IRCAM
Représentations musicales

Stage de 3ème année de l'École Polytechnique
Master 1 de Mathématiques

Sous la direction de Moreno Andreatta

# Théorie des ensembles homométriques

Guillaume Lachaussée

Paris, 25 juin 2010

# Table des matières

# Introduction

La théorie de l'homométrie est née dans les années 1930, à partir d'un problème issu de la cristallographie. La question était de déterminer la structure d'un cristal à partir des motifs de diffraction, obtenus par rayons X. Dans des conditions idéales (desquelles on peut se rapprocher avec une bonne approximation dans les expériences), on mesure l'intensité de la transformée de Fourier de la structure du cristal. Une information manque : la phase de cette transformée de Fourier et la question est alors de savoir si on peut malgré tout retrouver la strucure recherchée.

Cette théorie, largement développée par la suite, trouve des applications dans de nombreux domaines, dont la musicologie où la question est de caractériser un ensemble de notes (ligne mélodique, accord) à partir des sous-ensembles qui le composent (notamment les intervalles musicaux).

Nous commencerons par présenter la problématique originale des ensembles homométriques en précisant les implications musicales et les résultats de structure dus à Rosenblatt ([14] et [12]). Nous introduirons ensuite la notion de $k$-deck qui permet de poser de façon générale la question de la reconstructibilité. Dans une troisième partie, on donnera les valeurs exactes des indices de reconstructibilité dans le cas de multi-ensembles de groupes abéliens finis, nous fondant sur le travail de Pebody ([10]). Enfin, nous reviendrons au cas particulier qui intéresse plus spécifiquement la musicologie qui est celui d'ensembles de $\mathbb{Z}_n$ en introduisant de nouvelles techniques (dues à Pebody dans [11]) permettant une bonne appréhension de ce cas particulier.

# 1 Les ensembles homométriques et leur structure

## 1.1 Formalisme général

Le problème original consiste à caractériser une répartition spatiale d'atomes, affectés éventuellement de poids différents (en fonction de leur taille). Il s'agit donc de déterminer un ensemble de points de $\mathbb{R}^n$.

Plus généralement, soit $G$ un groupe abélien et soit $A$ un multi-ensemble fini d'éléments de ce groupe (on autorise la répétition, ou de façon équivalente, on attribue des poids entiers). On pose $\Delta A = \{x - y \mid x, y \in A\}$ le multi-ensemble des différences. Pour tout multi-ensemble fini, le cardinal correspond au nombre d'éléments comptés avec multiplicité.

Remarque : même si $A$ est un ensemble, $\Delta A$ est généralement un multi-ensemble

**Définition 1.1.1.** *Soient $A$ et $B$ deux multi-ensembles de $G$. On dit qu'ils sont homométriques si $\Delta A = \Delta B$*

**Lemme 1.1.2.** *Soit $A$ un multi-ensemble. $\forall v \in G$, $\Delta(A + \{v\}) = \Delta A$ et $\Delta(-A) = \Delta A$.*

*Démonstration.* On a, $\forall x, y \in A$, $\forall v \in G$,

$$x - y = (x + v) - (y + v) = (-y) - (-x)$$

∎

On voit donc qu'il est illusoire de vouloir reconstituer de façon univoque un multi-ensemble à partir du multi-ensemble des différences puisque les multi-ensembles obtenus par translation et inversion auront le même multi-ensemble des différences. La question est alors de savoir si la reconstitution est néanmoins possible modulo inversion et translation (qui ne changent rien à la structure dans le cas du cristal).

**Lemme 1.1.3.** *Soient $U$ et $V$ deux multi-ensembles. Alors les multi-ensembles*

$$\begin{aligned} U + V &= \{u + v \mid u \in U, v \in V\} \\ U - V &= \{u - v \mid u \in U, v \in V\} \end{aligned}$$

*sont homométriques.*

*Démonstration.* On a $\forall u_1, u_2 \in U; \forall v_1, v_2 \in V$;

$$(u_1 + v_1) - (u_2 + v_2) = (u_1 - v_2) - (u_2 - v_1)$$

∎

On peut alors facilement construire des contre-exemples (au moins dans le cas d'un groupe sans élément d'ordre fini, comme $\mathbb{R}$ ou $\mathbb{Z}$).
Posons ainsi $U = \{6, 7, 9\}$ et $V = \{-6, 2, 6\}$, on obtient :

$$\begin{aligned} U + V &= \{0, 1, 3, 8, 9, 11, 12, 13, 15\} \\ U - V &= \{0, 1, 3, 4, 5, 7, 12, 13, 15\} \end{aligned}$$

qui sont donc homométriques mais sans être reliés par translation/inversion.

À défaut de pouvoir systématiquement remonter du multi-ensemble des différences à la classe d'équivalence (modulo inversion et translation) de l'ensemble de départ, on va chercher à caractériser la structure des ensembles homométriques, en tentant une décomposition de la forme $U + V$.

## 1.2 Contextualisation musicale

### 1.2.1 Les principes de la *set theory*

La *set theory* a été introduite et développée par plusieurs musicologues américains (voir [3] et surtout [17]) comme outil d'analyse de la musique atonale. Les notions musicales habituelles sont volontairement bousculées par les compositeurs atonaux (au premier rang desquels la deuxième école de Vienne : Schönberg, Berg, Webern) si bien que l'analyse musicale voit la plupart de ses outils habituels inefficaces pour appréhender cette musique. La *set theory* en quittant elle aussi l'ancrage dans la tonalité, permet de décrire et comprendre de façon pertinente de nombreuses œuvres post-tonales.

On commence par considérer non plus les notes elles-mêmes mais des classes d'équivalence de notes (*pitch class*) selon deux relations d'équivalence : la transposition à l'octave et l'enharmonie. Ainsi, tous les *do* de la tessiture d'un instrument seront considérés comme équivalents, de même que les *si* ♯ et *ré* ♭♭. On a ainsi 12 classes d'équivalence, pour chacune des douze notes de la gamme chromatique, que l'on numérote de 0 à 11 avec comme convention que la classe de *do* est 0.

Cette équivalence n'est pas arbitraire mais est motivée par l'esthétique de la musique atonale qui considère les notes de façon libre comme des hauteurs, indépendamment de fonctions précises qu'elles ont dans le cadre tonal (et qui créaient une différence entre *si* ♯ sensible de la tonalité d'*ut* ♯ *mineur* et *do* tonique d'*ut majeur*).

On peut alors voir très simplement les intervalles comme la différence modulo 12 entre deux classes d'équivalence de notes (on compte alors le nombre de demi-tons). C'est ainsi que la tierce mineure (ou la dixième mineure) correspondent à l'intervalle 3 dont le complémentaire, la sixte majeure correspond à l'intervalle $9 = 12 - 3$. Or, on considère des classes de hauteurs

donc on doit également considérer comme équivalents des intervalles complémentaires. On numérote finalement les intervalles de 0 (unisson, octave, etc.) à 6 (triton, équivalent à lui-même par complémentation).

Ce formalisme étant mis en place, on va pouvoir commencer à le mettre en œuvre en considérant des *ensembles* de hauteurs (*pitch class sets*). Ces ensembles sont ceux qui apparaissent pertinents du point de vue de l'analyse musicale (accord harmonique, phrase mélodique considérée dans son ensemble, etc.). L'ensemble est alors ramené à une partie de $\mathbb{Z}_{12}$ selon les principes évoqués ci-dessus.

Il nous faut toutefois rajouter deux nouvelles notions d'équivalence pour de tels ensembles : l'équivalence modulo translation et l'équivalence modulo inversion. La première correspond à la notion musicale de transposition et il est naturel de considérer que deux ensembles de notes transposés représentent le même objet musical (ainsi en est-il en analyse tonale quand on parle d'une *septième de dominante* par exemple, indépendamment de la tonalité dans laquelle elle apparaît). La seconde, moins évidente, est toutefois logique si on se rappelle que l'on considère des classes de hauteurs et des classes d'intervalles. En effet, il n'est dès lors plus pertinent de distinguer entre un ensemble et son image miroir (donné mathématiquement en remplaçant tout élément $x$ par $12 - x$) qui ont la même structure en termes d'intervalles (on a simplement « changé de sens »). Cette similarité est d'ailleurs fortement perceptible à l'oreille même si elle n'induit pas un sentiment d'identité aussi fort que dans le cas de la transposition.

Formellement, on s'est donc ramené à la considération de sous-ensembles de $\mathbb{Z}_{12}$ modulo l'action du groupe diédral $\mathbb{D}_{12}$.

### 1.2.2 Forme standard

Dans le but de classifier et de reconnaître ces ensembles de notes, il nous faut choisir un représentant de chaque classe d'équivalence modulo l'action de $\mathbb{D}_{12}$. Ce choix est canonique et le représentant obtenu s'appelle la *forme standard* (*prime form*).

Étant donné un ensemble, que l'on ordonne, on considère tous ses renversements (avec le même sens qu'en harmonie classique) et les renversements de son image miroir (tout cela modulo 12) que l'on ramène par translation à des ensembles contenant 0. On retient alors l'ensemble le plus « ramassé », *i.e.* celui tel que le dernier élément soit le plus petit, et s'il y en a plusieurs qui ont cette propriété, tel que l'avant-dernier élément soit le plus petit parmi ceux-ci, etc. Il s'agit formellement de l'ordre lexicographique inversé. Pour la clarté, considérons un exemple.

Soit l'accord parfait majeur sur *mi* : (*mi, sol* ♯*, si*). En termes de classes

de hauteurs, cela correspond à l'ensemble $\{4, 8, 11\} \subset \mathbb{Z}_{12}$. L'image miroir est $\{1, 4, 8\}$. Énumérons les translatés :

- $\{4, 8, 11\}$
- $\{8, 11, 4\}$
- $\{11, 4, 8\}$

et pour l'inversé

- $\{1, 4, 8\}$
- $\{4, 8, 1\}$
- $\{8, 1, 4\}$

ce qui ramené à 0 donne :

- $\{0, 4, 7\}$
- $\{0, 3, 8\}$
- $\{0, 5, 9\}$

et pour l'inversé

- $\{0, 3, 7\}$
- $\{0, 4, 9\}$
- $\{0, 5, 8\}$

On retient donc les deux formes $\{0, 4, 7\}$ et $\{0, 3, 7\}$ et finalement la forme standard est la seconde en classant selon l'avant-dernier élément et on l'écrit alors entre crochets $[0, 3, 7]$.

### 1.2.3 Vecteur intervallique et $Z$-relation

Quand on considère un ensemble de hauteurs, pas nécessairement sous forme standard, on peut faire apparaître son contenu intervallique en utilisant les équivalences entre intervalles évoquées précédemment. Ainsi, le contenu intervallique est invariant par transposition, inversion, renversement. Comme les seules classes d'intervalles que l'on utilise sont celles de 1 à 6 (l'unisson ou l'octave correspondent à des répétitions de note dont on ne tient pas compte quand on considère l'ensemble), on peut noter le contenu intervallique par une suite d'entiers entre crochets, sans virgule.

Si l'on prend toujours l'exemple de l'accord parfait majeur sur *mi* : (*mi, sol* ♯*, si*), alors on compte une quinte juste (équivalente à une quarte juste, d'indice 5), une tierce majeure (d'indice 4) et une tierce mineure (d'indice 3). On n'a aucun intervalle de type 1, 2 ou 6. Donc le vecteur intervallique est donné par [001110].

On fait en réalité apparaître, avec le vecteur intervallique, le multi-ensemble des différences dont on a vu qu'il ne caractérisait pas complètement l'ensemble, même à translation et inversion près. Deux ensembles qui ont le même vecteur intervallique sans être dans la même classe d'équivalence pour l'action de $\mathbb{D}_{12}$ sont dits en $Z$-relation. Là encore, la pertinence musicale de

cette notion vient que deux tels ensembles, même s'ils ne sont pas reliés par transpostion ou inversion, ont une analogie indéniable à l'oreille, précisément parce que leur structure intervallique est la même.

Considérons par exemple les ensembles $[0, 1, 3, 7]$ et $[0, 1, 4, 6]$. Ils sont déjà sous forme standard et ces formes sont distinctes donc ils ne sont pas dans la même classe d'équivalence. En revanche, on voit facilement qu'ils ont le même contenu intervallique, à savoir [111111], ils sont donc en $Z$-relation.

## 1.3 Structure dans le cas continu

On s'intéresse d'abord au cas continu, en pratique, on se place dans $\mathbb{R}^n$.

**Définition 1.3.1.** *Soient $x_1, \cdots, x_n$ $n$ variables qui commutent. On pose $\mathbb{A} = \mathbb{Z}, \mathbb{R}$ ou $\mathbb{C}$.*
*On définit $\mathbb{A}[\mathbb{R}^n]$ comme l'ensemble des combinaisons linéaires formelles :*

$$T(x) = \sum_{v \in \mathbb{R}^n} a_v x^v$$

*avec $a_v \in \mathbb{A}$ non nul pour un nombre fini de $v$ et $x^v = x_1^{v_1} \cdots x_n^{v_n}$.*
*La multiplication est donnée par la règle $x^v x^w = x^{v+w}$.*

Dans le cas où $\mathbb{A}$ est un corps, on a ainsi construit la $\mathbb{A}$-algèbre du groupe $\mathbb{R}^n$. On peut également voir les éléments comme des distributions $T = \sum_{v \in \mathbb{R}^n} a_v \delta_v$ où $\delta_v$ représente la distribution de Dirac au point $v$. Pour cette section cependant, il sera plus commode de travailler avec la notation pseudo-polynomiale.

**Théorème 1.3.2.** *Avec $\mathbb{A} = \mathbb{Z}, \mathbb{R}$ ou $\mathbb{C}$, l'anneau $\mathbb{A}[\mathbb{R}^n]$ est localement un anneau factoriel,* i.e. *tout élément se décompose en produit d'une unité et de facteurs irréductibles.*
*Les unités de $\mathbb{A}[\mathbb{R}^n]$ sont de la forme $ux^v$ où $v \in \mathbb{R}^n$ et $u$ est une unité de $\mathbb{A}$.*

*Démonstration.* Soit $T$ un élément de $\mathbb{A}[\mathbb{R}^n]$, il existe un nombre fini de $v$ tels que $a_v \neq 0$.
On considère alors le réseau $L$ engendré par $\{v \mid a_v \neq 0\}$, il est isomorphe à $\mathbb{Z}^m$. Or $\mathbb{A}$ est factoriel, donc

$$\mathbb{A}[\mathbb{Z}^m] = \mathbb{A}[x_1, x_1^{-1}, x_2, x_2^{-1}, \cdots, x_m, x_m^{-1}$$

aussi et on peut obtenir la factorisation de $T$ recherchée. ∎

Remarque : c'est bien le fait de pouvoir se ramener à $\mathbb{A}[\mathbb{Z}^m]$ à chaque fois que l'on considère une famille finie d'éléments de $\mathbb{A}[\mathbb{R}^n]$ qui fait fonctionner la démonstration. En effet, $\mathbb{A}[\mathbb{Z}^m]$ est un anneau factoriel, ce qui donne la factorialité locale à $\mathbb{A}[\mathbb{R}^n]$. Mais même dans le cas où $\mathbb{A} = \mathbb{C}$, $\mathbb{A}[\mathbb{R}^n]$ n'est pas globalement un anneau factoriel. Considérons ainsi l'exemple suivant :

$$\begin{aligned} 1-x &= (1-x^{\frac{1}{2}})(1+x^{\frac{1}{2}}) \\ &= (1-x^{\frac{1}{4}})(1+x^{\frac{1}{4}})(1+x^{\frac{1}{2}}) \\ &= (1-x^{\frac{1}{2^{i+1}}})\prod_{j=1}^{i+1}(1+x^{\frac{1}{2^j}}) \end{aligned}$$

**Définition 1.3.3.** *Soit $T$ un élément de $\mathbb{A}[\mathbb{R}^n]$, $T(x) = \sum_{v\in\mathbb{R}^n} a_v x^v$.*
*On pose $T^*(x) = \sum_{v\in\mathbb{R}^n} \bar{a_v} x^{-v}$.*
*On dit alors que deux éléments $T_1$ et $T_2$ de $\mathbb{A}[\mathbb{R}^n]$ sont homométriques si*

$$T_1(x)T_1^*(x) = T_2(x)T_2^*(x)$$

La cohérence entre les deux définitions de l'homométrie vient alors de ce qu'on associe à un multi-ensemble $T$ de $\mathbb{R}^n$ l'élément $T(x) = \sum_{v\in T} x^v$ (la sommation se fait sur le multi-ensemble, si un élément est présent $n$ fois dans le multi-ensemble, il sera alors affecté d'un coefficient $n$ dans $T(x)$).
On a alors :

$$T(x)T^*(x) = \sum_{v,w\in T} x^{v-w} = \sum_{y\in\Delta T} x^y$$

et deux multi-ensembles sont alors homométriques si et seulement si les éléments associés de $\mathbb{A}[\mathbb{R}^n]$ le sont.

On parvient alors au résultat de factorisation de Rosenblatt et Seymour ([14]) :

**Théorème 1.3.4.** *Deux éléments $T_1(x)$ et $T_2(x)$ de $\mathbb{A}[\mathbb{R}^n]$ sont homométriques si et seulement si il existe $P(x), Q(x) \in \mathbb{A}[\mathbb{R}^n]$ et $c \in \mathbb{A}$ de module 1 tels que :*

$$\begin{aligned} T_1(x) &= P(x)Q(x) \\ T_2(x) &= cP(x)Q^*(x) \end{aligned}$$

*Démonstration.* Le sens réciproque est évident car $c\bar{c} = 1$ et $(Q^*)^*(x) = Q(x)$ puisque la conjugaison et le passage à l'inverse sont des involutions.
Comme $\mathbb{A}[\mathbb{R}^n]$ est un anneau localement factoriel, on peut trouver $P_0(x)$, $B_1(x)$, $B_2(x) \in \mathbb{A}[\mathbb{R}^n]$ avec $B_1(x)$ et $B_2(x)$ premiers entre eux tels que :

$$T_1(x) = P_0(x)B_1(x) \text{ et } T_2(x) = P_0(x)B_2(x)$$

On peut ensuite trouver de la même manière $Q_0(x), C_1(x), C_2(x) \in \mathbb{A}[\mathbb{R}^n]$ avec $C_1(x)$ et $C_2(x)$ premiers entre eux tels que :

$$B_1(x) = Q_0(x)C_1(x) \text{ et } B_2^*(x) = Q_0(x)C_2(x)$$

L'équation d'homométrie $T_1(x)T_1^*(x) = T_2(x)T_2^*(x)$ nous donne alors, après simplification :

$$C_1(x)C_1^*(x) = C_2(x)C_2^*(x) \tag{1.3.1}$$

On a $C_1(x)$ et $C_2(x)$ premiers entre eux par construction. Il en est alors de même pour $C_1^*(x)$ et $C_2^*(x)$. De plus, $C_1(x)$ et $C_2^*(x)$ sont premiers entre eux car l'existence d'un facteur premier commun contredirait le fait que $B_1(x)$ et $B_2(x)$ sont premiers entre eux. De même $C_1^*(x)$ et $C_2(x)$ sont premiers entre eux.

Soit alors un facteur premier $D(x)$ divisant $C_1(x)$, il divise $C_2(x)C_2^*(x)$ et doit donc diviser $C_2(x)$ ou $C_2^*(x)$, ce qui contredit les résultats précédents. Ainsi, $C_1(x)$ est une unité de $\mathbb{A}[\mathbb{R}^n]$. De même, $C_2(x)$ est une unité.
On peut alors trouver $u_1, u_2$ des unités de $\mathbb{A}$ et $v_1, v_2 \in \mathbb{R}^n$ tels que :

$$C_1(x) = u_1 x^{v_1} \text{ et } C_2(x) = u_2 x^{v_2}$$

De 1.3.1, on tire alors $u_1\bar{u_1} = u_2\bar{u_2}$ et on pose $c = u_1/\bar{u_2}, j_1 = \frac{1}{2}(v_1 - v_2), j_2 = \frac{1}{2}(v_1 + v_2)$.

On définit enfin $P(x) = \bar{u_2}x^{j_1}P_0(x)$ et $Q(x) = cx^{j_2}Q_0(x)$, ce qui achève la démonstration. ∎

Remarque : en conservant les notations de la démonstration, on peut aboutir à une forme légèrement différente. En posant, $P(x) = u_1P_0(x)$ et $Q(x) = Q_0(x)$ et en remplaçant $v_2$ par $-v_2$, on obtient :

$$T_1(x) = x^{v_1}P(x)Q(x) \text{ et } T_2(x) = cx^{v_2}P(x)Q^*(x)$$

C'est cette forme qui permet la généralisation à $k$ éléments homométriques.

**Théorème 1.3.5.** *Soient $T_1(x), \cdots, T_k(x)$ des éléments de $\mathbb{A}[\mathbb{R}^n]$. Ils sont homométriques si et seulement s'il existe des éléments $P_1(x), \cdots, P_k(x) \in \mathbb{A}[\mathbb{R}^n]$, des sous-ensembles $I_1, \cdots, I_k$ de $\{1, \cdots, r\}$, des constantes $c_1, \cdots, c_k \in \mathbb{A}$ de module 1 et des vecteurs $v_1, \cdots, v_k \in \mathbb{R}^n$ tels que pour tout $j \in \{1, \cdots, k\}$ :*

$$T_j(x) = c_j x^{v_j} \prod_{i \in I_j} P_i(x) \prod_{i \notin I_j} P_i^*(x)$$

*Démonstration.* Il s'agit simplement de prendre une factorisation de $A_1(x)$ en facteurs premiers (unique aux termes associés près) puis, pour tout $j \in \{2, \cdots, k\}$ d'appliquer le théorème 1.3.4 au couple $A_1(x), A_j(x)$. ∎

Remarque : Généralisation à tout groupe apériodique

Si l'on prend un groupe abélien $G$ quelconque sans élément d'ordre fini à la place de $\mathbb{R}^n$, on obtient les mêmes résultats car on a la même structure localement factorielle (voire globalement factorielle dans le cas d'un groupe discret).

## 1.4 Structure dans le cas fini

Soit désormais $G$ un groupe abélien fini. On a alors, d'après le théorème de Kronecker :

$$G \simeq \bigoplus_{j=1}^{t} \mathbb{Z}_{n_j} \tag{1.4.1}$$

On utilisera dans la suite plutôt les notations sous forme de distributions pour les éléments de $\mathbb{A}[G]$. L'anneau $\mathbb{A}[G]$ n'est alors plus localement factoriel, ce n'est même plus un anneau intègre. On a en effet, $\forall g \in G\backslash\{0\}$ :

$$(\delta_g - \delta_0)(\delta_{(N-1)g} + \cdots + \delta_0) = \delta_{Ng} - \delta_0 = 0$$

où $N \in \mathbb{N}$ est l'ordre du groupe $G$.

