N° d'ordre : 380/2025-C/MT

Cotutelle Internationale de Thèse

Université des Sciences et de la Technologie Houari Boumediene

Ecole Doctorale Recherche Opérationnelle et Mathématiques Discrètes

Université Paris 8

Ecole Doctorale Cognition, Langage, Interaction

Thèse de Doctorat

Présentée pour l'obtention du grade de docteur

en : Mathématiques

Spécialité : Recherche Opérationnelle, Mathématiques Discrètes

Par : **BOUKHECHE Safia**

Sujet

Contributions aux problèmes des suites à somme nulle classiques et pondérées

Soutenue le 16/10/2025, devant le jury composé de :

M. Mohand Ouamar HERNANE	Professeur à l'USTHB / FMT	Président
M. Hacène BELBACHIR	Professeur à l'USTHB / FMT	Directeur de thèse
M. Wolfgang SCHMID	Professeur à Paris 8	Co-Directeur de thèse
M. Pedro A. GARCÍA SÁNCHEZ	Professeur à l'Université de Grenade	Examinateur
Mme. Gautami BHOWMIK	HDR à l'Université de Lille	Examinatrice
M. Abdelkader BOUYAKOUB	Professeur à l'ENSM	Examinateur
M. Abdellah MOKRANE	Professeur à Paris 8	Examinateur
M. Boualem BENSEBA	Professeur à l'USTHB	Examinateur

Table des matières

Chapitre

1 Introduction

Les problèmes des suites à somme nulle font partie de la combinatoire additive, également appelée combinatoire arithmétique, qui est une branche active des mathématiques, à la croisée de la théorie des nombres et de la combinatoire. Au cœur de la combinatoire additive se trouvent l'étude de la structure additive des ensembles et de suites, souvent formulés sur des groupes abéliens. L'un des problèmes centraux de cette théorie consiste à déterminer le plus petit entier k, tel que toute suite de k éléments du groupe contienne une sous-suite à somme nulle, c'est-à-dire que la somme de tous les éléments de la sous-suite est égale à zéro. Cet entier est connu sous le nom de la constante de Davenport. Ce dernier a suscité de nombreuses recherches scientifiques où des résultats significatifs ont été obtenus.

Dans le cadre de cette thèse, nous plongeons au cœur des problèmes liés aux suites à somme nulle, qu'elles soient de nature classique ou pondérée. Les suites classiques sont celles où chaque élément contribue de manière égale à la somme totale, tandis que les suites pondérées introduisent des coefficients spécifiques pour chaque élément, ce qui permet d'étudier des situations plus complexes et variées. Notre champ d'étude est spécifiquement centré sur l'analyse des suites qui présentent la remarquable propriété d'avoir une somme totale égale à zéro (suites à somme nulle), qui évoluent au sein des groupes abéliens, notamment ceux qui sont de nature finie.

Le choix de nous concentrer sur les groupes abéliens finis repose sur deux motivations. La première est liée aux applications arithmétiques, où ces groupes jouent un rôle central dans la résolution de ces problèmes. La seconde est la longue tradition de recherche dans ce domaine, qui nous permet de nous appuyer sur des résultats antérieurs, tout en visant à apporter de nouvelles contributions originales.

Cette thématique jouit désormais d'une tradition solidement établie dans le domaine mathématique, voir, par exemple [16], [21, Chapitres 5 et 6], [28, Partie 2], [50, Chapitre 9].

Nous rappelons qu'une collection d'éléments $g_1 \dots g_l$ d'un groupe abélien fini $(G, +, 0_G)$ est dite de somme nulle si la somme de tous ces éléments est l'élément neutre du groupe, c'est-à-dire si $g_1 + \cdots + g_l = 0_G$. Si tous les éléments g_i sont distincts, on parle alors d'un ensemble à somme nulle. Et si on admet des répétitions des éléments, on parle alors d'une suite à somme nulle. Cependant, on ne tient généralement pas compte de l'ordre

des éléments de la suite et, formellement, les suites dans notre contexte sont des éléments du monoïde abélien libre sur G. Nous renvoyons aux préliminaires, voir le Chapitre 3 pour plus de détails. En plus de l'étude des constantes à somme nulle telles que la constante d'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 les groupes abéliens, principalement sur les groupes abéliens finis. L'une des principales raisons est qu'ils représentent une classe importante de monoïdes auxiliaires dans la théorie de la factorisation, voir, par exemple [17, 18, 21]. Tout monoïde de Krull, en particulier le monoïde multiplicatif de tout domaine de Dedekind admet un homomorphisme de transfert vers un monoïde de suites à somme nulle. Une autre raison est qu'il s'agit de monoïdes faciles à définir, mais qui présentent des phénomènes riches en ce qui concerne leur arithmétique. Ces dernières années, l'étude des « problèmes à somme nulle » a été élargie par l'introduction de « poids ». Intuitivement, cela signifie qu'au lieu de considérer simplement la somme des éléments, on permet d'attribuer des poids aux éléments. Par exemple, en autorisant les poids de l'ensemble $\{1, 3\}$, on considère des sommes de la forme suivante $\sum_{i=1}^{l} w_i g_i$ où $w_i \in \{1, 3\}$, c'est-à-dire que l'on peut attribuer un « poids » différent à certains éléments en choisissant que w_i soit égal à 3 plutôt qu'à 1.

Bien entendu, dans un groupe abélien fini, le terme « poids » doit être compris au sens figuré. Mais nous nous rappelons qu'un premier exemple de problème à somme nulle est né de la question de l'existence de points dans un réseau entier (un réseau dont les éléments sont des entiers relatifs) dont le point de barycentre est à nouveau un point du réseau [32], et dans ce contexte, l'idée d'attribuer des poids différents aux points aurait un sens plus littéral du terme.

Il se trouve 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 « multiplication par w » comme un endomorphisme du groupe abélien G. L'idée d'autoriser tout endomorphisme de G comme « poids », plutôt que seulement ceux induits par la multiplication par un entier, devient alors très naturelle. Des généralisations de la notion de « poids » allant au-delà sont possibles et apparaissent dans la littérature, mais nous ne les étudierons pas dans le présent document, voir [54] et [28, Chapitre 16].

Cette généralisation, qui introduit des poids, a reçu un intérêt considérable, voir, par exemple, [1, 2]. Ces recherches se sont toutefois concentrées sur l'étude des constantes à somme nulle. Dans cette thèse, nous commençons une étude des monoïdes de suites sur des groupes abéliens finis qui admettent des sommes nulles avec des poids. Pour une définition précise, voir le chapitre 3.

Après avoir collecté les principales définitions, nous étudions les propriétés algébriques de base de ces monoïdes. Ensuite, nous étudions en détail certains invariants arithmétiques classiques pour ces monoïdes, à savoir les élasticités, voir, par exemple [3, 14, 19, 33] et les unions d'ensembles de longueurs, voir, par exemple [13, 15].

Il s'avère que ces recherches présentent des similitudes avec celles de l'arithmétique des suites de produit un (produit égal à un) sur les groupes non abéliens, voir [20, 42]. 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 le Chapitre 8, en En démontrant que ces monoïdes apparaissent lors de l'étude des monoïdes des normes des entiers algébriques. Un lien étroitement lié apparaît déjà dans [30] et plus implicitement dans [41, Section 9.2]. Il est important de souligner que tous les détails et résultats de ces études sont disponibles dans l'article [8], qui constitue l'article principal de cette thèse et a été rédigé en collaboration avec Kamil Merito, Oscar Ordaz, Wolfgang A. Schmid et moi-même. En particulier, les chapitres 4 à 8 de cette thèse s'inspirent directement de cet article, chacun développant ou traduisant certains de ses résultats.

Enfin, nous concluons en présentant des résultats concernant le nombre de suites à somme nulle minimales dans un groupe abélien fini, en nous appuyant sur les résultats obtenus pour toutes les suites.

Motivation

Dans $\mathbb{Z}$ tout élément non nul admet "une décomposition unique" en nombres premiers. Soit K, un corps de nombres et soit $\mathcal{O}_K$, l'anneau d'entiers algébriques. Alors tout élément admet une décomposition en éléments irréductibles.

Cependant, il se peut que cette factorisation ne soit plus unique, ce qui suscite un intérêt pour comprendre l'origine de ce phénomène. Afin de l'expliquer, l'idée de groupe de classes d'idéaux a été introduite (et même, avant cela, la notion d'idéal). Ceci étaient des problèmes centraux de la théorie des nombres algébriques du 19e siècle. La réponse trouvée est que $\mathcal{O}_K$ factoriel (factorisation unique) équivaut à $\mathcal{O}_K$ principal (tout idéal est un idéal principal) ce qui revient à dire que $\mathrm{Cl}(\mathcal{O}_K)$, le groupe de classes est d'ordre 1.

En 1960, Carlitz a démontré que $\mathcal{O}_K$ est « demi-factoriel », ce qui est équivalent au $\#\,\mathrm{Cl}(\mathcal{O}_K) \leq 2$. Rappelons que « demi-factoriel » signifie que tout élément possède la propriété que chacune de ses factorisations en élément irréductible a le même nombre de facteurs.

Un autre phénomène arithmétique a donc été classifié par le groupe de classes. Ensuite, Narkiewicz s'est posé la question : comment pourrait-on caractériser les groupes de classes par des propriétés arithmétiques dans le cas général. Cette question a stimulé une multitude de travaux visant à comprendre l'arithmétique de $\mathcal{O}_K$ en fonction de $\mathrm{Cl}(K)$. Pour cela, de nombreuses constantes et quantités ont été introduites, telles que l'ensemble de longueurs, l'élasticité, le degré de chaînage, l'ensemble de distances, etc. En particulier,

les chercheurs ont remarqué que pour $\mathcal{O}_K$, beaucoup de ces constantes peuvent être étudiées plus efficacement en considérant le monoïde de suites à somme nulle sur le groupe de classes.

Il existe un homomorphisme de monoïde $\theta\colon \mathcal{O}_K^* \to \mathcal{B}(\mathrm{Cl}(\mathcal{O}_K))$ qui préserve certaines de ces constantes. On a $\rho(\mathcal{O}_K) = \rho(\mathcal{B}(\mathrm{Cl}(\mathcal{O}_K))$ et $\mathsf{c}(\mathcal{O}_K) = \mathsf{c}(\mathcal{B}(\mathrm{Cl}(\mathcal{O}_K))$.

La même approche fonctionne pour tout monoïde de Krull, en particulier pour n'importe quel anneau de Dedekind. Étant donné que n'importe quel groupe abélien peut être isomorphe à un groupe de classes d'un anneau de Dedekind, d'où on peut étudier le problème d'une manière abstraite comme suit.

On considère $\mathcal{B}(G)$ pour $(G, +)$ groupe abélien fini. Déterminer les propriétés de $\mathcal{B}(\mathrm{Cl}(\mathcal{O}_K)$ est, d'une certaine manière, équivalent à déterminer les constantes arithmétiques de $\mathcal{O}_K$. Nous étudions des problèmes de suites à somme nulle pour classifier les phénomènes arithmétiques observés dans $\mathcal{O}_K$ pour K, corps de nombres. Il est courant de considérer aussi des problèmes de suites à somme nulle avec des poids, principalement pour la constante de Davenport, Harborth, etc. Pour l'instant, on n'a pas étudié cette question avec des poids. Ceci est peut-être dû au fait qu'il n'y avait pas de motivations arithmétiques. Dans cette thèse, nous présentons une étude systématique de ce type de questions et nous donnons également une application arithmétique, voir le Chapitre 8.

Chapitre

2 Notations

— $\mathbb{N}$: l'ensemble des entiers strictement positifs.
— $\mathbb{N}_0$=$\mathbb{N} \cup \{0\}$: l'ensemble des entiers positifs.
— Pour a et b des nombres réels, on note par $[a, b] = \{x \in \mathbb{Z} \colon a \leq x \leq b\}$: l'intervalle des nombres entiers.
— Pour $c \in \mathbb{N}$:

$$\mathbb{N}_{\geq c} = \mathbb{N} \backslash [1, c-1] = c + \mathbb{N}_0.$$

— Pour $x \in \mathbb{R}$, on note :

$$\begin{aligned} \lfloor x \rfloor &: \text{ le plus grand entier inferieur ou égal à } x \\ \lceil x \rceil &: \text{ le plus petit entier superieur ou ou égal à } x. \end{aligned}$$

— $(G, +, 0)$: le groupe abélien fini d'élément neutre égal à 0.
— C_n : le groupe cyclique d'ordre n.
— $\mathsf{r}(G)$: le rang de groupe G.
— $\#G$ ou $|G|$: l'ordre de groupe G.
— $\exp(G)$: l'exposant de G.
— $G[d]$: la d-torsion de G.
— μ : la fonction de Möbius.
— $(e_1, \ldots, e_s)$: une base de G.
— $A + B$: l'ensemble somme de Minkowski des sous-ensembles A et B de G.
— H : un monoïde commutatif et simplifiable.
— $H^\times$: l'ensemble des éléments inversibles de H.
— $H_{\text{red}} = H/H^\times$: le monoïde réduit associé à H.
— $\mathcal{A}(H)$: l'ensemble des atomes de H, qui, dans le cas où H est un monoïde commutatif et simplifiable, coïncide avec l'ensemble des éléments irréductibles.
— $\mathcal{P}(H)$: l'ensemble des éléments premiers de H.
— $\mathcal{F}(P)$: le monoïde abélien libre sur P.
— $|S| = \ell$: la longueur de la suite S.
— $\sigma(S)$: la somme de la suite S.
— $\mathcal{B}(G)$: l'ensemble de toutes les suites à somme nulle.
— $\mathsf{Z}(H)$=$\mathcal{F}(\mathcal{A}(H_{\text{red}}))$: le monoïde des factorisations de H.

— $\mathsf{Z}_H(a) = \pi_H^{-1}(aH^\times)$, $a \in H$: l'ensemble des factorisations de a dans H.
— $|z|$: la longueur de la factorisation z.
— $\mathsf{L}_H(a)$: l'ensemble des longueurs de a dans H.
— $\mathcal{L}(H)$: le système des ensembles de longueurs de H.
— Ω : un ensemble de poids.
— $\pm$: l'ensemble des poids $\{+\,\mathrm{id}_G, -\,\mathrm{id}_G\}$.
— $\sigma_\Omega(S)$: l'ensemble de toutes les sommes Ω-pondérées de S.
— $\sigma_\pm(S)$: l'ensemle des sommes $\pm$-pondérées de S.
— $\mathcal{A}(G)$: l'ensemle des suites à somme nulle minimales.
— $\mathsf{D}(G)$: la constante de Davenport classique.
— $\mathcal{B}_\pm(G)$: l'ensemble des suites S tel que $0 \in \sigma_\pm(S)$.
— $\mathcal{A}(\mathcal{B}_\pm(G))$: l'ensemble des atomes de monoide $\mathcal{B}_\pm(G)$.
— $\mathsf{D}(\mathcal{B}_\pm(G))$: la constante arithmétique de Davenport $\pm$-pondérée.
— K : un corps de nombres galoisien.
— $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$: le groupe de Galois de K.
— $\mathcal{O}_K$: l'anneau d'entiers de K.
— $\mathcal{P}_K$: l'ensemble des idéaux premiers non nuls.
— $\mathcal{I}_K = \mathcal{F}(\mathcal{P}_K)$: le monoïde abélien libre des idéaux non nuls de $\mathcal{O}_K$.
— $\mathcal{H}_K$: le sous-monoïde des idéaux principaux non nuls.
— N : la norme absolue.
— $\mathbb{P} \subseteq \mathbb{N}$: l'ensemble des nombres premiers.
— Pour $p \in \mathbb{P}$, $P_p \in \mathcal{P}_K$: un idéal premier qui contient p.

Chapitre

3 Préliminaires

Dans ce chapitre, nous posons les bases nécessaires pour la compréhension approfondie des concepts qui seront explorés tout au long de notre étude. Nous commençons par rappeler les fondements de la théorie des groupes, une branche fondamentale des mathématiques. Cette théorie examine la structure et les propriétés des ensembles munis d'une opération binaire qui satisfait des propriétés spécifiques, telles que l'associativité et l'existence de l'élément neutre. Nous présentons également les concepts clés liés aux groupes, tels que le rang, l'ordre et l'exposant d'un groupe, en les illustrant par des exemples concrets pour faciliter la compréhension.

Nous poursuivons en introduisant la notion de monoïde, une structure algébrique moins contraignante que les groupes, mais néanmoins importante dans notre étude. Les monoïdes sont des ensembles munis d'une opération binaire associative et d'un élément neutre. À la différence des groupes, ils ne nécessitent pas d'inverses pour chaque élément. Cette généralisation nous permettra d'explorer plus en profondeur les suites à sommes nulles.

En parlant de suites à sommes nulles, nous abordons un aspect crucial de notre thèse. Nous discutons de la constante de Davenport, un concept clé dans la théorie des suites à sommes nulles. Cette constante est liée à la plus petite valeur k telle que toute suite de k éléments d'un groupe abélien contienne une sous-suite dont la somme des termes est nulle. Comprendre cette constante constitue une grande importance pour notre recherche, car elle représente l'un des problèmes centraux de la combinatoire additive.

Enfin, nous clôturons ce chapitre en explorant les notions de factorisation non unique. Ce concept joue une grande importance dans divers domaines mathématiques, en particulier en théorie des nombres et en algèbre. Il s'agit de la possibilité de décomposer un nombre ou un élément d'un anneau de différentes manières en facteurs premiers. Cette notion de non-unicité de la factorisation aura des implications intéressantes dans notre étude des suites à sommes nulles.

En résumé, ce chapitre constitue la première étape de notre exploration en fournissant les bases essentielles pour la suite de notre travail. Nous établirons ainsi une fondation solide pour aborder plus en détail les problèmes liés aux suites à sommes nulles et à la factorisation non unique dans les chapitres ultérieurs.

3.1 Théorie des groupes

Dans cette section, nous allons revoir les principes fondamentaux de la théorie des groupes, qui serviront de base à notre analyse par la suite. Il est important de noter que, tout au long de notre étude, nous adopterons la convention d'écrire tous les groupes abéliens sous forme additive et que nous nous intéressons à des groupes de cardinalité finie.

Définition 1. (Groupe abélien) Soient G un ensemble et $+$ une loi de composition interne sur G. On dit que $(G, +)$ est un groupe lorsque les conditions suivantes sont vérifiées :

- La loi $+$ est associative : $\forall (x, y, z) \in G^3, (x + y) + z = x + (y + z)$.
- La loi $+$ admet un élément neutre : $\exists 0_G \in G, \forall x \in G, x + 0_G = x$ et $0_G + x = x$.
- Tout élément de G admet un élément symétrique pour la loi $+$: $\forall x \in G, \exists (-x) \in G, x + (-x) = 0_G$ et $(-x) + x = 0_G$.

De plus, si la loi $+$ est commutative, autrement dit :

$$\forall (x, y) \in G^2, x + y = y + x.$$

alors le groupe est dit abélien.

Définition 2. (Sous-groupe) Soient $(G, +)$ un groupe et H une partie de G. On dit que H est un sous-groupe de $(G, +)$ si les conditions suivantes sont vérifiées :

- $H \neq \emptyset$.
- H est stable par la loi $+$: $\forall (x, y) \in H^2, x + y \in H$.
- H est stable par passage au symétrique pour la loi $+$: $\forall x \in H, -x \in H$.

3.1.1 Morphisme de groupes

Rappelons dans cette partie quelques notions fondamentales sur les morphismes de groupes. Il s'agit d'applications entre groupes qui respectent la loi de composition. Nous aborderons en particulier les homomorphismes, les isomorphismes et les automorphismes, qui jouent un rôle central dans l'étude des structures algébriques.

Définition 3. (Morphisme de groupes) Soit $(G, +)$ et $(H, \Diamond)$ deux groupes, et f une application de G dans H. On dit que f est un morphisme de groupes de $(G, +)$ dans $(H, \Diamond)$ si : $\forall (x, y) \in G^2, f(x + y) = f(x) \Diamond f(y)$.

Remarque 4. - *On appelle aussi homomorphisme de groupes tout morphisme de groupe.*

- *On note* $\mathrm{Hom}(G, H)$ *l'ensemble des morphismes d'un groupe* G *dans un groupe* H*.*
- *On appelle endomorphisme de groupe tout morphisme d'un groupe* G*.*
- *On note* $\mathrm{End(G)}$ *l'ensemble des endomorphismes d'un groupe* G*.*

Définition 5. (Isomorphisme) Soit G et H deux groupes. Une application f de G dans H est un isomorphisme de groupe si $f \in \mathrm{Hom(G, H)}$ et s'il existe $g \in \mathrm{Hom(G, H)}$ tel que $g \circ f = \mathrm{Id}_G$ et $f \circ g = \mathrm{Id}_H$.

Proposition 6. *Soient deux groupes* G *et* H*.*

1. *Si* f *est une application de* G *dans* H*, alors :* f *est un isomorphisme de groupe si et seulement si* $f \in \mathrm{Hom(G, H)}$ *et* f *est bijective.*
2. f *un isomorphisme de* G *sur* H *implique que* f^{-1} *est un isomorphisme de* H *sur* G*.*

Définition 7. S'il existe un isomorphisme d'un groupe G sur un groupe H, on dit que G et H sont des groupes isomorphes, et on écrit : $G \simeq H$.

Définition 8. (Automorphisme) Soit G un groupe. Un isomorphisme de G sur lui même est appelé automorphisme du groupe G. L'ensemble des automorphismes d'un groupe G est noté $\mathrm{Aut}(G)$.

Définition 9. (Somme directe)

La somme directe de deux groupes abéliens G et F, notée $G \oplus F$, est un groupe dont les éléments sont des couples ordonnés (g, f), où $g \in G$ et $f \in F$. L'opération de groupe sur ces couples est définie composante par composante, c'est-à-dire :

$$(g_1, f_1) + (g_2, f_2) = (g_1 +_G g_2, f_1 +_F f_2).$$

pour tous $(g_1, f_1), (g_2, f_2) \in G \oplus F$, où $+$ représente l'opération de groupe sur G et F.

Propriété 10.

- L'opération $+$ munit $G \oplus F$ d'une structure de groupe abélien.
- L'élément neutre est le couple $(0_G, 0_F)$.
- L'opposé de (g, f) est le couple $(-g_G, -f_F)$.

Remarque 11. *À partir de la somme de deux groupes et par récurrence, on peut définir la somme directe de* k *groupes pour tout* $k \geq 2$*.*

Remarque 12. *Nous discutons brièvement la distinction entre les groupes de classes de congruences et les groupes cycliques abstraits.*

La notation C_n désigne un groupe cyclique d'ordre n, c'est-à-dire un groupe abélien engendré par un seul élément. Dans notre contexte nous utilisons la notation additive.

Rappelons que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes de congruences modulo n qui forme un groupe par rapport à l'addition induite par l'opération sur les entiers relatifs. Ce groupe est engendré par la classe de 1. Il s'agit notamment d'un groupe cyclique d'ordre n.

Tout groupe cyclique $C_n = \langle g \rangle$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. À savoir l'application :

$$\begin{aligned} \Phi : \ \mathbb{Z}/n\mathbb{Z} &\to C_n \\ k + n\mathbb{Z} &\mapsto \underbrace{g + \cdots + g}_{k \text{ fois}} \end{aligned}$$

est un isomorphisme.

Il en découle que tous les groupes cycliques d'ordre n sont isomorphes. Toutefois l'isomorphisme n'est pas canonique puisque un groupe cyclique à priori n'a pas d'élément générateur distingué, contrairement à $\mathbb{Z}/n\mathbb{Z}$ pour lequel la classe de 1 se distingue par ses propriétés multiplicatives.

Autrement dit, sur C_n, à priori il n'y a aucune opération multiplicative.

Théorème 13. *(Kronecker (1870)) (Théorème fondamental des groupes abéliens finis). Soit G un groupe commutatif fini non trivial. Il existe un unique ensemble d'entiers positifs $n_1, \ldots, n_r$ avec $1 < n_1 \mid \cdots \mid n_r$, tel que*

$$G \cong C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}.$$

Remarque 14. *Nous renvoyons à la section 3.2 pour les définitions générales de* r(G), exp(G) *et de l'ordre de groupe.*

- *L'entier r dans le théorème précédent correspond à* r(G), *le rang de G. De plus si le groupe G est de cardinal strictement supérieur à 1, alors n_r est l'exposant du groupe G, noté* exp(G).
- *Dans le théorème, nous avons exclu le cas d'un groupe trivial, toutefois, notons qu'on pourrait dire que dans ce cas l'ensemble $n_1, \ldots, n_r$ serait l'ensemble vide et notamment, le rang du groupe est égal à 0 et son exposant est égal à 1.*
- *On écrit C_n^r pour $\underbrace{C_n \oplus \cdots \oplus C_n}_{r \text{ fois}}$ la somme directe de r groupes cycliques d'ordre n.*

Définition 15. Soit s un entier naturel non nul et soit $(e_1, \ldots, e_s)$ une famille de s éléments de G.

- On dit que la famille est indépendante si :

$$\text{Soit } (m_1, \ldots, m_s) \in \mathbb{Z}^s, \sum_{i=1}^{s} m_i e_i = 0 \text{ alors pour tout } i \in \{1, \ldots, s\},\ m_i = 0$$

.

- On dit qu'une famille $(e_1, \ldots, e_s)$ est génératrice si

$$\text{Pour tout } g \in G, \text{ il existe } (m_1, \ldots, m_s) \in \mathbb{Z}^s \text{ tel que } g = m_1 e_1 + \cdots + m_s e_s.$$

- On dit que la famille est une base de G si elle est à la fois indépendante et génératrice.

Notons que tout groupe abélien est un $\mathbb{Z}-$module et le concept de famille génératrice rappelé en haut correspond au concept de famille génératrice pour les modules. En revanche, le concept de famille indépendante ne correspond pas au concept de famille libre qu'on utilise pour les modules.

3.2 Rang, ordre et exposant d'un groupe

Dans cette section, nous rappelons les concepts de rang, d'ordre et d'exposant d'un groupe G. Soit $(G,+)$ un groupe abélien fini.

3.2.1 Le rang

Définition 16. Le rang d'un groupe est le cardinal minimal d'un ensemble de générateurs. On le note par $\mathrm{r}(G)$.

Nous donnons ci-dessous quelques résultats principaux du rang.

- Si G est un groupe cyclique, alors :

$$\mathrm{r}(G) = 1.$$

- Si $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ avec $1 < n_1 \mid \cdots \mid n_r$, alors :

$$\mathrm{r}(G) = r.$$

- Si $G = C_{m_1} \oplus \cdots \oplus C_{m_s}$, alors pour un nombre premier p, on appelle le p-rang de G noté $\mathrm{r}_p(G)$, le cardinal de l'ensemble

$$\{i \in \{1,\ldots,s\} \text{ tel que } p \mid m_i\},$$

c'est-à-dire le nombre de facteurs C_{m_i} de G dont l'ordre m_i est divisible par p.
Le rang de G est le maximum des p-rang, c'est-à-dire :

$$\mathrm{r}(G) = \max\{\mathrm{r}_p(G) \mid p \text{ premier}\}.$$

De plus, on a,

$$\mathrm{r}^*(G) = \sum_{p\in\mathbb{P}} \mathrm{r}_p(G)$$

qui représente le rang total de G.

