Quelques résultats combinatoires en théorie additive des nombres

Eric Balandraud

$N°$ d'ordre : 3159

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par **Éric BALANDRAUD**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : **Mathématiques Pures**

****

QUELQUES RÉSULTATS COMBINATOIRES EN THÉORIE ADDITIVE DES NOMBRES

****

Soutenue le 5 Mai 2006 à l'Institut de Mathématiques de Bordeaux

Après avis de :

F. HENNECART	Professeur, Université Jean Monnet (Saint-Etienne)	**Rapporteur**
G. ZÉMOR	Maître de conférences, École Nationale Supérieure des Télécommunications	**Rapporteur**

Devant la commission d'examen composée de :

Yu. BILU	Professeur, Université Bordeaux I	
J-M. DESHOUILLERS	Professeur, Université Victor Segalen (Bordeaux II)	**Directeur**
F. HENNECART	Professeur, Université Jean Monnet (Saint-Etienne)	**Président**
A. PLAGNE	Chercheur, École polytechnique	**Directeur**
O. SERRA	Professeur, Universitat Politècnica de Catalunya	
G. ZÉMOR	Maître de conférences, École Nationale Supérieure des Télécommunications	

- 2006 -

Remerciements

Je tiens en premier lieu à remercier Alain Plagne, qui m'a suivi tout le long de mon travail. Cela a été un réel plaisir de travailler avec lui. Je le remercie à la fois pour son sérieux et sa rigueur et aussi pour son humour et sa décontraction.

Je veux remercier aussi Jean-Marc Deshouillers, pour sa disponibilité et son aide pour l'achèvement de cette thèse.

Un remerciement particulier va à François Hennecart qui m'a initié à l'étude de la théorie additive des nombres lors de mon D.E.A. et qui s'est intéressé à mon travail tout au long de ma thèse.

Merci aussi à Oriol Serra dont un résultat sur la coloration des groupes finis est à l'origine de la première partie de ma thèse.

Je remercie Gilles Zémor pour tout le temps et l'intérêt qu'il a consacré à la lecture de mon travail.

Enfin, je veux remercier Yuri Bilu pour sa disponibilité et sa patience.

Durant ces trois années de thèse, j'ai eu l'occassion d'apprendre beaucoup. Si l'on apprend par la lecture et l'étude, on apprend aussi autour d'une tasse de café. Je remercie tous ceux qui m'ont fait le plaisir de partager leurs connaissances et un peu de café avec moi. Il s'agit principalement de mes directeurs de thèse, mais aussi d'autres professeurs de l'université Bordeaux 1, et évidemment de mes collègues thésards.

Mes amis et proches ont été non seulement témoins de mes efforts, mais aussi acteurs par leur soutien et leurs encouragements. Je veux les remercier. Il y a les amis de longue date : Gaëlle, Alex mon logeur parisien, David, Elsa et Michal, mon voisin et ma voisine Christophe et Séverine. Il y a aussi toute la petite bande de triathlètes, qui m'ont aussi appris beaucoup, et les autres amis bordelais Audrey, Lénaïk et Olivier. Merci à Nelly pour son écoute, son amitié et ses opinions cinématographiques.

Je remercie particulièrement mes camarades thésards Mourad, Florent et Matthieu, qui ont suivi tous les détails en direct. Il y a tant de choses pour lesquelles, je peux les remercier : les conversations, les mathématiques, les concerts, les heures de badminton, les crêpes, les blagues...

Il m'est très agréable de remercier toute ma famille, en particulier ma petite cousine Cécile toujours prête à m'écouter, mon frère Joël, ma belle-sœur Virginie et ma petite nièce Laure. Merci finalement à ma mère pour ses attentions et son soutien permanent. Une pensée particulière me vient pour mon père, avec qui j'aurais apprécié de partager ces moments.

Table des matières

INTRODUCTION

Cette thèse comporte deux parties indépendantes. La première partie traite d'un problème de coloration dans les groupes finis. La seconde développe une méthode dite isopérimétrique liée à la théorie additive des nombres et plus précisément à la théorie d'addition d'ensembles dans les groupes. La thèse est composée de trois articles (soumis pour publication) et de compléments dans chaque partie.

