UNIVERSITÉ PARIS 8
VINCENNES-SAINT-DENIS

École doctorale
**C**ognition, **L**angage, **I**nteraction

Spécialité
Mathématiques

# THÈSE DE DOCTORAT DE L'UNIVERSITÉ PARIS VIII

Présentée par

**Kamil MERITO ALI**

Pour obtenir le grade de

**DOCTEUR**

Sujet de la thèse :

# Suites à somme nulle pondérées et applications

Soutenue le xxx xxx 2024 devant le jury composé de :

| | |
|---|---|
| M. Wolfgang Schmid | Directeur de thèse |
| M. xxxx xxxx | Rapporteur |
| M. xxxx xxxx | Rapporteur |
| M. xxxx xxxx | Examinateur |
| Mme. xxxx xxxx | Examinateur |
| M. xxxx xxxx | Examinateur |

# Remerciements

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué à la réalisation de cette thèse.

Tout d'abord, je remercie chaleureusement mon directeur de thèse, le professeur Wolfgang Schmid, pour son soutien indéfectible, ses conseils précieux et sa patience tout au long de ce parcours. Son expertise et sa vision m'ont guidé dans mes recherches et m'ont permis de surmonter les défis rencontrés.

Je souhaite également remercier les membres du jury, en particulier [Noms des rapporteurs et examinateurs], pour avoir accepté d'évaluer mon travail et pour leurs commentaires constructifs qui ont enrichi cette thèse.

Je remercie mes collègues et amis du laboratoire LAGA, pour les discussions stimulantes, leur camaraderie et leur soutien moral. Ensemble, nous avons partagé des moments d'échanges intellectuels qui ont grandement enrichi ma réflexion.

Je n'oublie pas ma famille, dont l'amour et le soutien inconditionnels m'ont permis de poursuivre mes études avec détermination. Merci à mes parents, pour avoir toujours cru en moi et m'avoir encouragé à suivre mes passions.

Enfin, je remercie tous ceux qui, de près ou de loin, ont contribué à l'aboutissement de ce travail, que ce soit par leurs conseils, leur soutien ou leur amitié.

À chacun d'entre vous, je vous adresse mes sincères remerciements.

# Résumé

Cette thèse explore les suites à somme nulle pondérées dans des groupes abéliens finis ainsi que leurs propriétés arithmétiques. Elle commence par une introduction aux concepts mathématiques clés, notamment les groupes, monoïdes, et l'arithmétique des suites, afin de mieux comprendre les suites à somme nulle pondérées. Ces suites sont définies comme des suites d'éléments d'un groupe abélien dont la somme pondérée est nulle.

Nous analysons les propriétés fondamentales de ces suites, comme la constante de Davenport, qui détermine la longueur minimale d'une suite dans un groupe abélien contenant une sous-suite à somme nulle. Cette étude est ensuite étendue aux monoïdes de séquences pondérées, avec une attention particulière aux propriétés de ces structures et à leur arithmétique.

En plus de ces résultats, nous rappelons certains concepts de la théorie des codes, sans toutefois proposer de nouvelles optimisations dans ce domaine. L'accent est mis sur la compréhension des suites à somme nulle et leur rôle dans des contextes mathématiques plus larges.

# Table des matières

# 1 | Introduction générale

## Sommaire

Dans ce chapitre, nous rappelons plusieurs concepts fondamentaux issus de l'algèbre et de la théorie des codes. Il nous a semblé utile d'inclure cette introduction, étant donné que notre thèse touche à plusieurs domaines connexes. Une attention particulière sera accordée aux monoïdes réguliers et commutatifs, qui jouent un rôle central dans notre travail.

# 1.1 Groupes

## 1.1.1 Monoïdes

Soit $S$ est un ensemble. Une application

$$S \times S \longrightarrow S$$

est parfois appelé une **loi de composition interne** sur $S$. Si $x$ et $y$ sont des éléments de $S$, leur produit est l'image du couple du couple $(x, y)$ par cette application et sera noté $xy$. (Nous écrivons parfois $x.y$ et, dans certains cas , il est commode d'adopter une notation additive et d'écrire $x + y$. Cet élément est alors la somme de $x$ et de $y$. On réserve en général la notation $x + y$ aux cas ou on a $x + y = y + x$.)
Soit $S$ un ensemble muni d'une loi de composition interne. Si $x, y$ et $z$ sont des éléments $S$, nous pouvons former leur produit de deux manières : $(xy)z$ ou $x(yz)$. Si $(xy)z = x(yz)$ pout tout $x, y, z$ dans $S$ nous disons que la loi de composition est **associative**.
$S$ admet un élément neutre noté $e$.
Un **monoïdes** est un ensemble $G$ muni d'une loi de composition interne associative et ayant un élément neutre (Il en résulte, en particulier, que $G$ n'est pas vide).
Soient $G$ un monoïde et $x_1, \ldots, x_n$ des éléments de $G$ ($n$ étant un entier $> 1$). Leur produit est défini par récurrence :

$$\prod_{\nu=1}^{n} x_\nu = x_1 \cdots x_n = (x_1 \cdots x_{n-1})x_n.$$

On a la règle

$$\prod_{\nu=1}^{m} x_\nu . \prod_{\nu=1}^{n} x_{m+\nu} = \prod_{\nu=1}^{m+n} x_\nu.$$

qui exprime essentiellement qu'on peut insérer des parenthèses de quelque manière que ce soit dans le produit , sans modifier sa valeur.
On écrit également

$$\prod_{m+1}^{m+n} x_\nu \text{ au lieu de lieu de } \prod_{\nu=1}^{n} x_{m+\nu}$$

et on définit

$$\prod_{\nu=1}^{0} x_\nu = e.$$

Par convention le produit est égal à l'élément neutre. Il est possible de définir des lois de composition plus générales, c'est-à-dire des applications $S_1 \times S_2 \longrightarrow S_3$ pour des ensembles arbitraires . L'associativité et la commuatativité signifie peuvent être définies dans tout contexte ou elles ont un sens. Par exemple, pour la commuatativité, nous avons besoin d'une loi de composition

$$f : S \times S \longrightarrow T$$

Les deux ensembles de départ étant les mêmes. La **commutativité** signifie alors que l'on a $f(x, y) = f(y, x)$, ou $xy = yx$ si nous omettons les symboles de l'application $f$.
Si la loi de composition de $G$ est commutative , on dit aussi que $G$ est **commutatif** (ou **abélien**).

**Définition 1.1.1**
Un monoïde $H$ est dit régulier si, pour tout élément $a \in H$, il existe un élément $b \in H$ tel que :

$$a \cdot b \cdot a = a$$

**Définition 1.1.2**
Un **groupe** $G$ est un monoïde tel que, pour tout élément $x \in G$, il existe $y \in G$ tel que $xy = yx = e$. Un tel élément $y$ est appelé un **inverse** de $x$. Un tel inverse est unique , car si $y'$ étant aussi un inverse de $x$, alors

$$y' = y'e = y'(xy) = (y'x)y = ey = y.$$

L'inverse est noté $x^{-1}$ (ou $-x$ si la loi de composition est notée additivement, auquel cas il est appelé **l'opposé** de $x$) (voir le chapitre 1 de [29]).

**Définition 1.1.3**
Si $G$ est un groupe fini, son nombre d'éléments $|G|$ est appelé l'ordre de $G$.

**Définition 1.1.4**
Soient $G, G'$ deux groupes.

Une application $f : G \longrightarrow G'$ est un morphisme de groupes si

$$f(xy) = f(x)f(y), \text{ pour tous } x, y \in G$$

**Définition 1.1.5**
Un isomorphisme du groupe est un morphisme bijectifs.

Deux groupes $G$ et $G^{'}$ sont isomorphismes s'il existe au moins un isomorphisme de groupes $f : G \longrightarrow G^{'}$. On note cela $G \simeq G^{'}$.

Un automorphisme d'un groupe $G$ est un isomorphisme de groupe de $G$ sur lui-même.L'ensemble des automorphismes de $G$ est noté $Aut(G)$.

**Définition 1.1.6**
Soit $f : G \longrightarrow G^{'}$ un morphisme de groupes. Le noyau de $f$ est le sous-groupe de $G$, noté $Ker(f)$, défini par

$$Ker(f) = f^{-1}(\{1_{G'}\}) = \{x \in G | f(x) = 1_{G'}\}.$$

L'image de $f$ est le sous-groupe de $G^{'}$, noté $Im(f)$, défini par

$$Im(f) = f(G) = \{f(g) | g \in G\}.$$

**Définition 1.1.7**
Soit $G$ est un groupe. Le centre d'un groupe est l'ensemble

$$Z(G) = \{z \in G | zg = gz, \text{ pour tout } g \in G\}.$$

C'est sous-groupe abélien de $G$, distingué dans $G$. $Z(G) = G$ si, et seulement si $G$ est abélien.

**Définition 1.1.8**
On dit que $G$ est monogène s'il peut être engendré par un élément, et cyclique s'il est monogène fini.

**Définition 1.1.9**
Soit $E$ un ensemble, et soit $G$ un groupe. Une action(ou une opération) à gauche de $G$ sur $E$ est une application

$$\begin{array}{c} G \times E \longrightarrow E \\ (g, x) \longmapsto g \cdot x \end{array}$$

Vérifiant les propriétés suivantes :

1. Pour tout $x \in E$, on a $1_G.x$ ;

2. Pour tous $g, g^{'} \in G$, et tout $x \in E$, on a $x \in E$, on a $g \cdot (g^{'} \cdot x) = gg^{'} \cdot x$.
   Dans ce cas , on dit que $G$ opère sur $E$ ou agit sur $E$.

**Définition 1.1.10**
Soit $G$ un groupe opérant sur $G$. On dit que $G$ agit fidèlement sur $E$ si pour tout $g \in E$, on a

$$g \cdot x = x, \text{ pour tout } x \in E, \Longrightarrow g = 1_G.$$

Autrement dit, $G$ agit fidèlement sur $E$ si le mophisme $\varphi : G \longrightarrow \mathcal{G}(E)$ associé est injectif.
On dit que le groupe $G$ agit transitivement sur $E$ pour tous $x, x^{'} \in E$, il existe $g \in G$ tel que $x^{'} = g \cdot x$.

**Définition 1.1.11**
L'ensemble

$$Stab_G(x) = \{g \in G | g \cdot x = x\}$$

est appelé le stabilisateur de $x$(sous l'action de $G$). On vérifie facilement que c'est un sous-groupe de $G$.

**Définition 1.1.12**
$G$ opérant sur un ensemble $E$, et soit $x \in E$. L'ensemble

$$\mathcal{O}_x = \{g \cdot x | g \in G\} \subset E$$

est appelé l'orbite de $x$ sous l'action de $G$, ou $G$-orbite de $x$. C'est la classe d'équivalence de $x$ pour la relation d'équivalence sur $G$ induite par l'action de $G$ sur $E$.

On dit que $x \in E$ est un point fixe sous l'action de $G$ si l'on a $g \cdot x = x$,pour tout $g \in G$. L'ensemble des points fixes est noté $E^G$.

**Définition 1.1.13**
Soit $G$ un groupe, et soit $H$ un sous-groupe distingué dans $G$. Le groupe $G/H$ est appelé le quotient de groupe $G$ par $H$.

**Définition 1.1.14**
Soit $G$ un groupe quelconque. On dit que $G$ est d'exposant fini s'il existe un entier $n \geqslant 1$ tel que

$$x^n = 1_G, \text{ pour tout } x \in G.$$

Dans ce cas, on appelle exposant de $G$ le plus petit entier $n \geqslant 1$ vérifiant cette propriété. On le note $exp(G)$.

**Définition 1.1.15**
Soit $G$ un groupe abélien fini.
Alors, il existe des entiers $d_1, \cdots, d_s \geqslant 2$ vérifiant $d_1|d_2|\cdots|d_s$ tels que

$$G \simeq C_{d_1} \times \cdots \times C_{d_s}.$$

De plus, la suite d'entiers $(d_1, \cdots, d_s)$ est unique, et ne dépend que de la classe d'isomorphisme de $G$.

**Corollaire 1.1.1**
Soit $G$ est un groupe abélien fini . Alors, on a un isomorphisme de groupes

$$G \simeq \prod_p \prod_{k\geqslant 1} C_{p^{n_{p,k}}}$$

où $p$ parcourt l'ensemble des nombres premiers, les entiers $n_{n,k}$ sont presque tous nuls, et $(n_{p,k})_{k\geqslant 1}$ est une suite d'entiers décroissante pour tout $p$. De plus, les entiers $n_{p,k}$ sont uniques , et ne dépendent que la classe d'isomorphisme de $G$.

**Définition 1.1.16**
L'ordre d'un élément $g$ dans un groupe $G$ est le plus petit entier positif $n$ tel que : $g^n = e$ où $e$ est l'élément neutre du groupe. Si aucun entier positif $n$ ne satisfait cette condition, on dit que l'ordre de $g$ est infini.

**Définition 1.1.17**
Un $p$-groupe est un groupe fini dont l'ordre est une puissance d'un nombre premier $p$. Cela signifie que l'ordre du groupe $G$, noté $|G|$, est de la forme $p^n$, où $p$ est un nombre premier et $n$ un entier positif.

**Définition 1.1.18**
Un groupe $p$-élémentaire est un groupe abélien fini dans lequel chaque élément a un ordre qui est une puissance de $p$. Un exemple classique est le produit direct de $k$ groupes cycliques d'ordre $p$, c'est-à-dire : $G \cong C_p \times C_p \times \cdots \times C_p$ (avec $k$ facteurs).

**Définition 1.1.19**
On appelle le rang de G et on le note $\mathsf{r}(G)$, le cardinal minimal d'un ensemble générateur de $G$.

## 1.2 Suites à somme nulle

Soit $G$ un groupe abélien additif avec $\exp(G) = n$.
$S = g_1, \cdots, g_l$ est une suite.
Si de plus, la somme de tous les éléments de $S$ est nulle c'est-à-dire $\sum_i^l g_i = 0$, on

dit que $S$ est une suite à somme nulle.

**Notations et quelques outils principaux**

Il existe des entiers $n_1, \cdots, n_r$ tel que $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$. Plus précisement il y a $1 < n_1 | \cdots | n_r$ tel que $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, les $n_i$ sont uniques.
Soit $G$ un ensemble fini, nous notons $\mathcal{F}(G)$, le monoïde commutatif libre engendré par $G$.
Nous utilisons la notation multiplicative pour ce monoïde.

Donc un élément de $\mathcal{F}(G)$ s'écrit comme

$$S = \prod_{g \in G} g^{v_g(S)} \text{ ou } v_g(S) \in \mathbb{N}_0$$

Dans notre contexte, on appelle un tel élément une suite sur $G$.
On peut aussi écrire

$$S = g_1 \cdots g_l \text{ avec les } g_i \in G\,;$$

les $g_i$ sont uniques à l'ordre près.

- $D(G)$,le plus petit entier $l \in \mathbb{N}$ de telle sorte que chaque suite $S \in \mathcal{F}(G)$ de longueur $S \geqslant l$ possède une sous-suite non vide à somme nulle. L'invariant $D(G)$ est appelé la constante de Davenport de $G$.
- $d(G)$ désigne la longueur maximale d'une suite libre de sous-suite à somme nulle sur $G$.
- $\eta(G)$ est le plus petit entier $l \in \mathbb{N}$ de telle sorte que chaque suite $S \in \mathcal{F}(G)$ de longueur $|S| \geqslant l$.

Nous appelons $v_g(S)$, la multiplicité de $p$ dans $S$ et nous disons que $S$ contient $g$ si $v_g(S) > 0$.

$S$ est sans facteur carrée si $v_g(S) \leqslant \forall g \in G, 1$ étant l'élément neutre appartenant à $\mathcal{F}(G)$.

Une suite $S_1$ est appelée une sous-suite de $S$ si $S_1 \mid S$ dans $\mathcal{F}(G)$. Elle est appelée une sous-suite propre de $S$ si elle est une sous-suite avec $1 \neq S_1 \neq S$.

Si une suite $S \in \mathcal{F}(G)$ est écrite de la forme $S = g_1 \cdots g_l$, nous supposons implicitement que $l \in \mathbb{N}_0$ et $g_1 \cdots g_l \in G$. Nous appelons :

- $|S| = l = \sum_{g \in G} v_p(S) \in \mathbb{N}_0$ la longueur $S$
- $supp(S) = \{g \in G | v_p(S) > 0\} \subset G$ le support de $S$.

$G$, un groupe abélien fini, si nous considérons une suite sur $G$ ou plus généralement sur un sous-ensemble d'un tel groupe c'est-à-dire nous considérons $\mathcal{F}(G)$, $\mathcal{F}(G_0)$ ou $(G, +)$ groupe abélien et $G_0 \subset G$, nous avons en plus les notions suivantes :

- $\sigma(S) = \sum_1^l g_i = \sum_{g \in G} v_g(S) g \in G$ la somme de $S$.

— $\sum_k(S) = \{\sum_{i\in I} g_i | I \subset [1,l] \text{ avec } |I| = k\}$

Une suite $S$ est une suite libre de sous-suite à somme nulle si $0 \notin \sum(S)$.

Une suite $S$ est une suite à somme nulle si $\sigma(S) = 0$.

Une suite $S$ est une suite courte à somme nulle si elle est une suite à somme nulle de longueur $|S| \in [1, \exp(G)]$.

## 1.3 Préliminaires

Dans cette section, nous allons rappeler les notations, la terminologie et les résultats dont nous aurons besoin, plus particulièrement pour les monoïdes et les groupes abéliens. Les notations seront en grande partie cohérentes avec celles de la théorie de factorisations [18]. Pour $a, b \in \mathbb{Z}$, nous définissons $[a, b] = \{z \in \mathbb{Z} \mid a \leqslant z \leqslant b\}$ et nous l'appellerons un intervalle. Pour un ensemble $A$, nous désignons par $|A| \in \mathbb{N}_0 \cup \{\infty\}$ sa cardinalité. Pour un nombre réel $x$ soit $\lceil x \rceil = \min\{z \in \mathbb{Z} | x \leqslant z\}$ et $\lfloor x \rfloor = \max\{z \in \mathbb{Z} | x \geqslant z\}$.

En général, nous utilisons la notation additive pour les groupes abéliens. On désigne par $C_n$ un groupe cyclique d'ordre $n$. Pour $(G, +, 0_G)$, un groupe abélien fini, il existe $n_1, \ldots, n_r$ tel que $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$. Plus précisement il y a $1 < n_1 | \cdots | n_r$ tel que $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, les $n_i$ sont uniques. Soit $G$ un groupe abélien fini écrit de manière additive, par $\mathsf{r}(G)$ nous désignons son rang et par $\exp(G)$ son exposant. Si $G_0 \subset G$ est un sous-ensemble, alors $\langle G_0 \rangle \subset G$ désigne le sous-groupe généré par $G_0$ , où $\langle \varnothing \rangle = \{0\}$. L'ensemble $G_0$ (respectivement ses éléments) est dit indépendant, si $0 \notin G_0, \varnothing \neq G_0$ et compte tenu des éléments distincts $e_1, \ldots, e_r \in G_0$ et $a_1, \ldots, a_r \in \mathbb{Z}$, alors $\sum_{i=0}^{r} a_i e_i = 0$ implique que $a_1 e_1 = \cdots = a_r e_r = 0$. Si nous disons que $e_1, \ldots, e_r$ est indépendant, alors nous supposerons que les éléments $e_1, \ldots, e_r$ sont distincts.

Pour les sous-ensembles $A, B$ de $G$, on a $A + B = \{a + b : a \in A, b \in B\}$ désigne la somme de $A$ et $B$. Dans cet article, par monoïde, nous entendons toujours un semi-groupe commutatif si $a, b, c$ sont des éléments du monoïde avec $ab = ac$, alors $b = c$. En général, nous utilisons la notation multiplicative pour les monoïdes. Si nous voulons inclure le cas non commutatif, nous le soulignons explicitement et parlons de monoïdes non nécessairement commutatifs (ils ont toujours une identité et satisfont la loi d'annulation).

Un élément $a$ d'un monoïde $H$ est inversible s'il existe un élément $a'$ de $H$ tel que $aa' = 1_H$ où $1_H$ désigne l'identité de $H$. L'ensemble des éléments inversibles de $H$ est noté $H^\times$. Un monoïde réduit associé à $H$, noté $H_{\text{red}} = H/H^\times$ a pour seul élément inversible $1_H$. Un élément $a \in H$ est irréductible ou un atome (dans $H$) si $a = bc$ avec $b, c \in H$ implique que $b$ ou $c$ sont inversibles. L'ensemble des éléments irréductibles de $H$ est noté $\mathcal{A}(H)$. Un élément $p \in H/H^\times$ est dit premier si $p|bc$ avec $b, c \in H$ implique que $p|b$ ou $p|c$. L'ensemble des éléments premiers de $H$ est

noté $\mathcal{P}(H)$. Il n'est pas difficile de voir que $\mathcal{P}(H) \subseteq \mathcal{A}(H)$. En général, l'égalité n'est pas vraie. En effet, pour un monoïde atomique $H$ l'égalité est possible si et seulement si $H$ est factoriel, c'est-à-dire si chaque élément $a$ a une factorisation unique en éléments irréductibles.

Une séquence sur $P$ est formellement définie comme un élément de $\mathcal{F}(P)$ , le monoïde abélien libre sur $P$. Ainsi, pour une séquence $S \in \mathcal{F}(P)$, il existe unique $\nu_p \in \mathbb{N}_0$ egal à 0 tels que $S = \prod_{p \in P} p^{\nu_p}$. On appelle alors $\nu_p$ la multiplicité de $p$ dans $S$ ou encore sa valorisation $p$-adique de $S$. On la note $\mathsf{V}_p(S)$ Alternativement, il existe de façon ordonnée $(p_1, \ldots, p_l) \in P$ (pas nécessairement distincts) tels que $S = p_1 \cdots p_l$. De manière informelle, une séquence est une collection d'éléments de $P$ où les répétitions sont autorisées et où l'ordre des éléments est négligé. On peut aussi les appeler des séquences non ordonnées ou des multtiensembles. Nous appelons l'élément identité du monoïde de séquences, la séquence vide, et nous le désignons simplement par 1, sauf risque de confusion. De plus, nous désignons par $|S| = l$ la longueur de $S$. Formellement, une sous-séquence de $S$ est une séquence $T$ qui divise $S$ dans le monoïde de séquences, de sorte que $T = \prod_{i \in I} p_i$ pour $I \subseteq [1, l]$ . De plus, nous notons par $T^{-1}S$ la séquence accomplissant $(T^{-1}S)T = S$, c'est-à-dire $T^{-1}S = \prod_{i \in [1,l] \setminus I} p_i$.Cela correspond à l'idée intuitive d'une sous-séquence d'une séquence. Si $P'$ est un ensemble et $f : P \longrightarrow P'$ une application , alors f peut-être étendue à un homomorphisme de monoïdes de $\mathcal{F}(P)$ à $\mathcal{F}(P')$, que nous continuerons à désigner par $f$. En particulier,pour une séquence $S$ nous désignons par $-S$ la séquence où chaque terme $g$ dans $S$ est remplacé par $-g$.

On considère souvent des suites sur un sous-ensemble $G_0$ d'un groupe abélien. Dans ce cas, pour une séquence $S = g_1 \ldots g_l \in \mathcal{F}(G_0)$,on désigne par $\sigma(S) = \sum_{i=1}^{l} g_i$ sa somme, et l'ensemble $\sum(S) = \{\sigma(T) : 1 \neq T | S\}$ est appelé l'ensemble des sous-sommes (non vides) de $S$. Une suite dont la somme est 0, est appelée une séquence à somme nulle. La séquence $S$ est dite libre de somme nulle si $0 \notin \sum(S)$. L'ensemble de toutes les séquences sur $G_0$ qui sont des séquences à somme nulle est désigné par $\mathcal{B}(G_0)$ et il est facile de voir que $\mathcal{B}(G_0)$ un sous-monoïde de $\mathcal{F}(G_0)$. Si $G'$ est un groupe abélien et $f : G \longrightarrow G'$ est un homomorphisme de groupe, alors l'image de $\mathcal{B}(G)$ sur $f$ est contenue dans $\mathcal{B}(G')$.

Ensuite, nous rappelons la notion de séquences qui admettent une somme nulle pondérée. Généralement, on avait pris les ensembles d'entiers comme ensembles de poids. Pour $W \subseteq \mathbb{Z}$ un ensemble de poids, un élément de la forme $\sum_{i=1}^{l} w_i g_i$ avec $w_i \in W_i$ est appelé une somme pondérée $W$ de $S$. Pour notre application actuelle, une autre notion de poids plus générale est nécessaire. (voir [24]).

Pour un sous-ensemble $\Omega \subseteq End(G)$ d'endomorphismes du groupe abélien fini $G$, un élément $\sum_{i=1}^{l} \omega_i(g_i)$ avec $\omega_i \in \Omega$ est appelé somme $\Omega$ pondérée de $S$. Nous désignons par $\sigma_\Omega(S)$ l'ensemble de toutes les sommes pondérées $\Omega$ de $S$. Nous disons que $S$ admet une somme nulle pondérée $\Omega$ de $S$ si $0 \in \sigma_\Omega(S)$, nous appelons

aussi une telle séquence une somme nulle pondérée $\Omega$. Nous désignons l'ensemble de toutes les séquences à somme nulle $\Omega$ pondérées sur $G_0$ par $\mathcal{B}_\Omega(G_0)$. Explicitement, une séquence $S = g_1 \dots g_l$ avec $g_i \in G_0$ est dans $\mathcal{B}_\Omega(G_0)$ si il existe $\omega_i \in \Omega$ tel que $\omega_1(g_1) + \dots + \omega_l(g_l) = 0$. S'il n'y a pas de risque de confusion, nous nous contentons d'écrire $\omega g$ au lieu de $\omega(g)$.

Un élément est appelé somme partielle $\Omega$ pondérée de $S$ s'il est une somme $\Omega$ pondérée d'une sous-séquence non vide de $S$. Nous désignons l'ensemble de toutes les sommes partielles $\Omega$ pondérées de $S$ par $\sum_\Omega(S)$. La séquence $S$ est appelée libre de somme nulle $\Omega$ pondérée si $0 \notin \sum_\Omega(S)$. Dans ce contexte, nous appelons $\Omega$ ensemble de poids.

Pour voir le lien entre les deux notions, il suffit de rappeler que, pour un entier $w$, la multiplication par un entier $w$ induit un endomorphisme du groupe abélien $G$. Ainsi, ceci peut être considéré comme une généralisation de la notion de poids. Dans un souci d'exhaustivité, nous notons que différents entiers peuvent induire le même endomorphisme, en ce sens il ne s'agit pas d'une généralisation au sens très strict. Cependant, ceci est essentiellement sans conséquence dans notre contexte, et dans tous les cas, il est courant de ne considérer que les ensembles de poids intégraux qui ne contiennent pas d'entiers distincts qui sont congruents modulo l'exposant du groupe, auquel cas chaque entier donne un endomorphisme distinct. Ainsi, à toutes fins pratiques, cette dernière notion généralise la première notion de poids. Nous rappelons qu'il existe une notion encore plus générale de poids pour les séquences. A savoir, plutôt que des endomorphismes d'un groupe abélien, on considère des homomophismes entre deux groupes abéliens(voir [41]).

Le cas $\Omega = \{\mathsf{id}_G\}$ correspond au problème sans poids. Il faut cependant noter que $\sigma_{\mathsf{id}_G}(S)$ n'est pas $\sigma(S)$ mais $\{\sigma(S)\}$. En particulier lorsqu'il est utilisé comme indice, nous utilisons le symbole $\pm$ pour désigner l'ensemble des poids $\{+\mathsf{id}_G, -\mathsf{id}_G\}$, et nous utilisons la terminologie pondérée plus ou moins ou tout simplement pondérée $\pm$ pour désigner cet ensemble de poids. Nous écrivons habituellement $+\mathsf{id}_G$ au lieu de $\mathsf{id}_G$.

Nous rappelons quelques concepts supplémentaires de la théorie de la factorisation. Un monoïde $H$ est dit atomique si chaque élément non invertible de $H$ peut être écrit comme un produit fini d'éléments irréductibles. Le monoïde de factorisations de $H$, noté $\mathsf{Z}(H)$, est le monoïde $\mathcal{F}(\mathcal{A}(H_{\text{red}}))$. De manière informelle, les éléments du monoïde de factorisations correspondent à des factorisations d'éléments de $H$ en éléments irréductibles. Les factorisations qui ne diffèrent que par l'ordre des termes ou la multiplication par des unités étant considérées comme égales.

L'homomorphisme $\pi_H : \mathsf{Z}(H) \longrightarrow H_{\text{red}}$ , qui fait correspondre le produit formel $a_1 \cdots a_k$ à sa valeur, est appelé l'homomorphisme de factorisation. Il est surjectif si et seulement si $H$ est atomique. Pour $a \in H$, l'ensemble $\mathsf{Z}_H(a) = \pi_H^{-1}(aH^\times)$

est appelé l'ensemble des factorisations de $a$ dans $H$ ; si le monoïde $H$ est évident du contexte, nous supprimons $H$ de la notation. Pour $z \in \mathsf{Z}(H)$, on appelle $|z|$, qui est défini comme $\mathsf{Z}(H)$ un monoïde libre, la longueur de la factorisation. De manière informelle, c'est le nombre d'éléments irréductibles dans la factorisation où les multiplicités sont prises en compte. De plus, on appelle $\mathsf{L}_H(a) = \{|z| : z \in \mathsf{Z}_H(a)\}$ l'ensemble des longueurs de $a$ dans $H$. L'ensemble de longueurs de systèmes est defini par $\mathcal{L}(H) = \{\mathsf{L}_H(a) : a \in H\}$ Le monoïde est appelé monoïde de factorisation borné, monoïde BF en abrégé, si $\mathsf{L}_H(a)$ est finie pour chaque $a \in H$. De même, les monoïdes pour lesquels les ensembles de factorisations sont finis sont appelés monoïdes à factorisation finie. On note que $H$ est factoriel si et seulement si $|\mathsf{Z}_H(a)| = 1$ pour $a \in H$. on dit que $H$ est demi-factoriel si $|\mathsf{L}_H(a)| = 1$ pour chaque $a \in H$ . Soit $H$ et $\mathcal{B}$ des monoïdes. Un homomorphisme monoïde $\Theta : H \longrightarrow \mathcal{B}$ est appelé un homomorphisme de transfert lorsqu'il possède les deux propriétés suivantes :

— $\mathcal{B} = \Theta(H)\mathcal{B}^\times$ et $\Theta^{-1}(\mathcal{B}^\times) = H^\times$
— Si $u \in H$ et $b, c \in \mathcal{B}$ avec $\Theta(u) = bc$, alors il existe $v, w \in H$ tel que $u = vw$, $\Theta(v) \simeq b$ et $\Theta(w) \simeq c$

La pertinence de cette notion est due au fait qu'elle préserve de nombreuses propriétés arithmétiques. En particulier, si $\Theta : H \longrightarrow \mathcal{B}$ est un homomorphisme de transfert alors $\mathsf{L}_H(a) = \mathsf{L}_\mathcal{B}(\Theta(a))$, $\mathcal{L}(H) = \mathcal{L}(\mathcal{B})$. Nous nous référons, par exemple, à [14], section 1.3. Plus récemment, cette notion a été généralisée aux monoïdes non nécessairement commutatifs(Voir [4] (sans détails ici)). Il existe divers invariants arithmétiques qui sont dérivés des ensembles de longueurs. Nous rappelons quelques uns. Pour une présentation plus complète (voir par exemple, [15], [18], [21], [23]. Soit $k \in \mathbb{N}$ et soit $H$ un monoïde atomique. Pour éviter les complications dans les cas triviaux nous supposons que $H \neq H^\times$. Alors,

$$\mathcal{U}_k(H) = \bigcup_{\mathsf{L} \in \mathcal{L}(H), k \in \mathsf{L}} \mathsf{L}$$

désigne l'union des ensembles de longueur de $H$ contenant $k$. De plus, on fixe $\rho_k(H) = \sup \mathcal{U}_k(H)$ et $\lambda_k(H) = \min \mathcal{U}_k(H)$.