On définit alors une base $(e_1, e_2, \cdots, e_N)$ du groupe $G$ à partir des images inverses des éléments $(1, 0, \cdots); (0, 1, 0, \cdots); \cdots; (\cdots, 0, 1)$ par l'isomorphisme 1.4.1.

On a alors, pour tout $j \in \{1, \cdots, t\}$, $e_j$ d'ordre $n_j$ et un élément générique de $G$ s'écrit sous la forme $i_1 e_1 + \cdots i_N e_N$, ou de manière plus concise $(i_1, \cdots, i_n)$ avec $i_j \in \{1, \cdots, n_j\}$.

Pour pouvoir traiter le cas de $G$ fini, on introduit la transformée de Fourier discrète des distributions de $\mathbb{A}[G]$. Dans toute la suite, $\Gamma$ désignera le groupe dual de $G$, canoniquement isomorphe à $G$ car $G$ est abélien fini.

Soit $D$ une distribution de $\mathbb{A}[G]$, on a

$$D = \sum_{(i_1,\cdots,i_n)\in G} a(i_1, \cdots, i_n)\delta_{i_1 e_1} * \cdots * \delta_{i_t e_t}$$

La transformée de Fourier est alors donnée, pour tout caractère $\gamma \in \Gamma$, par :

$$\mathcal{F}D(\gamma) = \widehat{D}(\gamma) = \sum_{(i_1,\cdots,i_n)\in G} a(i_1,\cdots,i_n)\gamma(x_1)^{-i_1}\cdots\gamma(x_t)^{-i_t}$$

où les $\gamma(x_j)$ sont des racines $n_j$-èmes de l'unité. On peut cependant utiliser aussi la notation polynomiale, avec :

$$D = \sum_{(i_1,\cdots,i_n)\in G} a(i_1,\cdots,i_n)x_1^{i_1}\cdots x_t^{i_t}$$

en se plaçant dans l'anneau $\mathbb{A}[x_1,\cdots,x_t]/I$ où les indéterminées $x_1,\cdots,x_t$ commutent et où $I$ est l'idéal engendré par les $x_j^{n_j} - 1$ pour $j \in 1,\cdots,t$.

Avec cette notation, on a alors la transformée de Fourier de $D$ en $\gamma$, $\widehat{D}(\gamma)$ qui est égale à $D\left(\overline{\gamma(x_1)},\cdots,\overline{\gamma(x_t)}\right)$.

**Définition 1.4.1.** *Une unité $U$ de $\mathbb{A}[G]$ est dite spectrale si elle vérifie $U * U^* = \delta_0$. Ainsi $U$ est une unité spectrale si et seulement si $U$ et $\delta_0$ sont homométriques.*

Les unités de $\mathbb{A}[G]$ ne peuvent s'écrire sous forme générique comme c'était le cas avec $G$ apériodique. C'est pourquoi il est pertinent de faire apparaître ce type particulier d'unités.

On arrive alors au théorème de structure dans le cas fini, dû à Rosenblatt ([12]).

**Théorème 1.4.2.** *Soient $D$ et $E$ des éléments de $\mathbb{A}[G]$. Ils sont homométriques si et seulement si il existe une unité spectrale $U \in \mathbb{A}[G]$ telle que $U * D = E$.*

On aura besoin dans la preuve d'un lemme technique que l'on démontrera plus tard :

**Lemme 1.4.3.** *Pour $D \in \mathbb{A}[\mathbb{Z}_n]$, il existe $W \in \mathbb{A}[\mathbb{Z}_n]$ tel que*

$$\forall\gamma \in \Gamma, \widehat{W}(\gamma) = \begin{cases} 1 & \text{si } \widehat{D}(\gamma) = 0 \\ 0 & \text{sinon} \end{cases}$$

*Démonstration du théorème 1.4.2.*

Cas 1 : $\mathbb{A} = \mathbb{C}$

On définit $u : \Gamma \longrightarrow \mathbb{C}$ par $u(\gamma) = 1$ si $\widehat{D}(\gamma) = 0$ et $u(\gamma) = \frac{\widehat{E}(\gamma)}{\widehat{D}(\gamma)}$ sinon.

Comme $G$ est fini, la transformée de Fourier fournit une bijection entre les distributions $\mathbb{C}[G]$ (qui sont en l'occurrence les fonctions de $G$ à valeurs dans $\mathbb{C}$) et les fonctions de $\Gamma$ à valeurs dans $\mathbb{C}$. On peut donc trouver $U \in \mathbb{C}[G]$ tel que $\widehat{U} = u$.

$D$ et $E$ sont homométriques, *i.e.* $D * D^* = E * E^*$, d'où, en utilisant la transformée de Fourier, $\widehat{D * D^*} = \widehat{E * E^*}$, soit $\widehat{D}\widehat{D^*} = \widehat{E}\widehat{E^*}$ et donc, pour tout $\gamma \in \Gamma$, $|\widehat{D}(\gamma)|^2 = |\widehat{E}(\gamma)|^2$.

On a donc, pour tout $\gamma \in \Gamma$,

$$\begin{aligned}\widehat{U * U^*}(\gamma) &= \widehat{U}(\gamma)\overline{\widehat{U}(\gamma)} \\ &= |\widehat{U}(\gamma)|^2 \\ &= 1 \\ &= \widehat{\delta_0}(\gamma)\end{aligned}$$

Par injectivité de la transformée de Fourier, $U$ est une unité spectrale. De plus, on a $\widehat{U}\widehat{D} = \widehat{E}$ (les modules sont égaux donc si $\widehat{D}(\gamma)$ s'annule, $\widehat{E}(\gamma)$ aussi) donc, toujours par injectivité de la transformée de Fourier, on a, $U * D = E$.

Si $\mathbb{A} \neq \mathbb{C}$, rien ne permet d'affirmer *a priori* que la distribution $U$ ainsi définie appartient bien à $\mathbb{A}[G]$

Cas 2 : $G = \mathbb{Z}_n$

Les caractères de $\mathbb{Z}_n$ sont identifiables aux racines $n$-èmes de l'unité en faisant correspondre $\gamma(1)$ à $\gamma$. Dans la suite, on fera l'abus de notation que cela permet.

On peut alors, en prenant le $W$ donné par le lemme 1.4.3, trouver un $U \in \mathbb{A}(\mathbb{Z}_n)$ tel que

$$U * (D + W) = E + W$$

En effet, la technique est la même que dans la démonstration du lemme 1.4.3 (*cf. infra*) en utilisant le fait que $\widehat{D + W}$ ne s'annule jamais sur $\mathbb{U}_n$ (c'est pour cela que l'on a construit $W$).

Soit $\gamma \in \mathbb{U}_n$.

- Si $\widehat{D}(\gamma) \neq 0$, alors on a $\widehat{U}(\gamma)\widehat{D}(\gamma) = \widehat{E}(\gamma)$. Comme $D$ et $E$ sont homométriques, on a $|\widehat{D}(\gamma)|^2 = |\widehat{E}(\gamma)|^2$, donc $|\widehat{U}(\gamma)| = 1$.
- Si $\widehat{D}(\gamma) = 0$, alors par égalité des modules, on a également $\widehat{E}(\gamma) = 0$ et donc $\widehat{U}(\gamma)\widehat{W}(\gamma) = \widehat{W}(\gamma)$ et $\widehat{W}(\gamma) = 1$ donc $\widehat{U}(\gamma) = 1$

Finalement, quel que soit $\gamma \in \mathbb{U}_n$, on a $|\widehat{U}(\gamma)| = 1$ et $\widehat{U}(\gamma)\widehat{D}(\gamma) = \widehat{E}(\gamma)$, donc par transformée de Fourier inverse, $U * D = E$ et $U$ est une unité spectrale.

Cas 3 : $G$ quelconque

On étend le cas précédent par récurrence en utilisant 1.4.1, on ne détaille pas ici les aspects techniques.

∎

*Démonstration du lemme 1.4.3.* Écrivons $D$ sous forme polynomiale et définissons $F = \mathrm{PGCD}(D, x^n - 1)$ dans l'anneau $\mathbb{A}[x]$ (le groupe est monogène). On peut alors trouver $M_1, M_2 \in \mathbb{A}[x]$ tels que

$$D = M_1 F \quad \text{et} \quad x^n - 1 = M_2 F \tag{1.4.2}$$

D'après le théorème de Bézout, il existe $A, B \in \mathbb{A}[x]$ tels que :

$$F = AD + B(x^n - 1) \tag{1.4.3}$$

Soit $\gamma \in \mathbb{U}_n$ tel que $D(\gamma) = 0$. Alors, d'après 1.4.3, $F(\gamma) = 0$.

Réciproquement, si $F(\gamma) = 0$, alors d'après 1.4.2, $\gamma \in \mathbb{U}_n$ et $D(\gamma) = 0$. Ainsi

$$\exists a \in \mathbb{A}, F(x) = a \prod_{\substack{\gamma \in \mathbb{U}_n \\ D(\gamma)=0}} (x - \gamma)$$

Si $\gamma \in \mathbb{U}_n$ et $D(\gamma) \neq 0$, alors $F(\gamma) \neq 0$ et donc $M_2(\gamma) = 0$. On ne peut cependant pas avoir simultanément, pour $\gamma \in \mathbb{U}_n$, $D(\gamma) = 0$ et $M_2(\gamma) = 0$ car d'après 1.4.3 et 1.4.2, on aurait alors $\gamma$ racine double de $x^n - 1$.

On définit alors $V = D + M_2$ et on a

$$V(\gamma) \neq 0 \quad \forall \gamma \in \mathbb{U}_n$$

On réduit $V$ modulo $x^n - 1$, et on note encore $V$ le polynôme obtenu, de degré au plus $n - 1$.

On cherche alors $T \in \mathbb{A}[x]$ de degré au plus $n - 1$ tel que

$$TV \equiv 1 \mod (x^n - 1)$$

Si on écrit $V = \sum_{i=0}^{n-1} v_i x^i$ et $T = \sum_{i=0}^{n-1} t_i x^i$, alors on se ramène à la résolution du système :

$$\begin{cases} 1 &= t_0 v_0 + t_1 v_{n-1} + \cdots + t_{n-1} v_1 \\ 0 &= t_0 v_1 + t_1 v_0 + \cdots + t_{n-1} v_2 \\ \vdots & \\ 0 &= t_0 v_{n-1} + t_1 v_{n-2} + \cdots + t_{n-1} v_0 \end{cases}$$

La matrice du système est

$$C_V = \begin{pmatrix} v_0 & v_{n-1} & \cdots & v_1 \\ v_1 & v_0 & \cdots & v_2 \\ \vdots & \vdots & \ddots & \vdots \\ v_{n-1} & v_{n-2} & \cdots & v_0 \end{pmatrix}$$

qui est la matrice circulante relative au polynôme $V$ dont le déterminant est

$$\det C_V = \prod_{\gamma \in \mathbb{U}_n} V(\gamma)$$

qui est non nul d'après des calculs précédents. On peut donc trouver une solution au système linéaire et donc le polynôme $T$ recherché.

On pose enfin $W_0 = TD$. Soit $\gamma \in \mathbb{U}_n$.

- Si $D(\gamma) \neq 0$, alors, d'après ce qui précède, $M_2(\gamma) = 0$ et, de $T(D + M_2) \equiv 1 \mod (x^n - 1)$, on tire $W_0(\gamma) = T(\gamma)D(\gamma) = 1$.
- Si $D(\gamma) = 0$, alors, $W_0(\gamma) = T(\gamma)D(\gamma) = 0$.

D'après la remarque faite quant au calcul de la transformée de Fourier à partir de la forme polynomiale, $W = \delta_0 - W_0$ fournit l'élément recherché.

∎

# 2 $k$-deck et reconstructibilité

## 2.1 Reconstructibilité et $Z$-relation

Deux ensembles sont homométriques s'ils ont le même ensemble de différences. On a vu en 1.1 que cela ne suffit pas à reconstruire l'ensemble de départ. C'est d'ailleurs cette non-reconstructibilité qui est utilisée pour faire apparaître des ensembles de notes non équivalents (par transposition/inversion) mais avec la même structure intervallique, définissant ainsi la $Z$-relation (*cf.* 1.2.3).

On cherche alors à généraliser la notion d'ensembles homométriques avec quelque chose de plus fin, qui révèle plus d'informations sur la strucutre interne des ensembles considérés. On souhaite ainsi obtenir une caractérisation des ensembles qui permette leur reconstructibilité.

## 2.2 Généralités sur le $k$-deck

### 2.2.1 Définitions

Étant donné un multi-ensemble $A$, inclus dans un groupe abélien $G$, connaître son multi-ensemble des différences était équivalent à connaître le multi-ensemble des couples qu'il contenait modulo translation. On généralise donc ceci aux $k$-uplets contenus dans le multi-ensemble $A$.

Il nous faut d'abord une définition adéquate d'un multi-ensemble.

**Définition 2.2.1.** *Un $G$-multiensemble fini est une application de $G$ dans $\mathbb{N}$ presque nulle.*

*Un $G$-ensemble fini est une application de $G$ dans $\{0,1\}$ presque nulle.*

À chaque élément de $G$, on associe sa multiplicité. Comme on n'a pas fait d'hypothèses sur le cardinal de $G$, on impose que les applications soient presque nulles pour que les multi-ensembles soient de cardinal fini. L'ensemble sous-jacent à un $G$-multiensemble $f$ ainsi défini est alors donné par $\{g \in G \mid f(g) > 0\}$ et le cardinal du multi-ensemble est donné par $\sum_{g\in G} f(g)$.

La définition du $k$-deck est l'une des plus conflictuelles qui soient dans la bibliographie. Nous choisissons de donner la nôtre, certes plus complexe de prime abord, mais qui permet de traiter tous les cas (en levant les ambiguïtés) tout en rendant correctement compte de la structure. Commençons néanmoins par nous restreindre au cas de $G \subset \mathbb{R}$ pour tout ce paragraphe, on verra comment généraliser la définition au paragraphe 2.2.4.

**Définition 2.2.2.** *Soit un $G$-multiensemble $f$, on définit son $k$-deck par l'application $f_k : G_+^{\{k-1\}} \longrightarrow \mathbb{N}$ par*

$$f_k(g_1, \cdots, g_{k-1}) = \sum_{g \in G} \prod_{i=0}^{k-1} f(g + g_i)$$

*où $g_0 = 0$ et où $G_+^{\{k-1\}}$ désigne l'ensemble des $(k-1)$-uplets tels que :*

$$0 = g_0 \leq g_1 \leq g_2 \leq \cdots \leq g_{k-1}$$

*et la sommation est finie.*

### 2.2.2 Exemple

Considérons le 3-deck du multi-ensemble $\{1, 2, 2, 3, 4\}$. Ce $\mathbb{Z}$-multiensemble est donné formellement par l'application $f$ de $\mathbb{Z}$ dans $\mathbb{N}$ définie par :

$$\begin{cases} f(1) &= 1 \\ f(2) &= 2 \\ f(3) &= 1 \\ f(4) &= 1 \\ f(n) &= 0 \ \forall n \in \mathbb{Z} \setminus \{1, 2, 3, 4\} \end{cases}$$

Le calcul du 3-deck nous donne alors :

$$\begin{cases} f_3(1,1) &= 1 \\ f_3(1,2) &= 4 \\ f_3(1,3) &= 2 \\ f_3(2,3) &= 1 \\ f_3(0,1) &= 1 \\ f_3(0,2) &= 1 \\ f_3(m,n) &= 0 \ \text{ sinon} \end{cases}$$

Cherchons à interpréter cela en termes ensemblistes : $f_3(1,1) = 1$ signifie que $f$ contient une copie (modulo translation) du 3-uplet (0,1,1), en effet, elle est donnée par (1,2,2).

$f_3(1,2) = 4$ signifie que $f$ contient 4 copies (modulo translation) du 3-uplet (0,1,2), en effet, il s'agit de deux exemplaires de (1,2,3) (puisqu'on dispose de deux « 2 » différents dans le multi-ensemble) et de deux exemplaires de (2,3,4) (pour la même raison).

$f_3(0,1) = 1$ signifie que $f$ contient une copie (modulo translation) du 3-uplet (0,0,1), en effet, elle est donnée par (2,2,3).

Les autres cas sont similaires et on voit qu'il y a bien coïncidence entre la définition formelle et la façon naturelle de compter les $k$-uplets modulo translation.

### 2.2.3 Reconstructibilité

La question est alors la même qu'avec les ensembles homométriques, on cherche à reconstruire un multi-ensemble connaissant son $k$-deck.

**Définition 2.2.3.** *Soit $f$ un $G$-multiensemble. On dit que $f$ est $k$-reconstructible si, pour tout $G$-multiensemble $g$, on a*

$$g_r = f_r \ \forall r \leq k \Longrightarrow \exists t \in G, g(x) = f(x+t)$$

*c'est-à-dire que les seuls multi-ensembles qui ont le même $r$-deck que $f$ (pour $r$ variant de 1 à $k$) sont les translatés de $f$.*

Là encore, il est illusoire de vouloir reconstituer de façon univoque le multi-ensemble, les multi-ensembles translatés ayant le même $k$-deck pour tout $k$. Cependant, c'est la seule transformation que l'on doit prendre en compte, car dès que $k > 2$, on peut distinguer entre un multi-ensemble et son « inversé » (ce qui n'était pas le cas pour $k = 2$).

**Définition 2.2.4.** *Soit $f$ un $G$-multiensemble. On définit l'indice de reconstructibilité de $f$ par*

$$r(f) = \inf\{k \mid f \text{ est } k\text{-reconstructible}\}$$

*La borne inférieure est bien définie car l'ensemble est non vide, en effet tout $G$-multiensemble $f$ est $|f|$-reconstructible.*

*On définit l'indice de reconstructibilité de $G$ par*

$$r(G) = \sup\{r(f) \mid f \text{ est un } G\text{-multiensemble}\}$$

*On définit un deuxième indice de reconstructibilité, pour les seuls ensembles*

$$r_e(G) = \sup\{r(f) \mid f \text{ est un } G\text{-ensemble}\}$$

L'enjeu va être alors d'étudier ces indices de reconstructibilité.

### 2.2.4 Généralisation à un groupe agissant sur un ensemble

On a jusqu'à présent considéré un multi-ensemble de $G$ et on a défini le $k$-deck en fonction des copies modulo translation. On peut généraliser la notion de $k$-deck à une autre action que celle de $G$ sur lui-même par translation.

Soit $X$ un ensemble quelconque et soit $G$ un sous-groupe de $\mathrm{Aut}(X)$. Ainsi $G$ agit sur $X$ de telle sorte que pour tout $g \in G$, la séquence $(g \cdot x)_{x \in X}$ est une permutation de $X$.

On a alors une action naturelle de $G$ sur $\tilde{\mathcal{P}}(X)$, l'ensemble des multi-ensembles de $X$. On peut évidemment définir les orbites pour cette action, sachant que tous les éléments d'une même orbite auront, en particulier, le même cardinal.

**Définition 2.2.5.** *Deux multi-ensembles sont alors $G$-équivalents s'ils appartiennent à la même orbite (dans le cas de l'action de $G$ sur lui-même par translation, on a ainsi fait apparaître la notion de multi-ensembles translatés).*

On note $\mathfrak{X}_n$ l'ensemble des orbites de multi-ensembles de cardinal $n$.

**Définition 2.2.6.** *Soit $f$ un multi-ensemble de $X$. On a alors une application $f_k : \mathfrak{X}_k \longrightarrow \mathbb{N}$ définie comme suit : étant donné une orbite $\mathfrak{P} \in \mathfrak{X}_k$, on choisit un multi-ensemble $P \in \mathfrak{P}$ avec $P = \{p_1, \cdots, p_k\}$ et on pose*

$$f_k(\mathfrak{P}) = \sum_{g \in G} \prod_{i=1}^{k} f(g \cdot p_i)$$

Remarques :

- La définition est rigoureuse car le nombre obtenu ne dépend pas du choix du multi-ensemble $P \in \mathfrak{P}$. En effet, si l'on prend un autre multi-ensemble $Q$, alors, comme ils sont dans la même orbite, on trouvera $g_0 \in G$ tel que $Q = g_0 \cdot P$, ce qui signifie - quitte à renuméroter les éléments de $Q$ - que $q_i = g_0 \cdot p_i$ et il s'agit alors simplement d'une translation d'indice dans la somme sur $G : g \to g_0 g$.
- Cette définition est cohérente avec celle donnée ci-dessus pour $G \subset \mathbb{R}$ agissant sur lui-même par translation. Dans ce cas, on a un choix canonique d'un multi-ensemble de chaque orbite en imposant que les éléments soient ordonnés et que l'élément minimal soit 0.

On peut traiter de façon simple le cas de $G$ agissant par translation sur lui-même avec $G \not\subset \mathbb{R}$, si l'on peut trouver un choix canonique de représentants d'un $k$-uplet. Dans le cas de $\mathbb{Z}_n$ (très utile dans la pratique), on choisit des représentants sous forme de classes d'entiers naturels $(a_1, \cdots, a_k)$ ordonnés par ordre croissant, tels que $a_1 = 0$ et que le $a_k$ obtenu soit minimal parmi tous les choix possibles (si plusieurs représentants ont cette propriété, on impose alors que $a_{k-1}$ soit minimal, etc.). Formellement, il s'agit d'un ordre lexicographique inversé parmi tous les représentants croissants commençant par 0.

Exemple :

Considérons l'ensemble $\{0, 4, 8, 9, 11\}$ dans $\mathbb{Z}_{12}$. Les différents représentants sous forme de séquences d'entiers naturels ordonnés sont obtenus par permutation circulaire puis translation qui annule le premier élément, on a ainsi :

- $\{0, 4, 8, 9, 11\}$
- $\{0, 4, 5, 7, 8\}$
- $\{0, 1, 3, 4, 8\}$
- $\{0, 2, 3, 7, 11\}$
- $\{0, 1, 5, 9, 10\}$

La minimalité de $a_5$ est obtenue pour les deuxième et troisième permutations, on arbitre entre les deux selon $a_4$ et le représentant est finalement celui de la troisième permutation : $\{0, 1, 3, 4, 8\}$

On reconnaît le procédé utilisé pour trouver la forme standard d'un ensemble de notes dans le cadre de la *set theory* (cf. 1.2.1), sauf qu'on s'est ici restreint à l'action de $\mathbb{Z}_n$ sur $\mathbb{Z}_n$ et non à celle de $\mathbb{D}_n$ sur $\mathbb{Z}_n$.

