de T^* ci-dessus, on utilise l'inégalité de Hölder :

$$\|T^*(f)\|_2^2 = \frac{1}{N}\sum_{x\in\mathbb{Z}_N} T(c)(x)\overline{f(x)} \leq \|T(c)\|_{L^p}\|f\|_{L^{p'}} \leq \|T\|_{2\to p}\|T^*(f)\|_2\|f\|_{L^{p'}}$$

et en simplifiant par $\|T^*(f)\|_2$, l'inégalité obtenue prouve que $\|T^*\|_{p'\to 2} \leq \|T\|_{2\to p}$.

La deuxième remarque est qu'on peut expliciter T^*. En fait, pour tout $c \in \mathbb{C}^\Gamma$ et pour tout $f \in \mathbb{C}^{\mathbb{Z}_N}$

$$\begin{aligned}\langle T(c), f\rangle_{\mathbb{Z}_N} &= \frac{1}{N}\sum_{x\in\mathbb{Z}_N}\sum_{\xi\in\Gamma} c(\xi)\omega^{-\xi x}\overline{f(x)}\\ &= \sum_{\xi\in\Gamma} c(\xi)\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\overline{f(x)\omega^{\xi x}}\\ &= \left\langle c, \frac{1}{N}\hat{f}_{|\Gamma}\right\rangle,\end{aligned}$$

donc l'adjoint de T est la transformée de Fourier renormalisée et restreinte à Γ. L'inégalité de Rudin dit donc que

$$\frac{1}{N}\|\hat{f}_{|\Gamma}\|_2 \leq \|T^*\|_{p'\to 2}\|f\|_{L^{p'}} \leq \|T\|_{2\to p}\|f\|_{L^{p'}} \leq K\sqrt{p}\|f\|_{L^{p'}}$$

pour Γ dissocié et $f \in \mathbb{C}^{\mathbb{Z}_N}$.

Lemme 3.13. *Soit $\rho \in]0,1]$. Soit $X \subseteq \mathbb{Z}_N$. Si $\Gamma \subseteq \mathrm{Spec}(X,\rho)$ est dissocié, alors $|\Gamma| = \mathcal{O}(\frac{1}{\rho^2}\log\frac{N}{|X|})$.*

Démonstration. Posons $\alpha = |X|/N$. On applique l'inégalité de Rudin « duale » à la fonction X. On a $\|X\|_{L^{p'}} = \alpha^{1/p'}$ et

$$\begin{aligned}\|\widehat{X}_{|\Gamma}\|_2^2 &= \sum_{\xi\in\Gamma} |\widehat{X}(\xi)|^2 \\ &\geq |\Gamma|(\rho|X|)^2,\end{aligned}$$

car $\Gamma \subseteq \mathrm{Spec}(X,\rho)$. L'inégalité donne $|\Gamma|\rho^2\alpha^2 \leq K^2 p\alpha^{2/p'} = K^2 p\alpha^2\alpha^{-2/p}$ (lorsque mise au carré), soit $|\Gamma| \leq \frac{K^2}{\rho^2} p\alpha^{-\frac{2}{p}}$. Pour optimiser, on prend $p = \max(2, 2\log\frac{1}{\alpha})$ et on trouve $|\Gamma| = \mathcal{O}(\frac{1}{\rho^2}\log\frac{1}{\alpha})$. □

Remarque. Le réel $\alpha \in]0,1]$ représente en fait la « densité » de X dans $\mathbb{Z}_N$. Plus celle-ci est faible, plus Γ est grand *a priori*. Or essayons d'appliquer directement la formule de Parseval à Γ :

$$N|X| = \sum_{\xi\in\mathbb{Z}_N} |\widehat{X}(\xi)|^2 \geq \sum_{\xi\in\Gamma} |\widehat{X}(\xi)|^2 \geq |\Gamma|\rho^2|X|^2,$$

donc $|\Gamma| \leq \frac{1}{\rho^2}\frac{1}{\alpha}$. La borne est donc bien plus mauvaise (en α^{-1}) que celle fournie par le lemme 3.13. Mais rappelons que dans notre cas, l'ensemble X est justement très petit (α petit devant 1). Par suite, le lemme 3.13 est bien plus fort.

La démonstration du lemme de Chang est maintenant l'affaire de quelques lignes.

Démonstration du théorème 3.7. Soient ρ, X comme dans l'énoncé de 3.7. On prend Γ un sous-ensemble de $\mathrm{Spec}(X,\rho)$, qui est dissocié et maximal pour cette propriété. D'après le lemme précédent, $|\Gamma| = \mathcal{O}(\frac{1}{\rho^2}\log\frac{N}{|X|})$.

Il reste à montrer que $\mathrm{Spec}(X,\rho) \subseteq \mathrm{Span}(\Gamma)$. D'un côté, on a $\Gamma \subseteq \mathrm{Span}(\Gamma)$. De l'autre, pour tout $\xi_0 \in \mathrm{Spec}(X,\rho)\setminus\Gamma$, $\Gamma\cup\{\xi_0\}$ n'est pas dissocié par maximalité de Γ. C'est-à-dire qu'il existe $\epsilon_0 \in \{-1,0,1\}$ et $\epsilon : \Gamma \to \{-1,0,1\}$ non tous deux nuls, tels que

$$\epsilon_0\xi_0 + \sum_{\xi\in\Gamma} \epsilon(\xi)\xi = 0.$$

Or $\epsilon_0 \neq 0$ puisque Γ est dissocié, donc

$$\xi_0 = \sum_{\xi\in\Gamma} -\epsilon_0\epsilon(\xi)\xi,$$

c'est-à-dire $\xi_0 \in \mathrm{Span}(\Gamma)$. □

On va utiliser ce résultat sous la forme du corollaire suivant, qui nous permet de trouver un ensemble de Bohr dont on maîtrise mieux les paramètres :

Corollaire 3.14. *Soient $\rho \in]0,1]$ et $X \subseteq \mathbb{Z}_N$. Alors il existe $\Gamma \subseteq \mathbb{Z}_N$ tel que $B(\Gamma, \frac{1}{6|\Gamma|}) \subseteq B(\mathrm{Spec}(X,\rho), \frac{1}{6})$. De plus, $|\Gamma| = \mathcal{O}(\frac{1}{\rho^2}\log\frac{N}{|X|})$.*

Démonstration. Soient $\rho \in]0,1]$ et $X \subseteq \mathbb{Z}_N$. On note $S = \mathrm{Spec}(X,\rho)$. D'après le théorème 3.7, il existe $\Gamma \subseteq S$ de taille $\mathcal{O}(\frac{1}{\rho^2}\log\frac{N}{|X|})$ tel que $S \subseteq \mathrm{Span}(\Gamma)$. Montrons que $B(\Gamma, \frac{1}{6|\Gamma|}) \subseteq B(S, \frac{1}{6})$.