La valeur $\rho_k(H)$ est parfois appelée la $k^{ième}$ élasticité locale de $H$. Cette terminologie est dérivée de celle de l'élasticité d'un monoïde notée $\rho(H)$. Si $A \subseteq \mathbb{N}$, nous appellons $\rho(A) = \frac{\sup A}{\min A} \in \mathbb{Q}_{\geqslant 1} \cup \{\infty\}$,l'élasticité de $A$, et nous fixons $\rho(\{0\}) = 1$. L'élasticité d'un élément $a \in H$, notée $\rho(a)$ est juste $\rho(L_H(a))$. Enfin, l'élasticité de $H$, notée $\rho(H)$, est définie par $\sup\{\rho(a) : a \in H\} \in \mathbb{Q}_{\geqslant 1} \cup \{\infty\}$. Il n'est pas difficile de voir $\rho(H) = \lim_{k \to \infty} \frac{\rho_k(H)}{k}$.

Nous terminons en rappelant la définition de l'ensemble des distances (successives) d'un monoïde (voir,[22]).Nous ne l'étudions pas spécifiquement dans cet article , mais avons besoin de l'invoquer dans certains arguments. Pour $A \in \mathbb{Z}$,

on désigne par $\Delta(A)$ l'ensemble des distances (successives) de $A$, c'est-à-dire l'ensemble de tous les $d \in \mathbb{N}$ pour lesquels il existe un certain $l \in A$ tel que $A \cap [l, l+\mathsf{d}] = [l, l+\mathsf{d}]$. Clairement, $\Delta(A) \subseteq \{\mathsf{d}\}$ si et seulement si seulement si $A$ est une progression arithmétique de raison $d$. Un ensemble $A$ est appelé intervalle s'il est une progression arithmétique de raison 1. On définit $\Delta(H) = \cup_{a \in H} \Delta(L(a))$. Le monoïde est demi-factorial si et seulement si $\rho(H) = 1$ et si et seulement si $\Delta(H) = 0$.

Nous rappelons brièvement la notion de monoïde de Krull. Pour un sous-monoïde $H'$ d'un monoïde $H$, on dit que $H' \subseteq H$ est saturé lorsque $a|b$ dans $H$ et si et seulement si $a|b$ dans $H'$. Un monoïde $H$ qui est un sous-monoïde saturé d'un monoïde factoriel est appelé un monoïde de Krull. Il est bien connu qu'un monoïde de Krull admet un homomorphisme de transfert vers un monoïde de séquences à somme nulle sur son groupe de classe, plus précisément vers le monoïde de séquences à somme nulle sur les sous-ensembles de classes contenant des diviseurs premiers. Un monoïde est appelé Krull de transfert s'il admet un homomorphisme de transfert vers un monoïde de séquences à somme nulle (voir [14], section 4). De nombreux monoïdes d'intérêt arithmétique sont des monoïdes de Krull ou au moins des Krull de transfert, et ils sont sans doute la classe de monoïdes la plus étudiée en factorisation (voir [14], [23], [37]). Dans le présent article, ils ne jouent pas un rôle important et nous nous abstenons de donner plus de détails.

# 2 | Monoïdes de séquences sur des groupes abéliens finis définis par des sommes nulles par rapport à un ensemble donné de poids et applications aux factorisations des normes d'entiers algébriques

## 2.1 Résumé historique de l'article

L'étude de l'arithmétique des monoïdes de séquences à somme nulle sur des groupes abéliens finis est un sujet classique en raison de leur rôle crucial dans la compréhension de l'arithmétique des monoïdes de Krull (de transfert). Plus récemment, les séquences qui admettent, pour un ensemble donné de poids, une somme nulle pondérée ont reçu une attention particulière.Pourtant, l'accent a été mis sur les constantes de somme nulle plutôt que sur l'arithmétique des monoïdes formés par ces séquences. Nous commençons une étude systématique de l'arithmétique de ces monoïdes. Nous montrons que pour une large classe de poids, les unions d'ensembles de longueurs sont des intervalles et nous obtenons divers résultats sur l'élasticité de ces monoïdes. Des résultats plus détaillés sont obtenus pour le cas particulier des séquences pondérées. De plus,nous appliquons nos résultats pour obtenir des résultats sur les factorisations des normes des entiers algébriques.

## 2.2 Introduction

L'étude des séquences à somme nulle sur les groupes abéliens (finis) est très considérée actuellement (voir [13],[18],chapitres 5 et 6, [24], partie II, [39], chapitre 9). Nous rappelons qu'une collection d'éléments $g_1 \dots g_l$ d'un groupe abélien fini $(G, +, 0_G)$ est dit de somme nulle si la somme de tous ces éléments est la somme nulle c'est-à-dire $g_1 + \cdots + g_l = 0_G$. Si tous les éléments $g_i$ sont distincts, alors l'un d'entre eux est un élément neutre. Les éléments $g_i$ sont distincts, on parle alors d'un ensemble à somme nulle. Si les éléments ne sont pas supposés être distincts, alors on parle d'une suite à somme nulle.

Cependant, on ne tient généralement pas compte de l'ordre des éléments de la suite. Formellement, les séquences dans notre contexte sont des éléments d'un monoïde libre abélien.Pour cela, nous privilégions le terme séquence. Ce sont des éléments du monoïde abélien libre sur $G$. Nous nous référons à la section 2 pour plus de détails. Outre l'étude des constantes à somme nulle telles que la constante Erdős-Ginzburg-Ziv et la constante de Davenport. Des efforts considérables ont été consacrés à l'étude de l'arithmétique des monoïdes de suites à somme nulle sur des groupes abéliens, principalement des groupes abéliens finis. Une raison principale est qu'ils constituent une classe importante de monoïdes auxiliaires dans la théorie de la factorisation (voir, [14],[15],[18]). Tout monoïde de Krull, en particulier le monoïde multiplicatif de tout domaine de Dedekind admet un homomorphisme de transfert vers un monoïde de séquences à somme nulle. Une autre raison est qu'il s'agit de monoïdes faciles à décrire mais qui présentent des phénomènes riches en ce qui concerne leur arithmétique. Ces dernières années, l'étude des problèmes à somme nulle a été étendue en introduisant des poids. Intuitivement, cela signifie

qu'au lieu de considérer simplement la somme des éléments, on écrit par exemple, si l'on autorise les poids de l'ensemble $\{1, 3\}$, cela signifie qu'il faut considérer des sommes de la forme $\sum_{i=1}^{l} w_i g_i$ ou $w_i \in \{1, 3\}$, c'est-à-dire que l'on peut attribuer un poids différent à certains éléments en choisissant une valeur différente $w_i$ égal à 3 plutot que 1. Bien sûr, dans un groupe abélien fini, le poids doit être compris de manière figurative. Mais nous rappelons qu'un premier exemple de problème à somme nulle est né de la question de l'existence de points d'un treillis intégral dont le barycentre est à nouveau un point du treillis [27]. Dans ce contexte, l'idée d'attribuer des poids différents aux points aurait un sens plus littéral. Il s'avère que pour certaines applications, une notion plus générale de poids est pertinente. La généralisation devient intuitive, lorsqu'on interprète pour un entier $w$ la notion de **la multiplication** par $w$ comme un endomorphisme du groupe abélien $G$. Ensuite, l'idée de permettre tout endomorphisme de $G$ comme un poids, plutôt que seulement ceux induits par la multiplication par un entier devient très naturelle. Des généralisations de la notion de poids même au-delà de cela sont possibles et apparaissent dans la littérature, mais nous ne les considérons pas dans le présent document (voir [41] et [24], chapitre 16). Cette généralisation, introduisant les poids, a suscité un intérêt considérable (voir, par exemple, [1], [2]). Ces recherches se sont toutefois concentrées sur l'étude des constantes à somme nulle. Dans cet article, nous commençons une étude des monoïdes de séquences sur des groupes abéliens finis qui admettent des sommes nulles avec des poids. Pour une définition précise, voir la section 2. Après avoir rassemblé les principales définitions, nous étudions les propriétés algébriques de base de ces monoïdes. Ensuite, nous étudions en détail certains invariants arithmétiques classiques de ces monoïdes, à savoir les élasticités (voir, par exemple, [3],[11],[17], [28]) et les unions d'ensembles de longueurs (voir, par exemple, [10], [12]). Il s'avère que ces recherches présentent des similitudes avec celles de l'arithmétique des séquences de produit sur les groupes non abéliens (voir les récents travaux de l'auteur [16], [34]). Nous terminons en montrant que nos résultats ne sont pas seulement une généralisation naturelle de résultats existants, mais qu'ils ont aussi des applications réelles. Nous donnons une application arithmétique dans la section 2.7, à savoir que nous montrons que ces monoïdes apparaissent lors de l'étude des monoïdes de normes d'entiers algébriques, une connexion étroitement liée apparaît déjà dans [25] et, plus implicitement, dans [33], section 9.2.

## 2.3 Les monoïde des séquences admettant une somme nulle $\Omega$ pondérée

L'objectif de cette section est d'introduire des monoïdes de séquences sur un groupe abélien fini $G$ qui admettent une somme nulle pondérée $\Omega$ pour un ensemble général de poids $\Omega \subseteq \mathsf{End}(G)$ et d'établir les premiers résultats sur leur arithmétique. Nous établissons l'ensemble des résultats généraux. Dans la section 5, nous affinerons certains de ces résultats. Dans la section 2.6, nous obtenons des résultats plus détaillés pour le cas des poids $\pm$ c'est-à-dire pour le cas particulier $\Omega = \{+\mathsf{id}_G, -\mathsf{id}_G\}$.

On désigne, pour $G_0$ un sous-ensemble d'un groupe abélien fini, par $\mathcal{B}_\Omega(G_0) = \{S \in \mathcal{F}(G_0) : 0 \in \sigma_\Omega(S)\}$ l'ensemble des suites sur $G_0$ qui admettent une somme nulle $\Omega$ pondérée sur $G_0$. Comme nous l'avons déjà remarqué de telles séquences sont également appelées séquences à somme nulle $\Omega$ pondérée , et l'on peut donc parler de $\mathcal{B}_\Omega(G_0)$ comme l'ensemble des suites à somme nulle $\Omega$ pondérée. Pour éviter toute confusion, nous soulignons que ce sont les sommes qui sont pondérées et non les séquences elles-mêmes, les éléments de $\mathcal{B}_\Omega(G_0)$ sont simplement des séquences sur $G_0$, c'est-à-dire $\mathcal{B}_\Omega(G_0) \subseteq \mathcal{F}(G_0)$.

Notant que $\sigma_\Omega(S_1S_2) = \sigma_\Omega(S_1) + \sigma_\Omega(S_2)$ et $\sigma_\Omega(1_{\mathcal{F}(G_0)}) = \{0\}$, il s'ensuit que $\mathcal{B}_\Omega(G_0)$ est un sous-monoïde de $\mathcal{F}(G_0)$ puisque $\{\omega(\sigma(S)) : \omega \in \Omega\} \subseteq \sigma_\Omega(S)$, il s'ensuit que si $0 = \sigma(S)$, donc $0 \in \sigma(S)$ donc $\mathcal{B}(G_0) \subseteq \mathcal{B}_\Omega(G_0)$.

$\mathcal{B}_\Omega(G_0)$ est un sous-monoïde du monoïde libre $\mathcal{F}(G_0)$ , il s'ensuit que $\mathcal{B}_\Omega(G_0)$ est atomique et même un BF-monoïde (voir [18], Corollaire 1.3.3). Nous montrons que $\mathcal{B}_\Omega(G_0)$ est un monoide de type fini, ce qui donne divers résultats de finitude supplémentaires pour $\mathcal{B}_\Omega(G_0)$. Par définition, une séquence $S \in \mathcal{B}_\Omega(G_0)\backslash\{1\}$ est irréductible dans $\mathcal{B}_\Omega(G_0)$, autrement dit $S \in \mathcal{A}(\mathcal{B}_\Omega(G_0))$ s'il n'est pas possible d'écrire $S = S_1S_2$ avec $S_1, S_2 \in \mathcal{B}_\Omega(G_0)\backslash\{1\}$. Nous appelons une telle séquence une séquence minimale $\Omega$ pondérée à somme nulle. Nous soulignons que, contrairement au problème sans poids, cette définition n'équivaut pas, en général, à dire que la séquence $S$ à somme nulle pondérée $\Omega$ n'a pas de sous-séquence appropriée et non vide $\Omega$ pondérée. En d'autres termes, il est possible que $S = S_1T$ avec $S, S_1 \in \mathcal{B}_\Omega(G_0)$ et $T \in \mathcal{F}$ mais $T \notin \mathcal{B}_\Omega(G_0)$. Cela est dû au fait que $\rho_\Omega(S_1), \rho_\Omega(T)$ sont des sous-ensembles de $G$ et il est bien possible que pour les sous-ensembles $A, B$ d'un groupe abélien on a $0 \in A + B = \{a + b : a \in A, b \in B\}$ et $0 \in A$ mais $0 \notin B$ alors que pour les éléments $a, b \in G$ bien sûr, $0 = a + b$ et $a = 0$ implique $0 = b$. C'est-à-dire que $\mathcal{B}_\Omega(G_0)$ n'est pas nécessairement un sous-monoïde saturé de $\mathcal{F}(G_0)$ , et donc pas nécessairement Krull. Bien sûr, dans certains cas spécifiques, il peut encore être Krull. Nous discutons de ce problème vers la fin de cette section.

Les constantes de Davenport jouent un rôle important dans les recherches sur l'arithmétique des monoïdes de séquences à somme nulle. Comme mentionné plus

haut, il existe diverses recherches sur les constantes de Davenport avec des poids. Cependant, il faut être prudent car ces constantes ne répondent pas aux constantes les plus pertinentes dans le contexte actuel. Pour expliquer cette situation, nous rappelons deux définitions de Cziszter, Domokos et Geroldinger [8], section 2.5.

Soit $H$ un monoïde BF et soit $|.| : H \longrightarrow (\mathbb{N}_0, +)$ est un homomorphisme de monoïdes, qui dans ce qui, dans ce contexte, est appelé une fonction de degré, par exemple, si $H$ est un sous-ensemble d'un monoïde libre, alors la fonction de longueur habituelle est une fonction de degré. Alors, pour $k \in \mathbb{N}$, la $k^{ième}$ grande constante de Davenport de $H$(par rapport à la fonction de degré donnée) est définie comme $\sup\{|a| : a \in \mathcal{M}_k\}$ où $\mathcal{M}_k = \{a \in H : \max \mathsf{L}(a) \leqslant k\}$. Pour $k = 1$, l'indice est supprimé et $\mathsf{D}(H) = D_1(H)$ est appelée la constante de Davenport de $H$.

Soit $H$ un sous-monoïde d'un monoïde libre $F$ et que $|.|$ désigne la fonction de longueur habituelle sur $F$, et, pour $k \in \mathbb{N}$, $M_k^*$ est l'ensemble de tous les $f \in F$ tels que $f$ n'est pas divisible (dans $F$) par un produit de $k$ éléments non inversibles dans $H$. La kième petite constante de Davenport de $H$, notée $d_k(H)$, est définie comme $\sup\{|f| : f \in \mathcal{M}_k^*\}$. Encore une fois, pour $k = 1$, on écrit simplement $d(H)$ et on l'appelle la petite constante de Davenport de $H$. De la définition, il en résulte que $1 + d_k(H)$ est le plus petit $l \in \mathbb{N} \cup \{\infty\}$ pour chaque tout $f \in F$ de longueur au moins $l$ soit divisible (dans $F$) par un produit de $k$ non-unités dans $H$.

Dans de nombreuses situations courantes, il est vrai que $1 + \mathsf{d}_k \leqslant \mathsf{D}_k(H)$ et même rarement l'égalité est vraie. C'est notamment le cas pour $H = \mathcal{B}(G)$, ce qui permet d'utiliser les deux définitions de façons interchangeables. Cependant, en général, ce n'est pas vrai et il est même possible que $\mathsf{d}_k(H)$ soit supérieur à $\mathsf{D}_k(H)$. En particulier, la constante de Davenport avec poids que l'on trouve habituellement dans la littérature et qui est souvent désignée par $\mathsf{D}_\Omega(G)$, est en fait $1+\mathsf{d}(\mathcal{B}_\Omega(G))$, mais pas $\mathsf{D}(\mathcal{B}_\Omega(G))$. Compte tenu de cela, pour éviter tout risque de confusion, nous utilisons systématiquement la notation des monoïdes, et nous n'utilisons pas la notation abrégée habituelle qui permet d'éviter les erreurs de notation. Nous rappelons un résultat de finitude bien connu pour la constante de Davenport (voir, par exemple, [18], Théorème 3.4.2).

**Proposition 2.3.1**
Soit $G$ un groupe abélien et soit $G_0 \subseteq G$ un sous-ensemble fini. Alors $\mathsf{D}(\mathcal{B}(G_0))$ est fini. Nous montrons ensuite, pour des sous-ensembles de groupes abéliens finis, que $\mathsf{D}(\mathcal{B}_\Omega(G_0))$ est borné au-dessus par $\mathsf{D}(\mathcal{B}(G))$.

**Lemme 2.3.1**
Soit $G$ un groupe abélien fini et $G_0 \subseteq G$ est un ensemble fini. Alors $\mathsf{D}(\mathcal{B}_\Omega(G_0)) \leqslant \mathsf{D}(\mathcal{B}(G))$. De plus, $\mathcal{A}(\mathcal{B}_\Omega(G_0)) \cap \mathcal{B}(G_0) \subseteq \mathcal{A}(\mathcal{B}(G))$.

**Démonstration :**
Soit $g_1 \dots g_l$ une séquence dans $\mathcal{A}(\mathcal{B}_\Omega(G_0))$. Alors pour chaque $i \in [1, l]$, il existe

un certain $\omega_i \in \Omega$ tel que $\sum_{i=1}^{l} w_i g_i = 0$. Nous affirmons que $(\omega_1 g_1)\dots(\omega_i g_i) \in \mathcal{A}(\mathcal{B}(G))$.Par construction, la somme de la séquence est 0. Il reste à montrer que c'est une séquence à somme nulle minimale. Supposons au contraire qu'il existe $\theta \neq I \subsetneq [1,l]$ tel que $\prod_{i\in I}(\omega_i g_i)$ et $\prod_{i\in[1,l]\setminus I}(\omega_i g_i)$ sont des séquences à somme nulle. Alors $(\prod_{i\in I} g_i)$ et $(\prod_{i\in[1,l]\setminus I} g_i)$ sont des suites à somme nulle $\Omega$ pondérées. Contradiction.

Ainsi, pour chaque $S \in \mathcal{A}(\mathcal{B}_\Omega(G_0))$, il existe un $S' \in \mathcal{A}(\mathcal{B}(G))$ de même longueur. Ceci implique directement que $D(\mathcal{B}_\Omega(G_0))) \leqslant D(\mathcal{B}(G))$. L'affirmation supplémentaire est facilement visible en rappelant que $\mathcal{B}(G_0) \subseteq \mathcal{B}_\Omega(G_0)$ et donc chaque factorisation dans $\mathcal{B}(G_0)$ permet d'obtenir $\mathcal{B}_\Omega(G_0)$. ■

**Théorème 2.3.1**
Soit $G$ un groupe abélien fini. Alors $1 + \mathsf{d}(\mathcal{B}_\Omega(G)) \leqslant \mathsf{D}(\mathcal{B}_\Omega(G)) \leqslant \mathsf{D}(\mathcal{B}(G))$.

**Démonstration :**
Par le lemme 2.3.1, nous avons $\mathsf{D}(\mathcal{B}_\Omega(G)) \leqslant \mathsf{D}(\mathcal{B}(G))$. Nous montrons maintenant que $1 + \mathsf{d}(\mathcal{B}_\Omega(G)) \leqslant \mathsf{D}(\mathcal{B}_\Omega(G))$. Soit $S$ une séquence de longueur $l = \mathsf{D}(\mathcal{B}_\Omega(G))$ . Nous montrons qu'elle a une sous-séquence à somme nulle pondérée $\Omega$. Nous considérons la séquence $(-\sigma(S))S$, qui est dans $\mathcal{B}(G)$ et donc aussi dans $\mathcal{B}_\Omega(G)$ par l'inclusion $\mathcal{B}(G) \subseteq \mathcal{B}_\Omega(G)$. Or, $|(-\sigma(S))S| > \mathsf{D}(\mathcal{B}_\Omega(G)$. Par conséquent, ce n'est pas une suite minimale à somme nulle pondérée $\Omega$ et il existe des $S_1, S_2 \in \mathcal{B}_\Omega(G)$ non vides tels que $(-\sigma(S))S = S_1S_2$.Il s'ensuit que $S_1$ ou $S_2$ est une sous-séquence de $S$, ce qui établit qu'elle a une somme nulle pondérée $\Omega$ non vide.

Nous avons donc établi que toute séquence de longueur $\mathsf{D}(\mathcal{B}_\Omega(G))$ a une sous-séquence non vide à somme nulle $\Omega$ pondérée. Puisque, par définition, $1+\mathsf{d}(\mathcal{B}_\Omega(G))$ est le plus petit entier positif ayant cette propriété, nous avons $1 + \mathsf{d}(\mathcal{B}_\Omega(G)) \leqslant \mathsf{D}(\mathcal{B}_\Omega(G))$. ■

**Corollaire 2.3.1**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G$. Soit $\Omega \subseteq \mathsf{End}(G)$ est un ensemble de poids. Le monoïde $\mathcal{B}_\Omega(G_0)$ est finiment engendré.

**Démonstration :**
Puisque la longueur des éléments de $\mathcal{A}(\mathcal{B}_\Omega(G_0))$ est bornée par $\mathsf{D}(\mathcal{B}_\Omega(G_0))$, qui est finie par le lemme 2.3.1, il s'ensuit que l'ensemble $\mathcal{A}(\mathcal{B}_\Omega(G_0))$ est fini, c'est-à-dire que le monoïde est finiment engendré.

Ce résultat a des conséquences immédiates et fortes sur l'arithmétique de ces monoïdes que nous discutons ci-dessous. Cependant, nous établissons d'abord une autre borne inférieure sur la constante de Davenport dont nous aurons besoin par la suite. ■

**Lemme 2.3.2**
Soit $G = G_1 \oplus G_2$ un groupe abélien fini. Soit $\Omega \subseteq \mathsf{End}(G)$ un ensemble d'endomorphismes qui forme un groupe par composition et tel que $\omega(G_i) \subseteq G_i$ pour $i \in \{1, 2\}$. Alors $\mathsf{D}(\mathcal{B}_\Omega(G)) \geqslant \mathsf{D}(\mathcal{B}_\Omega(G_1)) + \mathsf{D}(\mathcal{B}_\Omega(G_2)) - 1$.

**Démonstration :**
Pour $i \in \{1, 2\}$, soit $A_i$ un élément de $\mathcal{A}(\mathcal{B}_\Omega(G_i))$ de longueur maximale. De plus, soit $g_i$ un élément fixe de $A_i$ et soit $A_i = g_i F_i$. Puisque $0 \in \sigma_\Omega(A_i)$ pour $i \in \{1, 2\}$, il existe $\omega_i \in \Omega$ tel que $\omega_i g_i \in -\sigma_\Omega(F_i)$. On considère $A = (\omega_1 g_1 + \omega_2 g_2) F_1 F_2$ et on affirme qu'il est contenu dans $\mathcal{A}(\mathcal{B}_\Omega(G)))$. Nous commençons par montrer que $0 \in \sigma_\Omega(A)$. Puisque $\Omega$ est un groupe, il existe $\epsilon \in \Omega$ tel que $\epsilon \circ \omega_i = \omega_i$ pour $i \in \{1, 2\}$.

Or, $\epsilon(\omega_1 g_1 + \omega_1 g_1) \in -(\sigma_\Omega(F_1) + \sigma_\Omega(F_2)) = -(\sigma_\Omega(F_1 F_2))$, implique que $0 \in \sigma_\Omega(A)$. Il reste à montrer qu'il n'existe pas de décomposition $A = A'A''$ avec $A'$ et $A''$ non vides telle que $0 \in \sigma_\Omega(A')$ et $0 \in \sigma_\Omega(A'')$. Supposons au contraire qu'une telle décomposition existe. Sans perte de généralité, nous pouvons supposer que $\omega_1 g_1 + \omega_2 g_2$ apparaît dans $A'$. Nous écrivons $A' = (\omega_1 g_1 + \omega_2 g_2) F_1' F_2'$ et$A'' = F_1'' F_2''$ ou $F_i = F_i' F_i''$ pour $i \in \{1, 2\}$.

Puisque $0 \in \sigma_\Omega(A'')$ et $\sigma_\Omega(F_i'') \subseteq G_i$ pour $i \in [1, 2]$, $0 \in \sigma_\Omega(F_i'')$. De plus, il existe est $\omega \in \Omega$ tel que $\omega(\omega_1 g_1 + \omega_2 g_2) \in -\sigma_\Omega(F_1' F_2')$ . Il s'ensuit que $\omega(\omega_i g_i) \in -\sigma_\Omega(F_i')$ pour $i \in [1, 2]$ . Or, puisque $\omega o \omega_i \in \Omega$, cela implique que $0 \in \sigma_\Omega(g_i F_i')$. Donc, $A_i = (g_i F_i') F_i''$ et $0 \in \sigma_\Omega(g_i F_i')$ et $0 \in \sigma_\Omega(F_i'')$. Puisqu'au moins l'un des $F_1''$ et $F_2''$ est non vide et que $g_1 F_1'$ et $g_2 F_2'$ ,toutes deux non vides, nous obtenons une contradiction avec le fait que $A_1$ ou $A_2$ soit irréductible. ■
Nous passons maintenant à l'arithmétique des monoïdes de suites à somme nulle pondérée.

**Théorème 2.3.2**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G$. Soit $\Omega \subseteq \mathsf{End}(G)$ un ensemble de poids. Soit $H = \mathcal{B}_\Omega(G_0)$.

1. L'ensemble $\Delta(H)$ et la constante $\rho(H)$ sont finis.
2. Il existe $M \in \mathbb{N}_0$ tel que chaque ensemble de longueurs $L$ de $H$ est une progression multiprogression avec une borne $M$ et de différence $d \in \Delta(H) \cup \{0\}$, c'est-à-dire que $L = y + (L_1 \cup L^* \cup (\max L^* + L_2)) \subseteq y + \mathcal{D} + d\mathbb{Z}$, $\{0, d\} \subseteq \mathcal{D} \subseteq [0, d]$, $-L_1, L_2 \subseteq [1, M]$, $\min L^* = 0$ et $L^* = [0, \max L^*] \cap \mathcal{D} + d\mathbb{Z}$.
3. Il existe $M' \in \mathbb{N}_0$ tel que chaque $k \in \mathbb{N}_0$ l'ensemble $\mathcal{U}_k(H)$ soit une progression avec une borne $M'$ et de différence $d' = \min \Delta(H)$, c'est-à-dire que $\mathcal{U}_k(H) = y' + (U_1 \cup U^* \cup (\max U^* + U_2)) \subseteq y' + d'\mathbb{Z}$ avec $y' \in \mathbb{N}_0$, $-U_1, U_2 \subseteq [1, M']$, $\min U^* = 0$ et $U^* = [0, \max U^*] \cap d'\mathbb{Z}$.

**Démonstration :**
Par le corollaire 2.3.1, le monoïde est finiment engendré. L'affirmation découle maintenant de résultats sur monoïdes finiment engendrés, voir en particulier [18], Théorèmes 2.3.1 et 2.3.2, et pour la partie finale, voir [10], theorème 2.3.1. ■
On sait aussi que divers autres invariants arithmétiques de $H$ sont finis, notamment le degré caténaire $\mathsf{c}(H)$ et le degré $\mathsf{t}(H)$, en particulier le monoïde est localement simplifié ; de plus, dans le résultat ci-dessus l'ensemble des distances $\Delta(H)$ peut être remplacé par $\Delta^*(H)$ et on sait que l'élasticité est acceptée. Nous renvoyons aux références mentionnées dans la preuve juste au-dessus et à [23], section 3. Nous rappelons que le deuxième point du résultat est appelé théorème de structure pour les ensembles de longueurs, tandis que le troisième est appelé théorème de structure pour les unions. Dans la section 5, nous affinons le théorème de structure des unions pour cette classe de monoïdes en montrant que, pour une large classe de poids, le théorème de structure des unions ne s'applique pas et les ensembles sont effectivement des progressions arithmétiques, avec la différence 1, c'est-à-dire des intervalles d'entiers.

Nous terminons cette section par quelques résultats algébriques supplémentaires sur ces monoïdes. Nous montrons qu'en général, ils ne sont pas des monoïdes de Krull, ni même des monoïdes de Krull de transfert. Cependant, ils sont toujours des C-monoïdes. Nous renvoyons à [18], section 2.9 pour une définition. Pour le cas particulier des suites à somme nulle pondérée plus-moins, il est possible de caractériser complètement quand un tel monoïde est Krull et Krull de transfert. Ceci est fait dans la proposition 2.3.1, qui est due à Geroldinger et Zhong incluant l'idée principale du lemme qui la précède.

**Lemme 2.3.3**
Soit $G$ un groupe abélien avec $\exp(G) \geqslant 3$. Soit $\Omega$ un ensemble de poids tel que $\{+\mathsf{id}_G, -\mathsf{id}_G\} \subseteq \Omega \subseteq \mathsf{Aut}(G)$. Alors $\mathcal{B}_\Omega(G)$ n'est pas un monoïde de Krull de transfert.