3.2.2 L'ordre

Définition 17. (L'ordre d'un élément d'un groupe)
Soit G un groupe abélien fini. Pour $g \in G$, on appelle $\mathrm{ord}(g)$ ou encore $\mathrm{ord}_G(g)$ le plus petit entier $n \geq 1$ tel que

$$n \cdot g = 0_G.$$

Remarque 18. $\mathrm{ord}(g) = \mathrm{ord}(-g)$.

Remarque 19. *Soit* $k \in \mathbb{N}$, $\mathrm{ord}(kg) = \frac{\mathrm{ord}(g)}{\mathrm{pgcd}(k,\mathrm{ord}(g))}$.

Remarque 20. *Pour* $G = \mathbb{Z}/n\mathbb{Z}$, *on a :*

$$\mathrm{ord}(\overline{k}) = \frac{n}{\mathrm{pgcd}(k,n)} \text{ et si } k \mid n \text{ alors, } \mathrm{ord}(\overline{k}) = \frac{n}{k}.$$

Remarque 21. *On a toujours*

$$\mathrm{ord}(g) \mid \#G.$$

C'est-à-dire que l'ordre de chaque élément est un diviseur de l'ordre de groupe d'après le théorème de Lagrange.

Remarque 22. *L'ordre du groupe* G, *noté par* $\#G$ *peut être égal au ppcm des ordres de ses éléments, mais cela n'est vrai que si* G *est cyclique.*

3.2.3 L'exposant d'un groupe

Définition 23. Soit G un groupe abélien fini. On appelle exposant de G, noté $\exp(G)$, le plus petit entier positif m tel que pour tous les éléments $g \in G$,

$$m \cdot g = 0_G.$$

Autrement dit, $\exp(G)$ est le plus petit commun multiple de tous les ordres des éléments du groupe G.

$$\exp(G) = \mathrm{ppcm}\{\mathrm{ord}(g) \mid g \in G\}.$$

Nous présentons, dans le tableau ci-dessous, la valeur de $\exp(G)$ pour certains groupes.

G	$\exp(G)$
C_n	n
$G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ avec $1 < n_1 \mid \cdots \mid n_r$	n_r
$G = C_{m_1} \oplus \cdots \oplus C_{m_s}$	$\mathrm{ppcm}\{m_i : i \in \{1,\ldots,s\}\}$

Remarque 24. *Pour* $\#G = 1$, *on a :*

$$\exp(G) = 1 \text{ et } \mathrm{r}(G) = 0.$$

Définition 25. On dit que G est un p-groupe si $\exp(G) = p^k$, où p est un nombre premier et $k \in \mathbb{N}$.

Définition 26. On dit que G est un p-groupe élémentaire si $\exp(G) = p$.

Définition 27. Soit G un groupe abélien fini et d un entier. La d-torsion de G, noté e $G[d]$, est l'ensemble des éléments $g \in G$ tels que l'ordre de g divise d. Elle est donnée par

$$G[d] = \{g \in G\colon \ \mathrm{ord}(g) \mid d\}\,.$$

De plus, on pose

$$dG = \{dg\colon g \in G\}.$$

Définition 28. Soit G un groupe abélien fini. Soit $g \in G$. Notons

$$e(g) = \max\{d\colon d \mid \exp(G), g \in dG\}.$$

Notons que si $g = 0$ alors $e(g) = \exp(G)$.

Définition 29. La fonction de Möbius, notée $\mu\colon \mathbb{N}^* \to \{-1, 0, 1\}$ est la fonction définie par

- $\mu(1) = 1$,
- si n a un facteur carré, alors $\mu(n) = 0$,
- si n est le produit de nombres premiers tous distincts, $n = p_1 \cdot ... \cdot p_k$, alors $\mu(n) = (-1)^k$.

3.3 Structure de monoïde

Dans cette partie, nous allons présenter les notions liées à la structure d'un monoïde.

Définition 30. (Semi-groupe) Un semi-groupe est un ensemble muni d'une loi de composition interne associative. Il est dit commutatif si la loi est de plus commutative.

Définition 31. Soient H un ensemble et $\times$ une loi de composition interne sur H. On dit que $(H, \times)$ est un monoïde lorsque les conditions suivantes sont vérifiées :

- La loi $\times$ est associative : $\forall (x, y, z) \in H^3, (x \times y) \times z = x \times (y \times z)$.
- La loi $\times$ admet un élément neutre : $\exists e \in H, \forall x \in H, x \times e = x$ et $e \times x = x$.

En d'autres termes, on dit que H est un monoïde si c'est un semi-groupe qui possède en plus un élément neutre. De plus, si les éléments de H se commutent entre eux, on dit que H est un monoïde commutatif.

Définition 32. Un sous-monoïde d'un monoïde $(H, \times)$ est un sous-ensemble H' de H vérifiant :

- $\forall (x, y) \in H'^2, x \times y \in H'$,
- $e \in H'$, où e est l'élément neutre de H.

Définition 33. Un élément $a \in H$ est dit simplifiable si $ab = ac$ implique $b = c$ pour tout $b, c \in H$. De plus, si tous les éléments de H sont simplifiables, on dit que H est simplifiable.

Soulignons que, dans le cadre de notre thèse, nous adoptons la convention suivante (sauf indication contraire) : tout monoïde est commutatif et simplifiable. En effet, toutes les structures que nous étudions, notamment les différents monoïdes de suites à somme nulle, sont commutatifs et simplifiables.

Présentons maintenant la définition d'un monoïde libre.

Définition 34. Un monoïde $\mathcal{F}$ est dit libre (abélien avec une base $P \subset \mathcal{F}$) si pour chaque $a \in \mathcal{F}$, a a une représentation unique de la forme :

$$a = \prod_{p \in P} p^{v_p(a)}, \text{ avec } v_p(a) \in \mathbb{N}_0 \text{ et } v_p(a) > 0 \text{ uniquement pour un nombre fini de } p \in P.$$

Dans ce cas, $\mathcal{F}$ est déterminé de manière unique par P, et réciproquement, P est déterminé de manière unique par $\mathcal{F}$. Nous posons $\mathcal{F} = \mathcal{F}(P)$ et appelons

$$|a|_{\mathcal{F}} = |a| = \sum_{p \in P} v_p(a)$$

la longueur de a.

Précisons que nous maintenons la notation multiplicative pour les monoïdes, puisque, pour le monoïde des suites à somme nulle sur un groupe abélien, cela permet de distinguer la loi du monoïde de celle du groupe abélien sous-jacent.

3.4 Factorisation non-unique

Avant de présenter les concepts de base de la factorisation non unique, nous renvoyons à [17] et [21] pour plus de détails.

3.4.1 Les concepts de base de la factorisation non unique

Soit H un monoïde multiplicatif (rappelons que comme dans toute cette thèse , il est simplifiable et commutatif) et G un groupe additif abélien et fini. On note par :

- $H^\times$ l'ensemble des éléments inversibles de H, et on dit que H réduit si $H^\times = \{1\}$.
- $H_{\text{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ est le monoïde réduit associé.
- $\mathrm{q}(H)$ le groupe quotient de H. Un groupe abélien Q est appelé un groupe quotient du monoïde H si H est un sous-semi-groupe de Q et $Q = \{a^{-1}b \mid a, b \in H\}$. Par exemple, on a $\mathrm{q}(\mathbb{N}) = \mathbb{Q}_{>0}$. Tout monoïde commutatif et simplifiable possède un groupe quotient qui est déterminé de manière unique à un isomorphisme canonique près et noté par $\mathrm{q}(H)$. Si un monoïde H est écrit de manière additive, alors son groupe quotient est également noté de façon additive, et l'on a $\mathrm{q}(H) = \{a - b \mid a, b \in H\}$. Par exemple, on a $\mathrm{q}(\mathbb{N}_0) = \mathbb{Z}$ et $\mathrm{q}(\mathbb{R}_{\geq 0}) = \mathbb{R}$. Voir la section des prérequis de [21] pour plus de détails.

Soit $a, b \in H$. On dit que :

- a divise b et on écrit $a \mid b$, s'il existe un élément $c \in H$ tel que $b = ac$.
- a et b sont associés et on écrit $a \simeq b$ si $a \mid b$ et $b \mid a$.

Soit D un monoïde commutatif et simplifiable, et soit $H \subset D$ un sous-monoïde. On dit que H est saturé dans D si, pour tout $a, b \in H$ et $c \in D$, on a :

$$bc = a \quad \text{implique} \quad c \in H.$$

Autrement dit, si $b \mid a$ dans D alors $b \mid a$ dans H.

Un élément $a \in H$ est appelé :

- un atome (ou un élément irréductible) si $a \notin H^\times$ et, pour tous $b, c \in H$, $a = bc$ implique que $b \in H^\times$ ou $c \in H^\times$. On note $\mathcal{A}(H)$ l'ensemble de tous les atomes de H.
- un élément premier si $a \notin H^\times$ et, pour tous $b, c \in H$, $a \mid bc$ implique que $a \mid b$ ou $a \mid c$.

Le monoïde H est appelé :

- atomique si chaque élément $a \in H \setminus H^\times$ est un produit d'atomes.
- factoriel si l'une des conditions équivalentes suivantes est satisfaite :

1. Chaque élément $a \in H \setminus H^\times$ est un produit d'éléments premiers.
2. H est atomique, et chaque atome est un élément premier.
3. Chaque élément $a \in H \setminus H^\times$ est un produit d'atomes, et cette factorisation est unique aux éléments associés et à l'ordre des facteurs près.
4. H_{red} est libre (dans ce cas, H_{red} est libre avec une base $\{pH^\times \mid p \in P\}$ où P désigne l'ensemble des éléments premiers de H).

Notons que tout élément premier est un atome, et tout monoïde factoriel est atomique. Un élément $a \in H$ est un atome (un élément premier) de H si et seulement si $aH^\times$ est un atome (un élément premier) de H_{red}. Ainsi H_{red} est atomique (factoriel) si et seulement si H a cette propriété.

Soit H un monoïde atomique et soit $\mathsf{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\text{red}}))$ le monoïde libre, dont la base est l'ensemble des atomes de H_{red}. On appelle $\mathsf{Z}(H)$ le monoïde de factorisation de H.

L'homomorphisme

$$\pi_H = \pi \colon \mathsf{Z}(H) \to H_{\text{red}}, \text{ défini par } \pi(\mathsf{Z}) = \prod_{u \in A(H_{\text{red}})} u^{v_u(\mathsf{Z})}$$

est appelé l'homomorphisme de factorisation de H. Pour $a \in H$, nous définissons

$$\mathsf{Z}_H(a) = \mathsf{Z}(a) = \pi^{-1}(aH^\times) \subset \mathsf{Z}(H),$$

et nous appelons les éléments $z \in \mathsf{Z}(a)$ les factorisations de a.

Ce concept de factorisation formalise l'idée que l'on considère comme égales deux factorisations qui diffèrent uniquement par l'ordre de leurs facteurs et de leurs éléments associés.

On dit que a a une factorisation unique si $|\mathsf{Z}(a)| = 1$.

Pour une factorisation $z \in \mathsf{Z}(a)$, on appelle :

- $|z|$: la longueur de z,
- $\mathsf{L}_H(a) = \mathsf{L}(a) = \{|z| \mid z \in \mathsf{Z}(a)\} \subset \mathbb{N}_0$: l'ensemble des longueurs de a,
- $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$: le système des ensembles de longueurs de H.

Remarque 35. *Notons que* $0 \in \mathsf{L}(a)$ *si et seulement si* $a \in H^\times$ *et dans ce cas* $\mathsf{L}(a) = \{0\}$. *Nous avons* $1 \in \mathsf{L}(a)$ *si et seulement si* a *est un atome et donc* $\mathsf{L}(a) = \{1\}$.

Notons aussi que, le monoïde H est :

- Atomique si et seulement si $\mathsf{Z}(a) \neq \emptyset$ pour tout $a \in H$.
- Factoriel si et seulement si $|\mathsf{Z}(a)| = 1$ pour tout $a \in H$.

- Pour tout $b \in H$, on a

$$\mathsf{Z}(a)\mathsf{Z}(b) \subset \mathsf{Z}(ab) \text{ et } \mathsf{L}(a) + \mathsf{L}(b) \subset \mathsf{L}(ab).$$

De plus, le monoïde H est appelé :

- Demi-factoriel si $|\mathsf{L}(a)| = 1$ pour tout $a \in H$.
- FF-monoïde (un monoïde à factorisation finie) si $\mathsf{Z}(a)$ est fini et non vide pour tout $a \in H$.
- BF-monoïde (monoïde à factorisation bornée) si $\mathsf{L}(a)$ est fini et non vide pour tout $a \in H$.

3.5 Quelques invariants arithmétiques

Afin de décrire la structure des ensembles de longueurs, nous introduisons les invariants arithmétiques suivants. Pour plus de détails, voir [17, Section 3.A]. Pour cela, nous rappelons les notions et notations suivantes :

$$\sup \emptyset = \max \emptyset = \min \emptyset = 0.$$

- Soit $A, B \subset \mathbb{Z}$ des sous-ensembles finies et non vides, alors l'ensemble des sommes de A et B est défini par :

$$A + B = \{a + b \mid a \in A \text{ et } b \in B\}.$$

- On dénote par $\Delta(A)$ l'ensemble de distances de A, c'est-à-dire si $A = \{a_1, a_2, \ldots, a_t\}$ avec $t \in \mathbb{N}$ et $a_1 < \cdots < a_t$, alors :

$$\Delta(A) = \{a_{\nu+1} - a_\nu \mid \nu \in [1, t-1]\} \text{ avec } \Delta(\emptyset) = \emptyset.$$

- Un sous-ensemble $P \subset \mathbb{Z}$ est dit une progression arithmétique de raison $d \in \mathbb{N}$ si P est fini et non vide et $\Delta(P) \subset \{d\}$.
- Si $\emptyset \neq A \subset \mathbb{N}$, on appelle :

$$\rho(A) = \frac{\max A}{\min A} \in \mathbb{Q}_{\geq 1}$$

l'élasticité de A et on pose : $\rho(\{0\}) = 1$.

Exemple 36. Soit $A = \{2k, 2k+3, 2k+6, \ldots, 5k\}$ tel que $k \in \mathbb{N}$, alors :

$$\rho(A) = \frac{\max A}{\min A} = \frac{5k}{2k} = \frac{5}{2}.$$

3.5.1 Le degré de chaînage

Commençons tout d'abord par définir la notion de distance entre deux factorisations. Soit H un monoïde atomique et $\mathsf{Z}(H)$ son monoïde de factorisation.

Définition 37. Pour deux factorisations $z, z' \in \mathsf{Z}(H)$, on note par $\mathrm{d}(z, z')$ la distance entre z et z' définie par

$$\mathrm{d}(z, z') = \max\{|z| - |g|, |z'| - |g|\}$$

où $g = \mathrm{pgcd}(z, z')$ désigne la plus longue sous-suite qui divise à la fois z et z', composée de tous les termes communs entre z et z'.

Exemple 38. Soit $G = C_5 \oplus C_5$. Alors, pour $g_0 = 2e_1 + 2e_2$, on sait que les seules factorisations de $(-g_0) \cdot e_1^2 \cdot e_2^2 \cdot g_0 \cdot (-e_1)^2 \cdot (-e_2)^2$ sont : $z = ((-g_0) \cdot e_1^2 \cdot e_2^2) \cdot \big(g_0 \cdot (-e_1)^2 \cdot (-e_2)^2\big)$ qui est de longueur 2 et $z' = ((-g_0)\, g_0) \cdot ((-e_1)\, e_1) \cdot ((-e_1)\, e_1) \cdot ((-e_2)\, e_2) \cdot ((-e_2)\, e_2)$ qui est de longueur 5. De plus, comme les deux factorisations z, z' n'ont pas de facteur commun. Donc $g = \mathrm{pgcd}(z, z') = 1$ et $|g| = 0$ car il s'agit de la suite vide qui est de longueur 0. D'où, $\mathrm{d}(z, z') = \max\{(2-0), (5-0)\} = 5$. On en déduit donc que la distance entre z et z' est égale à 5.

Définition 39. Soit H un monoïde atomique.

1. Le degré de chaînage $\mathrm{c}(a)$, pour $a \in H$ est le plus petit $N \in \mathbb{N}_0 \cup \{\infty\}$ tel que, pour toute paire de factorisations z, z' de a, il existe une suite finie $z = z_0, z_1, \ldots, z_k = z'$ dans $\mathsf{Z}(a)$ de factorisations de a telle que $\mathrm{d}(z_{i-1}, z_i) \le N$ pour tout $i \in [1, k]$.
2. Globalement, nous définissons

   $$\mathrm{c}(H) = \sup\{\mathrm{c}(a) \mid a \in H\}$$

   et nous appelons $\mathrm{c}(a)$ le degré de chaînage de H

Le lemme suivant regroupe quelques propriétés élémentaires.

Lemme 40. *Soit H un monoïde atomique et soit $a \in H$.*

1. $\mathrm{c}(a) \le \sup \mathsf{L}(a)$, *et* $\mathrm{c}(a) = 0$ *si et seulement si* $|\mathsf{Z}(a)| = 1$.
2. *Si* z, $z' \in \mathsf{Z}(a)$ *et* $z \ne z'$ *alors,* $2 + ||z| - |z'|| \le \mathrm{d}(z, z')$.
3. *Si* $|z| \ge 2$, *alors* $2 + \sup \Delta(\mathsf{L}(a)) \le \mathrm{c}(a)$. *En particulier,* $2 + \sup \Delta(H) \le \mathrm{c}(H)$.
4. *Si* $\mathrm{c}(a) \le 2$, *alors* $|\mathsf{L}(a)| = 1$, *et si* $\mathrm{c}(a) \le 3$, *alors* $|\mathsf{L}(a)|$ *est une progression arithmétique de raison* 1.

3.5.2 L'ensemble de distances

Définition 41. Soit H un BF-monoïde et soit $\mathsf{L}(a)$ l'ensemble des longueurs de a, avec $a \in H$ et $\mathcal{L}(H)$ le système de l'ensemble des longueurs de H.

1. Pour $a \in H$, nous appelons $\rho(a) = \rho(\mathsf{L}(a))$ l'élasticité de a et

$$\rho(H) = \sup\{\rho(a) \mid a \in H\} = \sup\{\rho(\mathsf{L}) \mid \mathsf{L} \in \mathcal{L}(H)\} \in \mathbb{R}_{\ge 1} \cup \{\infty\}$$

   l'élasticité de H.

2. Soit $k \in \mathbb{N}$. Si $H = H^\times$, nous posons $\rho_k(H) = \lambda_k(H) = k$, et si $H \neq H^\times$, alors nous définissons

$$\rho_k(H) = \sup\{\max \mathsf{L} \mid \mathsf{L} \in \mathcal{L}(H), k \in \mathsf{L}\} \in \mathbb{N}_{\ge 1} \cup \{\infty\}$$

   et

$$\lambda_k(H) = \min\{\min \mathsf{L} \mid \mathsf{L} \in \mathcal{L}(H), k \in \mathsf{L}\} \in [1, k].$$

3. Nous appelons

$$\Delta(H) = \bigcup_{\mathsf{L} \in \mathcal{L}(H)} \Delta(\mathsf{L}) \subset \mathbb{N}$$

   l'ensemble des distances de H.

Remarque 42.

1. *H est demi-factoriel si et seulement si $\Delta(H) = \emptyset$.*
2. *H est demi-factoriel si et seulement si $\rho_k(H) = k$, pour tout $k \in \mathbb{N}$.*
3. *$|\Delta(H)| = 1$ si et seulement si tous les ensembles de longueurs sont des progressions arithmétiques de même raison.*

Définition 43. Soit H un BF-monoïde, et soit $k \in \mathbb{N}$. On note par $\mathcal{U}_k(H)$ l'ensemble de tous les $m \in \mathbb{N}$ pour lesquels il existe $u_1, \ldots, u_k, v_1, \ldots, v_m \in \mathcal{A}(H)$ tels que

$$u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m.$$

Lemme 44. *Soit H un BF-monoïde avec $H \neq H^\times$, et soient $k, l \in \mathbb{N}$.*

- *$\mathcal{U}_1(H) = \{1\}$, $k \in \mathcal{U}_k(H)$, et*

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

  En particulier, on a :

$$\rho_k(H) = \sup \mathcal{U}_k(H) \quad \text{et} \quad \lambda_k(H) = \min \mathcal{U}_k(H).$$

Ainsi, les ensembles $\mathcal{U}_k(H)$ sont des unions d'ensembles de longueurs. Ils ont été introduits par S.T. Chapman et W.W. Smith en 1990.

3.5.3 La modération locale

Nous poursuivrons avec la modération locale. Nous commençons par la définition formelle, puis nous discutons de la signification de ce principe en détail et notamment son lien avec la ω-primalité, dont nous rappelons également la définition en bas.

Définition 45. Supposons que H soit atomique.

1. Pour $a, b \in H$ soit $\omega(a, b)$ désigne le plus petit $N \in \mathbb{N}_0 \cup \{\infty\}$ ayant la propriété suivante :
   Pour tous $n \in \mathbb{N}$ et $a_1, \ldots, a_n \in H$, si $a = a_1 \cdot \ldots \cdot a_n$ et $b \mid a$, alors il existe un sous-ensemble $\Omega \subset [1, n]$ tel que $|\Omega| \leq N$ et

   $$b \mid \prod_{\nu \in \Omega} a_\nu$$

   En particulier, si $b \nmid a$, alors $\omega(a, b) = 0$. Pour $b \in H$, nous définissons la ω-primalité de b par

   $$\omega(H, b) = \sup\{\omega(a, b) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}$$

   .

2. Pour $a \in H$ et $x \in \mathsf{Z}(H)$, on définit $\mathsf{t}(a, x) \in \mathbb{N}_0 \cup \{\infty\}$ comme le plus petit $N \in \mathbb{N}_0 \cup \{\infty\}$ ayant la propriété suivante : Si $\mathsf{Z}(a) \cap x\mathsf{Z}(H) \neq \emptyset$ et $z \in \mathsf{Z}(a)$, alors il existe $z' \in \mathsf{Z}(a) \cap x\mathsf{Z}(H)$ tel que $\mathrm{d}(z, z') \leq N$.
   Nous définissons la modération locale par

   $$\mathrm{t}(H, x) = \sup\{\mathrm{t}(a, x) \mid a \in H\} \in \mathbb{N}_0 \cup \{\infty\}$$

   et pour le sous-ensemble $X \subset \mathsf{Z}(H)$, nous définissons

   $$\mathrm{t}(a, X) = \sup\{\mathrm{t}(a, x) \mid x \in X\} \in \mathbb{N}_0 \cup \{\infty\}.$$

   H est appelé localement modéré si $\mathrm{t}(H, u) < \infty$ pour tout $u \in \mathcal{A}(H_{\mathrm{red}})$.

La modération locale est une propriété de finitude fondamentale dans la théorie des factorisations non uniques, dans le sens où, dans de nombreuses situations où l'on étudie la finitude d'un invariant arithmétique comme le degré chaînage ou l'ensemble des distances, la finitude locale doit être prouvée en premier lieu. Pour simplifier la notation, supposons que H est atomique et réduit, et que $u \in \mathcal{A}(H)$. Alors u est un nombre premier si et seulement si $\omega(H, u) = 1$. Ainsi, $\omega(H, u)$ mesure à quel point u est loin d'être un nombre

premier. Soit $a \in H$. Si $u \nmid a$, alors par définition $\mathrm{t}(a,u) = 0$. Supposons que $u \mid a$, alors $\mathrm{t}(a,u)$ est le plus petit $N \in \mathbb{N}_0 \cup \{\infty\}$ avec la propriété suivante : Si $z = a_1 \cdot \ldots \cdot a_n$ est une factorisation quelconque de a où $a_1, \ldots, a_n$ sont des atomes, alors il existe un sous-ensemble $\Omega \subset [1,n]$, disons $\Omega = [1,k]$, et une factorisation $z' = uu_2 \cdot \ldots \cdot u_l u_{k+1} \cdot \ldots \cdot a_n$, avec les atomes $u_2, \ldots, u_l$ telle que $\max\{k,l\} \le N$. Ainsi, $\mathrm{t}(a,u)$ mesure à quelle distance, par rapport à une factorisation donnée z de a, il existe une factorisation z' de a contenant u. Et si u n'est pas un élément premier, alors $\omega(H,u) \le \mathrm{t}(H,u)$. Supposons que u soit un élément premier. Alors, chaque factorisation de a contient u, et nous pouvons choisir $z' = z$ dans la définition ci-dessus, ce qui donne $\mathrm{d}(z,z') = \mathrm{d}(z,z) = 0$, et donc $\mathrm{t}(H,u) = 0$. Cependant, dans les monoïdes qui satisfont la condition de chaîne ascendante pour les v-idéaux, nous avons $\omega(H,u) < \infty$ pour tous les atomes $u \in \mathcal{A}(H)$, cela ne se vérifie pas pour les valeurs de $\mathrm{t}(H,u)$. Pour plus de détails, voir [23, Théorème 3.6 et 4.4].

3.6 Les suites à somme nulle

Précisons qu'on écrit les suites multiplicativement et on les considère comme des éléments d'un monoïde abélien libre sur G.

Définition 46. Soit $\mathcal{F}(G)$ un monoïde abélien libre, noté multiplicativement, avec une base de G. Les éléments de $\mathcal{F}(G)$ sont appelés des suites sur G. On écrit $S \in \mathcal{F}(G)$ et on note :

$$S = \prod_{g \in G} g^{v_g(S)}, \text{ avec } v_g(S) \in \mathbb{N}_0 \text{ pour tout } g \in G.$$

Et si une suite $S \in \mathcal{F}(G)$ est écrite sous la forme $S = g_1 \cdot ... \cdot g_l$, on suppose implicitement que $l \in \mathbb{N}_0$ et $g_1, \ldots, g_l \in G$.

- $v_g(S) = |\{i \in [1, l] : g_i = g\}| \in \mathbb{N}_0$: la multiplicité de g dans S.
- On dit que S contient g si $v_g(S) > 0$.

