Chapitre 1

Sur les bases additives dans les groupes abéliens

Ce chapitre reprend, à peu de choses près et en français, le texte d'un article écrit en collaboration avec Thái Hoàng Lê et Alain Plagne.

1.1 Introduction

Dans toute la suite, $(G,+)$ est un semi-groupe commutatif. De plus, on rappelle que si A est un sous-ensemble de G et h un entier, hA est l'ensemble formé des sommes de h éléments de A (non nécessairement distincts). Pour deux sous-ensembles A et B de G, on note $A \sim B$ si leur différence symétrique est finie.

On va s'intéresser à la notion de *base additive*. Bien qu'on en ait déjà parlé dans l'introduction générale du manuscrit, nous avons besoin ici de définir différents types de bases additives.

Définition 1.1. On dit que l'ensemble $A \subset G$ est
- *une base (asymptotique) faible* d'ordre au plus h si $A \cup \cdots \cup hA \sim G$.
- *une base faible parfaite* d'ordre au plus h si $A \cup \cdots \cup hA = G$.
- *une base (asymptotique)* d'ordre au plus h si $hA \sim G$.
- *une base parfaite* d'ordre au plus h si $hA = G$.

Si h est le plus petit entier tel que $hA \sim G$, on dit que A est une base d'ordre h et on note $\mathrm{ord}^*_G(A) = h$. Si un tel h n'existe pas, on pose $\mathrm{ord}^*_G(A) = \infty$. On définit évidemment l'ordre de la même façon pour les autres notions, et pour une base faible d'ordre h, on note $\mathrm{ord}_G(A) = h$.

On peut facilement relier ces notions grâce à la remarque suivante. Dans le cas où G contient 0, A est une base faible si et seulement si $A \cup \{0\}$ est une base, et on a $\mathrm{ord}_G(A) = \mathrm{ord}^*_G(A \cup \{0\})$. Bien entendu, les bases (faibles ou non) ne présentent

un intérêt que lorsque G est infini. En revanche, les bases parfaites (faibles ou non) ont un sens dans un cadre fini également.

Historiquement, les bases additives n'ont été étudiées que dans les cas $G = \mathbb{N}$ et $G = \mathbb{Z}$ (cf. [11] pour les entiers relatifs). En particulier, la question de savoir comment se comportait une base lorsqu'on lui enlevait un élément a donné lieu à de nombreux résultats, sur les fonctions E, X et S que nous introduirons dans les trois sous-sections qui suivent. Nous y donnerons certains résultats connus dans $\mathbb{N}$, et expliquerons comment ces fonctions se comportent dans un groupe G infini. Pour un panorama plus exhaustif de ce thème de recherche, dans le cas des entiers naturels, on conseille la lecture de [13] ou [5].

Mais avant de chercher des propriétés sur les bases additives dans un groupe quelconque, il est naturel de se poser la question d'existence de bases d'ordre h, pour $h \geq 1$. Le cas $h = 1$ est trivial. En effet, il suffit de considérer G tout entier ou G privé d'un nombre fini d'éléments selon ce qu'on veut obtenir. Dans le Théorème 1.1 ci-dessous, on montre un résultat plus fort que la simple existence d'une base d'ordre h. Il existe en fait une *base minimale* A d'ordre h, c'est-à-dire que pour tout $a \in A$, $A \setminus \{a\}$ n'est plus une base d'ordre h (cela peut être une base d'ordre plus élevé). Dit autrement, chaque élément de A est nécessaire à ce que A soit une base d'ordre h.

Théorème 1.1. *soient G un groupe abélien infini et h un entier, $h \geq 2$. Alors G admet une base parfaite minimale d'ordre h.*

La démonstration de ce théorème sera l'objet de la section 1.3.

1.1.1 Élements exceptionnels

La première question qu'on se pose est de savoir si lorsqu'on enlève un élément a de A une base additive, $A \setminus \{a\}$ est toujours une base. Considérons un premier exemple simple pour se familiariser avec ces problèmes. On considère dans $\mathbb{N}$ la base additive suivante, d'ordre 2 (celle-ci est d'ailleurs parfaite) :

$$A = \{1\} \cup 2\mathbb{N}.$$

$A \setminus \{1\}$ n'est plus une base, puisque cet ensemble n'engendre plus que les nombres pairs. Si on enlève un autre élément a, $A \setminus \{a\}$ reste une base ; elle n'est plus parfaite d'ordre 2, mais ce n'est pas ce qui nous intéresse ici.

Définition 1.2. Soit $a \in A$, où A est une base de G. On dit que a est un élément *exceptionnel* si $A \setminus \{a\}$ n'est plus une base de G. Dans le cas contraire, a est un élément *régulier*. On note A^* l'ensemble des éléments réguliers de A.

Dans l'exemple précédent, A admet un seul élément exceptionnel. Grekos [6] a montré que le nombre d'éléments exceptionnels de A peut être majoré par $h-1$, ce qui donne un sens à la définition suivante.

$$E(h) = \max_{hA\sim\mathbb{N}} |A \setminus A^*|. \tag{1.1}$$

Plagne, dans [15], a obtenu l'équivalent suivant, lorsque $h \to \infty$:

$$E(h) \sim 2\sqrt{\frac{h}{\log h}}. \tag{1.2}$$

Pour un groupe G quelconque, il n'est a priori pas clair que la fonction E_G est bien définie, c'est-à-dire que le nombre d'éléments exceptionnels peut être majoré en fonction de h seulement. Le théorème suivant répond affirmativement à ce problème, et montre de plus que la borne obtenue est la meilleure possible.

Théorème 1.2. *(i) Pour tout G groupe abélien infini et pour tout $h \geq 1$,*

$$E_G(h) \leq h-1,$$

(ii) il existe un groupe G infini qui vérifie $E_G(h) = h-1$ pour tout $h \geq 1$,

(iii) pour tout $h \geq 1$, il existe un groupe G infini (qui dépend de h) pour lequel $E_G(h) = 0$.

Remarque. En fait, $E_G(1) = 0$ pour tout G, donc seul le cas $h \geq 2$ nous intéressera réellement dans les preuves.

Comme on va le voir plus tard, les points (ii) et (iii) viendront de l'étude du cas $G = \mathbb{F}_p[t]$ l'anneau des polynômes sur le corps $\mathbb{F}_p$, pour lequel on a

$$E_{\mathbb{F}_p[t]}(h) = \left[\frac{h-1}{p-1}\right].$$

Le Théorème 1.2 sera démontré dans la section 1.4.

1.1.2 La fonction d'Erdős et Graham

On se demande maintenant, lorsque a est un élément régulier de A base d'ordre h, comment se comporte l'ordre de $A \setminus \{a\}$. Erdős et Graham [3] ont étudié cette question dans $\mathbb{N}$ et montré qu'on peut majorer l'ordre de $A \setminus \{a\}$ en fonction de h seulement, ce qui donne un sens à la fonction

$$X(h) = \max_{hA\sim\mathbb{N}} \max_{a\in A^*} \mathrm{ord}^*(A \setminus \{a\}). \tag{1.3}$$

À l'heure actuelle, les meilleures minoration et majoration de $X(h)$ sont dues à Plagne [14], qui a amélioré celles obtenues par Stöhr [16], Grekos [6] et Nash [12] notamment. On a

$$\left\lceil \frac{h(h+4)}{3} \right\rceil \leq X(h) \leq \frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil. \tag{1.4}$$

Erdős et Graham [4] ont conjecturé qu'il existe une constante α telle que $X(h) \sim \alpha h^2$ quand $h \to \infty$, mais ce problème est toujours ouvert. Les inégalités (1.4) conduisent à $X(1) = 1, X(2) = 4, X(3) = 7$, mais la valeur de $X(4)$ reste inconnue.

On s'intéresse ici à ce problème dans le cas d'un groupe G quelconque, et on définit de même

$$X_G(h) = \max_{hA \sim G} \max_{a \in A^*} \mathrm{ord}_G^*(A \setminus \{a\}). \tag{1.5}$$

Dans [3], Erdős et Graham utilisent une version différente de la fonction X, à savoir

$$\begin{aligned} x_G(h) &= \max\{\mathrm{ord}_G^*(A) : \cup_{i=1}^h iA \sim G \text{ et } \mathrm{ord}_G^*(A) < \infty\} \\ &= \max\{\mathrm{ord}_G^*(A) : \cup_{i=1}^h iA \sim G \text{ et } \langle A - A \rangle = G\} \end{aligned} \tag{1.6}$$

avec $G = \mathbb{N}$ dans leur cas, et où $\langle B \rangle$ désigne le sous-groupe engendré par un ensemble B dans G. Dans la mesure où il nous sera préférable de travailler avec l'une ou l'autre de ces deux fonctions selon les cas, voyons dès à présent pourquoi elles sont égales (lorsqu'elles sont bien définies).

Lemme 1.1. *Pour tout groupe infini G, $X_G = x_G$.*

Démonstration. Soient $h \geq 1$ et A une base d'ordre au plus h de G. Soit $a \in A$ un élément régulier de A, alors $B := A - a$ est également une base d'ordre au plus h et contient 0. Ainsi, $B \setminus \{0\}$ est une base faible. De plus,

$$\mathrm{ord}_G^*(B \setminus \{0\}) = \mathrm{ord}_G^*(A \setminus \{a\}),$$

ce qui implique $X_G(h) \leq x_G(h)$.