En effet, étant donné $x \in B(\Gamma, \frac{1}{6|\Gamma|})$, on a par définition $\|\frac{\xi x}{N}\| \leq \frac{1}{6|\Gamma|}$ pour tout $\xi \in \Gamma$. Soit à présent $s \in S$. Alors s est de la forme $\sum_{\xi\in\Gamma} \epsilon(\xi)\xi$ pour une certaine application $\epsilon : \Gamma \to \{-1, 0, 1\}$, et on a par l'inégalité triangulaire pour $\|\cdot\|$, la distance au plus proche entier,

$$\left\| \frac{\left(\sum_{\xi\in\Gamma} \epsilon(\xi)\xi\right) x}{N} \right\| = \left\| \sum_{\xi\in\Gamma} \epsilon(\xi) \frac{\xi x}{N} \right\| \leq \sum_{\xi\in\Gamma} |\epsilon(\xi)| \left\| \frac{\xi x}{N} \right\| \leq |\Gamma| \frac{1}{6|\Gamma|} = \frac{1}{6},$$

d'où $x \in B(S, \frac{1}{6})$. □

4 Étude des voisinages de Bohr

Nous avons réussi à trouver dans certains ensembles de voisinages de Bohr. Pour justifier la peine que l'on s'est donnée, il est temps d'exhiber le lien entre ces voisinages, et les progressions arithmétiques qui sont au cœur du théorème 0.2. Pour cela, nous avons recours à des résultats de géométrie des nombres.

4.1 Réseaux et propriétés

On se donne $d \in \mathbb{N}^*$.

Définition. Un *réseau* dans $\mathbb{R}^d$ est un sous-groupe additif discret de $\mathbb{R}^d$.

Pour $n = (n_1, \ldots, n_r) \in \mathbb{Z}^r$ et $v = (v_1, \ldots, v_r) \in (\mathbb{R}^d)^r$, on note $n \cdot v = n_1 v_1 + \cdots + n_r v_r$. Lorsque $v_1, \ldots, v_r$ sont linéairement indépendants, $\mathbb{Z}^r \cdot v := \{n \cdot v \mid n \in \mathbb{Z}^r\}$, le $\mathbb{Z}$–sous-module engendré par $v_1, \ldots, v_r$, est un réseau. En fait, les ensembles de ce type sont les seuls réseaux.

Proposition 4.1. *Si Λ est un réseau dans $\mathbb{R}^d$, alors il existe $r \in \mathbb{N}$ et des vecteurs $v_1, \ldots, v_r$ linéairement indépendants tels que $\Lambda = \mathbb{Z}^r \cdot (v_1, \ldots, v_r)$.*

On dit alors que $(v_1, \ldots, v_r)$ est une *base* de Λ et que Λ est de *rang* r. Le rang de Λ est d'ailleurs bien défini (*i.e.* il ne dépend pas du choix de la base), car le rang d'un réseau est simplement la dimension du sous-espace de $\mathbb{R}^d$ qu'il engendre.

Si $r = d$, on dit que Λ est *de rang maximal*.

Définition. Soit Λ un réseau $\mathbb{R}^d$ de rang maximal. On défini son *covolume* par $\mathrm{covol}(\Lambda) = |\det(v_1, \ldots, v_d)|$, où $(v_1, \ldots, v_d)$ est une base de Λ. Géométriquement, ce n'est rien d'autre que le volume d'une *maille* élémentaire $\{t_1 v_1 + \cdots + t_d v_d \mid t_i \in [0, 1[\}$.

Il faut montrer que cette définition ne dépend pas non plus de la base †. Essayons pour cela de définir le covolume d'une autre façon. On constate que pour certains ensembles $A \subseteq \mathbb{R}^d$ assez « gentils », le nombre de points à coefficients entiers dans une dilatation tA est de l'ordre de t^d fois un facteur : la mesure de A. Généralisons cette idée. Nous notons λ^* la mesure de Lebesgue.

†. Le raisonnement qui suit n'est pas le plus simple pour parvenir à nos fins, loin s'en faut, mais il est original et assez élémentaire.

Les ensembles « gentils » que nous considérerons seront des ensembles $A \subseteq \mathbb{R}^d$ muni de la norme euclidienne, qui sont ouverts, bornés, et tels que $\lambda^*(\partial A) = 0$ (où ∂A désigne la frontière de A, *i.e.* les éléments de l'adhérence de A qui ne sont pas dans A). Nous les appellerons abusivement des *ouverts de Jordan*. Dans la suite, on appelle aussi *ensemble élémentaire* toute réunion finie disjointe de pavés semi-ouverts[‡]. La gentillesse d'un ouvert de Jordan s'exprime alors sous forme d'un lemme :

Lemme 4.2. *Soit A de $\mathbb{R}^d$ un ouvert borné tel que $\lambda^*(\partial A) = 0$. Alors*

$$\lambda^*(A) = \inf_{E' \supseteq A} \lambda^*(E') = \sup_{E \subseteq A} \lambda^*(E),$$

où E et E' décrivent tous les ensembles élémentaires.

Preuve. Remarquons déjà que $\lambda^*(\overline{A}) = \lambda^*(A) + \lambda^*(\partial A) = \lambda^*(A)$.

Par définition de la mesure de Lebesgue, $\lambda^*(\overline{A}) = \inf_P \lambda^*(P)$, où l'infimum est pris sur les réunions dénombrables de pavés ouverts dans lesquelles A est inclus. Comme $\overline{A}$ est compact, on peut cependant se restreindre aux réunions finies, et aux réunions finies de pavés semi-ouverts (car leur mesure ne change pas qu'ils soient ouverts ou semi-ouverts). Or toute réunion finie de pavés semi-ouverts s'écrit aussi comme réunion finie et disjointe de pavés semi-ouverts, ce qui donne la première égalité.

Pour le deuxième point, nous avons déjà

$$\sup_{E \subseteq A} \lambda^*(E) \leq \lambda^*(A). \tag{6}$$

Grâce à la régularité de la mesure de Lebesgue, il existe un suite de compacts $K_n \subseteq A$ tels que $\lambda^*(K_n) \to \lambda^*(A)$ quand $n \to \infty$. Pour chaque compact K_n, notons $\delta_n := \frac{1}{3} d(K_n, \mathbb{R}^d \setminus A)$. C'est un réel strictement positif (car $\mathbb{R}^d \setminus A$ est un fermé disjoint du compact K_n). Si on quadrille l'espace $\mathbb{R}^d$ de pavés semi-ouverts disjoints de côté δ_n, on obtient un recouvrement E_n de K_n, fini car K_n est borné, et inclus dans A grâce à la définition de δ_n. Donc

$$\lambda^*(K_n) \leq \lambda^*(E_n) \leq \lambda^*(A),$$

et en faisant tendre n vers l'infini, on trouve l'inégalité contraire de (6), et donc l'égalité désirée. □

Le deuxième avantage des ouverts de Jordan est qu'ils sont stables par isomorphisme linéaire. Soient en effet A un ouvert de Jordan, et ϕ un isomorphisme linéaire de $\mathbb{R}^d$. En particulier, ϕ est un homéomorphisme de $\mathbb{R}^d$. Dès lors,

- $\phi(A)$ est aussi ouvert.
- $\phi(A)$ est borné (grâce à la continuité et la linéarité de ϕ)
- Comme ϕ est un homéomorphisme, $\partial(\phi(A)) = \phi(\partial A)$, et donc

$$\lambda^*(\partial(\phi(A))) = \lambda^*(\phi(\partial A)) = |\det \phi| \, \lambda^*(\partial A) = 0.$$

Ces instruments nous permettent de prouver le résultat annoncé :

‡. On entend par là les ensembles de la forme $[a_1, b_1[\times \cdots \times [a_d, b_d[$.

Proposition 4.3. *Soit Λ un réseau $\mathbb{R}^d$ de rang maximal. Si $A \subseteq \mathbb{R}^d$ est un ouvert de Jordan, alors $\frac{\lambda^*(tA)}{|\Lambda \cap tA|}$ converge quand $t \to \infty$, et la limite est $|\det(v_1, \ldots, v_d)|$, où $(v_1, \ldots, v_d)$ est une base de Λ.*

Cela montre donc $|\det(v_1, \ldots, v_d)|$ est le même, quelle que soit la base de Λ, car on peut définir le covolume d'un réseau par

$$\mathrm{covol}(\Lambda) = \lim_{t\to\infty} \frac{\lambda^*(tA)}{|\Lambda \cap tA|},$$

où A est un ouvert de Jordan quelconque.