Exemple 47. Soit la suite T définie par :

$$T = 1^3 \cdot 0 \cdot (-2)^5 \cdot 2 \in \mathcal{F}(\mathbb{Z}).$$

Il s'agit d'une suite d'entiers composée de 3 termes égaux à 1, un terme égal à 0, cinq termes égaux à (-2), et un terme égal à 2. De plus, on a :

$$v_1(T) = 3,\ v_0(T) = 1,\ v_{(-2)}(T) = 5,\ v_2(T) = 1 \text{ et } v_x(T) = 0 \text{ pour tous les autres } x \in \mathbb{Z}.$$

- Si $S, T \in \mathcal{F}(G)$ sont deux suites, alors $S \cdot T \in \mathcal{F}(G)$ est la suite obtenue par la concaténation des termes de T aprés ceux de S. Ainsi :

$$v_g(S \cdot T) = v_g(S) + v_g(T)\ \forall\ g \in G.$$

- On dit que S est carré libre si $v_g(S) \leq 1$ pour tout $g \in G$.
- L'élément neutre $1 \in \mathcal{F}(G)$ est appelé la suite vide.
- Une suite S_1 est dite sous-suite de S si $S_1 \mid S \in \mathcal{F}(G)$ (ce qui équivaut à $v_g(S_1) \leq v_g(S)$ pour tout $g \in G$). Elle est dite sous-suite propre de S si elle est une sous-suite telle que $1 \neq S_1 \neq S$.
- On note $T^{-1} \cdot S$ ou $S \cdot T^{-1}$ la suite obtenue en supprimant les termes de T de S. Ainsi, on a :

$$v_g(S \cdot T^{-1}) = v_g(T^{-1} \cdot S) = v_g(S) - v_g(T) \text{ pour tout } g \in G.$$

Exemple 48. Soit $T' = 1 \cdot (-2)^4 \cdot 2$, qui est une sous-suite de T (voir l'Exemple 47). Ainsi :

$$T'^{-1} \cdot T = T \cdot T'^{-1} = 1^2 \cdot 0 \cdot (-2).$$

- Soient $S, T \in \mathcal{F}(G)$, on note par le pgcd(S,T) la plus longue sous-suite qui divise à la fois S et T, composée de tous les termes communs entre S et T. On a alors :

$$v_g(\text{pgcd}(S,T)) = \min\{v_g(S), v_g(T)\} \text{ pour tout } \ g \in G.$$

Exemple 49. Considérons la suite T de l'Exemple 47 et soit la suite $S = 1^2 \cdot 0 \cdot 2^5 \cdot (-7)$, on obtient alors :

$$\text{pgcd}(S,T) = 1^2 \cdot 2 \cdot 0.$$

Pour une suite $S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G)$, nous appelons

- $|S| = l = \sum_{g \in G} v_g(S) \in \mathbb{N}_0$: la longueur de S,
- $\text{h}(S) = \max\{v_g(S) \mid g \in G\} \in [0, |S|]$: le maximum des multiplicités de S,
- $\text{supp(S)} = \{g \in G \mid v_g(S) > 0\} \subset G$: le support de S,
- $\sigma(S) = \sum_{i=1}^{l} g_i = \sum_{g \in G} v_g(S) g \in G$: la somme de S,
- $\sum_k(S) = \left\{ \sum_{i \in I} g_i \mid I \subset [1,l] \text{ avec } |I| = k \right\}$: l'ensemble des sous-sommes de k-termes de S pour tout $k \in \mathbb{N}$,
- $\sum_{\leq k}(S) = \bigcup_{j \in [1,k]} \sum_j(S)$, $\sum_{\geq k}(S) = \bigcup_{j \geq k} \sum_j(S)$, et $\sum(S) = \sum_{\geq 1}(S)$: l'ensemble des (toutes les) sous-sommes de S.

Exemple 50. Soit la suite T, $T = 1^3 \cdot 0 \cdot (-2)^5 \cdot 2$.
Or, $T = 1^3 \cdot 0 \cdot (-2)^5 \cdot 2 = 1 \cdot 1 \cdot 1 \cdot 0 \cdot (-2) \cdot (-2) \cdot (-2) \cdot (-2) \cdot (-2) \cdot 2$, on trouve alors :

- $|T| = l = \sum_{g \in G} v_g(T) = 3 + 1 + 5 + 1 = 10.$
- $\text{h}(T) = \max\{v_g(T) \mid g \in G\} = \max\{1, 3, 5\} = 5.$
- $\text{supp(T)} = \{g \in G \mid v_g(T) > 0\} = \{-2, 0, 1, 2\}.$
- $\sigma(T) = \sum_{g \in G} v_g(T) g = 3 \cdot 1 + 1 \cdot 0 + 5 \cdot (-2) + 1 \cdot 2 = -5.$
- $\sum_{k=2}(S) = \left\{ \sum_{i \in I} g_i \mid I \subset [1,10] \text{ avec } |I| = 2 \right\} = \{-4, -2, -1, 0, 1, 2, 3\}.$

La suite S est appelée :

- une suite sans somme nulle si $0 \notin \Sigma(S)$,
- une suite à somme nulle si $\sigma(S) = 0$,

- une suite à somme nulle minimale si c'est une suite à somme nulle non vide et que toute sous-suite propre est sans somme nulle,
- une suite à somme nulle courte si c'est une suite à somme nulle de longueur $|S| \in [1, \exp(G)]$.

Notons que pour toute application de groupes abéliens $\varphi : G \to G'$, il existe un unique homomorphisme

$$\overline{\varphi} : \mathcal{F}(G) \to \mathcal{F}(G'), \text{ tel que } \overline{\varphi}|_G = \varphi.$$

En général, nous écrivons simplement φ au lieu de $\overline{\varphi}$. Explicitement, $\varphi : \mathcal{F}(G) \to \mathcal{F}(G')$ est défini par :

$$\varphi(g_1 \cdot \ldots \cdot g_l) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_l), \text{ pour tous } l \in \mathbb{N}_0 \text{ et } g_1 \ldots g_l \in G.$$

Si $S \in \mathcal{F}(G)$, alors $|\varphi(S)| = |S|$ et $\operatorname{supp}(\varphi(S)) = \varphi(\operatorname{supp}(S))$. Si $\varphi : G \to G'$ est aussi un homomorphisme, alors $\sigma(\varphi(S)) = \varphi(\sigma(S))$, $\sum(\varphi(S)) = \varphi\left(\sum(S)\right)$ et $\varphi(\mathcal{B}(G)) \subset \mathcal{B}(G')$.

En particulier, nous utilisons l'inversion $(g \mapsto -g)$ et la translation $(g \mapsto g_0 + g)$, et pour $S = g_1 \cdot \ldots \cdot g_l \in \mathcal{F}(G)$, nous définissons :

$$-S = (-g_1) \cdot \ldots \cdot (-g_l) \text{ et } g_0 + S = (g_0 + g_1) \cdot \ldots \cdot (g_0 + g_l) \in \mathcal{F}(G).$$

Si $g \in G$ est un élément non nul et

$$S = (n_1 g) \cdot \ldots \cdot (n_l g), \text{ où } l \in \mathbb{N}_0 \text{ et } n_1, \ldots, n_l \in [1, \operatorname{ord}(g)],$$

alors la g-norme de S est définie par :

$$||S||_g = \frac{n_1 + \cdots + n_l}{\operatorname{ord}(g)}.$$

Si S est une suite à somme nulle pour laquelle $\{0\} \neq \langle \operatorname{supp}(S) \rangle \subset G$, et G est un groupe cyclique fini, alors l'indice de S est défini par :

$$\operatorname{ind}(S) = \min\{||S||_g \mid g \in G, \text{ avec } \langle \operatorname{supp(S)} \rangle = \langle g \rangle\} \in \mathbb{N}_0.$$

Nous posons $\operatorname{ind}(1) = 0$, et si $\operatorname{supp}(S) = \{0\}$, alors nous posons $\operatorname{ind}(S) = 1$.

Définition 51. Soit G un groupe abélien fini. Nous notons par

$$\mathcal{B}(G) = \{S \in \mathcal{F}(G) \mid \sigma(S) = 0\},$$

le monoïde des suites à somme nulle sur G. Il est aussi appelé « bloc monoïde ou monoïde de blocs ».

Exemple 52. Soit $G = C_3 = \{0, -e, e\}$. Alors :

$$\mathcal{B}(C_3) = \{S \in \mathcal{F}(C_3) \mid \sigma(S) = 0\} = \{0, (-e) \cdot e\}.$$

Notons que les éléments de $\mathcal{B}(G)$ sont appelés des suites à somme nulle, et les atomes de $\mathcal{B}(G)$ sont appelés des suites minimales à somme nulle et ils sont notés par $\mathcal{A}(G)$. Soit $\mathcal{A}^*(G)$ l'ensemble des suites qui ne possèdent aucune sous-suite à somme nulle.

Nous définissons maintenant les monoïdes de Krull qui jouent un rôle central dans la théorie de la factorisation. Nous résumons brièvement certaines de leurs propriétés. Pour plus de détails voir [21]. Les preuves complètes peuvent être trouvées dans [21] ou [29]. Il y a aussi des caractérisations plus algébriques des monoïdes de Krull, notamment en utilisant les v-idéaux.

Définition 53. (Monoïde de Krull) H est appelé monoïde de Krull si H_{red} est un sous-monoïde saturé d'un monoïde libre.

Proposition 54. *Les affirmations suivantes sont équivalentes :*

1. *H est un monoïde de Krull.*
2. *H_{red} est un monoïde de Krull et $H = H^\times \times H_0$ pour un certain sous-monoïde H_0 de H. Avec $H_0 \cong H_{\text{red}}$.*
3. *H est un sous-monoïde saturé d'un monoïde factoriel.*

Proposition 55. *Soit G un ensemble non vide.*

1. *$\mathcal{B}(G) \subset \mathcal{F}(G)$ est un sous-monoïde saturé de $\mathcal{F}(G)$, et donc $\mathcal{B}(G)$ est un monoïde de Krull.*
2. *$\mathcal{A}(G)$ est fini, et donc $\mathcal{B}(G)$ est de type fini (finitely generated en anglais, qui signifie ensemble engendré par un nombre fini d'éléments).*
3. *Les affirmations suivantes sont équivalentes :*
   - **(a)** $\#G \leq 2$.
   - **(b)** *$\mathcal{B}(G)$ est factoriel.*
   - **(c)** *$\mathcal{B}(G)$ est demi-factoriel.*

Une méthode centrale dans la théorie de la factorisation est d'étudier l'arithmétique dans des monoïdes auxiliaires et de transférer les résultats vers des monoïdes et des anneaux intègres d'intérêt arithmétique. Nous donnons donc une définition cruciale, celle d'un homomorphisme de transfert.

Définition 56. Une homomorphisme de monoïdes $\Theta : H \to \mathcal{B}$ est appelé un homomorphisme de transfert s'il possède les propriétés suivantes :

(T1) $\mathcal{B} = \Theta(H)\mathcal{B}^\times$ et $\Theta^{-1}(\mathcal{B}^\times) = H^\times$.

(T2) Si $u \in H, b, c \in \mathcal{B}$ et $\Theta(u) = bc$, alors il existe $v, w \in H$ tel que $u = vw, \Theta(v) \simeq b$ et $\Theta(w) \simeq c$.

Ainsi, la stratégie consiste à trouver, pour un monoïde donné H, un monoïde plus simple $\mathcal{B}$, et à étudier l'arithmétique dans $\mathcal{B}$, puis à transférer les résultats arithmétiques de $\mathcal{B}$ vers H. Pour plus de détails voir [21].

3.7 La constante de Davenport

Dans cette partie, nous faisons un bref rappel du développement historique de la constante de Davenport, suivie de sa définition et de la présentation de quelques résultats importants qui lui sont liés.

3.7.1 Origines et Définition

La constante de Davenport tire son nom du mathématicien britannique Harold Davenport, qui a été un contributeur important dans le domaine de la théorie des nombres. Il semble qu'il a évoqué le lien entre cette constante et des questions sur la factorisation des entiers algébriques lors d'un colloque en 1966 ; Olson en parle dans [44] et [43]. Or, comme évoqué en [45] ce lien se trouve déjà dans un article de Rogers [46].

Par ailleurs, nous établissons un nouveau lien entre les suites à somme nulle et la factorisation des entiers algébriques au chapitre 8.

La constante de Davenport est définie ainsi :

Définition 57. Soit G un groupe abélien fini noté additivement. La constante de Davenport notée $\mathsf{D}(G)$ est le plus petit entier $l \in \mathbb{N}$ tel que toute suite $S \in \mathcal{F}(G)$ de longueur $|S| \geq l$ a une sous-suite non vide à somme nulle.

En d'autres termes, pour toute suite de l éléments ou plus (avec répétition) dans G, il existe nécessairement une sous-suite non vide dont la somme est égale à 0.

Ce problème de déterminer la valeur exacte de la constante de Davenport reste ouvert pour de nombreux groupes abéliens, et la valeur exacte de la constante de Davenport n'est connue que pour des groupes abélien finis particuliers. Nous présentons ensuite quelques résultats classiques à son sujet, notre présentation suit [53] qui donne plus de détails.

Les premiers travaux approfondis sur cette constante datent de 1969 et ils sont dûs à plusieurs chercheurs, notamment Olson et un groupe de chercheurs à Amsterdam comme Baayen et van Emde Boas, voir par exemple : [44], [43] et [34].

De plus, Olson a démontré deux résultats, voir [44] et [43], donnant la valeur exacte de la constante de Davenport dans le cas des p-groupes abéliens finis (où l'exposant du groupe est une puissance d'un nombre premier), et des groupes abéliens finis de rang inférieur ou égal à deux. En dehors de ces résultats, peu d'autres sont connus.

3.7.2 Principaux résultats

Si $G = \oplus_{i=1}^{r} C_{n_i}$ est la somme directe de groupes cycliques C_{n_i}, où n_i représente l'ordre du groupe cyclique vérifiant $n_i \mid n_{i+1}$ et r est le rang du groupe G. Alors on peut définir $\mathsf{D}^*(G)$ comme

$$\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r}(n_i - 1).$$

Nous avons les deux inégalités suivantes :

$$\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r}(n_i - 1) \leq \mathsf{D}(G) \leq n_r\left(1 + \log\frac{|\,G\,|}{n_r}\right).$$

D'où, $\forall n \in \mathbb{N}^*$, $\mathsf{D}(C_n) = n$.

Dès la fin des années 1960, il était connu que $\mathsf{D}(G) = \mathsf{D}^*(G)$ dans certains cas. nous présentons un récapitulatif des cas où cette égalité est vérifiée.

- Pour les p-groupes et les groupes de rang au plus 2. Voir [44], [43] et [51].
- Pour le groupe $G \oplus C_n$ avec G est un p-groupe et $\mathsf{D}(G) \leq 2\exp(G) - 1$ et $\text{pgcd}(n, \exp(G)) = 1$. Voir [51] et [9] pour la généralisation.
- Pour les groupes de rang 3 (certains cas).
- Pour le groupe de rang 4 de la forme $C_2^3 \oplus C_{2n}$. Voir [4].

Il est également connu que $\mathsf{D}(G) = \mathsf{D}^*(G) + 1$ dans les cas suivants (dû à V. Ponomarenko, voir [48]) :

- Pour les groupes de la forme $C_2^{r-1} \oplus C_6$ où $r \in \{5, 6, 7\}$.
- Pour le groupe $C_3^3 \oplus C_6$.

Pour le cas où $\mathsf{D}(G) = \mathsf{D}^*(G) + 2$, on connaît la valeur de la constante de Davenport pour le groupe $C_2^7 \oplus C_6$, voir [48].

On sait aussi que la valeur de la constante de Davenport pour les groupes de la forme $C_2^4 \oplus C_{2k}$ avec $k \geq 70$ est :

$\mathsf{D}(C_2^4 \oplus C_{2k}) = 2k + 4 = \mathsf{D}^*(C_2^4 \oplus C_{2k})$, si k est pair. Et $\mathsf{D}(C_2^4 \oplus C_{2k}) = 2k + 5 = \mathsf{D}^*(C_2^4 \oplus C_{2k}) + 1$, si k est impair. Pour plus de détails, voir [10].

Chapitre

4 Le monoïde des suites qui admettent une somme nulle Ω-pondérée

L'objectif de ce chapitre est de présenter les monoïdes de suites sur un groupe abélien fini G qui admettent une somme nulle Ω-pondérée pour un ensemble général de poids $\Omega \subseteq \mathrm{End}(G)$ qu'on aura besoin dans les Chapitres 6 et 7 et d'établir des premiers résultats sur leur arithmétique. Plusieurs paramètres arithmétiques seront étudiés, notamment le fait que l'ensemble des distances est fini et que l'élasticité est également finie. Dans le Chapitre 6, nous affinerons certains de ces résultats. Ensuite, dans le Chapitre 7, nous présenterons des résultats plus détaillés pour le cas des poids plus-moins. C'est-à-dire pour le cas particulier $\{+\,\mathrm{id}_G, -\,\mathrm{id}_G\}$, voir [8, Section 3 et 6].

Définition 58. Soit G_0 un sous-ensemble d'un groupe abélien fini G et soit $\emptyset \neq \Omega \subseteq \mathrm{End}(G)$, alors

$$\sigma_\Omega(S) = \left\{ \sum_{i=1}^{l} \omega_i g_i \mid \omega_i \in \Omega \right\}$$

l'ensemble des sommes Ω-pondérées. Nous définissons l'ensemble des suites sur G_0 qui admettent une somme nulle Ω-pondérée sur G_0 par :

$$\mathcal{B}_\Omega(G_0) = \{S \in \mathcal{F}(G_0) \mid 0 \in \sigma_\Omega(S)\}\,.$$

Dans ce contexte l'ensemble Ω est appelé ensemble de poids. La condition que l'ensemble de poids est non vide est imposé puisque sinon la définition de $\sigma_\Omega(S)$ n'a pas vraiment de sens. On pourrait dire dans ce cas que l'ensemble $\sigma_\Omega(S)$ est vide, sauf pour la suite vide, dans ce cas-là le monoïde $\mathcal{B}_\Omega(G_0)$ sera réduit au monoïde trivial $1_{\mathcal{F}(G_0)}$.

Comme mentionné précédemment, ces suites sont également appelées suites à somme nulle Ω-pondérée, et on peut donc désigner $\mathcal{B}_\Omega(G_0)$ comme étant l'ensemble des suites à somme nulle Ω-pondérée.

Pour éviter toute confusion, nous soulignons que ce sont les sommes qui sont pondérées et non les suites elles-mêmes. Les éléments de $\mathcal{B}_\Omega(G_0)$ sont simplement des suites sur G_0, c'est-à-dire $\mathcal{B}_\Omega(G_0) \subseteq \mathcal{F}(G_0)$. Notons 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 $\mathcal{F}(G_0)$. Et puisque $\{\omega(\sigma(S))\colon \omega \in \Omega\} \subseteq \sigma_\Omega(S)$, il en résulte que si $0 = \sigma(S)$, alors $0 \in \sigma_\Omega(S)$. Notant que ici nous utilisons le fait que Ω est non vide et, donc $\mathcal{B}(G_0) \subseteq \mathcal{B}_\Omega(G_0)$. Comme $\mathcal{B}_\Omega(G_0)$ 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 [21, Corollaire 1.3.3].

Notons que pour le cas particulier où $\Omega = \{+\operatorname{id}_G, -\operatorname{id}_G\}$, nous utilisons la notation $\pm$ à la place de Ω. Ainsi,

$$\mathcal{B}_\pm(G) = \{S \in \mathcal{F}(G) \quad | \quad 0 \in \sigma_\pm(S)\},$$

où $\sigma_\pm(S) = \left\{ \sum_{i=1}^{l} \omega_i g_i \quad | \quad \omega_i \in \{+\operatorname{id}_G, -\operatorname{id}_G\} \right\}$ désigne l'ensemble des sommes $\pm$-pondérées.

Nous rappelons que $\mathcal{B}_\Omega(G_0)$ est un monoïde réduit, c'est-à-dire le seul élément inversible de ce dernier est la suite « vide » notée 1.

Définition 59. Une suite $S \in \mathcal{A}(\mathcal{B}_\Omega(G_0))$ est dite minimale à somme nulle Ω-pondérée. Rappelons que $S \in \mathcal{A}(\mathcal{B}_\Omega(G_0))$ veut dire que $S \in \mathcal{B}_\Omega(G_0) \setminus \{1\}$ est irréductible dans $\mathcal{B}_\Omega(G_0)$, c'est-à-dire, qu'il n'est pas possible d'écrire $S = S_1S_2$ avec $S_1, S_2 \in \mathcal{B}_\Omega(G_0) \setminus \{1\}$.

Nous soulignons qu'à la différence du problème sans poids, cette définition n'est pas, en général, équivalente à dire que la suite S à somme nulle Ω-pondérée n'a pas de sous-suite propre et non vide à somme nulle Ω-pondérée.

En d'autres termes, il est possible que $S = S_1T$ avec $S, S_1 \in \mathcal{B}_\Omega(G_0)$ et $T \in \mathcal{F}(G)$ mais que $T \notin \mathcal{B}_\Omega(G_0)$. L'idée est que $\sigma_\Omega(S_1), \sigma_\Omega(T)$ sont des sous-ensembles de G et il est tout à fait possible que pour des sous-ensembles A, B d'un groupe abélien, on ait $0 \in A + B = \{a + b : \ a \in A,\, b \in B\}$ et $0 \in A$, mais $0 \notin B$, alors que pour des éléments $a, b \in G$, il est évident que $0 = a + b$ et $0 = a$ 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 un monoïde de Krull. Bien entendu, dans certains cas spécifiques, cela pourrait néanmoins être le cas. Nous discutons ce problème vers la fin de ce chapitre.

Les constantes de Davenport jouent un rôle important dans l'étude de l'arithmétique des monoïdes de suites à somme nulle. Il existe diverses études sur les constantes de Davenport avec poids. Cependant, il est nécessaire de faire preuve de prudence, car ces constantes ne correspondent pas aux constantes les plus pertinentes dans le contexte

actuel. Pour expliquer la situation, rappelons deux définitions de Cziszter, Domokos et Geroldinger, voir [11, Section 2.5].

Soit H un BF-monoïde et soit $|\cdot| : H \to (\mathbb{N}_0, +)$ un homomorphisme de monoïdes qui, dans ce contexte, est appelé fonction de degré. Par exemple, si H est un sous-ensemble d'un monoïde libre, alors la fonction de longueur usuelle est une fonction de degré. En revanche pour des semi-groupes numériques, c'est-à-dire des sous-semi-groupes de $(\mathbb{N}_0, +)$ dont les compléments soient finis, l'homomorphisme d'inclusion est une fonction de longueur.

Alors, pour $k \in \mathbb{N}$ la k-ème grande constante de Davenport de H (par rapport à la fonction de degré donnée) est définie comme $\sup\{|a| \quad | \quad a \in \mathcal{M}_k(H)\}$ où $\mathcal{M}_k(H) = \{a \in H \quad | \quad \max \mathsf{L}(a) \leq k\}$. On la note $\mathsf{D}_k(H, |\cdot|)$ ou plus souvent $\mathsf{D}_k(H)$ lorsque la fonction de degré est évidente.

Pour $k = 1$, l'indice est négligé et $\mathsf{D}(H) = \mathsf{D}_1(H)$ est appelé la constante de Davenport de H. Notons que dans ce cas là $\mathsf{D}(H) = \sup\{|a| \quad | \quad a \in \mathcal{A}(H)\}$.

Soit H un sous-monoïde d'un monoïde libre F et soit $|\cdot|$ la fonction de longueur usuelle sur F, et pour $k \in \mathbb{N}$ soit $\mathcal{M}_k^*(H)$ l'ensemble de tous les $f \in$ F tels que f n'est pas divisible (dans F) par un produit de k éléments non-unités dans H. La k-ème petite constante de Davenport de H, notée $\mathsf{d}_k(H)$, est définie comme $\sup\{|f| \quad | \quad f \in \mathcal{M}_k^*(H)\}$. De nouveau, pour $k = 1$, on écrit simplement $\mathsf{d}(H)$ et on l'appelle la petite constante de Davenport de H. D'après la définition, il en résulte que $1 + \mathsf{d}_k(H)$ est le plus petit $l \in \mathbb{N} \cup \{\infty\}$ tel que tout $f \in$ F de longueur au moins l est divisible (dans $\mathcal{F}$) par un produit de k éléments non-unités dans H. Dans de nombreuses situations courantes, il est vrai que $1 + \mathsf{d}_k(H) \leq \mathsf{D}_k(H)$ et il arrive même que l'égalité soit vérifiée. Cela est particulièrement vrai pour $H = \mathcal{B}(G)$ ce qui permet d'utiliser les deux définitions de manière interchangeable. Cependant, en général, cela n'est pas vrai et il est même possible que $\mathsf{d}_k(H)$ dépasse $\mathsf{D}_k(H)$. En particulier, la constante de Davenport avec poids, que l'on trouve généralement dans la littérature et qui est souvent notée $\mathsf{D}_\Omega(G)$, est en fait $1 + \mathsf{d}(\mathcal{B}_\Omega(G))$, mais pas $\mathsf{D}(\mathcal{B}_\Omega(G))$. Dans notre contexte et afin d'éviter toute confusion, nous utilisons systématiquement la notation pour les monoïdes et ne faisons pas usage de la notation abrégée habituelle qui omet le $\mathcal{B}$.

Nous commençons par rappeler un résultat bien connu concernant la finitude de la constante de Davenport, voir, par exemple [21, Théorème 3.4.2].

Proposition 60. *Soit G un groupe abélien et soit $G_0 \subseteq G$ un sous-ensemble fini. Alors $\mathsf{D}(\mathcal{B}(G_0))$ est fini. Notons que la fonction de degré considérée ici est tout simplement la longueur de la suite donnée.*

Nous démontrons maintenant que pour des sous-ensemble d'un groupe abélien fini, $\mathsf{D}(\mathcal{B}_\Omega(G_0))$ est majoré par $\mathsf{D}(\mathcal{B}(G))$.

Lemme 61. *Soit G un groupe abélien fini et soit $G_0 \subseteq G$. Alors $\mathsf{D}(\mathcal{B}_\Omega(G_0)) \leq \mathsf{D}(\mathcal{B}(G))$. De plus, $\mathcal{A}(\mathcal{B}_\Omega(G_0)) \cap \mathcal{B}(G_0) \subseteq \mathcal{A}(\mathcal{B}(G))$.*

Démonstration. Soit $g_1 \dots g_\ell$ une suite dans $\mathcal{A}(\mathcal{B}_\Omega(G_0))$. Alors, pour chaque $i \in [1, \ell]$, il existe $\omega_i \in \Omega \neq \emptyset$ tel que $\sum_{i=1}^{\ell} \omega_i g_i = 0$. Nous montrons maintenant que $(\omega_1 g_1) \dots (\omega_\ell g_\ell) \in \mathcal{A}(\mathcal{B}(G))$. Par construction, la somme de la suite est 0. Il reste à montrer que c'est une suite à somme nulle minimale. Supposons, par l'absurde, qu'il existe un ensemble $\emptyset \neq I \subsetneq [1, \ell]$ tel que $\prod_{i\in I}(\omega_i g_i)$ et $\prod_{i\in[1,\ell]\setminus I}(\omega_i g_i)$ sont des suites à somme nulle. Alors $(\prod_{i\in I} g_i)$ et $(\prod_{i\in[1,\ell]\setminus I} g_i)$ sont des suites à somme nulle Ω-pondérées. D'où une contradiction.