Pour l'autre sens, d'après les définitions de X_G et x_G, on a clairement $h \leq X_G(h)$ et $h \leq x_G(h)$. Si $x_G(h) = h$, alors

$$X_G(h) = h = x_G(h),$$

puisque $X_G(h) \leq x_G(h)$. Ainsi, on peut supposer $x_G(h) > h$ (remarquons que c'est en fait toujours le cas, dès que $h \geq 2$ d'après le Théorème 1.1). Soit B une base faible d'ordre au plus h de G satisfaisant

$$h < \mathrm{ord}_G^*(B) < \infty.$$

Alors $0 \notin B$ (sinon, $\mathrm{ord}^*_G(B) = \mathrm{ord}_G(B) \leq h$). Posons $A = B \cup \{0\}$. A est donc une base d'ordre au plus h et 0 est un élément régulier de A car $A \setminus \{0\} = B$. En outre,

$$\mathrm{ord}^*_G(A \setminus \{0\}) = \mathrm{ord}^*_G(B),$$

ce qui donne bien $x_G(h) \leq X_G(h)$. □

L'étude de X_G est nettement moins concluante que celle de E_G. En effet, on ne sait même pas si $X_G(h)$ est fini pour tout G. Cependant, nous sommes capables de répondre à ce problème et donner des bornes pour $X_G(h)$ pour une large catégorie de groupes.

Avant d'énoncer nos résultats, nous avons besoin de rappeler la définition de la fonction arithmétique Ω :

$$\Omega(n) = \alpha_1 + \cdots + \alpha_k, \tag{1.7}$$

si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la factorisation en produit de nombres premiers distincts de n.

Rappelons de plus que nous désignons par $m \cdot A$ le sous-ensemble de G

$$m \cdot A = \{ma : a \in A\}.$$

En adaptant l'idée d'Erdős et Graham, on obtient le théorème suivant.

Théorème 1.3. *Soit G un groupe abélien infini tel que pour tout entier $1 \leq m \leq h$, le quotient $G/m \cdot G$ est fini, alors*

$$X_G(h) \leq h^2 + h \cdot \max_{1 \leq m \leq h} \Omega\left(|G/m \cdot G|\right) + h - 1. \tag{1.8}$$

Parmi les groupes qui satisfont l'hypothèse du Théorème 1.3, on retrouve notamment les groupes abéliens de type fini, les groupes divisibles (i.e les groupes G tels que $m \cdot G = G$ pour tout $m \in \mathbb{Z}^+$, ce qui inclut $\mathbb{R}$ et $\mathbb{Q}$) et $\mathbb{Z}_p$ (les entiers p-adiques).

Pour ce qui est de la minoration, on démontre que l'inégalité (1.4) se généralise aux groupes admettant $\mathbb{Z}$ comme quotient.

Théorème 1.4. *Soit G un groupe abélien infini. Supposons qu'il existe un sous-groupe H de G tel que $G/H \cong \mathbb{Z}$ (isomorphisme algébrique), alors pour tout entier $h \geq 1$, on a*

$$X_G(h) \geq \left\lceil \frac{h(h+4)}{3} \right\rceil.$$

Cela pourrait laisser penser que $X_G(h)$ a une croissance quadratique. Nous montrons que ce n'est en fait pas le cas, en exhibant une classe de groupes pour lesquels $X_G(h)$ a une croissance linéaire.

Théorème 1.5. *Soient p un nombre premier et G un groupe abélien infini qui a la propriété que tout élément non nul de G est d'ordre p.*

(i) Pour tout entier $h \geq p$, on a

$$X_G(h) \leq ph + p - 1.$$

(ii) Pour tout entier $h \geq 3(p-1)/2$, on a

$$X_G(h) \geq 2h - 3p + 3.$$

En particulier, si $p = 2$, $X_G(h) \sim 2h$ quand $h \to \infty$.

Bien que nous ne soyons pas capables de dire en général si $X_G(h)$ est fini, on peut le confirmer et même en donner un encadrement lorsque $h = 2$ ou $h = 3$.

Théorème 1.6. *Pour tout groupe abélien infini G, on a*

(i) $3 \leq X_G(2) \leq 5$.

(ii) $4 \leq X_G(3) \leq 17$.

La section 1.5 sera consacrée aux démonstrations de ces différents résultats.

1.1.3 La fonction de Grekos

Dans les exemples de constructions de bases donnant de bonnes minorations pour $X(h)$, on s'aperçoit que bien souvent, seul un nombre fini d'éléments a de A^* vérifient $\mathrm{ord}^*(A \setminus \{a\}) = X(h)$. C'est l'origine de l'introduction de la fonction S définie par la formule suivante

$$S(h) = \max_{hA \sim \mathbb{N}} \limsup_{a \in A^*} \mathrm{ord}^*(A \setminus \{a\}).$$

Cette fonction, due à Grekos, désigne, en d'autres mots, la valeur minimale de s telle que pour tout A satisfaisant $hA \sim \mathbb{N}$, il n'y a qu'un nombre fini d'éléments $a \in A$ vérifiant

$$\mathrm{ord}^*(A \setminus \{a\}) > s.$$

Il a été conjecturé par Grekos que l'ordre de grandeur de S est plus petit que celui de X, ce qui a été confirmé par Cassaigne et Plagne [3] qui ont prouvé que

$$h + 1 \leq S(h) \leq 2h \tag{1.9}$$

pour tout $h \geq 2$ (évidemment, $S(1) = 1$). On sait aussi que $S(2) = 3$, mais la valeur de $S(3)$ reste inconnue. Déterminer s'il existe une constante β telle que $S(h) \sim \beta h$ quand $h \to \infty$ est un problème ouvert qui paraît extrêmement difficile.

De manière analogue, on définit $S_G(h)$ dans un groupe abélien G infini comme étant la valeur minimale de s telle que pour tout A satisfaisant $hA \sim G$, le nombre de $a \in A$ vérifiant

$$\mathrm{ord}^*(A \setminus \{a\}) > s$$

est fini. À nouveau, il n'est a priori pas clair que S_G est bien définie. Déjà, d'après la définition, on a

$$S_G(h) \leq X_G(h).$$

On montre dans le théorème suivant non seulement que $S_G(h)$ est bien défini pour tout groupe abélien infini, et pour tout $h \geq 1$, mais aussi que les bornes dans (1.9) restent valables. On généralise en fait les arguments de [2]. Nous avons cependant besoin de la notion de *moyennabilité* sur les groupes, ce qui rend la preuve non élémentaire.

Théorème 1.7. *Pour tout groupe abélien infini G, on a $h + 1 \leq S_G(h) \leq 2h$.*

Au contraire du Théorème 1.2, on ne sait pas si ces bornes sont les meilleures possibles. Cependant, on peut démontrer que dans le cas $h = 2$, la borne inférieure est la bonne.

Théorème 1.8. *Pour tout groupe abélien infini G, on a $S_G(2) = 3$.*

Remarque. Le théorème précédent veut exactement dire que si on considère une base A d'ordre 2 de G, il y a un nombre fini d'éléments a qui vérifient $\mathrm{ord}^*_G(A \setminus \{a\}) > 3$. En fait, à travers la preuve, on verra qu'il ne peut exister qu'*un seul* tel élément a.

Nous introduirons la notion de *moyennabilité* et prouverons ces deux résultats dans la section 1.6.

Avant de passer aux preuves des résultats énoncés dans cette introduction, nous allons démontrer quelques résultats préliminaires.

1.2 Résultats préliminaires

1.2.1 Quelques observations

On commence par donner quelques lemmes, dont certains s'apparentent parfois à des remarques tellement ils sont immédiats. On les donnera d'ailleurs quelquefois sans preuve.

Lemme 1.2. *Soient G un groupe abélien infini et $A \subset G$. Si A est une base (respectivement une base parfaite) de G et $b \in G$, alors $A - b = \{a - b : a \in A\}$ est une base (respectivement une base parfaite) de même ordre.*

Démonstration. Cela découle immédiatement du fait que pour tout entier h, $h(A-b) = hA - hb$. □

On a en fait déjà utilisé ce résultat dans la preuve du Lemme 1.1.

Si H est un sous-groupe de G, pour tout $x \in G$, on note $\overline{x}$ la classe de x dans G/H. Les trois prochains lemmes vont nous permettre d'introduire les systèmes de représentants associés à un quotient G/H, utiles à la construction de bases pour G.

Lemme 1.3. *soient G un groupe abélien et H un sous-groupe de G. Considérons $\Lambda \subset G$ un système de représentants de G/H dans G, c'est-à-dire, pour tout $x \in G$, il y a exactement un élément $\lambda \in \Lambda$ tel que $x+H = \lambda+H$. Alors, pour tout $x \in G$, il y a une unique façon d'écrire*

$$x = \lambda + g$$

avec $\lambda \in \Lambda, g \in H$. En particulier, si $H \neq G$ et $H \neq \{0\}$ alors $\Lambda \cup H$ est une base parfaite d'ordre 2 de G.

Nous aurons besoin d'un système de représentants particulier que nous introduisons maintenant.

Lemme 1.4. *Soient G un groupe abélien et H un sous-groupe de G. Alors, il existe un système de représentants Λ de G/H dans G tel que $0 \in \Lambda$ et $\Lambda = -\Lambda$.*

Démonstration. On choisit un représentant dans chaque classe de G suivant H. Bien entendu, on commence par choisir 0 comme représentant de la classe H. Ensuite, si λ est le représentant d'une classe B, alors on choisit $-\lambda$ comme représentant de la classe $-B$. □

On observe ensuite que les bases parfaites d'un quotient peuvent facilement s'étendre au groupe tout entier, ce qui n'est pas le cas pour les bases non parfaites.

Lemme 1.5. *Soient G un groupe abélien infini et H un sous-groupe de G. Soient également $A \subset G/H$,*

$$B = \{x \in G : \overline{x} \in A\}$$

et h un entier supérieur ou égal à 1. On a alors :

(i) $hA = G/H$ si et seulement si $hB = G$,

(ii) $\bigcup_{i=1}^{h} iA = G/H$ si et seulement si $\bigcup_{i=1}^{h} iB = G$.

Le lemme suivant précise que toute base est parfaite, quitte à augmenter l'ordre de 1.

Lemme 1.6. *Soient G un groupe abélien infini et $A \subset G$.*

(i) Si $hA \sim G$, *alors* $(h+1)A = G$,

(ii) Si $\bigcup_{i=1}^{h} iA \sim G$, *alors* $\bigcup_{i=2}^{h+1} iA = G$.