La question de la reconstructibilité demeure, mais formulée différemment :

**Définition 2.2.7.** *Soit $f$ un multi-ensemble de $X$ (on a toujours l'action de $G$ sur $X$ par permutation). On dit que $f$ est $k$-reconstructible si, pour tout multi-ensemble $g$, on a*

$$g_r = f_r \ \forall r \leq k \Longrightarrow \exists t \in G, g = t \cdot f$$

*c'est-à-dire que les seuls multi-ensembles qui ont le même $r$-deck que $f$ (pour $r$ variant de 1 à $k$) sont les éléments de l'orbite de $f$.*

On peut alors définir comme en 2.2.4 les indices de reconstructibilité que l'on va chercher à calculer de manière exacte ou à borner asymptotiquement.

On distingue en fait entre le cas des ensembles et des multi-ensembles (on peut souvent améliorer les résultats dans le cas des ensembles) et également entre le cas générique d'un groupe $G$ agissant sur un ensemble $X$ et celui – très utile en pratique – d'un groupe abélien fini ($\mathbb{Z}_n$ en particulier) agissant sur lui-même par translation.

## 2.3 Indice de reconstructibilité pour un groupe agissant sur un ensemble

Il y a deux bornes distinctes sur cet indice. La première affirme que tout ensemble de cardinal $k$ est $(k-1)$-reconstructible dès que $k \geq 3$, résultat dû au mathématicien russe Mnukhin ([7], [8], [9]) et dont la démonstration

révèle la complexité intrinsèque du problème. La seconde due à Alon, Caro, Krasikov et Roditty ([1]) donne une borne meilleure et qui est toujours la meilleure connue à ce jour si l'on ne fait pas d'hypothèse supplémentaire sur $G$ ou sur $X$.

La borne de Mnukhin n'est d'aucune utilité en pratique puisque celle de [1] est meilleure. Toutefois, elle a constitué une avancée décisive et déploie des techniques de démonstration algébriques et combinatoires intéressantes. Cependant ces techniques ne nous seront pas utiles pour la suite du propos et nous choisissons de ne pas reproduire pas ici sa démonstration.

Nous reprenons donc les résultats de [1]. Comme on travaille ici avec des ensembles et non des multi-ensembles, on peut utiliser les notations classiques des actions de groupe. $G$ agit donc sur $X$ et si on prend $Y$ et $S$ deux sous-ensembles de $X$, on note :

- $Y^G = \{gY \mid g \in G\}$ l'orbite de $Y$ pour l'action naturelle de $G$ sur $\mathcal{P}(X)$.
- $G_Y = \{g \in G \mid gY = Y\}$ le stabilisateur de $Y$ sous l'action de $G$.
- $Y^{G_S} = \{gY \mid g \in G, gS = S\}$ l'orbite de $Y$ sous l'action de $G_S$ (le stabilisateur de $S$).

Ce sont Krasikov et Roditty qui ont introduit la notion de $k$-deck pour tout $k$. Des travaux précédents faisaient déjà apparaître le 2-deck (ensembles homométriques) et surtout le $(n-1)$-deck qui est la clé de la ERC (*Edge Reconstruction Conjecture* qui suppose la reconstructibilité d'un graphe à partir des sous-graphes obtenus en supprimant un côté). Leur définition est d'ailleurs assez impropre, mais le résultat obtenu, sous la forme d'un théorème général et technique permet de donner des bornes asymptotiques à de nombreux problèmes de reconstructibilité. On ne suppose rien sur les cardinaux de $G$ et de $X$, la seule restriction porte sur le fait de considérer des ensembles et non des multi-ensembles.

**Théorème 2.3.1.** *Soit $Y$ un sous-ensemble de $X$ de cardinal $m$, non $k$-reconstructible. On suppose qu'il existe un sous-ensemble $S$ de $Y$ de cardinal $t$, avec $|G_S| < \infty$ et $k \geq t$.*

*Alors il existe un ensemble $T$ avec $S \subset T \subset Y$ et $|T| \geq k+1$ et $\epsilon \in \{0,1\}$ tels que pour tout ensemble $K$ vérifiant $S \subset K \subset T$ et $|K| \equiv \epsilon \mod 2$, on peut trouver $g \in G$ tel que $T \cap gY = K$.*

*Démonstration.* Comme $Y$ n'est pas $k$-reconstructible, il existe un sous-ensemble $Y'$ de $X$, avec $Y' \notin Y^G$ et $f_j^Y = f_j^{Y'}$ pour tout $j \in \{1, \cdots, k\}$ (les ensembles ont le même $j$-deck pour $1 \leq j \leq k$).

Pour tout ensemble $A$ contenant $S$, on pose $\varphi_1(A) = f_{|A|}^Y(A)$ et $\varphi_2(A) = f_{|A|}^{Y'}(A)$ (on compte le nombre de copies de $A$ dans les orbites $Y^G$ et $Y'^G$). Il

faut d'abord vérifier que ces deux fonctions sont bien définies (*i.e.* le résultat obtenu est fini). On a :

$$Y^G = \{g_1 Y, g_2 Y, \cdots, g_n Y, \cdots\}$$

Si l'orbite est finie, $\varphi_1(A) \leq |Y^G|$ et il n'y a rien à prouver. Si l'orbite est infinie, considérons d'abord ce qui se passe pour $A = S$. Il s'agit de compter les $i \in \mathbb{N}$ tels que

$$S \subset g_i Y \Longleftrightarrow g_i^{-1} S \subset Y$$

Or, $S$ et $Y$ étant finis (de cardinaux respectifs $t$ et $m$), il n'y a qu'un nombre fini d'inclusions possibles de $g_i^{-1}S$ dans $Y$, $\binom{m}{t}$ au maximum. Par le principe de Dirichlet, on trouve donc $i < j$ tels que $g_i^{-1}S = g_j^{-1}S$, soit $g_j g_i^{-1} \in G_S$. Or $|G_S| < \infty$, si bien qu'on borne finalement $\varphi_1(S)$ par $\binom{m}{t}|G_S|$.

Si on considère $A$ contenant $S$, alors le même raisonnement fonctionne puisque $G_A \subset G_S$ (il y a plus d'éléments à stabiliser). Finalement, $\varphi_1$ et $\varphi_2$ sont bien définies.

On pose $\varphi = \varphi_1 - \varphi_2$ et, d'après les hypothèses du théorème, on a alors :

$$\varphi(A) = 0 \quad \forall\ S \subset A, |A| \leq k$$

$\varphi(Y) = 1 - 0 = 1 \neq 0$ donc on peut trouver $T$ minimal pour l'inclusion tel que $S \subset T \subset Y$ et $\varphi(T) \neq 0$. On a alors $|T| > k$ et on pose $\varphi(T) = b$.

On garde le système de représentants $(g_1, g_2, \cdots, g_n, \cdots)$ de l'orbite $Y^G$ et on prend un système de représentants $(g'_1, g'_2, \cdots, g'_n, \cdots)$ de l'orbite $Y'^G$.

Soit $K$ tel que $S \subset K \subset T$. On cherche alors à compter les éléments de l'orbite $Y^G$ dont l'intersection avec $T$ est exactement $K$.

$$|\{g_i \mid g_i Y \cap T = K\}| = \sum_{K \subset K' \subset T} (-1)^{|K'-K|} \varphi_1(K')$$

En effet, $\varphi_1(K)$ nous donne l'ensemble des éléments de l'orbite dont l'intersection avec $T$ contient $K$ (puisque $K \subset T$). Il faut alors enlever les éléments dont l'intersection contient plus que $K$ par un principe d'inclusion/exclusion. Le raisonnement est similaire à celui qui permet d'aboutir à la formule de Poincaré établissant le cardinal d'une union d'ensembles finis, et on obtient ainsi la formule annoncée.

De même :

$$|\{g'_i \mid g'_i Y' \cap T = K\}| = \sum_{K \subset K' \subset T} (-1)^{|K'-K|} \varphi_2(K')$$

ce qui donne finalement, en utilisant la minimalité de $T$ :

$$\begin{aligned} |\{g_i \mid g_i Y \cap T = K\}| - |\{g'_i \mid g'_i Y' \cap T = K\}| &= \sum_{K \subset K' \subset T} (-1)^{|K'-K|} \varphi(K') \\ &= (-1)^{|T-K|} b \end{aligned}$$

On chosit $\epsilon$ tel que $\epsilon \equiv |T| \mod 2$.

Pour tout $K$ tel que $S \subset K \subset T$ et $|K| \equiv \epsilon \mod 2$, la différence calculée est strictement positive, donc le premier ensemble est non vide. On peut donc trouver un $g_i$ tel que $g_i Y \cap T = K$.

De même, pour tout $K$ tel que $|K| \equiv 1 - \epsilon \mod 2$, la différence calculée est strictement négative, donc le deuxième ensemble est non vide. On peut donc trouver un $g'_i$ tel que $g'_i Y' \cap T = K$. ∎

On obtient alors le corollaire suivant :

**Corollaire 2.3.2.** *Soit $Y$ un sous-ensemble de $X$ de cardinal $m$. On suppose qu'il existe un sous-ensemble $S$ de $Y$ de cardinal $t$, avec $|G_S| < \infty$.*

*Si $k > t + \log_2(|Y^{G_S}|) + \log_2(\binom{m}{t})$, alors $Y$ est $k$-reconstructible.*

*Démonstration.* On pose $|Y^{G_S}| = s$ et supposons par l'absurde que $Y$ est non $k$-reconstructible. D'après le théorème 2.3.1, il existe $T$ avec $S \subset T \subset Y$, $|T| \geq k+1$ et $\epsilon \in \{0,1\}$ tels que pour tout $K$ avec $S \subset K \subset T$, $|K| \equiv \epsilon \mod 2$, il existe $g \in G$ vérifiant $T \cap gY = K$.

On pose $U = \{gY \mid g \in G, S \subset gY\}$. En réutilisant les notations de la démonstration du théorème 2.3.1, on a $|U| = \varphi_1(S)$. Donc $|U| \leq s\binom{m}{t}$. Or si l'on considère les $K$ donnés par le théorème, on voit qu'ils fournissent $2^{|T|-t-1}$ différentes intersections possibles entre $T$ et des éléments de l'orbite de $Y$ (contenant alors nécessairement $S$). En effet, on a $S \subset T \subset Y$ donc il s'agit de choisir parmi $w = |T| - |S|$ éléments, mais la condition de parité imposée nous donne la somme

$$\sum_{k=0}^{\lfloor \frac{w}{2} \rfloor} \binom{w}{2k} \text{ ou } \sum_{k=0}^{\lfloor \frac{w-1}{2} \rfloor} \binom{w}{2k+1}$$

selon la parité de $|T|$. Or on a la formule $\binom{w}{j} = \binom{w-1}{j-1} + \binom{w-1}{j}$ donc

$$\begin{aligned} \sum_{k=0}^{\lfloor \frac{w}{2} \rfloor} \binom{w}{2k} &= \sum_{k=0}^{\lfloor \frac{w}{2} \rfloor} \binom{w-1}{2k} + \binom{w-1}{2k-1} \\ &= \sum_{k=0}^{w-1} \binom{w-1}{k} \\ &= 2^{w-1} \end{aligned}$$

et

$$\begin{aligned}\sum_{k=0}^{\lfloor\frac{w-1}{2}\rfloor}\binom{w}{2k+1} &= \sum_{k=0}^{\lfloor\frac{w-1}{2}\rfloor}\binom{w-1}{2k+1}+\binom{w-1}{2k}\\ &= \sum_{k=0}^{w-1}\binom{w}{k}\\ &= 2^{w-1}\end{aligned}$$

Finalement :

$$2^{k-t} \leq 2^{|T|-t-1} \leq |U| \leq s\binom{m}{t}$$

ce qui contredit l'hypothèse sur $k$. ∎

Si l'on prend désormais le cas particulier où $G$ est fini (ce qui arrive très souvent dans la pratique), on a une autre estimation, plus simple.

**Corollaire 2.3.3.** *Soit $Y$ un sous-ensemble de $X$ sur lequel agit $G$ (supposé fini). Alors, si $k > \log_2(|G|) - \log_2(|G_Y|)$, $Y$ est $k$-reconstructible. En particulier, si $k > \log_2(|G|)$, tout sous-ensemble de $X$ est $k$-reconstructible.*

Remarque : Dans la deuxième formule, on ne fait apparaître que le cardinal de $G$, mais la dépendance en $X$ existe car $G$ est un groupe d'automorphismes de $X$, et la reconstructibilité ne se fait de toute façon que modulo l'action de $G$ sur $X$.

*Démonstration.* La formule des classes s'applique puisque $G$ est fini : $|Y^G| = \frac{|G|}{|G_Y|}$. Si $Y$ n'est pas $k$-reconstructible, alors d'après le théorème 2.3.1 (avec $S = \emptyset$), il existe un sous-ensemble $T$ de $Y$ de cardinal $|T| \geq k+1$ qui a au moins $2^{|T|-1}$ intersections différentes avec $Y^G$ (calcul similaire à celui du corollaire précédent). Ainsi :

$$\frac{|G|}{|G_Y|} \geq 2^{|T|-1} \geq 2^k$$

ce qui contredit l'hypothèse sur $k$. ∎

## 2.4 Cas particulier de $\mathbb{Z}_n$

On introduit ici un formalisme (largement inspiré de [11]) apparu initialement comme un jeu mathématique, celui des colliers. C'est en fait une spécification du problème de $k$-reconstructibilité d'un ensemble sur lequel agit un groupe.

**Définition 2.4.1.** *Un $(n,t)$-collier $C$ est un sous-ensemble de $\mathbb{Z}_n$ à $t$ éléments. Il s'agit de penser à un collier comme à un cercle de $n$ perles, celles qui sont dans $C$ sont noires (au nombre de $t$) et celles qui ne sont pas dans $C$ sont blanches.*

Remarque : Le choix des deux couleurs n'est pas déterminant et le lecteur pourra les ajuster à son goût.

**Définition 2.4.2.** *Deux colliers $C_1$ et $C_2$ sont $\mathbb{Z}_n$-équivalents s'il existe $i \in \mathbb{Z}_n$ tel que $C_2 = C_1 + i$. Cela correspond à effectuer une rotation du collier d'un angle de $\frac{i\pi}{n}$.*

*Deux colliers $C_1$ et $C_2$ sont $\mathbb{D}_n$-équivalents s'il existe $i \in \mathbb{Z}_n$ tel que $C_2 = C_1 + i$ ou $C_2 = -C_1 + i$. Cela correspond à effectuer une rotation du collier d'un angle de $\frac{i\pi}{n}$ ou à retourner le collier puis à effectuer une rotation de $\frac{i\pi}{n}$.*

$\mathbb{D}_n$ est le groupe diédral, groupe des isométries laissant invariant un polygone régulier à $n$ côtés (le groupe est de cardinal $2n$).

**Définition 2.4.3.** *On dit que $C_2$ est un $\mathbb{Z}_n$-sous-collier (resp. un $\mathbb{D}_n$-sous-collier) de $C_1$ si $C_2$ est $\mathbb{Z}_n$-équivalent (resp. $\mathbb{D}_n$-équivalent) à un sous-ensemble de $C_1$.*

Le $k$-deck apparaît alors être le multi-ensemble des classes d'équivalence des sous-colliers possédant $k$ perles noires. On peut d'ailleurs, dans le cadre de ce formalisme, penser à un sous-collier comme à un $(n,k)$-collier où il ne demeure que $k$ perles noires du collier original, les autres ayant été remplacées par des perles blanches. La question de la reconstructibilité peut d'ailleurs se poser en termes de personnes $k$-aveugles, qui souffrent d'une forme particulière de cécité qui les empêche de voir plus de $k$ boules noires à la fois, et qui doivent néanmoins pouvoir identifier (ou reconstruire) le collier complet. Il faut d'ailleurs distinguer entre les personnes $k$-$\mathbb{Z}_n$-aveugles qui ne peuvent qu'effectuer des rotations du collier et les personnes $k$-$\mathbb{D}_n$-aveugles qui peuvent également le retourner.

**Proposition 2.4.4.** *Soit $C$ un $(n,t)$-collier. Alors $C$ est $k$-$\mathbb{Z}_n$-reconstructible pour $k > \log_2(n)$ et $k$-$\mathbb{D}_n$-reconstructible pour $k > \log_2(2n)$*

*Démonstration.* Il suffit d'appliquer le corollaire 2.3.3 pour $X = \mathbb{Z}_n$, $Y = C$, avec $G = \mathbb{Z}_n$ (dans le premier cas) et $G = \mathbb{D}_n$ (dans le second cas). ∎

On peut améliorer ce résultat à l'aide du corollaire 2.3.2

**Proposition 2.4.5.** *Soit $C$ un $(n,t)$-collier. Alors, $C$ est $k$-$\mathbb{Z}_n$-reconstructible pour $k > 1 + \log_2(t)$ et $k$-$\mathbb{D}_n$-reconstructible pour $k > 1 + \log_2(2t)$*

*Démonstration.* On garde les notations de la preuve de la proposition précédente, et on prend $S = \{x\}$ ($x$ quelconque dans $\mathbb{Z}_n$), d'où $t = 1$ et $|G_S| = 1$ (identité) dans le cas de la $\mathbb{Z}_n$-reconstructibilité, $|G_S| = 2$ (identité et réflexion d'axe passant par $x$) dans le cas de la $\mathbb{D}_n$-reconstructibilité. La borne est donnée par le corollaire 2.3.2 ∎

On a donc obtenu une borne pour la reconstructibilité de chaque collier et également une borne pour l'indice de reconstructibilité de l'ensemble $\mathbb{Z}_n$ sur lequel agit $\mathbb{Z}_n$ ou $\mathbb{D}_n$ :

$$r_e(\mathbb{Z}_n, \mathbb{Z}_n) \leq \log_2(n) + 1 \text{ et } r_e(\mathbb{D}_n, \mathbb{Z}_n) \leq \log_2(2n) + 1$$

## 2.5 Cas général : groupe agissant sur un multi-ensemble

Dans ce cas, qui est le plus général possible, on ne dispose d'aucune donnée et une généralisation à partir des résultats de Mnukhin ([9]) ou de Alon, Caro, Krasikov et Roditty ([1]) semble malaisée. C'est donc, à notre connaissance, un problème ouvert et vraisemblablement peu étudié, car dans le cas le plus utile en pratique (où $G$ est un groupe abélien fini agissant sur lui-même par translation), on dispose d'une telle borne, que nous allons calculer dans le chapitre suivant.

# 3 Groupes abéliens finis

Ce chapitre est consacré à l'étude du cas particulier d'un groupe abélien fini $G$ agissant sur lui-même par translation. La démarche est fondée sur l'article de Luke Pebody [10] qui traite le cas des multi-ensembles de $G$ et qui réussit, non seulement à montrer que l'indice de reconstructibilité est borné asymptotiquement (contrairement à ce qu'avaient conjecturé beaucoup d'auteurs, pensant que cet indice restait faible en moyenne, mais était susceptible de prendre des valeurs élevées pour certains entiers), mais encore à donner la valeur exacte de cet indice pour tous les groupes abéliens finis. On suit la démonstration de Pebody en approfondissant certaines preuves, qui – quoique souvent techniques – nous paraissent révéler la puissance des concepts introduits. Inversement, nous omettrons quelques preuves faciles mais laborieuses qui ne nous paraissent pas indispensables pour la compréhension.

On s'intéresse donc aux groupes abéliens finis, dont on a vu en 1.4.1 une écriture canonique :

$$G \simeq \bigoplus_{j=1}^{t} \mathbb{Z}_{n_j}$$

$t$ est le rang du groupe $G$ et on a $n_{j-1} \mid n_j$ avec $n_1 > 1$.

## 3.1 Multiplicité d'un groupe

**Définition 3.1.1.** *Soient $x, y$ deux éléments de $G$. On dit qu'ils sont associés s'ils engendrent le même sous-groupe de $G$.*

**Proposition 3.1.2.** *Soit $g$ un élément d'ordre $n$. Les éléments associés à $g$ sont exactement les $\lambda g$ où $\lambda$ est premier avec $n$.*

*Démonstration.* On note $< g >$ le groupe engendré par $g$.

Soit $g'$ un élément associé à $g$. Alors $< g >=< g' >$ donc il existe $\lambda \in \mathbb{Z}$ tel que $g = \lambda g'$. Supposons par l'absurde que $\lambda$ ne soit pas premier avec $n$, soit $d$ leur PGCD. On a alors $\frac{n}{d} g = \frac{n}{d} \lambda g' = nkg' = 0$ car le groupe $< g' >$ est d'ordre $n$. Or $\frac{n}{d} < n$ et $g$ est alors d'ordre strictement inférieur à $n$, ce qui fournit une contradiction.

Réciproquement, soit $\lambda$ premier avec $n$. On définit le morphisme

$$\begin{array}{rccc} \phi & : & < g > & \longrightarrow & G \\ & & kg & \longmapsto & \lambda kg \end{array}$$

On a alors évidemment $|\mathrm{Im}(\phi)| \leq | < g > |$. De plus, par le théorème de Bézout, il existe $u$ et $v$ dans $\mathbb{Z}$ tels que $\lambda u + nv = 1$ soit $\lambda ug = g$ donc $g \in \mathrm{Im}(\phi)$ et ainsi $< g > \subset \mathrm{Im}(\phi)$. Finalement, $\mathrm{Im}(\phi) =< \lambda g >=< g >$. ∎

**Définition 3.1.3.** *Soit $h$ une fonction de $G$ dans $\mathbb{C}$. On dit que $h$ est auxiliaire si l'ensemble des zéros de $h$ est une union de classes d'éléments associés. De façon équivalente, $h$ est auxiliaire si*

$$h(x) = 0 \Longrightarrow h(y) = 0 \ \forall y \text{ associé à } x$$

**Définition 3.1.4.** *Étant donné une fonction auxiliaire $h$, on dit qu'un multi-ensemble $S$ est $h$-déséquilibré si*

$$\sum_{s \in S} s = 0 \text{ et } \prod_{s \in S} h(s) \notin \{0, 1\}$$

**Définition 3.1.5.** *Étant donné une fonction auxiliaire $h$, on dit que $h$ est triviale s'il n'existe pas de multi-ensemble $h$-déséquilibré.*

*Dans le cas contraire, on définit la multiplicité de $h$, $m(h)$ comme le cardinal du plus petit multi-ensemble $h$-déséquilibré.*

**Définition 3.1.6.** *On définit enfin la multiplicité du groupe $G$ par*

$$m(G) = \sup\{m(h) \mid h \text{ est une fonction auxiliaire non triviale de } G\}$$

Tout l'enjeu de cette section est alors d'une part de montrer que $m(G) = r(G)$ et d'autre part d'estimer $m(G)$. En réalité, on a besoin de raffiner un peu la définition de la multiplicité.