Démonstration. Ramenons-nous au cas où le réseau est $\mathbb{Z}^d$. La famille $(v_1, \ldots, v_d)$ est une base de l'espace vectoriel $\mathbb{R}^d$, donc il existe donc un automorphisme linéaire ϕ de $\mathbb{R}^d$ tel que pour $1 \leq i \leq d$, $\phi(v_i) = e_i$, avec $(e_1, \ldots, e_d)$ la base usuelle de $\mathbb{R}^d$. Par la formule de changement de variable, pour U mesurable, $\lambda^*(\phi(U)) = |\det \phi|\, \lambda^*(U)$. De plus, comme ϕ est injective, $\phi(\Lambda \cap tA) = \phi(\Lambda) \cap t\phi(A)$. On a alors

$$\frac{\lambda^*(tA)}{|\Lambda \cap tA|} = \frac{|\det \phi|^{-1}\, \lambda^*(t\phi(A))}{|\phi(\Lambda) \cap \phi(tA)|} = |\det(v_1, \ldots, v_d)| \frac{t^d\, \lambda^*(\phi(A))}{|\mathbb{Z}^d \cap t\phi(A)|}.$$

Notons $B := \phi(A)$; c'est un ouvert de Jordan, d'après la remarque précédente. Il suffit donc de montrer que $t^{-d}|\mathbb{Z}^d \cap tB|$ converge vers $\lambda^*(B)$. C'est le résultat que nous avons isolé dans le lemme qui suit. □

Lemme 4.4. *Si $B \subseteq \mathbb{R}^d$ est un ouvert de Jordan, alors*

$$\lim_{t\to\infty} \frac{|\mathbb{Z}^d \cap tB|}{t^d} = \lambda^*(B).$$

Démonstration. C'est le cas pour les pavés : soit $P = [a_1, b_1[\times \cdots \times [a_d, b_d[$. On a $\lambda^*(P) = \prod_{i=1}^d (b_i - a_i)$, et

$$|\mathbb{Z}^d \cap tP| = \prod_{i=1}^d |\mathbb{Z} \cap [ta_i, tb_i[| = \prod_{i=1}^d (\lceil tb_i \rceil - \lceil ta_i \rceil) \underset{t\to\infty}{\sim} t^d \prod_{i=1}^d (b_i - a_i).$$

Donc $\lim t^{-d}|\mathbb{Z}^d \cap tP| = \lambda^*(P)$. On en déduit que la propriété vraie aussi pour un ensemble élémentaire : soit $E = \bigsqcup_{i=1}^n P_i$ un tel ensemble. Alors

$$t^{-d}|\mathbb{Z}^d \cap tE| = \sum_{i=1}^n t^{-d}|\mathbb{Z}^d \cap tP_i| \xrightarrow[t\to\infty]{} \sum_{i=1}^n \lambda^*(P_i) = \lambda^*(E).$$

Soit E et E' des ensembles élémentaires tels que $E \subseteq B \subseteq E'$. On a

$$t^{-d}|\mathbb{Z}^d \cap tE| \leq t^{-d}|\mathbb{Z}^d \cap tB| \leq t^{-d}|\mathbb{Z}^d \cap tE'|,$$

donc, à la limite

$$\lambda^*(E) \leq \liminf_{t\to\infty} t^{-d}|\mathbb{Z}^d \cap tB| \leq \limsup_{t\to\infty} t^{-d}|\mathbb{Z}^d \cap tB| \leq \lambda^*(E').$$

Avec le lemme 4.2, on en déduit l'égalité des limites inférieure et supérieure, et

$$\lim_{t\to\infty} t^{-d}|\mathbb{Z}^d \cap tB| = \lambda^*(B).$$

□

Comme conséquence, nous trouvons un lien entre le covolume d'un réseau et celui d'un sous-réseau (*i.e.* un sous-groupe) de ce réseau.

Proposition 4.5. *Si $\Lambda \subseteq \Gamma \subseteq \mathbb{R}^d$ sont des réseaux de rang maximal alors,*

$$\mathrm{covol}(\Lambda) = |\Gamma/\Lambda| \cdot \mathrm{covol}(\Gamma).$$

Démonstration. Prenons $v = (v_1, \ldots, v_d)$ une base de Λ, et notons P la maille $\{t_1 v_1 + \cdots t_d v_d \mid t_i \in [0,1[\}$. Pour tout $t \in \mathbb{N}$, on écrit tP comme réunion de translatés de P :

$$tP = \bigsqcup_{0 \leq n_1, \ldots, n_d < t} (P + (n_1, \ldots, n_d) \cdot v),$$

donc $|\Gamma \cap tP| = \sum |\Gamma \cap (P + (n_1, \ldots, n_d) \cdot v)| = t^d |\Gamma \cap P|$ (on utilise ici le fait que $\Lambda \subseteq \Gamma$). Et on vérifie sans difficulté que la projection canonique dans le quotient induit une bijection de $\Gamma \cap P$ dans Γ/Λ. D'où

$$\mathrm{covol}(\Gamma) = \lim_{t \to \infty} \frac{\lambda^*(tP)}{|\Gamma \cap tP|} = \lim_{\substack{t \to \infty \\ t \in \mathbb{N}}} \frac{t^d \, \lambda^*(P)}{|\Gamma \cap tP|} = \lim_{\substack{t \to \infty \\ t \in \mathbb{N}}} \frac{\lambda^*(P)}{|\Gamma \cap P|} = \frac{\mathrm{covol}(\Lambda)}{|\Gamma/\Lambda|}.$$

□

4.2 Théorème de Minkowski

Définition. Soient $\Lambda \subseteq \mathbb{R}^d$ un réseau, K un ouvert convexe de $\mathbb{R}^d$. On appelle le *k-ième minimum successif* de K par rapport à Λ, le réel

$$\lambda_k(K, \Lambda) = \inf\{\lambda > 0 \mid \lambda K \text{ contient } k \text{ vecteurs linéairement indépendants de } \Lambda\}.$$

On note λ_k à la place de $\lambda_k(K, \Lambda)$ lorsqu'il n'y a pas d'ambiguïté.

Théorème 4.6 (Deuxième théorème de Minkowski)**.** *Soient $\Lambda \subseteq \mathbb{R}^d$ un réseau, K un ouvert convexe borné de $\mathbb{R}^d$. Si K est de plus symétrique par rapport à l'origine, alors*

$$\lambda_1 \cdots \lambda_d \, \lambda^*(K) \leq 2^d \, \mathrm{covol}(\Lambda).$$

Nous ne donnons pas la preuve de ce théorème, qui nous éloignerait trop du sujet. On peut par exemple se reporter à [5]. Nous prouvons en revanche un petit lemme :

Lemme 4.7. *Soient $\Lambda \subseteq \mathbb{R}^d$ un réseau de rang maximal, K un ouvert convexe borné de $\mathbb{R}^d$, symétrique par rapport à l'origine. Notons $\lambda_1, \ldots, \lambda_d$ la famille des minima successifs de K par rapport à Λ.*

Il existe une base $(b_1, b_2, \ldots, b_d)$ de Λ telle que pour tout $1 \leq i \leq d$, $b_i \in \lambda_i \overline{K}$.

Preuve. Nous construisons cette base par récurrence.