Démonstration. Supposons $hA \sim G$, et soit x un élément quelconque de G. Comme $x - A$ est infini, il a nécessairement une intersection non vide avec hA. Ainsi, $x \in (h+1)A$.

Supposons à présent $\bigcup_{i=1}^{h} iA \sim G$, et soit x quelconque dans G. Comme $x - A$ est infini, il a nécessairement une intersection non vide avec rA pour $1 \leq r \leq h$. Ainsi,

$$x \in (r+1)A \subset \bigcup_{i=2}^{h+1} iA.$$

□

Pour établir des bornes de X_G, on aura besoin du résultat suivant, qui dit que si deux sous-ensembles de la forme nA ont une intersection non vide, alors on peut trouver une suite arbitrairement longue de sous-ensembles de A dont l'intersection est non vide.

Lemme 1.7. *Soient* $A \subset G$ *et* m, n *des entiers naturels non nuls. Si*

$$c \in nA \cap (n+m)A$$

alors pour tout entier naturel k, *on a*

$$kc \in knA \cap (kn+m)A \cap \cdots \cap (kn+km)A.$$

1.2.2 Caractérisation des bases à la façon d'Erdős et Graham

Dans [3], Erdős et Graham ont prouvé qu'une base faible A de $\mathbb{N}$ est une base si et seulement si

$$\text{pgcd}(A - A) = 1 \tag{1.10}$$

où $A - A = \{a_1 - a_2 : a_1, a_2 \in A\}$. Cela donne immédiatement un critère de régularité pour un élément d'une base de $\mathbb{N}$. En effet, si A est une base de $\mathbb{N}$, alors $a \in A$ est régulier si et seulement si

$$\text{pgcd}(A \setminus \{a\} - A \setminus \{a\}) = 1. \tag{1.11}$$

Nous allons à présent généraliser ces caractérisations dans le cas d'un groupe arbitraire. Ce n'est plus le pgcd$(A - A)$ qui intervient désormais (cela n'a pas de sens dans G quelconque), mais $\langle A - A \rangle$, le sous-groupe engendré par $A - A$ dans G.

Lemme 1.8. *Soient G un groupe abélien infini et A une base faible de G. Alors A est une base si et seulement si $\langle A - A\rangle = G$.*

Démonstration. Supposons que A soit une base faible d'ordre au plus h, c'est-à-dire,

$$G \sim \bigcup_{i=1}^{h} iA.$$

Posons $H = \langle A - A\rangle$. L'image de a dans G/H est la même pour tout $a \in A$. Ainsi, pour tout s, l'image de sA dans G/H est un singleton. Cela signifie que A ne peut être une base que si $G = H$.

Réciproquement, supposons $G = H$. On commence par montrer qu'il existe n tel que

$$nA \cap (n+1)A \neq \emptyset.$$

En effet, soit a un élément de A, on peut d'après l'hypothèse écrire a comme une combinaison linéaire d'éléments de $A - A$

$$a = \sum_{k=1}^{t} \alpha_k (a_k - b_k)$$

avec $a_k, b_k \in A$ et $\alpha_k \in \mathbb{N}^*$ pour tout k.

Ainsi, l'élément

$$c = a + \sum_{k=1}^{t} \alpha_k b_k = \sum_{k=1}^{t} \alpha_k a_k$$

est à la fois dans nA et $(n+1)A$, en posant $n = \sum_{k=1}^{t} \alpha_k$. D'après le Lemme 1.7,

$$(h-1)c \in \bigcap_{i=0}^{h-1} ((h-1)n + i)A.$$

Or, pour tout $x \in G$, sauf un nombre fini, on a

$$x - (h-1)c \in \bigcup_{i=1}^{h} iA.$$

Il vient alors que pour tout $x \in G$, sauf un nombre fini,

$$x = x - (h-1)c + (h-1)c \in ((h-1)n + h)A.$$

Ainsi, A est une base d'ordre au plus $(h-1)n + h$. □

On en vient maintenant à la condition de régularité d'un élément a.

Lemme 1.9. *Soient G un groupe abélien infini et A une base de G. Alors $a \in A$ est régulier si et seulement si $\langle A \setminus \{a\} - A \setminus \{a\} \rangle = G$.*

Démonstration. On aimerait appliquer le Lemme 1.8, mais on ne sait pas si $A \setminus \{a\}$ est une base faible. Cependant, remarquons que $B := A - a$ est également une base (Lemme 1.2), qui de plus contient 0. Ainsi, $B \setminus \{0\}$ est une base faible. D'où

$$\begin{aligned} A \setminus \{a\} \text{ est une base} &\iff B \setminus \{0\} \text{ est une base} \\ &\iff \langle B \setminus \{0\} - B \setminus \{0\} \rangle = G \\ &\iff \langle A \setminus \{a\} - A \setminus \{a\} \rangle = G. \end{aligned}$$

□

1.3 Existence de bases additives

Dans le cas de $\mathbb{N}$, il est connu depuis Härtter [9] que $\mathbb{N}$ admet des bases minimales de tout ordre (sa preuve n'est pas constructive). Un exemple concret de base minimale d'ordre h de $\mathbb{N}$ est donné par

$$A = \left\{ \sum_{f \in \mathcal{F}} 2^f : \mathcal{F} \text{ est un ensemble fini de } \mathbb{N} \text{ inclus dans une classe modulo } h \right\}.$$

On pourra lire [10] pour trouver des propriétés supplémentaires de cette base.

Montrons d'abord que dès qu'il existe une représentation spéciale des éléments de G similaire à celle de $\mathbb{N}$ que l'on vient juste de donner, il existe des bases minimales parfaites de tout ordre.

Proposition 1.1. *Soit G un groupe abélien infini. Supposons qu'il existe une suite infinie de sous-ensembles $(\Lambda_i)_{i=0}^{\infty}$ de G satisfaisant les propriétés suivantes :*

(i) $0 \in \Lambda_i$, *pour tout* $i \in \mathbb{N}$,

(ii) $-\Lambda_i = \Lambda_i$, *pour tout* $i \in \mathbb{N}$,

(iii) Tout élément $x \in G$ admet une unique *représentation de la forme*

$$x = \lambda_0(x) + \lambda_1(x) + \cdots$$

où $\lambda_i(x) \in \Lambda_i$ pour tout i, et $\lambda_i(x) \neq 0$ pour un nombre fini d'indices i. En d'autres termes, G est égal à la "somme directe" $\oplus_{i=0}^{\infty} \Lambda_i$. [1]

Alors, pour tout entier $h \geq 2$, G admet une base parfaite minimale d'ordre h.

1. On ne peut en fait pas parler de somme directe ici, les Λ_i étant seulement des ensembles, pas des groupes.

Démonstration. Pour $x \in G$, l'ensemble $\{i \in \mathbb{N} : \lambda_i(x) \neq 0\}$ est appelé le *support* de x.

Clairement, si x et y ont des supports disjoints,

$$\lambda_i(x+y) = \lambda_i(x) + \lambda_i(y).$$

Considérons $\mathbb{N} = N_1 \cup \cdots \cup N_h$ une partition de $\mathbb{N}$ en h ensembles infinis (disjoints). Notons A_j l'ensemble des $x \in G$ à support dans N_j, et posons finalement

$$A = \cup_{j=1}^{h} A_j.$$

Par définition, $0 \in A$. De plus, tout élément $x \in G$ peut s'écrire de manière *unique* comme

$$x = a_1 + \cdots + a_h \tag{1.12}$$

avec $a_j \in A_j$ pour tout $j = 1, \ldots, h$. Lorsque $a_1, \ldots, a_h \neq 0$, x ne peut être écrit comme une somme de moins de h éléments de A. Cela montre que A est une base parfaite d'ordre h. Cependant, A n'est pas minimale. On va en fait montrer que $B := A \setminus \{0\}$ est une base parfaite minimale d'ordre h.

Tout d'abord, prouvons que $hB = G$. Dans l'expression (1.12), certains (peut-être même tous) des a_j peuvent valoir 0. Étant donné $a \in A_j$, on peut l'écrire

$$a = (a + \lambda) + (-\lambda)$$

où λ est n'importe quel élément de $\Lambda_k \setminus \{0\}$ et $k \in N_j$ est un élément hors du support de a. Remarquons que d'après l'hypothèse, $-\lambda \in \Lambda_k$ également. Ainsi, tout élément de A_j, qu'il soit nul ou non, peut s'écrire comme somme de deux éléments non nuls de A_j. On peut donc faire croître le nombre d'éléments non nuls dans (1.12) jusqu'à h, ce qui montre bien $hB = G$.

Il nous reste à voir que B est minimale. Soit donc a un élément de B. Sans perte de généralité, on peut supposer que $a \in A_1 \setminus \{0\}$. Considérons un élément $x \in G$ de la forme

$$x = a + a_2 + \cdots + a_h$$

avec $a_j \in A_j \setminus \{0\}$ pour tout $j = 2, \ldots, h$. Comme les N_j forment une partition de $\mathbb{N}$, il y a bien une unique façon d'écrire x comme somme de h éléments de B, et a apparaît dans cette expression. Ainsi, x ne peut pas s'écrire comme somme de h éléments de $B \setminus \{a\}$. Comme il y a une infinité de tels x, on a $\mathrm{ord}^*(A \setminus \{a\}) \geq h+1$, et B est bien minimale. □

Venons-en à présent à la preuve du Théorème 1.1.

Preuve du Théorème 1.1. Il nous reste à construire une suite $(\Lambda_i)_{i=0}^{\infty}$ d'ensembles satisfaisant les hypothèses de la Proposition 1.1. Pour cela, on distingue deux cas.