**Définition 3.1.7.** *Une fonction auxiliaire $h$ est dite forte si pour tout $x \in G$ tel que $h(x) \neq 0$, tout élément associé $\lambda x$ (avec $\lambda$ premier à l'ordre de $x$) vérifie $h(\lambda x) = h(x)^\lambda$. Dans le cas contraire, elle est dite faible.*

**Proposition 3.1.8.** *Une fonction auxiliaire triviale est forte.*

*Démonstration.* Soit $h$ une fonction auxiliaire triviale. Soit $x$ tel que $h(x) \neq 0$. Alors $-x$ est associé à $x$ donc $h(-x) \neq 0$. Or $x + (-x) = 0$ et $h$ étant triviale, l'ensemble $(x, -x)$ est $h$-équilibré donc $h(x)h(-x) \in \{0, 1\}$ et la valeur nulle étant exclue, $h(x)h(-x) = 1$. Donc $h(-x) = h(x)^{-1}$.

Soit maintenant $\lambda x$ un élément quelconque associé à $x$. Traitons le cas où $\lambda > 0$ (l'autre cas est similaire). On a

$$\lambda x - \underbrace{x - x - \cdots - x}_{\lambda \text{ fois}} = 0$$

Le multi-ensemble $(\lambda x, (-x)^\lambda)$ est $h$-équilibré donc $h(\lambda x)h(-x)^\lambda \in \{0, 1\}$. La valeur nulle est exclue car $\lambda x$ est associé à $x$ (avec $h(x) \neq 0$) donc $h(\lambda x)h(-x)^\lambda = 1$ et finalement $h(\lambda x) = h(x)^\lambda$ en utilisant $h(-x) = h(x)^{-1}$.

∎

On définit alors les multiplicités faible et forte d'un groupe.

$$m_1(G) = \sup\{m(h) \mid h \text{ est une fonction auxiliaire forte non triviale de } G\}$$

$$m_2(G) = \sup\{m(h) \mid h \text{ est une fonction auxiliaire faible de } G\}$$

## 3.2 Multiplicité faible

Il va s'agir dans ce paragraphe d'évaluer la multiplicité faible et de montrer qu'elle est toujours inférieure à l'indice de reconstructibilité du groupe.

Commençons par un lemme technique mais primordial d'artihmétique, dû à H.W. Lenstra (cité dans [10]).

**Lemme 3.2.1.** *Soient $k, m, n$ des entiers avec $n > 0, k > 1$. Si $n$ est impair ou $m - k$ est pair, alors il existe un multi-ensemble de $k$ entiers (comptés avec multiplicité) $S = \{a_1, \cdots, a_k\}$ tels que*

$$\sum_{i=1}^{k} a_i = m \quad et \quad \forall i \in \{1, \cdots, n\},\ a_i \wedge n = 1$$

*Démonstration.*

Cas 1 : $k = 2$

On décompose $n$ en produits de facteurs premiers, $n = \prod_{i=1}^{r} p_i^{k_i}$ où les $p_i$ sont des nombres premiers distincts et les $k_i$ des entiers strictement positifs.

Pour chaque $i$, on définit alors $x_i = \min\{x \in \mathbb{N}^* \mid p_i \not| (m - x)\}$. On a alors $x_i \in \{1, 2\}$ si bien que, si $p_i \neq 2$, $0 < x_i < p_i$ et donc $x_i$ n'est pas divisible par $p_i$. Dans le cas où $p_i = 2$, $n$ est nécessairement pair et donc l'hypothèse du lemme impose $m$ pair, si bien que $x_i = 1$ et là encore $0 < x_i < p_i$.

Par le théorème chinois, il existe un entier $x$ congru à $x_i$ modulo $p_i^{k_i}$ pour tout $i$. Alors aucun des $p_i$ ne divise $x$ ou $m - x$ si bien que le multi-ensemble $S = \{x, m - x\}$ a la propriété recherchée.

Cas 2 : $k > 2$

On a alors $n$ impair ou $m - (k - 2)$ pair, en conséquence directe de l'hypothèse du lemme. Ainsi, d'après le cas précédent, il existe un multi-ensemble $S$ de deux entiers premiers à $n$ et dont la somme est $m - (k - 2)$. On pose alors $T = S \cup \{1^{k-2}\}$ où on a ajouté $k - 2$ copies de l'entier 1 et $T$ a la propriété recherchée.

∎

On introduit les notations suivantes qui seront utiles pour la suite.

Étant donné un multi-ensemble d'entiers $S$, un élément $x$ de $G$ et une fonction auxiliaire $h$, on pose $\sum S = \sum_{s\in S} s$ et $h(S,x) = \prod_{s\in S} h(sx)$

**Proposition 3.2.2.** *Soit $h$ une fonction auxilaire. Supposons que pour tout $x \in G$ et pour tout multi-ensemble $S$ d'entiers premiers à l'ordre de $x$ avec $|S| \leq 6$ et $\sum S = 0$, on ait $h(S,x) \in \{0,1\}$. Alors $h$ est forte.*

*Par contraposée, on obtient donc que $m_2(G) \leq 6$.*

*Démonstration.* Soit $x \in G$ tel que $h(x) \neq 0$ (si on ne peut pas trouver un tel $x$, alors $h$ est nulle et donc forte) avec $x$ d'ordre $n$. Soit $\lambda x$ un élément associé à $x$ (on a donc $\lambda \wedge n = 1$), on doit donc montrer que $h(\lambda x) = h(x)^\lambda$.

D'après le lemme de Lenstra (3.2.1), pour tout entier $l$, il existe un multi-ensemble $S$ avec $|S| \leq 3$ (selon la parité de $l$, on peut prendre $|S| = 2$ ou $|S| = 3$) tel que $\sum S = l$ et chacun des éléments de $S$ est premier à $n$. On pose alors $f(l) = h(S,x)$ ; vérifions que cela définit bien une fonction de $\mathbb{Z}$ dans $\mathbb{C}$. Tout entier $l$ est accessible comme $\sum S$, mais on n'a pas unicité *a priori*.

Soit donc $T$ un multi-ensemble d'entiers premiers à $n$ avec $|T| \leq 3$ et $\sum T = \sum S = l$. On a alors $|S \cup (-T)| \leq 6$ et $\sum S \cup (-T) = 0$ et tous les entiers de $S \cup (-T)$ sont premiers à $n$ donc on a, par hypothèse, $h(S \cup (-T), x) \in \{0,1\}$. Or, $\forall \lambda \in S \cup (-T), \lambda x$ est associé à $x$ donc $h(\lambda x) \neq 0$. Ainsi $h(S \cup (-T), x) = 1$, soit $h(S,x) = h(T,x)$ par les mêmes calculs que dans la démonstration de 3.1.8 et $f$ est bien définie.

Montrons enfin que $\forall l, f(l+1) = h(x)f(l)$.

– $l$ est pair et donc s'écrit $l_1 + l_2$ où $l_1$ et $l_2$ sont premiers à $n$. Alors

$$\begin{aligned} f(l+1) &= h(\{l_1, l_2, 1\}, x) \\ &= h(\{l_1, l_2\}, x)h(x) \\ &= f(l)h(x) \end{aligned}$$

– $l$ est impair donc $l+1$ s'écrit $l_1 + l_2$ où $l_1$ et $l_2$ sont premiers à $n$. Alors

$$\begin{aligned} f(l+1) &= h(\{l_1, l_2\}, x) \\ &= h(\{l_1, l_2\}, x)h(x)h(-x) \\ &= h(\{l_1, l_2, -1\}, x)h(x) \\ &= f(l)h(x) \end{aligned}$$

∎

On peut, selon la même technique et en faisant une étude détaillée de cas,

améliorer ce résultat, en prouvant que $m_2(G) \leq k$ avec :

$$k = \begin{cases} 1 & \text{si } |G| = 1 \\ 2 & \text{si } G = \mathbb{Z}_2^n \\ 3 & \text{si } G \text{ est un groupe d'ordre impair} \\ 4 & \text{si } G \text{ est un groupe d'ordre pair non divisible par 3} \\ 6 & \text{si } G \text{ est un groupe d'ordre divisible par 6} \end{cases}$$

On a en fait mieux.

**Théorème 3.2.3.** *$m_2(G) = k \leq r(G)$ où $k$ est défini comme ci-dessus.*

*Démonstration.* On sait déjà que $m_2(G) \leq k$, il faut donc montrer que $k \leq m_2(G), r(G)$. On remarque que $m_2$ et $r$ sont des fonctions croissantes pour la relation d'ordre « est un sous-groupe de » et il suffit donc, pour chaque $k$ d'étudier les groupes minimaux pour cette relation d'ordre. Il s'agit alors à chaque fois d'exhiber des multi-ensembles qui ne sont pas $(k-1)$-reconstructibles et des fonctions auxiliaires faibles qui n'ont pas de multi-ensembles déséquilibrés de taille inférieure strictement à $k$.

Cas 1 : $k$=1

$r(\mathbb{Z}_1) \geq 1$ car les 0-decks de $\{0^1\}$ et de $\{0^2\}$ sont les mêmes. De plus, l'ensemble vide n'est déséquilibré pour aucune fonction auxiliaire.

Cas 2 : $k$=2

$r(\mathbb{Z}_2) \geq 2$ car les $\leq$ 1-decks de $\{0^2\}$ et de $\{0, 1\}$ sont les mêmes. De plus, la fonction $h$ définie par $h(0) = 1$ et $h(x) = -1$ sinon est auxiliaire avec aucun multi-ensemble $h$-déséquilibré de taille 1.

Cas 3 : $k$=3

$r(\mathbb{Z}_p) \geq 3$ (pour $p$ premier) car les $\leq$ 2-decks de $\{0, 1^2\}$ et de $\{0^2, 1\}$ sont les mêmes et les multi-ensembles ne sont pas dans la même orbite par translation. La fonction $h$ auxiliaire définie dans le point précédent n'admet pas de multi-ensemble $h$-déséquilibré de taille 1 ou 2.

Cas 4 : $k$=4

$r(\mathbb{Z}_2 p) \geq 4$ (pour $p$ premier) car les multi-ensembles

$$\{0^3, 1^4, 2^2, \cdots, (p-1)^2, p^1, (p+1)^0, (p+2)^2, \cdots, (2p-1)^2\}$$

et

$$\{0^2, 1^2, \cdots, (p-2)^2, (p-1)^0, p^1, (p+1)^2, \cdots, (2p-3)^2, (2p-2)^4, (2p-1)^3\}$$

ont les mêmes $\leq$ 3-decks (par symétrie) mais ne sont pas dans la même orbite par translation. De plus, la fonction auxiliaire $h$ définie par $h(0) = h(2) = 0$ et $h(1) = 3 = h(3)^{-1}$ n'admet pas de multi-ensemble déséquilibré de taille inférieure ou égale à 3.

Cas 5 : $k$=6

$r(\mathbb{Z}_6) \geq 6$ puisque les multi-ensembles

$$\{0^{11}, 1^{16}, 2^{13}, 3^5, 4^5, 6^3\}$$

et

$$\{0^{15}, 1^{15}, 2^8, 3^1, 4^1, 5^8\}$$

ont les mêmes $\leq$ 5-decks. Par ailleurs, la fonction auxiliaire définie par $h(2) = h(3) = h(4) = 0$ et $h(1) = 3 = h(5)^{-1}$ n'admet pas de multi-ensemble déséquilibré de taille inférieure ou égale à 5.

∎

## 3.3 Transformée de Fourier discrète

### 3.3.1 Principes

Nous allons maintenant tâcher d'évaluer la multiplicité forte d'un groupe. On va ainsi montrer que $m_1(G) \leq r(G)$. De plus, la transformée de Fourier discrète va permettre de construire des fonctions auxiliaires à partir de multi-ensembles non reconstructibles donnant ainsi l'inégalité inverse $r(G) \leq m(G)$.

L'outil très puissant que constitue la transformée de Fourier a été utilisé dans quasiment tous les articles qui traitent de la reconstructibilité (à l'exception notable des travaux de Mnukhin [7], [8], [9]). Par bijection, on travaille dans l'espace de Fourier, où les constructions et les propriétés apparaissent plus naturellement.

Pour pouvoir manipuler plus aisément la transformée de Fourier, il nous faut élargir la notion de multi-ensemble à celle de $\mathbb{Q}$-multiensemble, *i.e.* l'application $f$ définissant le multi-ensemble est désormais à valeurs dans $\mathbb{Q}$ et plus seulement dans $\mathbb{N}$. On élargit alors naturellement les notions de $k$-deck et de $k$-reconstructibilité. Toutefois, les notions obtenues ne sont pas plus générales, car si $f$ et $g$ ont le même $\mathbb{Q}$-$k$-deck, $q_1 f + q_2$ et $q_1 g + q_2$ ont le même $\mathbb{N}$-$k$-deck pour $q_1, q_2$ bien choisis dans $\mathbb{Q}$.

On a défini la transformée de Fourier discrète au paragaphe 1.4. On va toutefois en rappeler brièvement les principes.

On révèle la strucutre de groupe de rang $t$ de $G$. On a donc

$$G \simeq \bigoplus_{j=1}^{t} \mathbb{Z}_{n_j}$$

et on note $(i_1, i_2, \cdots, i_t)$ un élément de $G$ (avec $i_j$ considéré modulo $n_j$). À chaque $\mathbb{Q}$-multiensemble $f$, on peut alors associer le polynôme générateur de $f$ à $t$ variables :

$$P_f(x_1, x_2, \cdots, x_t) = \sum_{(i_1,\cdots,i_t)\in G} f(i_1, \cdots, i_t) \prod_{j=1}^{t} x_j^{i_j}$$

$G$ est abélien fini donc $G$ est canoniquement isomorphe à son dual $\Gamma = \widehat{G}$, on peut donc définir la transformée de Fourier d'un multi-ensemble $f$ comme l'application de $G$ dans $\mathbb{C}$ :

$$\mathcal{F}f(i_1, i_2, \cdots, i_t) = P_f(\omega_1^{-i_1}, \omega_2^{-i_2}, \cdots, \omega_t^{-i_t})$$

où $\omega_j = e^{\frac{2\pi}{n_j}}$. On a alors la formule d'inversion classique :

$$\mathcal{F}^{-1}\mathcal{F}f(i_1, i_2, \cdots, i_t) = |G| f(i_1, i_2, \cdots, i_t)$$

où

$$\mathcal{F}^{-1}g(i_1, i_2, \cdots, i_t) = P_g(\omega_1^{i_1}, \omega_2^{i_2}, \cdots, \omega_t^{i_t})$$

Il s'agit à partir de là de transcire les notions en termes de transformée de Fourier. Dans la suite, on notera $\widehat{f}$ pour $\mathcal{F}$.

**Proposition 3.3.1.** *Soient $f$ et $f'$ deux multi-ensembles. Alors $f_k = f'_k$ si et seulement si*

$$\sum_{i=1}^{k} g_i = 0 \Longrightarrow \prod_{i=1}^{k} \widehat{f}(g_i) = \prod_{i=1}^{k} \widehat{f'}(g_i)$$

*Démonstration.* Cette proposition est celle qui fournit la « traduction » dans l'espace de Fourier. On va la démontrer dans le cas où $G = \mathbb{Z}_n$, la généralisation étant technique et peu éclairante.

Soit donc $\omega = e^{\frac{2i\pi}{n}}$. Les caractères $\chi_m$ sont alors donnés par :

$$\chi_m(x) = \omega^{mx} \text{ pour } m \text{ variant de } 0 \text{ à } n-1$$

Soit $\mathfrak{P}$ une orbite de multi-ensembles de cardinal $k$ pour l'action de $\mathbb{Z}_n$ sur lui-même par translation. On peut trouver $g_1, \cdots, g_{k-1} \in \mathbb{Z}_n$ tels que $(0, g_1, \cdots, g_{k-1}) \in \mathfrak{P}$, et, par définition :

$$f_k(\mathfrak{P}) = \sum_{x\in\mathbb{Z}_n} f(x) f(x+g_1) \cdots f(x+g_{k-1})$$

Dans la suite de la démonstration, on note $f_k(g_1, \cdots, g_{k-1})$ pour $f_k([0, g_1, \cdots, g_{k-1}])$ où on a pris la classe modulo l'action de $\mathbb{Z}_n$ sur lui-même par translation. On prend alors la transformée de Fourier à $(k-1)$ variables du $k$-deck (en utilisant toujours l'isomorphisme canonique entre $\mathbb{Z}_n$ et son dual) :

$$\begin{aligned}
\widehat{f_k}(z_1, \cdots, z_{k-1}) &= \sum_{g_1, \cdots, g_{k-1} \in \mathbb{Z}_n} f_k(g_1, \cdots, g_{k-1}) \omega^{-g_1 z_1} \cdots \omega^{-g_{k-1} z_{k-1}} \\
&= \sum_{x \in \mathbb{Z}_n} \sum_{g_1, \cdots, g_{k-1} \in \mathbb{Z}_n} f(x) f(x+g_1) \cdots f(x+g_{k-1}) \omega^{-g_1 z_1} \cdots \omega^{-g_{k-1} z_{k-1}} \\
&= \sum_{x \in \mathbb{Z}_n} f(x) \left( \sum_{g_1 \in \mathbb{Z}_n} f(x+g_1) \omega^{-g_1 z_1} \right) \cdots \left( \sum_{g_{k-1} \in \mathbb{Z}_n} f(x+g_{k-1}) \omega^{-g_{k-1} z_{k-1}} \right) \\
&= \sum_{x \in \mathbb{Z}_n} f(x) \left( \widehat{f}(z_1) \omega^{z_1 x} \right) \cdots \left( \widehat{f}(z_{k-1}) \omega^{z_{k-1} x} \right) \\
&= \widehat{f}(z_1) \cdots \widehat{f}(z_{k-1}) \sum_{x \in \mathbb{Z}_n} f(x) \omega^{(z_1 + \cdots + z_{k-1}) x} \\
&= \widehat{f}(z_1) \cdots \widehat{f}(z_{k-1}) \widehat{f}(-(z_1 + \cdots + z_{k-1}))
\end{aligned}$$

Comme la transformée de Fourier est bijective, on a bien l'équivalence recherchée. ∎

**Proposition 3.3.2.** *Soient $f$ et $f'$ deux multi-ensembles. Alors $f$ et $f'$ sont dans la même orbite par translation si et seulement si il existe des racines $n_j$-èmes de l'unité $\mu_j$ telles que*

$$\widehat{f}(i_1, i_2, \cdots, i_t) = \widehat{f'}(i_1, i_2, \cdots, i_t) \prod_{j=1}^{t} \mu_j^{i_j}$$

*Démonstration.* Si $f'$ et $f$ sont dans la même orbite par translation, il existe $(x_1, \cdots, x_t) \in G$ tel que $f'(i_1, \cdots, i_t) = f(i_1 + x_1, \cdots, i_t + x_t)$ pour tout $(i_1, \cdots, i_t) \in G$. On obtient alors par le calcul le résultat classique :

$$\widehat{f'}(i_1, \cdots, i_t) = \widehat{f}(i_1, \cdots, i_t) \prod_{j=1}^{j=t} \omega_j^{-i_j x_j}$$

ce qui donne le résultat recherché avec $\mu_j = \omega_j^{-x_j}$.

Réciproquement, si

$$\widehat{f}(i_1, i_2, \cdots, i_t) = \widehat{f'}(i_1, i_2, \cdots, i_t) \prod_{j=1}^{t} \mu_j^{i_j}$$

on choisit $x_j$ donné par $\mu_j = \omega_j^{-x_j}$ et on a alors

$$\widehat{f}(i_1, \cdots, i_t) = \widehat{g}(i_1, \cdots, i_t)$$

où $g(i_1, \cdots, i_t) = f'(i_1 - x_1, \cdots, i_t - x_t)$ par les mêmes calculs que précédemment. Comme la transformée de Fourier est bijective, on a $g = f$ et donc $f$ et $f'$ sont dans la meme orbite par translation. ∎

### 3.3.2 Fonctions auxiliaires

On va maintenant pouvoir commencer à utliser la transformée de Fourier pour construire des fonctions auxiliaires.

**Lemme 3.3.3.** *Soit $f$ un multi-ensemble. Alors $\widehat{f}$ est auxiliaire.*

*De plus, si $f'$ est un multi-ensemble tel que $f_2 = f'_2$, alors $\widehat{f}$ et $\widehat{f'}$ ont les mêmes zéros.*

*Démonstration.* Soient $g'$ et $g$ deux éléments associés de $G$. Il s'agit de montrer que si $\widehat{f}(g) = 0$, alors $\widehat{f}(g') = 0$.

Soit $\mu$ l'ordre de $g = (i_1, \cdots, i_t)$. D'après le lemme 3.1.2, il existe un entier $\lambda$ premier avec $\mu$ tel que $g' = \lambda g$. D'après le théorème de la progression arithmétique de Dirichlet, il existe un nombre premier $\lambda'$ congru à $\lambda$ modulo $\mu$ et qui ne soit pas un facteur de $n_t$ (il suffit de choisir $\lambda'$ suffisamment grand, $n_t$ est l'ordre du dernier groupe cyclique apparaissant dans la décomposition de $G$). Alors, en posant

$$P(x) = P_f(x^{-\frac{n_t}{n_1} i_1}, \cdots, x^{-\frac{n_t}{n_t} i_t})$$

(qui est bien défini car $n_{j-1} \mid n_j \mid n_t$), on obtient $\widehat{f}(g) = P(\omega_t)$ et $\widehat{f}(g') = P(\omega_t^{\lambda'})$ (en effet, $\omega_t^{\frac{n_j}{n_t}} = \omega_j$).

Or $\omega_t$ et $\omega_t^{\lambda'}$ sont deux racines primitives $t$-èmes de l'unité, donc il existe un automorphisme $\sigma$ laissant $\mathbb{Q}$ invariant, tel que $\sigma(\omega_t) = \omega_t^{\lambda'}$, si bien que

$$P(\omega_t^{\lambda'}) = P(\sigma(\omega_t)) = \sigma(P(\omega_t))$$

donc $\widehat{f}(g) = 0$ implique $\widehat{f}(g') = 0$.