Le premier chapitre présente un résultat lié à la théorie de Ramsey[(1)]. Cette théorie étudie les colorations d'objets mathématiques (arêtes ou sommets d'un graphe, entiers naturels, éléments d'un groupe...). Les résultats classiques de théorie de Ramsey prouvent l'existence ou estiment le nombre de sous-objets monochromatiques. Par exemple, le théorème de Van der Waerden[(2)] montre que, pour tout entier k, il existe un entier n, tel que toute coloration des entiers de 1 à n contient une progression arithmétique monochromatique de longueur k. Des résultats d'un genre nouveau sont apparus ces dernières années, ils sont parfois appelés anti-Ramsey ou Ramsey arc-en-ciel, il s'agit cette fois de donner des conditions impliquant l'existence de sous-objets arc-en-ciel (c'est-à-dire comportant des couleurs distinctes). Ainsi en 2003, Jungić et Radoičić[(3)] ont montré que pour toute coloration en trois couleurs des entiers de 1 à $3n$ telle que chaque classe de couleur contienne n éléments, il existe une progression arithmétique à trois termes arc-en-ciel.

---

(1) R. Graham, B. Rothschild, J.H. Spencer, *Ramsey theory*, John Wiley and sons, New-York, 1980.

(2) B. L. Van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. **15** (1927), 212-216.

(3) V. Jungić, R. Radoičić, *Rainbow 3-term arithmetic progressions*, Integers **3** (2003), A18.

Une découverte de Datskovsky[4] de 2003 montre que le nombre de triplets de Schur ((x, y, z) tel que $x + y = z$) monochromatiques dans une coloration de $\mathbb{Z}/n\mathbb{Z}$ en deux couleurs, ne dépend pas de la distribution des couleurs mais uniquement des cardinaux des classes de couleurs. Par la suite, Cameron, Cilleruelo et Serra[5] donnèrent une généralisation de ce phénomène combinatoire pour des équations généralisant les équations linéaires dans les groupes finis colorés avec deux couleurs. Ils donnèrent en application des bornes inférieures pour les nombres de progressions arithmétiques à trois ou quatre termes monochromatiques dans des groupes finis colorés avec trois ou quatre couleurs. Un autre type d'applications leur permet de déterminer le nombre de triplets pythagoriciens dans $\mathbb{Z}/p\mathbb{Z}$, avec p premier et de calculer le symbole de Legendre de -1 et de 2 modulo p.

Dans la première partie de cette thèse, nous considérons une coloration quelconque d'un groupe fini et une équation que l'on supposera régulière en un certain sens (qui comprend les équations classiques : équation de Schur $x+y-z = 0$ et de Sidon $x + y - z - t = 0$). Nous donnons une généralisation de l'idée qui permit à Cameron, Cilleruelo et Serra de prouver que le nombre de solutions monochromatiques ne dépend que des cardinaux des classes de couleurs pour une coloration en deux couleurs. En considérant les nombres de solutions correspondant aux différentes colorations possibles des solutions de l'équation, nous montrons qu'il existe des combinaisons linéaires entre ces nombres qui ne dépendent que des cardinaux des classes de couleurs et pas de la répartition des couleurs. Qui plus est, ces combinaisons linéaires s'expriment de manière parallèle en combinaisons linéaires des cardinaux des classes de couleurs. Par exemple, pour une équation à trois variables dans un groupe de cardinal n coloré avec trois couleurs (A, B, C), le nombre de solutions monochromatiques moins la moitié du nombre de solutions arc-en-ciel vaut exactement :

$$\frac{1}{n}(|A|^3 + |B|^3 + |C|^3 - 3|A||B||C|).$$

Cela établit une relation entre les résultats de type Ramsey et les résultats de type anti-Ramsey.