Premier cas : G admet un élément d'ordre infini. On peut alors supposer que $\mathbb{Z} < G$. Soit alors Λ_0 un système de représentants $G/\mathbb{Z}$ dans G. Par le Lemme 1.3, tout élément $x \in G$ peut s'écrire d'une unique façon

$$x = n + \lambda_0$$

avec $\lambda_0 \in \Lambda_0$ et $n \in \mathbb{Z}$. De plus, on peut, d'après le Lemme 1.4, choisir Λ_0 tel que $0 \in \Lambda_0$ et $\Lambda_0 = -\Lambda_0$. Remarquons que tout entier relatif n s'écrit d'une *unique* manière comme

$$n = \sum_{i=0}^{k} a_i 3^i$$

où $a_i \in \{0, 1, -1\}$ pour tout i (cette représentation est connue dans la littérature sous le nom de *système ternaire balancé*). Posons $\Lambda_i = \{0, 3^{i-1}, -3^{i-1}\}$ pour $i \geq 1$. Ainsi, tout élément $x \in G$ admet une unique représentation de la forme

$$x = \lambda_0(x) + \lambda_1(x) + \cdots \tag{1.13}$$

avec $\lambda_i(x) \in \Lambda_i$ pour tout i, et $\lambda_i(x) \neq 0$ pour un nombre fini d'indices i.
Deuxième cas : Tout élément de G est d'ordre fini.

Soit $g_1 \in G$. D'après l'hypothèse, $G_1 := \langle g_1 \rangle$ est fini. On considère alors $g_2 \in G \setminus G_1$, et on pose $G_2 := \langle g_1, g_2 \rangle$. On a donc $G_1 \lneq G_2$ et G_2 est fini. On construit ainsi une chaîne infinie strictement croissante de sous-groupes de G

$$G_1 \lneq G_2 \lneq \cdots .$$

Pour tout entier $i \geq 2$, considérons $\Lambda_i \ni 0$ un système de représentants de G_i/G_{i-1} dans G_i vérifiant de plus $\Lambda_i = -\Lambda_i$. D'après le Lemme 1.3, on peut écrire tout $x \in G_i$ de manière unique, sous la forme

$$x = \lambda + g$$

avec $\lambda \in \Lambda_i$ et $g \in G_{i-1}$. Posons de plus $\Lambda_1 = G_1$. Ainsi, tout $x \in \cup_{i=1}^{\infty} G_i$ peut s'écrire d'une unique façon comme

$$x = \lambda_1(x) + \lambda_2(x) + \cdots$$

avec $\lambda_i(x) \in \Lambda_i$ pour tout $i = 1, 2, \ldots$, et seul un nombre fini de $\lambda_i(x)$ est non nul (en effet, si $x \in G_k$, alors $\lambda_i(x) = 0$ pour tout $i \geq k + 1$).

Finalement, définissons $\Lambda_0 \ni 0$ un système de représentants de $G/\cup_{i=1}^{\infty} G_i$ dans G, tel que $\Lambda_0 = -\Lambda_0$. Alors, tout x de G admet une unique décomposition de la forme

$$x = \lambda_0(x) + \lambda_1(x) + \lambda_2(x) + \cdots$$

où $\lambda_i(x) \in \Lambda_i$ pour tout $i = 0, 1, 2, \ldots$, et où il n'y a qu'un nombre fini de $\lambda_i(x)$ non nuls. Puisque $\Lambda_1 = G_1$, on a bien $\Lambda_i = -\Lambda_i$ pour tout i. Le théorème est alors démontré. □

1.4 La fonction E

Dans cette section, on s'intéresse aux nombres d'éléments exceptionnels d'une base additive dans un groupe abélien G. Rappelons simplement la définition de la fonction E_G :

$$E_G(h) = \max_{hA \sim G} |A \setminus A^*|$$

où A^* est l'ensemble des éléments réguliers de A.

Preuve du Théorème 1.2 (i). On doit donc montrer que si $hA \sim G$, alors A ne peut pas avoir plus de $h-1$ éléments exceptionnels.

D'après le Lemme 1.9, si $a \in A$ est un élément exceptionnel, alors $\langle A - A \rangle = G$ tandis que $\langle A \setminus \{a\} - A \setminus \{a\} \rangle \neq G$. S'il existe $a' \in A \setminus \{a\}$ tel que

$$a - a' \in \langle A \setminus \{a\} - A \setminus \{a\} \rangle,$$

alors pour tout $a'' \in A \setminus \{a\}$,

$$a - a'' = a - a' + a' - a'' \in \langle A \setminus \{a\} - A \setminus \{a\} \rangle,$$

et finalement

$$\langle A \setminus \{a\} - A \setminus \{a\} \rangle \supset \langle A - A \rangle = G.$$

Ainsi, $a - a'$ n'est pas dans $\langle A \setminus \{a\} - A \setminus \{a\} \rangle$ pour tout $a' \in A \setminus \{a\}$.

Supposons, par l'absurde, qu'il existe au moins h éléments exceptionnels $a_1, \ldots, a_h$ dans A. G étant infini, A l'est également. Considérons a_0 un élément de $A \setminus \{a_1, \ldots, a_h\}$. Comme $hA \sim G$, il existe $a \in A \setminus \{a_0, a_1, \ldots, a_h\}$ tel que

$$a_0 + a_1 + a_2 + \cdots + a_h - a$$

soit égal à la somme $b_1 + \cdots + b_h$ de h éléments de A. En conséquence,

$$\sum_{i=0}^{h} (a_i - a) = \sum_{i=1}^{h} (b_i - a).$$

Certains b_i peuvent être égaux à certains a_i. On est face à deux possibilités :

Premier cas : $\{a_1, a_2, \ldots, a_h\} \neq \{b_1, b_2, \ldots, b_h\}$. Cela signifie qu'une fois qu'on a enlevé de chaque côté les termes identiques, il reste du côté gauche de l'égalité au moins un a_i avec $i \neq 0$. Mais cela implique que $a_i - a \in \langle A \setminus \{a_i\} - A \setminus \{a_i\} \rangle$, ce qui fournit une contradiction.
Deuxième cas : $\{a_1, a_2, \ldots, a_h\} = \{b_1, b_2, \ldots, b_h\}$. Cela nous conduit à $a_0 = a$, à nouveau une contradiction. □

Remarque. Dans $\mathbb{N}$, le fait que toute base admet un nombre fini d'éléments exceptionnels provient immédiatement du critère d'Erdős et Graham (1.10) (cf. [13, Théorème 1]). Cependant, nous n'avons pas pu généraliser cette preuve à un groupe général, dans la mesure où elle utilisait une propriété bien spécifique à $\mathbb{Z}$, à savoir que toute suite strictement croissante de sous-groupes est finie.

Les assertions du Théorème 1.2 (ii) et (iii) sont des conséquences immédiates de la proposition suivante.

Proposition 1.2. *Soit $G = \mathbb{F}_p[t]$ l'anneau des polynômes sur le corps $\mathbb{F}_p$. Pour tout entier $h \geq 2$, on a*

$$E_G(h) = \left[\frac{h-1}{p-1}\right].$$

En particulier, si $p = 2$, $E_G(h) = h-1$ pour tout $h \geq 2$. Et si $p > h$, $E_G(h) = 0$. On ne peut donc pas obtenir une minoration universelle non triviale de E_G.

Démonstration. Commençons par montrer que

$$E_G(h) \leq \left[\frac{h-1}{p-1}\right].$$

On va avoir pour cela recours à des arguments similaires à ceux de la preuve du Théorème 1.2 (i).

Supposons que $A \subset \mathbb{F}_p[t]$ est une base d'ordre h, et que $a_1, \ldots, a_k$ sont tous les éléments exceptionnels de A. Supposons de plus, par l'absurde, que $k(p-1) \geq h$. Alors, il existe des entiers $0 \leq \alpha_1, \ldots, \alpha_k \leq p-1$ tels que

$$\alpha_1 + \cdots + \alpha_k = h.$$

Considérons a_0 un élément de $A \setminus \{a_1, \ldots, a_k\}$. Étant donné que $hA \sim G$ et que A est infini, il existe $a \in A \setminus \{a_0, a_1, \ldots, a_k\}$ tel que

$$\sum_{i=1}^{k} \alpha_i a_i + a_0 - a$$

peut s'écrire comme la somme $\sum_{j=1}^{h} b_i$ de h éléments de A. Ainsi,

$$\sum_{i=1}^{k} \alpha_i (a_i - a) + (a_0 - a) = \sum_{j=1}^{h} (b_i - a).$$

Comme $a_0 - a \neq 0$, les multi-ensembles $\{a_1(\alpha_1 \text{ fois}), \ldots, a_k(\alpha_k \text{ fois})\}$ et $\{b_1, \ldots, b_h\}$ sont distincts. Une nouvelle fois, lorsqu'on simplifie des deux côtés de l'égalité par les termes identiques, on constate qu'il existe $1 \leq i \leq k$, et $0 < \beta \leq \alpha_i$ tels que

$\beta(a_i - a)$ appartient à $\langle A \setminus \{a_i\} - A \setminus \{a_i\}\rangle$. $\mathbb{F}_p$ étant un corps, cela implique que $a_i - a$ appartient à ce sous-espace, ce qui contredit le Lemme 1.9 car a_i est exceptionnel.

Finalement, $h - 1 \geq (p-1)k$, d'où $k \leq [(h-1)/(p-1)]$.

Pour montrer qu'il y a bien égalité, on va s'intéresser à un exemple assez simple. Posons

$$k = \left[\frac{h-1}{p-1}\right].$$

En écrivant la division euclidienne de h par $p-1$, il vient $h = k(p-1) + r + 1$ où $0 \leq r < p-1$.

Définissons alors

$$A = \left\{1, t, \cdots, t^{k-1}\right\} \bigcup t^k \cdot \mathbb{F}_p \bigcup \cdots \bigcup t^{k+r-1} \cdot \mathbb{F}_p \bigcup t^{k+r} \cdot \mathbb{F}_p[t].$$

(Les ensembles $t^k \cdot \mathbb{F}_p, \ldots, t^{k+r-1} \cdot \mathbb{F}_p$ n'apparaissent pas si $r = 0$.)