Commençons par trouver le premier vecteur. Par définition de λ_1, pour tout $n \geq 1$ entier, il existe $b_1^n \in (\lambda_1 + \frac{1}{n})K$ non nul et appartenant au réseau Λ. Tous les b_1^n sont dans $(\lambda_1 + 1)K$. Puisque Λ est discret et que $(\lambda_1 + 1)K$ est borné, $(\lambda_1 + 1)K \cap \Lambda$ est nécessairement fini, donc la suite $(b_1^n)_{n \geq 1}$ ne comprend qu'un nombre fini de termes. Il existe ainsi une suite d'entiers $(n_k)_k$ croissant

vers l'infini, telle que $(b_1^{n_k})$ est constante. Notons b_1 sa valeur : $b_1 \in \Lambda$, est non nul, et pour tout $k \geq 1$, $b_1 \in (\lambda_1 + \frac{1}{n_k})K$. Comme $\frac{1}{n_k} \to 0$ quand $k \to \infty$, on en déduit que toute boule centrée en b_1 rencontre $\lambda_1 K$, et qu'alors,

$$b_1 \in \overline{\lambda_1 K} = \lambda_1 \overline{K}.$$

Supposons ensuite construits $b_1, \ldots, b_{k-1}$, et trouvons b_k. On procède en fait de la même façon. Fixons $n \geq 1$: il existe une famille libre $(v_1, \ldots, v_k)$ de vecteurs de Λ dans $(\lambda_k + \frac{1}{n})K$. L'un d'eux, que l'on note b_k^n, n'appartient pas à $\mathrm{Vect}(b_1, \ldots, b_{k-1})$, qui est de dimension $k-1$. Dans ce cas, la famille $(b_1, \ldots, b_{k-1}, b_k^n)$ est libre. Muni de la suite $(b_k^n)_{n \geq 1}$ de vecteurs de $(\lambda_k + 1)K$, nous concluons exactement de la même manière qu'au paragraphe précédent. □

4.3 Progression arithmétique dans un voisinage de Bohr

À l'aide du deuxième théorème de Minkowski, on montre qu'un ensemble de Bohr contient une « grande » progression arithmétique. Ici, N est toujours un nombre premier impair.

Proposition 4.8 (Ruzsa [10]). *Soient $\Gamma \subseteq \mathbb{Z}_N$ un ensemble de cardinal k, et $\delta \in]0, \frac{1}{2}[$. Alors l'ensemble de Bohr $B(\Gamma, \delta)$ contient une progression arithmétique propre de dimension k et de taille $\geq (\delta/k)^k N$.*

Démonstration. Le cas $\Gamma = \{0\}$ est simple, car alors $B(\Gamma, \delta) = \mathbb{Z}_N$ tout entier. On suppose donc que Γ contient des élément non nuls [§]. Soient $\xi_1, \ldots, \xi_k$ les éléments de Γ. Prenons pour chacun de ξ_i un représentant $r_i \in \mathbb{Z}$.

Posons $\Lambda = N\mathbb{Z}^k + (r_1, \ldots, r_k)\mathbb{Z}$. Montrons qu'il s'agit bien d'un réseau. C'est un sous-groupe de $(\mathbb{R}^k, +)$. De plus, $N\mathbb{Z}^k$ en est un sous-groupe. Le groupe quotient $\Lambda / N\mathbb{Z}^k$ est monogène, engendré par $\bar{r}$, la classe de $(r_1, \ldots, r_k)$, dont l'ordre est N. En effet, $N\bar{r} = 0$, donc l'ordre de $\bar{r}$ divise N, mais N est premier, donc c'est N (ce n'est pas 1, car $\bar{r} \neq 0$ par la remarque introductive). Donc $\Lambda / N\mathbb{Z}^k$ est cyclique d'ordre N. On en déduit qu'à l'intérieur de chaque cube de côté N, il y a un nombre fini d'éléments de Λ (au plus N), et par conséquent, Λ est discret.

D'après la proposition 4.5,

$$\mathrm{covol}(\Lambda) = \frac{\mathrm{covol}(N\mathbb{Z}^k)}{|\Lambda / N\mathbb{Z}^k|} = \frac{N^k}{N} = N^{k-1}.$$

Soit K le l^∞–cube $\{x \in \mathbb{R}^k \mid \|x\|_\infty < \delta N\}$ (où la norme $\|\cdot\|_\infty$ désigne le maximum des valeurs absolues des composantes du vecteur). K est ouvert, convexe et symétrique par rapport à l'origine, et de mesure $(2\delta N)^k$. Soient $\lambda_1, \ldots, \lambda_k$ les minima successifs de K par rapport à Λ. Par 4.7, on trouve une base $(b_1, \ldots, b_k)$ de Λ telle que $b_i \in \lambda_i \overline{K}$. Chaque b_i est de la forme $b_i = Nv_i + x_i(r_1, \ldots, r_k)$ avec $v_i \in \mathbb{Z}^k$ et $x_i \in \mathbb{Z}$. Notons $\bar{x}_i$ la classe de x_i dans $\mathbb{Z}_N$. Le fait que $b_i \in \lambda_i \overline{K}$ implique que $\left\|\frac{b_i}{N}\right\|_\infty \leq \lambda_i \delta$, donc que $\left\|\frac{\xi \bar{x}_i}{N}\right\| \leq \lambda_i \delta$ pour tout $\xi \in \Gamma$. On est donc ramené à considérer la progression suivante

$$Q = \left\{ \mu_1 \bar{x}_1 + \cdots + \mu_k \bar{x}_k \;\middle|\; \mu_i \in \mathbb{Z} \text{ et } |\mu_i| \leq \left\lfloor \frac{1}{k\lambda_i} \right\rfloor \right\}.$$

§. On peut aussi supposer qu'il ne contient pas 0, puisque 0 ne joue aucun rôle.

Montrons que $Q \subseteq B(\Gamma, \delta)$. En effet, pour tout $\xi \in \Gamma$, on a

$$\left\| \frac{\xi \cdot (\mu_1 \bar{x}_1 + \cdots + \mu_k \bar{x}_k)}{N} \right\| \leq \sum_{i=1}^{k} |\mu_i| \left\| \frac{\xi \bar{x}_i}{N} \right\| \leq \sum_{i=1}^{k} \left\lfloor \frac{1}{k\lambda_i} \right\rfloor \lambda_i \delta \leq \delta.$$

La taille de Q est

$$\prod_{i=1}^{k} \left(2 \left\lfloor \frac{1}{k\lambda_i} \right\rfloor + 1 \right) \geq \prod_{i=1}^{k} \frac{1}{k\lambda_i} = \frac{1}{k^k \lambda_1 \cdots \lambda_k}.$$

D'après le deuxième théorème de Minkowski,

$$\lambda_1 \cdots \lambda_k \leq \frac{2^k \operatorname{covol}(\Lambda)}{\lambda^*(K)} = \frac{2^k N^{k-1}}{(2\delta N)^k} = \frac{1}{\delta^k N}.$$

Par suite, la taille de Q est au moins $(\delta/k)^k N$.