**Démonstration :**
Supposons au contraire qu'il existe un homomorphisme de transfert $\theta : \mathcal{B}_\Omega(G) \longrightarrow \mathcal{B}(G_0)$ où $G_0$ est un sous-ensemble de tout groupe abélien. Soit $g \in G$ avec $\mathsf{ord}(g) \geqslant 3$. Nous observons que

$$A_1 = g^2, A_2 = (2g)^2, \text{ et } A_3 = g^2(2g)$$

sont des atomes de $\mathcal{B}_\Omega(G)$, en effet, le fait que $A_1, A_2, A_3 \in \mathcal{B}_\Omega(G)$ découle de $\{+\mathsf{id}_G, -\mathsf{id}_G\} \subseteq \Omega$, le fait qu'ils sont irréductibles, car $\omega(g)$ et $\omega(2g)$ sont non nuls pour chaque $\omega \in \Omega$. Puisque $A_3^2 = A_1^2 A_2$, on a $\theta(A_3^2) = \theta(A_1^2 A_2)$ et il s'ensuit que

$$\theta(A_3)^2 = \theta(A_1)^2\theta(A_2) \in \mathcal{B}(G_0) \subseteq \mathcal{F}(G_0).$$

Par conséquent, $\theta(A_1)^2$ divise $\theta(A_3)^2$ dans $\mathcal{F}(G_0)$ et donc $\theta(A_1)$ divise $\theta(A_3)$ dans $\mathcal{F}(G_0)$. Ceci implique que $\theta(A_1)$ divise $\theta(A_3)$ dans $\mathcal{B}(G_0)$ et donc $\theta(A_1) = \theta(A_3)$ (car les deux éléments sont des atomes). On obtient donc $\theta(A_2) = 1$, ce qui est en contradiction avec la première condition de la définition de l'homomorphisme de transfert. ■

**Proposition 2.3.2**
Soient $G$ un groupe abélien et $\mathcal{B}_{\pm}(G)$ le monoïde des suites à somme $\pm$ nulle. Alors les affirmations suivantes sont équivalentes :

1. $G$ est un 2-groupe élémentaire.
2. $\mathcal{B}_{\pm}(G)$ est un monoïde de Krull.
3. $\mathcal{B}_{\pm}(G)$ est un monoïde de transfert de Krull.

**Démonstration :**

— $(a) \Rightarrow (b)$ Si $G$ est un 2-groupe élémentaire, alors $\mathcal{B}_{\pm}(G) = \mathcal{B}(G)$ comme $-g = g$ pour chaque $g \in G$, et $\mathcal{B}(G)$ est un monoïde de Krull.
— $(b) \Rightarrow (c)$ Évident.
— $(c) \Rightarrow (a)$ Puisque les conditions sur l'ensemble des poids du lemme 2.3.2 sont vérifiées, $\mathcal{B}_{\pm}(G)$ ne peut être qu'un transfert de monoïde de Krull lorsque $G$ ne contient aucun élément d'ordre au moins 3, c'est-à-dire que $G$ est 2-groupe élémentaire.

Autrement dit, à moins que $\mathcal{B}_{\pm}(G) = \mathcal{B}(G)$, le monoïde $\mathcal{B}_{\pm}(G)$ n'est pas un monoïde de Krull. Cependant,nous montrons maintenant que pour un ensemble abélien fini $G$ et $\Omega$ un ensemble de poids, le monoïde $\mathcal{B}_{\Omega}(G)$ est un C-monoïde. À cette fin, nous rappelons un résultat de Cziszter, Domokos et Geroldinger [8], Proposition 2.3.2 dans un cas particulier. ■

**Proposition 2.3.3**
Soit $H$ un monoïde de type fini et réduit. Supposons que $H$ soit un sous-monoïde d'un monoïde libre $\mathcal{F}(P)$. Les affirmations suivantes sont équivalentes :

1. $H$ est un C-monoïde défini dans $\mathcal{F}(P)$ et pour tout $p \in P$ il existe un $a \in H$ tel que $\mathsf{V}_p(a) > 0$.
2. Pour tout $a \in \mathcal{F}(P)$, il existe un $n_a \in \mathbb{N}$ tel que $a^{n_a} \in H$.

**Théorème 2.3.3**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G$. Soit $\Omega \subseteq \mathsf{End}(G)$ un ensemble de poids. Le monoïde $\mathcal{B}_{\Omega}(G_0)$ est un C-monoïde défini dans $\mathcal{F}(G_0)$.

**Démonstration :**
Par la proposition 2.3.3, il suffit de montrer que pour $S \in \mathcal{F}(G_0)$ il existe $n \in \mathbb{N}$ tel que $S^n \in \mathcal{B}_\Omega(G_0)$. Soit $\omega \in \Omega$. On note $n$ le plus petit commun multiple de $\{\mathsf{ord}(\omega(g)) : g|S\}$. Alors $0 = \sigma(\omega(S^n)) \in \sigma_\Omega(S^n)$. ■

## 2.4 Quelques résultats généraux auxiliaires

Nous rassemblons quelques résultats qui sont utiles pour nos investigations mais qui ne sont pas spécifiques aux monoïdes de séquences à somme nulle (pondérée). Pour la plupart, ils concernent les ensembles $\mathcal{U}_k$ et des notions connexes(Voir [14], Lemme 2.3.3 pour plus de détails).

**Lemme 2.4.1**
Soit $H$ un monoïde atomique avec $k, l \in \mathbb{N}_0$ . Alors les affirmations suivantes sont vraies.

1. $\mathcal{U}_k(H) = \{k\}$ pour $k \in \{0, 1\}$ et $k \in \mathcal{U}_k(H)$ pour tout $k \in \mathbb{N}$.
2. Pour $k, l \in \mathbb{N}$, on a $l \in \mathcal{U}_k(H)$ si et seulement si $k \in \mathcal{U}_l(H)$.
3. $\mathcal{U}_k(H) + \mathcal{U}_l(H) \subseteq \mathcal{U}_{k+l}(H)$.
4. $\lambda_{k+l}(H) \leqslant \lambda_k(H) + \lambda_l(H) \leqslant k + l \leqslant \rho_k(H) + \rho_l(H) \leqslant \rho_{k+l}(H)$.
5. $\rho_k(H) \leqslant k\rho(H)$ et $k \leqslant \lambda_k(H)\rho(H)$.

Nous faisons quelques observations générales supplémentaires sur ces constantes.

**Lemme 2.4.2**
Soit $H$ un monoïde atomique. Soit $k \in \mathbb{N}$.

1. $\rho_{\lambda_k(H)}(H) \geqslant k$.
2. Si $\rho_k(H)$ est fini, alors $\lambda_{\rho_k(H)}(H) \leqslant k$.

**Démonstration :**

1. Puisque par définition $\lambda_k(H) \in \mathcal{U}_k(H)$, il résulte du lemme 2.4.1 que $k \in \mathcal{U}_{\lambda_k(H)}(H)$. Puisque par définition $\rho_{\lambda_k(H)}(H) = \sup \mathcal{U}_{\lambda_k(H)}(H)$, il est donc évident que $\rho_{\lambda_k(H)}(H) \geqslant k$.
2. Puisque $\rho_k(H)$ est fini, nous avons $\rho_k \in \mathcal{U}_k(H)$ et encore une fois par le Lemme 2.4.1 $k \in \mathcal{U}_{\rho_k(H)}(H)$ et donc $\lambda_{\rho_k(H)}(H) \leqslant k$.

■

**Lemme 2.4.3**
Soit $H$ un monoïde atomique. Soit $k \in \mathbb{N}$. Supposons que $\mathcal{U}_i(H)$ soit un intervalle pour chaque $i \leqslant k$. Alors, nous avons $\lambda_k(H) = \min\{i : \rho_i(H) \geqslant k\}$.

**Démonstration :**
Soit $j \in \mathbb{N}$ minimal tel que $\rho_j(H) \geqslant k$, notons que puisque $\rho_k(H) \geqslant k$ d'après le lemme 2.4.1 $j$ existe et $j \leqslant k$.

Puisque $j \leqslant k \leqslant \rho j(H)$ et que $\mathcal{U}_j(H)$ est un intervalle, il s'ensuit que $k \in \mathcal{U}_j(H)$. Ainsi, par le lemme 2.4.1 nous avons $j \in \mathcal{U}_k(H)$ et donc $\lambda_k(H) \leqslant j$. Puisque par le lemme 2.4.1, nous avons $\rho_{\lambda_k(H)}(H) \geqslant k$, il s'ensuit que $\min\{i : \rho_i(H) \geqslant k\} \leqslant \lambda_k(H)$. ■

**Lemme 2.4.4**
Soit $H$ un monoïde atomique. Soit $k \in \mathbb{N}$. Supposons que $\mathcal{U}_i(H)$soit un intervalle pour chaque $i \leqslant k$. Alors $\rho_k(H) = \sup\{i : \lambda_i(H) \leqslant k\}$.

**Démonstration :**
Soit $j \in \mathbb{N}$ avec $j \geqslant k$ tel que $\lambda_j(H) \leqslant k$ pour chaque $j$. Puisque $\lambda_j(H) \leqslant k \leqslant j$ et $\mathcal{U}_j(H)$ est un intervalle, il s'ensuit que $k \in \mathcal{U}_j(H)$. Ainsi, par le Lemme 2.4.1, nous avons $j \in \mathcal{U}_k(H)$ et donc $\rho_k(H) \geqslant j$. : Ainsi, $\rho_k(H) \geqslant \sup\{i : \lambda_i(H) \leqslant k\}$. Si $\sup\{i : \lambda_i(H) \leqslant k\}$ est infini, il s'ensuit que $\rho_k(H) = \infty$. Supposons que $\sup\{i : \lambda_i(H) \leqslant k\}$ soit fini et que $j > \sup\{i : \lambda_i(H) \leqslant k\}$. Supposons que $\rho_k(H) \geqslant j$. Puisque $\mathcal{U}_k(H)$ est un intervalle, il s'ensuit que $j \in \mathcal{U}_k(H)$. Or, cela implique que $k \in \mathcal{U}_j(H)$ et donc $k \geqslant \lambda_j(H)$, ce qui est en contradiction avec $j > \sup\{i : \lambda_i(H) \leqslant k\}$. Ainsi $\rho_k(H) < j$. ■
Le lemme suivant est une légère généralisation de [34], lemme 2.4.2.

**Lemme 2.4.5**
Soit $P$ un ensemble et soit $S_1, \ldots, S_k, T_1, \ldots, T_l \in \mathcal{F}(P)$ des suites non vides telles que

$$S_1, \ldots, S_k = T_1, \ldots, T_l.$$

Si $k < l$, alors il existe $i_0 \in [1, k]$ et distincts $j_1, j_2 \in [1, l]$ tels qu'il existe $p_1, p_2 \in P$ satisfaisant $p_1 | T_{j_1}, p_2 | T_{j_2}$ et $p_1 p_2 | S_{i_0}$.

**Démonstration :**
On suppose que $k < l$ et on procède par induction sur $k$. On fixe $k = 1$. Supposons que pour deux $h, h'$ avec $hh' | S_1$, il n'y a pas de $j, j' \in [1, l]$, tels que $h | T_j$ et $h' | T_{j'}$. Il s'ensuit que $S_1 = S_k | T_j$ pour $j \in [1, l]$ et $S_k | T_l$. Nous obtenons

$$1_{\mathcal{F}(G)} = T_1 T_2 \ldots (T_l S_k^{-1})$$

.

Une contradiction puisque $T_1$ n'est pas vide. Supposons maintenant $k \geqslant 2$ et supposons que l'affirmation est vraie pour $k-1$. On a $S_1, \ldots, S_k = T_1, \ldots, T_l$, comme précédemment on obtient que $S_k | T_l$. Nous considérons $S_1, \ldots, S_{k-1} = T_1, \ldots, T_{l-1}(T_l S_k^{-1})$. Maintenant, on peut suivre l'hypothèse d'induction appliquée à : $S_1, \ldots, S_{k-1} = T_1, \ldots, T_{l-1}(T_l S_k^{-1})$ ■

Dans le lemme ci-dessous, qui est essentiellement dans [3] voir en particulier le théorème 2.3.2 et dans [18],Proposition 2.3.3, nous adoptons la convention que $a/0 = \infty$ pour $a \in \mathbb{R}_{\geqslant 0} \cup \{\infty\}$. Notons que la condition que $H$ n'est pas factoriel, garantit que $\mathcal{A}(H)/\mathcal{P}(H) \neq \varnothing$. Bien sûr, pour un monoïde factoriel $H$ on a $\rho(H) = 1$ et donc rien n'est perdu en excluant ce cas.

**Lemme 2.4.6**

Soit $H$ un monoïde atomique qui n'est pas factoriel. Soit $r : H \longrightarrow (\mathbb{R}_{\geqslant 0}, +)$ un homomorphisme de monoïde.

1. Soit $r_1 = \inf\{r(a) : a \in \mathcal{A}(H)\}$ et soit $R_1 = \sup\{r(a) : a \in \mathcal{A}(H)\}$. Alors $\rho(H) \leqslant R_1/r_1$.
2. Soit $r_2 = \inf\{r(a) : a \in \mathcal{A}(H)/\mathcal{P}(H)\}$ et soit $R_2 = \sup\{r(a) : a \in \mathcal{A}(H)/\mathcal{P}(H)\}$. Alors $\rho(H) \leqslant R_2/r_2$.

**Démonstration :**

Puisque $r$ est un homomorphisme de monoïde, il s'ensuit que $r(u) = 0$ pour chaque $u \in H^\times$. Sans perte de généralité, nous pouvons supposer que le monoïde est réduit.

1. Soit $a_1, \ldots, a_k, b_1, \ldots, b_l \in \mathcal{A}(H)$ tels que $a_1 \ldots a_k = b_1 \ldots b_l$. Il suffit de montrer que $l/k \leqslant \frac{R_1}{r_1}$. Puisque ceci est trivialement vrai pour $r_1 = 0$, on peut supposer que $r_1 > 0$ . On note que

   $$kR_1 \geqslant r(a_1) + \cdots + r(a_k) = r(a_1 \cdots a_k) = r(b_1 \cdots b_l) = r(b_1 + \cdots + r(b_l) \geqslant lr_1,$$

2. Soit $a_1, \ldots, a_k, b_1, \ldots, b_l \in \mathcal{A}(H)$ tels que $a_1 \ldots a_k = b_1 \ldots b_l$. Il suffit de montrer que $l/k \leqslant \frac{R_2}{r_2}$ . Comme ci-dessus, nous pouvons supposer que $r_2 > 0$ : De plus, nous pouvons supposer $l \geqslant k$. Supposons d'abord q'aucun $a_1, \ldots, a_k, b_1, \ldots, b_l$ est premier. Alors, bien sûr, nous pouvons conclure

   $$kR_2 \geqslant r(a_1) + \cdots + r(a_k) = r(a_1 \cdots a_k) = r(b_1 \ldots b_l) = r(b_1 + \cdots + r(b_l) \geqslant lr_2$$

Supposons que ce ne soit pas le cas, disons, en renumérotant si nécessaire, que $a_{(k-r)-1}, \ldots, a_k$ sont premiers alors que $a_1, \ldots, a_{k-r}$ ne sont pas premiers. Il s'ensuit, en renumérotant si nécessaire, que $a_{k-r+i} = b_{l-r+i}$ pour chaque $1 \leqslant i \leqslant r$ et que $a_1 \ldots a_{k-r} = b_1 \ldots b_{l-r}$. On remarque que si l'un des $b_j$ pour $j \in [1, l]$ est premier, également l'un des $a_i$ pour $i \in [1, l-r]$ serait premier. Ainsi, aucun des $a_1, \ldots, a_{k-r}, b_1, \ldots, b_{l-r}$ est premier. Si $k - r = 0$, alors $k = l$ et la borne tient clairement. On suppose que $k - r \neq 0$. On obtient comme ci-dessus

$$(k-r)R_2 \geqslant (l-r)r_2$$

Et ainsi

$$\tfrac{l-r}{k-r} \leqslant \tfrac{R_2}{r_2}.$$

Maintenant, on note pour $l' \geqslant k' > r' \geqslant 0$, on a $\frac{l'}{k'} \leqslant \frac{l'-r'}{k'-r'}$ Ainsi

$$\tfrac{l}{k} \leqslant \tfrac{l-r}{k-r} \leqslant \tfrac{R_2}{r_2}.$$

La preuve est ainsi terminée. ■

## 2.5 Résultats sur $\mathcal{U}_k(H)$ pour les monoïdes de séquences à somme nulle pondérée

Le but de cette section est d'obtenir divers résultats pour $\mathcal{U}_k(H)$ pour les monoïdes de séquences $\Omega$ pondérées à somme nulle qui vont au-delà de ce qui a déjà été établi dans le théorème 2.3.3. Tout d'abord, nous établissons que, sous certaines hypothèses sur les poids, ces ensembles sont des intervalles, c'est-à-dire des progressions arithmétiques avec la raison 1. Nous étudions ensuite les maxima et les minima de ces ensembles, à savoir $\rho_k(H)$ et $\lambda_k(H)$, ce qui donne une description complète de ces ensembles. Pour la preuve de nos résultats, nous utilisons les résultats de la section 3 de [12] qui sont valables pour $\mathcal{B}_\Omega(G)$, nous les résumons dans le lemme suivant.

**Lemme 2.5.1**
Soit $H$ un monoïde atomique. On suppose que $\Delta(H) \neq \varnothing$ et $d = \min \Delta(H)$. Alors on a :

1. $\Delta(\mathcal{U}_k(H)) \subseteq d\mathbb{N}$, et il existe $k^* \in \mathbb{N}$ pour chaque $\min \Delta(\mathcal{U}_k(H)) = d$ pour tout $k \geqslant k^*$.
2. $\sup \Delta(\mathcal{U}_k(H)) \leqslant \sup \Delta(H)$ pour tout $k \in \mathbb{N}$.
3. Si $k \in \mathbb{N}$ et $\mathcal{U}_m(H) \cap \mathbb{N}_{\geqslant m}$ est une progression arithmétique de raison $d$ pour tous les $m \in [\lambda_k(H), k]$, $\mathcal{U}_k(H) \cap [0, k]$ est une progression arithmétique de raison $d$.
4. Les affirmations suivantes sont équivalentes :
   (a) $\mathcal{U}_k(H) \cap \mathbb{N}_{\geqslant k}$ est une progression arithmétique de raison $d$ pour tout $k \in \mathbb{N}$.
   (b) $\mathcal{U}_k(H)$ est une progression arithmétique de raison $d$ pour tout $k \in \mathbb{N}$.

Nous montrons que les ensembles $\mathcal{U}_k(\mathcal{B}_\Omega(G))$ sont des intervalles si l'ensemble des poids $\Omega \subseteq \mathsf{End}(G)$ est un groupe par rapport à la composition des endomorphismes. Nous soulignons que $\Omega$ peut être un groupe tout en ne contenant pas $\mathsf{id}_G$, ce qui complique légèrement l'argument. En effet, dans d'autres résultats, nous supposons en plus que $\mathsf{id}_G \in \Omega$, en d'autres termes, nous faisons l'hypothèse plus forte que $\Omega$ est un sous-groupe de $Aut(G)$.

**Théorème 2.5.1**
Soit $G$ un groupe abélien fini. Soit $\Omega \subseteq \mathsf{End}(G)$. Si $\Omega$ est un groupe par rapport à la composition d'endomorphismes, alors $\mathcal{U}_k(\mathcal{B}_\Omega(G))$ un intervalle pour chaque $k \in \mathbb{N}$.

**Démonstration :**
Par le lemme 2.4.2, il suffit de montrer que $\mathcal{U}_k(\mathcal{B}_\Omega(G))$ est un intervalle pour chaque $k \in \mathbb{N}$. Cela signifie que nous devons montrer que $[k, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Soit $l \in [k, \rho_k(\mathcal{B}_\Omega(G))]$ minimal tel que $[l, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Ceci est bien défini car bien sûr pour $l = \rho_k(\mathcal{B}_\Omega(G))$ nous avons $[l, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Nous voulons montrer que $l = k$. Supposons au contraire que $l > k$. Nous considérons l'ensemble de tous les $B \in \mathcal{B}_\Omega(G)$ avec $\{k, j\} \subseteq \mathsf{L}(B)$ pour $j \geqslant l$. Soit $B_0$ un tel élément tel que $|B_0|$ est minimal parmi tous ces éléments. Maintenant, soit $B_0 = U_1 \dots U_k = V_1 \dots V_j$. Par le lemme 2.4.1, après renumérotation, nous pouvons supposer qu'il y a

$$g_1 g_2 | U_1 \text{ tel que } g_1 | V_{j-1} \text{ et } g_2 | V_j.$$

Soit $\omega_i \in \Omega$ tel que $\sum_{i=1}^{|U_1|} \omega_i g_i = 0$. Soit $g_0 = \omega_1 g_1 + \omega_2 g_2$. On met $U_1' = g_0 (g_1 g_2)^{-1} U_1$ et $V_{j-1}' = g_0 V_{j-1} V_j (g_1 g_2)^{-1}$. On note que $-g_0 = -(\omega_1 g_1 + \omega_2 g_2) \in \sigma_\omega((g_1 g_2)^{-1} U_1)$. Puisque $\Omega$ est un groupe, il s'ensuit que $\omega(-g_0) \in \sigma_\Omega((g_1 g_2)^{-1} U_1)$ pour chaque $\omega \in \Omega$. Par conséquent, nous avons $0 \in \sigma_\Omega(U_1')$. Nous affirmons que $0 \in \rho_\Omega(V_{j-1}')$ est également valable. Pour le voir, notons que $0 \in \sigma_\Omega(V_{j-1}')$ implique $-\omega_1' g_1 \in \sigma_\Omega(g_1^{-1} V_{j-1})$ pour $\omega_1' \in \Omega$. Puisque $\Omega$ est un groupe, il s'ensuit que $-\omega_1' g_1 \in \sigma_\Omega(G)$. Puisque $\Omega$ est un groupe, il s'ensuit que $-\omega_1' g_1 \in \sigma_\Omega(g_1^{-1} V_{j-1})$ pour tout $\omega_1' \in \Omega$ en particulier $-\omega_1 g_1 \in \sigma_\Omega(g_1^{-1} V_{j-1})$. De la même façon, on obtient $-\omega_2 g_2 \in \sigma_\Omega(g_2^{-1} V_j)$. Ainsi, $-g_0 = -(w_1 g_1 + \omega_2 g_2) \in \sigma_\Omega(V_{j-1} V_j (g_1 g_2)^{-1})$ et puisque $\Omega$ est un groupe, on a $\omega(-g_0) \in \sigma_\Omega(V_{j-1} V_j (g_1 g_2)^{-1})$ pour $\omega \in \Omega$. Donc $0 \in \sigma_\Omega(V_{j-1}')$. Ainsi, $U_1', V_{j-1}' \in \mathcal{B}_\Omega(G)$. En effet, $U_1'$ est dans $\mathcal{A}(\mathcal{B}_\Omega(G))$ car une factorisation de $U_1'$ serait directement une factorisation de $U_1$. Pour $V_{j-1}'$, ceci n'est pas clair à ce stade. Soit

$$B_0' = U_1' U_2 \dots U_k = V_1 \dots V_{j-2} V_{j-1}' \ .$$

Il est clair que $B_0' \in \mathcal{B}_\Omega(G)$ et que $|B_0'| < |B_0|$. Puisque $U_1'$ est un atome, il s'ensuit que $k \in \mathsf{L}(B_0')$. Par notre hypothèse sur $B_0$, il s'ensuit donc que $\mathsf{L}(B_0')$ ne

contient aucun élément supérieur ou égal à $l$, c'est-à-dire $\max \mathsf{L}(B'_0) < l$. Puisque $B'_0 = V_1 \dots V_{j-2} V'_{j-1}$, il s'ensuit que $j - 2 + \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) < l$.

Comme $V'_{j-1}$ n'est pas la suite vide, $\max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) \geqslant 1$. Enfin $j \geqslant l$, donne la chaîne d'inégalités suivante : $l - 2 + 1 \leqslant j - 2 + \max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) < l$ . Ainsi, $j-2+\max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) = l-1$ et $k \in \mathsf{L}(B'_0)$ aussi. Il s'ensuit que $l-1 \in \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Ainsi, $[l-1, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Contradiction avec la définition de $l$. ■

Nous procédons à l'établissement d'un résultat qui est utile pour les recherches sur les élasticités et les problèmes connexes.

**Lemme 2.5.2**

Soit $G$ un groupe abélien fini. Soit $\Omega \subseteq \mathsf{End}(G)$ et soit $j \in [2, \mathsf{D}(\mathcal{B}_\Omega(G))]$.

1. Si $\Omega$ est un semi-groupe par rapport à la composition, alors il existe un certain $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ avec $|A| = j$.
2. $\Omega \subseteq \mathsf{End}(G)$ est un sous-groupe, alors il existe $B \in \mathcal{B}_\Omega(G)$ tel que $\{2, j\} \subseteq \mathsf{L}(B)$.

**Démonstration :**

1. Soit $C \in \mathcal{A}(\mathcal{B}_\Omega(G))$ avec une longueur $l = \mathsf{D}(\mathcal{B}_\omega(G))$. Supposons que $C = \prod_{i=1}^{l} g_i$ et $\sum_{i=1}^{l} \omega_i g_i = 0$ avec $\omega_i \in \Omega$. Soit $s = \sum_{i=1}^{l-j+1} \omega_i g_i$ et $A = s \prod_{i=l-j+2}^{l} g_i$. Alors, $A \in \mathcal{B}_\Omega(G)$, puisque pour $\omega \in \Omega$, on a $\omega(\sum_{i=1}^{l-j+1} \omega_i(g_i) = 0$ et donc $\omega(s) + \sum_{i=l-j+2}^{l} (\omega \circ \omega_i)(g_i) = 0$. De plus, il s'ensuit que que $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$, puisqu'une factorisation non triviale de $A$ donnerait directement une factorisation non triviale de $C$, notez que nous avons encore besoin que $\Omega$ soit un semi-groupe. Puisque $|A = j|$, ceci prouve la première affirmation.
2. Soit $C \in \mathcal{A}(\mathcal{B}_\Omega(G))$ avec $|A| = j$ . Notons que $0 \nmid A$. Il est facile de voir $-A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ . Nous considérons $B = (-A)A$. Par définition $2 \in \mathsf{L}(B)$.Pour chaque $g \in G$, on a $(-g)g \in \mathcal{B}_\Omega(G)$. Puisque $\omega \in \Omega$ est un endomorphisme de $G$, on a toujours $\omega(-g) = -\omega(g)$. Puisque $\Omega$ ne contient que des monomorphismes, il s'ensuit que $(-g)g \in \mathcal{A}(\mathcal{B}_\Omega(G))$. Donc $\max \mathsf{L}(B) = |A|$ et l'affirmation est établie.

■

**Lemme 2.5.3**

Soit $G$ un groupe abélien fini. Soit $\Omega \subseteq \mathsf{End}(G)$. Soit $k \in \mathbb{N}$. Alors $\rho_{2k}(\mathcal{B}_\Omega(G)) \geqslant kD(\mathcal{B}_\Omega(G))$ et $\rho_{2k+1}(\mathcal{B}_\Omega(G)) \geqslant 1 + kD(\mathcal{B}_\Omega(G))$.

**Démonstration :**

Soit $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ de longueur maximale. On sait que Soit $-A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ et

on considère $B = (-A)^k A$. Par définition, $2k \in \mathsf{L}(B)$.Puisque pour chaque $g \in G$, on a $(-g)g \in \mathcal{B}_\Omega(G)$ (notez que $\omega \in \Omega$ est un endomorphisme de $G$ on a toujours $\omega(-g) = -\omega(g)$). Il s'ensuit que $\max \mathsf{L}(B) \geqslant k|A|$ et l'affirmation est établie. La deuxième affirmation est une conséquence immédiate de la première, par exemple, on peut considérer $0B$.

Nous voulons maintenant utiliser le lemme 2.4.1 pour établir que $\rho_{2k}(\mathcal{B}_\Omega(G)) = k\mathsf{D}(\mathcal{B}_\Omega(G))$ dans divers cas. Pour cela, il est utile d'avoir une borne inférieure sur la longueur d'un atome qui n'est pas premier. L'exemple suivant donne un atome de longueur 1 qui n'est pas premier. Cependant, pour divers ensembles de poids, nous pouvons montrer que la longueur d'un atome qui n'est pas premier est au moins 2, ce qui nous permet d'établir l'égalité mentionnée ci-dessus. ■

**Exemple 2.5.1**
Soit $G = C_2 \oplus C_6$ et soit $e_1, e_2 \in G$ soient indépendants avec $\mathsf{ord}(e_1) = 2$ et $\mathsf{ord}(e_2) = 6$. Soit $\Omega = \{+2\mathsf{id}_G, +\mathsf{id}_G, -\mathsf{id}_G\}$. Alors $e_1$ est dans $\mathcal{A}(\mathcal{B}_\Omega(G))$ car $2\mathsf{id}_G(e_1) = 0$. Mais $e_1$ n'est pas $\mathcal{P}(\mathcal{B}_\Omega(G))$ car $e_1 \nmid e_1(e_1+e_2)e_2$ alors $e_1|(e_1(e_1+e_2)e_2)^2$. Cependant, sous certaines conditions sur l'ensemble des poids, cela reste vrai. ▮

**Lemme 2.5.4**
Soient $G$ un groupe abélien fini, $\Omega \subseteq End(G)$ et $A \in \mathcal{A}(\mathcal{B}_\Omega(G))\mathcal{P}(\mathcal{B}_\Omega(G))$.

1. Si $\Omega$ ne contient que des monomorphismes, alors $|A| \geqslant 2$.
2. Si $\Omega$ est un semi-groupe commutatif par rapport à la composition, alors $|A| \geqslant 2$.

**Démonstration :**
Supposons que $\Omega$ ne contient que des monomorphismes. Il s'ensuit directement que les seuls éléments dans $\mathcal{B}_\Omega(G)$ longueur inférieure à 2 sont la suite vide et la suite 0. La première n'est pas dans $\mathcal{A}(\mathcal{B}_\Omega(G))$ tandis que la seconde est dans $\mathcal{P}(\mathcal{B}_\Omega(G))$ et la première affirmation suit.

Supposons maintenant que $\Omega$ est fermé par composition. Supposons qu'il existe un atome de longueur 1, disons que, pour $a \in G$, on a $a \in \mathcal{B}_\Omega(G))$. Cela signifie qu'il existe $\omega' \in \Omega$ tel que $\omega'(a) = 0$. Nous devons montrer que $a \in \mathcal{P}(\mathcal{B}_\Omega(G))$. Soit $C, D \in \mathcal{B}_\Omega(G)$ tel que $a|CD$ (la divisibilité tient en $\mathcal{B}_\Omega(G)$). Nous avons besoin d'affirmer que $a|C$ ou $a|D$ (dans $\mathcal{B}_\Omega(G)$). Sans perte de généralité, nous pouvons supposer que $C$ contient $a$, c'est-à-dire que $a$ divise $C$ dans $\mathcal{F}(G)$. Nous devons montrer que $a$ divise $C$ dans $\mathcal{B}_\Omega(G)$. Soit $C = af_1 \dots f_r$. Nous savons qu'il existe $\omega_0, \omega_1, \dots, \omega_r$ tel que $\omega_0(a), \omega_1(f_1), \cdots, \omega_r(f_r) = 0$. Nous appliquons $\omega'$ à cette expression et obtenons $(\omega'\omega_0)(a) + (\omega'\omega_1)(f_1) + \dots, (\omega'\omega_r)(f_r) = 0$. Donc $(\omega'\omega_0)(a) = (\omega'\omega_0)(a) = \omega_0(0) = 0$. Donc , $(\omega'\omega_1)(f_1) + \cdots, (\omega'\omega_r)(f_r) = 0$ et puisque $\omega'\omega_i \in \Omega$ pour tout $i \in [1, r]$, il s'ensuit que $f_1 \dots f_r \in \mathcal{B}_\Omega(G)$. ■

Les résultats établis jusqu'ici permettent pour déterminer les divers ensembles de poids $\Omega$ les constantes $\rho_k(\mathcal{B}_\Omega(G))$ pour $k$ pair. Le cas des $k$ impairs est plus complexe et nous l'abordons pour le cas particulier des poids plus-moins dans la section suivante.