En particulier,

$$\widehat{f}(g) = 0 \Leftrightarrow \widehat{f}(-g) = 0 \Leftrightarrow \widehat{f}(g)\widehat{f}(-g) = 0$$

Or, si $f_2 = f'_2$, alors pour tout $g$, $\widehat{f}(g)\widehat{f}(-g) = \widehat{f'}(g)\widehat{f'}(-g)$ d'après 3.3.1 et finalement $\widehat{f}(g) = 0 \Leftrightarrow \widehat{f'}(g) = 0$. ∎

On introduit alors, pour deux $G$-multiensembles $f$ et $f'$ vérifiant $f_2 = f'_2$, la double fonction de Fourier $h_{f,f'}$ définie par

$$h_{f,f'}(x) = \begin{cases} \frac{\widehat{f}(x)}{\widehat{f'}(x)} & \text{si } \widehat{f'}(x) \neq 0 \\ 0 & \text{sinon} \end{cases} \tag{3.3.1}$$

On a alors immédiatement le fait qu'une double fonction de Fourier est auxiliaire. On va se servir de cette double fonction de Fourier pour caractériser la relation entre deux multi-ensembles. On a d'abord besoin d'un lemme technique sur les fonctions auxiliaires en général.

**Lemme 3.3.4.** *Une fonction auxiliaire $h : G \longrightarrow \mathbb{C}$ est triviale si et seulement si il existe des racines $n_j$-èmes de l'unité $w_j$ telles que pour tout $g = (g_1, \cdots, g_t) \in G$, $h(g) = \prod_{j=1}^{t} w_j^{g_j}$ ou $h(g) = 0$.*

*Démonstration.* Soit $h$ une fonction auxiliaire vérifiant la propriété énoncée. Pour montrer qu'elle est triviale, il s'agit de montrer qu'il n'existe pas de multi-ensemble $h$-déséquilibré.

Soit donc un multi-ensemble $S$ tel que $\sum_{s\in S} s = 0$. On cherche à déterminer la valeur de $\prod_{s\in S} h(s)$. On indice les éléments de $S$, $s^\alpha$ pour $\alpha \in \{1, \cdots, k\}$ (où $k = |S|$) et on les décompose selon la base de $G$ en $(s_1^\alpha, \cdots, s_t^\alpha)$.

- S'il existe $s^\alpha \in S$ tel que $h(s^\alpha) = 0$ alors le produit est nul est le multi-ensemble est équilibré.
- Supposons donc que $\forall \alpha \in \{1, \cdots, k\}, h(s^\alpha) \neq 0$. On a alors $h(s^\alpha) = \prod_{j=1}^{t} w_j^{s_j^\alpha}$ et

$$\begin{aligned} \prod_{s\in S} h(s) &= \prod_{\alpha=1}^{k} h(s^\alpha) \\ &= \prod_{\alpha=1}^{k}\prod_{j=1}^{t} w_j^{s_j^\alpha} \\ &= \prod_{j=1}^{t} w_j^{\sum_{\alpha=1}^{k} s_j^\alpha} \\ &= \prod_{j=1}^{t} w_j^{(\sum_{\alpha=1}^{k} s^\alpha)_j} \\ &= 1 \end{aligned}$$

Il n'existe donc pas de multi-ensemble $h$-déséquilibré, *i.e.* $h$ est triviale.

Réciproquement, supposons que $h$ est triviale. On note $(e_j)_{j\in\{1,\cdots,t\}}$ la base canonique du groupe $G$. On considère l'ensemble $Z(h) = \{x \in G \mid h(x) = 0\}$.

– $Z(h) = \emptyset$. Alors comme $h$ ne s'annule jamais, la condition de trivialité devient :

$$\sum_{s \in S} s = 0 \Longrightarrow \prod_{s \in S} h(s) = 1$$

Soit alors $g = (g_1, \cdots, g_t) \in G$. On a $g - g_1 e_1 - \cdots - g_t e_t = 0$ donc $h(g) = h(e_1)^{g_1} \cdots h(e_t)^{g_t}$. On pose $h(e_j) = w_j$ et de $n_j e_j = 0$, on tire $h(e_j)^{n_j} = 1$ et donc $w_j$ est bien une racine $n_j$-ème de l'unité.

– $Z(h)$ est non vide et on cherche alors à construire $h'$ auxiliaire triviale et qui coïncide avec $h$ partout sauf en certains points où $h$ s'annule mais pas $h'$. Par récurrence, on se ramène alors au cas précédent et en remontant, la propriété est donc vérifiée à chaque étape puisque $h$ s'annule ou bien est égale à un produit de la forme voulue.

• $G' = G \setminus Z(h)$ est un sous-groupe (strict) de $G$. Soit $x \in Z(h)$. Soit $\lambda$ minimal dans $\mathbb{N}^*$ tel que $\lambda x$ appartienne à $G'$ (un tel $\lambda$ existe bien car l'ensemble de tels entiers est non vide, en effet $|G|x = 0 \in G'$). On pose alors $h'(x)$ égal à n'importe quelle racine $\lambda$-ème de $h(\lambda x)$. Comme on veut que $h'$ soit triviale, elle doit être nécessairement forte, et du coup, on a défini les valeurs de $h'$ sur les éléments associés à $x$. Pour tous les autres éléments, $h'$ coïncide avec $h$ (il n'y a pas de conflit dans la définition car, $h$ étant auxiliaire et s'annulant en $x$, elle s'annulait également en tous les associés de $x$). $h$' est auxiliaire et il faut vérifier qu'elle est triviale. Le seul cas à considérer est celui d'un multi-ensemble de somme nulle comportant un nombre non nul de $x$ ou de ses associés (la présence d'autres éléments de $G \setminus G'$ donne automatiquement un produit nul).

$$n_0 x + n_1 \alpha_1 x + \cdots + n_k \alpha_k x + m_1 y_1 + \cdots + m_l y_l = 0$$

avec $n_0, \cdots, n_k, m_1, \cdots, m_l \in \mathbb{N}$; $\alpha_1 x, \cdots, \alpha_k x$ les associés de $x$ et $y_1, \cdots, y_l \in G'$.
En regroupant les termes en $x$, on aboutit à $\beta x \in G'$ donc $\lambda \mid \beta$ et en calculant la valeur de $h'$ sur les associés, on obtient

$$\begin{array}{rl} & h'(x)^{n_0} h'(\alpha_1 x)^{n_1} \cdots h'(\alpha_k x)^{n_k} \\ = & h'(x)^{n_0} h'(x)^{\alpha_1 n_1} \cdots h'(x)^{\alpha_k n_k} \\ = & h'(x)^{\beta} \\ = & h(\lambda x)^{\mu} \end{array}$$

On s'est donc ramené à la considération de multi-ensembles $h$-déséquilibrés qui n'existent pas car $h$ est triviale. Finalement, $h'$ est triviale.

• $G \setminus Z(h)$ n'est pas un sous-groupe de $G$. On pose alors

$$G' = < G \setminus Z(h) >$$

le sous-groupe de $G$ engendré par les $x$ tels que $h(x) \neq 0$. On définit alors $h'$ par :

$$h'(x) = \begin{cases} 0 & \text{si } x \notin G' \\ h(x_1) \cdots h(x_k) & \text{si } x = x_1 + \cdots + x_k \in G' \end{cases}$$

Il faut d'abord vérifier que $h'$ est bien définie. Soit $x \in G'$. On a alors une écriture de la forme $x = x_1 + \cdots + x_k$ avec $x_i \in G \setminus Z(h)$, mais il faut vérifier que la valeur de $h'$ ne dépend pas de cette écriture. Si $x = x_1 + \cdots + x_k = y_1 + \cdots + y_l$, alors $x_1 + \cdots + x_k - y_1 - \cdots - y_l = 0$. La trivialité de $h$ nous donne alors $h(x_1) \cdots h(x_k)h(-y_1) \cdots h(-y_l) \in \{0, 1\}$. Or la valeur 0 est à exclure puisque tous les $x_i$ et tous les $y_j$ sont dans $G \setminus Z(h)$ (et les $-y_j$ sont associés aux $y_j$). Finalement $h(x_1) \cdots h(x_k)h(-y_1) \cdots h(-y_l) = 1$ et donc $h(x) = h(x_1) \cdots h(x_k) = h(y_1) \cdots h(y_l)$.
Vérifions maintenant que $h'$ est triviale. Soit $S$ un multi-ensemble tel que $\sum S = 0$. On écrit chaque $s^\alpha$ sous la forme $s^\alpha = s^\alpha_1 + \cdots + s^\alpha_{k(\alpha)}$ et on a alors $\sum S = \sum_\alpha \sum_{i=1}^{k(\alpha)} s_i^\alpha$ et $\prod_{s \in S} s = \prod_\alpha \prod_{i=1}^{k(\alpha)} h(s_i^\alpha)$ si bien qu'on s'est ramené à la considération de multi-ensembles $h$-déséquilibrés qui n'existent pas car $h$ est triviale.

∎

On aboutit ainsi à une caractérisation très simple des multi-ensembles dans la même orbite par translation, en combinant les résultats des lemmes 3.3.3 et 3.3.4.

**Corollaire 3.3.5.** *Deux multi-ensembles $f$ et $f'$ vérifiant $f_2 = f'_2$ sont dans la même orbite par translation si et seulement si $h_{f,f'}$ est triviale.*

On peut alors comprendre le lien entre multiplicité et indice de reconstructibilité.

**Théorème 3.3.6.** *Soient $f$ et $f'$ deux multi-ensembles avec $f_2 = f'_2$. Alors $m(h_{f,f'}) = \inf\{k \mid f_k \neq f'_k\}$. Ainsi $r(G)$ est la multiplicité maximale d'une double fonction de Fourier non triviale.*

*Démonstration.* Dans la démonstration, on notera $h$ pour $h_{f,f'}$.

Remarquons d'abord que

$$h(x_1) \cdots h(x_k) = 0 \iff \widehat{f}(x_1) \cdots \widehat{f}(x_k) = \widehat{f'}(x_1) \cdots \widehat{f'}(x_k) = 0$$

$$h(x_1) \cdots h(x_k) = 1 \iff \widehat{f}(x_1) \cdots \widehat{f}(x_k) = \widehat{f'}(x_1) \cdots \widehat{f'}(x_k) \neq 0$$

Ainsi

$$h(x_1)\cdots h(x_k) \notin \{0,1\} \iff \widehat{f}(x_1)\cdots\widehat{f}(x_k) \neq \widehat{f'}(x_1)\cdots\widehat{f'}(x_k)$$

et il existe un multi-ensemble $\{x_1,\cdots,x_k\}$ (on ne suppose pas les $x_i$ distincts) $h$-déséquilibré si et seulement si $f_k \neq f'_k$ (en utilisant 3.3.1). ∎

On a encore besoin de deux lemmes techniques avant de pouvoir obtenir le résultat souhaité.

**Lemme 3.3.7.** *Soit $f$ une fonction auxiliaire forte et $x$ un élément d'ordre $k$. Alors $f(x)$ est nul ou bien est une racine $k$-ème de l'unité.*

*Démonstration.* Soit $x$ tel que $f(x) \neq 0$. Pour tout $\lambda$ premier à $k$, $\lambda x$ est associé à $x$ et $f(\lambda x) = f(x)^\lambda$. Mais on a également $(\lambda + k) \wedge k = 1$ donc $f((\lambda+k)x) = f(x)^{\lambda+k}$. Or $x$ est d'ordre $k$ donc $(\lambda+k)x = \lambda x$ et ainsi $f(x)^{\lambda+k} = f(x)^\lambda \neq 0$ donc $f(x)^k = 1$. ∎

**Lemme 3.3.8.** *Toute fonction auxiliaire forte est la transformée de Fourier d'un $\mathbb{Q}$-multiensemble. Par conséquent, toute fonction auxiliaire forte est une double fonction de Fourier.*

*Démonstration.* Soit $f$ une fonction auxiliaire forte. La relation d'équivalence « être associé » dans $G$ fournit une partition de $G$ en classes. Soit $C$ une telle classe, on considère la restriction de $f$ à $C$, $f_{|C}$. On a alors $f = \sum_C f_{|C}$ et $\widehat{f} = \sum_C \widehat{f_{|C}}$.

Soit $x = (x_1,\cdots,x_t) \in C$.

- Si $f(x) = 0$ alors $f_{|C} = 0$ ($f$ est auxiliaire) et $\widehat{f_{|C}} = 0$.
- Sinon, soit $k$ l'ordre de $x$. Les éléments de $C$ sont alors les $\lambda x$ pour $\lambda \wedge k = 1$ et $f(\lambda x) = f(x)^\lambda \neq 0$.

Soit alors $(i_1,\cdots,i_t) \in G$, on a :

$$\begin{aligned}
\widehat{f_{|C}}(i_1,\cdots,i_t) &= \sum_{(y_1,\cdots,y_t)\in G} f_{|C}(y_1,\cdots,y_t)\prod_{j=1}^{t}\omega_j^{-i_j y_j} \\
&= \sum_{(y_1,\cdots,y_t)\in G} f_{|C}(y_1,\cdots,y_t)\prod_{j=1}^{t}\omega_j^{-i_j y_j} \\
&= \sum_{\substack{1\leq\lambda\leq k\\ \lambda\wedge k=1}} f(x_1,\cdots,x_t)^\lambda \prod_{j=1}^{t}\omega_j^{-i_j\lambda x_j} \\
&= \sum_{\substack{1\leq\lambda\leq k\\ \lambda\wedge k=1}} \prod_{j=1}^{t}\left(f(x_1,\cdots,x_t)\omega_j^{-i_j x_j}\right)^\lambda
\end{aligned}$$

Or, $x$ est d'ordre $k$ donc $kx_j \equiv 0 \mod n_j$ soit $kx_j = \alpha_j n_j$ et $\left(\omega_j^{-i_j x_j}\right)^k = \omega_j^{-i_j \alpha_j n_j} = 1$. Donc $\omega_j^{-i_j x_j}$ est une racine $k$-ème de l'unité et d'après le lemme précédent, $f(x)\omega_j^{-i_j x_j}$ aussi.

On a donc une somme de la forme

$$\sum_{\substack{1 \leq \lambda \leq k \\ \lambda \wedge k = 1}} \xi^\lambda$$

où $\xi$ est une racine $k$-ème de l'unité. Des considérations arithmétiques et algébriques relativement simples permettent de montrer que cette somme est entière.

Finalement, $\widehat{f}$ est à valeurs entières et la formule d'inversion de Fourier nous donne

$$\begin{aligned} f &= \frac{1}{|G|}\mathcal{F}\mathcal{F}^{-1}f \\ &= \frac{1}{|G|}\mathcal{F}\mathcal{F}\check{f} \\ &= \mathcal{F}\left(\frac{1}{|G|}\mathcal{F}\check{f}\right) \end{aligned}$$

où $\check{f}$ est définie par $\check{f}(x) = f(-x)$ et est donc une fonction auxiliaire forte, pour laquelle les calculs précédents s'appliquent. Ainsi $\mathcal{F}\check{f}$ est à valeurs entières et $f$ est la transformée de Fourier d'un $\mathbb{Q}$-multiensemble. ∎

On arrive au théorème souhaité.

**Théorème 3.3.9.** *Soit $G$ un groupe abélien fini. Alors $m(G) = r(G)$.*

*Démonstration.* $r(G)$ est la multiplicité maximale d'une double fonction de Fourier non triviale (d'après le théorème 3.3.6).

$m(G)$ est la multiplicité maximale d'une fonction auxiliaire non triviale.

Comme les doubles fonctions de Fourier sont des fonctions auxiliaire, $m(G)$ est le maximum d'un ensemble plus grand donc $m(G) \geq r(G)$.

Ce maximum est atteint, soit $h$ une fonction auxiliaire non triviale avec $m(h) = m(G)$.

- Si $h$ est forte, alors $h$ est une double fonction de Fourier, d'après le lemme 3.3.8 et donc $m(G) = m(h) \leq r(G)$.
- Si $h$ est faible, alors d'après le théorème 3.2.3, $m(G) = m(h) \leq k \leq r(G)$.

∎

## 3.4 Multiplicité forte

La dernière étape consiste donc à évaluer la multiplicité forte d'un groupe. Pour cela, commençons par introduire deux nouveaux indices pour tout groupe abélien fini.

**Définition 3.4.1.** *Soit $S$ un sous-ensemble du groupe $G$. On dit qu'un élément $x$ est* redondant *par rapport à $S$ si $x$ est contenu dans le sous-groupe engendré par $S \setminus \{x\}$.*

*Un sous-ensemble qui ne contient pas d'éléments redondants est dit* essentiel.

*On définit alors $i(G)$,* l'indice essentiel *du groupe, par*

$$i(G) = \sup\{|S| \mid S \text{ est un sous-ensemble essentiel}\}$$

**Définition 3.4.2.** *Soit $S = \{x_1, \cdots, x_k\} \subset G$. On dit que $S$ est* indépendant *si*

$$x_i \neq 0 \ \forall i \quad et \quad \sum_{i=1}^{k} a_i x_i = 0 \Longrightarrow a_i x_i = 0 \ \forall i$$

*On définit alors $i'(G)$,* l'indice d'indépendance *du groupe, par*

$$i'(G) = \sup\{|S| \mid S \text{ est un sous-ensemble indépendant}\}$$

**Proposition 3.4.3.** *Pour tout groupe abélien fini $G$, on a $i(G) = i'(G)$.*

*Démonstration.* Soit $S$ un ensemble indépendant. Supposons par l'absurde qu'il ne soit pas essentiel. Il existe alors $x \in S$ redondant, et donc $x = \sum \alpha_i x_i$ et on obtient une combinaison linéaire non nulle entre éléments de $S$ ce qui contredit son indépendance. Ainsi

$$\{\text{Sous-ensembles indépendants}\} \subset \{\text{Sous-ensembles essentiels}\}$$

et $i'(G) \leq i(G)$.

Réciproquement, soit $T$ un ensemble essentiel. On définit une nouvelle notion pour les besoins de la démonstrations.

Étant donné un élément $x \in T$ et un élément $g \in G$, on dit que $g$ est $x$-évitable si $g$ est dans le groupe engendré par $T \setminus \{x\}$. Si $g$ est $x$-évitable pour tout $x$ dans $T$, on dit que $g$ est totalement évitable.

Comme $T$ est essentiel, aucun de ses éléments n'est totalement évitable.

Soit $H$ l'ensemble des éléments totalement évitables de $G$. $H = \bigcap_{x \in T} < T \setminus \{x\} >$ donc $H$ est un sous-groupe de $G$ comme intersection de sous-groupes. Soit $T' = \{x + H \mid x \in T\}$, on va chercher à montrer qu'il est indépendant dans le groupe quotient $G/H$, *i.e.* $\sum_{x \in T} a_x(x + H) = H \Longrightarrow$

$a_x(x+H) = H\ \forall x \in T$. Pour cela, il est nécessaire et suffisant de voir que si $\sum_{x\in T} a_x x \in H$ alors $a_x x \in H$ pour tout $x$.

Soit donc $a = \sum_{x\in T} a_x x$ totalement évitable et soit $x \in T$. Alors $a_x x$ est naturellement $y$-évitable pour tout $y \neq x$. De plus $a_x x = a - \sum_{y\neq x} a_y y$ est la différence entre deux éléments $x$-évitables donc est $x$-évitable. Finalement, $a_x x$ est totalement évitable.

$T'$ est donc un ensemble indépendant dans $G/H$, si bien que $|T'| \leq i'(G/H)$. Or $G/H$ est isomorphe à un sous-groupe $K$ de $G$ et l'isomorphisme transporte un ensemble indépendant de $G/H$ sur un ensemble indépendant de $K$ donc de $G$. Donc $i'(G/H) \leq i'(G)$.

De plus $|T'| = |T|$ car, dans le cas contraire, il existerait $x_i$ et $x_j$ tels que $x_i + H = x_j + H$ et donc $h \in H$ tel que $x_i = x_j + h$. Mais alors $x_j$ et $h$ sont $x_i$-évitable donc $x_i$ également, c'est-à-dire que $x_i$ est redondant dans $T$, ce qui fournit une contradiction.

Comme on peut réaliser cette construction pour tout ensemble essentiel $T$, on a finalement $i(G) \leq i'(G)$. ∎

On va maintenant faire le lien entre l'indice essentiel (ou d'indépendance) d'un groupe et sa multiplicité forte.

**Théorème 3.4.4.** *Soit $G$ un groupe abélien d'indice essentiel $i$. Soit $h$ une fonction auxiliare forte non triviale. Alors il existe un multi-ensemble $h$-déséquilibré d'au plus $i+1$ éléments distincts (on s'intéresse à l'ensemble sous-jacent au multi-ensemble).*

*Démonstration.* Par contraposée, il s'agit de prouver que si une fonction auxiliaire forte n'admet pas d'ensemble déséquilibré d'au plus $i+1$ éléments, alors elle est triviale.

Soit $S = \{x \mid h(x) \neq 0\}$. Alors, par définition de l'indice essentiel, il existe $T \subset S$ tel que $< T >=< S >$ avec $|T| \leq i$. On peut alors écrire chaque $x \in S$ sous la forme $x = \sum_{t\in T} f_x(t)t$.

$h(x) \neq 0$, $h(t) \neq 0$ et $x - \sum_{t\in T} f_x(t)t = 0$ donc $h(x)\prod_{t\in T} h(-t)^{f_x(t)} = 1$ (le multi-ensemble est équilibré car contenant au plus $i+1$ éléments distincts, et la valeur 0 est exclue) soit $h(x) = \prod_{t\in T} h(t)^{f_x(t)}$.

Soit maintenant un multi-ensemble $S'$ de $G$ vérifiant $\sum S' = 0$. On veut montrer que $S'$ est nécessairement équilibré. Si $\prod_{x\in S'} h(x) = 0$, $S'$ est équilibré. Dans le cas contraire, tous les éléments de $S'$ sont contenus dans $S$ (par définition de $S$), si bien que

$$\prod_{x\in S'} h(x) = \prod_{x\in S'}\prod_{t\in T} h(t)^{f_x(t)} = \prod_{t\in T} h(t)^{\sum_{x\in S'} f_x(t)}$$

Or on a

$$\sum_{t\in T}(\sum_{x\in S'} f_x(t))t = \sum S' = 0$$

et on s'est donc ramené à la considération d'un multi-ensemble comportant au plus $i$ éléments distincts, qui est donc équilibré. Ainsi $h$ n'admet aucun multi-ensemble déséquilibré et donc est triviale. ∎

Il s'agit maintenant de réussir à lier l'indice essentiel d'un groupe à sa structure. On a besoin pour cela de faire intervenir les sous-groupes de Sylow dont on rappelle la définition et les propriétés.