Ainsi, pour tout $S \in \mathcal{A}(\mathcal{B}_\Omega(G_0))$, il existe $S' \in \mathcal{A}(\mathcal{B}(G))$ de même longueur. Cela implique directement que $\mathsf{D}(\mathcal{B}_\Omega(G_0)) \leq \mathsf{D}(\mathcal{B}(G))$. L'affirmation supplémentaire est évident en rappelant que $\mathcal{B}(G_0) \subseteq \mathcal{B}_\Omega(G_0)$, ce qui implique que chaque factorisation dans $\mathcal{B}(G_0)$ donne une factorisation dans $\mathcal{B}_\Omega(G_0)$. □

Ensuite, nous établissons que chaque suite de longueur $\mathsf{D}(\mathcal{B}_\Omega(G))$ possède une sous-suite non vide à somme nulle Ω-pondérée.

Théorème 62. *Soit G un groupe abélien fini. Alors* $1+\mathsf{d}(\mathcal{B}_\Omega(G)) \leq \mathsf{D}(\mathcal{B}_\Omega(G)) \leq \mathsf{D}(\mathcal{B}(G))$.

Démonstration. D'après le Lemme 61, nous avons $\mathsf{D}(\mathcal{B}_\Omega(G)) \leq \mathsf{D}(\mathcal{B}(G))$. Nous allons maintenant montrer que $1 + \mathsf{d}(\mathcal{B}_\Omega(G)) \leq \mathsf{D}(\mathcal{B}_\Omega(G))$. Soit S une suite de longueur $\ell = \mathsf{D}(\mathcal{B}_\Omega(G)))$. Démontrons qu'elle possède une sous-suite à somme nulle Ω-pondérée non vide. Considérons la suite $(-\sigma(S))S$, c'est-à-dire, on ajoute le terme $-\sigma(S)$ à la suite S. Notons que cette suite appartient à $\mathcal{B}(G)$ et, par l'inclusion $\mathcal{B}(G) \subseteq \mathcal{B}_\Omega(G)$, elle appartient également à $\mathcal{B}_\Omega(G)$.

Or, $|(-\sigma(S))S| = 1+|S| > \mathsf{D}(\mathcal{B}_\Omega(G))$. Par conséquent, ce n'est pas une suite à somme nulle minimale Ω-pondérée, et il existe des sous-suites non vides $S_1, S_2 \in \mathcal{B}_\Omega(G)$ telles que $(-\sigma(S))S = S_1 S_2$.

Il s'ensuit que S_1 ou S_2 est une sous-suite de S, ce qui prouve que S possède une sous-suite à somme nulle Ω-pondérée non vide.

Ainsi, nous avons établi que toute suite de longueur $\mathsf{D}(\mathcal{B}_\Omega(G))$ a une sous-suite à somme nulle Ω-pondérée non vide. Puisque, par définition, $1 + \mathsf{d}(\mathcal{B}_\Omega(G))$ est le plus petit entier positif ayant cette propriété, d'où $1 + \mathsf{d}(\mathcal{B}_\Omega(G)) \leq \mathsf{D}(\mathcal{B}_\Omega(G))$. □

Exemple 63. Soient $G = C_{19}$ et $\Omega = \{-\mathrm{id}_G; +\mathrm{id}_G\}$. Un exemple d'une suite sans somme nulle Ω-pondérée est $S = e \cdot 2e \cdot 4e \cdot 8e$ (Rappelons que S est de longueur maximale puisque $\mathsf{d}(\mathcal{B}_\pm(G)) = 4$, nous renvoyons au [1] et [38]). On a $-\sigma(S) = 4e$ et la suite $(4e)e(2e)(4e)(8e) \in \mathcal{A}(\mathcal{B}_\pm(G))$. Notons qu'il existe des sous-suites propres à somme nulle $\pm$-pondérée, notamment $(4e)^2$ mais qu'il n'existe pas de décompositions en sous-suites à somme nulle Ω-pondérée. Remarquons qu'il y a des suites encore plus longues dans $\mathcal{A}(\mathcal{B}_\pm(G))$ notamment e^{19}. Nous voyons plus bas que $\mathsf{D}(\mathcal{B}_\pm(C_{19})) = \mathsf{D}(\mathcal{B}(C_{19})) = 19$.

Nous montrons maintenant que $\mathcal{B}_\Omega(G_0)$ est de type fini. Nous établissons immédiatement le corollaire suivant :

Corollaire 64. *Soit G un groupe abélien fini et soit $G_0 \subseteq G$. Soit $\Omega \subseteq \mathrm{End}(G)$ un ensemble de poids. Le monoïde $\mathcal{B}_\Omega(G_0)$ est de type fini.*

Démonstration. Comme la longueur des éléments de $\mathcal{A}(\mathcal{B}_\Omega(G_0))$ est majorée par $\mathsf{D}(\mathcal{B}_\Omega(G_0))$, qui est fini d'après le Lemme 61, il en résulte que l'ensemble $\mathcal{A}(\mathcal{B}_\Omega(G_0))$ est fini, c'est-à-dire que le monoïde est de type fini. □

Ce résultat a des conséquences immédiates et importantes pour l'arithmétique de ces monoïdes, que nous discutons ci-dessous. Cependant, avant cela, nous établissons un nouveau minorant de la constante de Davenport, dont nous aurons besoin par la suite.

Lemme 65. *Soit $G = G_1 \oplus G_2$ un groupe abélien fini. Soit $\Omega \subseteq \mathrm{End}(G)$ un ensemble d'endomorphismes qui forme un groupe sous la composition des endomorphismes et tel que $\omega(G_i) \subseteq G_i$ pour $i \in \{1, 2\}$. Alors $\mathsf{D}(\mathcal{B}_\Omega(G)) \geq \mathsf{D}(\mathcal{B}_\Omega(G_1)) + \mathsf{D}(\mathcal{B}_\Omega(G_2)) - 1$.*

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 fixé 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 $\omega_i g_i \in -\sigma_\Omega(F_i)$. Nous considérons maintenant $A = (\omega_1 g_1 + \omega_2 g_2) F_1 F_2$ et affirmons qu'elle est contenue dans $\mathcal{A}(\mathcal{B}_\Omega(G))$. Nous commençons par montrer que $0 \in \sigma_\Omega(A)$. Puisque Ω est un groupe, il existe $\epsilon \in \Omega$ tel que $\epsilon \circ \omega_i = \omega_i$ pour $i \in \{1, 2\}$.

Maintenant, $\epsilon(\omega_1 g_1 + \omega_2 g_2) \in -(\sigma_\Omega(F_1) + \sigma_\Omega(F_2)) = -(\sigma_\Omega(F_1 F_2))$, ce qui implique que $0 \in \sigma_\Omega(A)$. Il reste à montrer qu'il n'y a pas de décomposition $A = A'A''$ avec A' et A'' non vides telles que $0 \in \sigma_\Omega(A')$ et $0 \in \sigma_\Omega(A'')$. Supposons, par l'absurde, 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 alors $A' = (\omega_1 g_1 + \omega_2 g_2) F_1' F_2'$ et $A'' = F_1'' F_2''$, où $F_i = F_i' F_i''$ pour $i \in \{1, 2\}$.

Puisque $0 \in \sigma_\Omega(A'')$ et $\sigma_\Omega(F_i'') \subseteq G_i$ pour $i \in \{1, 2\}$, il s'ensuit que $0 \in \sigma_\Omega(F_i'')$. De plus, il existe $\omega \in \Omega$ tel que $\omega(\omega_1 g_1 + \omega_2 g_2) \in -\sigma_\Omega(F_1' F_2')$. Cela implique que $\omega(\omega_i g_i) \in -\sigma_\Omega(F_i')$ pour $i \in \{1, 2\}$. Maintenant, comme la composition des endomorphismes ω et ω_i est dans Ω par hypothèse sur Ω, cela signifie que $0 \in \sigma_\Omega(g_i F_i')$. Ainsi, $A_i = (g_i F_i') F_i''$ et $0 \in \sigma_\Omega(g_i F_i')$ et $0 \in \sigma_\Omega(F_i'')$. Puisque au moins l'un de F_1'' et F_2'' est non vide et que $g_1 F_1'$ et $g_2 F_2'$ sont bien sûr tous les deux non vides, on obtient une contradiction avec le fait que A_1 ou A_2 soient irréductibles. □

Nous abordons maintenant l'arithmétique des monoïdes de suites à somme nulle pondérée. Nous nous référons à la Section 3.5 du Chapitre 3 pour les définitions des différents invariants arithmétiques qu'on va utiliser après.

Théorème 66. *Soit G un groupe abélien fini et soit $G_0 \subseteq G$. Soit $\Omega \subseteq \mathrm{End}(G)$ 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 un* $M \in \mathbb{N}_0$ *tel que chaque ensemble de longueurs* L *de* H *est une multi-progression presque arithmétique avec une borne* M *et une raison* $d \in \Delta(H) \cup \{0\}$, *c'est-à-dire que* $\mathsf{L} = y + (\mathsf{L}_1 \cup \mathsf{L}^* \cup (\max \mathsf{L}^* + \mathsf{L}_2)) \subseteq y + \mathcal{D} + d\mathbb{Z}$ *avec* $y \in \mathbb{N}_0$, $\{0, d\} \subseteq \mathcal{D} \subseteq [0, d]$, $-\mathsf{L}_1, \mathsf{L}_2 \subseteq [1, M]$, $\min \mathsf{L}^* = 0$ *et* $\mathsf{L}^* = [0, \max \mathsf{L}^*] \cap \mathcal{D} + d\mathbb{Z}$.

3. *Il existe un* $M' \in \mathbb{N}_0$ *tel que pour chaque* $k \in \mathbb{N}_0$, *l'ensemble* $\mathcal{U}_k(H)$ *est une progression presque arithmétique avec une borne* M' *et une raison* $d' = \min \Delta(H)$, *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. D'après le Corollaire 64, le monoïde est de type fini. L'affirmation découle alors des résultats sur les monoïdes de type fini, en particulier ceux établis dans [21, Théorème 3.1.4 et 4.4.11], et pour la dernière partie, voir [13, Théorème 3.6]. □

Il est également connu que plusieurs autres invariants arithmétiques de H sont finis, y compris le degré de chaînage $\mathrm{c}(H)$ et le degré de modération $\mathrm{t}(H)$, en particulier, le monoïde est localement modéré ; de plus, dans le résultat ci-dessus, l'ensemble des distances $\Delta(H)$ peut être remplacé par $\Delta^*(H)$; Rappelons que $\Delta^*(H)$ est définie comme l'ensemble des $\min\Delta(\mathrm{H}')$ où H' traverse les sous-monoïdes non demi-factoriels et clos par diviseur de H.

Ainsi, il est connu que l'élasticité est atteinte. Nous nous renvoyons aux références mentionnées dans la preuve juste au-dessus et à [27, 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 (d'ensemble de longueurs).

Dans le Chapitre 6, nous affinons le théorème de structure pour les unions pour cette classe de monoïdes en montrant que, pour une large classe de poids, les ensembles sont en effet des progressions arithmétiques, avec une raison 1, c'est-à-dire des intervalles d'entiers.

Nous concluons ce chapitre en présentant 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 par transfert. Cependant, ils sont toujours des C-monoïdes ; nous renvoyons à [21, Section 2.9] pour une définition. Pour le cas particulier des suites à somme nulle plus-moins pondérée, il est possible d'obtenir une classification complète lorsque le monoïde est Krull et krull par transfert. Cela est donné dans la Proposition 68, due à Geroldinger et Zhong, qui inclut l'idée principale du lemme qui la précède.

Lemme 67. *Soit* G *un groupe abélien tel que* $\exp(G) \geq 3$. *Soit* Ω *un ensemble de poids tel que* $\{+\mathrm{id}_G, -\mathrm{id}_G\} \subseteq \Omega \subseteq \mathrm{Aut}(G)$. *Alors* $\mathcal{B}_\Omega(G)$ *n'est pas un monoïde de Krull par transfert.*

Démonstration. Supposons par l'absurde qu'il existe un homomorphisme de transfert $\theta\colon \mathcal{B}_\Omega(G) \to \mathcal{B}(G_0)$, où G_0 est un sous-ensemble de n'importe quel groupe abélien. Soit $g \in G$ tel que $\mathrm{ord}(g) \geq 3$. Nous posons

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

Montrons qu'ils 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 $\{+\mathrm{id}_G, -\mathrm{id}_G\} \subseteq \Omega$ donc $g+(-g), 2g+(-2g)$ et $g+g+(-2g)$ sont des sommes pondérées de A_1, A_2, A_3 respectivement. Nous prouvons maintenant que A_1, A_2, A_3 sont irréductibles. Pour cela, il suffit de noter qu'une décomposition de A_i est impossible puisque l'un des deux facteurs est de longueur 1 donc les sommes possibles sont $\omega(g)$ ou $\omega(2g)$ pour $\omega \in \Omega$ mais aucun de ces éléments n'est nul.

Puisque $A_3^2 = A_1^2A_2$, nous avons $\theta(A_3^2) = \theta(A_1^2A_2)$ et il en découle 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 $\mathcal{F}(G_0)$. Ce qui implique que $\theta(A_1)$ divise $\theta(A_3)$ dans $\mathcal{B}(G_0)$, et donc $\theta(A_1) = \theta(A_3)$ (car ces deux éléments sont des atomes). Ainsi, nous obtenons $\theta(A_2) = 1$, ce qui est une contradiction avec la première condition de la définition d'un homomorphisme de transfert, voir la Définition 56. □

Proposition 68. *Soit G un groupe abélien et $\mathcal{B}_\pm(G)$ le monoïde des suites à somme nulle $\pm$-pondérée. Alors les affirmations suivantes sont équivalentes :*

(a) G est un 2-groupe élémentaire.

(b) $\mathcal{B}_\pm(G)$ est un monoïde de Krull.

(c) $\mathcal{B}_\pm(G)$ est un monoïde de Krull par transfert.

Démonstration. (a) ⇒ (b) Si G est un 2-groupe élémentaire, alors $\mathcal{B}_\pm(G) = \mathcal{B}(G)$, car $-g = g$ pour chaque $g \in G$, et $\mathcal{B}(G)$ est un monoïde de Krull.

(b) ⇒ (c) Évident.

(c) ⇒ (a) Étant donné que les conditions sur l'ensemble des poids dans le Lemme 67 sont vérifiées, $\mathcal{B}_\pm(G)$ ne peut être un monoïde de Krull par transfert que lorsque G ne contient aucun élément d'ordre au moins égal à 3, c'est-à-dire lorsque G est un 2-groupe élémentaire car l'ordre de chaque élément est 2 (sauf pour 0 qui est d'ordre 1) et l'exposant de groupe est alors 2, c'est-à-dire le groupe G est un 2-groupe élémentaire. □

En d'autres termes, 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 allons maintenant montrer que pour un groupe abélien fini G et Ω un ensemble de poids, le monoïde $\mathcal{B}_\Omega(G)$ est un C-monoïde. Nous rappelons la

définition de C-monoïde mais uniquement pour le cas d'un monoïde réduit ; on dit qu'un monoïde réduit H est un C-monoïde s'il est un sous-monoïde d'un monoïde libre F tel que le semi-groupe de classes $\mathcal{C}(H, F)$ est fini. Rappelons qu'on dit que deux éléments $y, y' \in F$ sont H-équivalents si $y^{-1}H \cap F = y'^{-1}H \cap F$ et que le semi-groupe de classes est formé par les classes d'équivalences des éléments de F par rapport à cette relation (il s'agit en effet d'une relation d'équivalence et même de congruence et pour cela $\mathcal{C}(H, F)$ est bien un semi-groupe par rapport à la loi de composition héritée).

Nous n'utilisons pas directement la définition pour montrer que nos monoïdes sont des C-monoïdes, par contre, nous utilisons un résultat de Cziszter, Domokos et Geroldinger [11, Proposition 2.6.3] dans un cas particulier que nous rappelons ci-dessous.

Proposition 69. *Soit H un monoïde réduit et de type fini. 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 chaque $p \in P$, 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 70. *Soit G un groupe abélien fini et $G_0 \subseteq G$. Soit $\Omega \subseteq \mathrm{End}(G)$ un ensemble de poids. Le monoïde $\mathcal{B}_\Omega(G_0)$ est un C-monoïde, défini dans $\mathcal{F}(G_0)$.*

Démonstration. D'après la Proposition 69, il suffit de montrer que pour $S \in \mathcal{F}(G_0)$, il existe un $n \in \mathbb{N}$ tel que $S^n \in \mathcal{B}_\Omega(G_0)$. Soit $n \in \mathbb{N}$ et $\omega \in \Omega$. Notons que $n \cdot \omega(\sigma(S)) \in \sigma_\Omega(S^n)$. Pour $n = \exp(G)$, on trouve alors $0 \in \sigma_\Omega(S^n)$ puisque $\omega(\sigma(S)) \in G$ et $\exp(G) \cdot h = 0$, pour tout $h \in G$. □

Chapitre

5 Quelques résultats auxiliaires généraux

Nous présentons, dans ce chapitre, quelques résultats qui sont utiles pour nos investigations, bien qu'ils ne soient pas spécifiquement liés aux monoïdes de suites à somme nulle (pondérée). Ces résultats portent principalement sur les ensembles $\mathcal{U}_k(H)$ et les notions associées. Pour plus de détails, nous renvoyons au [17, Lemme 5.2].

Lemme 71. *Soit H un monoïde atomique avec $k, l \in \mathbb{N}_0$. Alors les propositions suivantes sont vraies.*

1. $\mathcal{U}_k(H) = \{k\}$ *pour* $k \in \{0, 1\}$ *et* $k \in \mathcal{U}_k(H)$ *pour chaque* $k \in \mathbb{N}$.
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. $\lambda_{k+l}(H) \le \lambda_k(H) + \lambda_l(H) \le k + l \le \rho_k(H) + \rho_l(H) \le \rho_{k+l}(H)$.
5. $\rho_k(H) \le k\rho(H)$ *et* $k \le \lambda_k(H)\rho(H)$.

Nous présentons quelques observations générales supplémentaires sur ces invariants.

Lemme 72. *Soit H un monoïde atomique. Soit $k \in \mathbb{N}$.*

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

Démonstration.

1. Étant donné que par définition $\lambda_k(H) \in \mathcal{U}_k(H)$, il en résulte d'après le Lemme 71 que $k \in \mathcal{U}_{\lambda_k(H)}(H)$. Et d'après le Lemme 44 on a $\rho_{\lambda_k(H)}(H) = \sup \mathcal{U}_{\lambda_k(H)}(H)$, il est donc évident que $\rho_{\lambda_k(H)}(H) \ge k$.
2. Puisque $\rho_k(H)$ est fini, nous avons $\rho_k(H) \in \mathcal{U}_k(H)$, et de nouveau d'après le Lemme 71, $k \in \mathcal{U}_{\rho_k(H)}(H)$ et donc $\lambda_{\rho_k(H)}(H) \le k$.

□

Lemme 73. *Soit H un monoïde atomique. Soit $k \in \mathbb{N}$. Supposons que $\mathcal{U}_i(H)$ soit un intervalle pour chaque $i \le k$. Alors, nous avons $\lambda_k(H) = \min\{i \colon \rho_i(H) \ge k\}$.*

Démonstration. Soit $j \in \mathbb{N}$ minimal tel que $\rho_j(H) \geq k$; notons que, puisque $\rho_k(H) \geq k$ d'après le Lemme 72 un tel j existe et $j \leq k$. Étant donné que $j \leq k \leq \rho_j(H)$ et que $\mathcal{U}_j(H)$ est un intervalle, il en découle que $k \in \mathcal{U}_j(H)$. Ainsi, d'après le Lemme 71, nous avons $j \in \mathcal{U}_k(H)$ et donc $\lambda_k(H) \leq j$. Et d'après le Lemme 72, nous avons $\rho_{\lambda_k(H)}(H) \geq k$, il en résulte que $\min\{i \colon \rho_i(H) \geq k\} \leq \lambda_k(H)$. □

Lemme 74. *Soit H un monoïde atomique. Soit $k \in \mathbb{N}$. Supposons que $\mathcal{U}_i(H)$ soit un intervalle pour chaque $i \leq k$. Alors, nous avons $\rho_k(H) = \sup\{i \colon \lambda_i(H) \leq k\}$.*

Démonstration. Soit $j \in \mathbb{N}$ tel que $j \geq k$ et $\lambda_j(H) \leq k$; notons que, puisque $\lambda_k(H) \leq k$, un tel j existe.

Puisque $\lambda_j(H) \leq k \leq j$ et que $\mathcal{U}_j(H)$ est un intervalle, il s'ensuit que $k \in \mathcal{U}_j(H)$. Ainsi, d'après le Lemme 71, nous avons $j \in \mathcal{U}_k(H)$, et donc $\rho_k(H) \geq j$. Ainsi, $\rho_k(H) \geq \sup\{i \colon \lambda_i(H) \leq k\}$.

Si $\sup\{i \colon \lambda_i(H) \leq k\}$ est infini, il en découle que $\rho_k(H) = \infty$. Admettons que $\sup\{i \colon \lambda_i(H) \leq k\}$ soit fini et que $j > \sup\{i \colon \lambda_i(H) \leq k\}$. Supposons que $\rho_k(H) \geq j$. Puisque $\mathcal{U}_k(H)$ est un intervalle, il s'ensuit que $j \in \mathcal{U}_k(H)$. Cependant, cela implique que $k \in \mathcal{U}_j(H)$ et donc $k \geq \lambda_j(H)$, ce qui est une contradiction avec $j > \sup\{i \colon \lambda_i(H) \leq k\}$. Ainsi, $\rho_k(H) < j$ et l'affirmation s'en suit. □

Nous donnons maintenant un lemme qui est une légère généralisation de [42, Lemme 5.1].

Lemme 75. *Soit P un ensemble et soient $S_1, \ldots, S_k, T_1, \ldots, T_\ell \in \mathcal{F}(P)$ des suites non vides telles que*

$$S_1 \ldots S_k = T_1 \ldots T_\ell.$$

Si $k < \ell$, alors ils existent des indices $i_0 \in [1, k]$ et des indices distincts $j_1, j_2 \in [1, \ell]$ tels qu'ils existent $p_1, p_2 \in P$ satisfaisant $p_1 \mid T_{j_1}$, $p_2 \mid T_{j_2}$ et $p_1 p_2 \mid S_{i_0}$.

Démonstration. Nous supposons que $k < \ell$ et procédons par induction sur k. Fixons $k = 1$. Supposons que pour tout h, h' tel que $hh' \mid S_1$, il n'existe pas d'indices distincts $j, j' \in [1, \ell]$ tels que $h \mid T_j$ et $h' \mid T_{j'}$. Il en découle que $S_1 = S_k \mid T_j$ pour un certain $j \in [1, \ell]$, disons $S_k \mid T_\ell$. Nous obtenons ainsi :

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

une contradiction, car T_1 n'est pas vide. Supposons maintenant que $k \geq 2$ et admettons que l'affirmation est vraie pour $k - 1$, nous avons $S_1 \ldots S_k = T_1 \ldots T_\ell$; comme précédemment, nous obtenons $S_k \mid T_\ell$. Nous considérons maintenant $S_1 \ldots S_{k-1} = T_1 \ldots T_{\ell-1}(T_\ell S_k^{-1})$. Par conséquent, la conclusion découle directement de l'hypothèse d'induction appliquée à $S_1 \ldots S_{k-1} = T_1 \ldots T_{\ell-1}(T_\ell S_k^{-1})$. □

Dans le lemme ci-dessous, qui est essentiellement tiré de [3], voir en particulier le Théorème 2.1 et [21, Proposition 1.4.2], nous adoptons la convention selon laquelle $a/0 = \infty$ pour $a \in \mathbb{R}_{\geq 0} \cup \{\infty\}$. Soulignons que la condition selon laquelle H n'est pas factoriel garantit que $\mathcal{A}(H) \setminus \mathcal{P}(H) \neq \emptyset$.

Bien évidemment, pour un monoïde factoriel H, on a $\rho(H) = 1$, et ainsi rien n'est perdu en excluant ce cas.

Lemme 76. *Soit H un monoïde atomique qui n'est pas factoriel. Soit $r : H \to (\mathbb{R}_{\geq 0}, +)$ un homomorphisme de monoïdes.*

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

Démonstration. Puisque r est un homomorphisme de monoïde, il s'ensuit que $r(u) = 0$ pour tout $u \in H^\times$. 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 $l/k \leq R_1/r_1$. Comme cela est trivial pour $r_1 = 0$, nous supposons que $r_1 > 0$. Nous notons que

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

   et ainsi le résultat en découle.

2. Soit $a_1, \ldots, a_k, b_1, \ldots, b_l \in \mathcal{A}(H)$ tels que $a_1 \ldots a_k = b_1 \ldots b_l$. Nous devons montrer que $l/k \leq R_2/r_2$. Comme précédemment, nous pouvons supposer que $r_2 > 0$. De plus, supposons que $l \geq k$.

   Supposons d'abord qu'aucun des éléments $a_1, \ldots, a_k, b_1, \ldots, b_l$ n'est premier. Dans ce cas, nous pouvons conclure que :

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

   Ainsi, le résultat suit.

   Supposons que ce ne soit pas le cas, c'est-à-dire que, en renumérotant si nécessaire, les éléments $a_{(k-r)+1}, \ldots, a_k$ sont premiers tandis que $a_1, \ldots, a_{k-r}$ ne le sont pas. Il s'ensuit, en renumérotant si nécessaire, que $a_{k-r+i} = b_{l-r+i}$ pour tout $1 \leq i \leq r$ et que $a_1 \ldots a_{k-r} = b_1 \ldots b_{l-r}$. Nous remarquons que si l'un des b_j pour $j \in [1, l-r]$ est premier, l'un des a_i pour $i \in [1, l-r]$ le serait aussi. Ainsi, aucun des $a_1, \ldots a_{k-r}, b_1, \ldots, b_{l-r}$ n'est premier. Si $k - r = 0$, alors $k = l$ et la

borne est évidemment vérifiée. Supposons que $k - r \neq 0$. Nous obtenons comme précédemment

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

et donc

$$\frac{l - r}{k - r} \leq \frac{R_2}{r_2}.$$

Maintenant, notons que pour $l' \geq k' > r' \geq 0$, on a $\frac{l'}{k'} \leq \frac{l'-r'}{k'-r'}$. Ainsi,

$$\frac{l}{k} \leq \frac{l - r}{k - r} \leq \frac{R_2}{r_2}.$$

Cela termine la preuve.