Il ne reste plus qu'à montrer que Q est propre. Supposons que

$$\mu_1 \bar{x}_1 + \cdots + \mu_k \bar{x}_k = \mu'_1 \bar{x}_1 + \cdots + \mu'_k \bar{x}_k, \qquad \text{avec } |\mu_i|, |\mu'_i| \leq \left\lfloor \frac{1}{k\lambda_i} \right\rfloor.$$

Alors, le vecteur $b = (\mu_1 - \mu'_1)b_1 + \cdots + (\mu_k - \mu'_k)b_k$ appartient à $N\mathbb{Z}^k$. On a de plus $\|b\|_\infty \leq \sum_{i=1}^{k} \frac{2}{\lambda_i k} \|b_i\|_\infty \leq 2\delta N < N$ grâce au choix de δ. Donc $b = 0$ et pour tout i, $\mu_i = \mu'_i$, puisque $(b_1, \ldots, b_k)$ est une base de $\mathbb{R}^k$. On en conclut que Q est une progression arithmétique propre (son cardinal est égal à sa taille). □

5 Preuve du théorème de Freiman-Ruzsa

5.1 Lemme de recouvrement de Chang

Ce que nous avons prouvé jusqu'ici nous a permis de montrer que certains ensembles, reliés plus ou moins directement à A, contiennent des progressions arithmétiques propres. Notre but est cependant de *recouvrir* A par des progressions arithmétiques. Pour arriver au théorème de Freiman, il nous faut donc un autre ingrédient : le *lemme de recouvrement* de Chang.

Définition. Soit B et R deux parties d'un groupe abélien. On dit que R est *B–libre* si pour tout $x, y \in R$ distincts, $x + B$ et $y + B$ sont disjoints.

Remarquons que si R est B–libre, alors $R + B$ est la réunion disjointe de $|R|$ translatés de B, et donc le cardinal de $R + B$

$$|R + B| = |R||B|. \tag{7}$$

Une autre remarque simple est que si R, partie B–libre de A, est maximale (au sens de l'inclusion) pour cette propriété, alors $A \subseteq R + B - B$.

Démonstration. En effet, soit a un élément de A, alors $a + B$ rencontre $r_0 + B$ pour un $r_0 \in R$, car si $(a + B) \cap (r + B) = \emptyset$ pour tout r, alors en particulier $a \notin R$, et de plus $R \cup \{a\}$ serait B–libre ce qui contredit la maximalité de R. Donc il existe $r_0 \in R$ et $b, b' \in B$ tels que $a + b = r_0 + b'$, ce qui prouve que $a \in r_0 + B - B \subseteq R + B - B$. □

Ces deux remarques permettent déjà d'obtenir un premier lemme de recouvrement, dû à Ruzsa.

Lemme 5.1 (Ruzsa [10]). *Soient $A, B \subseteq G$ un groupe abélien. Il existe $R \subseteq A$ de cardinal au plus $\frac{|A+B|}{|B|}$ tel que $A \subseteq R + B - B$. Autrement dit, A peut être recouvert par au plus $\frac{|A+B|}{|B|}$ translatés de $B - B$.*

Preuve. Il suffit de prendre $R \subseteq A$ B–libre maximal. On a donc $A \subseteq R+B-B$. Pour majorer $|R|$, on a par (7), $|R||B| = |R + B| \leq |A + B|$. □

Les bornes dans le théorème de Freiman que nous permettrait d'obtenir ce lemme sont cependant bien trop grandes. Il nous faut raffiner les arguments, et prouver un nouveau lemme, où l'on contrôle cette fois le cardinal des ensembles recouvrant A :

Lemme 5.2 (Chang [1]). *Soient $A, B \subseteq G$ un groupe abélien. Supposons $|A + A| \leq C|A|$ et $|A + B| \leq L|B|$ pour C, L réels positifs. Alors il existe $t \leq \log_2(\lceil C \rceil L)$ et $S_0, \ldots, S_{t-1}$ et R_t des parties de A de cardinal $\leq 2\lceil C \rceil$ telles que $A \subseteq B - B + S_0 - S_0 + \cdots + S_{t-1} - S_{t-1} + R_t$.*

Démonstration. Quitte à remplacer C par $\lceil C \rceil$, on suppose que C est entier.

Nous allons trouver ces ensembles grâce à un algorithme. Pour initialiser, posons $B_0 = B$. On définit ensuite des ensembles B_i et S_i récursivement. Pour un B_i donné, on prend $R_i \subseteq A$ une partie B_i–libre maximale. Si $|R_i| \leq 2C$ alors on pose $t = i$ et l'algorithme se termine. Sinon, on prend S_i un sous-ensemble de R_i de cardinal $2C$, et on continue avec $B_{i+1} := B_i + S_i$.

Montrons que l'algorithme précédent se termine rapidement ¶. Pour tout $i < t$, $S_i \subseteq R_i$, donc est un sous-ensemble d'un ensemble B_i–libre ; il est ainsi B_i–libre lui-même. D'après (7), $|B_{i+1}| = |B_i + S_i| = |S_i||B_i| = 2C|B_i|$. Par récurrence, on obtient que pour $i \leq t$, $|B_i| = (2C)^i|B|$. D'autre part, $B_i = B + S_0 + \cdots + S_{i-1}$, donc $B_i \subseteq B + iA$. Par l'inégalité triangulaire de Ruzsa 1.2 et les inégalités de Plünnecke 1.1, on majore le cardinal de $B + iA$:

$$|B + iA| \leq \frac{|A + B||A - iA|}{|A|} \leq LC^{i+1}|B|.$$

D'où $(2C)^i|B| = |B_i| \leq |B + iA| \leq LC^{i+1}|B|$. Par conséquent, $2^i \leq CL$ pour tout $i \leq t$. En particulier, $t \leq \log_2(CL)$.

On est ainsi assuré que l'algorithme termine et fournit un t. Il reste à prouver que tous ces ensembles recouvrent A de la manière souhaitée. Comme R_t est une partie B_{t-1}–libre de A maximale, par le lemme précédent, $A \subseteq B_{t-1} - B_{t-1} + R_t$, c'est-à-dire $A \subseteq B - B + S_0 - S_0 + \ldots + S_{t-1} - S_{t-1} + R_t$.

□

5.2 Preuve du théorème de Freiman-Ruzsa

Tous les éléments sont à présent réunis pour prouver le théorème de Freiman-Ruzsa.

¶. Bien sûr, pour l'instant, t peut être éventuellement infini.

Preuve du théorème 0.2. Soit $A \subseteq \mathbb{Z}$ tel que $|A+A| \leq C|A|$. D'après le théorème de Bertrand, il existe un entier premier N compris entre $24C^{24}|A|$ et $48C^{24}|A|$.

Le lemme de Ruzsa (2.2), dont les hypothèses sont bien vérifiées, permet d'affirmer l'existence de $A' \subseteq A$ qui est 12–isomorphe à $T \subseteq \mathbb{Z}_N$, et tel que $|A'| \geq |A|/12$. Notons $\varphi : A' \to T$ l'isomorphisme de Freiman. On a déjà remarqué que dans ces conditions, φ^{-1} induit une bijection naturelle de $T+T$ sur $A'+A'$, et donc

$$|T+T| = |A'+A'| \leq |A+A| \leq C|A| \leq 12C|A'| = 12C|T|.$$

À partir de là, on peut choisir $X \subseteq T$ et $Y \subseteq T+T$ qui satisfont le lemme de Schoen (3.5) avec $\varepsilon = (\log C)^{-1/2}$. Comme $|T| = |A'| \geq |A|/12 \geq \frac{N}{12 \cdot 48C^{24}}$, le cardinal de X

$$\begin{aligned} |X| \geq (2(12C)^2)^{-2^{1/\varepsilon}}|T| &\geq (288C^2)^{-2^{1/\varepsilon}}|T| \\ &\geq (288C^2)^{-2^{1/\varepsilon}} 2^{-10} C^{-24} N. \end{aligned}$$

D'après le corollaire 3.6, $X+Y-X-Y$ contient un voisinage de Bohr $B(S, \frac{1}{6}) \subseteq X+Y-X-Y$, avec $S = \mathrm{Spec}(X, \frac{1}{2}(12C)^{-\varepsilon})$, et par un corollaire du lemme spectral de Chang (3.14), il existe $\Gamma \subseteq \mathbb{Z}_N$ tel que $B(\Gamma, (6|\Gamma|)^{-1}) \subseteq B(S, \frac{1}{6})$, avec $|\Gamma| \leq \kappa \cdot 4(12C)^{2\varepsilon} \log(N/|X|)$.