**Définition 3.4.5.** *Soit $p$ un nombre premier. On dit d'un groupe $H$ que c'est un $p$-groupe si son cardinal est une puissance de $p$.*

**Définition 3.4.6.** *Soit $G$ un groupe quelconque et $p$ un nombre premier. On définit un $p$-Sylow du groupe $G$ comme un $p$-sous-groupe maximal de $G$.*

**Théorème 3.4.7.** *Soit $G$ un groupe de cardinal $n = p^n s$ avec $p$ premier et $p \not| s$. Alors il existe un $p$-Sylow de $G$ d'ordre $p^n$.*

On peut alors caractériser l'indice essentiel d'un groupe en fonction de ses $p$-Sylow.

**Proposition 3.4.8.** *L'indice essentiel d'un groupe abélien $G$ est égal à la somme des rangs de tous ses sous-groupes de Sylow.*

*Démonstration.* Soit $j(G)$ la somme des rangs des sous-groupes de Sylow. On considère un ensemble indépendant $S$ de taille $i(G)$ pour lequel la somme des ordres des éléments est minimale. Pour un élément $x \in S$, on note $o(x)$ son ordre dans $G$.

On va montrer que tout élément de $S$ a un ordre égal à une puissance d'un nombre premier. Supposons que ce ne soit pas le cas, et soit $x \in S$ dont l'ordre est divisible par deux nombres premiers distincts $p$ et $q$. On a alors $px \neq 0$ et $o(px) < o(x)$ si bien que l'ensemble formé en remplaçant $x$ par $px$ dans $S$ n'est pas essentiel (s'il l'était, il contredirait la minimalité de $S$ pour la somme des ordres). Ainsi $px$ est dans le groupe engendré pas $S \setminus \{x\}$. De même, $qx$ est dans le groupe engendré pas $S \setminus \{x\}$. Or $p$ et $q$ étant premiers entre eux, par le théorème de Bézout, $x$ est dans le groupe engendré par $px$ et $qx$ donc dans le groupe engendré par $S \setminus \{x\}$, *i.e.* est redondant, ce qui fournit une contradiction.

Ainsi tous les éléments de $S$ sont d'ordre une puissance première et apparaissent ainsi dans un $p$-Sylow de $< S >$. Les différents éléments de $S$

qui apparaissent dans un $p$-Sylow sont alors nécessairement moins nombreux que le rang du $p$-Sylow par indépendance de $S$ et on a finalement $i(G) \leq j(< S >) \leq j(G)$.

Réciproquement, en considérant les sous-groupes de Sylow de $G$ et en formant l'union de familles génératrices minimales pour chacun de ces sous-groupes, on obtient un ensemble essentiel de taille $j(G)$ et alors $j(G) \leq i(G)$. ∎

On va maintenant pouvoir calculer la multiplicité forte des groupes. On commence par le cas le plus simple, celui des $p$-groupes et on reconstruit alors la multiplicité d'un groupe en fonction de ses $p$-groupes de Sylow.

On commence par remarquer, que pour le $p$-groupe de rang 1, $\mathbb{Z}_p$, la multiplicité forte $m_1(\mathbb{Z}_p) = -\infty$ car toute fonction auxiliaire forte est triviale (ce qu'on voit facilement à l'aide du lemme 3.3.7).

**Lemme 3.4.9.** *Soit $G$ un $p$-groupe de rang $t$. Alors $m_1(G) \leq 2t + 1$.*

*Démonstration.* Soit $h$ une fonction auxiliaire forte non triviale. D'après les lemmes 3.4.8 et 3.4.4, il existe un multi-ensemble déséquilibré avec au plus $t + 1$ éléments distincts. On considère un multi-ensemble déséquilibré qui minimise le nombre d'éléments distincts $r$. Posons $S = \{x_1, \cdots, x_r\}$ et $\lambda_1, \cdots, \lambda_r \in \mathbb{N}$ tels que $\sum \lambda_i x_i = 0$ et $\prod h(x_i)^{\lambda_i} \notin \{0, 1\}$. La minimalité de $r$ nous assure que pour tout $i \in \{1, \cdots, r\}, \lambda_i \neq 0$ et $h(x_i) \neq 0, 1$. On dispose pour l'instant d'un multi-ensemble de cardinal $\sum \lambda_i$. L'enjeu va être de garder la même somme et le même produit mais considérés comme émanant d'un nombre inférieur d'éléments.

On ne peut pas se contenter du multi-ensemble dont les éléments sont $(\lambda_i x_i)$ car on ne sait pas si $h(\lambda_i x_i) = h(x_i)^{\lambda_i}$. $h$ est forte mais cette égalité peut être prise en défaut si $\lambda_i$ n'est pas premier à l'ordre de $x_i$, en l'occurrence si $p$ divise $\lambda_i$ ($G$ est un $p$-groupe donc tous ses éléments, sauf 0, ont un ordre égal à une puissance de $p$).

Cas 1 : $r \leq t$

Pour chaque $i \in \{1, \cdots, r\}$, il existe d'après 3.2.1 un multi-ensemble d'entiers premiers à $p$, $S_i$ avec $|S_i| \leq 2$ et $\sum S_i = \lambda_i$. On pose alors $M = \bigcup_{i=1}^{r} \bigcup_{\mu_i \in S_i} (\mu_i x_i)$, multi-ensemble de cardinal au plus $2r$ vérifiant

$$\sum M = \sum_{i=1}^{r} \sum_{\mu_i \in S_i} (\mu_i x_i) = \sum_{i=1}^{r} \lambda_i x_i = 0$$

et

$$\begin{aligned}\prod_{i=1}^{r}\prod_{\mu_i\in S_i} h(\mu_i x_i) &= \prod_{i=1}^{r}\prod_{\mu_i\in S_i} h(x_i)^{\mu_i} \text{ car } h \text{ est forte et } \mu_i \wedge p = 1\\ &= \prod_{i=1}^{r} h(x_i)^{\lambda_i} \text{ car } \sum S_i = \lambda_i\\ &\neq 0, 1\end{aligned}$$

On dispose ainsi d'un multi-ensemble $h$-déséquilibré de cardinal $2r \leq 2t+1$ et donc $m(h) \leq 2t+1$.

Cas 2 : $r = t+1$

Si on effectue le même raisonnement que dans le cas précédent, on aboutit à $m(h) \leq 2(t+1)$ ce qui est plus grand que la borne que l'on cherche à obtenir. On va en fait utiliser l'indice d'indépendance de $G$ (égal au rang de $G$ car c'est un $p$-groupe). Ainsi, l'indice essentiel de $G$ est $t$ donc $S$, de cardinal $t+1$, contient un élément redondant. Quitte à permuter les indices supposons que $x_{t+1}$ est redondant, *i.e.* $x_{t+1} \in < S \setminus \{x\} >$. On peut donc trouver des $\alpha_j$ tels que $x_{t+1} = \sum_{j=1}^{t} \alpha_j x_j$.

Il faut alors distinguer deux sous-cas.

- $h(x_{t+1}) \neq \prod_{j=1}^{t} h(x_j)^{\alpha_j}$
  On utilise là encore, le lemme de Lenstra (3.2.1) et pour chaque $j \in \{1, \cdots, t\}$, on trouve un multi-ensemble d'entiers premiers à $p$, $S_j$ avec $|S_j| \leq 2$ et $\sum S_j = -\alpha_j$.
  On pose alors $M = \{x_{t+1}\} \cup \bigcup_{j=1}^{t} \bigcup_{\mu_j\in S_j} (\mu_j x_j)$ et on voit par le même raisonnement que précédemment que $M$ est un multi-ensemble $h$-déséquilibré de cardinal au plus $2t+1$.

- $h(x_{t+1}) = \prod_{j=1}^{t} h(x_j)^{\alpha_j}$
  On a alors

$$\sum_{j=1}^{t} (\lambda_j + \lambda_{t+1}\alpha_j) x_j = 0 \quad \text{et} \quad \prod_{j=1}^{t} h(x_j)^{\lambda_j + \lambda_{t+1}\mu_j}$$

  Toujours selon la même idée, on prend pour chaque $j$ un multi-ensemble d'entiers premiers à $p$, $S_j$ avec $|S_j| \leq 2$ et $\sum S_j = \lambda_j + \lambda_{t+1}\alpha_j$.
  On pose alors $M = \bigcup_{j=1}^{t} \bigcup_{\mu_j\in S_j} (\mu_j x_j)$ et on voit par le même raisonnement que précédemment que $M$ est un multi-ensemble $h$-déséquilibré de cardinal au plus $2t$.

On a donc dans tous les cas $m(h) \leq 2t+1$ donc $m_1(G) \leq 2t+1$.

On peut en fait améliorer le résultat précédent en prenant en compte de manière plus précise la structure de $p$-groupe.

**Lemme 3.4.10.** *Soit $G$ un $p$-groupe de rang $t$. Soit $k$ le rang du sous-groupe $pG$. Alors $m_1(G) \leq k + t + 1$.*

*Démonstration.* On a $k \leq t$, si $k = t$, il n'y a rien à montrer en utilisant le lemme précédent. Supposons donc que $k < t$.

La stratégie est la même qu'au lemme précédent. On sait d'après 3.4.8 et 3.4.4 qu'il existe un multi-ensemble déséquilibré avec au plus $t + 1$ éléments distincts. On considère un multi-ensemble déséquilibré qui minimise le nombre d'éléments distincts $r$. Posons $S = \{x_1, \cdots, x_r\}$ et $\lambda_1, \cdots, \lambda_r \in \mathbb{N}$ tels que $\sum \lambda_i x_i = 0$ et $\prod h(x_i)^{\lambda_i} \notin \{0, 1\}$. La minimalité de $r$ nous assure que pour tout $i \in \{1, \cdots, r\}, \lambda_i \neq 0$ et $h(x_i) \neq 0, 1$.

Comme $pG$ est de rang $k$, son indice essentiel est $k$ et le groupe engendré par les $px_j (1 \leq j \leq r)$ est engendré par seulement $k$ d'entre eux (au plus). Quitte à réordonner les éléments, on peut supposer que

$$< px_j \mid 1 \leq j \leq r >=< px_j \mid 1 \leq j \leq k >$$

Cas 1 : $\forall i > k, p \not| \lambda_i$

Alors, pour tout $i > k$, $\lambda_i x_i$ est associé à $x_i$ et vérifie donc $h(\lambda_i x_i) = h(x_i)^{\lambda_i}$. Pour $i \leq k$, on ne sait rien *a priori* et on utilise toujours la même technique à partir du lemme de Lenstra (3.2.1) qui permet de considérer $\lambda_i x_i$ comme la somme d'au plus deux éléments associés à $x_i$.

On a finalement $m(h) \leq (r - k) + (2k) = k + r \leq k + t + 1$.

Cas 2 : $\exists i > k, p \mid \lambda_i$

Choisissons un tel $i_0$. On a alors $\lambda_{i_0} x_{i_0} = \alpha p x_{i_0}$. Or $i_0 > k$ donc $px_{i_0} \in < px_1, \cdots, px_k >$. On peut donc trouver des entiers $\mu_j$ tels que $px_{i_0} = \sum_{j=1}^{k} \gamma_j p x_j$ d'où, en posant $\mu_j = \alpha\gamma_j$, $\lambda_{i_0} x_{i_0} = \sum_{j=1}^{k} \mu_j p x_j$.

Si $h(x_{i_0})^{\lambda_{i_0}} = \prod_{j=1}^{k} h(x_j)^{p\mu_j}$, alors, en posant $\lambda'_j = \lambda_j + p\mu_j$ pour $j \in \{1, \cdots, k\}$ et $\lambda'_j = \lambda_j$ pour $j > k, j \neq i_0$, on obtient

$$\sum_{j \neq i_0} \lambda'_j x_j = 0 \text{ et } \prod_{j \neq i_0} h(x_j)^{\lambda'_j} \notin \{0, 1\}$$

ce qui contredit la minimalité de $r$.

On a donc $h(x_{i_0})^{\lambda_{i_0}} \neq \prod_{j=1}^{k} h(x_j)^{p\mu_j}$, ce qui permet de constituer, selon la même technique, un multi-ensemble $h$-déséquilibré à partir

d'au plus deux associés de $x_{i_0}$ de somme $\lambda_{i_0} x_{i_0}$ et d'au plus deux associés pour chaque $x_j$ ($j \neq i_0$) de somme $-p\mu_j x_j$.
On a alors $m(h) \leq 2(k+1) \leq k+t+1$ (car on a $k < t$)

∎

On va en fait voir que ce résultat est optimal, dans le cas où $G \neq \mathbb{Z}_p$, *i.e.* $G$ n'est pas simple.

**Théorème 3.4.11.** *Soit $G$ un $p$-groupe de rang $t$, non simple. Soit $k$ le rang du sous-groupe $pG$.*
*Alors $m_1(G) = t + k + 1$.*

*Démonstration.* On dispose déjà de l'inégalité $m_1(G) \leq k + t + 1$.

$G$ contient un sous-groupe $H$ isomorphe à $\mathbb{Z}_{p^2}^k \oplus \mathbb{Z}_p^{t-k}$. De plus, $m_1(G) \leq m_1(H)$ donc il suffit d'étudier le cas où $G = \mathbb{Z}_{p^2}^k \oplus \mathbb{Z}_p^{t-k}$, ce que l'on fera dans la suite.

Soit $(e_1, \cdots, e_t)$ la famille génératrice canonique de $G$ telle que $e_1, \cdots, e_k$ sont d'ordre $p^2$ et $e_{k+1}, \cdots, e_t$ sont d'ordre $p$. On pose $\beta = p(e_1 + \cdots + e_k) + (e_{k+1} + \cdots + e_t)$ et $\omega = e^{\frac{2i\pi}{p}}$. On va chercher à définir une fonction auxiliaire forte non triviale $h$.

On pose $h(e_i) = 1$ et $h(\lambda) = \omega$. Comme $h$ est forte, cela définit naturellement $h$ sur les classes associées. Ainsi, pour tout $\mu$ que ne divise pas $p$, on a $h(\mu e_i) = 1$ et $h(\mu\lambda) = \omega^\mu$. Et cela est correctement défini, car $G$ n'étant pas simple, les classes de $\lambda$ et celles de chacun des $e_i$ sont disjointes. Dans tous les autres cas (*i.e.* pour toutes les autres classes), on pose $h(x) = 0$.

La fonction ainsi définie est évidemment auxiliaire et forte. Elle est non triviale car le multi-ensemble $\{\lambda, (-e_1)^p, \cdots, (-e_k)^p, (-e_{k+1}), \cdots, (-e_t)\}$ est $h$-déséquilibré.

Soit donc $T$ un multi-ensemble $h$-déséquilibré, on partitionne $T$ selon les classes associées : $T_j = \{x \in T \mid \text{ x est associé à } e_j\}$ pour $1 \leq j \leq t$ et $T_{t+1} = \{x \in T \mid x \text{ est associé à } \lambda\}$. On a ainsi tous les éléments de $T$ car si on avait un autre élément $x$, alors $h(x) = 0$, et $T$ ne serait pas déséquilibré.

On a alors $\prod_{t \in T_j} t = 1$ pour tout $1 \leq j \leq t$ et ainsi $\prod_{t \in T_{t+1}} t \notin \{0, 1\}$. Comme $h$ est forte, cela implique que $\sum T_{t+1} \neq 0$ (en effet, par contraposée, si la somme est nulle, comme il s'agit d'éléments associés à $x$, on arrive à $h(\lambda)^0 = 1$). Ainsi $\sum T_{t+1} = \lambda'$ est associé à $\lambda$ et $|T_{t+1}| \geq 1$. Comme les coefficients de $e_i$ dans $\lambda'$ sont non nuls, $|T_i| \geq 1$ pour tout $1 \leq i \leq t$. De plus les coefficients de $e_i$ dans $\lambda'$ sont des multiples de $p$ pour tout $1 \leq i \leq k$ et alors $|T_i| \geq 2$. Ainsi, $|T| \geq k + t + 1$ et donc $m_1(G) \geq m(h) \geq k + t + 1$. ∎

## 3.5 Résultat général

On connaît ainsi la multiplicité forte de tous les $p$-groupes et il s'agit alors de retrouver la multiplicité forte d'un groupe à partir de la multiplicité de ses sous-groupes de Sylow. On se contentera d'expliquer la démarche générale, sans rentrer dans les détails, très techniques et peu éclairants.

**Définition 3.5.1.** *Soient $G_1$ et $G_2$ deux groupes dont les ordres sont premiers entre eux. Soit $h$ une fonction auxiliaire forte sur $G_1$ et $\eta$ une fonction auxiliaire forte sur $G_1 \oplus G_2$.*

*On dit que $\eta$ est une $G_1 \oplus G_2$-extension de $h$ si*

$$\forall (g_1, g_2) \in G_1 \times G_2, \eta(g_1 + g_2) \neq 0 \Longrightarrow \eta(g_1 + g_2) = h(g_1)$$

*Si de plus,*

$$\forall g_1 \in G_1, h(g_1) \neq 0 \Longrightarrow \exists g_2 \in G_2, \eta(g_1 + g_2) = h(g_1)$$

*on dit que $\eta$ est une $G_1 \oplus G_2$-extension totale de $h$.*

**Définition 3.5.2.** *Soient $G_1$ et $G_2$ deux groupes dont les ordres sont premiers entre eux. On définit l'indice $\mu(G_1, G_1 \oplus G_2)$ comme la multiplicité maximale d'une $G_1 \oplus G_2$-extension totale non triviale d'une fonction auxiliaire forte de $G_1$.*

L'idée est alors, pour chaque $p$-Sylow de $G$, $S_p$, de considérer $\mu(S_p, G)$ puis de relier la multiplicité forte de $G$ à ces valeurs $\mu(S_p, G)$.

**Théorème 3.5.3.** *On note $p_i$ le $i$-ème nombre premier. On a alors $G = \bigoplus_i S_{p_i}$ et on note :*

- *$a_i$ le rang de $S_{p_i}$ (qui vaut 0 si $p_i$ ne divise pas $|G|$)*
- *$b_i$ le rang de $p_i S_{p_i}$*
- *$c_i = \sum_{j \neq i} a_j$ (cette somme est bien finie car la famille $(a_j)$ est presque nulle)*

$$\mu(S_{p_i}, G) = \begin{cases} -\infty & \text{si } S_{p_i} \text{ est simple} \\ d_i & \text{sinon} \end{cases}$$

*où*

$$d_i = \begin{cases} \min(a_i + b_i + 2c_i + 1, 2a_i + c_i + 2, 3a_i + 3) & \text{si } p_i = 2 \\ \min(a_i + b_i + c_i + 1, 2a_i + 2 & \text{sinon} \end{cases}$$

*Démonstration.* On écrit $G = S_{p_i} \oplus H_{p_i}$. On considère une fonction auxiliaire forte $h$ de $G$ et une $G$-extension totale $\eta$. Dans le cas où $S_{p_i}$ est simple, il suffit de voir que $\eta$ est nécessairement triviale ($h$ est elle-même triviale).

Dans les autres cas, on distingue selon la parité de $|S_{p_i}|$ en utilisant les résultats des lemmes 3.4.8 et 3.4.4 pour construire des multi-ensembles $\eta$-déséquilibrés de cardinal $d_i$. Ainsi, quelle que soit la $G$-extension totale, on borne supérieurement sa multiplicité et finalement on obtient un majorant de $\mu(S_{p_i}, G)$.

Dans un second temps, on révèle la structure des classes associées de $G$ montrant que, pour obtenir un multi-ensemble déséquilibré, on doit nécessairement faire apparaître au moins $d_i$ d'éléments, prouvant ainsi l'inégalité inverse. ∎

L'étape suivante consiste à montrer que le cas des groupes simples est particulier et que dans tous les autres cas, on récupère la multiplicité à partir des sous-groupes de Sylow.

On a besoin pour cela d'isoler un cas particulier.

**Définition 3.5.4.** *On dit qu'un groupe $G$ est* fin *s'il est de la forme $\mathbb{Z}_{2^k}$ pour $k \geq 2$, ou $\mathbb{Z}_{2^k 3^l}$ pour $k, l \geq 1$, ou $\mathbb{Z}_2 \oplus Z_{2.3^l}$.*

**Théorème 3.5.5.**

$$m_1(G) = \begin{cases} -\infty & \text{si } G \text{ est simple} \\ \max_i d_i & \text{sinon} \end{cases}$$

On combine ensuite ces résultats avec ceux obtenus pour la multiplicité faible et on obtient le résultat final

**Théorème 3.5.6.** *Soit $G$ un groupe abélien fini. Alors*

$$m(G) = r(G) = \begin{cases} \max_i d_i & \text{si } G \text{ n'est pas fin} \\ 4 & \text{si } G = \mathbb{Z}_{2^k} \text{pour } k \geq 2 \\ 6 & \text{sinon} \end{cases}$$

Précisons en particulier le résultat obtenu pour le cas de $\mathbb{Z}_n$ où $n \geq 1$.

**Corollaire 3.5.7.**

$$r(\mathbb{Z}_n) = \begin{cases} 1 & \text{si } n = 1 \\ 2 & \text{si } n = 2 \\ 3 & \text{si } n = p^k \text{ où } p \text{ est un nombre premier impair et } k \geq 1 \\ 3 & \text{si } n = pq \text{ où } p, q \text{ sont des nombres premiers impairs} \\ 4 & \text{si } n \text{ est n'importe quel autre nombre impair} \\ 4 & \text{si } n = 2^k \text{ où } k \geq 1 \\ 4 & \text{si } n = 2 \cdot p^k \text{ où } k \geq 1 \text{ et } p \text{ un nombre premier impair} > 3 \\ 5 & \text{si } n = 2^l \cdot p^k \text{ où } l > 1, k \geq 1 \text{ et } p \text{ un nombre premier impair} > 3 \\ 6 & \text{si } n \text{ est n'importe quel autre nombre pair} \end{cases}$$

# 4 Raffinement dans le cas d'ensembles de $\mathbb{Z}_n$

On a réussi à donner dans le chapitre précédent la valeur de l'indice de reconstructibilité pour tous les groupes abéliens finis. Il y a toutefois un cas particulier très fréquent, qui est celui des *ensembles* (et non multi-ensembles) de $\mathbb{Z}_n$ agissant sur lui-même par translation et il va s'agir d'estimer la reconstructibilité $r_e(\mathbb{Z}_n)$ dans ce cas particulier.

Ceux-ci ont déjà été présentés au paragraphe 2.4 où on évoquait des $(n,t)$-colliers (colliers de $n$ perles dont $t$ sont noires). Dans ce chapitre, on parlera de façon plus générale de $\mathbb{Z}_n$-colliers, car souvent l'information sur le nombre de perles noires n'est pas connue ou n'est pas pertinente. De plus, on se restreint à l'action de $\mathbb{Z}_n$ sur lui-même (et non de $\mathbb{D}_n$ sur $\mathbb{Z}_n$) donc il n'y a pas d'ambiguïté sur le groupe agissant.