Des applications sont données d'une part au décompte de progressions arithmétiques à trois termes arc-en-ciel dans un groupe coloré avec trois couleurs, chaque couleur apparaissant le même nombre de fois ; d'autre part au décompte de points sur une conique quelconque dans un corps fini. Le résultat est aussi généralisé à des systèmes d'équations.

---

[4] B.A. Datskovsky, *On the number of monochromatic Schur triples*, Adv. in Appl. Math. **31** (2003), 193-198.

[5] P. Cameron, J. Cilleruelo, O. Serra, *On monochromatic solutions of equations in groups*, preprint, (2005).

Le second chapitre se place dans le contexte de la théorie additive des nombres et plus particulièrement de la théorie d'addition d'ensembles. Il s'agit d'étudier dans un groupe, les ensembles finis A et B de "petite somme", c'est-à-dire tels que $|A+B| < |A| + |B| - 1$, où $A+B$ est l'ensemble des éléments de la forme $a+b$, avec $a \in A$ et $b \in B$. Le théorème de Cauchy-Davenport établit que de tels ensembles n'existent dans les groupes $\mathbb{Z}/p\mathbb{Z}$, avec p premier, que si $|A+B| = p$. C'est le premier résultat de ce domaine. Il a été établi par Cauchy[6] en 1813, qui l'utilisa pour montrer que dans $\mathbb{Z}/p\mathbb{Z}$ tout élément est somme de k puissances k-ièmes. Davenport[7] redémontra le théorème en 1935, ignorant le travail de Cauchy. Ce n'est qu'en 1947 que Davenport[8] réalisa que Cauchy l'avait devancé.

Dans le cas des groupes $\mathbb{Z}/p\mathbb{Z}$, avec p premier, le théorème de Vosper décrit la structure des ensembles A et B tels que leur somme soit de cardinal minimal, $|A+B| = |A| + |B| - 1$. Dans un groupe cyclique quelconque et sous certaines contraintes sur l'ensemble B, Chowla montra qu'il ne pouvait y avoir de petite somme. Dans un groupe abélien fini G, une généralisation du théorème de Cauchy-Davenport fut obtenue par Mann : elle fait apparaître les sous-groupes finis de G.

Le théorème de Kneser[9] démontré en 1955, montre que si A et B sont deux sous-ensembles d'un groupe abélien quelconque G, tels que $|A+B| < |A| + |B| - 1$ alors l'ensemble $A+B$ est périodique (i.e. il existe un sous-groupe fini $H \neq \{0\}$ tel que $H + A + B = A + B$). Ce théorème s'est depuis révélé être un outil majeur en théorie additive des nombres, notamment au travers de ses nombreuses applications. Il se démontre classiquement par des méthodes de transformation des ensembles A et B. Par exemple, la transformée de Cauchy-Dyson associe à la paire (A,B) et $e \in A - B$, la paire $(A(e), B(e))$ telle que $A(e) = A \cup (B+e)$ et $B(e) = B \cap (A-e)$. Les propriétés de cette transformation et un raisonnement par récurrence permettent de conclure. Cependant ces méthodes ne sont pas descriptives et ne donnent que peu d'idées des ensembles considérés.

---

[6] A.-L. Cauchy, *Recherches sur les nombres*, J. Ecole Polytech. **9** (1813), 99-116.
[7] H. Davenport, *On the addition of residue classes*, J. Lond. Math. Soc. **10** (1935), 30-32.
[8] H. Davenport, *A historical note*, J. Lond. Math. Soc. **22** (1947), 100-101.
[9] M. Kneser, *Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429-434.

