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

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

## 2.7.2 Extensions galoisiennes

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

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

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

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

mais l'inclusion est stricte en général.

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

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

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

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

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

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

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

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

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

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

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

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

et nous fixons :

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

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

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

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

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

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

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

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

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

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

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

et donc

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

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

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

et puisque

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

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

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

et, pour

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Alors $n = n'n''$

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

■

Nous soulignons quelques conséquences du résultat précédent.

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

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

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

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

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

### 2.7.3 Les entiers algébriques

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

et

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

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

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

d'où

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

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

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

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

On suppose maintenant $l \geqslant 1$.

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

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

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

■

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

## 3.1 Résumé historique de l'article

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

## 3.2 Introduction

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

## 3.3 Distances

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

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

De plus, nous définissons :

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

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

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

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

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

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

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

## 3.4 Quelques constructions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

nulle minimale de longueur 1. ■

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

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

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

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

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

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

et soit

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

et

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# 4 | Applications

## 4.1 Codes correcteurs

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

### 4.1.1 Codes linéaires

Pour cette partie, voir le livre [9]

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

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

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

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

**Analyse du message reçu**

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

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

**Calcul matriciel**

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

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

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

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

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