**Théorème 2.5.2**
Soit $G$ un groupe abélien fini. Soit $\Omega \subseteq End(G)$. Si $\Omega$ ne contient que des monomorphismes ou si $\Omega$ est un semi-groupe commutatif, par rapport à la composition, alors $\rho_{2k}(\mathcal{B}_\Omega(G)) = k\mathsf{D}(\mathcal{B}_\Omega(G))$ pour chaque $k \in \mathbb{N}$, de plus,

$$1 + k\mathsf{D}(\mathcal{B}_\Omega(G)) \leqslant \rho_{2k+1}(\mathcal{B}_\Omega(G)) \leqslant k\mathsf{D}(\mathcal{B}_\Omega(G)) + \left\lfloor \frac{\mathsf{D}(\mathcal{B}_\Omega(G))}{2} \right\rfloor.$$

En particulier, dans ce cas $\rho(\mathcal{B}_\Omega(G)) = \frac{\mathsf{D}(\mathcal{B}_\Omega)}{2}$.

**Démonstration :**
Les bornes inférieures sont établies par le lemme 2.4.2. Les bornes supérieures découlent des lemmes 2.4.1 et 2.4.2. L'affirmation finale est une conséquence directe des bornes et du fait que $\rho(H) = \sup_{k\in\mathbb{N}} \rho_k(H)/k$. Le résultat suivant est connu pour les monoïdes de suites à somme nulle sans poids (voir [14], Corollaire 2.3.1). La structure de notre preuve est très similaire à la version sans poids. ■

**Théorème 2.5.3**
Soit $G$ un groupe abélien fini. Soit $\Omega \subseteq Aut(G)$ un sous-groupe. Soit $\mathsf{D}$ la constante de Davenport de $\mathcal{B}_\Omega(G)$ et supposons que $\mathsf{D} \geqslant 2$. Alors, pour $k \in \mathbb{N}_0$, en laissant $l \in \mathbb{N}_0$ et $j \in [0, \mathsf{D}-1]$ tel que $k = l\mathsf{D} + j$, nous avons

$$\lambda_k(\mathcal{B}_\Omega(G)) = \begin{cases} 2l & \text{si } j = 0 \\ 2l+1 & \text{si } j \in [1, \rho_{2l+1}(\mathcal{B}_\Omega(G)) - l\mathsf{D}] \\ 2l+2 & \text{si } j \in [\rho_{2l+1}(\mathcal{B}_\Omega(G)) - l\mathsf{D} + 1, \mathsf{D}-1] \end{cases}$$

**Démonstration :**
Pour $|G| = 2$, le monoïde $\mathcal{B}_\Omega(G)$ est demi-factoriel. Donc $\mathcal{U}_k(\mathcal{B}_\Omega(G)) = \{k\}$ pour chaque $k$ et l'affirmation est fondamentalement triviale. Notons que par hypothèse $\mathsf{D} = 2$ (et non 1).

Si $l = 0$, alors pour $j \in [0, 1]$ on a $\mathcal{U}_j(\mathcal{B}_\Omega(G)) = \{j\}$ et l affirmation est établie. Pour $j \in [2, \mathsf{D}-1]$, nous savons par le lemme 2.4.2 qu'il existe un ensemble de longueurs qui contient $\{2, j\}$. Ceci montre que $\lambda_j(\mathcal{B}_\Omega(G)) \leqslant 2$. Puisque pour $j \geqslant 2$, on a que $\lambda_j(\mathcal{B}_\Omega(G)) \geqslant 2$, l'affirmation est établie.

On peut donc supposer que $l \geqslant 1$. Si $j = 0$, l'affirmation est une conséquence du théorème 2.5.2. Pour voir ceci, notons que, puisque $\rho_{2l}(\mathcal{B}_\Omega(G)) =$

$l\mathsf{D}(\mathcal{B}_\Omega(G))$, il existe un ensemble de longueurs $L$ avec $\{2l, l\mathsf{D}\} \subseteq L$. Ceci montre que $\lambda_{l\mathsf{D}}(\mathcal{B}_\Omega(G)) \leqslant 2l$. De plus, il ne peut exister un $L'$ avec $\{l', l\mathsf{D}\} \subseteq L$ pour $l' < 2l$ car $l\mathsf{D}/l'$ dépasserait l'élasticité $\mathsf{D}/2$ du monoïde $\mathcal{B}_\Omega(G)$. Donc $\lambda_{l\mathsf{D}}(\mathcal{B}_\Omega(G)) = 2l$.

Supposons que $j \geqslant 1$. Puisque $k \leqslant \lambda_k(\mathcal{B}_\Omega(G))\rho(\mathcal{B}_\Omega(G))$ par le lemme 2.4.1, il s'ensuit que pour $k = l\mathsf{D} + j$, on a

$$2l + \frac{2J}{\mathsf{D}} = \frac{l\mathsf{D}+j}{\frac{\mathsf{D}}{2}} \leqslant \lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G))$$

En particulier $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) \geqslant 2l$ et donc $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) \geqslant 2l + 1$. Dans l'autre sens, nous avons par le lemme 2.4.1 que

$$\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) \leqslant \lambda_{l\mathsf{D}}(\mathcal{B}_\Omega(G)) + \lambda_j(\mathcal{B}_\Omega(G)) \leqslant 2l + \lambda_j(\mathcal{B}_\Omega(G)) \leqslant 2l + 2$$

où nous avons utilisé que $\lambda_{l\mathsf{D}}(\mathcal{B}_\Omega(G)) = 2l$ et $\lambda_j(\mathcal{B}_\Omega(G)) \leqslant 2$ comme déjà établi. Pour $j = 1$, nous obtenons $2l < \lambda_{l\mathsf{D}+1}(\mathcal{B}_\Omega(G)) \leqslant 2l + \lambda_1(\mathcal{B}_\Omega(G)) = 2l + 1$, et donc $\lambda_{l\mathsf{D}+1}(\mathcal{B}_\Omega(G)) = 2l + 1$. Nous supposons que $j \geqslant 2$, si $j \in [2, \rho_{2l+1}(\mathcal{B}_\Omega(G)) - l\mathsf{D}]$, alors $j + l\mathsf{D} \leqslant \rho_{2l+1}(\mathcal{B}_\Omega(G))$, puisque $\mathcal{U}_{2l+1}(\mathcal{B}_\Omega(G))$ est un intervalle par le théorème 2.5.2, cela implique que $j + l\mathsf{D} \in \mathcal{U}_{2l+1}(\mathcal{B}_\Omega(G))$ et donc que $\mathcal{U}_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) \leqslant 2l + 1$, ce qui montre que $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) = 2l + 1$.

Si $j > \rho_{2l+1}(\mathcal{B}_\Omega(G)) - l\mathsf{D}$, alors $j + l\mathsf{D} > \rho_{2l+1}(\mathcal{B}_\Omega(G))$, ceci implique que $j + l\mathsf{D} \notin \mathcal{U}_{2l+1}(\mathcal{B}_\Omega(G))$ et donc $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) > 2l + 1$, ce qui montre que $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) = 2l + 2$. ■

## 2.6 Résultats des séquences pondérées

L'objectif de cette section est d'établir d'autres résultats sur $\mathcal{B}_\Omega(G)$ dans le cas spécifique où l'ensemble des poids est égal à $\{+\mathsf{id}_G, -\mathsf{id}_G\}$, que nous appelons séquences à somme nulle pondérée plus-moins.Nous désignons cet ensemble de poids à l'aide de l'indice $\pm$, c'est-à-dire que $\mathcal{B}_\pm(G)$ signifie $\mathcal{B}_{\{+\mathsf{id}_G, -\mathsf{id}_G\}}(G)$. Puisque $\{+\mathsf{id}_G, -\mathsf{id}_G\}$ est un sous-groupe commutatif de $Aut(G)$, les résultats de la section précédente sont applicables, et nous savons que pour $G$ un groupe abélien fini :

— $\mathcal{U}_k(\mathcal{B}_\pm(G))$ est un intervalle pour $k \in \mathbb{N}$ (voir Théorème 2.5.2)

— $\rho_{2k}(\mathcal{B}_\pm(G)) = kD(\mathcal{B}_\pm(G))$ pour $k \in \mathbb{N}$ (voir Théorème 2.5.2)

Nous allons d'une part étudier la valeur réelle de $D(\mathcal{B}_\Omega(G))$, et d'autre part étudier la valeur de $\rho_k(\mathcal{B}_\pm(G))$ pour $k$ impair. Il s'avère que les résultats dépendent de la parité de l'ordre du groupe.

Nous commençons par étudier l'ensemble des atomes de $\mathcal{B}_\pm(G))$ Nous avons remarqué à la section 3 que $\mathcal{A}(\mathcal{B}_\pm(G)) \cap \mathcal{B}(G) \subseteq \mathcal{A}(\mathcal{B}_\Omega(G))$. Inversement, s'il est clair que $\mathcal{A}(\mathcal{B}(G)) \subseteq \mathcal{B}_\pm(G)$, les éléments de $\mathcal{A}(\mathcal{B}(G))$, qui sont irréductibles dans le monoïde $\mathcal{B}(G)$, pourraient bien ne pas être irréductibles dans $\mathcal{B}_\pm(G))$ plus large.

Par exemple, dans $C_4 = \langle e \rangle$, la suite $e^4$ est une suite minimale à somme nulle sur $C_4$, c'est-à-dire $e^4 \in \mathcal{A}(\mathcal{B}(C_4))$. Cependant, dans $\mathcal{B}_{\pm}(C_4)$, elle admet la factorisation $e^2 \cdot e^2$. Nous montrons que pour les groupes d'ordre impair cela n'arrive jamais.

**Théorème 2.6.1**
Soit $G$ un groupe abélien tel que $|G|$ est impair. Alors, $\mathcal{A}(\mathcal{B}(G)) \subseteq \mathcal{A}(\mathcal{B}_{\pm}(G))$.

**Démonstration :**
Soit $A \in \mathcal{A}(\mathcal{B}(G))$. Puisque $\mathcal{B}(G) \subseteq \mathcal{B}_{\pm}(G)$, il s'ensuit que $A \in \mathcal{B}_{\pm}(G)$. Supposons au contraire que $A = A_1A_2$ avec $A_1$ et $A_2$ non vides tels que $0 \in \sigma_{\pm}(A_1)$ et $0 \in \sigma_{\pm}(A_2)$. On peut maintenant décomposer $A_1$ et $A_2$ selon le choix des poids qui conduisent à la somme zéro. Cette décomposition peut ne pas être unique. Soit $A_1 = A_1^+A_1^-$ telle que $0 = \sigma_{\pm}(A_1^+) - \sigma_{\pm}(A_1^-)$, et de même pour $A_2$. Donc $\sigma_{\pm}(A_1^+) = \sigma_{\pm}(A_1^-)$ et $\sigma_{\pm}(A_2^+) = \sigma_{\pm}(A_2^-)$. Nous avons $A = A_1^+A_1^-A_2^+A_2^-$. Nous introduisons quelques notations abrégée $\sigma_{\pm}(A_1^-) = s_1^-$, $\sigma_{\pm}(A_1^+) = s_1^+$, $\sigma_{\pm}(A_2^-) = s_2^-$, $\sigma_{\pm}(A_2^+) = s_2^+$. Nous avons noté que $s_1^+ = s_1^-$ et $s_2^+ = s_2^-$. Puisque $\rho(A) = 0$, il s'ensuit que $s_1^+ + s_1^- + s_2^+ + s_2^- = 0$. Par conséquent, on a $s_1^+ + s_1^+ + s_2^+ + s_2^+ = 0$, c'est-à-dire $2s_1^+ + 2s_2^+ = 0$. Cela signifie que $2(s_1^+ + s_2^+) = 0$ et puisque l'ordre de $G$ est impair, nous avons $s_1^+ + s_2^+ = 0$. Par conséquent, $A_1^+A_2^+$ est une sous-séquence à somme nulle de $A$ (sans poids). Puisque A est une séquence minimale à somme nulle, ce n'est possible que lorsque $A_1^+A_2^+$ est vide ou égal à $A$. Il en va de même pour $A_1^+A_2^-$, $A_1^-A_2^+$, $A_1^-A_2^-$. Or, exactement l'un de $A_1^+A_2^+$ et $A_1^-A_2^-$ est égal à $A$ et l'autre est vide. Par symétrie, on peut supposer que $A_1^+A_2^+ = A$ et $A_1^-A_2^-$ est vide. Or, alors $A_1^+$ et $A_2^+$ sont des suites à somme nulle avec ou sans poids et $A = A_1^+A_2^+$, ce qui est contradictoire. ■

En particulier, le résultat ci-dessus montre que dans le cas où l'ordre de $G$ est impair, l'inclusion $\mathcal{A}(\mathcal{B}_{\pm}(G)) \cap \mathcal{B}(G) \subseteq \mathcal{A}(\mathcal{B}(G))$ est une égalité. Cependant, cela n'implique pas que $\mathcal{A}(\mathcal{B}_{\pm}(G)) = \mathcal{A}(\mathcal{B}(G))$ car, en général, il existe des éléments dans $\mathcal{A}(\mathcal{B}_{\pm}(G))$ qui ne sont pas dans $\mathcal{B}(G)$. Par exemple, pour $C_3 = \langle e \rangle$, nous avons que $e^2 \in \mathcal{A}(\mathcal{B}_{\pm}(C_3))$ mais $e^2 \notin \mathcal{B}(C_3)$.

Comme corollaire immédiat de ce résultat, nous obtenons que pour les groupes d'ordre impair, la constante de Davenport de $\mathcal{B}_{\pm}(G)$. est égale à la constante de Davenport classique.

**Corollaire 2.6.1**
Soit $G$ un groupe abélien d'ordre impair. Alors $\mathsf{D}(\mathcal{B}_{\pm}(G)) = \mathsf{D}(\mathcal{B}(G))$.

**Démonstration :**
Directement à partir du théorème 2.5.1 et du lemme 2.3.3 ■

Bien que la valeur de $\mathsf{D}(\mathcal{B}(G))$ ne soit pas connue en général, il existe des résultats connus qui peuvent être utilisés pour obtenir des résultats explicites pour

$\mathsf{D}(\mathcal{B}_{\pm}(G))$ pour les groupes d'ordre impair. En particulier, pour $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$, avec $1 < n_1 | \ldots n_r$, on a $\mathsf{D}(\mathcal{B}(G)) \geqslant 1 + \sum_{i=1}^{r}(n_i - 1)$ et l'égalité est connue pour tenir si $G$ a un rang au plus égal à deux, c'est-à-dire $r \leqslant 2$, ou si $G$ est un $p$-groupe, c'est-à-dire que $n_r$ est une puissance première. L'égalité est également valable dans certains autres cas, mais pas en général. Voir à [13], section 3 pour un aperçu. La situation concernant $\mathsf{D}(\mathcal{B}_{\pm}(G))$ pour les groupes d'ordre pair est plus compliquée. Nous traitons complètement le cas des groupes cycliques d'ordre pair et obtenons ensuite une borne inférieure générale. Pour ce faire, nous rappelons un résultat sur la structure des longues séquences minimales à somme nulle et des concepts connexes. Notre présentation suit [14], Section 7, les résultats sont dus à Savchev et Chen [36] et Yuan [40].

**Définition 2.6.1**

1. Une séquence $S \in \mathcal{F}(G)$ est dite lisse, ou plus précisément $g$-lisse, s'il existe $g \in G$ tel que $S = (n_1 g) \ldots (n_l g)$, ou $1 = n_1 \leqslant \cdots \leqslant n_l$, $n = n_1 + \cdots + n_l < \mathsf{ord}(g)$ et $\sum(S) = \{g, 2g, \ldots, ng\}$.
2. Une séquence $S \in \mathcal{F}(G)$ est appelée une séquence à somme nulle minimale séparable si $S \in \mathcal{A}(\mathcal{B}(G))$ et $S = (g_1 + g_2)T$ pour $g_1, g_2 \in G$ et $T \in \mathcal{F}(G)$ tels que $g_1 g_2 T_2 \in \mathcal{A}(\mathcal{B}(G))$.

**Théorème 2.6.2**
Soit $G$ un groupe cyclique d'ordre $n \geqslant 3$.

1. Si $S \in \mathcal{F}(G)$ est libre à somme nulle et $|S| \geqslant \frac{n+1}{2}$, alors $S$ est $g$-lisse pour $g \in G$ avec $\mathsf{ord}(g) = n$.
2. Soit $A \in \mathcal{A}(\mathcal{B}(G))$ de longueur $|A| \geqslant \lfloor \frac{n}{2} \rfloor + 2$. Alors $A = (n_1 g) \cdots (n_l g)$ pour$g \in G$ avec $\mathsf{ord}(g) = n$, $1 = n_1 \leqslant \cdots \leqslant n_l$, $n_1 + \cdots + n_l = n$. De plus, si $A$ n'est pas divisible, alors $A = g^n$.

**Lemme 2.6.1**
Soit $g \in G$ et $k, l, n_1 \ldots, n_l \in \mathbb{N}$ tels que $l \geqslant \frac{k}{2}$ et $n = n_1 + \cdots + n_l < k \leqslant \mathsf{ord}(g)$. Si $1 \leqslant n_1 \leqslant \ldots \leqslant n_l$ et $S = (n_1 g) \ldots (n_l g)$, alors $\sum(S) = \{g, 2g, \ldots, ng\}$, et $S$ est $g$-lisse. Nous établissons une borne inférieure pour $\mathsf{D}(\mathcal{B}_{\pm}(C_n))$ pour $n$ pair.

**Lemme 2.6.2**
Soit $n \geqslant 2$ pair. Alors

$$\mathsf{D}(\mathcal{B}_{\pm}(C_n)) \geqslant 1 + \tfrac{n}{2}$$

**Démonstration :**
Soit $n = 2m$. Soit $C_n = \langle e \rangle$. Pour $n = 2$, on note que $e^2$ est un élément de $\mathcal{A}(\mathcal{B}_{\pm}(C_n))$, ce qui établit l'affirmation dans ce cas. Supposons maintenant que $n \geqslant 4$. Nous montrons que $A = e^m(me)$ est un élément de $\mathcal{A}(\mathcal{B}_{\pm}(C_n))$. Supposons

que $A = A_1A_2$ avec à $\in \sigma_{\pm}(A_i)$ pour $i \in \{1,2\}$. Sans perte de généralité, nous pouvons supposer que $me|A_1$. Soit $A_1 = (me)e^k$ avec $k \in [0,m]$.

Puisque $0 \in \sigma_{\pm}(A_i)$, il s'ensuit qu'il existe $\epsilon_1, \ldots, \epsilon_k \in \{+\mathsf{id}_G, -\mathsf{id}_G\}$ tels que $me + \sum_{i=1}^{k} \epsilon_i e = 0$(on peut supposer que le poids de $me$ est $+\mathsf{id}_G$). Or, cela signifie que $\sum_{i=1}^{k} \epsilon_i e = me$. Puisque $\sum_{i=1}^{k} \epsilon_i e$ est égal à $de$ où $d$ est la différence entre les nombres de poids $+\mathsf{id}_G$ et $-\mathsf{id}_G$, on obtient que $|d|$ est au plus $k$. Ainsi, $de = me$ n'est possible que pour $k = m$. Par conséquent, $A_1 = A$ et $A$ est bien dans $\mathcal{A}(\mathcal{B}_{\pm}(C_n))$. ■

**Théorème 2.6.3**
Soit $n$ impair. Alors, on a : $\mathsf{D}(\mathcal{B}_{\pm}(C_n)) = 1 + \frac{n}{2}$.

**Démonstration :**
L'affirmation est facilement établie pour $n = 2$, nous supposons que $n \geqslant 4$. Par le Lemme 2.4.3 nous savons que $\mathsf{D}(\mathcal{B}_{\pm}(C_n)) \geqslant 1 + \frac{n}{2}$. Il reste à montrer que $\mathsf{D}(\mathcal{B}_{\pm}(C_n)) \leqslant 1 + \frac{n}{2}$. Soit $S = g_1 \cdots g_l \in \mathcal{A}(\mathcal{B}_{\pm}(C_n))$ et supposons au contraire que $|S| \geqslant \frac{n}{2} + 2$. Puisque $0 \in \sigma_{\pm}(S)$, il existe $\epsilon_i \in \{+\mathsf{id}_G, -\mathsf{id}_G\}$ tels que $(\epsilon_1 g_1) + \cdots + (\epsilon_l g_l) = 0$, donc $A = (\epsilon_1 g_1) + \cdots + (\epsilon_l g_l) \in \mathcal{B}_{\pm}(C_n)$. En fait, cette suite à somme nulle $A$ doit être minimale, puisqu'une décomposition de $A$ dans $\mathcal{B}(C_n)$ une décomposition de $S$ dans $\mathcal{B}_{\pm}(C_n)$. Par le théorème 2.5.1, il existe $e \in C_n$ tel que $C_n = \langle e \rangle$ et de plus on peut écrire $A = (a_1e)\cdots(a_le)$ avec $a_i \in [1,n]$ et $\sum_{i=1}^{l} a_i = n$. Nous supposons que $1 \leqslant a_1 \leqslant \cdots \leqslant a_l$. On montre que $a_1 = a_2 = a_3 = a_4 = 1$. Supposons au contraire que $a_4 \geqslant 2$, alors $\sum_{i=1}^{l} a_i \geqslant 3 + 2(l-3) \geqslant 3 + 2(\frac{n}{2} - 1) > n$, ce qui est contradictoire. D'où $A = e^4(a_5e)\ldots(a_le)$. On considère $T = e^{-2}A$. Maintenant, on écrit $T = (b_1e)(b_2e)\cdots(b_{l'}e)$ ou $b_1 \leqslant \cdots \leqslant b_{l'}$, $\sum_{i=1}^{l'} b_i = n-2$ et $b_1 = b_2 = 2$. Remarquons que $l' = l - 2$ et $l' \geqslant \frac{n}{2}$. Notons maintenant que le lemme peut être appliqué à $T$. Nous avons que $\sum(T) = \{e, 2e, \ldots, (\mathsf{ord}(e) - 2)e\}$. Soit $T_1|T$ tel que $\sigma(T_1) = (\frac{(n-2)}{2})e$. Soit $T = T_1T_2$. D'où $\sigma(T_1) = \sigma(T_2)$. Donc on peut décomposer $A = e^2 \cdot T_1T_2$ et $0 \in \sigma_{\pm}(e^2)$. Donc $A \notin \mathcal{A}(\mathcal{B}_{\pm}(G))$. Puisque $\{+\mathsf{id}_G, -\mathsf{id}_G\}$ est un groupe sous composition d'endomorphismes, on peut conclure $S \in \mathcal{A}(\mathcal{B}_{\pm}(G))$, une contradiction. Ceci donne $\mathsf{D}(\mathcal{B}_{\pm}(C_n)) \leqslant 1 + \frac{n}{2}$. ■

**Corollaire 2.6.2**
Soit $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ avec $1 < n_1 | \cdots | n_r$ et soit $t \in [0,r]$ maximal tel que $2 \nmid n_t$. Alors $\mathsf{D}(\mathcal{B}_{\pm}(G)) \geqslant 1 + \sum_{i=1}^{t}(n_i - 1) + \sum_{i=t+1}^{r} \frac{n_i}{2}$.

**Démonstration :**
Par le lemme 2.3.3, nous savons que :

$$\mathsf{D}(\mathcal{B}_{\pm}(G)) \geqslant 1 + \sum_{i=1}^{r}(\mathsf{D}(\mathcal{B}_{\pm}(C_{n_i})) - 1)$$

L'affirmation suit maintenant en utilisant le fait que $\mathsf{D}(\mathcal{B}_{\pm}(C_{n_i}))$ est égal à $n_i$ pour les $n_i$ impairs (voir Corollaire 2.6.2) et égale à $1+\frac{n_i}{2}$ pour les $n_i$ pairs (voir le théorème 2.5.1). ■

Avec $n_i$ et $r, t$ comme ci-dessus, nous notons $\mathsf{D}^*(\mathcal{B}_{\pm}(G)) = 1+\sum_{i=1}^{t}(n_i-1)+\sum_{i=t+1}^{r}\frac{n_i}{2}$. Il serait intéressant d'avoir d'autres résultats sur la question de l'égalité dans l'inégalité $\mathsf{D}(\mathcal{B}_{\pm}(G)) \geqslant \mathsf{D}^*(\mathcal{B}_{\pm}(G))$, par exemple pour les groupes de rang deux d'ordre pair ou pour les 2-groupes. Enfin, nous signalons que les résultats ci-dessus montrent que $\mathsf{D}(\mathcal{B}_{\pm}(G))$ et $1+d(\mathcal{B}_{\pm}(G))$ sont très différents. Nous rappelons que cette dernière est bornée ci-dessus par $1+\lfloor \log_2 |G| \rfloor$. Voir [1], [31] pour d'autres résultats sur cette constante. Nous concluons cette section par quelques résultats sur les ensembles de longueurs et d'élasticités dans le cas où $G$ est un groupe d'ordre impair.

**Proposition 2.6.1**
Soit $G$ un groupe d'ordre impair. Pour chaque $B \in \mathcal{B}(G)$, on a $\mathsf{Z}_{\mathcal{B}(G)}(B) \subseteq \mathsf{Z}_{\mathcal{B}_{\pm}(G)}(B)$ et, en particulier,$\mathsf{L}_{\mathcal{B}(G)}(B) \subseteq \mathsf{L}_{\mathcal{B}_{\pm}(G)}(B)$.

**Démonstration :**
Soit $B \in \mathcal{B}(G)$. Soit $z \in Z_{\mathcal{B}(G)}(B)$. Cela signifie que $z = A_1 \cdots A_k$ avec $A_i \in \mathcal{A}(G)$. Or, puisque l'ordre de $G$ est impair, par le théorème 2.5.1, nous avons $\mathcal{A}(G) \subseteq \mathcal{A}(\mathcal{B}_{\pm}(G))$ et donc $A_i \in \mathcal{A}(\mathcal{B}_{\pm}(G))$ pour chaque $1 \leqslant i \leqslant k$. Autrement dit, $z \in Z_{\mathcal{B}_{\pm}(G)}(B)$. L'affirmation sur l'ensemble des longueurs est immédiate. ■

Le résultat précédent permet d'obtenir des résultats sur les élasticités.

**Corollaire 2.6.3**
Soit $G$ un groupe d'ordre impair. Pour $k \in \mathbb{N}$, on a $\mathcal{U}_k(\mathcal{B}(G)) \subseteq \mathcal{U}_k(\mathcal{B}_{\pm}(G))$, et en particulier $\rho_k(\mathcal{B}(G)) \leqslant \rho_k(\mathcal{B}_{\pm}(G))$,et $\lambda_k(\mathcal{B}(G)) \geqslant \lambda_k(\mathcal{B}_{\pm}(G))$.

**Démonstration :**
Ceci est immédiat d'après la proposition 2.6.1 et les définitions. ■

Dans le théorème 2.5.2, nous avons déjà déterminé $\rho_{2k}(\mathcal{B}_{\pm}(G))$ et remarqué que le problème pour les indices impairs est plus compliqué. Nous montrons maintenant comment nous pouvons utiliser les résultats obtenus pour le problème avec ou sans poids.

**Proposition 2.6.2**
Soit $G$ un groupe d'ordre impair. Soit $\mathsf{D} = \mathsf{D}(\mathcal{B}(G))$. Soit $l \in \mathbb{N}_0$.

1. Nous avons $\rho_{2k}(\mathcal{B}_{\pm}(G)) = \rho_{2k}(\mathcal{B}(G)) = k\mathsf{D}$ et $\rho(\mathcal{B}_{\pm}(G)) = \rho(\mathcal{B}(G)) = \frac{\mathsf{D}}{2}$.
2. Si $\rho_{2k+1}(\mathcal{B}(G)) = k\mathsf{D} + \lfloor \frac{\mathsf{D}}{2} \rfloor$, alors :

$$\rho_{2k+1}(\mathcal{B}_{\pm}(G)) = \rho_{2k+1}(\mathcal{B}(G)) = k\mathsf{D} + \left\lfloor \frac{\mathsf{D}}{2} \right\rfloor .$$

**Démonstration :**
Par le corollaire 2.6.3, nous avons $\mathsf{D} = \mathsf{D}(\mathcal{B}_{\pm}(G))$. La première partie est maintenant immédiate d'après le théorème 2.5.2. Pour la deuxième partie, toujours par le théorème 2.5.2, nous avons $\rho_{2k+1}(\mathcal{B}_{\pm}(G)) \leqslant k\mathsf{D} + \lfloor \frac{\mathsf{D}}{2} \rfloor$. Puisque par Corollaire 2.6.3, nous avons $\rho_{2k+1}(\mathcal{B}(G)) \leqslant \rho_{2k+1}(\mathcal{B}_{\pm}(G))$.l'affirmation suit. ■
Pour une étude détaillée de la question de savoir quand $\rho_{2k+1}(\mathcal{B}(G)) = k\mathsf{D} + \lfloor \frac{\mathsf{D}}{2} \rfloor$, nous nous référons à [11],[17]. Divers résultats sont obtenus et donnent directement le résultat analogue pour $\mathcal{B}_{\pm}(G)$. Il est inutile de copier essentiellement tous ces résultats. A titre d'exemple, nous énonçons le résultat suivant.

**Corollaire 2.6.4**
Soit $r \geqslant 2$ et que $n$ est une puissance d'un nombre premier impair. Alors, pour chaque $k \in \mathbb{N}$, on a :

$$\rho_{2k+1}(\mathcal{B}_{\pm}(C_n^r)) = k(1 + r(n-1)) + \frac{r(n-1)}{2}.$$

**Démonstration :**
C'est une conséquence directe de la proposition 2.6.2 et de [17], Corollaire 2.6.3 qui établit que $\rho_{2k+1}(\mathcal{B}(C_n^r)) = k(1 + r(n-1)) + \frac{(r(n-1))}{2}$ (nous avons introduit la valeur de $\mathsf{D}(C_n^r)$ et avons évalué la fonction plancher). Plus précisement ce résultat a été amélioré (voir théorème 2.8.1). ■

## 2.7 L'arithmétique des monoïdes de normes d'anneaux d'entiers algébriques

### 2.7.1 Anneaux et corps

Dans cette partie, nous donnons les définitions des anneaux et des corps.[5][Voir chapitre XIV]

**Définition 2.7.1**
Un anneau est un triplet $(A, +, \cdot)$, où $A$ est un ensemble vide , $+ : A \times A \longrightarrow A$ et $\cdot : A \times A \longrightarrow A$ sont deux lois internes, vérifiant les propriétés :
- Le couple $(A, +)$ est un groupe abélien.
- La loi $<< \cdot >>$ est associative, et possède un élément neutre ;
- La loi $<< \cdot >>$ est distributive par rapport à $<< + >>$.

Les éléments neutres pour les lois $<< + >>$ et $<< \cdot >>$ seront notés $0_A$ et $1_A$ respectivement.

On dit que l'anneau $(A, +, \cdot)$ est commutatif si $<< \cdot >>$ est commutative.

**Définition 2.7.2**
Soit $A$ un anneau. Un sous-anneau de $A$ est un sous-ensemble $B$ de $A$ vérifiant les conditions suivantes :

1. on a $1_A \in B$ ;
2. pour tous $x, y \in B, x + y, xy, -x \in B$.

**Définition 2.7.3**
Soit $A$ un anneau.
Un sous-ensemble $\alpha \subset A$ est un idéal à gauche si :

1. $\alpha$ est un sous-groupe additif de $(A, +)$ ;
2. pour tout $a \in A$ et pour tout $x \in \alpha$, on a $ax \in \alpha$.