Ces dernières années, Y. ould Hamidoune[10] a développé des idées issues de la théorie des graphes aux problèmes d'addition d'ensembles. Il mit sur pied une méthode, qu'il appela isopérimétrique, qui permit de nombreuses avancées. Notamment, elle permet de retrouver la plupart des conséquences du théorème de Kneser, mais apparemment pas directement le théorème de Kneser lui-même. Le graphe de Cayley associé à (G, B), où G est un groupe et $B \subset G$, est le graphe dont les sommets sont les éléments de G et les arêtes les couples (g_1, g_2), avec $g_2 - g_1 \in B$. Dans un tel graphe, si $0 \in B$, on peut définir le périmètre d'un sous-ensemble A de G, comme l'ensemble des sommets extérieurs à A, qui sont joints par une arête sortant de A, soit l'ensemble $(A+B) \setminus A$. Le principe de la méthode isopérimétrique consiste à caractériser la structure des ensembles de plus petit périmètre en considérant leurs unions et intersections.

Le premier article de cette seconde partie de la thèse développe une nouvelle approche isopérimétrique. Cette nouvelle approche se base essentiellement sur les mêmes idées que la méthode initiale, mais considère des objets légèrement différents. On s'intéresse ici non plus aux ensembles de plus petit périmètre, mais à tous les ensembles de périmètre inférieur à $|B| - 1$. Cette nouvelle méthode allie le double avantage de donner une nouvelle démonstration du théorème de Kneser et d'être compatible avec la méthode initiale, qu'elle permet de développer.

Le principe de cette approche consiste à mettre en évidence des ensembles caractéristiques de toutes les sommes par B (i.e de tous les $X+B$ avec $X \subset G$), qui seront appelés cellules pour B. L'étude de ces objets permet, entre autres, de formaliser une notion de dualité additive, qui apparaissait dans des résultats précédents, et qui correspond à une bijection entre les cellules pour B et celles pour $-B$. Une propriété remarquable est qu'une cellule pour B et sa cellule duale pour $-B$ partagent exactement le même périmètre dans le graphe de Cayley (G, B).

On introduit une notation qui a pour but de classer les cellules finies ou de complémentaire fini en fonction de la taille de leurs périmètres. Nous nous appuyons fortement sur une inégalité qui veut que la somme des tailles des périmètres de l'union et de l'intersection de deux ensembles soit plus petite que la somme des tailles des périmètres de ces deux ensembles.

---

[10] principalement dans Y. ould Hamidoune, *An isoperimetric method in additive Theory*, J. Algebra **179** (1996), 622-630.
Y. ould Hamidoune, *Subsets with small sums in abelian groups I : the Vosper property*, Europ. J. Combin. **18** (1997), 541-556.
Y. ould Hamidoune, *Some results in additive number theory I : the critical pair theory*, Acta arith. **96.2** (2000), 97-119.

Pour l'étude des ensembles de petite somme par B dans un groupe abélien, on établit alors des conditions visant à contrôler les tailles des unions et intersections des cellules pour B. En raisonnant par récurrence sur la taille de leur périmètre, nous établissons un résultat de structure pour toutes les cellules de périmètre strictement inférieur à $|B|-1$, ce dont on déduit une nouvelle preuve du théorème de Kneser.

Un des intérêts notables de la méthode isopérimétrique est qu'elle donne aussi des résultats dans un cadre non abélien, là où les anciennes techniques se montraient inefficaces. Le deuxième article de cette seconde partie s'intéresse particulièrement au cas où le groupe G est non abélien et établit un nouveau résultat pour les ensembles de petite somme. Pour cela, nous adaptons les deux premières étapes de la récurrence menant au théorème de Kneser dans le cas abélien.

En particulier, ce résultat permet de donner de nouvelles valeurs exactes de la fonction μ_G. Cette fonction, définie par $\mu_G(r,s) = \min\{|A+B|/A \subset G,\ |A|=r,\ B \subset G,\ |B|=s\}$, apparaît dans plusieurs problèmes de domaines très différents. L'étude de la fonction μ_G s'est faite en plusieurs étapes ces dernières années. Si aujourd'hui cette fonction est complètement déterminée pour un groupe G abélien fini[(11)], cas dans lequel on a :

$$\mu_G(r,s) = \min_{d||G|} \left\{ \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \right\},$$

il y a peu de résultats connus dans les groupes non abéliens. La méthode introduite dans cette partie permet d'obtenir des valeurs particulières de cette fonction dans le cas de deux familles infinies de groupes finis : l'une d'elle est une famille de groupes résolubles et l'autre de groupes simples. Ces résultats permettent en particulier de répondre par la négative à une question de la littérature[(11)], qui demande si la formule précédente est encore vraie lorsque le minimum est considéré sur les cardinaux des sous-groupes pour un groupe non-abélien.