Déjà, A est une base d'ordre $k(p-1) + r + 1 = h$. En effet, il est facile de voir que tout élément de $\mathbb{F}_p[t]$ peut s'écrire comme somme de $k(p-1) + r + 1$ éléments de A (remarquons que $0 \in A$). De plus, pour tout $P(t) \in \mathbb{F}[t] \setminus \{0\}$, l'élément

$$\sum_{i=0}^{k-1}(p-1)t^i + \sum_{i=k}^{k+r-1} t^i + P(t)t^{k+r}$$

ne peut pas s'exprimer comme somme d'au plus $h-1$ éléments de A.

Grâce au Lemme 1.9, on voit aisément que les éléments exceptionnels de A sont exactement

$$\left\{t^i : i = 0, \ldots, k-1\right\},$$

ce qui donne bien k éléments exceptionnels. □

1.5 La fonction X

Dans cette section, on étudie des bornes pour la fonction X_G. Rappelons qu'on pourra utiliser selon le contexte les deux définitions de la fonction, à savoir (1.5) et (1.6), qui sont équivalentes, d'après le Lemme 1.1.

1.5.1 Bornes générales

Afin de prouver le Théorème 1.3, nous aurons besoin du lemme suivant, faisant intervenir la fonction Ω définie en (1.7).

Remarque. On appelle *longueur* d'un groupe la taille $l(G)$ de sa plus longue chaîne de sous-groupes (i.e suite strictement croissante de sous-groupes). On obtient en fait ce maximum lorsque les quotients successifs G_{i+1}/G_i sont des groupes simples. Dans le cas de $\mathbb{Z}/n\mathbb{Z}$, si $n = \prod p_i^{\alpha_i}$, il est clair que $l(G) = \sum \alpha_i$. De plus, si G et G' sont de longueurs finies, $l(G \times G') = l(G) + l(G')$. Ainsi, pour un groupe abélien fini

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

de cardinal $n = \prod n_j = \prod p_i^{\beta_i}$, on a $l(G) = \sum \beta_i = \Omega(|G|)$. C'est dans ce rôle que Ω va intervenir dans la suite.

Lemme 1.10. *Soient G un groupe abélien fini qui est de plus m-torsion (c'est-à-dire, $mx = 0$ pour tout $x \in G$) et $A \subset G$ tel que $\langle A - A \rangle = G$. Alors, pour tout entier $s \geq \Omega(|G|)$, on a $smA = G$.*

Démonstration. Puisque $\langle A - A \rangle = G$, on peut choisir des éléments $a_1, a_2, \ldots$ dans A de telle façon que pour tout entier k, si $\langle A_k - A_k \rangle \neq G$, alors $\langle A_k - A_k \rangle \lneq \langle A_{k+1} - A_{k+1} \rangle$, où

$$A_k = \{a_1, \ldots, a_k\}.$$

D'après la remarque précédant l'énoncé du lemme, il existe $t \leq \Omega(|G|)$ tel que $\langle A_t - A_t \rangle = G$. Ainsi, tout élément $x \in G$ admet une représentation de la forme

$$x = \sum_{i,j=1}^{t} \alpha_{i,j}(a_i - a_j)$$

où $\alpha_{i,j} \in \mathbb{Z}$. Comme G est m-torsion, en réarrangeant les termes du membre de droite, on peut écrire

$$x = \sum_{i}^{t} \beta_i a_i$$

avec $0 \leq \beta_i < m$ pour tout $i = 1, \ldots, t$. On sait en plus que $\sum_{i=1}^{t} \beta_i$ est un multiple de m (car $\sum_{i=1}^{t} \beta_i \equiv \sum_{i,j=1}^{t} (\alpha_{i,j} - \alpha_{i,j}) \equiv 0 \pmod{m}$). Comme $0 \in mA$, on peut ajouter autant de zéros que l'on souhaite, ce qui assure que $x \in tmA \subset smA$, ce qu'on voulait obtenir. □

Preuve du Théorème 1.3. On utilise ici la définition (1.6). Soit A une base faible d'ordre au plus h de G satisfaisant $\langle A - A \rangle = G$. Posons

$$s = \max_{1 \leq m \leq h} \Omega\left(|G/m \cdot G|\right).$$

Comme $(h+1)A \subset G \sim \bigcup_{i=1}^{h} iA$, il existe un entier n tel que $1 \leq n \leq h$ et $nA \cap (h+1)A \neq \emptyset$.

Posons $m = h + 1 - n$ et considérons $c \in nA \cap (n+m)A$. D'après le Lemme 1.7, on a

$$(h-1)c \in \bigcap_{i=0}^{h-1} ((h-1)n + im)A.$$

Or, $G \setminus \left(\bigcup_{i=1}^{h} iA\right)$ est fini, d'où

$$m \cdot G \setminus \left(\bigcup_{i=1}^{h} miA\right)$$

est également fini. On en déduit alors que

$$(h-1)c + m \cdot G \setminus ((h-1)n + hm)A \tag{1.14}$$

est fini.

Par ailleurs, le groupe $G/m \cdot G$ est fini par hypothèse et clairement m-torsion. On a également $\langle \overline{A} - \overline{A} \rangle = G/m \cdot G$, où $\overline{A}$ désigne l'image de A par la projection $G \to G/m \cdot G$. D'après le Lemme 1.10, on sait que

$$sm\overline{A} = G/m \cdot G.$$

Autrement dit, il existe un système de représentants $\{x_1, \ldots, x_k\}$ de $G/m \cdot G$ dans G tel que

$$x_j \in smA \tag{1.15}$$

pour tout $j = 1, \ldots, k$.

Mais pour tout $x \in G$, il existe $1 \leq j \leq k$ tel que $x - (h-1)c - x_j \in m \cdot G$, ce qui conduit d'après (1.14) à ce que pour tout $x \in G$, sauf un nombre fini, on a

$$x - x_j \in ((h-1)n + hm)A. \tag{1.16}$$

En écrivant maintenant

$$x = x - x_j + x_j$$

et en utilisant (1.15) et (1.16), il vient

$$G \sim (sm + (h-1)n + hm)A.$$

Ainsi, A est une base d'ordre au plus

$$sm + (h-1)n + hm = sm + (h-1)(m+n) + m \leq h^2 + sh + h - 1,$$

car $m + n = h + 1$. □

Remarque. L'hypothèse du Théorème 1.3 est notamment satisfaite si $G/m \cdot G$ est fini pour tout m. Les groupes divisibles (i.e. tels que $m \cdot G = G$, pour tout $m \geq 1$), parmi lesquels $\mathbb{R}$ et $\mathbb{Q}$, vérifient évidemment cette propriété. On peut aisément voir que les groupes abéliens de type fini satisfont également cette propriété. C'est aussi le cas du groupe $\mathbb{Z}_p$ des entiers p-adiques, puisque $\mathbb{Z}_p/m \cdot \mathbb{Z}_p \cong \mathbb{Z}/p^l\mathbb{Z}$, où p^l est la plus grande puissance de p qui divise m. Les groupes *juste infinis* (tous leurs quotients non triviaux sont finis) forment une autre classe de groupes pour lesquels le précédent théorème s'applique. Remarquons que $\mathbb{Z}_p$ n'est pas juste infini, puisque $\mathbb{Z}_p/\mathbb{Z}$ est infini.

On s'intéresse maintenant à la minoration, à travers la preuve du Théorème 1.4. En fait, on va retrouver la minoration connue pour les entiers (cf. (1.4)), simplement parce que la base qui donne cette borne dans $\mathbb{N}$ est une base parfaite.

Preuve du Théorème 1.4. Soit

$$g = \left[\frac{h(h+4)}{3}\right] + 1$$

et $k = g - 1$. D'après le Théorème 20 de [14], il existe un ensemble $A \subset \mathbb{Z}/g\mathbb{Z}$ de deux éléments tel que :

(i) $A \cup 2A \cup \cdots \cup hA = \mathbb{Z}/g\mathbb{Z}$,

(ii) $(k-1)A \neq \mathbb{Z}/g\mathbb{Z}$,

(iii) $kA = \mathbb{Z}/g\mathbb{Z}$.

Comme $\mathbb{Z}$ est un quotient de G par hypothèse, $\mathbb{Z}/g\mathbb{Z}$ est également un quotient de G. C'est-à-dire qu'il existe un sous-groupe K de G tel que $G/K \cong \mathbb{Z}/g\mathbb{Z}$.

Soit alors $B = \{x \in G : \overline{x} \in A\}$, où $\overline{x}$ désigne la classe de x dans G/K. D'après le Lemme 1.5, B vérifie

(i) $B \cup 2B \cup \cdots \cup hB = G$,

(ii) $(k-1)B \neq G$,

(iii) $kB = G$.

Autrement dit, $\mathrm{ord}^*_G(B) = k$. Mais selon la définition (1.6), c'est exactement dire que

$$X_G(h) \geq k = \left[\frac{h(h+4)}{3}\right].$$

□

1.5.2 Le cas des groupes p-torsion

Dans cette section, on suppose que $px = 0$ pour tout $x \in G$, avec p un nombre premier. Dans ce cas de torsion, l'inclusion

$$nA \subset (n+p)A$$

est vraie pour tout n. Cette simple observation va nous permettre d'améliorer considérablement la majoration de $X_G(h)$.