Un sous-ensemble $\alpha \subset A$ est idéal à droite si :

1. $\alpha$ est un sous-groupe additif de $(A, +)$ ;
2. pour tout $a \in A$ et pour tout $x \in \alpha$, on a $xa \in \alpha$.

Un sous-ensemble $\alpha \subset A$ est un idéal bilatère si c'est idéal à gauche et à droite , c'est-à-dire :

1. $\alpha$ est un sous-groupe additif de $(A, +)$ ;
2. pour tout $a \in A$ et pour tout $x \in \alpha$, on a $ax \in \alpha$ et $xa \in \alpha$.

Lorsque $A$ est commutatif, ces trois notions coincident . Dans ce cas, on parle d'idéal de l'anneau $A$

**Définition 2.7.4**
Soit un anneau $A$ est un anneau à division s'il est non trivial et si tout élément non nul est inversible.
Un corps est un anneau à division qui est commutatif. Autrement dit, un corps est un anneau non trivial, commutatif, tel que tout élément non nul est inversible.

**Définition 2.7.5**
Soit $K$ un corps. Une extension de $K$ est un corps $L$ contenant $K$ comme sous-corps. On le note $L/K$.
On vérifie aisément que $L$, muni de son produit et de la loi externe

$$\begin{aligned} K \times L &\longrightarrow L \\ (\lambda, x) &\longrightarrow \lambda x, \end{aligned}$$

est un $K$-algèbre associative unitaire.
On appelle degré de $L/K$ la dimension de $L$comme $K$-espace vectoriel. On le note $[L : K]$.

**Définition 2.7.6**
Soit $L/K$ une extension de corps , et soit $\alpha \in L$.On dit que $\alpha$ est algébrique sur $K$ s'il existe un polynôme $P \in K[X]$ non nul tel que $P(\alpha) = 0$. On dit que $\alpha$ est transcendant sinon.

**Définition 2.7.7**
On dit qu'un polynôme $K[X]$ non constant est séparable sur $K$ si $P$ n'a que des racines simples sur $\bar{K}$. On dit que $\alpha \in \bar{K}$ est séparable sur $K$.
On dit qu'une extension $L/K$ est séparable sur $K$ si $L/K$ est algébrique, et si tout élément de $L$ est séparable sur $K$.

## 2.7.2 Extensions galoisiennes

Nous nous intéressons aux groupes des automorphismes d'une extension de degré fini. Nous verrons dans cette partie $Gal(L/K)$ avec l'image de l'application

$$Gal(L/K) \longrightarrow aut(L/K),$$

obtenue en composant à droite par l'inclusion $L \subset \bar{(}K)$. Comme nous l'avons déjà remarqué, on a alors une inclusion

$$Gal(L/K) \longrightarrow aut(L/K),$$

mais l'inclusion est stricte en général.

**Lemme 2.7.1**
Soit $L/K$ un extension de degré fini. Les propriétés suivantes sont équivalentes :

1. tout plogement sur $L/K$ est un automorphisme de $L/K$ ;
2. tout polynôme irréductible unitaire de $K[X]$ ayant au moins une racine dans $L$ est scindé dans $L$ ;
3. l'extension $L/K$ est le corps des racines d'un polynôme de $K[X]$.

**Définition 2.7.8**
Une extension $L/K$ de degré fini est dite normale si elle vérifie une des conditions suivantes équivalentes du lemme précédent.

**Définition 2.7.9**
Une extension $L/K$ de degré fini est dite normale si tout polynôme irréductible unitaire de $K[X]$ ayant au moins une racine dans $L$ est scindé dans $L$.

**Rémarque 2.7.1**
Une extension $L/K$ de degré fini est dite galoisienne si elle est normale et séparable. Dans ce cas, on note

$$|Gal(L/K)| = [L : K]$$

Dans la présente section, nous relions l'arithmétique de certains sous-monoïdes multiplicatifs des nombres naturels, définis par les normes des anneaux d'entiers algébriques, à l'arithmétique des monoïdes des nombres naturels, définis via les normes des anneaux d'entiers algébriques, à l'arithmétique des monoïdes de séquences à somme nulle pondérée sur des groupes abéliens finis. Une relation entre les problèmes sur les normes des entiers algébriques et les séquences à somme nulle pondérée a été étudiée dans [25], notre application est étroitement liée mais distincte.

Nous rappelons quelques notions et résultats standards de la théorie algébrique des nombres (voir, par exemple, [26],[32], [33]).

Soit $K$ un corps de nombres algébriques, $\Gamma = Gal(K/\mathbb{Q})$ son groupe de Galois, $\mathcal{O}_K$ son anneau d'entier, $\mathcal{P}_K$ l'ensemble des idéaux premiers non nuls, $\mathcal{I}_K = \mathcal{F}(\mathcal{P}_K)$ le monoïde abélien libre des idéaux non nuls de $\mathcal{O}_K$ et $\mathcal{H}_K$ le sous-monoïde des idéaux principaux non nuls. De plus,on note $G$ sa classe de groupes d'idéaux et pour un idéal $J \in \mathcal{I}_K$. Soit $[J] \in G$ sa classe d'idéal. Soit $N : \mathcal{I}_K \longrightarrow \mathbb{N}$ la norme absolue. Nous rappelons que $N(a\mathcal{O}_K) = |N_{K/\mathbb{Q}}(a)|$ pour chaque $a \in \mathcal{O}_K^*$, et $\{|N_{K/\mathbb{Q}}(a)| : a \in \mathcal{O}_K^*\} = N(\mathcal{H}_K) \subseteq N(\mathcal{I}_K)$ est un sous-monoïde. Nous voulons étudier l'arithmétique de ce monoïde.

Nous désignons par $\mathbb{P} \subseteq \mathbb{N}$ l'ensemble des nombres premiers. Pour $p \in \mathbb{P}$, on désigne par $P_p \in \mathcal{P}_K$ un idéal premier au-dessus de $p$. Pour $p \in \mathbb{P}$, nous avons $\{\gamma P_p : \gamma \in \Gamma\}$ est l'ensemble de tous les idéaux premiers situés au-dessus de $p$, et $N(\gamma P_p) = N(P_p) = p^{f_p}$ pour tout $\gamma \in \Gamma$. Nous rappelons que $\Gamma$ agit sur $G$ d'une manière naturelle,pour $g \in G$ et $\gamma \in \Gamma$, on a $\gamma g = [\gamma P]$ pour $g = [P]$ et ceci est bien défini. Par conséquent, il est logique de considérer $\Gamma$ comme un ensemble de poids pour les séquences sur $G$. De plus, puisque chaque classe contient un nombre infini d'idéaux premiers, on peut fixer, pour $p \in \mathbb{P}$, l'idéal premier $P_p \in \mathcal{P}_K$ de telle manière que $G = \{[P_p] : p \in \mathbb{P}\}$.

Nous observons que pour $n \in \mathbb{N}$, nous avons $n \in N(\mathcal{I}_K)$ si et seulement si $f_p | v_p(n)$ pour tout $p \in \mathbb{P}$. Pour un tel $n$, nous obtenons :

$$n = N\Big(\prod_{p\in\mathbb{P}} P_p^{v_p(n)/f_p}\Big)$$

et nous fixons :

$$\Theta(n) = \prod_{p\in\mathbb{P}} P_p^{v_p(n)/f_p} \in \mathcal{F}(G),$$

avec ces notations et conventions, nous obtenons le résultat suivant.

**Théorème 2.7.1**
Soit $K$ un corps de nombres algébriques, $\Gamma$ un groupe de Galois et un groupe de classe $G$.

1. Soit $n \in N(\mathcal{I}_K)$. Alors $n \in N(\mathcal{H}_K)$ si et seulement si $\Theta(n) \in \mathcal{B}_\Gamma(G)$.
2. $\Theta(n) : N(\mathcal{H}_K) \longrightarrow \mathcal{B}_\Gamma(G)$ est un homomophisme de transfert.

**Démonstration :**
Pour une suite $S = g_1 \dots g_l \in \mathcal{F}(G)$ et $\gamma \in \Gamma$, on définit $\gamma S = \gamma g_1 \dots \gamma g_l$. Si $S \in \mathcal{F}(G)$, alors nous avons $S \in \mathcal{B}_\Gamma(G)$ si et seulement s'il existe une décomposition

$$S = \prod_{\gamma\in\Gamma} S_\gamma \text{ tel que } \sum_{\gamma\in\Gamma} \gamma\sigma(S_\gamma) = 0.$$

Pour une classe $g \in G$, on pose $\mathbb{P}_g = \{p \in \mathbb{P} : [P_p] = g\}$.

1. Tout d'abord, nous supposons que $n = N(a\mathcal{O}_K)$, où $a \in \mathcal{O}_K^*$. Nous devons montrer que $\Theta(n) \in \mathcal{B}_\Gamma(G)$. Disons :

$$a\mathcal{O}_K = \prod_{P\in\mathcal{P}_K} P^{v_p(a)} = \prod_{P\in\mathbb{P}} \prod_{\gamma\in\Gamma} (\gamma P_p)^{v_{\gamma P_p}(a)},$$

et $0 = \sum_{\gamma\in\Gamma} \gamma \sum_{p\in\mathbb{P}} v_{\gamma P_p}(a)[P_p] \in G$. Nous obtenons alors

$$n = \prod_{p\in\mathbb{P}} \prod_{\gamma\in\Gamma} p^{f_p v_{\gamma P_p}(a)}$$

et donc

$$\frac{v_p(n)}{f_p} = \sum_{\gamma\in\Gamma} v_{\gamma P_p}(a)$$

pour chaque $p \in \mathbb{P}$. Il s'ensuit que :

$$\Theta(n) = \prod_{p\in\mathbb{P}} [P_p]^{v_p(n)/f_p} = \prod_{\gamma\in\Gamma} \prod_{p\in\mathbb{P}} [P_p]^{v_{\gamma P_p}(a)}$$

et puisque

$$\sum_{\gamma\in\Gamma} \gamma\sigma(\prod_{p\in\mathbb{P}} [P_p]^{v_{\gamma P_p}(a)}) = \sum_{\gamma\in\Gamma} \gamma \sum_{p\in\mathbb{P}} v_{\gamma P_p}(a)[P_p] = 0 \in G\ .$$

Nous avons vu que $\Theta(n) \in \mathcal{B}_\gamma(G)$. Réciproquement, soit :
$\Theta(n) = \prod_{p\in\mathbb{P}} [P_p]^{v_p(n)/f_p} \in \mathcal{B}_\gamma(G)$ et $\Theta(n) = \prod_{\gamma\in\Gamma} S_\gamma$, ou $\sum_{\gamma\in\Gamma} \gamma\sigma(S_\gamma) = 0$.
Nous devons montrer que $n$ est la norme d'un idéal principal. On pose

$$\Theta(n) = \prod_{g\in G} g^{N_g}$$

et, pour

$$\gamma \in \Gamma, S_\gamma = \prod_{g\in G} g^{N_{\gamma,g}}\ .$$

Pour tout $g \in G$, il s'ensuit que

$$N_g = \sum_{p \in \mathbb{P}_g} \frac{v_p(n)}{f_p} = \sum_{\gamma \in \Gamma} N_{\gamma,g} \ .$$

Pour $g \in G$, et $\gamma \in \Gamma$, nous séparons $N_{\gamma,g}$ de telle sorte que

$$N_{\gamma,g} = \sum_{p \in \mathbb{P}_p} N_{\gamma,p}$$

tel que $\sum_{\gamma,p} = \frac{v_p(n)}{f_p}$ pour chaque $p \in \mathbb{P}_g$ . Nous posons maintenant

$A = \prod_{g \in G} \prod_{p \in \mathbb{P}_g} \prod_{\gamma \in \Gamma} (\gamma P_p)^{N_{\gamma,g}} \in \mathcal{I}_K$ et $N(A) = \prod_{g \in G} \prod_{p \in \mathbb{P}_g} \prod_{\gamma \in \Gamma} p^{f_p N_{\gamma,p}}$.

Si $g \in G$ et $p \in \mathbb{P}_g$, alors

$$v_p(N(A)) = \sum_{\gamma \in \Gamma} f_p N_{\gamma,p} = v_p(n) \ ,$$

et donc $N(A) = n$. Puisque

$$[A] = \sum_{g \in G} \sum_{p \in \mathbb{P}_g} \sum_{\gamma \in \Gamma} N_{\gamma,p} \gamma g = \sum_{g \in G} \sum_{\gamma \in \Gamma} N_{\gamma,g} \gamma g = \sum_{\gamma \in \Gamma} \gamma \sigma(S_\gamma) = 0 \ ,$$

on obtient $A \in \mathcal{H}_K$, et par conséquent $n \in N(\mathcal{H}_K)$.

2. Nous devons montrer que $\Theta : N(\mathcal{H}_K) \longrightarrow \mathcal{B}_\Gamma(G)$ est un homomorphisme de transfert. D'après la définition et de la première partie de ce théorème, il est clair qu'il s'agit d'un homomorphisme et que T1 dans la définition de l'homomorphisme de transfert est vrai. Pour compléter l'argument, c'est-à-dire pour montrer que T2 est vrai, supposons que $n \in N(I_K)$ et $\Theta(n) = S'S''$ pour certains $S', S'' \in \mathcal{B}_\Gamma(G)$, et supposons que :

$\Theta(n) = \prod_{p \in \mathbb{P}} [P_p]^{v_p(n)/f_p} = \prod_{g \in G} g^{N_g}$, $S' = \prod_{g \in G} g^{N_{g'}}$ et $S'' = \prod_{g \in G} g^{N_{g''}}$,

où $N_g, N_{g'}, N_{g''} \in \mathbb{N}_0$ tels que

$$N_g = N_{g'} + N_{g''} = \textstyle\sum_{p \in \mathbb{P}_g} \frac{v_p(n)}{f_p} \text{ pour tout } g \in G.$$

Pour tout $g \in G$, séparons $N_{g'}, N_{g''}$ tel que

$N_{g'} = \sum_{p \in \mathbb{P}_g} N_{p'}$, $N_{g''} = \sum_{p \in \mathbb{P}_g} N_{p''}$, et $N_{p'} + N_{p''} = \frac{v_p(n)}{f_p}$ pour tout $p \in \mathbb{P}_g$

Pour $N'_p, N''_p \in \mathbb{N}_0$, nous posons

$$n' = \prod_{p \in \mathbb{P}} p^{f_p N'_p} \text{ et } n'' = \prod_{p \in \mathbb{P}} p^{f_p N''_p}.$$

Alors $n = n'n''$

$\Theta(n') = \prod_{g\in G}\prod_{p\in\mathbb{P}}[P_p]^{N'_p} = \prod_{g\in G} g^{\sum_{p\in\mathbb{P}_g} N'_g} = \prod_{g\in G} g^{N'_g} = S'$, et de même $\Theta(n'') = S''$.

■

Nous soulignons quelques conséquences du résultat précédent.

**Corollaire 2.7.1**
Soit $K$ un corps de nombres de Galois avec le groupe de classe $G$. Soit $H = N(\mathcal{H}_\mathcal{K})$ le monoïde de normes absolues.

1. L'ensemble $\Delta(H)$ et la constante $\rho(H)$ sont finis.
2. Pour $k \in \mathbb{N}$ l'ensemble $\mathcal{U}_k(H)$ est un intervalle.
3. Il existe un certain $M \in \mathbb{N}_0$ tel que chaque ensemble de longueurs $L$ de $H$ est une progression multiple presque arithmétique avec une borne $M$ et une différence $d \in \Delta(H) \cup \{0\}$, c'est-à-dire , $L = y + (L_1 \cup L^* \cup (\max L^* + L_2)) \subseteq y + \mathcal{D} + d\mathbb{Z}$ avec $y \in \mathbb{N}_0, \{0, d\} \subseteq \mathcal{D} \subseteq [0, d], -L_1, L_2 \subseteq [1, M], \min L^* = 0$ et $L^* = [0, \max L^*] \cap \mathcal{D} + d\mathbb{Z}$.

**Démonstration :**
Par le théorème 2.7.1, nous savons qu'il existe un homomorphisme de transfert de $H$ vers $\mathcal{B}_\Gamma(G)$ où $\Gamma$ désigne le groupe de Galois de $K$. Par le théorème 2.3.3 et le théorème 2.5.2, nous savons que $\mathcal{B}_\Gamma(G)$ a les propriétés requises. Puisque toutes les propriétés ne dépendent que de la longueur des factorisations, et que les homomorphismes de transfert préservent les ensembles de longueurs(voir la section 2 après avoir rappelé la définition de l'homomorphisme de transfert), l'affirmation est valable pour tous les cas. ■
Dans le cas des champs de nombres quadratiques, nous pouvons appliquer nos résultats sur les séquences pondérées.

**Corollaire 2.7.2**
Soit $K$ un corps de nombres quadratiques dont le nombre de classe est impair. Alors $\rho(N(\mathcal{H}_K)) = \rho(\mathcal{H}_K)$ et $\rho_{2k}(N(\mathcal{H}_K)) = \rho_{2k}(\mathcal{H}_K)$ pour chaque $k \in \mathbb{N}$.

**Démonstration :**
Comme dans le corollaire précédent, il suffit d'établir l'affirmation pour $\mathcal{B}_\Gamma(G)$ où $\Gamma$ désigne le groupe de Galois de $K$. Comme $K$ est un corps de nombres quadratiques, il s'ensuit que $|\Gamma| = 2$. De plus, si $\Gamma = \{id, \gamma\}$ alors $P_\gamma(P)$ est un idéal principal pour chaque idéal premier $P$ de $\mathcal{O}_K$. Ainsi, $[P] + [\gamma(P)] = 0$ pour chaque $P$, ce qui implique que $\gamma$ agit comme $-\mathsf{id}_G$ sur $G$. C'est-à-dire dans ce cas $\mathcal{B}_\Gamma(G) = \mathcal{B}_\pm(G)$ : L'affirmation requise suit maintenant par la proposition 2.6.2.
■

### 2.7.3 Les entiers algébriques

Soit $A$ un anneau intègre, de corps des fractions $K_A$. Un polynôme non constant irréductible $f \in A[X]$ est-il encore irréductible dans $K_A[X]$ dans $K_A[X]$ ? Pour cela, nous avons besoin de la notion d'élément entier $A$. Nous remarquons que si $L/K_A$ est une extension du corps, un élément $\alpha \in L$ algébrique sur $K$ est une racine d'un polynôme non constant à coefficient dans $A$.
En effet, soit $P \in K_A[X]$ est un polynôme non constant tel que $P(\alpha) = 0$. Si $d \in A\{0\}$ est un dénominateur commun aux coefficients de $P$, alors on a $dP \in A[X]$ et $(dP)(\alpha) \in A[X]$ et $(dP(\alpha)) = 0$. D'autre part, par définition , $\alpha$ est aussi racine d'un polynôme unitaire non constant à coefficients dans $K_A$. On peut se demander légitiment si $\alpha$ est une racine d'un polynôme unitaire à coefficients dans $A$.

**Définition 2.7.10**
Soit $B$ un anneau , et soit $A$ un sous-anneau de $B$. On dit que $x \in B$ est un entier de $A$ s'il existe un polynôme $P \in A[X]$ unitaire tel que $P(x) = 0$. En particulier, tout élément de $A$ est donc entier sur $A$.

**Définition 2.7.11**
Soit $A$ un anneau. On dit que $A$ est intégralement clos s'il est intègre , et si les seuls éléments de $K_A$ qui sont entiers sur $A$ sont les éléments de $A$.

**Théorème 2.7.2**
Soit $A$ un anneau intégralement clos, et $L/K_A$ une extension . Alors , $\alpha \in L$ est entier sur $A$ si,et seulement si, son polynôme minimal sur $K_A$ est à coefficients dans $A$.

**Théorème 2.7.3**
Soit $A$ un anneau intègre. Alors, les propriétés suivantes sont équivalentes :

1. tout polynôme non constant irréductible de $A[X]$ est encore irréductible dans l'anneau $K_A[X]$ ;
2. tout polynôme unitaire irréductible de $A[X]$ est encore irréductible dans l'anneau $K_A[X]$ ;
3. l'anneau $A$ est intégralement clos.

## 2.8 Résultats améliorés pour les monoides de séquences à somme nulle

Nos résultats sur les monoides de séquences à somme nulle ont recemment été améliorés par Alfred Geroldinger, Franz Halter-Koch et Qinghai Zhong ([19]). Ci-dessous un théorème amélioré avec démonstration.

**Théorème 2.8.1**
Soit $G$ un groupe abélien fini d'ordre impair tel que $\mathsf{D}(G) = \mathsf{D}^*(G) \geqslant 3$, et soit $k = k\mathsf{D}(G) + j \geqslant 2$, ou $l \in \mathbb{N}_0$ et $j \in [0, \mathsf{d}(G)]$. Alors, nous avons

$$\mathcal{U}_k(\mathcal{B}_{\pm}(G)) = \begin{cases} [2, \lfloor k\mathsf{D}(G)/2 \rfloor], & \text{si } j \in [2, \mathsf{d}(G)] \text{ et } l = 0 \\ [2l, \lfloor k\mathsf{D}(G)/2 \rfloor], & \text{si } j = 0 \text{ et } l \geqslant 1 \\ [2l+1, \lfloor k\mathsf{D}(G)/2 \rfloor], & \text{si } j \in [1, \mathsf{d}(G)/2] \text{ et } l \geqslant 1 \\ [2l+2, \lfloor k\mathsf{D}(G)/2 \rfloor], & \text{si } j \in [1 + \mathsf{d}(G)/2, d(G)] \text{ et } l \geqslant 1. \end{cases}$$

**Démonstration :**
Les principales parties de la recherche sont basées sur des travaux antérieurs effectués dans [19].

Pour commencer, les unions $\mathcal{U}_k(\mathcal{B}_{\pm}(G))$ sont des intervalles pour tout $k \in \mathbb{N}$ par le théorème 5.2 de [19]. Ainsi, pour déterminer leurs maxima $\rho_k(\mathcal{B}_{\pm}(G))$ et leur minima $\lambda_k(\mathcal{B}_{\pm}(G))$. Nous utilisons $\mathsf{D}(\mathcal{B}_{\pm}(G)) = \mathsf{D}(G) \geqslant 3$ car $|G|$ est impair (corollaire 6.2 dans [19]).

1. On a $\rho_k(\mathcal{B}_{\pm}(G))$. Nous avons besoin de montrer

$$\rho_k(\mathcal{B}_{\pm}(G)) = \lfloor k\mathsf{D}/2 \rfloor \text{ pour tout } k \geqslant 2.$$

Un simple argument de comptage (théorème 5.7 de [19])montre que pour $k \in \mathbb{N}$,

$$\rho_{2k}(\mathcal{B}_{\pm}(G)) = k\mathsf{D}(G) \text{ et } \rho_{2k+1}(\mathcal{B}_{\pm}(G)) \leqslant k\mathsf{D}(G) + \lfloor \tfrac{\mathsf{D}(G)}{2} \rfloor.$$

Ainsi, il reste donc à montrer que, pour $k \in \mathbb{N}$

$$\rho_{2k+1}(\mathcal{B}_{\pm}(G)) \geqslant k\mathsf{D}(G) + \left\lfloor \tfrac{\mathsf{D}(G)}{2} \right\rfloor.$$

Soit $k \in \mathbb{N}$. On supppose que $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, ou $r \in \mathbb{N}$ et $1 \leqslant n_1 | \ldots | n_r$ et soit $(e_1, \ldots, e_r)$, une base de $G$ avec $\mathsf{ord}(e_i) = n_i$ pour tout $i \in [1, r]$.Comme $G$ et $\mathsf{D}(G) = \mathsf{D}^*(G)$, $U_1 = e_1^{n_1-1} \cdot \ldots \cdot e_r^{n_r-1}(e_1 + \ldots + e_r)$ et $U_2 = (2e_1)^{n_1-1} \cdot \ldots \cdot (2e_r)^{n_r-1}(2e_1 + \ldots + 2e_r)$ sont des atomes de $\mathcal{B}(G)$ de longueur $\mathsf{D}(G)$.On a encore $|G|$ est impair, nous avons $\mathcal{A}(\mathcal{B}(G)) \subset \mathcal{A}(\mathcal{B}_{\pm}(G))$ par (théorème 6.1 dans [19]), donc $U_1$ et $U_2$ sont des atomes de $\mathcal{B}_{\pm}(G)$ de longueur $\mathsf{D}(\mathcal{B}_{\pm}(G))$. comme

$$V_1 = (e_1 + \ldots + e_r)^2$$

et

$$V_2 = V_1(2e_1 + \ldots + 2e_r)^2$$

sont des atomes de $\mathcal{B}_{\pm}(G)$, nous obtenons l'équation suivante, avec les produits des atomes dans le premier et second membre

$$U_1^k U_1^k U_2 = (e_1^2)^{k(n_1-1)} \cdot \ldots \cdot (e_r^2)^{k(n_r-1)} V_1^{k-1} V_2((2e_1)^2)^{(n_1-1)/2} \cdot \ldots \cdot ((2e_r)^2)^{(n_r-1)/2},$$

d'où

$$\rho_{2k+1}(\mathcal{B}_{\pm}(G)) \geqslant \sum_{i=1}^{r} k(n_i-1) + k - 1 + 1 + \sum_{i=1}^{r}(n_i-1)/2 = k\mathsf{D}(G) + \lfloor \mathsf{D}(G)/2 \rfloor.$$

2. On a $\lambda_k(\mathcal{B}_{\pm}(G))$. Soit $k = l\mathsf{D}(G) + j \geqslant 2$, ou $l \in \mathbb{N}_0$ et $j \in [0, \mathsf{d}(G)]$.Comme $\{+\mathsf{id}_G, -\mathsf{id}_G\} \subset Aut(G)$ est un sous-groupe, le théorème 5.8 dans [19] implique :

$$\lambda_k(\mathcal{B}_{\pm}(G)) = \begin{cases} 2l, & \text{pour } j = 0 \\ 2l+1, & \text{pour } j \in \left[1, \rho_{2l+1}(\mathcal{B}_{\pm}(G)) - l\mathsf{D}(G)\right] \\ 2l+2, & \text{pour } j \in \left[\rho_{2l+1}(\mathcal{B}_{\pm}(G)) - l\mathsf{D}(G) + 1, \mathsf{d}(G)\right]. \end{cases} \tag{2.1}$$

Si $l = 0$, alors $j \in [2, \mathsf{d}(G)] = \left[\rho_{2l+1}(\mathcal{B}_{\pm}(G)) - l\mathsf{D}(G) + 1, \mathsf{d}(G)\right]$, et l'équation 2.1 implique que $\lambda_k(\mathcal{B}_{\pm}) = 2$.

On suppose maintenant $l \geqslant 1$.

— Si $j = 0$, l'équation 2.1 implique $\lambda_k(\mathcal{B}_{\pm}(G)) = 2l$

— Si $j \in [1, \mathsf{d}(G)/2] = [1, \rho_{2l+1}(\mathcal{B}_{\pm}(G)) - l\mathsf{D}(G)]$,alors l'équation 2.1 implique $\lambda_k(\mathcal{B}_{\pm}(G)) = 2l + 1$

— Si $j \in [(\mathsf{D}(G)+1)/2, \mathsf{d}(G)] = [\rho_{2l+1}(\mathcal{B}_{\pm}(G)) - l\mathsf{D}(G) + 1, \mathsf{d}(G)]$, alors l'équation 2.1 implique $\lambda_k(\mathcal{B}_{\pm}(G)) = 2l + 2$.

■

# 3 | L'ensemble des distances minimales du monoïde des séquences à somme nulle pondérées et applications au problème de caractérisation

## 3.1 Résumé historique de l'article

Récemment, une investigation systématique des séquences à somme nulle pondérées a été lancée, motivée entre autres par des applications aux monoïdes des normes des entiers algébriques. Dans cet article, ces investigations sont poursuivies. L'accent est mis sur l'ensemble des distances minimales de ces monoïdes, qui est un invariant arithmétique important. Des applications au problème de caractérisation sont également discutées.

## 3.2 Introduction

Dans le présent article, nous poursuivons l'investigation des monoïdes de sous-séquences somme nulle pondérées. En particulier, nous étudions leurs ensembles de différences, c'est-à-dire l'ensemble des distances minimales des sous-monoïdes fermés sous-diviseurs, noté $\Delta^*(H)$. Cet ensemble a été largement étudié pour les monoïdes de Krull, principalement avec un groupe de classes fini voir [6], pour un résultat dans le cas des groupes de classes infinis, voir [7].

## 3.3 Distances

Nous rappelons la définition des distances successives et des notions associées. Pour un ensemble fini $A \subseteq \mathbb{Z}$, nous notons par $\Delta(A)$ l'ensemble des distances (successives) de $A$, c'est-à-dire, si $A = \{a_0, \ldots, a_k\}$ avec $a_0 < \cdots < a_k$, alors $\Delta(A) = \{a_1 - a_0, a_2 - a_1, \ldots, a_k - a_{k-1}\} = \{a_{i+1} - a_i : i \in [1, k]\}$. Autrement dit, pour chaque $a \in A$ qui n'est pas le maximum de $A$, nous avons $d \in \Delta(A)$ si $d$ est le plus petit $d \in \mathbb{N}$ tel que $a + d \in A$.

Pour un monoïde $H$ de type BF et $a \in H$, nous posons $\Delta(a) = \Delta(\mathsf{L}(a))$ et $\Delta(H) = \bigcup_{a \in H} \Delta(\mathsf{L}(a))$.

De plus, nous définissons :

$$\Delta^*(H) = \{\min \Delta(S) : S \subseteq H \text{ est un sous-monoïde fermé sous-diviseur et } \Delta(S) \neq \emptyset\}.$$

La pertinence de la notion $\Delta^*(H)$ est principalement due au fait qu'elle constitue un choix naturel dans le théorème de structure pour les ensembles de longueurs, voir [37], et au rôle important qu'elle joue dans le problème de caractérisation.

Spécifiquement, pour $H$ un monoïde de type fini, il existe un $M \in \mathbb{N}_0$ tel que chaque ensemble de longueurs $L$ de $H$ soit une presque progression arithmétique multiple avec borne $M$ et différence $d \in \Delta(H) \cup \{0\}$, c'est-à-dire :

$$L = y + (L_1 \cup L' \cup (\max L' + L_2)) \subseteq y + D + d\mathbb{Z}$$

avec $y \in \mathbb{N}_0$, $\{0, d\} \subseteq D \subseteq [0, d]$, $L_1, L_2 \subseteq [1, M]$, $\min L' = 0$ et $L' = [0, \max L'] \cap D + d\mathbb{Z}$.

De plus, si nous définissons $\Delta_1(H)$ comme l'ensemble de tous les $d$ tels que $L(H)$ contienne une progression arithmétique presque avec borne $M$ et différence $d$ de taille arbitrairement grande, il est connu que $\Delta(H) \subseteq \Delta_1(H) \subseteq \{d_0 \mid d : d \in \Delta(H)\}$. Rappelons qu'une progression arithmétique presque est une progression arithmétique multiple presque avec $D = \{0, d\}$, c'est-à-dire une progression arithmétique où certains éléments au début et à la fin peuvent être manquants.