On va voir que l'on peut obtenir des valeurs exactes de reconstructibilité qui sont un peu meilleures que celles données par le corollaire 3.5.7 (on a naturellement $r_e(\mathbb{Z}_n) \leq r(\mathbb{Z}_n)$). Plus précisément, on va raffiner un des cas que le corollaire 3.5.7 présente, celui qui donnait la valeur 4 pour « $n$ n'importe quel autre nombre impair ».

## 4.1 Joaillerie

Il s'agit dans ce paragraphe de donner des techniques qui vont permettre de construire des colliers ayant les mêmes $k$-decks mais n'étant pas isomorphes.

### 4.1.1 Résultats élémentaires

On commence par définir un indice qui va permettre de raffiner le cas impair.

**Définition 4.1.1.** *Soit $n \in \mathbb{N} \setminus \{0,1\}$ On définit $p(n)$ le nombre de facteurs premiers de $n$ comptés avec multiplicité.*

*Ainsi, en prenant la décomposition de $n$ en facteurs premiers, $n = \prod_i q_i^{k_i}$, on a $p(n) = \sum_i k_i q_i$.*

On a une borne supérieure sur $r_e(\mathbb{Z}_n)$ donnée par le corollaire 3.5.7, on va désormais donner des bornes inférieures.

**Proposition 4.1.2.**
- *Si $n > 3$, alors $r_e(\mathbb{Z}_n) \geq 2$*
- *Si $n > 5$, alors $r_e(\mathbb{Z}_n) \geq 3$*

*Démonstration.*

- $n > 3$
  Les colliers $\{0,1\}$ et $\{0,2\}$ ont le même 1-deck (cardinal) mais ils ne sont pas isomorphes (s'ils l'étaient, on aurait $n \mid 3$).
- $n > 5$
  Les colliers $\{0,1,3\}$ et $\{0,2,3\}$ ont les mêmes $\leq$ 2-decks. S'ils étaient isomorphes, il existerait $i$ tel que $i + \{0,1,3\} = \{0,2,3\} \mod n$. Alors $i \in \{0,2,3\}$ et $i+1 \in \{0,2,3\}$ donc $i = 2$ mais alors $i + 3 = 0 \mod n$, ce qui contredit $n > 5$.

∎

### 4.1.2 Techniques avancées

On suppose dans ce paragraphe que $n$ est un entier impair avec $p(n) \geq 4$ et que $n$ n'est pas une puissance de nombre premier. La décomposition de $n$ comporte donc au moins 4 nombres premiers (comptés avec multiplicité) dont au moins 2 sont distincts.

On peut donc écrire $n$ sous la forme $pqrs$ avec $r \wedge s = 1$ et $p, q, r, s > 2$. On conservera cette notation pour tout le paragraphe.

**Définition 4.1.3.** *Soit $m$ divisant $n$. On dit qu'un collier $S$ de $\mathbb{Z}_n$ est $m$-périodique si*

$$\forall x \in \mathbb{Z}_n, x \in S \iff x + m \in S$$

*On dit qu'un collier $S$ de $\mathbb{Z}_n$ est $m$-équilibré si le nombre d'éléments de $S$ équivalents à $i$ modulo $m$ est indépendant de $i$.*

**Définition 4.1.4.** *On considère $p$ $\mathbb{Z}_n$-colliers $S_0, \cdots, S_{p-1}$ et on définit le collier fusionné de $S_0, \cdots, S_{p-1}$, $F(S_0, \cdots, S_{p-1})$ comme le $\mathbb{Z}_{pn}$-collier contenant $px + i$ où $x \in S_i$ et $i$ varie de 0 à $p$.*

Remarque : Le procédé de fusion consiste à entremêler les colliers et non à les coller bout à bout, ce qui va permettre de construire des colliers intéressants.

**Proposition 4.1.5.** *Soient $S_1$ et $S_2$ deux colliers $q$-équilibrés de $\mathbb{Z}_{qrs}$. On suppose que $S_1$ est $qr$-périodique et que $S_2$ est $qs$-périodique.*

*On pose*

$$T_0 = F(\underbrace{S_1, S_2, \emptyset, \cdots, \emptyset}_{p \text{ colliers}})$$

*et*

$$T_1 = F(\underbrace{S_1 + 1, S_2, \emptyset, \cdots, \emptyset}_{p \text{ colliers}})$$

*Alors $T_0$ et $T_1$ ont les mêmes $\leq$ 3-decks.*

*Démonstration.* Soit $S$ un $\mathbb{Z}_n$-collier avec $|S| \leq 3$. Il s'agit de montrer que le nombre de $i$ tels que $S + i \subset T_a$ ne dépend pas de $a \in \{0, 1\}$.

Cas 1 : Les éléments de $S$ sont dans 3 classes distinctes modulo $p$

Alors il en est de même pour les éléments de $S + i$ pour tout $i$. Cependant ce n'est pas le cas pour $T_0$, ni pour $T_1$. Et le nombre des $i$ recherchés est 0.

Cas 2 : Les éléments de $S$ sont dans des classes non-consécutives modulo $p$

Alors il en est de même pour les éléments de $S + i$ pour tout $i$. Cependant ce n'est pas le cas pour $T_0$, ni pour $T_1$. Et le nombre des $i$ recherchés est 0.

Cas 3 : Tous les éléments de $S$ sont dans la même classe modulo $p$

Alors, quitte à translater $S$, on peut supposer que tous ses éléments sont des multiples de $p$, si bien qu'il existe un $\mathbb{Z}_{qrs}$-collier $S'$ tel que

$$S = F(\underbrace{S', \emptyset, \cdots, \emptyset}_{p \text{ colliers}})$$

Alors le nombre de copies de $S$ dans $T_a$ est égal à la somme du nombre de copies de $S'$ dans $S_1 + a$ d'une part et dans $S_2$ d'autre part. Le résultat est donc indépendant de $a$.

Cas 4 : Les éléments de $S$ sont dans deux classes consécutives modulo $p$

Alors, quitte à translater $S$, on peut supposer que tous ses éléments sont congrus à 0 ou 1 modulo $p$, si bien qu'il existe deux $\mathbb{Z}_{qrs}$-colliers $S'$ et $S''$ tels que

$$S = F(\underbrace{S', S'', \emptyset, \cdots, \emptyset}_{p \text{ colliers}})$$

On cherche alors à compter le nombre de $i$ tels que $i + S \subset T_a$. Or de tels $i$ sont exactement ceux de la forme $px$ avec $x + S' \subset S_1 + a$ et $x + S'' \subset S_2$.

Or $S_1$ est $qr$-périodique donc le prédicat $x + S' \subset S_1 + a$ ne dépend que de la classe de $x$ modulo $qr$. De même, le prédicat $x + S'' \subset S_2$ ne dépend que de la calsse de $x$ modulo $qs$.

De plus, $r \wedge s = 1$ donc à toute classe modulo $q$, on peut associer tous les couples possibles de classes induites modulo $qr$ et $qs$. Ainsi, le nombre de solutions de $i + S \subset T_a$ peut être calculé en sommant, pour $x$ parcourant les classes modulo $q$, le produit du nombre de solutions de $x + S' \subset S_1 + a$ par le nombre de solutions de $x + S'' \subset S_2$.

Or on a $|S| = |S'| + |S''| \leq 3$ donc $|S'| = 1$ ou $|S''| = 1$.

- $|S'| = 1$
  Alors, comme $S_1$ est $q$-équilibré, le nombre de solutions de $x + S' \subset S_1 + a$ est constant dans chaque classe modulo $q$, égal à $C$. Ainsi le nombre de solutions de $i + S \subset T_a$ est égal à $C$ fois le nombre de solutions de $x + S'' \subset S_2$ et ne dépend pas de $a$.
- $|S''| = 1$
  Alors, comme $S_2$ est $q$-équilibré, le nombre de solutions de $x + S'' \subset S_2$ est constant dans chaque classe modulo $q$, égal à $C'$. Ainsi le nombre de solutions de $i + S \subset T_a$ est égal à $C'$ fois le nombre de solutions de $x + S' \subset S_1 + a$ et ne dépend pas de $a$.

∎

**Lemme 4.1.6.** *Il existe des colliers $q$-équilibrés $S_1$ et $S_2$ de $\mathbb{Z}_{qrs}$ avec $S_1$ $qr$-périodique et $S_2$ $qs$-périodique et tels que*

$$T_0 = F(\underbrace{S_1, S_2, \emptyset, \cdots, \emptyset}_{p \text{ colliers}})$$

*et*

$$T_1 = F(\underbrace{S_1 + 1, S_2, \emptyset, \cdots, \emptyset}_{p \text{ colliers}})$$

*ne sont pas isomorphes.*

*Démonstration.* Soit $S_1$ (resp. $S_2$) l'ensemble des éléments de $\mathbb{Z}_{qrs}$ tels que le reste modulo $qr$ (resp. modulo $qs$) est inférieur strictement à $q$.

Considérons alors le nombre d'éléments $x$ tels que $x, x+1, x+p, x+p+1$ soient tous dans $T_0$. De tels $x$ sont de la forme $py$ où $y, y+1$ sont dans $S_1$ et dans $S_2$. Si $y$ est congru à $i$ modulo $q$, alors pour être dans $S_1$ (resp. dans $S_2$), il doit être congru à $i$ modulo $qr$ (resp. modulo $qs$). Ainsi, $y$ doit être égal à $i$ (modulo $qrs$). Or, la valeur $i = q - 1$ est la seule qui ne « fonctionne » pas car alors $y + 1 \notin S_1$ et $y + 1 \notin S_2$ (le reste modulo $qr$ resp. $qs$ est supérieur ou égal à $q$) Il y a donc $q - 1$ tels $x$.

De la même manière, les éléments $x$ tels que $x, x + 1, x + p, x + p + 1$ soient tous dans $T_1$ sont de la forme $py$ où $y, y + 1$ sont dans $S_2$ et $y, y - 1$ dans $S_1$. On a alors $y$ qui doit être égal à $i$ (modulo $qrs$) où $0 \leq i < q$. Pour $i = q - 1$, $y + 1 \notin S_2$ comme précédemment, mais si $i = 0$, alors $y - 1 \notin S_1$ (car $qrs - 1 = qr(s - 1) + (qr - 1)$ avec $qr - 1 \geq q$), si bien que l'on a seulement $q - 2$ tels $x$.

$T_0$ et $T_1$ n'ont pas le même 4-deck donc ne peuvent être isomorphes. ∎

**Corollaire 4.1.7.** *Soit $n$ un entier impair avec $p(n) \geq 4$ et qui ne soit pas une puissance d'un nombre premier.*

*Alors $r_e(\mathbb{Z}_n) \geq 4$*

On va maintenant chercher à améliorer l'indice de reconstructibilité par rapport à ce que donne le corollaire 3.5.7. Pour cela, on va utiliser un formalisme à base de polynômes.

## 4.2 Colliers polynomiaux

On a déjà vu en 1.3 et 1.4 qu'il pouvait être intéressant d'associer un polynôme (ou un pseudo-polynôme) à un multi-ensemble. Ici, on se restreint au cas de sous-ensembles de $\mathbb{Z}_n$. On va donc travailler avec des polynômes sur $\mathbb{Z}$ de degré au plus $n-1$ et à coefficients dans $\{0,1\}$.

En effet, étant donné un sous-ensemble $S$ de $\mathbb{Z}_n$, on lui associe le polynôme

$$P_S(x) = \sum_{i \in S} x^i$$

où l'on choisit les $i$ dans $\{0, \cdots, n-1\}$.

On note $\mathbb{U}_n$ l'ensemble des racines $n$-èmes de l'unité et $\mathbb{V}_n$ l'ensemble des racines primitives $n$-èmes de l'unité. On note $\Phi_n$ le $n$-ème polynôme cyclotomique, on a $\Phi_n(x) = \prod_{\xi \in \mathbb{V}_n}(x-\xi) \in \mathbb{Z}[x]$.

**Définition 4.2.1.** *Soit $S$ un sous-ensemble de $\mathbb{Z}_n$. On définit l'ensemble radical de $S$*

$$d(S) = \{i \in \mathbb{N} \setminus \{0,1\} \mid \ i \mid n \text{ et } \forall \xi \in \mathbb{V}_i, P_S(\xi) = 0\}$$

On va pouvoir caractériser les propriétés d'équilibre et de périodicité d'un $\mathbb{Z}_n$-collier à l'aide de l'ensemble radical.

**Théorème 4.2.2.** *Soit $k \mid n$. Alors un $\mathbb{Z}_n$-collier $S$ est $k$-équilibré si et seulement si $i \in d(S)$ pour tous les facteurs $i > 1$ divisant $k$.*

*$S$ est $k$-périodique si et seulement si $i \in d(S)$ pour tous les facteurs divisant $n$ qui ne divisent pas $k$.*

*Démonstration.* On effectue la division euclidienne de $P_S$ par $(x^k-1)$, $P_S = Q(x^k-1) + R$ avec $\deg R < k$.

Ainsi, pour $i \mid k, i > 1$, le coefficient de $x^i$ dans $R$ est égal à la somme des coefficients des $x^{i+kt}$ de $P_S$, qui est le nombre d'éléments de $S$ congrus à $i$ modulo $k$.

Donc $S$ est $k$-équilibré si et seulement si $R$ est un multiple scalaire de

$$\begin{aligned} 1 + x + \cdots + x^{k-1} &= \frac{x^k - 1}{x - 1} \\ &= \prod_{\substack{i \mid k \\ i \neq 1}} \Phi_i(x) \end{aligned}$$

Or $R$ est un multiple scalaire de $\frac{x^k-1}{x-1}$ si et seulement si $P_S$ l'est, ce qui par définition de l'ensemble radical, équivaut au fait que tous les facteurs de $k$, différents de 1 appartiennent à $d(S)$.

On pose $T_k(x) = 1+x^k+x^{2k}+\cdots+x^{n-k} = \frac{x^n-1}{x^k-1}$ et on effectue la division euclidienne de $P_S$ par $T_k$, $P_S = QT_k + R$ avec $\deg R < n-k$.

Alors $\deg Q = \deg P_S - (n-k) < k$. Plus précisément, si on pose $P_S = \sum_{i=0}^{n} a_i x^i$ (avec $a_i = 1$ si $i \in S$, $a_i = 0$ sinon), alors $Q = a_{n-1}x^{k-1}+a_{n-2}x^{k-2}+\cdots+a_{n-k}$ si bien que

$$R = \sum_{i=0}^{\frac{n}{k}-1}\sum_{j=0}^{k-1}(a_{ki+j} - a_{(n-k)+j})x^{ki+j}$$

et donc $R = 0$ si et seulement si $S$ est $k$-périodique. ∎

On va maintenant faire apparaître une propriété spécifique des ensembles radicaux.

**Proposition 4.2.3.** *Soient $p$ et $q$ deux nombres premiers distincts et soit $S$ un $\mathbb{Z}_{pq}$-collier. Si $pq \in d(S)$, alors $p \in d(S)$ ou $q \in d(S)$, c'est-à-dire que $S$ est $p$-périodique ou $q$-périodique.*

*Démonstration.* Comme $pq \in d(S)$, on a $\Phi_{pq} \mid P_S$. Or une racine est primitive $pq$-ème de l'unité si et seulement si elle est racine de $\frac{x^{pq}-1}{x^p-1}$ et de $\frac{x^{pq}-1}{x^q-1}$. Ainsi $\Phi_{pq} = \mathrm{PGCD}(\frac{x^{pq}-1}{x^p-1}, \frac{x^{pq}-1}{x^q-1})$.

Or $\mathbb{Z}[x]$ est un anneau euclidien donc il existe des polynômes $P_1$ et $P_2$ tels que $P_S = P_1\frac{x^{pq}-1}{x^p-1} - P_2\frac{x^{pq}-1}{x^q-1}$. On effectue alors la division euclidienne de $P_1$ par $\frac{x^p-1}{x-1}$, $P_1 = Q_1\frac{x^p-1}{x-1}+R_1$ avec $\deg R_1 < p-1$. De même, $P_2 = Q_2\frac{x^q-1}{x-1}+R_2$ avec $\deg R_2 < q-1$. Alors

$$P_S = (Q_1-Q_2)\frac{x^{pq}-1}{x-1} + R_1\frac{x^{pq}-1}{x^p-1} - R_2\frac{x^{pq}-1}{x^q-1} \tag{4.2.1}$$

Le degré de $P_S$ est au plus $pq-1$ donc $\deg(Q_1-Q_2) \leq 0$. Donc $Q_1-Q_2$ est une constante, que l'on note $\alpha$ dans la suite. Or les coefficients de $P_S$ sont dans $\{0,1\}$ donc il n'y a que deux possibilités pour la valeur de $\alpha$ : 0 ou 1.

Soient $i \in \{0,\cdots,p-1\}$ et $j \in \{0,\cdots,q-1\}$. D'après le lemme chinois, il existe un unique $k \in \{0,\cdots,pq-1\}$ tel que $k = i+pt$ $(0 \leq t < q)$ et $k = j+qu$ $(0 \leq u < p)$. On pose $R_1 = \sum_i a_i x^i$ et $R_2 = \sum_j b_j x^j$. Ainsi le coefficient de $x^k$ dans le membre de droite de 4.2.1 est égal à $\alpha + a_i - b_j$. Dans le membre de gauche, ce coefficient est 0 ou 1, il nous faut maintenant distinguer selon la valeur de $\alpha$.

- $\alpha = 0$
  Alors, pour tout $(i,j) \in \{0,\cdots,p-1\}\times\{0,\cdots,q-1\}$, $a_i \in \{b_j, b_j+1\}$. Or $b_{q-1} = 0$ et donc $a_i \in \{0,1\}$ pour tout $i$. De même, comme $a_{p-1} = 0$, $b_j \in \{-1,0\}$ pour tout $j$. Cependant, il est impossible qu'il existe un $i_0$ et un $j_0$ tels que $a_{i_0} = 1$ et $b_{j_0} = -1$ car alors le coefficient du $x^{k_0}$ correspondant serait égal à 2.
  Donc ou bien $a_i = 0$ pour tout $i$, auquel cas $R_1 = 0$ et $P_S$ est un multiple de $\frac{x^{pq}-1}{x^q-1}$ et donc $q \in d(S)$ ; ou bien $b_j = 0$ pour tout $j$, auquel cas $R_2 = 0$ et $P_S$ est un multiple de $\frac{x^{pq}-1}{x^p-1}$ et donc $p \in d(S)$. Or, si $q \in d(S)$, tous les facteurs de $pq$ qui ne sont pas des facteurs de $p$ sont dans $d(S)$ donc $S$ est $p$-périodique. De même, si $p \in d(S)$, $S$ est $q$-périodique.
- $\alpha = 1$
  Alors, pour tout $(i,j) \in \{0,\cdots,p-1\}\times\{0,\cdots,q-1\}$, $a_i \in \{b_j-1, b_j\}$. Or $b_{q-1} = 0$ et donc $a_i \in \{-1,0\}$ pour tout $i$. De même, comme $a_{p-1} = 0$, $b_j \in \{0,1\}$ pour tout $j$. Cependant, il est impossible qu'il existe un $i_0$ et un $j_0$ tels que $a_{i_0} = -1$ et $b_{j_0} = 1$ car alors le coefficient du $x^{k_0}$ correspondant serait égal à $-1$.
  La fin du raisonnement est similaire au cas précédent et on trouve alors également que $S$ est $p$-périodique ou $q$-périodique.

∎

On va maintenant pouvoir généraliser ce résultat.

**Proposition 4.2.4.** *Soient $p$ et $q$ deux nombres premiers distincts, soit $n > 1$ un entier quelconque. Soit $S$ un $\mathbb{Z}_{pqn}$-collier.*

*On suppose que $d(S)$ contient tous les facteurs de $n$ (sauf 1) et tous les facteurs de $pqn$ qui ne sont pas facteurs de $pn$ ou de $qn$. Alors $S$ est $pn$-périodique ou $qn$-périodique.*

*Démonstration.* On définit $S_0, S_1, \cdots, S_{n-1}$ des $\mathbb{Z}_{pq}$-colliers par $i \in S_j \Leftrightarrow (ni+j) \in S$. On a alors évidemment, $S = F(S_0, S_1, \cdots, S_(n-1))$, ce qui en notation polynomiale se traduit par

$$P_S(x) = \sum_{i=0}^{n-1} x^i P_{S_i}(x^n)$$

Tous les facteurs de $n$ (sauf 1) sont dans $d(S)$ donc, d'après le théorème 4.2.2, $S$ est $n$-équilibré, si bien que chaque $S_i$ contient le même nombre d'éléments. Si $|S_i| \equiv 0$ (resp. $|S_i| \equiv pq$), alors $S = \emptyset$ (resp. $S = \mathbb{Z}_{pqn}$) et dans les deux cas $d(S)$ contient tous les facteurs de $pqn$ (sauf 1) et la périodicité est évidente, il n'y a donc rien à montrer. Supposons dans la suite que $0 < |S_i| < pq$.

Si on considère un facteur de $pqn$, alors il est de la forme $pqk$ de $d(S)$, où $k$ est un facteur de $n$ (qui peut valoir 1), et on voit que toute racine $pqk$-ème primitive est une racine commune de $\frac{x^{pqn}-1}{x^{pn}-1}$ et de $\frac{x^{pqn}-1}{x^{qn}-1}$, et une racine de $P_S$ par définition de $d(S)$. Ainsi le PGCD de $\frac{x^{pqn}-1}{x^{pn}-1}$ et de $\frac{x^{pqn}-1}{x^{qn}-1}$ divise $P_S$. On peut donc trouver des polynômes $T$ et $U$ tels que

$$P_S = T\frac{x^{pqn}-1}{x^{pn}-1} + U\frac{x^{pqn}-1}{x^{qn}-1}$$

On décompose ensuite $T$ et $U$ de la même façon que ce que l'on a fait pour $S$, *i.e.* $T = \sum_{i=0}^{n-1} x^i T_i(x^n)$ et $U = \sum_{i=0}^{n-1} x^i U_i(x^n)$. On a alors

$$P_{S_i} = T_i\frac{x^{pq}-1}{x^{p}-1} + U_i\frac{x^{pq}-1}{x^{q}-1}$$

Ainsi $pq \in d(S_i)$ et donc, d'après la proposition 4.2.3, $S_i$ est $p$-périodique ou $q$-périodique. Or, la $p$-périodicité implique que le cardinal de l'ensemble est divisible par $p$. De même pour la $q$-périodicité. Comme $0 < |S_i| < pq$, $|S_i|$ ne peut être divisible par $p$ et par $q$ à la fois, il est donc divisible par un seul des deux nombres premiers, ce qui permet de caractériser sa période, en considérant seulement $|S_i|$ et donc indépendamment de $i$.