Enfin, par le résultat de Ruzsa sur les ensembles de Bohr (4.8), il existe une progression arithmétique propre $P \subseteq B(\Gamma, (6|\Gamma|)^{-1})$, de dimension $|\Gamma|$, et de taille supérieure à

$$\left(\frac{(6|\Gamma|)^{-1}}{|\Gamma|}\right)^{|\Gamma|} N = \left(\frac{1}{6|\Gamma|^2}\right)^{|\Gamma|} N.$$

Ainsi, $P \subseteq X+Y-X-Y \subseteq 3T-3T$, et en combinant les informations ci-dessus, on peut estimer

– la dimension de P :

$$d_P = |\Gamma| \leq \kappa \cdot 4(12C)^{2\varepsilon} \log\left((288C^2)^{2^{1/\varepsilon}} 2^{10} C^{24}\right).$$

Or $2^{1/\varepsilon} = 2^{\varepsilon \log C} = C^{\varepsilon \log 2} \leq C^{\varepsilon}$, grâce à la définition de ε. Le terme dominant en C dans la somme est donc celui en $2^{1/\varepsilon} 2 \log C$, si bien qu'il existe une constante absolue κ_1 telle que $d_P \leq \kappa_1 C^{3\varepsilon} \log C$.

– la taille de P, ou $|P|$ comme P est propre :

$$\begin{aligned} t_P &= \exp(-|\Gamma|(\log 6 + 2\log|\Gamma|))N \\ &\geq \exp(-\kappa_1 C^{3\varepsilon} \log C(\log 6 + 2\log\kappa_1 + 6\varepsilon \log C + 2\log\log C))N \\ &\geq \exp(-\kappa_2 C^{3\varepsilon} \log C \cdot (\log C)^{1/2})N, \end{aligned}$$

où κ_2 est une nouvelle constante, que l'on introduit grâce au fait que $\log C^{1/2}$ domine les autres termes de la parenthèse.
Or $\kappa_2 = (\log C)^{\log \kappa_2 / \log\log C} = (\log C)^{\circ(1)}$. Donc

$$t_P \geq \exp(-C^{3\varepsilon}(\log C)^{3/2+\circ(1)})N.$$

Il reste à « remonter » dans $\mathbb{Z}$. Considérons P', l'image de P par φ^{-1} (ou plutôt par l'application que φ^{-1} induit sur $3T-3T$, que l'on note encore φ^{-1}).

Comme φ^{-1} est un 12–isomorphisme de Freiman et que $P \subseteq 3T - 3T$, φ^{-1} est un 2–isomorphisme de P sur P'. Or l'image d'une progression arithmétique (généralisée) par un 2–homomorphisme de Freiman est également une progression arithmétique de taille inférieure ou égale (c'est le résultat du lemme 2.1), et puisque φ^{-1} est bijective, $|P'| = |P|$. Cela prouve que P' est également une progression arithmétique propre (son cardinal et sa taille coïncident).

Constatons enfin que grâce aux inégalités de Plünnecke (1.1),

$$|P' + A| \leq |3A - 3A + A| \leq C^7|A| \leq C^7 \exp(C^{3\varepsilon}(\log C)^{3/2+\circ(1)})|P'|,$$

car la taille de P est la même que celle de P', et car $N \geq 24C^{24}|A| > |A|$. Appliquons le lemme de recouvrement de Chang (5.2) à A et P', pour obtenir

$$\begin{aligned} A &\subseteq P' - P' + S_0 - S_0 + \ldots + S_{t-1} - S_{t-1} + R_t \\ &\subseteq P' - P' + \mathrm{Span}(S_0 \cup \cdots \cup S_{t-1} \cup R_t) =: Q, \end{aligned}$$

avec

$$\begin{aligned} t &\leq \log_2((C+1)C^7 \exp(C^{3\varepsilon}(\log C)^{3/2+\circ(1)}) \\ &\leq \log_2((C+1)C^7) + (\log 2)^{-1} C^{3\varepsilon}(\log C)^{3/2+\circ(1)} \\ &\leq \kappa_3 C^{3\varepsilon}(\log C)^{3/2+\circ(1)} \\ &\leq C^{3\varepsilon}(\log C)^{3/2+\circ(1)}. \end{aligned}$$

Or pour tout $H \subseteq G$, $\mathrm{Span}(H)$ est une progression arithmétique de dimension $|H|$, et de taille $3^{|H|}$. On a donc prouvé que A est inclus dans Q, qui, par le lemme 0.1, est une progression arithmétique de dimension

$$\begin{aligned} d_Q &\leq d_P + (t+1) \cdot 2(C+1) \\ &\leq C^{3\varepsilon}(\log C)^{1+\circ(1)} + 2(C+1)C^{3\varepsilon}(\log C)^{3/2+\circ(1)} \\ &\leq \kappa_4 C \cdot C^{3\varepsilon}(\log C)^{3/2+\circ(1)} \\ &= C^{1+3\varepsilon} \cdot C^{\frac{\log \kappa_4}{\log C} + \frac{(3/2+\circ(1))\log\log C}{\log C}} \\ &\leq C^{1+K\varepsilon} \end{aligned}$$

et de taille

$$\begin{aligned} t_Q &\leq (2^{d_P} t_P) 3^{(t+1)\cdot 2(C+1)} \\ &\leq C^6|A| \exp(d_P \log 2 + (t+1) \cdot 2(C+1) \log 3) \\ &\leq |A| \exp(C^{1+K\varepsilon}), \end{aligned}$$

par le même calcul que d_Q, pour une certaine constante K. Ce sont les bornes souhaitées, à condition de remarquer que $C^{1+K\varepsilon} = C \cdot \exp(K\varepsilon \log C) = C \cdot \exp(K(\log C)^{1/2})$. □

6 Généralisations du théorème

Nous avons démontré le théorème de Freiman-Ruzsa dans $\mathbb{Z}$. À vrai dire, il existe beaucoup d'autres énoncés de ce théorème. Nous essayons dans cette partie d'en présenter quelques uns.

6.1 Cas des groupes abéliens quelconques

Soit G un groupe abélien. On veut savoir si le théorème de Freiman-Ruzsa est vrai dans G :

Théorème 6.1 (Freiman-Ruzsa dans G). *Soit $A \subseteq G$ fini, tel que $|A+A| \leq C|A|$, avec C une constante réelle. Alors A est contenu dans une progression arithmétique généralisée,*
- *de dimension inférieure à $d(G,C)$,*
- *de taille inférieure à $f(G,C)|A|$.*

Mieux encore, y a-t-il des bornes « universelles » $d(C)$, $f(C)$ pour tous les groupes abéliens ? Ou pour certaines classes de groupe ?