Nous rappelons quelques faits bien connus. Soit $H$ un monoïde de type BF avec $\Delta(H) \neq \varnothing$. Alors, $\min \Delta(H) = \mathsf{pgcd}\Delta(H)$. En particulier, pour tout choix de $a \in H$ et $l, l' \in \mathsf{L}(a)$, on a $\min \Delta(H) \mid l' - l$.

## 3.4 Quelques constructions

Nous commençons par un lemme simple mais puissant. La restriction que $0 \notin G_0$ n'est pas une restriction réelle car $\mathcal{B}_{\pm}(G_0)$ et $\mathcal{B}_{\pm}(G_0 \cup \{0\})$ ont le même ensemble de distances.

**Lemme 3.4.1**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G \backslash \{0\}$ non vide. Soit $H = \mathcal{B}_{\pm}(G_0)$. Pour chaque $A \in \mathcal{A}(H)$, nous avons que $\{2, |A|\} \subseteq \mathsf{L}(A^2)$ et en particulier $\min \Delta(H) \mid |A| - 2$. De plus,

$$\min \Delta(H) \mid \mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\} = \mathsf{pgcd}\{|A| - |A'| : A, A' \in \mathcal{A}(H)\}.$$

**Démonstration :**
Soit $A = g_1 \ldots g_l \in \mathcal{A}(H)$. Remarquons que, puisque $g_i \neq 0$, nous avons $l \geqslant 2$ et $g_i^2 \in \mathcal{A}(H)$ pour chaque $i \in [1, l]$. Ainsi, $A^2$ et $g_1^2 \ldots g_l^2$ sont des factorisations du même élément, la première ayant une longueur de 2 et la seconde une longueur de $l = |A|$. Bien que $|A| - 2$ ne soit peut-être pas dans $\Delta(H)$, il est au moins une somme d'éléments de $\Delta(H)$, et comme $\min \Delta(H) = \mathsf{pgcd}\Delta(H)$, il s'ensuit que $\min \Delta(H) \mid |A| - 2$.

De plus, comme $\min \Delta(H) \mid |A| - 2$ pour chaque $A \in \mathcal{A}(H)$, il divise également $\mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\}$. Enfin, $\mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\} = \mathsf{pgcd}\{|A| - |A'| : A, A' \in \mathcal{A}(H)\}$, car il existe un certain $A'$ de longueur 2 et les propriétés élémentaires du plus grand commun diviseur s'appliquent. ■

Cet argument est clairement spécifique au cas des séquences somme nulle pondérées plus-moins. Cependant, il est possible de le considérer comme un cas particulier d'un argument plus général, qui engloberait également un argument similaire impliquant des nombres croisés dans le cas classique.

Une question naturelle est de savoir dans quelle mesure $\min \Delta(H)$ et $\mathsf{pgcd}\{|A|-2 : A \in \mathcal{A}(H)\}$ peuvent différer. Il s'avère qu'ils sont étroitement liés.

**Lemme 3.4.2**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G\backslash\{0\}$ non vide. Soit $H = \mathcal{B}_{\pm}(G_0)$. Alors

$$\min \Delta(H) \mid \mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\} \mid 2 \min \Delta(H).$$

En particulier, si $\mathsf{pgcd}\{|A|-2 : A \in \mathcal{A}(H)\}$ est impair, alors $\min \Delta(H) = \mathsf{pgcd}\{|A|-2 : A \in \mathcal{A}(H)\}$.

**Démonstration :**
La première relation de divisibilité est simplement le lemme 3.4.1. Nous devons montrer que $\mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\} \mid 2 \min \Delta(H)$. Posons $d = \sum_{i=1}^{k} |A_i| = \sum_{j=1}^{l} |C_j|$. Soit $B \in H$ tel que $B$ ait une factorisation de longueur $k$ et une autre de longueur $l = k + \min \Delta(H)$, disons $B = A_1 \ldots A_k = C_1 \ldots C_l$ avec $A_i, C_j \in \mathcal{A}(H)$.

Comme $\sum_{i=1}^{k} |A_i| = \sum_{j=1}^{l} |C_j|$, nous avons $\sum_{i=1}^{k} |A_i| \equiv \sum_{j=1}^{l} |C_j| \pmod{d}$. Maintenant, essentiellement par la définition de $d$, la longueur de chaque $A \in \mathcal{A}(H)$ est congruente à $2 \pmod{d}$. Par conséquent, $2k \equiv 2l \pmod{d}$, ce qui implique que $2 \min \Delta(H) \equiv 0 \pmod{d}$, comme prévu. Bien sûr, dans le cas où $d$ est impair, cela donne également $\Delta(H) \equiv 0 \pmod{d}$. ■

Il peut être intéressant de noter que dans le cas où $\mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\}$ est pair, il peut effectivement y avoir une divergence. Un simple exemple peut être obtenu en considérant des 2-groupes élémentaires. Rappelons que, dans ce cas, les séquences à somme nulle pondérées sont simplement des séquences à somme nulle classiques.

**Exemple 3.4.1**
Soit $G = C_2^4 = \langle e_1, e_2, e_3, e_4 \rangle$. Soit $G_0 = e_1 + \langle e_2, e_3, e_4 \rangle$ et $H = \mathcal{B}_{\pm}(G_0)$. Alors, $\min \Delta(H) = 1$ tandis que $\mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H)\} = 2$. ▮

Pour voir que c'est bien le cas, il suffit de noter d'une part que $|A|$ est nécessairement pair pour $A \in \mathcal{A}(H)$, ce qui est clair en considérant la projection sur $\langle e_1 \rangle$. D'autre part, en considérant $A_0 = (e_1+e_2+e_3+e_4)(e_1+e_2)(e_1+e_3)(e_1+e_4)$, $A_1 = (e_1+e_2+e_3+e_4)(e_1+e_2)(e_1+e_3)e_1$ et $A_2 = (e_1+e_2+e_3+e_4)(e_1+e_2+e_3)(e_1+e_4)e_1$, on a $A_1 A_2 = A_0 \cdot e_1^2 \cdot (e_1 + e_2 + e_3 + e_4)^2$, ce qui donne une distance de 1.

De plus, ce n'est pas un phénomène isolé et ce n'est pas limité à la distance minimale de 1. Par exemple, ([35], Théorème 5.6) fournit des exemples d'autres distances minimales pour les 2-groupes élémentaires.

**Proposition 3.4.1**
Nous avons $\Delta(\mathcal{B}_{\pm}(C_p)) \subseteq \Delta(\mathcal{B}_{\pm}(C_p^r))$ et réciproquement, chaque élément de $\Delta(\mathcal{B}_{\pm}(C_p^r))$ est le plus grand commun diviseur d'au plus $r$ éléments de $\Delta(\mathcal{B}_{\pm}(C_p))$.

**Démonstration :**
La première inclusion est évidente. Pour la seconde inclusion, nous rappelons que, d'après le lemme 4.2.1, chaque ensemble $G_0$ qui produit un élément de $\Delta(\mathcal{B}_{\pm}(C_p^r))$ autre que 1 peut être écrit comme $G_0 = G_1 \cup \cdots \cup G_k$ où $\langle G_i \rangle$ est cyclique pour chaque $i \in [1, k]$ et $\langle G_0 \rangle = \bigcup_{i=1}^{k} \langle G_i \rangle$. Maintenant, la distance minimale de $\mathcal{B}(G_0)$ est le plus grand commun diviseur des distances minimales de $\mathcal{B}_{\pm}(G_i)$ pour $i$ de 1 à $k$. ■

**Lemme 3.4.3**
Soit $G$ un groupe abélien fini. Soit $g \in G$ avec $\mathsf{ord}(g) = n \geqslant 2$ et soit $H = \mathcal{B}_{\pm}(\{g\})$.

1. Si $n$ est pair, alors $H$ est isomorphe à $(\mathbb{N}_0, +)$. En particulier, $\Delta(H) = \varnothing$ et $c(H) = 0$.
2. Si $n$ est impair, alors $H$ est isomorphe à $\langle 2, n \rangle$. En particulier, $\Delta(H) = \{n-2\}$ et $c(H) = n$.

**Démonstration :**
Pour $n$ pair, la suite à somme nulle minimale est $g^2$, donc ce monoïde $H$ est libre avec un seul élément premier. Si $n$ impair, les seules suites à somme nulle sont $g^2$ et $g^n$. De plus, nous avons $(g^2)^n = (g^n)^2$. C'est essentiellement la seule relation entre $g^2$ et $g^n$. ■

**Lemme 3.4.4**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G$. Soit $H = \mathcal{B}_{\pm}(G_0)$. Nous avons $\{\mathsf{ord}(g) - 2 : g \in G_0, \mathsf{ord}(g) \geqslant 3 \text{ impair}\} \subseteq \Delta(H)$.

**Démonstration :**
Soit $g \in G_0$ un élément non nul d'ordre impair. Soit $S = \mathcal{B}_{\pm}(\{g\})$. Alors $S \subseteq H$ est un sous-monoïde fermé par diviseurs, et ainsi $\Delta(S) \subseteq \Delta(H)$. Par le lemme 3.4.4, nous savons que $\Delta(S) = \{\mathsf{ord}(g) - 2\}$, et l'affirmation s'ensuit. ■

**Lemme 3.4.5**
Soit $G$ un groupe abélien fini et soit $G_0 \subseteq G$. Soit $H = \mathcal{B}_{\pm}(G_0)$.

1. Le monoïde $H$ est demi-factoriel si et seulement si $\mathsf{D}(H) \leqslant 2$.
2. Nous avons $\min \Delta(H) \mid \mathsf{D}(H) - 2$.

**Démonstration :**
Le point 2 est évident à partir du lemme 3.4.1, on rappelle que $\mathsf{D}(H) = \max\{|A| : A \in \mathcal{A}(H)\}$. Toujours par le lemme 3.4.1, si $\mathsf{D}(H) \geqslant 3$ alors $H$ n'est pas demi-factoriel. D'autre part si $\mathsf{D}(H) \leqslant 2$, il suffit d'observer que 0 est la suite à somme

nulle minimale de longueur 1. ■

**Corollaire 3.4.1**
Soit $G$ un groupe abélien fini et soit $G_0 \subset G$. Soit $H = \mathcal{B}_{\pm}(G_0)$. Nous avons :

$$\max \Delta^*(H) \leqslant \mathsf{D}(H) - 2$$

**Lemme 3.4.6**
Soit $G$ un groupe abélien fini et soit $H = \mathcal{B}_{\pm}(G)$. Alors, $\Delta(H) = \varnothing$ si et seulement si $G \leqslant 2$. Si $G \geqslant 3$, alors $1 \in \Delta(H)$ et en particulier $\min \Delta^*(H) = \min \Delta(H) = 1$.

**Démonstration :**
La première assertion est le lemme 6.1 dans [19], le fait que $\min \Delta(H) = 1$ est implicite dans sa preuve, et l'assertion sur $\min \Delta^*(H)$ en découle puisque $H$ est un sous-monoïde fermé par diviseurs de lui-même. ■

**Théorème 3.4.1**
Soit $G$ un groupe abélien fini d'exposant $n$ et soit $H = \mathcal{B}_{\pm}(G)$. Supposons que $n$ soit impair et qu'il soit au moins 3. Soit

$$D_1 = \{d - 2 : d \mid nd \geqslant 3\}$$

et soit

$$D_2 = \{d' \mid d : d \in D_1\}.$$

Alors, $D_1 \subseteq \Delta^*(H) \subseteq D_2$. En particulier, on a $\max \Delta^*(H) = n - 2$.

**Démonstration :**
Pour montrer que $D_1 \subseteq \Delta^*(H)$, il suffit de noter que pour chaque $d \mid n$, il existe un élément $g \in G$ d'ordre $d$ et d'invoquer le lemme 3.4.4. Pour voir que $\Delta^*(H) \subseteq D_2$, soit $S \subseteq H$ un sous-monoïde fermé par diviseurs, c'est-à-dire $S = \mathcal{B}_{\pm}(G_0)$ pour un certain $G_0 \subseteq G$, voir la proposition 3.4.3.

Si $\Delta(S) \neq \varnothing$, ce qui est le seul cas pertinent, alors $G_0$ contient un élément non nul $g$ dont l'ordre, noté $d$, divise $n$ et est donc impair. Par le Lemme 3.4.2, nous avons $\Delta(\mathcal{B}_{\pm}(g)) = \{d-2\}$. Par la proposition 3.4.3, il s'ensuit que $\min \Delta(S) \mid d-2$, et donc $\min \Delta(S) \in D_2$. ■

Bien que, à la lumière du théorème 3.4.1, nous ayons une compréhension relativement précise de $\Delta(H)$ pour $H = \mathcal{B}_{\pm}(G)$ où $G$ est un groupe d'ordre impair, la description n'est pas toujours exacte. Dans les résultats suivants, nous poursuivons l'exploration de cette question.Nous notons que, dans certains cas, la description est en fait complète.

**Corollaire 3.4.2**
Soit $n$ le plus grand des deux nombres premiers jumeaux, alors pour $H = \mathcal{B}_{\pm}(C_n)$, nous avons $\Delta(H) = \{1, n-2\}$.

**Démonstration :**
Puisque $n$ est un nombre premier, chaque élément non nul de $C_n$ a un ordre $n$. Comme $n-2$ est également un nombre premier, en utilisant la notation du théorème 3.4.1, nous avons $D_2 = \{1, n-2\}$. Comme, d'après le lemme 3.4.6, nous avons aussi $1 \in \Delta(H)$, l'énoncé est établi. ■
Cependant, si $n-2$ n'est pas premier, nous ne savons pas quels diviseurs de $n-2$ pourraient être contenus dans $\Delta(H)$. Nous montrons qu'au moins certains d'entre eux peuvent effectivement apparaître comme une distance minimale.

**Lemme 3.4.7**
Soit $n$ un entier impair de la forme $n = a^2 + 1$ pour un entier positif $a$. Alors, pour $H = \mathcal{B}_{\pm}(C_n)$, nous avons $a - 1 \in \Delta(H)$.

**Démonstration :**
Soit $C_n = \langle e \rangle$ et soit $G_0 = \{e, ae\}$. Nous montrons que pour $H_0 = \mathcal{B}_{\pm}(G_0)$, nous avons $\min \Delta(H_0) = a - 1$. D'après le lemme 3.4.2, il suffit d'étudier la longueur des éléments de $A(H_0)$.

Nous rappelons d'abord qu'il existe deux éléments de $\mathcal{A}(H_0)$ contenant uniquement $e$, à savoir $e^2$ et $e^n$. De même, il existe deux éléments contenant uniquement $ae$, à savoir $(ae)^2$ et $(ae)^n$ ; notons que l'ordre de $ae$ est $n$, puisque $a$ et $n$ sont premiers entre eux.

Supposons maintenant que $ev(ae)^w$, avec $v, w \geqslant 1$, appartient à $\mathcal{A}(H_0)$. Nous observons qu'en raison de la minimalité dans une somme nulle pondérée plus-moins de cette séquence, tous les poids de $e$ sont égaux, et de même, tous les poids de $ae$ sont égaux. Cela signifie que soit $ve + wae = 0$, soit $ve + w(-a)e = 0$. Dans le premier cas, $v = n - wa$, pour $w$ allant de 1 à $a$ (remarquons que $n - a^2 = 1$), produit en effet des séquences minimales de somme nulle pondérée plus-moins, tandis que pour $w > a$, la séquence serait divisible par $e(ae)^a$ et ne serait donc pas minimale. Dans le second cas, pour $v = a - k$, avec $k$ allant de 1 à $a - 1$, cela implique que $w = 1 + ka$ et ces séquences sont effectivement des séquences minimales de somme nulle pondérée plus-moins, alors que d'autres choix de $v$ et $w$ ne produisent pas de séquences minimales de somme nulle pondérée plus-moins.

La longueur de ces séquences est $(n - wa) + w = n - (a-1)w$, pour $w$ allant de 1 à $a$, et $(a - k) + (1 + ka) = a + 1 + k(a-1)$, pour $k$ allant de 1 à $a - 1$. Il en résulte que $\mathsf{pgcd}\{|A| - 2 : A \in \mathcal{A}(H_0)\} = a - 1$ ; observons que $a - 1$ divise $n - 2 = a^2 - 1$. ■
Le problème de déterminer l'ensemble $\Delta(H)$ entièrement, même pour $H = \mathcal{B}_{\pm}(C_n)$, pourrait être difficile. Il l'est certainement dans le cas sans pondérations. Il semble

plausible que les résultats sur les distances minimales dans le cas sans pondérations puissent être utilisés. Cependant, au moins pour les p-groupes élémentaires, le problème pour des groupes de rang plus élevé peut être presque entièrement réduit au problème pour les groupes cycliques.

**Lemme 3.4.8**
Soit $G = C_p^r$ un p-groupe élémentaire de rang $r$ pour un certain nombre premier impair $p$. Soit $G_0 \subseteq G \subseteq \{0\}$ et $H_0 = \mathcal{B}_\pm(G_0)$. Si $\min \Delta(H_0) > 1$, alors $G_0 = G_1 \cup \cdots \cup G_k$ où $\langle G_i \rangle$ est cyclique pour chaque $i \in [1,k]$ et $\langle G_0 \rangle = \bigcup_{i=1}^k \langle G_i \rangle$.

**Démonstration :**
Soit $G_0 \subseteq G$, et soit $e_1, \ldots, e_k$ une base de $\langle G_0 \rangle$. Pour prouver l'assertion, il suffit de montrer que si $G_0$ contient un élément $e_0 = \sum_{i=1}^k a_i e_i$ avec $a_i \in [0, p-1]$ et au moins deux des $a_i$ non nuls, alors $\min \Delta(H_0) = 1$.

Sans perte de généralité, nous pouvons supposer que tous les $a_i$ sont non nuls et que $k \geqslant 2$. De plus, nous pouvons supposer que $a_i < p/2$, car nous pourrions remplacer $e_i$ par $(-e_i)$ sans affecter le problème.

Soit maintenant $U = e_0 e_1^{p-a_1} e_2^{p-a_2} e_3^{a_3} \ldots e_k^{a_k}$ et $V = e_0^2 e_1^{p-2a_1} e_2^{p-2a_2} e_3^{2a_3} \ldots e_k^{2a_k}$. Ce sont tous deux des séquences minimales de somme nulle pondérée plus-moins. Nous avons $U^2 = V e_1^p e_2^p$, et ainsi la distance minimale est égale à 1. ■
Ce lemme montre que $\Delta(\mathcal{B}_\pm(C_p^r))$ et $\Delta(\mathcal{B}_\pm(C_p))$ sont très étroitement liés.

**Proposition 3.4.2**
Nous avons $\Delta(\mathcal{B}_\pm(C_p)) \subseteq \Delta(\mathcal{B}_\pm(C_p^r))$ et, réciproquement, chaque élément de $\Delta(\mathcal{B}_\pm(C_p^r))$ est le plus grand commun diviseur d'au plus $r$ éléments de $\Delta(\mathcal{B}_\pm(C_p))$.

**Démonstration :**
La première inclusion est évidente. Pour la seconde inclusion, nous rappelons que, d'après le Lemme 3.12, chaque ensemble $G_0$ qui produit un élément de $\Delta(\mathcal{B}_\pm(C_p^r))$ autre que 1 peut être écrit comme $G_0 = G_1 \cup \cdots \cup G_k$, où $\langle G_i \rangle$ est cyclique pour chaque $i \in [1,k]$ et $\langle G_0 \rangle = \bigcup_{i=1}^k \langle G_i \rangle$. Maintenant, la distance minimale de $\mathcal{B}_\pm(G_0)$ est le plus grand commun diviseur des distances minimales de $\mathcal{B}_\pm(G_i)$ pour $i$ allant de 1 à $k$. ■

**Lemme 3.4.9**
Soit $G$ un groupe abélien fini et soit $e_1, \ldots, e_r$ des éléments indépendants d'ordre pair, en notant $\mathrm{ord}(e_i) = 2^{m_i}$. Supposons que $m_1 + \cdots + m_r \geqslant 2$. Posons $e_0 = m_1 e_1 + \cdots + m_r e_r$, $G_0 = \{e_0, e_1, \ldots, e_r\}$ et $H = \mathcal{B}_\pm(G_0)$. Alors, nous avons

$$\Delta(H) = \{m_1 + \cdots + m_r - 1\}$$

et

$$c(H) = m_1 + \cdots + m_r + 1.$$

**Démonstration :**
Nous déterminons $\mathcal{A}(H)$. Clairement, $e_i^2 \in \mathcal{A}(H)$ pour chaque $0 \leqslant i \leqslant r$. Soit $A \in \mathcal{A}(H)$. Si $e_0 \nmid A$, alors les éléments distincts de $A$ sont indépendants, et le fait que $A$ soit minimal implique que $A$ est égal à $e_i^k$ pour un certain $1 \leqslant i \leqslant r$. Comme l'ordre de $e_i$ est pair, il en résulte que $k = 2$, voir Lemme 3.4.4. Si $e_0^2 \mid A$, nous affirmons que $e_0^2 = A$. Pour voir cela, il suffit de noter que l'ordre de $e_0$ est 2, et donc 0 est la seule somme nulle pondérée par $\pm$ de $e_0^2$, ce qui implique que $Ae_0^{-2}$ est aussi une somme nulle pondérée par $\pm$. La seule façon de ne pas contredire la minimalité de $A$ est que $Ae_0^{-2}$ soit vide.

Il reste donc à considérer le cas où $A$ contient $e_0$ exactement une fois. Nous montrons que dans ce cas, $A$ est égal à $U = e_0 \prod_{i=1}^r e_i^{m_i}$. Nous notons que $(m_i e_i)e_i^k$ est une séquence somme nulle minimale pondérée par $\pm$ si et seulement si $k = m_i$ ; nous nous référons au Lemme 6.6 dans [2.5.4] pour un argument détaillé. L'assertion découle maintenant de l'indépendance des $e_i$.

Ainsi, nous avons établi que $\mathcal{A}(H) = \{U, e_0^2, e_1^2, \ldots, e_r^2\}$. Maintenant, $U^2 = e_0^2 \prod_{i=1}^r (e_i^2)^{m_i}$ est la seule relation non triviale entre ces atomes, et l'assertion en découle. ■

Nous notons que $e_1, \ldots, e_r$ est un ensemble générateur indépendant d'éléments d'ordre pair, disons $\mathsf{ord}(e_i) = 2m_i$, avec $\mathsf{ord}(e_i) \mid \mathsf{ord}(e_{i+1})$, alors $\mathsf{D}(\mathcal{B}_\pm(G)) = m_1 + \cdots + m_r + 1$, et donc, pour un groupe avec $r_2(G) = \mathsf{r}(G)$, nous avons $\mathsf{D}(\mathcal{B}_\pm(G)) - 2 \in 2\Delta(\mathcal{B}_\pm(G))$.

**Proposition 3.4.3**
Soit $G$ un groupe abélien fini et soit $H = \mathcal{B}_\pm(G)$.

1. Si $G$ est cyclique d'ordre au moins 3, alors $\max \Delta^*(H) = \mathsf{D}(H) - 2$.
2. Si $G$ est un 2-groupe élémentaire d'ordre au moins 4, alors $\Delta^*(H) = [1, \mathsf{D}(H) - 2]$.
3. Si $G$ est un groupe d'exposant 4, alors $[1, \mathsf{D}^*(H) - 2] \subseteq \Delta^*(H) \subseteq [1, \mathsf{D}(H) - 2]$.
4. Si $G = C_n \oplus C_{2n}$ pour un certain $n$ impair avec $n \geqslant 3$, alors $\mathsf{D}^*(H) - 2 \leqslant \max \Delta^*(H) \leqslant \mathsf{D}(H) - 2$.

**Démonstration :**
Nous rappelons que nous avons toujours $\max \Delta^*(H) \leqslant \mathsf{D}(H) - 2$. Soit $G = \langle e_1 \rangle$ cyclique d'ordre $n \geqslant 3$. Si $n$ est impair, alors $\mathsf{D}(H) - 2 = n - 2$, et $\Delta(\{e\}) = n - 2$. Ainsi, l'affirmation s'ensuit. Dans tous les autres cas, sauf pour le cas 4, nous avons $\mathsf{r}_2(G) = \mathsf{r}(G)$ et nous avons $D^*(\mathcal{B}_\pm(G)) - 2 \in \Delta(\mathcal{B}_\pm(G))$. Si $n = 2m$ est pair, alors $\mathsf{D}(H) - 2 = m - 1$ et $\Delta(\{e, me\}) = m - 1$.

Si $G = \bigoplus_{i=1}^r \langle e_i \rangle$ est un 2-groupe élémentaire de rang $r$, alors $D^*(H) - 2 = r - 1$, et donc $r - 1$ est un élément de $\Delta(H)$. Puisque $H_s = \mathcal{B}_\pm(\bigoplus_{i=1}^s \langle e_i \rangle)$ est un sous-monoïde fermé par diviseurs de $H$ pour chaque $s \leqslant r$, nous avons que $\Delta(H_s) \subseteq$

$\Delta(H)$. Puisque $D^*(\mathcal{B}_\pm(\bigoplus_{i=1}^s \langle e_i \rangle)) = s+1$, l'affirmation s'ensuit en utilisant le même argument que pour $s = r$.

Supposons que $G = \bigoplus_{i=1}^r \langle e_i \rangle$ avec $\mathrm{ord}(e_i) \mid \mathrm{ord}(e_{i+1})$ soit un groupe d'exposant 4 et de rang $r$. Comme ci-dessus, nous avons $D^*(\mathcal{B}_\pm(G)) - 2 \in \Delta(\mathcal{B}_\pm(G))$. Pour compléter l'argument, il suffit de montrer que $G$ possède un sous-groupe $G'$ avec $D^*(\mathcal{B}_\pm(G')) = D$ pour chaque $D \in [3, D^*(\mathcal{B}_\pm(G))]$. Nous définissons $G_1 = \bigoplus_{i=1}^{r-1} \langle e_i \rangle \oplus \langle 2e_r \rangle$. Alors $D^*(\mathcal{B}_\pm(G_1)) = D^*(\mathcal{B}_\pm(G)) - 1$. L'argument suit alors par induction directe.

Soit $C_n \oplus C_{2n} = \langle e_1 \rangle \oplus \langle e_2 \rangle$ avec $\mathrm{ord}(e_1) = n$ et $\mathrm{ord}(e_2) = 2n$. Nous considérons $G_0 = \{e_1 + e_2, e_2\}$. Nous déterminons $A(\mathcal{B}_\pm(G_0))$. Clairement, nous avons $V_1 = (e_1 + e_2)^2$ et $V_2 = e_2^2$ et aucun autre élément n'implique uniquement l'un des deux éléments. De plus, nous trouvons $U = (e_1 + e_2)^n e_2^n$. Nous avons $U^2 = V_1^n V_2^n$ et en effet $L(U^2) = \{2, 2n\}$, et nous trouvons que $\Delta(\mathcal{B}_\pm(G_0)) = \{2n-2\}$. Nous rappelons que $D^*(H) = n - 1 + \frac{2n}{2} + 1 = 2n$, établissant ainsi l'affirmation. ■

**Proposition 3.4.4**
Soit $G$ un groupe abélien fini et soit $H = \mathcal{B}_\pm(G)$.

1. Alors $\max \Delta^*(H) = 1$ si et seulement si $\exp(G) = 3$, ou $G = C_2^2$, ou $G = C_4$.
2. Alors $\max \Delta^*(H) = 2$ si et seulement si $G = C_3^2$ ou $G = C_2 \oplus C_4$.

Nous terminons cette section avec un résultat qui peut sembler étrange au premier abord, mais qui est très utile dans le contexte de la section suivante.

**Théorème 3.4.2**
Soit $G$ un groupe abélien fini tel que $|G| \geqslant 5$. Les énoncés suivants sont équivalents :

1. $|G|$ est pair.
2. $\Delta^*(H)$ contient un élément pair.
3. $\Delta_1^*(H)$ contient un élément pair.

**Démonstration :**
Supposons que $\Delta^*(H)$ contienne un élément pair. Alors, $|G|$ ne peut pas être impair, car cela contredirait le théorème 3.4.1 étant donné que tous les éléments de $D_2$ sont impairs. Il reste à montrer que si $|G|$ est pair, alors $\Delta^*(H)$ contient un élément pair. Si $G$ n'est pas un 2-groupe, alors $G$ contient un élément d'ordre $2m$ pour un certain $m \geqslant 2$ impair. Par le lemme 4.2.1, nous savons que $m-1 \in \Delta^*(H)$, et cet élément est pair.

Supposons donc que $G$ soit un 2-groupe. Si le rang de $G$ est au moins 3, alors par la proposition 3.4.3, $\Delta^*(H)$ contient 2, et si le rang est 2, alors par le lemme 3.4.8, il contient $\exp(G)/2$, qui est pair car $\exp(G) \neq 2$ en raison de l'hypothèse $|G| \geqslant 4$.

Il reste à étudier le cas des 2-groupes cycliques. Nous notons que pour $h$, un élément d'ordre 8, le sous-monoïde des suites sur $\{e, 3e\}$ a une distance minimale de 2. ■

## 3.5 Codes correcteurs

Nous avons travaillé tout au long de notre article sur les longueurs,les distances et les différents invariants arithmétiques et les suites à somme nulle ayant un lien avec les distances minimales d'un code linéaire. A cet effet, nous allons rappeler et voir les codes linéaires avec ses paramètres.

### 3.5.1 Codes linéaires

Pour cette partie, voir le livre [9]

**$c$ comme sous-espace vectoriel**

On munit $A^n$ de sa structure naturelle d'espace vectoriel sur $\mathbb{F}_2$ : $A^n$ est isomorphe à $\mathbb{F}_2^n$ et on prend pour $C$ un sous-espace vectoriel de dimension $k$ de $A^n$. le codage $\gamma$ : $A^k ß A^n$ est une application linéaire injective qu'on peut définir de plusieurs manières. La matrice $G$ de $\gamma$ par rapport aux bases canoniques de $A^k$ et $A^n$ est appelé matrice génératrice du code. Ses colonnes sont les images dans $A^n$des vecteurs de la base canonique de $A^k$ et forme une base de $C$.
Comme $d_H(c, c^{'}) = \pi(c - c^{'})$ et que $c - c^{'} \in C$, la distance minimale $d$d'un code linéaire est égale au poids minimum d'un mot non nul de $C$.
Notons $E$ le sous-espace vectoriel de $A^n$ des suites commençant par $k-1$ bits 0. On a $dim(E) = n-k-1$, donc $dim(C) + dim(E) > dim(A^n)$. L'intersection de $C$ et $E$ n'est pas réduite à 0, par conséquent, il existe dans $C$ des éléments de poids inférieur ou égal à $n + 1 - k$, d'où

$$d \leqslant n - k + 1 = r + 1.$$

Cette majoration est naturelle ; elle signifie qu'il faut faire un effort sur la redondonce $r$ pour pouvoir corriger plus d'erreurs.

**Analyse du message reçu**

Le décodage des codes linéaires n'est pas, en général, un problème facile. On utilise les formes linéaires $A^n$ : $A$ s'annulant sur $C$. On dit qu'elles forment un espace vectoriel $C^{\perp}$ qu'on a appelé, au chapitre 10 , dual de l'espace vectoriel $C$ ; $C^{\perp}$ est de dimension $n - k$. On a vu aussi que les éléments de $A^n$ annulés par les formes linéaires de $C^{\perp}$ ; par conséquent, $C$ est le noyau d'une application linéaire $\eta$ : $A^n ß A^{n-k}$ ayant pour composantes les élements d'une base d'une base de $C^{\perp}$.