□

Dans cette thèse, nous appliquons ce résultat pour des monoïdes de suites à somme nulle (pondérée). Toutefois, notons que si $H = \langle n_1, \ldots, n_l \rangle$ un semi-groupe numérique alors le résultat avec la fonction de longueur donnée par l'inclusion donne $\rho(H) \leq \frac{n_l}{n_1}$ ce qui est par ailleurs la valeur exacte dans ce cas.

Chapitre

6 Résultats sur $\mathcal{U}_k(H)$ pour les monoïdes de suites à somme nulle pondérées

Le présent chapitre a pour but d'obtenir divers résultats sur $\mathcal{U}_k(H)$ pour les monoïdes de suites à somme nulle pondérées qui vont au-delà de ce qui a déjà été établi dans le Théorème 66. Tout d'abord, nous établissons que sous certaines hypothèses sur les poids, ces ensembles sont des intervalles, c'est-à-dire des progressions arithmétiques de raison 1. Nous étudions ensuite les maximums et les minimums de ces ensembles, c'est-à-dire $\rho_k(H)$ et $\lambda_k(H)$, ce qui, combiné, permet d'obtenir une description complète de ces ensembles.

Pour la démonstration de nos résultats, nous utilisons les résultats de [15, Section 3] qui sont valables pour $\mathcal{B}_\Omega(G)$; nous les résumons dans le lemme suivant.

Lemme 77. *Soit H un monoïde atomique. Supposons que $\Delta(H) \neq \emptyset$ et que $d = \min \Delta(H)$. Alors, on a :*

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

Ensuite, nous montrons que les ensembles $\mathcal{U}_k(\mathcal{B}_\Omega(G))$ sont des intervalles si l'ensemble des poids $\Omega \subseteq \mathrm{End}(G)$ est un groupe par rapport à la composition des endomorphismes. Nous soulignons que l'élément neutre de Ω n'est pas nécessairement id_G, ce qui introduit quelques complications supplémentaires dans l'argument. En effet, dans certains autres résultats, nous supposons en plus que $\mathrm{id}_G \in \Omega$, autrement dit, nous supposons que Ω est un sous-groupe de $\mathrm{Aut}(G)$.

Théorème 78. *Soit G un groupe abélien fini. Soit $\Omega \subseteq \mathrm{End}(G)$. Si Ω est un groupe par rapport à la composition des endomorphismes, alors $\mathcal{U}_k(\mathcal{B}_\Omega(G))$ est un intervalle pour tout $k \in \mathbb{N}$.*

Démonstration. D'après le Lemme 77, il suffit de montrer que $\mathcal{U}_k(\mathcal{B}_\Omega(G)) \cap \mathbb{N}_{\geq k}$ est un intervalle pour tout $k \in \mathbb{N}$. Cela signifie que nous devons montrer que $[k, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$.

Soit $\ell \in [k, \rho_k(\mathcal{B}_\Omega(G))]$ minimal tel que $[\ell, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Cela est bien défini car, bien évidemment, pour $\ell = \rho_k(\mathcal{B}_\Omega(G))$, nous avons $[\ell, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$.

Nous voulons montrer que $\ell = k$. Supposons, par l'absurde, que $\ell > k$. Nous considérons l'ensemble de tous les $B \in \mathcal{B}_\Omega(G)$ tels que $\{k, j\} \subseteq \mathsf{L}(B)$ pour certain $j \geq \ell$. Soit B_0 un tel élément tel que $|B_0|$ est minimal parmi tous ces éléments. Maintenant, soit $B_0 = U_1 \dots U_k = V_1 \dots V_j$.

D'après le Lemme 75, après une renumérotation, nous pouvons supposer qu'il existe

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

Soit $\omega_i \in \Omega$ tel que $\Sigma_{i=1}^{|U_1|} \omega_i g_i = 0$. Soit $g_0 = \omega_1 g_1 + \omega_2 g_2$. Posons $U_1' = g_0 (g_1 g_2)^{-1} U_1$ 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 Ω est un groupe, il s'ensuit que $\omega(-g_0) \in \sigma_\Omega((g_1 g_2)^{-1} U_1)$ pour un certain (en fait, pour chaque) $\omega \in \Omega$.

Par conséquent, nous avons $0 \in \sigma_\Omega(U_1')$. Nous affirmons que $0 \in \sigma_\Omega(V_{j-1}')$ est aussi vérifié. Pour voir cela, notons que $0 \in \sigma_\Omega(V_{j-1})$ implique que $-\omega_1' g_1 \in \sigma_\Omega(g_1^{-1} V_{j-1})$ pour un certain $\omega_1' \in \Omega$. Et comme Ω 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 manière, nous obtenons $-\omega_2 g_2 \in \sigma_\Omega(g_2^{-1} V_j)$. Ainsi, $-g_0 = -(\omega_1 g_1 + \omega_2 g_2) \in \sigma_\Omega(V_{j-1} V_j (g_1 g_2)^{-1})$ et puisque Ω est un groupe, on a $\omega(-g_0) \in \sigma_\Omega(V_{j-1} V_j (g_1 g_2)^{-1})$ pour certains (en fait, pour chaque) $\omega \in \Omega$. Par conséquent, $0 \in \sigma_\Omega(V_{j-1}')$.

Ainsi, $U_1', V_{j-1}' \in \mathcal{B}_\Omega(G)$. En effet, U_1' appartient à $\mathcal{A}(\mathcal{B}_\Omega(G))$, car une factorisation de U_1' entraînerait directement une factorisation de U_1. Toutefois, pour V_{j-1}' ce n'est pas encore 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 évident que $B_0' \in \mathcal{B}_\Omega(G)$ et $|B_0'| < |B_0|$.

Étant donné que U_1' est un atome, il en découle que $k \in \mathsf{L}(B_0')$. D'après notre hypothèse sur B_0, il s'ensuit que $\mathsf{L}(B_0')$ ne contient aucun élément supérieur ou égal à l, autrement dit $\max \mathsf{L}(B_0') < \ell$.

Comme $B_0' = V_1 \dots V_{j-2} V_{j-1}'$, il en découle que $j - 2 + \mathsf{L}_{\mathcal{B}_\Omega(G)}(V_{j-1}') \subseteq \mathsf{L}_{\mathcal{B}_\Omega(G)}(B_0')$. Puisque $\max \mathsf{L}(B_0') < \ell$, il en résulte que $j - 2 + \max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V_{j-1}') < \ell$.

Étant donné que V'_{j-1} est une suite non vide, on a $\max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) \geq 1$. Finalement, $j \geq \ell$, ce qui entraîne la relation d'inégalités suivante : $\ell-2+1 \leq j-2+\max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) < \ell$. Cela implique que, $j-2+\max \mathsf{L}_{\mathcal{B}_\Omega(G)}(V'_{j-1}) = \ell-1$, et donc $\ell-1 \in \mathsf{L}(B'_0)$. Puisque $k \in \mathsf{L}(B'_0)$, il s'ensuit que $\ell-1 \in \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Par conséquent, $[\ell-1, \rho_k(\mathcal{B}_\Omega(G))] \subseteq \mathcal{U}_k(\mathcal{B}_\Omega(G))$. Ce qui contredit la définition de ℓ. □

Nous allons maintenant établir un résultat qui sera utile pour l'étude des elasticités et des problèmes connexes.

Lemme 79. *Soit G un groupe abélien fini. Soit $\Omega \subseteq \mathrm{End}(G)$ et soit $j \in [2, \mathsf{D}(\mathcal{B}_\Omega(G))]$.*

1. *Si Ω est un semi-groupe par rapport à la composition, alors il existe un élément $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ tel que $|A| = j$.*
2. *Si $\Omega \subseteq \mathrm{Aut}(G)$ est un sous-groupe, alors il existe un élément $B \in \mathcal{B}_\Omega(G)$ 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, $A \in \mathcal{B}_\Omega(G)$, car pour $\omega \in \Omega$, on a $\omega(\sum_{i=1}^{l} \omega_i(g_i)) = 0$ et donc $\omega(s) + \sum_{i=l-j+2}^{l} (\omega \circ \omega_i)(g_i) = 0$.

De plus, il en découle que $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$. Étant donné qu'une factorisation non triviale de A entraînerait directement une factorisation non triviale de C. Notons qu'il nous faut à nouveau que Ω soit un semi-groupe. Puisque $|A| = j$, cela prouve la première assertion.

2. Soit $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ avec $|A| = j$. Notons que $0 \nmid A$. Il est facile de voir que $-A \in \mathcal{A}(\mathcal{B}_\Omega(G))$. Nous considérons $B = (-A)A$. Par définition $2 \in \mathsf{L}(B)$. Pour tout $g \in G$, on a $(-g)g \in \mathcal{B}_\Omega(G)$; notons que puisque $\omega \in \Omega$ est un endomorphisme de G, on a toujours $\omega(-g) = -\omega(g)$. Et comme Ω ne contient que des monomorphismes, il s'ensuit que $(-g)g \in \mathcal{A}(\mathcal{B}_\Omega(G))$. Ainsi $\max \mathsf{L}(B) = |A|$, et l'assertion est prouvée.

□

Lemme 80. *Soit G un groupe abélien fini. Soit $\Omega \subseteq \mathrm{End}(G)$. Soit $k \in \mathbb{N}$, alors $\rho_{2k}(\mathcal{B}_\Omega(G)) \geq k\,\mathsf{D}(\mathcal{B}_\Omega(G))$ et $\rho_{2k+1}(\mathcal{B}_\Omega(G)) \geq 1 + k\,\mathsf{D}(\mathcal{B}_\Omega(G))$.*

Démonstration. Soit $A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ avec une longueur maximale. Nous savons que $-A \in \mathcal{A}(\mathcal{B}_\Omega(G))$ et considérons $B = (-A)^k A^k$. Par définition, $2k \in \mathsf{L}(B)$. Puisque, pour chaque $g \in G$, on a $(-g)g \in \mathcal{B}_\Omega(G)$ (notons que, puisque $\omega \in \Omega$ est un endomorphisme de G, on a toujours $\omega(-g) = -\omega(g)$). Il s'ensuit que $\max \mathsf{L}(B) \geq k|A|$ et l'affirmation est établie. La deuxième affirmation est une conséquence immédiate de la première, par exemple, nous pouvons considérer $0B$, c'est-à-dire, on rajoute un terme 0 à la suite B. □

Nous utilisons maintenant le Lemme 76 pour établir que $\rho_{2k}(\mathcal{B}_\Omega(G)) = k\,\mathsf{D}(\mathcal{B}_\Omega(G))$ dans différents cas. À cette fin, il est utile d'avoir un minorant pour 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 d'au moins 2, ce qui nous permet d'établir l'égalité mentionnée ci-dessus.

Exemple 81. Soit $G = C_2 \oplus C_6$ et soit $e_1, e_2 \in G$ sont indépendants avec $\mathrm{ord}(e_1) = 2$ et $\mathrm{ord}(e_2) = 6$. Soit $\Omega = \{+2\,\mathrm{id}_G, +\mathrm{id}_G, -\mathrm{id}_G\}$. Alors $e_1 \in \mathcal{A}(\mathcal{B}_\Omega(G))$ car $2\,\mathrm{id}_G(e_1) = 0$. Cependant, $e_1 \notin \mathcal{P}(\mathcal{B}_\Omega(G))$ car $e_1 \nmid e_1(e_1+e_2)e_2$ tandis que $e_1 \mid (e_1(e_1+e_2)e_2)^2$.

Cependant, sous certaines conditions sur l'ensemble des poids, cela reste vrai.

Lemme 82. *Soit G un groupe abélien fini. Soit $\Omega \subseteq \mathrm{End}(G)$. Soit $A \in \mathcal{A}(\mathcal{B}_\Omega(G)) \setminus \mathcal{P}(\mathcal{B}_\Omega(G))$.*

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

Démonstration. Supposons que Ω ne contienne que des monomorphismes. Il en découle directement que les seuls éléments de $\mathcal{B}_\Omega(G)$ de 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 $\mathcal{P}(\mathcal{B}_\Omega(G))$, ce qui donne la première proposition.

Supposons maintenant que Ω est stable par composition. Supposons qu'il existe un atome de longueur 1, soit, pour $a \in G$, nous avons $a \in \mathcal{B}_\Omega(G)$. Cela signifie qu'il existe un certain $\omega' \in \Omega$ tel que $\omega'(a) = 0$.

Nous devons montrer que $a \in \mathcal{P}(\mathcal{B}_\Omega(G))$. Soient $C, D \in \mathcal{B}_\Omega(G)$ tels que $a \mid CD$ (la divisibilité est valable dans $\mathcal{B}_\Omega(G)$). Nous devons démontrer que $a \mid C$ ou $a \mid D$ (dans $\mathcal{B}_\Omega(G)$). Sans perte de généralité, supposons que C contienne a, autrement dit, 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 $\omega_0, \omega_1, \dots, \omega_r$ tels que $\omega_0(a) + \omega_1(f_1) + \dots + \omega_r(f_r) = 0$. Nous appliquons ω' à cette expression et obtenons, $(\omega'\omega_0)(a) + (\omega'\omega_1)(f_1) + \dots + (\omega'\omega_r)(f_r) = 0$.

Maintenant, $(\omega'\omega_0)(a) = (\omega_0\omega')(a) = \omega_0(0) = 0$. Ainsi, nous avons : $(\omega'\omega_1)(f_1) + \dots + (\omega'\omega_r)(f_r) = 0$, et comme $\omega'\omega_i \in \Omega$ pour chaque $i \in [1, r]$, il s'ensuit que $f_1 \dots f_r \in \mathcal{B}_\Omega(G)$, ce qui établit la proposition. □

Les résultats établis jusqu'à présent permettent de déterminer pour divers ensembles de poids Ω les constantes $\rho_k(\mathcal{B}_\Omega(G))$ pour k pair. Le cas de k impair est plus complexe, et nous l'abordons pour le cas particulier des poids plus-moins dans le chapitre suivant.

Théorème 83. *Soit G un groupe abélien fini. Soit $\Omega \subseteq \mathrm{End}(G)$. Si Ω ne contient que des monomorphismes ou si Ω est un semi-groupe commutatif par rapport à la composition, alors on a $\rho_{2k}(\mathcal{B}_\Omega(G)) = k\,\mathsf{D}(\mathcal{B}_\Omega(G))$ pour chaque $k \in \mathbb{N}$. De plus, $\rho(\mathcal{B}_\Omega(G)) = \mathsf{D}(\mathcal{B}_\Omega(G))/2$. et*

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

Démonstration. Rappelons d'abord que par le Lemme 71, on a $\rho_k(H) \le k\rho(H)$.

Les minorants pour $\rho_k(H)$ sont établis dans le Lemme 80. Avec l'inégalité rappelée en haut, ils donnent une minoration pour $\rho(H)$.

Le Lemme 76 donne une majoration pour $\rho(H)$. Notons que $r_1 = 2$ par le Lemme 82. Les majorants pour $\rho_k(H)$ découlent de la majoration de $\rho(H)$ et de l'inégalité $\rho_k(H) \le k\rho(H)$. □

Nous présentons maintenant un résultat connu pour les monoïdes de suites à somme nulle sans poids, voir [17, Corollaire 5.4]. La structure de notre démonstration est très similaire à celle de la version sans poids.

Théorème 84. *Soit G un groupe abélien fini. Soit $\Omega \subseteq \mathrm{Aut}(G)$ un sous-groupe. Soit D la constante de Davenport de $\mathcal{B}_\Omega(G)$ et supposons que $\mathsf{D} \ge 2$. Alors, pour $k \in \mathbb{N}_0$, en posant $l \in \mathbb{N}_0$ et $j \in [0, \mathsf{D}-1]$ tels 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. Ainsi, $\mathcal{U}_k(\mathcal{B}_\Omega(G)) = \{k\}$ pour chaque k, et l'affirmation est triviale ; notons que, par hypothèse $\mathsf{D} \ge 2$ (et non 1 donc $|G| \ne 1$). Supposons donc que $|G| \ge 3$.

Soit $k \in \mathbb{N}_0$ et $k = l\,\mathsf{D} + j$ avec $l \in \mathbb{N}_0$, $j \in [0, \mathsf{D}-1]$. Autrement dit, l est le quotient et j est le reste de la division euclidienne de k par D. Notamment, l et j sont déterminés d'une manière unique par k (et vice versa).

Nous traiterons d'abord le cas $l = 0$, puis pour $l \ge 1$, nous distinguerons les cas $j = 0$ puis $j \ge 1$ (en traitant d'abord le cas $j = 1$).

Passons maintenant à l'étude détaillée :

Si $l = 0$, alors pour $j \in [0, 1]$, nous avons $\mathcal{U}_j(\mathcal{B}_\Omega(G)) = \{j\}$ et l'affirmation est établie. Pour $j \in [2, \mathsf{D}-1]$, nous savons, d'après le Lemme 79, qu'il existe un ensemble de longueurs qui contient $\{2, j\}$. Cela montre que $\lambda_j(\mathcal{B}_\Omega(G)) \le 2$. Puisque, pour $j \ge 2$, nous avons que $\lambda_j(\mathcal{B}_\Omega(G)) \ge 2$, l'affirmation est établie.

Nous pouvons donc supposer que $l \geq 1$. Si $j = 0$, l'affirmation est une conséquence du Théorème 83. Pour le voir, notons que, puisque $\rho_{2l}(\mathcal{B}_\Omega(G)) = l\,\mathsf{D}(\mathcal{B}_\Omega(G))$, il existe un ensemble de longueurs L avec $\{2l, l\,\mathsf{D}\} \subseteq \mathsf{L}$. Cela montre que $\lambda_{l\,\mathsf{D}}(\mathcal{B}_\Omega(G)) \leq 2l$. De plus, il ne peut pas exister un L' tel que $\{l', l\,\mathsf{D}\} \subseteq \mathsf{L}'$ pour un $l' < 2l$, car $l\,\mathsf{D}\,/l'$ serait supérieur à l'élasticité $D/2$ du monoïde $\mathcal{B}_\Omega(G)$. Par conséquent, $\lambda_{l\,\mathsf{D}}(\mathcal{B}_\Omega(G)) = 2l$.

Supposons que $j \geq 1$. Comme $k \leq \lambda_k(\mathcal{B}_\Omega(G))\rho(\mathcal{B}_\Omega(G))$ d'après le Lemme 71, il en résulte que pour $k = l\mathsf{D} + j$, on a :

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

en particulier $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) > 2l$, et donc $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) \geq 2l+1$. Dans l'autre sens, d'après le Lemme 71, nous avons que

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

où nous avons utilisé que $\lambda_{l\mathsf{D}}(\mathcal{B}_\Omega(G)) = 2l$ et que $\lambda_j(\mathcal{B}_\Omega(G)) \leq 2$, comme cela a déjà été établi. Pour $j = 1$, nous obtenons que $2l < \lambda_{l\mathsf{D}+1}(\mathcal{B}_\Omega(G)) \leq 2l + \lambda_1(\mathcal{B}_\Omega(G)) = 2l + 1$, et donc $\lambda_{l\mathsf{D}+1}(\mathcal{B}_\Omega(G)) = 2l + 1$.

Supposons que $j \geq 2$. Si $j \in [2, \rho_{2l+1}(\mathcal{B}_\Omega(G)) - l\,\mathsf{D}]$, alors $j + l\,\mathsf{D} \leq \rho_{2l+1}(\mathcal{B}_\Omega(G))$. Comme $\mathcal{U}_{2l+1}(\mathcal{B}_\Omega(G))$ est un intervalle d'après le Théorème 78, cela implique que $j + l\,\mathsf{D} \in \mathcal{U}_{2l+1}(\mathcal{B}_\Omega(G))$ et donc $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) \leq 2l + 1$, 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 $j + l\,\mathsf{D} > \rho_{2l+1}(\mathcal{B}_\Omega(G))$. Cela 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 $\lambda_{l\mathsf{D}+j}(\mathcal{B}_\Omega(G)) = 2l+2$. □

Chapitre

7 Résultats sur les suites ±-pondérées

Ce chapitre vise à obtenir d'autres résultats sur $\mathcal{B}_\Omega(G)$ pour le cas particulier où l'ensemble des poids est égal à $\{+\mathrm{id}_G, -\mathrm{id}_G\}$, que nous appelons suites à somme nulle plus-moins pondérées ; et nous désignons cet ensemble de poids par l'indice $\pm$, c'est-à-dire que $\mathcal{B}_\pm(G)$ désigne $\mathcal{B}_{\{+\mathrm{id}_G, -\mathrm{id}_G\}}(G)$. Et puisque $\{+\mathrm{id}_G, -\mathrm{id}_G\}$ est un sous-groupe commutatif de $\mathrm{Aut}(G)$, les résultats du chapitre précédent sont applicables, et nous savons que pour G un groupe abélien fini :

— $\mathcal{U}_k(\mathcal{B}_\pm(G))$ est un intervalle pour chaque $k \in \mathbb{N}$, voir le Théorème 78.

— $\rho_{2k}(\mathcal{B}_\pm(G)) = k\,\mathsf{D}(\mathcal{B}_\pm(G))$ pour chaque $k \in \mathbb{N}$, voir le Théorème 83.

Nous allons étudier d'une part la valeur exacte de $\mathsf{D}(\mathcal{B}_\pm(G))$, et d'autre part la valeur de $\rho_k(\mathcal{B}_\pm(G))$ pour k impair. Il se trouve 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 dans le Chapitre 4 que $\mathcal{A}(\mathcal{B}_\pm(G)) \cap \mathcal{B}(G) \subseteq \mathcal{A}(\mathcal{B}(G))$. Inversement, 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 le monoïde plus grand $\mathcal{B}_\pm(G)$. Par exemple, dans $C_4 = \langle e \rangle$, la suite e^4 est une suite à somme nulle minimale dans C_4. Autrement dit, $e^4 \in \mathcal{A}(\mathcal{B}(C_4))$. 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 est impossible.

Théorème 85. *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 en découle que $A \in \mathcal{B}_\pm(G)$. Supposons le contraire, c'est-à-dire que $A = A_1 \cdot A_2$ avec A_1 et A_2 non vides, tels que $0 \in \sigma_\pm(A_1)$ et $0 \in \sigma_\pm(A_2)$. Nous pouvons désormais décomposer A_1 et A_2 en fonction du choix des poids qui donnent une somme nulle ; cette décomposition pourrait ne pas être unique. Soit $A_1 = A_1^+ A_1^-$ tel que $0 = \sigma(A_1^+) - \sigma(A_1^-)$, et de même pour A_2. Ainsi, $\sigma(A_1^+) = \sigma(A_1^-)$ et $\sigma(A_2^+) = \sigma(A_2^-)$. On a $A = A_1^+ A_1^- A_2^+ A_2^-$. Nous introduisons quelques notations abrégées : $\sigma(A_1^-) = s_1^-$, $\sigma(A_1^+) = s_1^+$, $\sigma(A_2^-) = s_2^-$, et $\sigma(A_2^+) = s_2^+$. Nous avons remarqué que $s_1^+ = s_1^-$ et $s_2^+ = s_2^-$. Puisque $\sigma(A) = 0$, il s'ensuit que $s_1^+ + s_1^- + s_2^+ + s_2^- = 0$.

Par conséquent, nous avons $s_1^+ + s_1^+ + s_2^+ + s_2^+ = 0$, 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 obtenons $s_1^+ + s_2^+ = 0$. Ainsi, $A_1^+ A_2^+$ forme une sous-suite à somme nulle de A (sans poids). Comme A est une suite à somme nulle minimale, cela n'est possible que si $A_1^+ A_2^+$ est vide ou égale à A. Il en est de même pour $A_1^+ A_2^-$, $A_1^- A_2^+$ et $A_1^- A_2^-$.

À présent, exactement l'une 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 que $A_1^- A_2^-$ est vide. Cependant, A_1^+ et A_2^+ sont des suites à somme nulle sans poids et $A = A_1^+ A_2^+$, ce qui est contradictoire. □

En particulier, le résultat ci-dessus montre que si 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 $e^2 \in \mathcal{A}(\mathcal{B}_\pm(C_3))$, cependant $e^2 \notin \mathcal{B}(C_3)$.

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 86. *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 85 et du Lemme 61. □

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 $1 < n_1 \mid \cdots \mid n_r$ on a $\mathsf{D}(\mathcal{B}(G)) \geq 1 + \sum_{i=1}^r (n_i - 1)$ et l'égalité est établie si G a un rang au plus deux, c'est-à-dire $r \leq 2$, ou si G est un p-groupe, c'est-à-dire si n_r est une puissance d'un premier. L'égalité est également vraie dans certains autres cas, mais pas en général. Nous nous référons au chapitre 1 3 et à [16, 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, puis nous obtenons un minorant général. Pour ce faire, nous rappelons un résultat sur la structure des suites longues minimales à somme nulle et des concepts associés. Notre approche est la même que celle de [17, Section 7] ; les résultats sont, à l'origine, dus à Savchev et Chen [47] et Yuan [52].

Définition 87. Soit G un groupe abélien fini.

1. Une suite $S \in \mathcal{F}(G)$ est dite lisse, ou plus précisément g-lisse, s'il existe $g \in G$ tel que $S = (n_1 g) \ldots (n_\ell g)$, où $1 = n_1 \leq \cdots \leq n_\ell$, $n = n_1 + \cdots + n_\ell < \mathrm{ord}(g)$ et $\Sigma(S) = \{g, 2g, \ldots, ng\}$.

2. Une suite $S \in \mathcal{F}(G)$ est appelée une suite scindable à somme nulle minimale si $S \in \mathcal{A}(\mathcal{B}(G))$, et $S = (g_1 + g_2)T$ pour certains $g_1, g_2 \in G$ et $T \in \mathcal{F}(G)$ tels que $g_1 g_2 T \in \mathcal{A}(\mathcal{B}(G))$.

Théorème 88. *Soit G cyclique d'ordre $n \geq 3$.*

1. *Si $S \in \mathcal{F}(G)$ est sans somme nulle et que $|S| \geq (n+1)/2$, alors S est g-lisse pour certain $g \in G$ avec $\mathrm{ord}(g) = n$.*
2. *Soit $A \in \mathcal{A}(\mathcal{B}(G))$ de longueur $|A| \geq \lfloor n/2 \rfloor + 2$. Alors $A = (n_1 g) \ldots (n_\ell g)$ pour quelque $g \in G$ avec $\mathrm{ord}(g) = n$, $1 = n_1 \leq \cdots \leq n_\ell$, $n_1 + \cdots + n_\ell = n$. De plus, si A n'est pas scindable, alors $A = g^n$.*

Lemme 89. *Soit $g \in G$ et $k, \ell, n_1, \ldots, n_\ell \in \mathbb{N}$ tels que $\ell \geq k/2$ et $n = n_1 + \cdots + n_\ell < k \leq \mathrm{ord}(g)$. Si $1 \leq n_1 \leq \cdots \leq n_\ell$ et $S = (n_1 g) \ldots (n_\ell g)$. Alors $\Sigma(S) = \{g, 2g, \ldots, ng\}$, et S est g-lisse.*

Nous établissons un minorant pour $\mathsf{D}(\mathcal{B}_\pm(C_n))$ pour n pair.