[(11)] S. Eliahou, M. Kervaire, A. Plagne, *Optimally small sumsets in finite abelian groups*, J. Number Theory **101** (2003), 338-348.

CHAPITRE 1

COLORATION DES SOLUTIONS D'UNE ÉQUATION DANS LES GROUPES FINIS

Ce chapitre est constitué de l'article "*Coloured solutions of equations in finite groups*" (soumis pour publication) ainsi que de compléments.

COLOURED SOLUTIONS OF EQUATIONS IN FINITE GROUPS

ÉRIC BALANDRAUD

Abstract. In this article, we consider the relations between colourings and some equations in finite groups. We will express relations linking the numbers of the differently coloured solutions of an equation that depend only on the cardinality of the colouring and not on the distribution of the colours. This gives a link between Ramsey theory that investigates the existence of monochromatic solutions and what is now called anti-Ramsey theory that investigates the existence of rainbow solutions. Both theories are in expansion. We will apply these results to the counting of rainbow three-term arithmetic progressions in any abelian group with equinumerous three-colouring and to the counting of points on a conic defined on a finite field. We will end by discussing the generalized case of a system of equations.

1. Introduction

Ramsey theory studies the links between colourings of mathematical objects (like graphs or numbers) and some of their substructures (subgraphs, arithmetic progressions). There is a huge number of references on this theory, among which, we can for instance quote the classical [4] and the recent book dealing with the special case of the integers [9]. Most theorems of Ramsey theory prove the existence of monochromatic objects, like the van der Waerden theorem [10] which is concerned with monochromatic arithmetic progressions.

It is only recently that a new type of results emerged: these are called anti-Ramsey results or rainbow Ramsey theorems, and give sufficient conditions implying the existence of rainbow objects (that is, objects composed of elements of distinct colours). Very recent results due to Axenovich and Fon-Der-Flaass [1] and to Jungić, Licht, Mahdian, Nešetřil, Radoičić [6, 7, 8] give conditions for the existence of rainbow three-term arithmetic progressions, mostly among integers, but also in cyclic groups.

In another recent work, Cameron, Cilleruelo and Serra [2], generalizing a discovery of Datskovsky [3] on Schur triples, have shown that the number of solutions of some equation in certain bicoloured groups depends only on the cardinalities of the chromatic classes and not on the distribution of the colours.

The purpose of this article is to give a generalisation of these results (mainly the last one) which is valid for any colouring: we exhibit some relationships between the numbers of the differently coloured solutions of some equations and the number of elements coloured in each colour (but not on the colouring itself, that is not on the way the elements are coloured).

2. Context, definitions and notations

In this paper, G denotes a finite group (its law will be denoted multiplicatively). We also consider the equation

$$E_g : \qquad \lambda_1(x_1) \cdot \ldots \cdot \lambda_d(x_d) = g,$$

where $g \in G$ is a parameter and $\lambda_1, \ldots, \lambda_d$ are bijective maps defined on G; the x_l's $(1 \leq l \leq d)$ being the unknowns. In such a situation, we shall say that the equation E_g is regular. We notice that classical equations considered in Ramsey theory are of this kind (whatever the group G is): Schur $(x + y - z = 0)$, van der Waerden $(x + y - 2z = 0)$ or Sidon $(x + y - z - t = 0)$ equations.

We consider a fixed c-colouring of G, $(A_1, ..., A_c)$, that is to say a partition of G, $\cup_{k=1}^{c} A_k = G$.

A solution $(x_1, \ldots, x_d)$ of a regular equation is called monochromatic if all the x_i's are in the same colour class. In this case, the number of colours that appear in this solution is equal to one and therefore *minimal*. A solution $(x_1, \ldots, x_d)$ of a regular equation is called a rainbow solution if the number of colours that appear in this solution is *maximal* (and therefore equal to $\min(c, d)$).