Preuve du Théorème 1.5 (i). Ici, nous utilisons à nouveau la définition (1.6) de X_G. On considère A une base faible d'ordre au plus h et on suppose $\mathrm{ord}^*_G(A) = k$. Comme $nA \subset (n+p)A$ pour tout n, $\cup_{i=h-p+1}^{h} A \sim G$ $(h \geq p)$. Le Lemme 1.6 implique que

$$\bigcup_{i=h-p+2}^{h+1} iA = G. \tag{1.17}$$

De plus, on a clairement

$$\bigcup_{i=h-p+3}^{h+2} iA = G. \tag{1.18}$$

Distinguons alors deux cas :

Premier cas : $(h+2)A \cap nA = \emptyset$, pour tout $h-p+3 \leq n \leq h+1$. Alors, d'après (1.17) et (1.18), et puisque $(h-p+2)A \subset (h+2)A$, il vient

$$(h-p+2)A = (h+2)A$$

En ajoutant pA des deux côtés, on obtient par récurrence

$$(h-p+2)A = (h+2+lp)A$$

pour tout $l \geq 0$. Si l est suffisamment grand, $h+2+lp \geq k$ et $(h+2+lp)A = G$. C'est pourquoi $(h-p+2)A = G$ et $k \leq h-p+2 \leq h$.
Deuxième cas : $nA \cap (h+2)A \neq \emptyset$ pour un certain $h-p+3 \leq n \leq h+1$. Posons dans ce cas $m = h+2-n$, et remarquons que m est premier avec p (car compris entre 1 et $p-1$). On procède comme au début de la preuve du Théorème 1.3. Si $c \in nA \cap (n+m)A$, alors d'après le Lemme 1.7, on a

$$(p-1)c \in \bigcap_{i=0}^{p-1} ((p-1)n + im)A. \tag{1.19}$$

Comme $\mathrm{pgcd}(m,p) = 1$, $\{im\}_{i=0}^{p-1}$ parcourt exactement toutes les classes modulo p. Si on considère $0 \leq j < p$ le représentant de im modulo p, alors $im \equiv j \pmod p$ et $im \geq j$, ce qui conduit à

$$(h-p+1+im)A \supset (h-p+1+j)A.$$

On en déduit que

$$\bigcup_{i=h-p+1}^{h} iA \subset \bigcup_{i=0}^{p-1}(h-p+1+im)A.$$

Ainsi,

$$G \sim \bigcup_{i=0}^{p-1}(h-p+1+im)A.$$

Pour tout $x \in G$, sauf un nombre fini, on a

$$x-(p-1)c \in \bigcup_{i=0}^{p-1}(h-p+1+im)A. \tag{1.20}$$

En combinant (1.20) et (1.19) on voit que pour tout $x \in G$, sauf un nombre fini,

$$\begin{aligned} x \in & ((h-p+1)+(p-1)m+(p-1)n)\,A \\ & = (h-p+1+(p-1)(h+2))A = (hp+p-1)A. \end{aligned}$$

Cela montre bien $\mathrm{ord}^*_G(A) \leq hp+p-1$. □

Afin d'obtenir une minoration de $X_G(h)$, on utilise la même idée que pour le Théorème 1.4, en exhibant une base parfaite dans un quotient de G. Remarquons que G est un espace vectoriel sur $\mathbb{F}_p$ et qu'en conséquence, tout quotient fini de G est isomorphe à $\mathbb{F}_p^d$, pour un certain d. Cette observation nous conduit à nous intéresser de plus près au cas de $\mathbb{F}_p^d$. Le prochain lemme permet de bien comprendre les bases faibles parfaites de cardinal d dans $\mathbb{F}_p^d$.

Lemme 1.11. *Soit $A = \{e_1, \ldots, e_d\} \subset \mathbb{F}_p^d$. A est une base faible parfaite de $\mathbb{F}_p^d$ si et seulement si les vecteurs $e_1, \ldots, e_d$ sont linéairement indépendants. Lorsque cette condition est satisfaite, tout élément de $\mathbb{F}_p^d$ peut s'exprimer comme somme de $\leq (p-1)d$ éléments de A, et on ne peut pas faire mieux que $(p-1)d$.*

Démonstration. Tout d'abord, il est évident que $iA \in \langle A \rangle$ pour tout i. Si A est une base faible parfaite, on a nécessairement $\langle A \rangle = \mathbb{F}_p^d$, ce qui implique que les vecteurs $e_1, \ldots, e_d$ sont linéairement indépendants. Supposons maintenant que les vecteurs $e_1, \ldots, e_d$ sont linéairement indépendants. Pour tous $0 \leq \alpha_1, \ldots, \alpha_d \leq p-1$, l'élément $\sum_{i=1}^d \alpha_i e_i$ est la somme de $\sum_{i=1}^d \alpha_i \leq (p-1)d$ éléments de A. En outre, $\sum_{i=1}^d (p-1)e_i$ ne peut pas s'écrire comme somme de moins de $(p-1)d$ éléments de A. □

Cela nous amène à une caractérisation des bases parfaites de cardinal $d+1$ dans $\mathbb{F}_p^d$.

Lemme 1.12. *Soit $A = \{e_1, \cdots, e_d, \alpha_1 e_1 + \cdots + \alpha_d e_d\} \subset \mathbb{F}_p^d$, avec les vecteurs $e_1, \ldots, e_d$ linéairement indépendants. Alors, A est une base parfaite de $\mathbb{F}_p^d$ si et seulement si*

$$\sum_{i=1}^{d} \alpha_i \not\equiv 1 \bmod p.$$

De plus, si cette condition est satisfaite, $d(p-1)A = \mathbb{F}_p^d$ et $(d(p-1)-1)A \neq \mathbb{F}_p^d$. Autrement dit, A est une base parfaite d'ordre $d(p-1)$.

Démonstration. Tout d'abord, A est une base parfaite si et seulement si $A - a$ est une base parfaite (Lemme 1.2). Remarquons tout de même que cette propriété n'est pas vraie pour une base vectorielle. On a :

$$A - e_1 = \{0, e_2 - e_1, \cdots, e_d - e_1, (\alpha_1 - 1)e_1 + \cdots + \alpha_d e_d\}.$$

Or, $(A - e_1)$ est une base parfaite si et seulement si $(A - e_1) \setminus \{0\}$ est une base faible parfaite. Et d'après le Lemme 1.11, il nous suffit de vérifier dans quels cas $(A - e_1) \setminus \{0\}$ est une famille de d vecteurs indépendants. On peut alors calculer le déterminant de cette famille :

$$\begin{aligned}
&\det(\{e_2 - e_1, \cdots, e_d - e_1, (\alpha_1 - 1)e_1 + \cdots + \alpha_d e_d\}) \\
&\qquad = \begin{vmatrix}
-1 & -1 & \cdots & \cdots & -1 & -1 & \alpha_1 - 1 \\
1 & 0 & \cdots & \cdots & 0 & 0 & \alpha_2 \\
0 & 1 & 0 & \cdots & 0 & 0 & \alpha_3 \\
0 & 0 & 1 & \ddots & \cdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & \vdots & & \ddots & 1 & 0 & \vdots \\
0 & 0 & \cdots & \cdots & 0 & 1 & \alpha_d
\end{vmatrix} \\
&\qquad = \sum_{i=1}^{d} \alpha_i - 1,
\end{aligned}$$

ce qui montre la première partie du lemme. L'ordre de A vient directement de la deuxième partie du Lemme 1.11. □

Nous sommes à présent en mesure de construire une base parfaite de $\mathbb{F}_p^d$ qui pourra jouer un rôle similaire à celui de la base A dans la preuve du Théorème 1.4.

Lemme 1.13. *Soient $e_1, \cdots, e_d$ des vecteurs linéairement indépendants de $\mathbb{F}_p^d$. Supposons que $d \not\equiv 1 \bmod p$. Alors, l'ensemble*

$$A = \{e_1, \cdots, e_d, e_1 + \cdots + e_d\}$$

satisfait les propriétés suivantes :

(i) tout élément de $\mathbb{F}_p^d$ peut s'écrire comme somme d'au plus $(d+1)(p-1)/2$ éléments de A,

(ii) $(d(p-1)-1)A \neq \mathbb{F}_p^d$,

(iii) $d(p-1)A = \mathbb{F}_p^d$.

Démonstration. Les deux dernières assertions découlent directement du Lemme 1.12 et de l'hypothèse $d \not\equiv 1 \bmod p$.

Pour démontrer la première assertion, posons $a = \sum_{i=1}^{d} e_i$. Considérons un élément quelconque $x = x_1e_1 + \cdots + x_de_d \in \mathbb{F}_p^d$, et définissons

$$\alpha_i = |\{x_j \equiv i \bmod p\}|\,.$$

Pour tout $0 \leq i \leq p-1$, on peut écrire

$$x = ia + \sum_{j=1}^{d}(x_j - i)e_j = ia + \sum_{j=1}^{d} y_j e_i$$

avec $0 \leq y_j \leq p-1$. Dans cette décomposition de x, on utilise $i + \alpha_{i+1} + 2\alpha_{i+2} + \cdots + (p-1)\alpha_{i+p-1}$ éléments de A. Ainsi, x peut s'écrire à l'aide de

$$\min_i \{i + \alpha_{i+1} + 2\alpha_{i+2} + \cdots + (p-1)\alpha_{i+p-1}\}$$

éléments de A.

Étant donné que

$$\begin{aligned}\sum_{i=0}^{p-1}(i + \alpha_{i+1} + 2\alpha_{i+2} + \cdots + (p-1)\alpha_{i+p-1}) &= \left(\sum_{i=0}^{p-1}\alpha_i\right)\frac{p(p-1)}{2} + \frac{p(p-1)}{2} \\ &= (d+1)\,\frac{p(p-1)}{2}\end{aligned}$$

le minimum sur les i est au plus $(d+1)(p-1)/2$, ce qui est bien le résultat souhaité. □

Remarque. Quand on démontre la première assertion, on utilise simplement le fait que $\min_i$ est plus petit que la moyenne sur tous les i. On pourrait potentiellement améliorer la borne $(d+1)(p-1)/2$ en travaillant plus précisément. Il nous paraît possible d'obtenir $d(p-1)/2$ à la place, mais ce ne serait pas d'un intérêt considérable.