La matrice $H$ d'une telle application est appelée matrice de contrôle ; elle est nulle pour tousles vecteurs du code et on a $HG = 0$.
Pour faire parvenir un message $x$, on envoie $c = \gamma(x)$ ; si$y$ est le message reçu,l'erreur est la suite $e = y - c$(on a aussi $e = y + c$ dans $A^n$) et on a $\eta(e) = \eta(y)$.
C'est à partir de $\eta(e)$ qu'il faut retrouver $e$ ; on peut alors trouver $c = y + e$, puis le message initial $x = \gamma^{-1}(c)$. Si $\eta(y) = 0$, on a $y \in C$, on pose $c = y$ et on retrouve $x$.

**Calcul matriciel**

Pour utiliser un code linéaire, le calcul matriciel s'impose. Nous adoptons pour cette section la notation suivante : si on a une suite de suite de bits $b = (b_1, \ldots, b_m)$, on note avec un prime la matrice colonne associée : $b^{'} = t(b_1 \ldots b_m)$ dont les coefficients sont les $b_i$. Pour envoyer le message $x = (x_1, \ldots, x_k)$ de $A^k$, on transmet le mot du code $c = \gamma(x)$ tel que $c^{'} = Gx^{'}$.
Notons que que l'usage est d'écrire , en théorie des codes, les vecteurs en ligne, ce qui conduit à transposer toutes les égalités matricielles qui vont suivre et oblige à une petite gymnastique que je ne vous impose pas.

**Code de Hamming(7,4,3)**

C'est en 1948, dans son grand article, que Shannon présente le code correcteur de Hamming. On peut s'en servir quand on suppose que la transmission peut créer au plus une erreur. Dans ce code, un message est une suite de 4 bits $x = (x_1, x_2, x_3, x_4) \in A^4$ qu'on code en $c = \gamma(x) = (u, v, x_1, w, x_2, x_3, x_4) \in A^7$, avec :
$u = x_1 + x_2 + x_4$,
$v = x_1 + x_3 + x_4$,
$w = x_2 + x_3 + x_4$.

La matrice de contrôle $H$ est donnée par ces trois égalités ($w + x_2 + x_3 + x_4 = 0$ donne la première ligne, etc.) et la matrice génératrice $G$ a pour colonnes les images par $\gamma$ des vecteurs de la base canonique, vecteurs formant uhne base du code $C$ :

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Les seize mots de $C$ s'obtiennent par combinaison linéaire des vecteurs de cette base. Les voici. $(0,0,0,0,0,0,0)(1,1,1,0,0,0,0)(1,0,0,1,1,0,0)(0,1,0,1,0,1,0)$
$(1,1,0,1,0,0,1)(0,1,1,1,1,0,0)(1,0,1,1,0,1,0)(0,0,1,1,0,0,1)$
$(1,1,0,0,1,1,0)(0,1,0,0,1,0,1)(1,0,0,0,0,1,1)(0,0,1,0,1,1,0)$
$(1,0,1,0,1,0,1)(0,1,1,0,0,1,1)(0,0,0,1,1,1,1)(1,1,1,1,1,1,1)$

On peut vérifier que la distance de Hamming de ce code est 3 et que le code est parfait : $A^7$ a $2^7 = 128$ éléments qui répartissent dans 16 boules de rayon 1 ayant 8 éléments. Ce code permet donc de corriger une erreur.
Quand on reçoit la suite $y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7)$ de sept bits, on calcule $Hy^{'}$. Si $Hy^{'} = 0$, le message a été transmis sans erreur et on pose $c = y$. Si $Hy^{'} \neq 0$, c'est qu'une erreur de transmission $e$ a lieu et il existe $c \in C$ tel que $d_H(y, c) = 1$ et $c = y + e$. Hamming explique que les colonnes de $H$ sont les écritures en binaire des nombres 1 à 7. Comme la suite $e$ ne comporte qu'un seul terme non nul, $He^{'} = Hy^{'}$ est la colonne de $H$ correspondant à la position de l'erreur et on trouve $e$.
C'est à partir de cette propriété que le code a été construit.
Par exemple , si on veut envoyer $x = (1, 0, 1, 1)$, on envoie le message codé $Gx^{'} = c^{'}$, avec $c = (0, 1, 1, 0, 0, 1, 1)$. Si on reçoit le message $y = (0, 1, 1, 0, 0, 0, 1)$ avec une erreur $e = (0, 0, 0, 0, 0, 1, 0)$, au rang 6, on a $Hy^{'} =$

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

, la sixième colonne de $H$, ce qui implique bien le rang 6. On peut considérer que c'est $x = (1, 0, 1, 1)$ qui a été envoyé.

### 3.5.2 Lien entre les codes linéaires et les suites à somme nulle pondérées

Dans cette section, nous développons le lien entre les problèmes à somme nulle entièrement pondérés et les problèmes sur les codes linéaires qui a déjà été mentionné dans l'introduction. Nous rappelons que pour les 2-groupes élémentaires, ce lien était déjà connu.Notons qu'en fait pour ces groupes, le problème à somme nulle pondérée coïncide avec le problème classique, et le lien est apparu dans ce context (Voir section 4 de [30]). De plus, nous rappelons que pour les 3-groupes élémentaires. le problème entièrement pondéré coïncide avec le problème pondéré plus-moins, ce qui est un intérêt particulier.

Avant de discuter du lien avec la théorie du code, nous rappelons quelques faits de base liés aux problèmes à somme nulle entièrement pondérés sur les $p$-groupes

élémentaires. Soit $p$ un nombre premier. Soit $G$ un groupe d'exposant $p$, et soit $A = \{1, \ldots, p-1\}$ l'ensemble des poids. Rappelons que $G$ peut être considéré d'une manière naturelle comme un espace vectoriel sur d'un corps avec $p$ éléments. Nous identifions également les éléments de $A$ avec les éléments non nuls de $\mathbb{F}_p$ d'une manière naturelle. De plus, nous rappelons qu'une séquence $S = g_1 \ldots g_n$ sur $G$ n'a pas de somme nulle pondérée par $A$ si et seulement si $(g_1, \ldots, g_n)$ est linéairement indépendante, en particulier.

$$D_A(C_p^r) = r + 1 \text{ et } s_{A,\leqslant r+1}(C_p^r) = r + 1.$$

Maintenant, nous rappelons brièvement quelques notions de la théori du code d'une manière adaptée à notre application. Comme nous l'avons dit plus haut, $C_p^n$ est d'une manière naturelle un espace vectoriel sur $\mathbb{F}_p$ le corps avec $p$ éléments. Nous fixons implicitement une base de $C_p^n$, et nous pouvons donc écrire ses éléments simplement comme $n$-tuples d'éléments de $\mathbb{F}_p$ :

$$C_p^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_p, 1 \leqslant i \leqslant n\}.$$

Un code linéaire $p$-aire de longueur $n$ et de dimension $k$ est un sous-espace vectoriel $C \subset C_p^n$ de dimension $k$. Brièvement, nous disons que $C$ est un $[n, k]$ $p$-code. Les éléments du code $C$ sont appelés mots-codes. Le support d'un élément $x = (x_1, x_2, \ldots, x_n)$ de $C_p^n$ est le sous-ensemble de $\{1, \ldots, n\}$ correspondant aux indices des coordonnées non nulles $x_i$(C'est l'usage du mot "support" courant dans la théorie du code, dans le contexte des suites à somme nulle, le mot "support" a typiquement un sens différent).Le poids d'un élément $x \in C_p^n$, noté $d(x)$ est la cardinalité du support de $x$. La distance minimale d'un code $C$ notée $d(C)$, est égale à la distance minimale $d(x)$ avec le support de $x$. La distance minimale d'un code $C$, notée $d(C)$ est égale au minimum $d(x)$ avec $x$ un mot du code non nul de $C$, c'est-à-dire que la distance minimale du code $C$ est égale à la cardinalité du support de $x$. Si $C$ a une distance minimale, la distance minimale est égale à la cardinalité minimale du support d'un élément non nul de $C$. Si $C$ a une distance minimale $d$, on dit que $C$ est un code $[n, k, d]_p$.Étant donné que dans la mesure où, dans le présent document, nous ne considérons que les codes linéaires, nous choisissons la manière rapide, mais pas très intuitive, d'introduire la distance minimale dans les codes linéaires.

Une matrice de contrôle de parité d'un code $[n, k]_p$. C'est une matrice $H$ de dimension $(n-k) \times n$ (avec rang complet) sur $F_p$ telle que $c \in C$ si et seulement si $Hc = 0$(où nous considérons $c$ comme une colonne vecteur). Pour $H = [g_1| \cdots |g_n]$, nous pouvons interpréter les colonnes $g_i$ comme des éléments de $C_p^{n-k}$ , où encore une fois, une base est fixée, et de cette manière, on peut attribuer à un $p$-code $[n, k]$ une suite $= g_1 \ldots g_n$ de longueur $n$ sur $C_p^{n-k}$ . Maintenant, $c = (c_1, \ldots c_n) \in C$ signifie que $\sum_{i=1}^n c_i g_i = 0$. Si $I$ noté le support de $c$, alors on a $\sum_{i \in I} c_i g_i = 0$ pour

$c_i \neq 0$. En d'autres termes, $\sum_{i\in I} c_i g_i = 0$ est une somme nulle pondérée $A$ de $S$ (éventuellement la somme vide). Sa longueur est exactement la cardinalité du support de $c$ c'est-à-dire $d(c)$. Inversement, si $\sum_{i\in I} c'_i g_i = 0$ est une somme nulle pondérée $A$ (éventuellement vide) de $S$, alors $c' = (c'_1, \ldots, c'_n)$, où nous fixons $c'_i = 0$ pour $i \notin J$, est un élément de $C$ avec un poids $|J|$, la longueur du sous-somme. Bien sûr, $0 \in C$ correspond au sous-somme zéro vide pondéré par $A$. Ainsi, nous avons donc une correspondance directe entre les mots de code non nuls et les sous-sommes nulles pondérées $A$. Nous résumons ces résultats dans les lemmes ci-dessous (rappelons que $A = \{1, \ldots, p-1\}$).

**Lemme 3.5.1**
La distance minimale d'un code linéaire $p$-aire $C$ est égale à la longueur minimale d'une somme nulle pondérée $A$ des colonnes d'une matrice de contrôle de parité de $C$.

**Démonstration :**
La discussion qui précède le confirme. ■

**Lemme 3.5.2**
Soit $S = g_1 \ldots g_n$ une suite sur $C_p^r$ (avec une base fixée) telle que l'ensemble de tous les $g_i$ est un ensemble générateur de $C_p^r$. De plus, laissons $H = [g_1| \ldots |g_n]$ représenter la matrice $r \times n$ sur le champ $\mathbb{F}_p$(nous identifions les $g'_i s$ avec leurs vecteurs de coordonnées, sous forme de colonnes). Le code $C_S$ avec la matrice de contrôle de parité $H$ est alors un code $[n, n-r]_p$. Et, chaque code $[n, n-r]_p$ peut être obtenu de cette manière.

**Démonstration :**
Puisque l'ensemble des $g'_i s$ est un ensemble générateur de $C_p^r$, la matrice $H$ a un rang complet c'est-à-dire un rang $r$. Par conséquent, $C_S$ est un sous-espace de $(n-r)$-dimension de $C_p^n$. Cela donne la première affirmation. La deuxième affirmation s'ensuit, puisque pour chaque code $[n, n-r]_p$, il existe une matrice de contrôle de parité $r \times n$, qui a un rang complet. ■

**Lemme 3.5.3**
Soit $d, r \in \mathbb{N}$ et $p$ premier. Alors $s_{A,\leqslant d}(C_p^r) - 1$ est égal au maximun $n$ tel qu'il existe un code $[n, n-r]_p$ de distance minimale au moins $d+1$.

**Démonstration :**
Par définition $s_{A,\leqslant d}(C_p^r)$, il existe une suite $S$ sur $C_p^r$ de longueur $s_{A,\leqslant d}(C_p^r) - 1$ qui n'a pas de somme nulle pondérée par $A$ d'une longueur maximale de $d$. En outre les éléments de $S$ engendrent $C_p^r$. [30, Voir Lemme 3.8] Ainsi,$C_S$ est un code

$[n, n-r]_p$, et il ne peut pas avoir un mot de code non nul de poids au plus d c'est-à-dire que sa distance minimale est au moins $d+1$ avec $d^{'} > d$, nous obtenons une suite $S_C$ Inversement, étant donné un code $[n, n-r, d']$ sur $C_p^r$ de longueur $n$ dont la somme nulle la plus courte pondérée par $A$ a une longueur $d' > d$. Ainsi, nous obtenons une suite $S_C$ sur $C_p^r$ de longueur $n$ dont la distance minimale est $d' > d$. Ainsi,$s_{A,\leqslant d}(C_p^r) > n$ , ce qui complète l'argument. ■

Nous terminons cette section générale sur le lien entre les codes linéaires et les problèmes de suites nulles pondérées $A$ en soulignant que l'existence de $m$ sous-suites nulles pondérées disjointes d'une suite $S$ correspond précisément à l'existence de $m$ mots du code non nuls dans $C_S$ dont les supports sont disjoints par paire. Cela rejoint une notion considérée dans la théorie du code, en particulier dans le cas où $m = 2$ du code. Nous rappelons que Cohen et Lempel [30, Voir section 4]ont appelé un code linéaire pour lequel deux mots du code non nuls n'ont pas de support disjoint, un code d'intersection. Nous nous référons à [30, Voir section 4]pour une discussion plus détaillée des codes intersectés (binaires) dans le contexte actuel.

## 3.6 Applications au problème de caractérisation

Il est évident que des groupes isomorphes $G$ et $G'$ produisent des monoïdes isomorphes de suites à somme nulle $\mathcal{B}(G)$ et $\mathcal{B}(G')$, et par conséquent, les systèmes d'ensembles de longueurs sont égaux $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$. La même chose est vraie si l'on considère des suites à somme nulle pondérées avec plus-moins (ou en fait, des suites à somme nulle pondérées pour tout choix de poids). Une question naturelle à poser est dans quelle mesure ces implications peuvent être inversées. Pour la première implication, cela s'appelle le Problème de l'isomorphisme, c'est-à-dire le problème de déterminer si l'isomorphie des monoïdes de suites à somme nulle (pondérées) implique l'isomorphie des groupes sous-jacents. Ce problème est complètement résolu pour les groupes abéliens finis sans poids et avec des poids plus-moins. De plus, la question analogue pour les groupes non commutatifs est également résolue.

En ce qui concerne la question impliquant les longueurs, cela s'appelle le Problème de caractérisation. Sous sa forme classique, il peut être énoncé en demandant si, pour $G$ et $G'$ des groupes abéliens finis tels que $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$, il en découle que $G$ et $G'$ sont isomorphes. L'histoire de ce problème remonte à plus de cinquante ans et est initialement apparue dans le contexte de la caractérisation arithmétique du groupe des classes d'un anneau d'entiers algébriques, d'où son nom. Nous mentionnons que la condition selon laquelle le groupe est fini est cruciale. Tous les groupes abéliens infinis produisent le même système d'ensembles de

longueurs, qui diffère de celui de tout groupe fini. Cela est connu sous le nom de Théorème de Kainrath.

Il est bien connu et facile de voir que $C_1$ et $C_2$ donnent tous deux lieu à des monoïdes semi-factoriels de suites à somme nulle ; en effet, les monoïdes sont même libres. À part cet exemple simple, il existe une autre paire de groupes non isomorphes connue qui produit le même système d'ensembles de longueurs pour leurs monoïdes de suites à somme nulle, à savoir $C_3$ et $C_2^2$. Il est donc courant d'imposer la condition supplémentaire que la constante de Davenport du groupe soit au moins 4. La conjecture actuelle est que ce sont les seuls cas où cela se produit et que, pour chaque groupe abélien fini $G$ qui n'est pas isomorphe à l'un de ces groupes, une condition qui assure cela est de supposer que $\mathsf{D}(\mathcal{B}(G)) \geqslant 4$. Il est en effet vrai que $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$ implique que $G$ et $G'$ sont isomorphes. Nous renvoyons à [38] et [42] pour un aperçu des résultats plus anciens sur le sujet et à [20] pour des contributions plus récentes. Une première recherche sur le problème de caractérisation pour les problèmes de somme nulle pondérés $\pm$, et plus largement sur le problème de décrire le système des ensembles de longueurs pour les problèmes de somme nulle pondérés plus-moins a été entreprise dans [22].

Comme dans le cas sans poids, $C_1$ et $C_2$ donnent tous deux lieu à des monoïdes demi-factoriels de séquences à somme nulle, en effet même des monoïdes libres. Pour d'autres groupes de petit ordre, les auteurs ont prouvé le résultat suivant.

**Théorème 3.6.1**
$\mathcal{L}(\mathcal{B}_{\pm}(C_2^2)) = \mathcal{L}(\mathcal{B}_{\pm}(C_3)) = \mathcal{L}(\mathcal{B}_{\pm}(C_4)) = \{y + 2k + [0, k] : y, k \in \mathbb{N}_0\}$. Réciproquement, si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \{y + 2k + [0, k] : y, k \in \mathbb{N}_0\}$ pour un groupe abélien fini $G$, alors $G$ est isomorphe à l'un des trois groupes $C_2^2$, $C_3$, $C_4$.

Notez que les ensembles $y + 2k + [0, k]$ sont simplement les ensembles $\{m, m + 1, m + 2, \ldots, n\}$ avec $\frac{n}{m} \leqslant \frac{3}{2}$. De plus, les auteurs ont résolu le problème de caractérisation pour les groupes cycliques d'ordre impair [22].

Dans la section actuelle, nous essayons de progresser davantage sur ce problème en utilisant nos résultats sur $\Delta^*$.

Dans la plupart des cas, il est assez difficile de décrire complètement $\mathcal{L}(H)$. Pour résoudre le problème de caractérisation, on procède souvent de la manière suivante. On établit que si $\mathcal{L}(H) = \mathcal{L}(H')$, alors certains invariants arithmétiques de $H$ et $H'$ sont égaux. En utilisant des résultats sur ces invariants arithmétiques, on obtient des informations sur $H$ et $H'$. Pour les invariants qui sont définis, ou du moins peuvent être définis, purement via le système de ensembles de longueurs, tels que $\rho$, $\rho_k$, $\lambda_k$, $U_k$, $\Delta$ et $\Delta_1$, il est clair que l'égalité de $\mathcal{L}(H)$ et $\mathcal{L}(H')$ implique l'égalité des invariants respectifs pour $H$ et $H'$. Puisque pour $H = \mathcal{B}_{\pm}(G)$ et $H' = \mathcal{B}_{\pm}(G')$, nous savons que $\rho_2(H) = \mathsf{D}(H)$ et $H' = \mathcal{B}_{\pm}(G')$, il en résulte que l'égalité de $\mathcal{L}(H)$ et $\mathcal{L}(H')$ implique aussi que $\mathsf{D}(H) = \mathsf{D}(H')$. De même, le fait que $\Delta^*(H) \subseteq \Delta_1^*(H) \subseteq \{d_0 \mid d : d \in \Delta^*(H)\}$ implique que, dans le cas où $\mathcal{L}(H) = \mathcal{L}(H')$, les

ensembles $\Delta^*(H)$ et $\Delta_1^*(H)$ sont étroitement liés.$\max \Delta^*(H) = \max \Delta_1^*(H')$ et plus précisément, si $M$ désigne ce maximum, alors les ensembles $\Delta^*(H) \cap \mathbb{N}_{>M/2}$ et $\Delta_1^*(H') \cap \mathbb{N}_{>M/2}$ sont égaux.

Ensuite, on utilise des résultats qui donnent les valeurs de ces invariants arithmétiques en termes d'invariants algébriques des groupes, afin d'établir des conditions sur les groupes, et idéalement leur isomorphisme.

**Théorème 3.6.2**
Soit $G$ un groupe abélien fini d'ordre impair et soit $G'$ un groupe abélien fini. Nous posons $H = \mathcal{B}_{\pm}(G)$ et $H' = \mathcal{B}_{\pm}(G')$. Si $\mathsf{L}(H) = \mathsf{L}(H')$, alors $\exp(G) = \exp(G')$ et $\mathsf{D}(G) = \mathsf{D}(G')$.

**Démonstration :**
Nous savons que $\rho(H) = \rho(H')$ et $\Delta(H) = \Delta(H')$. Par le théorème 3.4.1, nous savons que $\max \Delta_1(H) = \exp(G) - 2$.

Par le théorème 3.4.2, nous savons que $\Delta_1(H)$ ne contient que des éléments impairs. Ainsi, $\Delta_1(H')$ ne contient également que des éléments impairs, et $G'$ est donc un groupe d'ordre impair. Ainsi,$\max \Delta_1(H') = \exp(G_0) - 2$, et donc $\exp(G) = \exp(G')$.

Pour obtenir le résultat concernant les constantes de Davenport, il suffit de rappeler que $\rho(H) = \frac{\mathsf{D}(H)}{2}$ et $\rho(H') = \frac{D(H')}{2}$, et puisque $G$ et $G'$ sont impairs, nous avons $\mathsf{D}(H) = \mathsf{D}(G)$ et $\mathsf{D}(H') = \mathsf{D}(G')$. ■
Nous insistons sur le fait que les constantes de Davenport classiques de $G$ et $G'$ sont effectivement égales, car pour les groupes d'ordre impair ou, de manière équivalente, d'exposant impair, elles sont respectivement égales à $\mathsf{D}(\mathcal{B}_{\pm}(G))$ et $\mathsf{D}(\mathcal{B}_{\pm}(G'))$.

Ce résultat permet de prouver que les groupes élémentaires $p$-groupes pour $p$ impair sont caractérisés. Comme le même raisonnement permet de caractériser certains autres $p$-groupes et des groupes d'exposant impair, nous commençons par une proposition technique.

**Proposition 3.6.1**
Soit $G$ un groupe abélien fini d'exposant $n$ impair et de constante de Davenport $D$ tel qu'il n'existe aucun groupe non isomorphe à $G$ ayant également $n$ et la constante de Davenport $D$. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Par le théorème 4.2.2, nous savons que les exposants de $G$ et $G'$ sont égaux et que les constantes de Davenport de $G$ et $G'$ sont égales. L'affirmation est donc évidemment vraie par l'hypothèse sur $G$. ■
Nous notons d'abord que ce résultat fournit une preuve alternative de la caractérisation des groupes cycliques d'ordre impair.

**Corollaire 3.6.1**
Soit $G$ un groupe cyclique d'ordre impair. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Un groupe cyclique satisfait la condition de la proposition 4.2.1, car les groupes cycliques sont les seuls groupes pour lesquels l'exposant est égal à la constante de Davenport. ■

**Corollaire 3.6.2**
Soit $G$ un groupe élémentaire $p$-groupe pour $p$ impair. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Pour un groupe $G$ avec $\exp(G)$ premier, la constante de Davenport est donnée par $1 + \mathsf{r}(G)(\exp(G) - 1)$ et donc les $p$-groupes élémentaires satisfont la condition de la proposition 4.2.1. ■

**Corollaire 3.6.3**
Soit $G = C_p \oplus C_n$ où $n$ est impair et $p$ est le plus petit diviseur premier de $n$. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Il suffit de montrer que les groupes satisfont la condition de la proposition 4.2.1. Tout d'abord, rappelons que la constante de Davenport de $G$ est $n + p - 1$, car le groupe est de rang deux. Maintenant, si $G'$ est un groupe avec exposant $n$, alors soit $G'$ est cyclique, soit de la forme $H \oplus C_n$ où $1 \neq \exp(H) \mid n$. Dans le premier cas, la constante de Davenport de $G'$ est $n$, et donc elle n'est pas égale à celle de $G$. Dans le second cas, la constante de Davenport est au moins $n+\mathsf{D}(H)-1 \geqslant n+\exp(H)-1$ et donc strictement supérieure à $n + p - 1$, sauf si $\exp(H) = p$ et $\mathsf{D}(H) = \exp(H)$. Ainsi, nous obtenons que $H$ est cyclique d'ordre $p$, ce qui implique la conclusion. ■

**Lemme 3.6.1**
Soit $K$ un $p$-groupe avec constante de Davenport $D$.

1. Si $\mathsf{D} < p^2$ et $K'$ est un autre $p$-groupe avec constante de Davenport $\mathsf{D}$, alors $K$ et $K'$ sont isomorphes.
2. Si $\mathsf{D} \geqslant p^2$, alors il existe un $p$-groupe $K'$ avec constante de Davenport $\mathsf{D}$ tel que $K$ et $K'$ ne sont pas isomorphes.

**Démonstration :**
Pour voir le premier point, il suffit de noter que $\mathsf{D} < p^2$ implique que $\exp(K) < p^2$ et $\exp(K') < p^2$. Ainsi, les deux ont pour exposant $p$ et l'affirmation s'ensuit directement.

Pour le second point, nous distinguons deux cas. Supposons que l'exposant de $K$ est $p$, disons $K \equiv C_p^r$. D'après l'hypothèse sur la constante de Davenport, on obtient que $r \geqslant p+1$. Pourtant, $K' = C_p^{r-p-1} \oplus C_{p^2}$ a la même constante de Davenport.

Maintenant, supposons que l'exposant de $K$ n'est pas premier, disons qu'il est $p^k$ avec $k > 1$. Soit $K_0$ un groupe tel que $K \equiv K_0 \oplus C_{p^k}$. Ensuite, posons $K' = K_0 \oplus C^p_{(p^k-1)/(p-1)}$, qui a la même constante de Davenport. ■

**Corollaire 3.6.4**
Soit $G$ un $p$-groupe pour $p$ impair et supposons que $\mathsf{D}(G) < \exp(G) + p^2 - 1$. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Nous notons que le groupe $G$ satisfait la condition de la proposition 4.2.1. En effet, soit $G = K \oplus C_{\exp(G)}$. Alors $\mathsf{D}(G) = \exp(G) + \mathsf{D}(K) - 1$. Le résultat découle maintenant du lemme 3.4.8 ■

# 4 | Applications

## 4.1 Codes correcteurs

Nous avons travaillé tout au long de notre article sur les longueurs,les distances et les différents invariants arithmétiques et les suites à somme nulle ayant un lien avec les distances minimales d'un code linéaire. A cet effet, nous allons rappeler et voir les codes linéaires avec ses paramètres.

### 4.1.1 Codes linéaires

Pour cette partie, voir le livre [9]

**$c$ comme sous-espace vectoriel**

On munit $A^n$ de sa structure naturelle d'espace vectoriel sur $\mathbb{F}_2$ : $A^n$ est isomorphe à $\mathbb{F}_2^n$ et on prend pour $C$ un sous-espace vectoriel de dimension $k$ de $A^n$.
le codage $\gamma$ : $A^k ß A^n$ est une application linéaire injective qu'on peut définir de plusieurs manières. La matrice $G$ de $\gamma$ par rapport aux bases canoniques de $A^k$ et $A^n$ est appelé matrice génératrice du code. Ses colonnes sont les images dans $A^n$des vecteurs de la base canonique de $A^k$ et forme une base de $C$.
Comme $d_H(c, c^{'}) = \pi(c - c^{'})$ et que $c - c^{'} \in C$, la distance minimale $d$d'un code linéaire est égale au poids minimum d'un mot non nul de $C$.
Notons $E$ le sous-espace vectoriel de $A^n$ des suites commençant par $k-1$ bits 0. On a $dim(E) = n-k-1$, donc $dim(C) + dim(E) > dim(A^n)$. L'intersection de $C$ et $E$ n'est pas réduite à 0, par conséquent, il existe dans $C$ des éléments de poids inférieur ou égal à $n + 1 - k$, d'où

$$d \leqslant n - k + 1 = r + 1.$$

Cette majoration est naturelle ; elle signifie qu'il faut faire un effort sur la redondonce $r$ pour pouvoir corriger plus d'erreurs.

**Analyse du message reçu**

Le décodage des codes linéaires n'est pas, en général, un problème facile. On utilise les formes linéaires $A^n$ : $A$ s'annulant sur $C$. On dit qu'elles forment un

espace vectoriel $C^{\perp}$ qu'on a appelé, au chapitre 10 , dual de l'espace vectoriel $C$ ; $C^{\perp}$ est de dimension $n-k$. On a vu aussi que les éléments de $A^n$ annulés par les formes linéaires de $C^{\perp}$ ; par conséquent, $C$ est le noyau d'une application linéaire $\eta : A^n ß A^{n-k}$ ayant pour composantes les élements d'une base d'une base de $C^{\perp}$. La matrice $H$ d'une telle application est appelée matrice de contrôle ; elle est nulle pour tousles vecteurs du code et on a $HG = 0$.
Pour faire parvenir un message $x$, on envoie $c = \gamma(x)$ ; si$y$ est le message reçu,l'erreur est la suite $e = y - c$(on a aussi $e = y + c$ dans $A^n$) et on a $\eta(e) = \eta(y)$.
C'est à partir de $\eta(e)$ qu'il faut retrouver $e$ ; on peut alors trouver $c = y + e$, puis le message initial $x = \gamma^{-1}(c)$. Si $\eta(y) = 0$, on a $y \in C$, on pose $c = y$ et on retrouve $x$.

**Calcul matriciel**

Pour utiliser un code linéaire, le calcul matriciel s'impose. Nous adoptons pour cette section la notation suivante : si on a une suite de suite de bits $b = (b_1, \ldots, b_m)$, on note avec un prime la matrice colonne associée : $b^{'} = t(b_1 \ldots b_m)$ dont les coefficients sont les $b_i$. Pour envoyer le message $x = (x_1, \ldots, x_k)$ de $A^k$, on transmet le mot du code $c = \gamma(x)$ tel que $c^{'} = Gx^{'}$.
Notons que que l'usage est d'écrire , en théorie des codes, les vecteurs en ligne, ce qui conduit à transposer toutes les égalités matricielles qui vont suivre et oblige à une petite gymnastique que je ne vous impose pas.

**Code de Hamming(7,4,3)**

C'est en 1948, dans son grand article, que Shannon présente le code correcteur de Hamming. On peut s'en servir quand on suppose que la transmission peut créer au plus une erreur. Dans ce code, un message est une suite de 4 bits $x = (x_1, x_2, x_3, x_4) \in A^4$ qu'on code en $c = \gamma(x) = (u, v, x_1, w, x_2, x_3, x_4) \in A^7$, avec :
$u = x_1 + x_2 + x_4$,
$v = x_1 + x_3 + x_4$,
$w = x_2 + x_3 + x_4$.