Lemme 90. *Soit $n \geq 2$ pair. Alors*

$$\mathsf{D}(\mathcal{B}_\pm(C_n)) \geq 1 + \frac{n}{2}.$$

Démonstration. Soit $n = 2m$. Soit $C_n = \langle e \rangle$. Pour $n = 2$, nous notons 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 $n \geq 4$. Nous montrons que $A = e^m(me)$ est un élément de $\mathcal{A}(\mathcal{B}_\pm(C_n))$.

Supposons que $A = A_1 A_2$ avec $0 \in \sigma_\pm(A_i)$ pour $i \in \{1, 2\}$. Sans perte de généralité, nous pouvons supposer que $me \mid A_1$. Soit $A_1 = (me)e^k$ avec $k \in [0, m]$.

Étant donné que $0 \in \sigma_\pm(A_i)$, il s'ensuit qu'il existe $\epsilon_1, \ldots, \epsilon_k \in \{+\,\mathrm{id}_G, -\,\mathrm{id}_G\}$ tels que $me + \sum_{i=1}^k \epsilon_i e = 0$ (nous pouvons supposer que le poids de me est $+\,\mathrm{id}_G$). Cependant, cela signifie que $\sum_{i=1}^k \epsilon_i e = me$. Or, $\sum_{i=1}^k \epsilon_i e$ est égal à de où d est la différence entre le nombre de poids $+\,\mathrm{id}_G$ et $-\,\mathrm{id}_G$, nous obtenons que $|d|$ est au plus égal à k. Ainsi, $de = me$ n'est possible que si $k = m$. Par conséquent, $A_1 = A$ et A est bien dans $\mathcal{A}(\mathcal{B}_\pm(C_n))$. □

Théorème 91. *Soit n pair. Alors, on a*

$$\mathsf{D}(B_\pm(C_n)) = 1 + \frac{n}{2}.$$

Démonstration. L'affirmation est facilement établie pour $n = 2$; supposons maintenant que $n \geq 4$. D'après le Lemme 90, nous savons que $\mathsf{D}(\mathcal{B}_\pm(C_n)) \geq 1 + n/2$. Il reste à montrer que $\mathsf{D}(\mathcal{B}_\pm(C_n)) \leq 1 + n/2$. Soit $S = g_1 \cdots g_\ell \in \mathcal{A}(\mathcal{B}_\pm(C_n))$ et supposons, le contraire, que $|S| \geq n/2 + 2$. Puisque $0 \in \sigma_\pm(S)$ il existe $\epsilon_i \in \{+\,\mathrm{id}_G, -\,\mathrm{id}_G\}$ tels que $(\epsilon_1 g_1) + \cdots + (\epsilon_\ell g_\ell) = 0$.

Par conséquent, $A = (\epsilon_1 g_1) \dots (\epsilon_\ell g_\ell) \in \mathcal{B}(C_n)$. En effet, cette suite à somme nulle A doit être minimale, car une décomposition de A dans $\mathcal{B}(C_n)$ impliquerait une décomposition de S dans $\mathcal{B}_\pm(C_n)$.

D'après le Théorème 88, il existe $e \in C_n$ tel que $C_n = \langle e \rangle$ et de plus, nous pouvons écrire $A = (a_1 e) \cdots (a_\ell e)$ avec $a_i \in [1, n]$ et $\sum_{i=1}^{\ell} a_i = n$. Nous supposons que $1 \le a_1 \le \cdots \le a_\ell$.

Nous montrons que $a_1 = a_2 = a_3 = a_4 = 1$. Supposons, le contraire, que $a_4 \ge 2$. Alors $\sum_{i=1}^{\ell} a_i \ge 3 + 2 \cdot (\ell - 3) \ge 3 + 2 \cdot (n/2 - 1) > n$, ce qui est une contradiction.

Ainsi, $A = e^4(a_5 e) \dots (a_\ell e)$. Nous considérons $T = e^{-2}A$. Nous écrivons maintenant, $T = (b_1 e)(b_2 e) \cdots (b_{\ell'} e)$, où $b_1 \le \cdots \le b_{\ell'}$, $\sum_{i=1}^{\ell'} b_i = n - 2$ et $b_1 = b_2 = 1$. Notons que $\ell' = \ell - 2$ et $\ell' \ge n/2$. Nous remarquons que le Lemme 89 peut être appliqué à T. Nous avons donc $\Sigma(T) = \{e, 2e, \dots, (\mathrm{ord}(e) - 2)e\}$. Soit $T_1 \mid T$ tel que $\sigma(T_1) = ((n-2)/2)e$. Posons $T = T_1 T_2$. D'où $\sigma(T_1) = \sigma(T_2)$.

Par conséquent, nous pouvons donc décomposer $A = e^2 \cdot T_1 T_2$, et $0 \in \sigma_\pm(e^2)$ et $0 \in \sigma_\pm(T_1 T_2)$. Cela montre que, $A \notin \mathcal{A}(\mathcal{B}_\pm(G))$. Sachant que $\{+\mathrm{id}_G, -\mathrm{id}_G\}$ est un groupe sous la composition des endomorphismes, nous pouvons en conclure que $S \notin \mathcal{A}(\mathcal{B}_\pm(G)$, ce qui est une contradiction. On en déduit donc que $\mathsf{D}(\mathcal{B}_\pm(C_n)) \le 1 + n/2$. □

Corollaire 92. *Soit $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ avec $1 < n_1 \mid \cdots \mid n_r$ et que $t \in [0, r]$ soit maximal tel que $2 \nmid n_t$. Alors*

$$\mathsf{D}(\mathcal{B}_\pm(G)) \ge 1 + \sum_{i=1}^{t}(n_i - 1) + \sum_{i=t+1}^{r} \frac{n_i}{2}.$$

Démonstration. D'après le Lemme 65, nous savons que

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

L'affirmation découle maintenant du fait que $\mathsf{D}(\mathcal{B}_\pm(C_{n_i}))$ est égal à n_i lorsque n_i est impair, voir le Corollaire 86, et égal à $1 + n_i/2$ lorsque n_i est pair, voir le Théorème 91. □

Avec n_i et r, t définis ci-dessus, nous notons $\mathsf{D}^*(\mathcal{B}_\pm(G)) = 1 + \sum_{i=1}^{t}(n_i - 1) + \sum_{i=t+1}^{r} n_i/2$. Il serait intéressant d'avoir d'autres résultats sur la question de l'égalité dans l'inégalité $\mathsf{D}(\mathcal{B}_\pm(G)) \ge \mathsf{D}^*(\mathcal{B}_\pm(G))$, par exemple pour les groupes de rang deux d'ordre pair ou pour les 2-groupes.

Enfin, nous soulignons que les résultats ci-dessus montrent que $\mathsf{D}(\mathcal{B}_\pm(G))$ et $1 + \mathsf{d}(\mathcal{B}_\pm(G))$ sont assez différents. Nous rappelons que cette dernière est majorée par $1 + \lfloor \log_2 |G| \rfloor$. Nous nous référons à [1] et [38] pour d'autres résultats sur cette constante.

Nous concluons ce chapitre par quelques résultats sur les ensembles de longueurs et les élasticités dans le cas où G est un groupe d'ordre impair.

Proposition 93. *Soit G un groupe d'ordre impair. Pour chaque $B \in \mathcal{B}(G)$, nous avons $\mathsf{Z}_{\mathcal{B}(G)}(B) \subseteq \mathsf{Z}_{\mathcal{B}_\pm(G)}(B)$ 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 $z \in \mathsf{Z}_{\mathcal{B}(G)}(B)$. Cela signifie que $z = A_1 \dots A_k$ avec $A_i \in \mathcal{A}(G)$. Or, comme l'ordre de G est impair, d'après le Théorème 85, nous avons $\mathcal{A}(G) \subseteq \mathcal{A}(\mathcal{B}_\pm(G)$, et ainsi $A_i \in \mathcal{A}(\mathcal{B}_\pm(G))$ pour chaque $1 \le i \le k$. En d'autres termes, $z \in \mathsf{Z}_{\mathcal{B}_\pm(G)}(B)$. L'affirmation sur l'ensemble des longueurs est immédiate. □

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

Corollaire 94. *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 $\rho_k(\mathcal{B}(G)) \le \rho_k(\mathcal{B}_\pm(G))$, et $\lambda_k(\mathcal{B}(G)) \ge \lambda_k(\mathcal{B}_\pm(G))$.*

Démonstration. Cela découle immédiatement de la Proposition 93 et des définitions. □

Dans le Théorème 83, nous avons déjà déterminé $\rho_{2k}(\mathcal{B}_\pm(G))$ et remarqué que le problème pour les indices impairs est plus compliqué. Nous allons maintenant montrer comment nous pouvons utiliser les résultats obtenus pour le problème sans poids.

Proposition 95. *Soit G un groupe d'ordre impair. Soit $\mathsf{D} = \mathsf{D}(\mathcal{B}(G))$. Soit $k \in \mathbb{N}_0$.*

1. *On a $\rho_{2k}(\mathcal{B}_\pm(G)) = \rho_{2k}(\mathcal{B}(G)) = k\,\mathsf{D}$ et $\rho(\mathcal{B}_\pm(G)) = \rho(\mathcal{B}(G)) = \mathsf{D}/2$.*
2. *Si $\rho_{2k+1}(\mathcal{B}(G)) = k\,\mathsf{D} + \lfloor \mathsf{D}/2 \rfloor$, 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. D'après le Corollaire 86, nous avons $\mathsf{D} = \mathsf{D}(\mathcal{B}_\pm(G))$. La première partie est maintenant immédiate d'après le Théorème 83. Pour la seconde partie, encore une fois d'après le Théorème 83, nous avons $\rho_{2k+1}(\mathcal{B}_\pm(G)) \le k\,\mathsf{D} + \lfloor \mathsf{D}/2 \rfloor$. Puisque, d'après le Corollaire 94, nous avons $\rho_{2k+1}(\mathcal{B}(G)) \le \rho_{2k+1}(\mathcal{B}_\pm(G))$, l'assertion en découle. □

Pour une étude détaillée de la question de savoir quand $\rho_{2k+1}(\mathcal{B}(G)) = k\,\mathsf{D} + \lfloor \mathsf{D}/2 \rfloor$ est vérifiée, nous nous référons à [19] et [14]. Divers résultats y sont présentés, qui, grâce au résultat ci-dessus, donnent directement le résultat analogue pour $\mathcal{B}_\pm(G)$. Il n'y a pas besoin de recopier tous ces résultats. À titre d'exemple, nous énonçons un seul résultat.

Corollaire 96. *Soit $r \ge 2$ et soit n une puissance d'un nombre premier impair. Alors, pour chaque $k \in \mathbb{N}$, nous avons*

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

Démonstration. Ceci est une conséquence directe de la Proposition 95 et du [19, Corollaire 4.3] qui établit que $\rho_{2k+1}(\mathcal{B}(C_n^r)) = k(1 + r(n-1)) + (r(n-1))/2$ (notez que nous avons substitué la valeur de $\mathsf{D}(C_n^r)$ et évalué la fonction partie entière). □

Notons que Geroldinger, Halter-Koch et Zhong [22] ont obtenu des résultats plus puissants qui vont au-delà des nôtres. Notamment, ils ont obtenu une description complète de l'ensemble $\mathcal{U}_k$ pour les groupes d'ordres impairs avec une seule condition supplémentaire $\mathsf{D}(G) = \mathsf{D}^*(G) \geq 3$.

Théorème 97 ([22, Théorème 6.2]). *Soit G un groupe abélien fini d'ordre impair tel que $\mathsf{D}(G) = \mathsf{D}^*(G) \geq 3$, et Soit $k = l\mathsf{D}(G) + j \geq 2$, où $l \in \mathbb{N}_0$ et $j \in [0, \mathsf{d}(G)]$. Alors, nous avons :*

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

Chapitre

8 L'arithmétique des monoïdes de normes d'anneaux des entiers algébriques

Dans le présent chapitre, nous établissons un lien entre l'arithmétique de certains sous-monoïdes multiplicatifs des entiers naturels, définis via les normes des anneaux d'entiers algébriques, et l'arithmétique des monoïdes de suites pondérées à somme nulle sur des groupes abéliens finis. Une relation entre les problèmes sur les normes des entiers algébriques et les suites pondérées à somme nulle a été étudiée dans [30]. Notre application est étroitement liée mais distincte.

Nous rappelons quelques notions et résultats standards de la théorie algébrique des nombres (voir, par exemple, [31, 39, 41]).

Soit K un corps de nombres galoisien, $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$ son groupe de Galois, $\mathcal{O}_K$ son anneau d'entiers, $\mathcal{P}_K$ 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, désignons par G son groupe des classes d'idéaux et pour un idéal $J \in \mathcal{I}_K$, désignons par $[J] \in G$ sa classe d'idéaux. Soit $\mathsf{N}\colon \mathcal{I}_K \to \mathbb{N}$ la norme absolue. Nous rappelons que $\mathsf{N}(a\mathcal{O}_K) = |\mathsf{N}_{K/\mathbb{Q}}(a)|$ pour chaque $a \in \mathcal{O}_K^*$, et $\{|\mathsf{N}_{K/\mathbb{Q}}(a)|\colon a \in \mathcal{O}_K^*\} = \mathsf{N}(\mathcal{H}_K) \subseteq \mathsf{N}(\mathcal{I}_K)$ est un sous-monoïde. Nous voulons étudier l'arithmétique de ce monoïde.

Nous dénotons par $\mathbb{P} \subseteq \mathbb{N}$ l'ensemble des nombres premiers. Pour $p \in \mathbb{P}$, considérons $P_p \in \mathcal{P}_K$ comme un idéal premier qui contient p. Pour $p \in \mathbb{P}$, nous avons $\{\gamma P_p\colon \gamma \in \Gamma\}$ est l'ensemble de tous les idéaux premiers supérieurs à p, et $\mathsf{N}(\gamma P_p) = \mathsf{N}(P_p)$ pour tout $\gamma \in \Gamma$. Rappelons que $\mathsf{N}(P_p)$ est une puissance de p disant p^{f_p} ; On appelle f_p le degré résiduel de p. Nous rappelons que Γ 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 utile de considérer Γ comme un ensemble de poids pour les suites sur G. De plus, puisque chaque classe contient une infinité d'idéaux premiers, nous pouvons fixer, pour $p \in \mathbb{P}$, l'idéal premier $P_p \in \mathcal{P}_K$ de telle sorte que $G = \{[P_p]\colon p \in \mathbb{P}\}$.

Nous observons que pour $n \in \mathbb{N}$, nous avons $n \in \mathsf{N}(\mathcal{I}_K)$ si et seulement si $f_p \mid \mathsf{v}_p(n)$

pour tout $p \in \mathbb{P}$. Pour un tel n nous obtenons

$$n = \mathsf{N}\Big(\prod_{p\in\mathbb{P}} P_p^{\mathsf{v}_p(n)/f_p}\Big), \text{ et nous posons } \Theta(n) = \prod_{p\in\mathbb{P}} [P_p]^{\mathsf{v}_p(n)/f_p} \in \mathcal{F}(G).$$

En utilisant ces notations et conventions, nous obtenons le résultat suivant.

Théorème 98. *Soit K un corps de nombres galoisien avec le groupe de Galois Γ et le groupe des classes G.*

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

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

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

Pour une classe $g \in G$, nous posons $\mathbb{P}_g = \{p \in \mathbb{P} \colon [P_p] = g\}$.

1. Premièrement, nous supposons que $n = \mathsf{N}(a\mathcal{O}_K)$, où $a \in \mathcal{O}_K^*$. Nous cherchons à montrer que $\Theta(n) \in \mathcal{B}_\Gamma(G)$. Précisons que,

$$a\mathcal{O}_K = \prod_{P\in\mathcal{P}_K} P^{\mathsf{v}_P(a)} = \prod_{p\in\mathbb{P}} \prod_{\gamma\in\Gamma} (\gamma P_p)^{\mathsf{v}_{\gamma P_p}(a)}, \text{ et } 0 = \sum_{\gamma\in\Gamma} \gamma \sum_{p\in\mathbb{P}} \mathsf{v}_{\gamma P_p}(a)[P_p] \in G.$$

   Nous obtenons alors

$$n = \prod_{p\in\mathbb{P}} \prod_{\gamma\in\Gamma} p^{f_p\, \mathsf{v}_{\gamma P_p}(a)}, \text{ et par conséquent } \frac{\mathsf{v}_p(n)}{f_p} = \sum_{\gamma\in\Gamma} \mathsf{v}_{\gamma P_p}(a) \text{ pour chaque } p \in \mathbb{P}.$$

   Il s'ensuit que ;

$$\Theta(n) = \prod_{p\in\mathbb{P}} [P_p]^{\mathsf{v}_p(n)/f_p} = \prod_{\gamma\in\Gamma} \prod_{p\in\mathbb{P}} [P_p]^{\mathsf{v}_{\gamma P_p}(a)}$$

   et comme

$$\sum_{\gamma\in\Gamma} \gamma\sigma\Big(\prod_{p\in\mathbb{P}} [P_p]^{\mathsf{v}_{\gamma P_p}(a)}\Big) = \sum_{\gamma\in\Gamma} \gamma \sum_{p\in\mathbb{P}} \mathsf{v}_{\gamma P_p}(a)[P_p] = 0 \in G,$$

   nous constatons que $\Theta(n) \in \mathcal{B}_\Gamma(G)$.

   Réciproquement, soit

$$\Theta(n) = \prod_{p\in\mathbb{P}} [P_p]^{\mathsf{v}_p(n)/f_p} \in \mathcal{B}_\Gamma(G) \text{ et } \Theta(n) = \prod_{\gamma\in\Gamma} S_\gamma, \text{ où } \sum_{\gamma\in\Gamma} \gamma\sigma(S_\gamma) = 0.$$

Nous devons montrer que n est la norme d'un idéal principal. Nous posons

$$\Theta(n) = \prod_{g\in G} g^{N_g} \text{ et, pour } \gamma \in \Gamma,\ S_\gamma = \prod_{g\in G} g^{N_{\gamma,g}}.$$

Pour tout $g \in G$, il en résulte que

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

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

$$N_{\gamma,g} = \sum_{p\in\mathbb{P}_g} N_{\gamma,p} \text{ tel que } \sum_{\gamma\in\Gamma} N_{\gamma,p} = \frac{\mathsf{v}_p(n)}{f_p} \quad \text{pour chaque} \quad p \in \mathbb{P}_g.$$

Nous posons maintenant

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

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

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

et donc $\mathsf{N}(A) = n$. Et puisque

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

nous obtenons $A \in \mathcal{H}_K$, et par conséquent $n \in \mathsf{N}(\mathcal{H}_K)$.

2. Nous montrons que $\Theta : \mathsf{N}(\mathcal{H}_K) \to \mathcal{B}_\Gamma(G)$ est un homomorphisme de transfert (voir la définition 56). D'après la définition et 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 vérifiée. Pour compléter l'argument, il faut montrer que $T2$ est vérifiée. Considérons $n \in \mathsf{N}(\mathcal{I}_K)$ et $\Theta(n) = S'S''$ pour certains $S', S'' \in \mathcal{B}_\Gamma(G)$, et supposons que

$$\Theta(n) = \prod_{p\in\mathbb{P}}[P_p]^{\mathsf{v}_p(n)/f_p} = \prod_{g\in G} g^{N_g}, \quad S' = \prod_{g\in G} g^{N'_g} \text{ et } S'' = \prod_{g\in G} g^{N''_g},$$

où N_g, N'_g, $N''_g \in \mathbb{N}_0$ tel que

$$N_g = N'_g + N''_g = \sum_{p \in \mathbb{P}_g} \frac{\mathsf{v}_p(n)}{f_p} \text{ pour tout } g \in G.$$

Pour $g \in G$ divise (split) N'_g, N''_g tel que

$$N'_g = \sum_{p \in \mathbb{P}_g} N'_p, \quad N''_g = \sum_{p \in \mathbb{P}_g} N''_p, \text{ et } N'_p + N''_p = \frac{\mathsf{v}_p(n)}{f_p} \text{ pour tout } p \in \mathbb{P}_g$$

pour certains $N'_p, N''_p \in \mathbb{N}_0$. Nous posons maintenant

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

Alors $n = n'n''$,

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

□

Nous soulignons quelques conséquences du résultat précédent.

Corollaire 99. *Soit K un corps de nombres galoisien avec le groupe des classes G. Soit $H = \mathsf{N}(\mathcal{H}_K)$ le monoïde des normes absolues.*

1. *L'ensemble $\Delta(H)$ et la constante $\rho(H)$ sont finis.*
2. *Pour chaque $k \in \mathbb{N}$ 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 multiprogression quasi arithmétique avec une borne M et une différence $d \in \Delta(H) \cup \{0\}$, ce qui signifie que, $\mathsf{L} = y + (\mathsf{L}_1 \cup \mathsf{L}^* \cup (\max \mathsf{L}^* + \mathsf{L}_2)) \subseteq y + \mathcal{D} + d\mathbb{Z}$ avec $y \in \mathbb{N}_0$, $\{0, d\} \subseteq \mathcal{D} \subseteq [0, d]$, $-\mathsf{L}_1, \mathsf{L}_2 \subseteq [1, M]$, $\min \mathsf{L}^* = 0$ et $\mathsf{L}^* = [0, \max \mathsf{L}^*] \cap \mathcal{D} + d\mathbb{Z}$.*

Démonstration. Par le Théorème 98 nous savons qu'il existe un homomorphisme de transfert de H vers $\mathcal{B}_\Gamma(G)$ où Γ désigne le groupe de Galois de K.Par le Théorème 66 et le Théorème 78 nous savons que $\mathcal{B}_\Gamma(G)$ possède les propriétés recherchées. Étant donné que toutes les propriétés ne dépendent que de la longueur des factorisations et que les homomorphismes de transfert préservent les ensembles de longueurs (voir le Chapitre 3 après avoir rappelé la définition de l'homomorphisme de transfert), l'affirmation s'ensuit.

□

Dans le cas des corps de nombres quadratiques, nous pouvons appliquer nos résultats sur les suites plus-moins pondérées.

Corollaire 100. *Soit K un corps de nombres quadratiques dont le nombre des classes est impair, c'est à dire l'ordre du groupe de classe est impair. Alors $\rho(\mathsf{N}(\mathcal{H}_K)) = \rho(\mathcal{H}_K)$ et $\rho_{2k}(\mathsf{N}(\mathcal{H}_K)) = \rho_{2k}(\mathcal{H}_K)$ pour chaque $k \in \mathbb{N}$.*

Démonstration. Comme dans le corollaire précédent, il suffit d'établir l'affirmation pour $\mathcal{B}_\Gamma(G)$ où Γ représente le groupe de Galois de K. Puisque K est un corps de nombres quadratiques, il s'ensuit que $|\Gamma| = 2$. De plus, si $\Gamma = \{\mathrm{id}, \gamma\}$, 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 γ agit comme $-\mathrm{id}_G$ sur G. Autrement dit, dans ce cas, $\mathcal{B}_\Gamma(G) = \mathcal{B}_\pm(G)$. L'affirmation découle de la Proposition 95. □

Chapitre

9 Énumération des suites à somme nulle minimales sur un groupe abélien fini

Dans ce chapitre, nous cherchons à déterminer le nombre des suites à somme nulle minimales dans un groupe abélien fini G, de taille n, pour une longueur k donnée. Nous soulignons que, le mot suite est utilisé dans le même sens que dans les chapitres précédents, c'est-à-dire que l'ordre des éléments n'est pas important mais la répétition des éléments est autorisée. Dans la littérature, dans un contexte d'énumération ou encore de la combinatoire énumérative, il est plus courant de formuler ce type de résultats sous le nom de "multi-ensembles".

En effet, historiquement, la question a été traitée principalement dans le contexte d'énumération des ensembles. Pour plus de détails, voir les références [35] et [36]. Puis, elle a été généralisée dans le cas d'énumération des multi-ensembles à somme nulle, notés $M_G(k, g)$, voir [40].

Notamment, dans les articles cités ci-dessus, les auteurs ont donné des résultats dans le cas des suites de longueurs k dont la somme est égale à g sur des groupes abéliens finis, avec $g \in G$ et k un entier positif.

Soulignons que dans cette thèse, nous étudions la même question mais avec une condition supplémentaire sur la minimalité des suites à somme nulle. Où, on utilise les résultats sur les nombres de toutes les suites à somme nulle pour déterminer le nombre des suites à somme nulle minimales de certaines longueurs k.

Pour introduire nos résultats, nous utilisons des notations compatibles avec les notations des chapitres précédents.

Nous rappelons que $\mathcal{F}(G)$ est l'ensemble des suites sur G et $\mathcal{B}(G)$ est l'ensemble des suites à somme nulle. Dans ce chapitre, nous avons besoin des suites avec une somme donnée, donc nous introduisons les définitions suivantes :

Définition 101. Soit $\mathcal{B}_g(G) = \{S \in \mathcal{F}(G) \mid \sigma(S) = g\}$ l'ensemble des suites à somme égale à g.

Notons que $\mathcal{B}_0(G)$ est $\mathcal{B}(G)$.

Étant donné que, notre objectif est de compter le nombre de suites avec une longueur donnée. Nous définissons alors l'ensemble des suites dont la somme égale à g et la longueur égale à k.

Définition 102. Soit G un groupe abélien fini d'ordre n . Soit k, un entier positif, $g \in G$. Nous définissons :

1. L'ensemble des suites de longueur k sur G par :

$$\mathcal{F}(G,k) = \{S \mid |S| = k\}.$$

2. L'ensemble des suites à somme égale à g et de longueur k sur G par :

$$\mathcal{B}_g(G,k) = \{S \in \mathcal{F}(G,k) \mid \sigma(S) = g \text{ et } |S| = k\}.$$

Principalement, nous considérons le cas $g = 0$, et nous notons $\mathcal{B}(G,k)$ pour $\mathcal{B}_0(G,k)$.

Nous notons ainsi par $\#\mathcal{B}_g(G,k)$ le nombre des suites à somme égale à g et de longueur k. Et $\#\mathcal{B}(G,k)$ le nombre des suites à somme nulle de longueur k.

Nous rappelons quelques résultats existants déjà, qui donnent le nombre des multi-ensembles, pour plus de détails, voir [40]. Nous constatons que ce dernier dépend de plusieurs facteurs notamment, $\exp(G)$; $e(g)$; μ et $G[d]$, pour les définitions voir le Chapitre 3.

Théorème 103. *Soit G un groupe abélien fini d'ordre n et soit $g \in G$, et $k \in \mathbb{Z}$ avec $k > 0$. Alors, on a :*

$$\#\mathcal{B}_g(G,k) = \frac{1}{n} \sum_{s \mid \text{pgcd}(\exp(G),k)} \binom{n/s + k/s - 1}{k/s} \sum_{d \mid \text{pgcd}(e(g),s)} \mu(s/d) \#G[d].$$

Remarque 104.