Preuve du Théorème 1.5 (ii). Si $[2h/(p-1)-1] \not\equiv 1 \bmod p$, posons

$$d = \left[\frac{2h}{p-1} - 1\right].$$

Sinon, on choisit

$$d = \left[\frac{2h}{p-1} - 2\right].$$

La condition $h \geq 3(p-1)/2$ nous assure $d \geq 1$.

On considère $A \subset \mathbb{F}_p^d$ l'ensemble décrit dans le Lemme 1.13. D'après le travail effectué précédemment, et comme $(d+1)(p-1)/2 \leq h$ pour les deux choix de d, on a

(i) $A \cup 2A \cup \cdots \cup hA = \mathbb{F}_p^d$,

(ii) $(d(p-1)-1)A \neq \mathbb{F}_p^d$,

(iii) $d(p-1)A = \mathbb{F}_p^d$.

Or, il existe un sous-groupe K de G tel que $G/K \cong \mathbb{F}_p^d$. Si on définit $B = \{x \in G : \overline{x} \in A\}$, où $\overline{x}$ désigne la classe de x dans G/K, le Lemme 1.5 implique

(i) $B \cup 2B \cup \cdots \cup hB = G$,

(ii) $(d(p-1)-1)B \neq G$,

(iii) $d(p-1)B = G$.

On a donc bien

$$X_G(h) \geq \mathrm{ord}_G^*(B) = d(p-1) \geq (p-1)\left(\frac{2h}{p-1} - 3\right) = 2h - 3p + 3.$$

□

Dans la preuve, on obtient une meilleure borne dans le cas $d = [2h/(p-1) - 1] \not\equiv 1 \bmod p$, à savoir $X_G(h) \geq 2h - 2p + 2$. D'autre part, si $p = 2$, $d = 2h - 2$. Les Theorèmes 1.5 (i) et 1.5 (ii) donnent alors l'encadrement

$$2h - 2 \leq X_G(h) \leq 2h + 1$$

pour G un groupe 2-torsion. Il pourrait être intéressant de déterminer la valeur exacte de $X_{\mathbb{F}_2[t]}(h)$ par exemple.

1.5.3 $X_G(2)$ et $X_G(3)$

Dans cette section, on démontre le Théorème 1.6. Tout d'abord, les minorations $X_G(2) \geq 3$ et $X_G(3) \geq 4$ sont des conséquences immédiates du Théorème 1.1. Pour les majorations, on utilise encore une fois la définition (1.6) de X_G.

Preuve du Théorème 1.6(i). Supposons que

$$A \cup 2A \sim G$$

et $\mathrm{ord}^*_G(A) = k$ est fini. En adaptant la preuve du Lemme 1.6, pour tout $l \geq 2$, on a

$$lA \cup (l+1)A = G.$$

Premier cas : Il existe c dans $2A \cap 3A$. Dans ce cas, pour tout $x \in G$, sauf un nombre fini, $x - c \in A \cup 2A$. Ainsi, pour tout $x \in G$, sauf un nombre fini, $x = x - c + c \in 4A$, et $4A \sim G$.
Deuxième cas : $2A \cap 3A = \emptyset$. S'il existe $c \in 3A \cap 4A$, alors par le même procédé, on obtient $5A \sim G$. Supposons alors que $3A \cap 4A = \emptyset$. Comme $2A \cup 3A = 3A \cup 4A = G$, cela implique $2A = 4A$. Mais alors, $2A = 2mA$ pour tout $m \geq 1$. Si $2m > k$, on a $2mA = G$ et donc $2A = G$.

Dans tous les cas, $\mathrm{ord}^*_G(A) \leq 5$. □

Preuve du Théorème 1.6(ii). Supposons que

$$A \cup 2A \cup 3A \sim G$$

et $\mathrm{ord}^*_G(A) = k$ est fini. D'après le Lemme 1.6, pour tout $l \geq 2$, on a

$$lA \cup (l+1)A \cup (l+2)A = G.$$

Remarquons que si $iA \cap (i+1)A \neq \emptyset$, alors $2iA \cap (2i+1)A \cap (2i+2)A \neq \emptyset$, ce qui donne $(2i+3)A \sim G$. Ainsi, on peut supposer que

$$iA \cap (i+1)A = \emptyset \text{ pour } 1 \leq i \leq 7.$$

Autrement,

$$\mathrm{ord}^*(A) \leq 2i + 3 \leq 17.$$

On distingue cette fois-ci trois cas, ce qui est suffisant car $0 \in 2A \cup 3A \cup 4A$.

Premier cas : $0 \in 2A$. Dans ce cas, $4A \supset 2A$ et $5A \supset 3A$. Il vient alors $3A \cup 4A = G = 4A \cup 5A$. Par hypothèse, ce sont des partitions de G, ce qui conduit à $3A = 5A$. Mais alors, $3A = (2m+3)A$ pour tout $m \geq 1$. En conséquence, $3A = G$ et $\mathrm{ord}^*_G(A) \leq 3$.

Deuxième cas : $0 \in 3A$. On a donc $5A \supset 2A$ et $6A \supset 3A$. Comme $5A \cap 6A = \emptyset$, $5A \cap 3A = \emptyset$. Ainsi, $3A \cup 4A \cup 5A = G$ est une partition de G. D'autre part, comme $2A \cup 3A \cup 4A = G$, on en déduit que $2A = 5A$ Comme dans le cas précédent, on obtient $\mathrm{ord}^*_G(A) \leq 2$.

Troisième cas : $0 \in 4A$. Cette fois-ci, $6A \supset 2A$, $7A \supset 3A$, $8A \supset 4A$, et $2A \cup 3A \cup 4A = G = 6A \cup 7A \cup 8A = G$. Comme $7A$ est disjoint de $6A$ et $8A$, on en déduit $3A = 7A$. Et cela donne $\mathrm{ord}^*_G(A) \leq 3$. □

1.6 La fonction S

La clé pour généraliser les arguments de Cassaigne et Plagne [2] est la notion de *moyennabilité* d'un groupe.

1.6.1 Moyennabilité

On se place ici dans le cadre d'un groupe G abélien infini qu'on munit de la topologie discrète.

Remarque. En fait, on définit la moyennabilité plus généralement sur les groupes localement compacts, munis de la mesure de Haar μ (unique à translation près). Pour un tel groupe G, on note $L^\infty(G,\mu)$ l'espace de Banach des fonctions mesurables essentiellement bornées de G dans $\mathbb{C}$. S'intéresser ici seulement aux groupes discrets simplifiera notre propos, dans la mesure où on a dans ce cas $L^\infty(G,\mu) = l^\infty(G)$ l'ensemble des fonctions bornées de G dans $\mathbb{C}$.

Parmi les nombreuses définitions de la moyennabilité, on travaille avec celle faisant intervenir les *moyennes invariantes*.

Définition 1.3. Une moyenne invariante à droite sur G (avec G un groupe discret, non nécessairement abélien) est une fonctionnelle linéaire $\Lambda : l^\infty(G) \to \mathbb{R}$ vérifiant :

1. Λ est positive : si $f \geq 0$ sur G, alors $\Lambda(f) \geq 0$,
2. Λ est de norme 1 : $\Lambda(1_G) = 1$ où 1_G est la fonction caractéristique de G,
3. Λ est invariante à droite : $\Lambda(\tau_g f) = \Lambda(f)$ pour tout $f \in l^\infty(G)$ et $g \in G$, avec τ_g la translation à droite ($\tau_g(f(x)) = f(xg)$).

Dans le cas d'un groupe abélien, il ne sera pas nécessaire de préciser "à droite".

Définition 1.4. Le groupe G est dit *moyennable* s'il existe une moyenne invariante à droite sur G.

Commençons par énoncer le Théorème G.2.1 de [1] qu'on utilisera fondamentalement par la suite.

Théorème 1.9 (Markov,Kakutani)**.** *Tout groupe topologique* ***abélien*** *est moyennable.*

Même s'il s'agit du seul résultat utile pour nous, rappelons maintenant d'autres résultats bien connus à ce sujet. Pour un aperçu plus complet, on conseille fortement de lire [1, Appendice G].

La propriété de moyennabilité se transmet aux sous-groupes fermés et aux quotients d'un groupe. Or, il est assez facile de voir que le groupe libre à deux

éléments F_2 n'est pas moyennable. Pour cela, on peut se baser sur le graphe de Cayley du groupe, on s'aperçoit qu'une moyenne ne peut pas charger les points, puis, en utilisant l'invariance de la moyenne et les symétries du graphe, on peut montrer que la moyenne est nécessairement la fonction nulle. Ainsi, tout groupe qui contient F_2 n'est pas moyennable. Von Neumann s'est d'ailleurs demandé si c'était le seul cas d'obstruction à la moyennabilité. Mais on sait maintenant construire des groupes non moyennables qui ne contiennent pas F_2.

Remarque. Dans le cas des groupes localement compacts, dans la définition de la moyenne, on remplace $l^\infty(G)$ par $L^\infty(G, \mu)$. La preuve qui va suivre peut être adaptée à ces groupes lorsqu'ils sont abéliens, si on change la définition de l'ordre. En effet, il ne faut plus demander à ce que $hA \sim G$, mais plutôt $\mu(G \setminus hA) = 0$ dans ce cas.

1.6.2 Preuve du Théorème 1.7

Démonstration. La minoration $h + 1 \leq S_G(h)$ est une conséquence immédiate du Théorème 1.1. Il reste à démontrer la majoration. G est un groupe abélien, donc d'après le Théorème 1.9, on peut se munir de Λ une moyenne invariante sur G. G étant infini, on s'aperçoit aisément que $\Lambda(1_I) = 0$ pour tout sous-ensemble fini $I \subset G$, où 1_I est la fonction caractéristique de I (il suffit de le constater pour un singleton). En conséquence, pour tout B sous-ensemble G tel que $B \sim G$, par linéarité de Λ,

$$\Lambda(1_B) = \Lambda(1_G - 1_{G\setminus B}) = \Lambda(1_G) - \Lambda(1_{G\setminus B}) = 1. \tag{1.21}$$

Considérons A une base d'ordre h de G. Sans perte de généralité, on peut supposer que $0 \in A$.