Cas des groupes cycliques d'ordre premier. On remarquera qu'on a montré la proposition 2.2 en passant par ce cas. Il suffit donc de reprendre la preuve à partir de $\mathbb{Z}_p$, au lieu de $\mathbb{Z}$. On trouve donc bien le théorème de Freiman-Ruzsa pour le groupe $\mathbb{Z}_p$ avec p premier. Les bornes $d(C)$ et $f(C)$ sont les mêmes que dans le théorème 0.2. Ces bornes sont indépendantes de p.

Soulignons malgré tout l'importance de la proposition 2.2. Bien qu'on puisse faire directement de l'analyse de Fourier dans le groupe $\mathbb{Z}_p$, il nous faut plonger l'ensemble A dans un groupe où sa densité est assez grande, ce que permet de faire cette proposition.

Cas des groupes sans torsion. La proposition suivante réduit en fait ce cas à celui de $\mathbb{Z}$.

Proposition 6.2 (Ruzsa [10]). *Soit A un sous-ensemble fini d'un groupe sans torsion. Pour tout k, on peut plonger A dans $\mathbb{Z}$ par un isomorphisme de Freiman d'ordre k. On dit que $\mathbb{Z}$ est un k–modèle de A.*

Démonstration. En effet, le sous-groupe engendré par A est un groupe G (abélien), de type fini et sans torsion, donc isomorphe à $\mathbb{Z}^n$ pour un certain n, d'après la classification des groupes abéliens de type fini. Or cet isomorphisme de groupes induit un isomorphisme de Freiman à tout ordre de A sur son image. On peut donc supposer que A est un sous-ensemble fini de $\mathbb{Z}^n$.

On définit l'application « écriture en base t » comme suit

$$\phi_t : (a_1, \ldots, a_n) \in A \mapsto a_1 + a_2 t + \cdots + a_n t^{n-1} \in \mathbb{Z}.$$

ϕ_t est la restriction à A d'un morphisme de groupes. Pour qu'il soit un k–isomorphisme de Freiman, il faut et il suffit que le morphisme de groupe soit injectif sur $kA-kA$. C'est le cas quand t est assez grand ($t > 2k \max_{a\in A} \|a\|_\infty$). □

Même avec cette réduction, on ne peut pas appliquer le théorème de Freiman-Ruzsa dans $\mathbb{Z}$ directement, car le fait d'être recouvert par une progression arithmétique n'est pas une propriété qui se communique par isomorphisme de Freiman : seules les propriétés à « l'intérieur » de $lA - mA$, $l+m \leq k$ se remontent en arrière en passant par un k–isomorphisme.

On va donc tirer en arrière la propriété dite de « Bogolyubov-Ruzsa », en l'occurrence, $3A-3A$ contient une grande progression arithmétique. Ensuite, on

applique le lemme de recouvrement de Chang, qui est valable dans un groupe abélien quelconque. Ainsi on trouve le théorème de Freiman-Ruzsa dans les groupes sans torsion. Une fois de plus, les bornes (indépendantes du groupe en question) sont les mêmes que pour $\mathbb{Z}$. En particulier, le théorème de Freiman-Ruzsa s'énonce de la même manière que le théorème 0.2.

Cas des groupes dont l'ordre des éléments est borné. Soit G un groupe dont les éléments sont tous d'ordre inférieur à r. Dans ces groupes, il y a des progressions très particulières : les sous-groupes finis. On peut établir un analogue du théorème de Freiman-Ruzsa pour ces groupes en utilisant simplement les inégalités de Plünnecke-Ruzsa (théorème 1.1) et le lemme de recouvrement de Ruzsa (lemme 5.1). Le résultat est que si $A \subseteq G$ tel que $|A+A| \leq C|A|$, alors A est contenu dans un translaté d'un sous-groupe de cardinal $\leq f(r,C)|A|$, où $f(r,C)$ ne dépend que de r et C. Voir [11] ou [5, Théorème 9].

Cas général. Dans notre preuve du théorème 0.2, deux points sont à première vue spécifiques au groupe $\mathbb{Z}$. Le premier est la proposition 2.2, qui permet de trouver un bon modèle. Le deuxième point est que le modèle en question est un groupe très précis, $\mathbb{Z}_N$, dans lequel l'analyse de Fourier est agréable.

Pour résoudre le deuxième problème, il apparaît qu'il est possible de faire de l'analyse de Fourier dans tous les groupes abéliens finis. Comme espace de fréquences, au lieu de $\mathbb{Z}_N$, on choisit l'ensemble $\widehat{G}$ des morphismes de groupes de G dans $\mathbb{U}$[†]. La transformée de Fourier est définie pour toute fonction $f : G \to \mathbb{C}$ et tout caractère γ comme $\hat{f}(\gamma) = \int f\gamma \, d\mu_G$ où μ_G est une mesure de Haar[‡]. On reconnaît d'ailleurs la transformée de Fourier dans $\mathbb{Z}_N$ et celle dans $\mathbb{R}$. On définira dans le même esprit l'ensemble de Bohr $B(S,\delta) = \{x \in G \mid |\arg(\gamma(x))| \leq \delta\pi\}$.

Ainsi, tout ce que nous avons dit dans la section 3 se généralise dans les groupes abéliens finis. La proposition de Ruzsa sur les progressions arithmétiques dans les ensembles de Bohr (proposition 4.8) se généralise elle aussi, mais à condition d'élargir encore une fois la classe des progressions arithmétiques généralisée. En fait, un ensemble de Bohr contient un grand ensemble de la forme $H+P$, où H est un sous-groupe fini et P est une progression arithmétique généralisée propre, telle que H soit P-libre. Dans la suite, on appelle un tel ensemble une progression *de classes* propre.

Quant au premier problème, Green et Ruzsa ont trouvé un substitut de la proposition 2.2. Tout ensemble fini A admet un k–modèle fini de taille raisonnablement grande.

Donc, rassemblant tous ces ingrédients, on obtient le théorème de Freiman-Ruzsa pour les groupes abéliens arbitraires, avec une borne uniforme pour ces groupes (et un recouvrement au moyen de progressions de classes). On renvoie les lecteurs intéressés à [7].

---

†. On appelle ces morphismes les caractères de G. Ce sont en fait les caractères irréductibles de la théorie des représentations des groupes finis.

‡. C'est-à-dire, une mesure invariante par action de la loi du groupe, par exemple la mesure de probabilité uniforme.

Progrès récents : les travaux de T. Sanders

Il y a eu très récemment un progrès dû à Sanders [12], qui a utilisé une méthode probabiliste introduite par Croot et Sisask (dans [2]). Le résultat principal de Sanders, dans l'esprit des résultats de Bogolyubov-Ruzsa déjà cités, est le suivant.

Théorème 6.3 (Sanders). *Soit G un groupe abélien. Soient $A, S \subseteq G$ des ensembles finis non-vides tels que $|A+S| \leq C\min\{|A|,|S|\}$. Alors $A-A+S-S$ contient une progression de classes de dimension*† *$d(C)$ et de taille $\exp(-h(C))|A+S|$, où $d(C) = \mathcal{O}(\log^6 C)$ et $h(C) = \mathcal{O}(\log^6 C \log\log C)$.*

Pour en déduire le théorème de Freiman, on prend $S = A$, puis on applique derechef le lemme de recouvrement de Chang (5.2). Cela donne :

Théorème 6.4 (Théorème de Freiman-Ruzsa). *Soit G un groupe abélien. Soit $A \subseteq G$ un ensemble fini non-vide tel que $|A+A| \leq C|A|$. Alors A est contenu dans une progression de classes de dimension $d(C)$ et de taille $\exp(h(C))|A|$ où $d(C), h(C) = \mathcal{O}(C\log^6 C \log\log C)$.*

Rappelons qu'une progression de classes dans $\mathbb{Z}$ est simplement une progression arithmétique généralisée, puisque le seul sous-groupe fini de $\mathbb{Z}$ est $\{0\}$. Les bornes obtenues grâce à ce théorème sont donc meilleures que celles du théorème 0.2.