- *Notons que lorsque $g = k = 0$, il existe exactement une suite de longueur 0 dont la somme est nulle. Par conséquent, on a $\#\mathcal{B}_0(G,0) = 1$.*
- *Il est évident que pour $g \neq 0$ et $k = 0$, on a $\#\mathcal{B}_g(G,0) = 0$.*

Remarque 105.
Si $\text{pgcd}(\exp(G),k) = 1$*, la formule précédente est largement plus simple. En effet,*

$$\#\mathcal{B}_g(G,k) = \frac{1}{n}\binom{n+k-1}{k}.$$

Étant donné que nous nous intéressons au nombre de suites à somme nulle, c'est-à-dire au calcul de $\#\mathcal{B}_g(G,k)$ pour $g=0$, nous présentons maintenant le théorème principal de notre étude, qui découle du théorème précédent. Comme $g=0$, on en conclut que $e(g)=\exp(G)$, ce qui donne le théorème suivant.

Théorème 106. *Soit G un groupe abélien fini d'ordre n et soit $g\in G$, et $k\in\mathbb{Z}$ avec $k>0$. Alors :*

$$\#\mathcal{B}(G,k)=\frac{1}{n}\sum_{s\mid \mathrm{pgcd}(\exp(G),k)}\binom{n/s+k/s-1}{k/s}\sum_{d\mid s}\mu(s/d)\#G[d].$$

Nous rappelons que dans le cas où $\mathrm{pgcd}(\exp(G),k)=1$, la formule pour le cardinal de $\#\mathcal{B}_g(G,k)$ est particulièrement simple. Plus généralement, on constate que si on impose des restrictions sur le $\mathrm{pgcd}(\exp(G),k)$, on obtient des cas particuliers de théorème précédent sous une forme simplifiée. Par la suite, nous traitons quelques cas qui nous seront utiles pour déterminer le nombre de suites à somme nulle minimales. Nous commençons avec le cas $\mathrm{pgcd}(\exp(G),k)\mid p$, p premier.

Proposition 107. *Soit G un groupe abélien fini d'ordre n et p un nombre premier. Si $\mathrm{pgcd}(\exp(G),k)\mid p$, alors :*

$$\#\mathcal{B}(G,k)=\frac{1}{n}\left[\binom{n+k-1}{k}+\binom{\frac{n}{p}+\frac{k}{p}-1}{\frac{k}{p}}(p^{r_p(G)}-1)\right].$$

Démonstration. Nous avons

$$\#\mathcal{B}(G,k)=\frac{1}{n}\left[\sum_{s\mid \mathrm{pgcd}(\exp(G),k)}\binom{\frac{n}{s}+\frac{k}{s}-1}{\frac{k}{s}}\sum_{d\mid s}\mu(s/d)\#G[d]\right]$$

Comme $\mathrm{pgcd}(\exp(G),k)\mid p$ pour n'importe quel nombre premier p, on aura donc deux possibilités ; soit $s=1$, soit $s=p$. En développant la somme ci-dessus, nous aurons

$$\#\mathcal{B}(G,k)=\frac{1}{n}\left[\binom{n+k-1}{k}\mu(1)\#G[1]+\binom{\frac{n}{p}+\frac{k}{p}-1}{\frac{k}{p}}(\mu(p)\#G[1]+\mu(1)\#G[p])\right]$$

Puisque $\mu(1)=\#G[1]=1$; $\mu(p)=-1$ et $\#G[p]=p^{\mathrm{r}_p(G)}$, nous obtenons

$$\#\mathcal{B}(G,k)=\frac{1}{n}\left[\binom{n+k-1}{k}+\binom{\frac{n}{p}+\frac{k}{p}-1}{\frac{k}{p}}(p^{\mathrm{r}_p(G)}-1)\right].$$

□

Si la longueur k est un nombre premier, la proposition précédente se simplifie, et la formule est donnée par le corollaire suivant.

Corollaire 108. *Soit G un groupe abélien fini d'ordre n. Si k est un nombre premier, alors :*

$$\#\mathcal{B}(G,p) = \frac{1}{n}\binom{n+p-1}{p} + \frac{1}{p}(p^{\mathrm{r}_p(G)} - 1).$$

Démonstration. Nous utilisons la Proposition précédente 107 avec $k = p$, nous obtenons

$$\begin{aligned}\#\mathcal{B}(G,p) &= \frac{1}{n}\left[\binom{n+p-1}{p} + \binom{\frac{n}{p}+\frac{p}{p}-1}{\frac{p}{p}}(p^{\mathrm{r}_p(G)} - 1)\right] \\ &= \frac{1}{n}\left[\binom{n+p-1}{p} + \binom{\frac{n}{p}}{1}(p^{\mathrm{r}_p(G)} - 1)\right] \\ &= \frac{1}{n}\binom{n+p-1}{p} + \frac{1}{p}(p^{\mathrm{r}_p(G)} - 1).\end{aligned}$$

D'où, le résultat. □

Nous abordons maintenant le cas où la longueur k des suites est égale à p^2, p premier. Nous aurons donc besoin de ce résultat pour $p = 2$, mais nous le formulons de manière générale pour tout nombre premier, car cela n'affecte pas la complexité du résultat.

Proposition 109. *Soit G un groupe abélien fini d'ordre n. Pour p premier et $k = p^2$, alors :*

$$\#\mathcal{B}(G,p^2) = \frac{1}{n}\left[\binom{n+p^2-1}{p^2} + \binom{\frac{n}{p}+p-1}{p}(p^{\mathrm{r}_p(G)} - 1) + \frac{n}{p^2}p^{\mathrm{r}_p(G)}(p^{\mathrm{r}_{p^2}(G)} - 1)\right].$$

Démonstration. Si $p^2 \nmid \exp(G)$ alors $\operatorname{pgcd}(\exp(G), p^2) \mid p$ ce qui nous permet d'appliquer la Proposition 107 avec $k = p^2$. Il est important de noter que cela donne exactement la formule du résultat, car $\mathrm{r}_{p^2}(G) = 0$, ce qui entraîne la disparition de l'un des termes.

Supposons maintenant que $p^2 \mid \exp(G)$ avec $k = p^2$, alors $\operatorname{pgcd}(\exp(G), k) = p^2$ et $s = 1$ ou p ou p^2. En appliquant le Théorème 106, nous trouvons

$$\begin{aligned}\#\mathcal{B}(G,p^2) &= \frac{1}{n}\sum_{s\mid \operatorname{pgcd}(\exp(G),p^2)}\binom{n/s+p^2/s-1}{p^2/s}\sum_{d\mid s}\mu(s/d)\#G[d] \\ &= \frac{1}{n}\left[\binom{n+p^2-1}{p^2}\cdot(\mu(1)\#G[1]) + \binom{\frac{n}{p}+p-1}{p}\cdot(\mu(p)\#G[1]+\mu(1)\#G[p])\right. \\ &\quad \left.+\binom{\frac{n}{p^2}}{1}(\mu(p^2)\#G[1]+\mu(p)\#G[p]+\mu(1)\#G[p^2])\right] \\ &= \frac{1}{n}\left[\binom{n+p^2-1}{p^2} + \binom{\frac{n}{p}+p-1}{p}\cdot(-1+p^{\mathrm{r}_p(G)})\right. \\ &\quad \left.+\frac{n}{p^2}\cdot(-p^{\mathrm{r}_p(G)} + p^{\mathrm{r}_p(G)}\cdot p^{\mathrm{r}_{p^2}(G)})\right];\end{aligned}$$

d'où

$$\#\mathcal{B}(G,p^2) = \frac{1}{n}\left[\binom{n+p^2-1}{p^2} + \binom{\frac{n}{p}+p-1}{p}(p^{\mathrm{r}_p(G)} - 1) + \frac{n}{p^2}\cdot p^{\mathrm{r}_p(G)}\cdot(p^{\mathrm{r}_{p^2}(G)} - 1)\right].$$

□

Nous évoquons deux cas particuliers qui sont traités également dans le Corollaire 108 et la Remarque 105.

Remarque 110. *Pour G un groupe abélien fini d'ordre n et pour p premier. Si $p^2 \nmid \exp(G)$. Nous obtenons :*

1. *Si* $\text{pgcd}(p^2, \exp(G)) = 1$ *alors* $\text{r}_p(G) = \text{r}_{p^2}(G) = 0$ *et*

$$\#\mathcal{B}(G,p^2) = \frac{1}{n}\binom{n+p^2-1}{p^2}.$$

2. *Si* $\text{pgcd}(p^2, \exp(G)) = p$ *alors* $\text{r}_{p^2}(G) = 0$ *et*

$$\#\mathcal{B}(G,p^2) = \frac{1}{n}\left[\binom{n+p^2-1}{p^2} + \binom{\frac{n}{p}+p-1}{p}(p^{\text{r}_p(G)}-1)\right].$$

Dans la section suivante, nous déterminerons le nombre de suites à somme nulle de longueur $k = 2, ..., 5$.

9.1 Les valeurs de $\#\mathcal{B}(G,k)$, pour $k = 2, ..., 5$

Pour cette étude, il est nécessaire de disposer des résultats exacts concernant le nombre de suites à somme nulle afin de calculer le nombre de suites à somme nulle minimales, comme nous l'avons mentionné au début du chapitre. À cet effet, nous utiliserons le Corollaire 108 ainsi que la Proposition 109. Soulignons que nous nous limitons au cas $k \leq 5$, car pour le cas $k > 5$, il devient difficile de décomposer ces suites, car elles peuvent admettre plusieurs décompositions possibles.

Nous obtenons ainsi les résultats ci-dessous.

Corollaire 111. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{B}(G,2) = \frac{n}{2} + 2^{\text{r}_2(G)-1}.$$

Corollaire 112. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{B}(G,3) = \frac{n^2}{6} + \frac{n}{2} + 3^{\text{r}_3(G)-1}.$$

Corollaire 113. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{B}(G,4) = \frac{n^3}{24} + \frac{n^2}{4} + \frac{n}{3} + 2^{\text{r}_2(G)-3}(n + 2^{\text{r}_4(G)+1}).$$

Corollaire 114. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{B}(G,5) = \frac{n^4}{120} + \frac{n^3}{12} + \frac{7n^2}{24} + \frac{5n}{12} + 5^{\mathrm{r}_5(G)-1}.$$

Dans le reste de ce chapitre, nous nous concentrerons sur la détermination de formules explicites pour le nombre de suites minimales de somme nulle, de longueur allant de $k = 1$ à 5. À cette fin, nous rappellerons les notions et définitions nécessaires.

Nous avons déjà introduit la notation $\mathcal{A}(G)$ pour les suites à somme nulle minimales. Notons donc $\mathcal{A}(G,k)$ l'ensemble des suites à somme nulle minimales de longueur k, défini comme suit :

Définition 115. Soit G un groupe abélien fini d'ordre n.

$$\mathcal{A}(G,k) = \{A \in \mathcal{A}(G) \mid |A| = k\}.$$

Par $\#\mathcal{A}(G,k)$, nous désignons donc le nombre de suites à somme nulle minimales de longueur k.
Notons par $\bar{\mathcal{A}}(G)$ le complémentaire de $\mathcal{A}(G)$ dans $\mathcal{B}(G)$ et par $\bar{\mathcal{A}}(G,k)$ le complémentaire de $\mathcal{A}(G,k)$ dans $\mathcal{B}(G,k)$. Autrement dit, $\bar{\mathcal{A}}(G)$ est l'ensemble des suites à somme nulle non-minimales et $\bar{\mathcal{A}}(G,k)$ est l'ensemble des suites à somme nulle non-minimales de longueur k.

À partir des définitions précédentes, il est évident que

$$\#\mathcal{B}(G,k) = \#\mathcal{A}(G,k) + \#\bar{\mathcal{A}}(G,k).$$

Par conséquent, nous obtenons le lemme suivant.

Lemme 116. *Soit G un groupe abélien fini d'ordre n. Soit k un entier positif. Alors :*

$$\#\mathcal{A}(G,k) = \#\mathcal{B}(G,k) - \#\bar{\mathcal{A}}(G,k).$$

Rappelons qu'une formule pour $\mathcal{B}(G,k)$ est connue. Puisque tout élément de $\bar{\mathcal{A}}(G,k)$ est produit de suites à somme nulle strictement plus courte que k, il est envisageable de réduire le problème de déterminer le cardinal de $\bar{\mathcal{A}}(G,k)$ (et donc celui de $\mathcal{A}(G,k)$) à des questions sur des suites strictement plus courtes que k. De cette manière, on essaiera de déterminer le cardinal de $\mathcal{A}(G,k)$ de manière récursive. Dans ce chapitre, nous essayons de mettre en œuvre cette approche. Toutefois, il y a plusieurs problèmes qui émergent et nos résultats restent limités à certaines valeurs de k.

Plus précisément, nous utilisons les résultats cités ci-dessus afin de calculer le nombre de suites à somme nulle minimales pour les longueurs $k = 1, ..., 5$.

9.2 Cardinal des suites à somme nulle minimales de longueur $k = 1$

Proposition 117. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{A}(G, 1) = 1.$$

Démonstration. Il est clair qu'il n'y a qu'un seul cas $S = 0_G$ donc on n'a qu'une seule suite à somme nulle minimale de longueur 1. D'où le résultat. □

9.3 Cardinal des suites à somme nulle minimales de longueur $k = 2$

Proposition 118. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{A}(G, 2) = \frac{n + 2^{\mathrm{r}_2(G)}}{2} - 1,$$

avec $\mathrm{r}_2(G)$ est le 2-rang de G.

Démonstration. D'après le Lemme 116, nous avons

$$\#\mathcal{A}(G, 2) = \#\mathcal{B}(G, 2) - \#\bar{\mathcal{A}}(G, 2).$$

Nous avons ainsi, $\#\bar{\mathcal{A}}(G, 2) = 1$ car il existe une seule suite à somme nulle non-minimale de longueur 2, à savoir $S = 00$. Pour le calcul de $\#\mathcal{B}(G, 2)$, nous renvoyons au Corollaire 111. Nous obtenons

$$\begin{aligned}\#\mathcal{A}(G, 2) &= \frac{n}{2} + 2^{\mathrm{r}_2(G)-1} - 1 \\ &= \frac{n + 2^{\mathrm{r}_2(G)}}{2} - 1.\end{aligned}$$

□

Dans le cas où $k = 2$, il est également possible d'obtenir le même résultat en utilisant une preuve directe. En effet, la preuve est déjà fournie dans l'article [37].

Démonstration. Soit $S = g_1 g_2$ une suite de longueur $k = 2$. Si $\sigma(S) = 0$ alors $g_1 = -g_2$ et si $g_1 = 0$ alors $g_2 = 0$ ce qui signifie que la suite S n'est pas minimale. Si $g_1 \neq 0$, la suite S est minimale et elle est de la forme $g_1(-g_1)$. Par conséquent, tout élément non nul de G correspond à une suite à somme nulle minimale de longueur 2.
Or, g_1 et $(-g_1)$ correspondent à la même suite. L'idée consiste à prendre tous les éléments non nuls de G, puis à ôter ceux d'ordre égal à 2. On divise ensuite par 2 pour éliminer ces répétitions. Ce qui est égal à $\frac{|G|-2^{\mathrm{r}_2(G)}}{2}$. Puis, on ajoute ceux d'ordre égal à 2 donc $2^{\mathrm{r}_2(G)} - 1$. Notons que -1 vient de l'exclusion de l'élément 0. □

9.4 Cardinal des suites à somme nulle minimales de longueur $k = 3$

Proposition 119. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{A}(G,3) = \frac{n^2}{6} + 3^{\mathrm{r}_3(G)-1} - 2^{\mathrm{r}_2(G)-1}.$$

Pour démontrer cette proposition, nous utilisons le lemme suivant.

Lemme 120. *Pour G un groupe abélien fini d'ordre n, on a :*

$$\#\mathcal{A}(G,3) = \#\mathcal{B}(G,3) - \#\mathcal{B}(G,2).$$

Démonstration. Soit S une suite de longueur 3 avec $\sigma(S) = 0$ et telle que la suite S est non minimale. Alors S se décompose en $S = S_1 S_2$ avec $\sigma(S_1) = \sigma(S_2) = 0$. Forcément, une de ces deux suites, disons S_1, est de longueur 1 et elle est donc égale à 0. D'où, on a $S = 0S_2$ où la longueur de S_2 égale à 2. Par conséquent, les suites à somme nulle non minimales de longueur 3 sont en bijection avec les suites à somme nulle de longueur 2, d'où le résultat du lemme. □

Démonstration. D'après le lemme précédent, nous avons

$$\#\mathcal{A}(G,3) = \#\mathcal{B}(G,3) - \#\mathcal{B}(G,2).$$

En utilisant les résultats des Corollaires 111 et 112, nous obtenons

$$\begin{aligned}\#\mathcal{A}(G,3) &= \frac{n^2}{6} + \frac{n}{2} + 3^{\mathrm{r}_3(G)-1} - \frac{n}{2} + 2^{\mathrm{r}_2(G)-1} \\ &= \frac{n^2}{6} + 3^{\mathrm{r}_3(G)-1} - 2^{\mathrm{r}_2(G)-1}.\end{aligned}$$

D'où la preuve de la proposition. □

Exemple 121. Calculons $\#\mathcal{A}(G, 3)$ et $\#\mathcal{B}(G, 3)$ pour :

1. $G = C_2^2 \oplus C_4$. On a $\#G = 16$, $\mathrm{r}_2(G) = 3$ et $\mathrm{r}_3(G) = 0$, d'où

$$\#\mathcal{A}(C_2^2 \oplus C_4, 3) = 39.$$

On en déduit que le nombre des suites à somme nulle minimales de longueur 3 pour le groupe abélien fini $C_2^2 \oplus C_4$ est égal à 39.

Et

$$\#\mathcal{B}(C_2^2 \oplus C_4, 3) = 50.$$

Ainsi, le nombre de toutes les suites à somme nulle de longueur 3 pour le groupe abélien fini $C_2^2 \oplus C_4$ est égal à 50.

2. $G = C_4 \oplus C_4$.

On a $\#G = 16$, $\mathrm{r}_2(G) = 2$ et $\mathrm{r}_3(G) = 0$, d'où

$$\#\mathcal{A}(C_4 \oplus C_4, 3) = 41.$$

On en déduit que le nombre des suites à somme nulle minimales de longueur 3 pour le groupe abélien fini $C_4 \oplus C_4$ est égal à 41.

Et

$$\#\mathcal{B}(C_4 \oplus C_4, 3) = 50.$$

Ainsi, le nombre de toutes les suites à somme nulle de longueur 3 pour le groupe abélien fini $C_4 \oplus C_4$ est égal à 50.

Exemple 122. Calculons $\#\mathcal{A}(G, 3)$ et $\#\mathcal{B}(G, 3)$ pour :

1. $G = C_2 \oplus C_6$ On a $\#G = 12$, $\mathrm{r}_2(G) = 2$ et $\mathrm{r}_3(G) = 1$, d'où

$$\#\mathcal{A}(C_2 \oplus C_6, 3) = 23.$$

Et

$$\#\mathcal{B}(C_2 \oplus C_6, 3) = 31.$$

2. $G = C_{12}$. On a $\#G = 12$, $\mathrm{r}_2(G) = 1$ et $\mathrm{r}_3(G) = 1$, d'où

$$\#\mathcal{A}(C_{12}, 3) = 24.$$

Et

$$\#\mathcal{B}(C_2 \oplus C_6, 3) = 31.$$

Exemple 123. Calculons $\#\mathcal{A}(G, 3)$ et $\#\mathcal{B}(G, 3)$ pour :

1. $G = C_3 \oplus C_3$. On a $\#G = 9$, $\mathrm{r}_2(G) = 0$ et $\mathrm{r}_3(G) = 2$, d'où

$$\#\mathcal{A}(C_3 \oplus C_3, 3) = 16.$$

Et

$$\#\mathcal{B}(C_3 \oplus C_3, 3) = 21.$$

2. $G = C_9$. On a $\#G = 9$, $\mathrm{r}_2(G) = 0$ et $\mathrm{r}_3(G) = 1$, d'où

$$\#\mathcal{A}(C_9, 3) = 14.$$

Et

$$\#\mathcal{B}(C_9, 3) = 19.$$

Exemple 124. Calculons $\#\mathcal{A}(G, 3)$ et $\#\mathcal{B}(G, 3)$ pour :

1. $G = C_6 \oplus C_6$. On a $\#G = 36$ et $\mathrm{r}_2(G) = \mathrm{r}_3(G) = 2$, d'où

$$\#\mathcal{A}(C_6 \oplus C_6, 3) = 217.$$

Et

$$\#\mathcal{B}(C_6 \oplus C_6, 3) = 237.$$

2. $G = C_{36}$. On a $\#G = 36$ et $\mathrm{r}_2(G) = \mathrm{r}_3(G) = 1$, d'où

$$\#\mathcal{A}(C_{36}, 3) = 216.$$

Et

$$\#\mathcal{B}(C_{36}, 3) = 235.$$

Remarque 125.

1. *Si les groupes abéliens finis sont de même ordre et ont la même valeur de* $\mathrm{r}_3(G)$*, alors le nombre de suites à somme nulle de longueur* 3, $\#\mathcal{B}(G, 3)$ *est le même.*

2. *Si les groupes abéliens finis sont de même ordre mais ils n'ont pas la même valeur de* $\mathrm{r}_3(G)$ *alors on n'aura pas le même nombre de suites à somme nulle de longueur* 3, $\#\mathcal{B}(G, 3)$.

3. *Si deux groupes abéliens finis* G_1 *et* G_2 *sont de même ordre et tels que* $\mathrm{r}_3(G_1) \neq \mathrm{r}_3(G_2) \neq 0$ *et* $\mathrm{r}_2(G_1) = \mathrm{r}_2(G_2) = 0$ *alors on aura toujours le même nombre de suites à somme nulle non minimales de longueur* 3.

9.5 Cardinal des suites à somme nulle minimales de longueur $k = 4$

Proposition 126. *Soit G un groupe abélien fini d'ordre n. Alors :*

$$\#\mathcal{A}(G,4) = \frac{n^3}{24} - \frac{n^2}{24} + \frac{n}{12} + 2^{\mathrm{r}_2(G)-3}(-n+2-2^{\mathrm{r}_2(G)}+2^{\mathrm{r}_4(G)+1}) - 3^{\mathrm{r}_3(G)-1}.$$

Démonstration. Pour démontrer la proposition ci-dessus, nous utilisons le lemme suivant.

Lemme 127. *Soit G un groupe abélien d'ordre n. On a :*

$$\#\mathcal{A}(G,4) = \#\mathcal{B}(G,4) - \#\mathcal{B}(G,3) - \binom{\#\mathcal{A}(G,2)+1}{2}.$$

Démonstration. Nous décomposons $\mathcal{B}(G,4)$ en réunion disjointe comme suit :

$$\mathcal{B}(G,4) = \mathcal{A}(G,4) \uplus \mathcal{U}(G,4) \uplus \mathcal{D}(G,4).$$

Où $\mathcal{U}(G,4)$ désigne l'ensemble des suites qui admettent une sous-suite de longueur 1, et $\mathcal{D}(G,4)$ désigne l'ensemble des suites qui admettent une sous-suite de longueur 2 mais pas de longueur 1. La réunion est clairement disjointe. Pour montrer que toute suite dans $\mathcal{B}(G,4)$ apparaît dans cette réunion, il suffit de noter que toute suite $S \in \mathcal{B}(G,4)$ qui n'est pas minimale peut être écrite comme le produit de deux suites à somme nulle, dont au moins une est de longueur inférieure ou égale à 2. Notons que $\#\mathcal{U}(G,4) = \#\mathcal{B}(G,3)$, et $\#\mathcal{D}(G,4) = \binom{\#\mathcal{A}(G,2)+1}{2}$. Par conséquent, nous obtenons

$$\#\mathcal{A}(G,4) = \#\mathcal{B}(G,4) - \#\mathcal{B}(G,3) - \binom{\#\mathcal{A}(G,2)+1}{2}.$$

□

Calculons maintenant $\#\mathcal{A}(G,4)$ en utilisant les résultats des Corollaires 112 et 113, ainsi que de la Proposition 118. Nous obtenons :

$$\begin{aligned}\#\mathcal{A}(G,4) &= \frac{n^3}{24}+\frac{n^2}{4}+\frac{n}{3}+n\cdot 2^{\mathrm{r}_2(G)-3}+2^{\mathrm{r}_2(G)-2}\cdot 2^{\mathrm{r}_4(G)}\\ &\quad-\Big(\frac{n^2}{6}+\frac{n}{2}+3^{\mathrm{r}_3(G)-1}\Big)-\binom{\frac{n+2^{\mathrm{r}_2(G)}}{2}-1+1}{2}\\ &= \frac{n^3}{24}+\frac{2n^2}{24}-\frac{n}{6}+2^{\mathrm{r}_2(G)-3}(n+2^{\mathrm{r}_4(G)+1})-3^{\mathrm{r}_3(G)-1}\\ &\quad-\Big(\frac{n^2}{8}-\frac{2n}{8}+2^{\mathrm{r}_2(G)-2}(n+2^{\mathrm{r}_2(G)-1}-1)\Big)\end{aligned}$$

Après simplification, nous trouvons

$$\begin{aligned}\#\mathcal{A}(G,4) &= \frac{n^3}{24}-\frac{n^2}{24}+\frac{n}{12}+2^{\mathrm{r}_2(G)-3}(-n+2-2^{\mathrm{r}_2(G)}+2^{\mathrm{r}_4(G)+1})\\ &\quad-3^{\mathrm{r}_3(G)-1}.\end{aligned}$$

D'où le résultat ci-dessus. □

Exemple 128. Calculons $\#\mathcal{A}(G,4)$ et $\#\mathcal{B}(G,4)$ pour :

1. $G=C_2^2\oplus C_4$. On a $\#G=16$, $\mathrm{r}_2(G)=3$, $\mathrm{r}_3(G)=0$ et $\mathrm{r}_4(G)=1$, d'où

$$\#\mathcal{A}(C_2^2\oplus C_4,4)=143.$$

On en déduit que le nombre des suites à somme nulle minimales de longueur 4 pour le groupe abélien fini $C_2^2\oplus C_4$ est égal à 143.

Et

$$\#\mathcal{B}(C_2^2\oplus C_4,4)=260.$$

Ainsi, le nombre de toutes les suites à somme nulle de longueur 4 pour le groupe abélien fini $C_2^2\oplus C_4$ est égal à 260.

2. $G=C_4\oplus C_4$.

On a $\#G=16$, $\mathrm{r}_2(G)=\mathrm{r}_4(G)=2$ et $\mathrm{r}_3(G)=0$, d'où

$$\#\mathcal{A}(C_4\oplus C_4,4)=156.$$

On en déduit que le nombre des suites à somme nulle minimales de longueur 4 pour le groupe abélien fini $C_4\oplus C_4$ est égal à 156.