Pour chaque élément $a \in A$, on définit f_a une fonction sur G par

$$f_a(x) = \begin{cases} 1, & \text{si } x \in hA \setminus h\,(A \setminus \{a\}) \\ 0, & \text{autrement.} \end{cases}$$

Autrement dit, $f_a(x) = 1$ si et seulement si a est essentiel dans toute représentation de x comme somme de h éléments de A.

Comme il est fait dans la preuve de [2], on observe deux choses. Premièrement, pour tout $x \in G$ et tout sous-ensemble fini $I \subset A$, on a $\sum_{a\in I} f_a(x) \leq h$. En effet, si $x \notin hA$, alors clairement, $f_a(x) = 0$ pour tout $a \in A$. Supposons que $x \in hA$, et fixons une représentation

$$x = a_1 + \cdots + a_h$$

avec $a_i \in A$. Alors $f_a(x)$ peut valoir 1 seulement si a est l'un des a_i, et il y a au plus h tels éléments.

Mais alors, $h1_G - \sum_{a\in I} f_a \geq 0$. En utilisant la positivité et la linéarité de Λ, on a finalement prouvé le fait suivant.

Fait 1. Pour tout sous-ensemble fini $I \subset A$, on a

$$\sum_{a\in I} \Lambda(f_a) \leq h.$$

La deuxième chose que l'on veut montrer est :

Fait 2. Si $a \in A$ est tel que $\Lambda(f_a) < 1/h$, alors il existe $x \in G$ tel que

$$x + ia \in h(A \setminus \{a\})$$

pour tout $i = 0, 1, \ldots, h-1$.

En effet, comme Λ est invariante par translation et linéaire,

$$1 > h\Lambda(f_a) = \sum_{i=0}^{h-1} \Lambda\left(\tau_{ia} f_a\right) = \Lambda\left(\sum_{i=0}^{h-1} \tau_{ia} f_a\right).$$

Or, en posant

$$B = \left\{ x \in G \text{ tel que } \sum_{i=0}^{h-1} \tau_{ia} f_a(x) \geq 1 \right\},$$

si $B \sim G$, on a

$$\sum_{i=0}^{h-1} \tau_{ia} f_a \geq 1_B,$$

ce qui donne d'après (1.21)

$$\Lambda\left(\sum_{i=0}^{h-1} \tau_{ia} f_a\right) \geq \Lambda(1_B) = 1.$$

Ainsi, $B \not\sim G$, donc B^c, le complémentaire de B, est infini. Or, tout élément x de B^c vérifie

$$1 > \sum_{i=0}^{h-1} \tau_{ia} f_a(x) = \sum_{i=0}^{h-1} f_a(x + ia).$$

En conséquence, quelque soit $x \in B^c$, $f_a(x + ia) = 0$ pour tout $i = 0, 1, \ldots, h-1$.

Mais comme $hA \sim G$, il existe $x \in B^c$ tel que $x + ia \in hA$ pour tout $i = 0, 1, \ldots, h-1$. Et ce x vérifie donc

$$x + ia \in h(A \setminus \{a\})$$

pour tout $i = 0, 1, \ldots, h-1$, ce qui est le résultat souhaité.

D'après le Fait 1, on sait que pour tout $a \in A$, sauf un nombre fini, on a $a \neq 0$ et $\Lambda(f_a) < 1/h$ (on ne peut en effet pas avoir plus de h^2 élements a tels que $\Lambda(f_a) \geq 1/h$). Pour un tel a, considérons x vérifiant $x + ia \in h(A \setminus \{a\})$ pour tout $i = 0, 1, \ldots, h-1$, dont l'existence est donnée par le Fait 2. Ainsi, pour tout $y \in G$, sauf un nombre fini, on a $y - x \in hA$ et $y - x \neq ha$. Mais alors, si on écrit

$$y - x = a_1 + \cdots + a_h,$$

où les a_j sont dans A, il y a au plus $h-1$ a_j égaux à a. En notant i ce nombre $(0 \leq i \leq h-1)$, on a

$$y - x - ia \in (h-i)(A \setminus \{a\}).$$

Cela implique que

$$y = (y - x - ia) + (x + ia) \in (2h - i)(A \setminus \{a\}) \subset 2h(A \setminus \{a\})$$

car $A \setminus \{a\}$ contient 0. On a bien démontré que $A \setminus \{a\}$ est une base d'ordre au plus $2h$. □

1.6.3 Preuve du Théorème 1.8

Démonstration. On a déjà $S_G(2) \geq 3$. Il reste à montrer que $S_G(2) \leq 3$. Soit donc A une base d'ordre 2 de G. On dit que $b \in A$ est *mauvais* si $\mathrm{ord}^*(A \setminus \{b\}) \geq 4$ et *bon* autrement. L'objectif est de montrer que A n'admet qu'un nombre fini de mauvais éléments.

En considérant $A - c$ à la place de A, avec c un élément de A, on peut supposer que $0 \in A$.

Commençons par examiner les propriétés d'un mauvais élément $b \in A, b \neq 0$. Notons $A_b = A \setminus \{b\}$. A étant une base d'ordre 2, on a

$$G \sim 2A \sim 2A_b \cup (A_b + b)\,. \tag{1.22}$$

Soit a un élément quelconque de A_b. Alors,

$$G \sim 2A + a \sim (2A_b + a) \cup (A_b + b + a) \subset 3A_b \cup (A_b + b + a)\,. \tag{1.23}$$

De plus, comme $0 \in A_b$, on déduit de (1.22) l'inclusion

$$G \sim 2A_b \cup (A_b + b) \subset 3A_b \cup (A_b + b). \tag{1.24}$$

D'après (1.23) et (1.24), les ensembles $(A_b + b + a)$ et $(A_b + b)$ contiennent tous deux $G \setminus 3A_b$, à un nombre fini d'éléments près. Or, b étant mauvais, $G \setminus 3A_b$ est infini, ce qui implique que $(A_b + b + a) \cap (A_b + b)$ est infini. Autrement dit, on a démontré la chose suivante :

Propriété 1 : Pour tout $a \in A_b$, $(A_b + a) \cap A_b$ est infini.

Ensuite on prouve :

Propriété 2 : $(A_b + b) \cap A_b = \emptyset$.

En effet, supposons, par l'absurde, qu'il existe $a_1, a_2 \in A_b$ tels que $b + a_1 = a_2$. Pour tout $x \in A$, sauf un nombre fini, on a $x - a_1 \in 2A \setminus \{2b\}$. Si $x - a_1 \in 2A_b$, alors $x \in 3A_b$. Sinon, $x - a_1 \in A_b + b$, mais alors $x \in A_b + a_2 \subset 2A_b \subset 3A_b$. Ainsi $3A_b \sim G$, ce qui fournit une contradiction.

Supposons à présent qu'il existe un autre mauvais élément $b' \in A, b' \neq 0$. Par la Propriété 1, on sait que $(A_b + b') \cap A_b$ est infini. En conséquence, $(A \setminus \{b, b'\} + b') \cap (A \setminus \{b, b'\})$ est infini. Mais cela contredit la Propriété 2 (où on remplace b par b'). □

En fait, la preuve montre qu'il y a au plus un mauvais élément dans A. En effet, on a montré que pour tout $c \in A$, il y a au plus un mauvais élément dans A qui soit différent de c. En appliquant cette observation à un bon élément c (dont on connaît maintenant l'existence), cela implique qu'il y a bien au plus un mauvais élément dans A.

Bibliographie

[1] B. Bekka, P. de la Harpe, A. Valette, *Kazhdan's Property (T)*, New Mathematical Monographs, 11. Cambridge University Press, Cambridge, 2008.

[2] J. Cassaigne, A. Plagne, *Grekos' S function has a linear growth*, Proceedings of the American Mathematical Society 132 (2004), 2833–2840.

[3] P. Erdős, R. L. Graham, *On bases with an exact order*, Acta Arith. 37 (1980) 201–207.

[4] P. Erdős, R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monogr. Enseign. Math. 28, 1980.

[5] G. Grekos, *Extremal problems about asymptotic bases : a survey*, Combinatorial number theory, 237–242, de Gruyter, Berlin, 2007.

[6] G. Grekos, *Sur l'ordre d'une base additive*, Séminaire de Théorie des Nombres de Bordeaux (Talence, 1987–1988), Exp. No. 31, 13 pp.

[7] G. Grekos, *Extremal problems about additive bases*, Acta Math. Inform. Univ. Ostraviensis 6 (1998), no. 1, 87–92.

[8] G. Grekos, *Minimal additive bases and related problems*, Number theory days, 1980 (Exeter, 1980), 300–305, London Math. Soc. Lecture Note Ser., 56, Cambridge Univ. Press, Cambridge, 1982.

[9] E. Härtter, *Ein Beitrag zur Theorie der Minimalbasen*, J. reine angew. Math. 196 (1956), 170–204.

[10] M. B. Nathanson, *Minimal bases and powers of 2*, Acta Arith. 49 (1988), 525–532.

[11] M. B. Nathanson, *Unique representation bases for the integers*, Acta Arith. 108(1) (2003), 1–8.

[12] J. C. M. Nash, *Some applications of a theorem of M. Kneser*, J. Number Theory 44 (1993), 1–8.

[13] A. Plagne, *Problemas combinatorios sobre bases aditivas*, Gaceta de la Real Sociedad Matemática Española 9 (2006), 191–201.

[14] A. Plagne, *A propos de la fonction X d'Erdős et Graham*, Annales de l'Institut Fourier 54 (2004), no. 6, 1717–1767.

[15] A. Plagne, *Sur le nombre d'éléments exceptionnels d'une base additive*, Journal für die Reine und Angewandte Mathematik 616 (2008), 47–65.

[16] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I, II*, J. reine angew. Math. 194 (1955), 40–65 and 111–140.