La matrice de contrôle $H$ est donnée par ces trois égalités ($w + x_2 + x_3 + x_4 = 0$ donne la première ligne, etc.) et la matrice génératrice $G$ a pour colonnes les images par $\gamma$ des vecteurs de la base canonique, vecteurs formant uhne base du code $C$ :

$$\begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Les seize mots de $C$ s'obtiennent par combinaison linéaire des vecteurs de cette base. Les voici. $(0,0,0,0,0,0,0)(1,1,1,0,0,0,0)(1,0,0,1,1,0,0)(0,1,0,1,0,1,0)$
$(1,1,0,1,0,0,1)(0,1,1,1,1,0,0)(1,0,1,1,0,1,0)(0,0,1,1,0,0,1)$
$(1,1,0,0,1,1,0)(0,1,0,0,1,0,1)(1,0,0,0,0,1,1)(0,0,1,0,1,1,0)$
$(1,0,1,0,1,0,1)(0,1,1,0,0,1,1)(0,0,0,1,1,1,1)(1,1,1,1,1,1,1)$

On peut vérifier que la distance de Hamming de ce code est 3 et que le code est parfait : $A^7$ a $2^7 = 128$ éléments qui répartissent dans 16 boules de rayon 1 ayant 8 éléments. Ce code permet donc de corriger une erreur.
Quand on reçoit la suite $y = (y_1, y_2, y_3, y_4, y_5, y_6, y_7)$ de sept bits, on calcule $Hy^{'}$. Si $Hy^{'} = 0$, le message a été transmis sans erreur et on pose $c = y$. Si $Hy^{'} \neq 0$, c'est qu'une erreur de transmission $e$ a lieu et il existe $c \in C$ tel que $d_H(y, c) = 1$ et $c = y + e$. Hamming explique que les colonnes de $H$ sont les écritures en binaire des nombres 1 à 7. Comme la suite $e$ ne comporte qu'un seul terme non nul, $He^{'} = Hy^{'}$ est la colonne de $H$ correspondant à la position de l'erreur et on trouve $e$.
C'est à partir de cette propriété que le code a été construit.
Par exemple , si on veut envoyer $x = (1, 0, 1, 1)$, on envoie le message codé $Gx^{'} = c^{'}$, avec $c = (0, 1, 1, 0, 0, 1, 1)$. Si on reçoit le message $y = (0, 1, 1, 0, 0, 0, 1)$ avec une erreur $e = (0, 0, 0, 0, 0, 1, 0)$, au rang 6, on a $Hy^{'} =$

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

, la sixième colonne de $H$, ce qui implique bien le rang 6. On peut considérer que c'est $x = (1, 0, 1, 1)$ qui a été envoyé.

### 4.1.2 Lien entre les codes linéaires et les suites à somme nulle pondérées

Dans cette section, nous développons le lien entre les problèmes à somme nulle entièrement pondérés et les problèmes sur les codes linéaires qui a déjà été mentionné dans l'introduction. Nous rappelons que pour les 2-groupes élémentaires, ce lien était déjà connu.Notons qu'en fait pour ces groupes, le problème à somme nulle pondérée coïncide avec le problème classique, et le lien est apparu dans ce context (Voir section 4 de [30]). De plus, nous rappelons que pour les 3-groupes élémentaires. le problème entièrement pondéré coïncide avec le problème pondéré

plus-moins, ce qui est un intérêt particulier.

Avant de discuter du lien avec la théorie du code, nous rappelons quelques faits de base liés aux problèmes à somme nulle entièrement pondérés sur les $p$-groupes élémentaires. Soit $p$ un nombre premier. Soit $G$ un groupe d'exposant $p$, et soit $A = \{1, \ldots, p-1\}$ l'ensemble des poids. Rappelons que $G$ peut être considéré d'une manière naturelle comme un espace vectoriel sur d'un corps avec $p$ éléments. Nous identifions également les éléments de $A$ avec les éléments non nuls de $\mathbb{F}_p$ d'une manière naturelle. De plus, nous rappelons qu'une séquence $S = g_1 \ldots g_n$ sur $G$ n'a pas de somme nulle pondérée par $A$ si et seulement si $(g_1, \ldots, g_n)$ est linéairement indépendante, en particulier.

$$D_A(C_p^r) = r + 1 \text{ et } s_{A,\leqslant r+1}(C_p^r) = r + 1.$$

Maintenant, nous rappelons brièvement quelques notions de la théori du code d'une manière adaptée à notre application. Comme nous l'avons dit plus haut, $C_p^n$ est d'une manière naturelle un espace vectoriel sur $\mathbb{F}_p$ le corps avec $p$ éléments. Nous fixons implicitement une base de $C_p^n$, et nous pouvons donc écrire ses éléments simplement comme $n$-tuples d'éléments de $\mathbb{F}_p$ :

$$C_p^n = \{(x_1, x_2, \ldots, x_n) : x_i \in \mathbb{F}_p, 1 \leqslant i \leqslant n\}.$$

Un code linéaire $p$-aire de longueur $n$ et de dimension $k$ est un sous-espace vectoriel $C \subset C_p^n$ de dimension $k$. Brièvement, nous disons que $C$ est un $[n, k]$ $p$-code. Les éléments du code $C$ sont appelés mots-codes. Le support d'un élément $x = (x_1, x_2, \ldots, x_n)$ de $C_p^n$ est le sous-ensemble de $\{1, \ldots, n\}$ correspondant aux indices des coordonnées non nulles $x_i$(C'est l'usage du mot "support" courant dans la théorie du code, dans le contexte des suites à somme nulle, le mot "support" a typiquement un sens différent).Le poids d'un élément $x \in C_p^n$, noté $d(x)$ est la cardinalité du support de $x$. La distance minimale d'un code $C$ notée $d(C)$, est égale à la distance minimale $d(x)$ avec le support de $x$. La distance minimale d'un code $C$, notée $d(C)$ est égale au minimum $d(x)$ avec $x$ un mot du code non nul de $C$, c'est-à-dire que la distance minimale du code $C$ est égale à la cardinalité du support de $x$. Si $C$ a une distance minimale, la distance minimale est égale à la cardinalité minimale du support d'un élément non nul de $C$. Si $C$ a une distance minimale $d$, on dit que $C$ est un code $[n, k, d]_p$.Étant donné que dans la mesure où, dans le présent document, nous ne considérons que les codes linéaires, nous choisissons la manière rapide, mais pas très intuitive, d'introduire la distance minimale dans les codes linéaires.

Une matrice de contrôle de parité d'un code $[n, k]_p$. C'est une matrice $H$ de dimension $(n-k) \times n$ (avec rang complet) sur $F_p$ telle que $c \in C$ si et seulement si $Hc = 0$(où nous considérons $c$ comme une colonne vecteur). Pour $H = [g_1| \cdots |g_n]$,

nous pouvons interpréter les colonnes $g_i$ comme des éléments de $C_p^{n-k}$ , où encore une fois, une base est fixée, et de cette manière, on peut attribuer à un $p$-code $[n, k]$ une suite $= g_1 \dots g_n$ de longueur $n$ sur $C_p^{n-k}$ . Maintenant, $c = (c_1, \dots c_n) \in C$ signifie que $\sum_{i=1}^{n} c_i g_i = 0$. Si $I$ noté le support de $c$, alors on a $\sum_{i \in I} c_i g_i = 0$ pour $c_i \neq 0$. En d'autres termes, $\sum_{i \in I} c_i g_i = 0$ est une somme nulle pondérée $A$ de $S$ (éventuellement la somme vide). Sa longueur est exactement la cardinalité du support de $c$ c'est-à-dire $d(c)$. Inversement, si $\sum_{i \in I} c'_i g_i = 0$ est une somme nulle pondérée $A$ (éventuellement vide) de $S$, alors $c' = (c'_1, \dots, c'_n)$, où nous fixons $c'_i = 0$ pour $i \notin J$, est un élément de $C$ avec un poids $|J|$, la longueur du sous-somme. Bien sûr, $0 \in C$ correspond au sous-somme zéro vide pondéré par $A$. Ainsi, nous avons donc une correspondance directe entre les mots de code non nuls et les sous-sommes nulles pondérées $A$. Nous résumons ces résultats dans les lemmes ci-dessous (rappelons que $A = \{1, \dots, p-1\}$).

**Lemme 4.1.1**
La distance minimale d'un code linéaire $p$-aire $C$ est égale à la longueur minimale d'une somme nulle pondérée $A$ des colonnes d'une matrice de contrôle de parité de $C$.

**Démonstration :**
La discussion qui précède le confirme. ■

**Lemme 4.1.2**
Soit $S = g_1 \dots g_n$ une suite sur $C_p^r$ (avec une base fixée) telle que l'ensemble de tous les $g_i$ est un ensemble générateur de $C_p^r$. De plus, laissons $H = [g_1 | \dots | g_n]$ représenter la matrice $r \times n$ sur le champ $\mathbb{F}_p$(nous identifions les $g'_i s$ avec leurs vecteurs de coordonnées, sous forme de colonnes). Le code $C_S$ avec la matrice de contrôle de parité $H$ est alors un code $[n, n-r]_p$. Et, chaque code $[n, n-r]_p$ peut être obtenu de cette manière.

**Démonstration :**
Puisque l'ensemble des $g'_i s$ est un ensemble générateur de $C_p^r$, la matrice $H$ a un rang complet c'est-à-dire un rang $r$. Par conséquent, $C_S$ est un sous-espace de $(n-r)$-dimension de $C_p^n$. Cela donne la première affirmation. La deuxième affirmation s'ensuit, puisque pour chaque code $[n, n-r]_p$, il existe une matrice de contrôle de parité $r \times n$, qui a un rang complet. ■

**Lemme 4.1.3**
Soit $d, r \in \mathbb{N}$ et $p$ premier. Alors $s_{A,\leqslant d}(C_p^r) - 1$ est égal au maximun $n$ tel qu'il existe un code $[n, n-r]_p$ de distance minimale au moins $d+1$.

**Démonstration :**
Par définition $s_{A,\leqslant d}(C_p^r)$, il existe une suite $S$ sur $C_p^r$ de longueur $s_{A,\leqslant d}(C_p^r) - 1$ qui n'a pas de somme nulle pondérée par $A$ d'une longueur maximale de $d$. En outre les éléments de $S$ engendrent $C_p^r$. [30, Voir Lemme 3.8] Ainsi,$C_S$ est un code $[n, n-r]_p$, et il ne peut pas avoir un mot de code non nul de poids au plus d c'est-à-dire que sa distance minimale est au moins $d+1$ avec $d^{'} > d$, nous obtenons une suite $S_C$ Inversement, étant donné un code $[n, n-r, d']$ sur $C_p^r$ de longueur $n$ dont la somme nulle la plus courte pondérée par $A$ a une longueur $d' > d$. Ainsi, nous obtenons une suite $S_C$ sur $C_p^r$ de longueur $n$ dont la distance minimale est $d' > d$. Ainsi,$s_{A,\leqslant d}(C_p^r) > n$ , ce qui complète l'argument. ■

Nous terminons cette section générale sur le lien entre les codes linéaires et les problèmes de suites nulles pondérées $A$ en soulignant que l'existence de $m$ sous-suites nulles pondérées disjointes d'une suite $S$ correspond précisément à l'existence de $m$ mots du code non nuls dans $C_S$ dont les supports sont disjoints par paire. Cela rejoint une notion considérée dans la théorie du code, en particulier dans le cas où $m = 2$ du code. Nous rappelons que Cohen et Lempel [30, Voir section 4]ont appelé un code linéaire pour lequel deux mots du code non nuls n'ont pas de support disjoint, un code d'intersection. Nous nous référons à [30, Voir section 4]pour une discussion plus détaillée des codes intersectés (binaires) dans le contexte actuel.

## 4.2 Applications au problème de caractérisation

Il est évident que des groupes isomorphes $G$ et $G'$ produisent des monoïdes isomorphes de suites à somme nulle $\mathcal{B}(G)$ et $\mathcal{B}(G')$, et par conséquent, les systèmes d'ensembles de longueurs sont égaux $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$. La même chose est vraie si l'on considère des suites à somme nulle pondérées avec plus-moins (ou en fait, des suites à somme nulle pondérées pour tout choix de poids). Une question naturelle à poser est dans quelle mesure ces implications peuvent être inversées. Pour la première implication, cela s'appelle le Problème de l'isomorphisme, c'est-à-dire le problème de déterminer si l'isomorphie des monoïdes de suites à somme nulle (pondérées) implique l'isomorphie des groupes sous-jacents. Ce problème est complètement résolu pour les groupes abéliens finis sans poids et avec des poids plus-moins. De plus, la question analogue pour les groupes non commutatifs est également résolue.

En ce qui concerne la question impliquant les longueurs, cela s'appelle le Problème de caractérisation. Sous sa forme classique, il peut être énoncé en demandant si, pour $G$ et $G'$ des groupes abéliens finis tels que $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$, il en découle que $G$ et $G'$ sont isomorphes. L'histoire de ce problème remonte à plus de

cinquante ans et est initialement apparue dans le contexte de la caractérisation arithmétique du groupe des classes d'un anneau d'entiers algébriques, d'où son nom. Nous mentionnons que la condition selon laquelle le groupe est fini est cruciale. Tous les groupes abéliens infinis produisent le même système d'ensembles de longueurs, qui diffère de celui de tout groupe fini. Cela est connu sous le nom de Théorème de Kainrath.

Il est bien connu et facile de voir que $C_1$ et $C_2$ donnent tous deux lieu à des monoïdes semi-factoriels de suites à somme nulle ; en effet, les monoïdes sont même libres. À part cet exemple simple, il existe une autre paire de groupes non isomorphes connue qui produit le même système d'ensembles de longueurs pour leurs monoïdes de suites à somme nulle, à savoir $C_3$ et $C_2^2$. Il est donc courant d'imposer la condition supplémentaire que la constante de Davenport du groupe soit au moins 4. La conjecture actuelle est que ce sont les seuls cas où cela se produit et que, pour chaque groupe abélien fini $G$ qui n'est pas isomorphe à l'un de ces groupes, une condition qui assure cela est de supposer que $\mathsf{D}(\mathcal{B}(G)) \geqslant 4$. Il est en effet vrai que $\mathcal{L}(\mathcal{B}(G)) = \mathcal{L}(\mathcal{B}(G'))$ implique que $G$ et $G'$ sont isomorphes. Nous renvoyons à [38] et [42] pour un aperçu des résultats plus anciens sur le sujet et à [20] pour des contributions plus récentes. Une première recherche sur le problème de caractérisation pour les problèmes de somme nulle pondérés $\pm$, et plus largement sur le problème de décrire le système des ensembles de longueurs pour les problèmes de somme nulle pondérés plus-moins a été entreprise dans [22].

Comme dans le cas sans poids, $C_1$ et $C_2$ donnent tous deux lieu à des monoïdes demi-factoriels de séquences à somme nulle, en effet même des monoïdes libres. Pour d'autres groupes de petit ordre, les auteurs ont prouvé le résultat suivant.

**Théorème 4.2.1**
$\mathcal{L}(\mathcal{B}_{\pm}(C_2^2)) = \mathcal{L}(\mathcal{B}_{\pm}(C_3)) = \mathcal{L}(\mathcal{B}_{\pm}(C_4)) = \{y + 2k + [0, k] : y, k \in \mathbb{N}_0\}$. Réciproquement, si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \{y + 2k + [0, k] : y, k \in \mathbb{N}_0\}$ pour un groupe abélien fini $G$, alors $G$ est isomorphe à l'un des trois groupes $C_2^2$, $C_3$, $C_4$.

Notez que les ensembles $y + 2k + [0, k]$ sont simplement les ensembles $\{m, m + 1, m + 2, \ldots, n\}$ avec $\frac{n}{m} \leqslant \frac{3}{2}$. De plus, les auteurs ont résolu le problème de caractérisation pour les groupes cycliques d'ordre impair [22].

Dans la section actuelle, nous essayons de progresser davantage sur ce problème en utilisant nos résultats sur $\Delta^*$.

Dans la plupart des cas, il est assez difficile de décrire complètement $\mathcal{L}(H)$. Pour résoudre le problème de caractérisation, on procède souvent de la manière suivante. On établit que si $\mathcal{L}(H) = \mathcal{L}(H')$, alors certains invariants arithmétiques de $H$ et $H'$ sont égaux. En utilisant des résultats sur ces invariants arithmétiques, on obtient des informations sur $H$ et $H'$. Pour les invariants qui sont définis, ou du moins peuvent être définis, purement via le système de ensembles de longueurs, tels que $\rho$, $\rho_k$, $\lambda_k$, $U_k$, $\Delta$ et $\Delta_1$, il est clair que l'égalité de $\mathcal{L}(H)$ et $\mathcal{L}(H')$ implique l'égalité

des invariants respectifs pour $H$ et $H'$. Puisque pour $H = \mathcal{B}_{\pm}(G)$ et $H' = \mathcal{B}_{\pm}(G')$, nous savons que $\rho_2(H) = \mathsf{D}(H)$ et $H' = \mathcal{B}_{\pm}(G')$, il en résulte que l'égalité de $\mathcal{L}(H)$ et $\mathcal{L}(H')$ implique aussi que $\mathsf{D}(H) = \mathsf{D}(H')$. De même, le fait que $\Delta^*(H) \subseteq \Delta_1^*(H) \subseteq \{d_0 \mid d : d \in \Delta^*(H)\}$ implique que, dans le cas où $\mathcal{L}(H) = \mathcal{L}(H')$, les ensembles $\Delta^*(H)$ et $\Delta_1^*(H)$ sont étroitement liés.$\max \Delta^*(H) = \max \Delta_1^*(H')$ et plus précisément, si $M$ désigne ce maximum, alors les ensembles $\Delta^*(H) \cap \mathbb{N}_{>M/2}$ et $\Delta_1^*(H') \cap \mathbb{N}_{>M/2}$ sont égaux.

Ensuite, on utilise des résultats qui donnent les valeurs de ces invariants arithmétiques en termes d'invariants algébriques des groupes, afin d'établir des conditions sur les groupes, et idéalement leur isomorphisme.

**Théorème 4.2.2**
Soit $G$ un groupe abélien fini d'ordre impair et soit $G'$ un groupe abélien fini. Nous posons $H = \mathcal{B}_{\pm}(G)$ et $H' = \mathcal{B}_{\pm}(G')$. Si $\mathsf{L}(H) = \mathsf{L}(H')$, alors $\exp(G) = \exp(G')$ et $\mathsf{D}(G) = \mathsf{D}(G')$.

**Démonstration :**
Nous savons que $\rho(H) = \rho(H')$ et $\Delta(H) = \Delta(H')$. Par le théorème 3.4.1, nous savons que $\max \Delta_1(H) = \exp(G) - 2$.

Par le théorème 3.4.2, nous savons que $\Delta_1(H)$ ne contient que des éléments impairs. Ainsi, $\Delta_1(H')$ ne contient également que des éléments impairs, et $G'$ est donc un groupe d'ordre impair. Ainsi,$\max \Delta_1(H') = \exp(G_0) - 2$, et donc $\exp(G) = \exp(G')$.

Pour obtenir le résultat concernant les constantes de Davenport, il suffit de rappeler que $\rho(H) = \frac{\mathsf{D}(H)}{2}$ et $\rho(H') = \frac{D(H')}{2}$, et puisque $G$ et $G'$ sont impairs, nous avons $\mathsf{D}(H) = \mathsf{D}(G)$ et $\mathsf{D}(H') = \mathsf{D}(G')$. ■
Nous insistons sur le fait que les constantes de Davenport classiques de $G$ et $G'$ sont effectivement égales, car pour les groupes d'ordre impair ou, de manière équivalente, d'exposant impair, elles sont respectivement égales à $\mathsf{D}(\mathcal{B}_{\pm}(G))$ et $\mathsf{D}(\mathcal{B}_{\pm}(G'))$.

Ce résultat permet de prouver que les groupes élémentaires $p$-groupes pour $p$ impair sont caractérisés. Comme le même raisonnement permet de caractériser certains autres $p$-groupes et des groupes d'exposant impair, nous commençons par une proposition technique.

**Proposition 4.2.1**
Soit $G$ un groupe abélien fini d'exposant $n$ impair et de constante de Davenport $D$ tel qu'il n'existe aucun groupe non isomorphe à $G$ ayant également $n$ et la constante de Davenport $D$. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Par le théorème 4.2.2, nous savons que les exposants de $G$ et $G'$ sont égaux et

que les constantes de Davenport de $G$ et $G'$ sont égales. L'affirmation est donc évidemment vraie par l'hypothèse sur $G$. ■
Nous notons d'abord que ce résultat fournit une preuve alternative de la caractérisation des groupes cycliques d'ordre impair.

**Corollaire 4.2.1**
Soit $G$ un groupe cyclique d'ordre impair. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Un groupe cyclique satisfait la condition de la proposition 4.2.1, car les groupes cycliques sont les seuls groupes pour lesquels l'exposant est égal à la constante de Davenport. ■

**Corollaire 4.2.2**
Soit $G$ un groupe élémentaire $p$-groupe pour $p$ impair. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Pour un groupe $G$ avec $\exp(G)$ premier, la constante de Davenport est donnée par $1 + \mathsf{r}(G)(\exp(G) - 1)$ et donc les $p$-groupes élémentaires satisfont la condition de la proposition 4.2.1. ■

**Corollaire 4.2.3**
Soit $G = C_p \oplus C_n$ où $n$ est impair et $p$ est le plus petit diviseur premier de $n$. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Il suffit de montrer que les groupes satisfont la condition de la proposition 4.2.1. Tout d'abord, rappelons que la constante de Davenport de $G$ est $n + p - 1$, car le groupe est de rang deux. Maintenant, si $G'$ est un groupe avec exposant $n$, alors soit $G'$ est cyclique, soit de la forme $H \oplus C_n$ où $1 \neq \exp(H) \mid n$. Dans le premier cas, la constante de Davenport de $G'$ est $n$, et donc elle n'est pas égale à celle de $G$. Dans le second cas, la constante de Davenport est au moins $n+\mathsf{D}(H)-1 \geqslant n+\exp(H)-1$ et donc strictement supérieure à $n + p - 1$, sauf si $\exp(H) = p$ et $\mathsf{D}(H) = \exp(H)$. Ainsi, nous obtenons que $H$ est cyclique d'ordre $p$, ce qui implique la conclusion. ■

**Lemme 4.2.1**
Soit $K$ un $p$-groupe avec constante de Davenport $D$.

1. Si $\mathsf{D} < p^2$ et $K'$ est un autre $p$-groupe avec constante de Davenport $\mathsf{D}$, alors $K$ et $K'$ sont isomorphes.
2. Si $\mathsf{D} \geqslant p^2$, alors il existe un $p$-groupe $K'$ avec constante de Davenport $\mathsf{D}$ tel que $K$ et $K'$ ne sont pas isomorphes.

**Démonstration :**
Pour voir le premier point, il suffit de noter que $\mathsf{D} < p^2$ implique que $\exp(K) < p^2$ et $\exp(K') < p^2$. Ainsi, les deux ont pour exposant $p$ et l'affirmation s'ensuit directement.

Pour le second point, nous distinguons deux cas. Supposons que l'exposant de $K$ est $p$, disons $K \equiv C_p^r$. D'après l'hypothèse sur la constante de Davenport, on obtient que $r \geqslant p+1$. Pourtant, $K' = C_p^{r-p-1} \oplus C_{p^2}$ a la même constante de Davenport.

Maintenant, supposons que l'exposant de $K$ n'est pas premier, disons qu'il est $p^k$ avec $k > 1$. Soit $K_0$ un groupe tel que $K \equiv K_0 \oplus C_{p^k}$. Ensuite, posons $K' = K_0 \oplus C^p_{(p^k-1)/(p-1)}$, qui a la même constante de Davenport. ■

**Corollaire 4.2.4**
Soit $G$ un $p$-groupe pour $p$ impair et supposons que $\mathsf{D}(G) < \exp(G) + p^2 - 1$. Si $\mathcal{L}(\mathcal{B}_{\pm}(G)) = \mathcal{L}(\mathcal{B}_{\pm}(G'))$, alors $G \cong G'$.

**Démonstration :**
Nous notons que le groupe $G$ satisfait la condition de la proposition 4.2.1. En effet, soit $G = K \oplus C_{\exp(G)}$. Alors $\mathsf{D}(G) = \exp(G) + \mathsf{D}(K) - 1$. Le résultat découle maintenant du lemme 3.4.8 ■

# Publications

— Boukheche, S., Merito, K., Ordaz, O., and Schmid, W. A. (2022). Monoids of sequences over finite abelian groups defined via zero-sums with respect to a given set of weights and applications to factorizations of norms of algebraic integers. Communications in Algebra, 50(10), 4195-4217.
— Chouly, F., Loubani, J., Lozinski, A., Méjri, B., Merito, K., Passos, S., and Pineda, A. (2020). Computing bi-tangents for transmission belts.

# Bibliographie


[1] Sukumar Das Adhikari, David J Grynkiewicz, and Zhi-Wei Sun. On weighted zero-sum sequences. *Advances in Applied Mathematics*, 48(3) :506–527, 2012. 15, 34

[2] Sukumar Das Adhikari and Purusottam Rath. Davenport constant with weights and some related questions. *Integers*, 6 :A30, 2006. 15

[3] DD Anderson and David F Anderson. Elasticity of factorizations in integral domains. *Journal of pure and applied algebra*, 80(3) :217–235, 1992. 15, 24

[4] Nicholas R Baeth and Daniel Smertnig. Factorization theory : from commutative to noncommutative settings. *Journal of Algebra*, 441 :475–551, 2015. 11

[5] Grégory Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018. 35

[6] Safia Boukheche, Kamil Merito, Oscar Ordaz, and Wolfgang A Schmid. Monoids of sequences over finite abelian groups defined via zero-sums with respect to a given set of weights and applications to factorizations of norms of algebraic integers. *Communications in Algebra*, 50(10) :4195–4217, 2022. 46

[7] ST Chapman, WA Schmid, and WW Smith. On minimal distances in krull monoids with infinite class group. *Bulletin of the London Mathematical Society*, 40(4) :613–618, 2008. 46

[8] Kálmán Cziszter, Mátyás Domokos, and Alfred Geroldinger. The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics. *Multiplicative Ideal Theory and Factorization Theory : Commutative and Non-commutative Perspectives*, pages 43–95, 2016. 17, 21

[9] Jean-Pierre Escofier. *Toute l'algèbre de la Licence-4e éd. : Cours et exercices corrigés*. Dunod, 2016. 55, 65

[10] Yushuang Fan, Alfred Geroldinger, Florian Kainrath, and Salvatore Tringali. Arithmetic of commutative semigroups with a focus on semigroups of ideals and modules. *Journal of Algebra and its Applications*, 16(12) :1750234, 2017. 15, 20

[11] Yushuang Fan and Qinghai Zhong. Products of k atoms in krull monoids. *Monatshefte für Mathematik*, 181 :779–795, 2016. 15, 35

[12] Michael Freeze and Alfred Geroldinger. Unions of sets of lengths. *Functiones et Approximatio Commentarii Mathematici*, 39(1) :149–162, 2008. 15, 25

[13] Weidong Gao and Alfred Geroldinger. Zero-sum problems in finite abelian groups : a survey. *Expositiones Mathematicae*, 24(4) :337–369, 2006. 14, 32

[14] Alfred Geroldinger. Additive group theory and non-unique factorizations. *Combinatorial number theory and additive group theory*, pages 1–86, 2009. 11, 12, 14, 22, 29, 32

[15] Alfred Geroldinger. Sets of lengths. *The American Mathematical Monthly*, 123(10) :960–988, 2016. 11, 14

[16] Alfred Geroldinger, David J Grynkiewicz, Jun Seok Oh, and Qinghai Zhong. On product-one sequences over dihedral groups. *Journal of Algebra and Its Applications*, 21(04) :2250064, 2022. 15

[17] Alfred Geroldinger, David J Grynkiewicz, and Pingzhi Yuan. On products of k atoms ii. *arXiv preprint arXiv :1503.06164*, 2015. 15, 35

[18] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations : Algebraic, combinatorial and analytic theory*. Chapman and Hall/CRC, 2006. 8, 11, 14, 16, 17, 20, 24

[19] Alfred Geroldinger, Franz Halter-Koch, and Qinghai Zhong. On monoids of weighted zero-sum sequences and applications to norm monoids in galois number fields and binary quadratic forms. *Acta Mathematica Hungarica*, 168(1) :144–185, 2022. 42, 43, 44, 50

[20] Alfred Geroldinger and Wolfgang Schmid. A characterization of class groups via sets of lengths. *Journal of the Korean Mathematical Society*, 56(4) :869–915, 2019. 61, 71

[21] Alfred Geroldinger, Wolfgang A Schmid, and Qinghai Zhong. Systems of sets of lengths : transfer krull monoids versus weakly krull monoids. *Rings, polynomials, and modules*, pages 191–235, 2017. 11

[22] Alfred Geroldinger and Pingzhi Yuan. The set of distances in krull monoids. *Bulletin of the London Mathematical Society*, 44(6) :1203–1208, 2012. 11, 61, 71

[23] Alfred Geroldinger and Qinghai Zhong. Factorization theory in commutative monoids. In *Semigroup Forum*, volume 100, pages 22–51. Springer, 2020. 11, 12, 20

[24] David J Grynkiewicz. *Structural additive theory*, volume 30. Springer, 2013. 9, 14, 15

[25] Franz Halter-Koch. Arithmetical interpretation of weighted davenport constants. *Archiv der Mathematik*, 103 :125–131, 2014. 15, 38

[26] Franz Halter-Koch. *An Invitation to Algebraic Numbers and Algebraic Functions*. CRC Press, 2020. 38

[27] Heiko Harborth. Ein extremalproblem für gitterpunkte. 1973. 15

[28] Florian Kainrath. Elasticity of finitely generated domains. *Houston J. Math*, 31(1) :43–64, 2005. 15

[29] Serge Lang. *Algèbre*. Dunod, 2020. 3

[30] Luz E Marchan, Oscar Ordaz, Irene Santos, and Wolfgang A Schmid. Multi-wise and constrained fully weighted davenport constants and interactions with coding theory. *Journal of Combinatorial Theory, Series A*, 135 :237–267, 2015. 57, 59, 60, 67, 70

[31] Luz E Marchan, Oscar Ordaz, and Wolfgang A Schmid. Remarks on the plus–minus weighted davenport constant. *International Journal of Number Theory*, 10(05) :1219–1239, 2014. 34

[32] James S Milne. Algebraic number theory (v3. 08), 2020. 38

[33] Władysław Narkiewicz and Władysław Narkiewicz. Algebraic numbers and integers. *Elementary and Analytic Theory of Algebraic Numbers*, pages 43–83, 2004. 15, 38

[34] Jun Seok Oh. On the algebraic and arithmetic structure of the monoid of product-one sequences. 2020. 15, 23

[35] Maciej Radziejewski and Wolfgang A Schmid. Weakly half-factorial sets in finite abelian groups. 2007. 48

[36] Svetoslav Savchev and Fang Chen. Long zero-free sequences in finite cyclic groups. *Discrete mathematics*, 307(22) :2671–2679, 2007. 32

[37] WA Schmid. Some recent results and open problems on sets of lengths of krull monoids with finite class group. In *Multiplicative Ideal Theory and Factorization Theory : Commutative and Non-commutative Perspectives*, pages 323–352. Springer, 2016. 12, 46

[38] Wolfgang A Schmid. The inverse problem associated to the davenport constant for $c_2 \oplus c_2 \oplus c_{2n}$, and applications to the arithmetical characterization of class groups. *the electronic journal of combinatorics*, 18(1) :P33, 2011. 61, 71

[39] Terence Tao and Van H Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006. 14

[40] Pingzhi Yuan. On the index of minimal zero-sum sequences over finite cyclic groups. *Journal of Combinatorial Theory, Series A*, 114(8) :1545–1551, 2007. 32

[41] Xiangneng Zeng and Pingzhi Yuan. Weighted davenport's constant and the weighted egz theorem. *Discrete mathematics*, 311(17) :1940–1947, 2011. 10, 15

[42] Qinghai Zhong. A characterization of finite abelian groups via sets of lengths in transfer krull monoids. *Communications in Algebra*, 46(9) :4021–4041, 2018. 61, 71