Et

$$\#\mathcal{B}(C_4\oplus C_4,4)=252.$$

Ainsi, le nombre de toutes les suites à somme nulle de longueur 4 pour le groupe abélien fini $C_4\oplus C_4$ est égal à 252.

Exemple 129. Calculons $\#\mathcal{A}(G, 4)$ et $\#\mathcal{B}(G, 4)$ pour :

1. $G = C_2 \oplus C_6$ On a $\#G = 12$, $\mathrm{r}_2(G) = 2$, $\mathrm{r}_3(G) = 1$ et $\mathrm{r}_4(G) = 0$, d'où

$$\#\mathcal{A}(C_2 \oplus C_6, 4) = 60.$$

Et

$$\#\mathcal{B}(C_2 \oplus C_6, 4) = 119.$$

2. $G = C_{12}$. On a $\#G = 12$ et $\mathrm{r}_2(G) = \mathrm{r}_3(G) = \mathrm{r}_4(G) = 1$, d'où

$$\#\mathcal{A}(C_{12}, 4) = 64.$$

Et

$$\#\mathcal{B}(C_2 \oplus C_6, 4) = 116.$$

Exemple 130. Calculons $\#\mathcal{A}(G, 4)$ et $\#\mathcal{B}(G, 4)$ pour :

1. $G = C_3 \oplus C_3$. On a $\#G = 9$, $\mathrm{r}_2(G) = \mathrm{r}_4(G) = 0$ et $\mathrm{r}_3(G) = 2$, d'où

$$\#\mathcal{A}(C_3 \oplus C_3, 4) = 24.$$

Et

$$\#\mathcal{B}(C_3 \oplus C_3, 4) = 55.$$

2. $G = C_9$. On a $\#G = 9$, $\mathrm{r}_2(G) = \mathrm{r}_4(G) = 0$ et $\mathrm{r}_3(G) = 1$, d'où

$$\#\mathcal{A}(C_9, 4) = 26.$$

Et

$$\#\mathcal{B}(C_9, 4) = 55.$$

Exemple 131. Calculons $\#\mathcal{A}(G, 4)$ et $\#\mathcal{B}(G, 4)$ pour :

1. $G = C_6 \oplus C_6$. On a $\#G = 36$, $\mathrm{r}_2(G) = \mathrm{r}_3(G) = 2$ et $\mathrm{r}_4(G) = 0$, d'où

$$\#\mathcal{A}(C_6 \oplus C_6, 4) = 1872.$$

Et

$$\#\mathcal{B}(C_6 \oplus C_6, 4) = 2299.$$

2. $G = C_{36}$. On a $\#G = 36$ et $\mathrm{r}_2(G) = \mathrm{r}_3(G) = \mathrm{r}_4(G) = 1$, d'où

$$\#\mathcal{A}(C_{36}, 4) = 1884.$$

Et

$$\#\mathcal{B}(C_{36}, 4) = 2290.$$

Remarque 132.

1. *Si les groupes abéliens finis sont de même ordre et la même valeur de* $\mathrm{r}_2(G) = \mathrm{r}_4(G)$*, alors le nombre de suites à somme nulle de longueur* 4, $\#\mathcal{B}(G, 4)$ *est le même.*
2. *Le nombre de suites à somme nulle de longueur* 4 *dépend de l'ordre de groupe et de la valeur de* $\mathrm{r}_2(G)$ *et* $\mathrm{r}_4(G)$*.*
3. *Le nombre de suites à somme nulle minimales de longueur* 4 *dépend de l'ordre de groupe* G*, la valeur de* $\mathrm{r}_2(G)$*,* $= \mathrm{r}_3(G)$ *et de* $\mathrm{r}_4(G)$*.*

9.6 Cardinal des suites à somme nulle minimales de longueur $k = 5$

Proposition 133. *Soit* G *un groupe abélien fini d'ordre* n*. Alors :*

$$\#\mathcal{A}(G, 5) = \frac{n^4}{120} - \frac{n^3}{24} + \frac{5n^2}{24} + \frac{n}{12} + 2^{\mathrm{r}_2(G)-2} \cdot (-\frac{n^2}{3} + \frac{n}{2} - 2 + 2^{\mathrm{r}_2(G)} - 2^{\mathrm{r}_4(G)}) + 3^{\mathrm{r}_3(G)-1} \cdot (1 - \frac{n}{2} - 2^{\mathrm{r}_2(G)-1}) + 5^{\mathrm{r}_5(G)-1}.$$

Pour démontrer la proposition ci-dessus, nous utilisons le lemme suivant.

Lemme 134. *Soit* G *un groupe abélien d'ordre* n*. On a :*

$$\#\mathcal{A}(G, 5) = \#\mathcal{B}(G, 5) - \#\mathcal{B}(G, 4) - \#\mathcal{A}(G, 3)\#\mathcal{A}(G, 2).$$

Démonstration. Nous décomposons $\mathcal{B}(G, 5)$ en réunion disjointe comme suit :

$$\mathcal{B}(G, 5) = \mathcal{A}(G, 5) \uplus \mathcal{U}(G, 5) \uplus \mathcal{D}(G, 5).$$

Où $\mathcal{U}(G, 5)$ désigne l'ensemble des suites qui admettent une sous-suite de longueur 1, et $\mathcal{D}(G, 5)$ désigne l'ensemble des suites qui admettent une sous-suite de longueur 2 mais pas de longueur 1. La réunion est clairement disjointe. Pour démontrer que toute suite dans $\mathcal{B}(G, 5)$ apparaît dans cette réunion, il suffit de noter que toute suite $S \in \mathcal{B}(G, 5)$ qui n'est pas minimale peut être écrite comme le produit de deux suites à somme nulle, dont une est de longueur inférieure ou égale à 2.

Nous avons $\#\mathcal{U}(G, 5) = \#\mathcal{B}(G, 4)$ et $\#\mathcal{D}(G, 5) = \#\mathcal{A}(G, 3)\#\mathcal{A}(G, 2)$.

Par conséquent, nous obtenons

$$\#\mathcal{A}(G, 5) = \#\mathcal{B}(G, 5) - \#\mathcal{B}(G, 4) - \#\mathcal{A}(G, 3)\#\mathcal{A}(G, 2).$$

Avant de calculer $\#\mathcal{A}(G,5)$, nous expliquons pourquoi le cardinal de $\#\mathcal{D}(G,5) = \#\mathcal{A}(G,3) \cdot \#\mathcal{A}(G,2)$.
Soit $B \in \mathcal{D}(G,5)$. Montrons qu'il existe un $A_2 \in \mathcal{A}(G,2)$ et un $A_3 \in \mathcal{A}(G,3)$ tel que $B = A_2A_3$. De plus, A_2 et A_3 sont uniques.

1. Commençons par prouver l'existence de telles suites minimales. Il est évident que B est divisible par un élément de $\mathcal{A}(G,2)$. Autrement dit, $B = A_2 \cdot S$, où $A_2 \in \mathcal{A}(G,2)$ et $S \in \mathcal{B}(G,3)$. Puisque B n'a pas de suite à somme nulle de longueur 1, on en déduit que S n'a pas de sous-suite de longueur 1 non plus. Donc forcément, S est minimale, et donc $S \in \mathcal{A}(G,3)$.
2. Démontrons maintenant l'unicité. Supposons que $A_2A_3 = A_2'A_3'$. Nous avons $A_2 = g(-g)$ tel que $g \in G$. Par conséquent, $g(-g) \nmid A_3'$. Ainsi, $g \mid A_2'$ ou $-g \mid A_2'$. D'autre part, $A_2' = h(-h)$ tel que $h \in G$. Dans tous les cas, cela implique que $A_2 = A_2'$, et donc $A_3 = A_3'$. D'où l'unicité.

□

Démonstration. Calculons maintenant $\#\mathcal{A}(G,5)$, en utilisant les résultats des Corollaires 113 et 114, ainsi que des Propositions 118 et 119. Nous obtenons :

$$\begin{aligned}\#\mathcal{A}(G,5) &= \frac{n^4}{120} + \frac{n^3}{12} + \frac{7n^2}{24} + \frac{5n}{12} + 5^{\mathrm{r}_5(G)-1} - \big(\frac{n^3}{24} + \frac{n^2}{4} + \frac{n}{3} + n \cdot 2^{\mathrm{r}_2(G)-3} + 2^{\mathrm{r}_2(G)-2} \cdot 2^{\mathrm{r}_4(G)}\big) \\ &\quad - (\frac{n^2}{6} + 3^{\mathrm{r}_3(G)-1} - 2^{\mathrm{r}_2(G)-1})(\frac{n + 2^{\mathrm{r}_2(G)}}{2} - 1) \\ &= \frac{n^4}{120} - \frac{n^3}{24} + \frac{5n^2}{24} + \frac{n}{12} + 2^{\mathrm{r}_2(G)-2} \cdot (-\frac{n^2}{3} + \frac{n}{2} - 2 + 2^{\mathrm{r}_2(G)} - 2^{\mathrm{r}_4(G)}) \\ &\quad + 3^{\mathrm{r}_3(G)-1} \cdot (1 - \frac{n}{2} - 2^{\mathrm{r}_2(G)-1}) + 5^{\mathrm{r}_5(G)-1}.\end{aligned}$$

D'où le résultat ci-dessus.

□

Exemple 135. Calculons $\#\mathcal{A}(G,5)$ et $\#\mathcal{B}(G,5)$ pour :

1. $G = C_2^2 \oplus C_4$. On a $\#G = 16$, $\mathrm{r}_2(G) = 3$, $\mathrm{r}_3(G) = \mathrm{r}_5(G) = 0$ et $r_4(G) = 1$, d'où

$$\#\mathcal{A}(C_2^2 \oplus C_4, 5) = 246.$$

On en déduit que le nombre des suites à somme nulle minimales de longueur 5 pour le groupe abélien fini $C_2^2 \oplus C_4$ est égal à 246.

Et

$$\#\mathcal{B}(C_2^2 \oplus C_4, 5) = 969.$$

Ainsi, le nombre de toutes les suites à somme nulle de longueur 5 pour le groupe abélien fini $C_2^2 \oplus C_4$ est égal à 969.

2. $G = C_4 \oplus C_4$.

On a $\#G = 16$, $\mathrm{r}_2(G) = \mathrm{r}_4(G) = 2$ et $\mathrm{r}_3(G) = \mathrm{r}_5(G) = 0$, d'où

$$\#\mathcal{A}(C_4 \oplus C_4, 5) = 348.$$

On en déduit que le nombre des suites à somme nulle minimales de longueur 5 pour le groupe abélien fini $C_4 \oplus C_4$ est égal à 348.

Et

$$\#\mathcal{B}(C_4 \oplus C_4, 5) = 969.$$

Ainsi, le nombre de toutes les suites à somme nulle de longueur 5 pour le groupe abélien fini $C_4 \oplus C_4$ est égal à 969.

Exemple 136. Calculons $\#\mathcal{A}(G, 5)$ et $\#\mathcal{B}(G, 5)$ pour :

1. $G = C_2 \oplus C_6$ On a $\#G = 12$, $\mathrm{r}_2(G) = 2$, $\mathrm{r}_3(G) = 1$ et $\mathrm{r}_4(G) = \mathrm{r}_5(G) = 0$, d'où

$$\#\mathcal{A}(C_2 \oplus C_6, 5) = 84.$$

Et

$$\#\mathcal{B}(C_2 \oplus C_6, 5) = 364.$$

2. $G = C_{12}$. On a $\#G = 12$, $\mathrm{r}_2(G) = \mathrm{r}_3(G) = \mathrm{r}_4(G) = 1$ et $\mathrm{r}_5(G) = 0$, d'où

$$\#\mathcal{A}(C_{12}, 5) = 105.$$

Et

$$\#\mathcal{B}(C_2 \oplus C_6, 5) = 364.$$

Exemple 137. Calculons $\#\mathcal{A}(G, 5)$ et $\#\mathcal{B}(G, 5)$ pour :

1. $G = C_3 \oplus C_3$. On a $\#G = 9$, $\mathrm{r}_2(G) = \mathrm{r}_4(G) = \mathrm{r}_5(G) = 0$ et $\mathrm{r}_3(G) = 2$, d'où

$$\#\mathcal{A}(C_3 \oplus C_3, 5) = 24.$$

Et

$$\#\mathcal{B}(C_3 \oplus C_3, 5) = 143.$$

2. $G = C_9$. On a $\#G = 9$, $\mathrm{r}_2(G) = \mathrm{r}_4(G) = \mathrm{r}_5(G) = 0$ et $\mathrm{r}_3(G) = 1$, d'où

$$\#\mathcal{A}(C_9, 5) = 32.$$

Et

$$\#\mathcal{B}(C_9, 5) = 143.$$

Exemple 138. Calculons $\#\mathcal{A}(G, 5)$ et $\#\mathcal{B}(G, 5)$ pour :

1. $G = C_6 \oplus C_6$. On a $\#G = 36$, $\mathrm{r}_2(G) = \mathrm{r}_3(G) = 2$ et $\mathrm{r}_4(G) = \mathrm{r}_5(G) = 0$, d'où

$$\#\mathcal{A}(C_6 \oplus C_6, 5) = 11856.$$

Et

$$\#\mathcal{B}(C_6 \oplus C_6, 5) = 18278.$$

2. $G = C_{36}$. On a $\#G = 36$, $\mathrm{r}_2(G) = \mathrm{r}_3(G) = \mathrm{r}_4(G) = 1$ et $\mathrm{r}_5(G) = 0$, d'où

$$\#\mathcal{A}(C_{36}, 5) = 12101.$$

Et

$$\#\mathcal{B}(C_{36}, 5) = 18278.$$

Exemple 139. Calculons $\#\mathcal{A}(G, 5)$ et $\#\mathcal{B}(G, 5)$ pour :

1. $G = C_5 \oplus C_5$. On a $\#G = 25$, $\mathrm{r}_2(G) = \mathrm{r}_3(G) = \mathrm{r}_4(G) = 0$ et $\mathrm{r}_5(G) = 2$, d'où

$$\#\mathcal{A}(C_5 \oplus C_5, 5) = 2688.$$

Et

$$\#\mathcal{B}(C_5 \oplus C_5, 5) = 4755.$$

2. $G = C_{25}$. On a $\#G = 25$, $\mathrm{r}_2(G) = \mathrm{r}_3(G) = \mathrm{r}_4(G) = 0$ et $\mathrm{r}_5(G) = 1$, d'où

$$\#\mathcal{A}(C_{25}, 5) = 2685.$$

Et

$$\#\mathcal{B}(C_{25}, 5) = 4751.$$

Remarque 140.

1. *Si les groupes abéliens finis sont de même ordre et* $\mathrm{r}_5(G) = 0$*, alors le nombre de suites à somme nulle de longueur* 5 *est le même.*

2. *Le nombre de suites à somme nulle minimales dépend de l'ordre de groupe* G*, la valeur de* $\mathrm{r}_2(G)$ $\mathrm{r}_3(G)$*,* $\mathrm{r}_4(G)$ *et* $\mathrm{r}_5(G)$*.*

Soulignons que nous nous limitons au cas $k = 5$, car, pour des valeurs plus grandes, la factorisation des suites en éléments irréductibles devient plus complexe. Ce cas fait actuellement l'objet d'une étude en cours, mais n'est pas présenté dans cette thèse ; il constitue l'une de nos perspectives de recherche.

Chapitre

10 Conclusion

En résumé, cette thèse aborde deux grands axes. Le premier concerne l'étude de l'arithmétique des monoïdes de suites à somme nulle pondérées et se compose de cinq chapitres : le chapitre 4 dont l'objectif est de présenter les monoïdes de suites sur un groupe abélien fini G qui admettent une somme nulle Ω-pondérée pour un ensemble général de poids $\Omega \subseteq \mathrm{End}(G)$ et d'établir des premiers résultats sur leur arithmétique. Le chapitre 5, où nous présentons quelques résultats qui sont utiles pour nos investigations, bien qu'ils ne soient pas spécifiquement liés aux monoïdes de suites à somme nulle (pondérée). Ces résultats portent principalement sur les ensembles $\mathcal{U}_k(H)$ et les notions associées. Pour plus de détails, nous renvoyons au [17, Lemme 5.2]. Puis, le chapitre 6, où le but est d'obtenir divers résultats sur $\mathcal{U}_k(H)$ pour les monoïdes de suites à somme nulle pondérées qui vont au-delà de ce qui a déjà été établi dans le Théorème 66. Tout d'abord, nous établissons que sous certaines hypothèses sur les poids, ces ensembles sont des intervalles, c'est-à-dire des progressions arithmétiques de raison 1. Nous étudions ensuite les maximums et les minimums de ces ensembles, c'est-à-dire $\rho_k(H)$ et $\lambda_k(H)$, ce qui, combiné, permet d'obtenir une description complète de ces ensembles. Ensuite, le chapitre 7 qui vise à obtenir d'autres résultats sur $\mathcal{B}_\Omega(G)$ pour le cas particulier où l'ensemble des poids est égal à $\{+\mathrm{id}_G, -\mathrm{id}_G\}$. Enfin, le chapitre 8,dans lequel nous établissons un lien entre l'arithmétique de certains sous-monoïdes multiplicatifs des entiers naturels, définis via les normes des anneaux d'entiers algébriques, et l'arithmétique des monoïdes de suites pondérées à somme nulle sur des groupes abéliens finis. Une relation entre les problèmes sur les normes des entiers algébriques et les suites pondérées à somme nulle a été étudiée dans [30]. Notre application est étroitement liée mais reste distincte.

Le second axe est dédié à l'étude du nombre de suites à somme nulle classiques. Notre contribution consiste à déterminer le nombre exact de suites à somme nulle minimales pour de petites longueurs. Bien que la condition sur la longueur soit assez forte, cela a permis de mettre en évidence certains phénomènes intéressants. Notamment, il s'avère que le nombre de suites à somme nulle minimales dépend de la structure du groupe de manière plus subtile que le nombre de suites à somme nulle de la même longueur, où les résultats sont présentés dans le chapitre 9.

Les perspectives de travaux futurs dans la continuité de cette thèse sont multiples et diverses. En ce qui concerne l'arithmétique des suites à somme nulle pondérées, il reste

de nombreuses constantes à explorer, pour lesquelles des résultats existent déjà dans le cas classique, mais qui n'ont pas encore été étudiées dans le cas pondéré.

En ce qui concerne le nombre de suites à somme nulle minimales, plusieurs pistes de recherche s'ouvrent. La première consiste à obtenir des résultats pour des suites plus longues, bien que cela puisse s'avérer difficile. Une autre piste intéressante serait d'étendre ces résultats aux suites avec poids. En effet, plusieurs travaux ont été réalisés sur les monoïdes de suites à somme nulle pondérée après la publication de notre article [8]. Pour plus de détails, nous renvoyons à [12], [22] et [24].

Bibliographie

[1] S.D. Adhikari, D.J. Grynkiewicz, Z-W. Sun, On weighted zero-sum sequences, Adv. in Appl. Math. 48 (2012), 506 – 527.

[2] S.D. Adhikari, P. Rath, Davenport constant with weights and some related questions. Integers 6 (2006), A30.

[3] D. D. Anderson, D. F. Anderson, Elasticity of factorizations in integral domains, J. Pure App. Algebra 80 (1992), 217 – 235.

[4] P.C. Baayen, $(C_2 \oplus C_2 \oplus C_2 \oplus C_{2n})$. ZW 6/69 (1969).

[5] N. R. Baeth, D. Smertnig, Factorization theory : from commutative to noncommutative settings. J. Algebra 441 (2015), 475 – 551.

[6] G. Bhowmik, J-C. Schlage-Puchta, Davenport's constant for groups of the form $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$. In : Additive combinatorics 43 (2007), p. 307 – 326.

[7] G. Bhowmik, I. Halupczok, J-C. Schlage-Puchta, Inductive methods and zero-sum free sequences. Integers 9.5 (2009), p. 515 – 536.

[8] S. Boukheche, K. Merito, O. Ordaz, W.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 (2022), 4195 – 4217.

[9] S.T. Chapman, M. Freezeet, W.D. GaoW, W. Smith, On Davenport constant of finite abelian groups. Far East Journal of Mathematical Sciences, 5.1 (2002), p. 47 – 54.

[10] F. Chen, S. Savchev, Long minimal zero-sum sequences in the groups $C_{r-1}^2 \oplus C_{2k}$. Integers 14 (2014), A23.

[11] K. Cziszter, M. Domokos, A. Geroldinger, The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics. Springer Proceedings in Mathematics and Statistics Multiplicative Ideal Theory and Factorization Theory, (2016), p. 43 – 95.

[12] F. Fabsits, A. Geroldinger, A. Reinhart, Q. Zhong, On monoids of plus-minus weighted zero-sum sequences : the isomorphism problem and the characterization problem, J. Commut. Algebra 16 (2024), 1 – 23.

[13] Y. Fan, A. Geroldinger, F. Kainrath, S. Tringali, Arithmetic of commutative semigroups with a focus on semigroups of ideals and modules. J. Alg. App. 16 (2017) : 1750234 (42 pages).

[14] Y. Fan, Q. Zhong, Products of k atoms in krull monoids, Monatsh. Math. 181 (2016), 779 – 795.

[15] M. Freeze, A. Geroldinger, Unions of sets of lengths. Funct. Approximatio, Comment. Math, 39 (2008), 149 – 162.

[16] W. D. Gao, A. Geroldinger, Zero-sum problems in finite abelian groups : a survey, Expo. Math. 24 (2006), 337 – 369.

[17] A. Geroldinger, Additive group theory and non-unique factorizations. In : A. Geroldinger and I. Z. Ruzsa (eds.) Combinatorial Number Theory and Additive Group Theory, Birkhäuser (2009), 1 – 86.

[18] A. Geroldinger, Sets of lengths, Amer. Math. Monthly 123 (2016), 960 – 988.

[19] A. Geroldinger, D.J. Grynkiewicz, P. Yuan, On products of k atoms II, Mosc. J. Comb. Number Theory 5 (2015), 73 – 129.

[20] A. Geroldinger, D. J. Grynkiewicz, J. S. Oh, Q. Zhong, On product-one sequences over dihedral groups. Journal of Algebra and Its Applications Vol. 21, No. 04, 2250064 (2022).

[21] A. Geroldinger, F. Halter-Koch, Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory, Chapman Hall/CRC, 2006.

[22] A. Geroldinger, F. Halter-Koch, Q. 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 (2022), p. 144 – 185.

[23] A. Geroldinger, W. Hassler, Local tameness of v-noetherian monoids, J. Pure Appl. Algebra 212 (2008), 1509 – 1524.

[24] A. Geroldinger, F. Kainrath, On sets of lengths in monoids of plus-minus weighted zero-sum sequences, prepublication.

[25] A. Geroldinger, W. A. Schmid, Q. Zhong, Systems of sets of lengths : transfer krull monoids versus weakly krull monoids. In : M. Fontana (ed.) et al, Rings, polynomials, and modules, Springer (2017), 191 – 235.

[26] A. Geroldinger, P. Yuan, The set of distances in krull monoids, Bull. Lond. Math. Soc. 44 (2012), 1203 – 1208.

[27] A. Geroldinger, Q. Zhong, Factorization theory in commutative monoids, Semigroup Forum, 100 (2020), 22 – 51.

[28] D. Grynkiewicz, Structural additive theory, Springer, 2013.

[29] F. Halter-Koch, Ideal systems, Marcel Dekker, 1998.

[30] F. Halter-Koch, Arithmetical interpretation of weighted Davenport constants. Arch. Math. 103 (2014), 125 – 131.

[31] F. Halter-Koch, An invitation to algebraic numbers and algebraic functions. CRC Press, 2020.

[32] H. Harborth, Ein extremal problem für gitterpunkte, J. Reine Angew. Math. 262/263 (1973), 356 – 360.

[33] F. Kainrath, Elasticity of finitely generated domains. Houston J. Math, 31 (2005), 43 – 64.

[34] D. Kruyswijk P. Van Emde Boas, A combinatorial problem on finite abelian groups, 3. Stichting Mathematisch Centrum. Zuivere Wiskunde (1969).

[35] J. Li, D. Wan, On the subset sum problem over finite fields, Finite Fields Appl. 14 (4) (2008), 911 – 929.

[36] J. Li, D. Wan, Counting subset sums of finite abelian groups, J. Combin. Theory Ser. A 119 (2012), no. 1, 170 – 182.

[37] J. S. Liberman, Enumerating atoms of block monoids : Mémoire de master. University of Central Missouri, 2010.

[38] L. E. Marchan, O. Ordaz, W. A. Schmid, Remarks on the plus-minus weighted Davenport constant, Int. J. Number Theory 10 (2014), 1219 – 1239.

[39] J. S. Milne, Algebraic number theory (v3.08), Available at www.jmilne.org/math/, 166 pp, 2020.

[40] A. Muratovic-Ribic, Q. Wang, The multisubset sum problem for finite abelian groups, Ars Math. Contemp. 8 417-423 (2015).

[41] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Springer, 2004.

[42] J. S. Oh, On the algebraic and arithmetic structure of the monoid of product-one sequences. J. Comm. Alg. 12 (2020), 409 – 433.

[43] J.E. Olson, A combinatorial problem on finite abelian groups, I. Journal of number theory 1.1 (1969), p. 8 – 10.

[44] J.E. Olson, A combinatorial problem on finite abelian groups, II. Journal of Number Theory 1.2 (1969), p. 195 – 199.

[45] P. Rath, K. Srilakshmi, R. Thangadurai, On Davenport's constant. International Journal of Number Theory 4.01 (2008), p. 107 – 115.

[46] K. Rogers, A combinatorial problem in Abelian groups. Mathematical Proceedings of the Cambridge Philosophical Society. T. 59. 3. Cambridge University Press. 1963, p. 559 – 562.

[47] S. Savchev, F. Chen, Long zero-free sequences in finite cyclic groups, Discrete Math. 307 (2007), 2671 – 2679.

[48] W. 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. Electron. J. Combin. 18.1(2011), p. 33 – 42.

[49] W. A. Schmid, Some recent results and open problems on sets of lengths of Krull monoids with finite class group. In : S. T. Chapman (ed.) et al, Multiplicative ideal theory and factorization theory, Springer (2016), 323 – 352.

[50] T. Tao, V. Vu, Additive combinatorics, Cambridge University Press, 2006.

[51] P. Van Emde Boas, A combinatorial problem on finite abelian groups, 2. ZW-1969-007 Stichting Mathematisch Centrum (1969).

[52] P. Yuan, On the index of minimal zero-sum sequences over finite cyclic groups, J. Comb. Th., Ser. A, 114 (2007), 1545 – 1551.

[53] H. Zerdoum, Problèmes de suites à somme nulle sur les groupes abéliens finis : une approche explicite. Thèse de doctorat. Université Paris 8, 2021.

[54] X. Zeng, P. Yuan, Weighted Davenport's constant and the weighted EGZ Theorem, Discrete Math. 311 (2011), 1940 – 1947.