Partant de la progression $P \subseteq 2A-2A$ obtenue par le théorème 6.3, on peut aussi appliquer le lemme de recouvrement de Ruzsa (5.1) à la progression de classes P contractée‡ d'un facteur $\frac{1}{2}$. On obtient ainsi une autre version du théorème de Freiman-Ruzsa§ :

Théorème 6.5 (Théorème de Freiman-Ruzsa, autre version). *Soit G un groupe abélien. Soit $A \subseteq G$ un ensemble fini non-vide tel que $|A+A| \leq C|A|$. Alors A peut être recouvert par $k(C)$ translatés d'une progression de classes de dimension $d(C)$ et de taille au plus $f(C)|A|$ où $k(C) = \exp(\mathcal{O}(\log^6 C \log\log C))$, $d(C) = \mathcal{O}(\log^6 C)$ et $f(C) = C^4$.*

Dans cette version du théorème de Freiman-Ruzsa, au lieu de recouvrir A par une seule progression, on s'autorise le recours à une réunion de translatés d'une progression. Ce qui est remarquable est qu'on peut alors choisir une progression de taille polynomiale. Beaucoup de mathématiciens pensent que cette version est la « bonne » formulation du théorème de Freiman-Ruzsa, et que la borne $k(C)$ peut être choisie polynomiale elle aussi. Mais cela reste un problème ouvert.

6.2 Cas des groupes non abéliens

Dans un cadre plus général, celui de groupes non abéliens, certains résultats restent valables (comme l'inégalité triangulaire de Ruzsa 1.2), mais d'autres s'écroulent, et c'est le cas de la pierre d'angle de notre preuve que sont les inégalités de Plünnecke-Ruzsa (1.1).

†. Il s'agit toujours de la dimension de la composante « progression ».

‡. À proprement parler, on contracte la composante « progression » de P.

§. On pouvait, bien sûr, faire la même chose avec notre version du lemme de Bogolyubov-Ruzsa, mais les bornes ne sont pas intéressantes.

Revenons sur la preuve que nous en avons donnée : on a utilisé de manière essentielle l'hypothèse de commutativité sur G, notamment dans l'argument $(\star)$. En fait, en le formulant légèrement différemment, le lemme de Petridis (1.3) reste vrai (voir [9]), mais c'est alors dans la preuve des inégalités de Plünnecke que la commutativité devient cruciale. Bref, dans tous les cas, on utilise le caractère abélien de G.

Donnons un contre-exemple très concret dans le cas non abélien, inspiré par [8].

Soit $p > 2$ un nombre premier à ajuster. Considérons $G = \mathfrak{S}_p$ (dont on notera la loi multiplicativement), et posons H le sous-groupe engendré par la permutation circulaire $\sigma := \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix}$. H contient p éléments (c'est l'ordre de σ). De plus, on note τ la transposition $(1\ \ 2)$, et $B := H \cup \{\tau\}$. B contient $p+1$ éléments.

- Majorons $|BB| = |HH \cup H\tau \cup \tau H| \leq |H| + |H| + |H| < 3|B|$, car si H est un sous-groupe de G, $HH = H$.
- En revanche, BBB s'avère de taille beaucoup plus imposante puisqu'il contient $H\tau H$.

Lemme 6.6. $|H\tau H| = |H|^2$.

Ainsi, minorons

$$|BBB| \geq |H\tau H| = |H|^2 \geq (|B| - 2)|B| = (p-1)|B|.$$

Si l'on choisit $p > 3^3+1$, cette minoration est contraire à l'inégalité de Plünnecke-Rusza. Prouvons le lemme :

Preuve du lemme. On montre que l'application

$$\begin{cases} H \times H \to H\tau H \\ (\sigma^k, \sigma^l) \mapsto \sigma^k \tau \sigma^l \end{cases}$$

est une injection. Comme elle est aussi surjective par définition de $H\tau H$, cela prouvera l'égalité des cardinaux, qui est le résultat. Prouver l'injectivité revient à prouver que la seule solution de $\tau\sigma^k\tau = \sigma^l$ est $k = l = 0 \bmod p$.

Examinons les puissances de σ. Ce sont encore des p–cycles. Si $k \in \mathbb{Z} \setminus p\mathbb{Z}$, on peut écrire

$$\sigma^k = \begin{pmatrix} 1 & \overline{1+k} & \overline{1+2k} & \cdots & \overline{1+(p-1)k} \end{pmatrix},$$

où $\overline{x}$ désigne le reste de la division euclidienne de x par p. Soit $j \in \{1, \ldots, p-1\}$ tel que $2 = \overline{1+jk}$ (on a alors $2 \equiv_p 1+jk$, et $jk \equiv_p 1$). Ensuite, comme conjuguer par τ revient à intervertir 1 et 2,

$$\tau\sigma^k\tau = \tau\sigma^k\tau^{-1} = \begin{pmatrix} 2 & \overline{1+k} & \overline{1+2k} & \cdots & 1 & \cdots & \overline{1+(p-1)k} \end{pmatrix},$$

avec 1 en $(j+1)^{\text{e}}$ place. Supposons que $\tau\sigma^k\tau = \sigma^l$. Alors, en considérant respectivement les images de 2 et de 1, on a les égalités suivantes modulo p :

$$\begin{aligned} 2 + l &\equiv_p 1 + k, \\ 1 + l &\equiv_p 1 + (j+1)k. \end{aligned}$$

ce qui prouve (en soustrayant) que $jk \equiv_p -1$, et donc que $1 \equiv_p -1$, ce qui est absurde.

En définitive, si $\tau\sigma^k\tau = \sigma^l$ pour des $k, l \in \mathbb{Z}$, alors $k \in p\mathbb{Z}$. Mais dans ce cas, $\sigma^l = \mathrm{id}$, c'est-à-dire que $l \in p\mathbb{Z}$. □

Références

[1] Mei-Chu Chang. A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113(3) :399–419, 2002.

[2] Ernie Croot and Olof Sisask. A probabilistic technique for finding almost-periods of convolutions. *Geom. Funct. Anal.*, 20(6) :1367–1396, 2010.

[3] G. A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translated from the Russian, Translations of Mathematical Monographs, Vol 37.

[4] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3) :465–588, 2001.

[5] Ben Green. Structure theory of set addition. 2002. unpublished lecture notes.

[6] Ben Green. Spectral structure of sets of integers. In *Fourier analysis and convexity*, Appl. Numer. Harmon. Anal., pages 83–96. Birkhäuser Boston, Boston, MA, 2004.

[7] Ben Green and Imre Z. Ruzsa. Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc. (2)*, 75(1) :163–175, 2007.

[8] H. A. Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)*, 167(2) :601–623, 2008.

[9] G. Petridis. New Proofs of Plünnecke-type Estimates for Product Sets in Non-Abelian Groups. *ArXiv e-prints*, January 2011.

[10] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.*, 65(4) :379–388, 1994.

[11] Imre Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, (258) :xv, 323–326, 1999. Structure theory of set addition.

[12] T. Sanders. On the Bogolyubov-Ruzsa lemma. *ArXiv e-prints*, October 2010.

[13] Tomasz Schoen. Near optimal bounds in freiman's theorem. *Duke Math. J.*, 158(1) :1–12, 2011.

[14] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.