Finalement, $S_i$ est $p$-périodique pour tout $i$ ou bien $S_i$ est $q$-périodique pour tout $i$. Dans le premier cas, $S$ est alors $np$-périodique ; dans le second cas, $S$ est $nq$-périodique. ∎

## 4.3 Cas de $p^2q$

Soient $p$ et $q$ deux nombres premiers distincts. On dispose avec la proposition 4.1.2 d'une borne inférieure sur la reconstructibilité des $\mathbb{Z}_{p^2q}$-colliers. La borne plus fine donnée par le corollaire 4.1.7 ne s'applique pas car $p(p^2q) < 4$.

On a donc $r_e(\mathbb{Z}_{p^2q}) \geq 3$, on va montrer dans ce paragraphe que cette valeur est exacte. On va pour cela réutiliser les techniques utilisées avec les multi-ensembles (notamment le paragraphe 3.3). On commence par un résultat technique.

**Lemme 4.3.1.** *Soit $f$ une fonction auxiliaire forte de $\mathbb{Z}_n$ ($n$ quelconque). $f$ est triviale si et seulement si pour tous entiers $x, y, z$ vérifiant $xy \mid n, xz \mid n, y \wedge z = 1$ et $y, z > 1$, on a $f(xy)^z = f(xz)^y$ ou $f(xy)f(xz) = 0$.*

*Démonstration.* Supposons $f$ triviale. On considère $x, y, z$ comme dans l'énoncé du lemme. On utilise alors le lemme 3.3.4 qui affirme qu'il existe une racine $n$-ème de l'unité $\omega$ telle que $f(xy) = 0$ ou $f(xy) = \omega^{xy}$ et, de même, $f(xz) = 0$ ou $f(xz) = \omega^{xz}$.

Alors, soit $f(xy)f(xz) = 0$, soit $f(xy)^z = \omega^{xyz} = f(xz)^y$.

Réciproquement, on doit voir que si la propriété du lemme est vérifiée, alors il existe une racine $n$-ème de l'unité $\omega$ telle que pour tout $i \in \mathbb{Z}_n$, $f(i) \in \{0, \omega^i\}$. On suppose que $f(1) \neq 0$ et on pose alors $f(1) = \omega$.

Soit $i \in \{1, \cdots, n\}$.

- Si $i \wedge n = 1$, alors $i$ est associé à 1 et la force de $f$ suffit alors à montrer que $f(i) = f(1)^i = \omega^i$.
- Si $i \wedge n = d \neq 1$, alors $i$ est un multiple de $d$ donc l'ensemble engendré par $i$ dans $\mathbb{Z}_n$ est contenu dans celui engendré par $d$ ($< i > \subset < d >$). Or, d'après le théorème de Bézout, il existe $u, v$ entiers tels que $ui + nv = d$ donc dans $\mathbb{Z}_n$ $< d > \subset < i >$. Finalement, $d$ et $i$ engendrent le même sous-groupe de $\mathbb{Z}_n$ donc par définition, ils sont associés. Par force de $f$, il suffit donc de montrer le résultat pour $i \mid n$.
  Si $f(i) = 0$ il n'y a rien à montrer, sinon en prenant $x = 1, y = i, z = \alpha$ (où $\alpha$ est associé à 1 mais est différent de 1), on obtient : $f(i)^\alpha = f(\alpha)^i = \omega^{\alpha i}$ pour tout $\alpha$ premier à $n$ et différent de 1.
  Ainsi, $\frac{f(i)}{\omega^i}$ est une racine $\alpha$-ème de l'unité pour tout $\alpha$ premier à $n$ et différent de 1 et donc est égal à 1. On a bien alors $f(i) = \omega^i$.

Dans le cas où on ne suppose plus $f(1) \neq 0$, alors ou bien $f$ est identiquement nulle et il n'y a rien à montrer ou bien on trouve une classe associée pour laquelle $f$ ne s'annule pas et on procède au même raisonnement que ci-dessus pour les autres classes associées où $f$ ne s'annule pas. ∎

**Proposition 4.3.2.** *Soient $S_1$ et $S_2$ deux $\mathbb{Z}_{p^2q}$-colliers qui ont les mêmes $\leq 3$-decks mais qui ne sont pas dans la même orbite par translation. Soit $f$ leur double fonction de Fourier (cf. 3.3.1).*

*Alors $f(p)f(q) \neq 0$ et $f(p)^q \neq f(q)^p$. On a de plus $f(pq) = f(1) = 0$.*

*Démonstration.* D'après le corollaire 3.3.6, comme $S_1$ et $S_2$ ne sont pas dans la même orbite par translation, leur double fonction de Fourier est forte mais pas triviale. Ainsi, d'après le lemme 4.3.1, on peut trouver $x, y, z$ avec $y \neq 1, z \neq 1, y \wedge z = 1$ tels que $xy \mid p^2q, xz \mid p^2q$ et $f(xy)f(xz) \neq 0, f(xy)^z \neq f(xz)^y$.

On a donc $xyz \mid p^2q$ mais $xyz \neq p^2q$ sans quoi la force de $f$ entraînerait $f(xy)^z = 1 = f(xz)^y$. $y \neq 1, z \neq 1, y \wedge z = 1$ donc $y$ et $z$ doivent être respectivement une puissance de $p$ et une puissance de $q$. Finalement $\{y, z\} = \{p, q\}$ avec $x = 1$ et donc $f(p)f(q) \neq 0$ et $f(p)^q \neq f(q)^p$.

D'après le théorème 3.3.6, la multiplicité de $f$ est supérieure ou égale à 4, donc en particulier elle n'admet pas de multi-ensemble déséquilibré de cardinal 3. Ainsi, l'ensemble $\{p, -(p-1), -1\}$ est $f$-équilibré, donc $f(p)f(-(p-$

$1))f(-1) \in \{0,1\}$. Si $f(1) \neq 0$, comme $-1$ et $-(p-1)$ sont associés à 1 ($p \geq 3$), on a, par force de $f$, $f(-1) = f(1)^{-1}$ et $f(-(p-1)) = f(1)^{-(p-1)}$ et $f(p) \neq 0$. Finalement $f(p) = f(1)^{1+(p-1)} = f(1)^p$. De même, on montre que $f(q) = f(1)^q$.

On a alors, $f(p)^q = f(1)^{pq} = f(q)^p$, ce qui fournit une contradiction. Ainsi $f(1) = 0$.

En considérant l'ensemble $\{pq, -p(q-1), -p\}$, on montre de la même façon par l'absurde que $f(pq) = 0$. ∎

On va maintenant voir que de telles conditions sont en contradiction avec la proposition 4.2.4, ce qui permet de borner supérieurement l'indice de reconstructibilité.

**Corollaire 4.3.3.** $r(\mathbb{Z}_{p^2q}) = 3$

*Démonstration.* On sait déjà que $r(\mathbb{Z}_{p^2q}) \geq 3$. Supposons que $r(\mathbb{Z}_{p^2q}) > 3$. On peut alors trouver deux $\mathbb{Z}_{p^2q}$-colliers $S_1$ et $S_2$ qui ont les mêmes $\leq 3$-decks et qui ne sont pas dans la même orbite par translation.

Si $f$ est leur double fonction de Fourier, la proposition 4.3.2 nous donne $f(1) = f(pq) = 0$ et $f(p) \neq 0, f(q) \neq 0$. On remarque que $\widehat{S}_i(k) = P_{S_i}(\xi^k_{p^2q})$ où $\xi_{p^2q} = e^{\frac{2i\pi}{p^2q}}$. Or $\xi^k_{p^2q}$ est une racine primitive $\frac{p^2q}{k \wedge p^2q}$-ème de l'unité. Donc $\widehat{S}_i(k) = 0 \Leftrightarrow \frac{p^2q}{k \wedge p^2q} \in d(S_i)$.

Or, d'après le lemme 3.3.3, $\widehat{S_1}$ et $\widehat{S_2}$ ont les mêmes zéros donc $\widehat{S_1}(x) = 0 \Leftrightarrow \widehat{S_2}(x) = 0 \Leftrightarrow f(x) = 0$.

Ainsi, de $f(1) = 0$ on tire que $\frac{p^2q}{1 \wedge p^2q} = p^2q \in d(S_i)$. De $f(pq) = 0$, on tire que $\frac{p^2q}{pq \wedge p^2q} = p^{\in} d(S_i)$. $f(p) \neq 0$ et $f(q) \neq 0$ impliquent que $p^2, pq \notin d(S_i)$.

La proposition 4.2.4 s'applique avec $n = p : d(S_i)$ contient tous les facteurs de $p$ autres que 1 et tous les facteurs de $p^2q$ qui ne sont pas des facteurs de $p^2$ ou de $pq$. Ainsi les $S_i$ sont $p^2$-périodiques ou $pq$-périodiques donc $d(S_i)$ contient $pq$ ou $p^2$, ce qui fournit une contradiction. ∎

## 4.4 Cas de $pqr$

De la même façon, dans le cas où $n = pqr$ est le produit de trois nombres premiers distincts, on va pouvoir donner la valeur exacte de l'indice de reconstructibilité pour les ensembles. La démarche générale est la même que dans le paragraphe précédent, on considère deux $\mathbb{Z}_{pqr}$-colliers qui ont les mêmes $\leq 3$-decks mais qui ne sont pas dans la même orbite par translation. Soit $f$ leur double fonction de Fourier.

**Lemme 4.4.1.** *Il y a deux facteurs premiers de $pqr$ (disons $p$ et $q$ quitte à changer les notations) tels que $f(p)f(q) \neq 0$ et $f(p)^q \neq f(q)^p$. De plus, $f(pq) = f(1) = 0$.*

*Démonstration.* La démarche est la même que dans la démonstration du lemme 4.3.2. Comme $f$ est non triviale, on trouve $x, y, z$ tels que $xyz \mid pqr$ avec $y \neq 1, z \neq 1, y \wedge z = 1$ tels que $xy \mid pqr, xz \mid pqr$ et $f(xy)f(xz) \neq 0, f(xy)^z \neq f(xz)^y$.

On a alors $xyz < pqr$ donc $xyz$ a au plus deux facteurs premiers. Or $y$ et $z$ ont chacun au moins un facteur premier, donc on a $x = 1$ et quitte à changer les notations, on prend $y = p, z = q$ ($r$ est donc le facteur premier restant). Alors on a bien, $f(p)f(q) \neq 0$ et $f(p)^q \neq f(q)^p$.

On en déduit, de même qu'au lemme 4.3.2 que $f(pq) = f(1) = 0$. ∎

**Lemme 4.4.2.** $f(r) = 0$

*Démonstration.* $p$ et $q$ sont distincts donc premiers entre eux, donc on peut trouver d'après le théorème de Bézout $u$ et $v$ tels que $pu + qv = 1$. En posant $c = ur$ et $d = vr$, on a donc $r = pc + qd = p(c + qt) + q(d - pt)$ pour tout entier $t$. Or $r$ est premier impair et ne divise pas $q$ donc il existe un $t_0$ tel que $r \nmid c + qt_0$ et $r \nmid c + q(t_0 + 1)$. On pose alors $a = c + qt_0$ et $b = d - pt_0$.

Comme $r \nmid pa$, on a nécessairement $r \nmid qb$. De même, $q \nmid pa$ et $p \nmid qb$. Ainsi $\mathrm{PGCD}(qb, pqr) = q$ et donc $qb$ et $q$ sont associés (*cf.* démonstration du lemme 4.3.1) et $f(qb) = f(q)^b$ par force de $f$. De même, $f(pa) = f(p)^a$ et si l'on suppose que $f(r) \neq 0$, $f(-r) = f(r)^{-1}$.

Or, la multiplicité de $f$ étant strictement supérieure à 3, l'ensemble $\{pa, qb, -r\}$ est $f$-équilibré et donc on obtient, $f(r) = f(p)^a f(q)^b$ et de même

$$f(r) = f(p)^{a+q} f(q)^{b-p} = f(p)^a f(q)^b \frac{f(p)^q}{f(q)^p} = \frac{f(p)^q}{f(q)^p} f(r)$$

Or $f(p)^q \neq f(q)^p$ et on obtient donc une contradiction quant à la non-nullité de $f(r)$. ∎

On va maintenant voir que de telles conditions sont en contradiction avec la proposition 4.2.4, ce qui permet de borner supérieurement l'indice de reconstructibilité.

**Corollaire 4.4.3.** $r(\mathbb{Z}_{pqr}) = 3$

*Démonstration.* On sait déjà que $r(\mathbb{Z}_{pqr}) \geq 3$. Supposons que $r(\mathbb{Z}_{pqr}) > 3$. On peut alors trouver deux $\mathbb{Z}_{pqr}$-colliers $S_1$ et $S_2$ qui ont les mêmes $\leq 3$-decks et qui ne sont pas dans la même orbite par translation.

On a alors $f(x) = 0$ pour $x \in \{1, r, pq\}$ et $f(x) \neq 0$ pour $x \in \{p, q\}$ d'après les lemmes 4.2.2 et 4.2.3. On montre alors, de même que dans la démonstration du corollaire 4.3.3 que $r, pq, pqr \in d(S_i)$ et $pr, qr \notin d(S_i)$.

En prenant $n = r$, on voit que les hypothèses du corollaire 4.2.4 sont vérifiées donc $r(S_i)$ doit contenir $pr$ ou $qr$, ce qui fournit une contradiction. ∎

## 4.5 Résultat général

Il ne reste plus qu'à combiner les différents résultats des paragraphes précédents.

**Théorème 4.5.1.** *Soit $n$ un entier impair. Alors*

$$r(\mathbb{Z}_n) = \begin{cases} 1 \text{ si } n \in \{1, 3\} \\ 2 \text{ si } n \in \{5\} \\ 3 \text{ si } p(n) < 4 \text{ ou si } n \text{ est une puissance d'un nombre premier} \\ 4 \text{ sinon} \end{cases}$$

*Démonstration.* On a évidemment $r(\mathbb{Z}_1) = 1$. Si on se place dans $\mathbb{Z}_3$, deux colliers sont isomorphes si et seulement si ils ont le même cardinal, donc la connaissance du 1-deck est nécessaire et suffisante à la détermination d'un collier à translation près. Donc $r(Z_3) = 1$.

Si on se place dans $\mathbb{Z}_5$, des colliers contenant 0,1,4 ou 5 perles noires sont déterminés, à translation près, par leur cardinal donc le 1-deck suffit. Si un collier contient 2 perles noires, il est isomorphe à $\{0, 1\}$ ou à $\{0, 2\}$ qui ont le même 1-deck mais pas le même 2-deck. De même, si un collier contient 3 perles noires, il est isomorphe à $\{0, 1, 2\}$ ou à $\{0, 1, 3\}$ qui ont le même 1-deck mais pas le même 2-deck. Finalement, $r(\mathbb{Z}_5) = 2$.

Le troisième cas correspond aux entiers de la forme $p^k, pq, pqr$ ou $p^2q$. Les deux dernières possibilités ont été traitées dans les corollaires 4.3.3 et 4.4.3 respectivement. Dans les deux premières possibilités, on combine la borne inférieure donnée par la proposition 4.1.2 et la borne supérieure donnée dans le cas des multi-ensembles par le corollaire 3.5.7.

Pour le dernier cas, on combine la borne inférieure donnée par la proposition 4.1.2 et la borne supérieure donnée dans le cas des multi-ensembles par le corollaire 3.5.7. ∎

La question demeure alors de savoir ce qu'il en est du cas $n$ pair. On ne dispose pas à l'heure actuelle d'une meilleure valeur que celle donnée par le corollaire 3.5.7, même si la plupart des auteurs conjecturent que $r_e(\mathbb{Z}_n) = 4$.

Les techniques ci-dessus ne sont pas directement transposables car on a techniquement besoin du fait que les nombres premiers en jeu sont $> 2$. Cependant, Pebody propose une heuristique à la fin de son article [11] qui consiste à utiliser la même démarche générale que précédemment. On considère un ensemble $S$ non 4-reconstructible et on en déduit des propriétés pour l'ensemble radical $d(S)$ qui finissent par aboutir à une contradiction.

# Conclusion

On voit donc que la théorie de l'homométrie est très vaste et qu'elle met en œuvre des outils mathématiques très divers, de l'arithmétique à la combinatoire en passant par l'algèbre. Si la question de départ est relativement simple et naturelle, les objets et concepts pertinents sont loin d'être évidents. La lecture de la bibliographie révèle d'ailleurs le raffinement progressif du formalisme au fur et à mesure de l'avancement de cette théorie.

On a choisi ici de replacer le problème dans toute sa généralité (groupe agissant sur un multi-ensemble) et de donner des définitions qui sont formellement rigoureuses, même si on doit souvent les spécifier pour des raisons pratiques ou pour des cas particuliers.

Bien que le travail réalisé ait permis une synthèse des principaux résultats concernant la théorie de l'homométrie, avec le raffinement et la précision de certaines preuves, la théorie de l'homométrie est loin d'être une branche fermée des mathématiques. C'est pourquoi nous terminons par une liste de problèmes ouverts, que nous n'avons pu que survoler, l'assimilation des différents concepts et leur compréhension fine pour permettre cette synthèse avec complémentation des preuves lacunaires ayant été particulièrement exigeante.

- On a vu dans la première partie que la structure des multi-ensembles homométriques était bien déterminée dans le cas d'un groupe abélien sans élément d'ordre fini. La généralisation à un groupe abélien quelconque fait apparaître les unités spectrales dont la structure est encore mal connue, même si certains résultats ont pu être dégagés dans des cas particuliers ([2]).
- Comme nous l'avons mentionné à la fin de la deuxième partie, on ne dispose d'aucune estimation dans le cas le plus général de reconstructibilité qui est celui d'un groupe d'automorphismes agissant sur un multi-ensemble. Si les restrictions à un ensemble (au lieu d'un multi-ensemble) ou à un groupe abélien fini (au lien d'un groupe quelconque) ont pu être traitées, elles ne peuvent se généraliser simplement.
- Le cas le plus étudié en pratique, notamment en musicologie, est celui des ensembles de $\mathbb{Z}_n$. Si on a pu obtenir des valeurs exactes dans le cas où $n$ est impair, le cas de $n$ pair (crucial en musique, notamment pour $n = 12$) est toujours à l'état de conjecture.
- Enfin, la question la plus difficile et sur laquelle on dispose de très peu de résultats est la question duale de la reconstructibilité, celle de l'énumération de multi-ensembles ayant le même $k$-deck. Dans le cas du 2-deck et de $n = 12$, cette énumération a été effectuée dans des buts de classification. On dispose d'algorithmes permettant une telle

énumération dans des cas particuliers ([6]), mais cela ne nous renseigne pas sur la structure des multi-ensembles que l'on fait apparaître, et ne fournit pas d'heuristique pour le cas général.

# Remerciements

Je tiens à remercier Moreno Andreatta pour m'avoir permis d'effectuer un stage à la confluence de deux matières qui me tiennent particulièrement à cœur : la musique et les mathématiques. Je lui sais gré de la confiance qu'il m'a accordée pour mener à bien une tâche qui s'est avérée plus délicate que je ne l'escomptais.

Je salue également mes collègues de l'Ircam, du bureau aérien et du bureau souterrain, pour leur bonne humeur, leur sympathie et leur bienveillance.

Je souhaite remercier Claire Lestringant et Michel Multan qui ont toujours répondu très promptement à mes demandes d'article *via* la Bibliothèque de l'École Polytechnique et qui ont donc constitué une aide précieuse pour mon travail.

Enfin, je désire rendre hommage à Clément Gomez, à qui je dois une année mathématique riche et sympathique et qui demeure un ami attentif aux joies et déceptions du travail mathématique.

# Références


[1] N. Alon, Y. Caro, I. Krasikov, and Y. Roditty. Combinatorial reconstruction problems. *Journal of Combinatorial Theory Series B*, 47 :153–161, October 1989.

[2] Emmanuel Amiot. On the group of spectral units with finite order, May 2009.

[3] Allen Forte. *The Structure of Atonal Music*. Yale University Press, 1973.

[4] Philippe Jaming and Mihail N. Kolountzakis. Reconstruction of functions from their triple correlations. *New York Journal of Mathematics*, 9 :149–164, November 2003.

[5] Tamás Keleti and Mihail N. Kolountzakis. On the determination of sets by their triple correlation in finite cyclic groups, March 2006.

[6] John Mandereau. Etude des ensembles homométriques et leur application en théorie mathématique de la musique et en composition assistée par ordinateur. *Ircam/Université Paris 6*, June 2009.

[7] Valery B. Mnukhin. The k-orbit reconstruction and the orbit algebra. *Acta Applicandae Mathematicae*, 29 :83–117, November 1992.

[8] Valery B. Mnukhin. The reconstruction of oriented necklaces. *Journal of Combinatorics, Information and System Sciences*, 20 :261–272, November 1995.

[9] Valery B. Mnukhin. The k-orbit reconstruction for abelian and hamiltonian groups. *Acta Applicandae Mathematicae*, 52 :149–162, July 1998.

[10] Luke Pebody. The reconstructibility of finite abelian groups. *Combinatorics, Probability and Computing*, 13 :867–892, November 2004.

[11] Luke Pebody. Reconstructing odd necklaces. *Combinatorics, Probability and Computing*, 16 :503–514, July 2007.

[12] Joseph Rosenblatt. Phase retrieval. *Communications in Mathematical Physics*, 95 :317–343, September 1984.

[13] Joseph Rosenblatt. Reconstructing subsets of $\mathbb{Z}_n$. *Journal of Combinatorial Theory Series A*, 83 :169–187, August 1998.

[14] Joseph Rosenblatt and Paul D. Seymour. The structure of homometric sets. *SIAM. Journal on Algebraic and Discrete Methods*, 3 :343–350, September 1982.

[15] Marjorie Senechal. A point set puzzle revisited. *European Journal of Combinatorics*, 29 :1933–1944, November 2008.

[16] Steven S. Skiena, Warren D. Smith, and Paul Lemke. Reconstructing sets from interpoint distances (extended abstract). In *SCG '90 : Proceedings of the sixth annual symposium on Computational geometry*, pages 332–339, New York, NY, USA, 1990. ACM.

[17] Joseph N. Straus. *Introduction to Post-Tonal Theory.* Prentice Hall, 1990.