To ease the reading, we will denote the set of indices:

$$I_{c,d} = \Big\{(i_1, \ldots, i_c) \in \mathbb{N}^c / \sum_{k=1}^{c} i_k = d\Big\}.$$

As these indices are taken among all writings of d as a sum of c integers, we have $|I_{c,d}| = \binom{d+c-1}{d} = q_{c,d}$ such indices.

For $(i_1, \ldots, i_c) \in I_{c,d}$, we define:

$$s_{(i_1,\ldots,i_c)} = \left| \left\{ (x_1, \ldots, x_d) \in G^d \middle/ \begin{array}{c} \lambda_1(x_1) \cdot \ldots \cdot \lambda_d(x_d) = g, \\ \sum_{l=1}^{d} |\{x_l\} \cap A_k| = i_k, \text{ (for } k = 1, \ldots, c) \end{array} \right\} \right|,$$

the number of solutions to E_g with exactly i_k elements in A_k (for any $1 \leq k \leq c$).

We will use the $q_{c,d}$-dimensional vector space over $\mathbb{Q}$, indexed on $I_{c,d}$. That is, we denote

$$(e_{(i_1,\ldots,i_c)})_{(i_1,\ldots,i_c)\in I_{c,d}}$$

the canonical basis of $\mathbb{Q}^{q_{c,d}}$.

Two linear forms over this vector space will be of particular importance in what follows. We first define F_s to be the linear form:

$$F_s : \left| \begin{array}{ccc} \mathbb{Q}^{q_{c,d}} & \to & \mathbb{Q} \\ \sum_{(i_1,\ldots,i_c)\in I_{c,d}} a_{(i_1,\ldots,i_c)} e_{(i_1,\ldots,i_c)} & \mapsto & \sum_{(i_1,\ldots,i_c)\in I_{c,d}} a_{(i_1,\ldots,i_c)} s_{(i_1,\ldots,i_c)}. \end{array} \right.$$

This is a linear combination of the numbers of differently coloured solutions. Finally we denote F_p the linear form

$$F_p : \left| \begin{array}{ccc} \mathbb{Q}^{q_{c,d}} & \to & \mathbb{Q} \\ \sum_{(i_1,\ldots,i_c)\in I_{c,d}} a_{(i_1,\ldots,i_c)} e_{(i_1,\ldots,i_c)} & \mapsto & \sum_{(i_1,\ldots,i_c)\in I_{c,d}} a_{(i_1,\ldots,i_c)} \binom{d}{i_1 \ \ldots \ i_c} \prod_{k=1}^{c} |A_k|^{i_k}. \end{array} \right.$$

Notice that F_p is a polynomial in the cardinalities $|A_k|$ of the coloured sets.

3. Main result

The following theorem expresses the fact that F_s and $\frac{1}{|G|}F_p$ happen to coincide on a vector subspace of $\mathbb{Q}^{q_{c,d}}$, that does not depend on the distribution of the sets A_k.

Theorem 1. *Let G be a finite group, $g \in G$ and E_g be a regular equation in d unknowns $\lambda_1(x_1) \cdot \ldots \cdot \lambda_d(x_d) = g$.*

If $(A_1, ..., A_c)$ is a c-colouring of G, then the two linear forms F_s and $\frac{1}{|G|}F_p$ coincide on the vector space R generated by the vectors:

$$v_{(j_1,\ldots,j_c)} = \sum_{(i_1,\ldots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) e_{(i_1,\ldots,i_c)},$$

where $j_1, \ldots, j_c$ are nonnegative integers such that $\sum_{k=1}^{c} j_k \leqslant d - 1$.

Notice that in this theorem, we adopt the usual convention that $\binom{i}{j} = 0$ if $i < j$.

Proof. Elementary properties of the law group and the bijectivity of the maps λ_l $(1 \leq l \leq d)$ show that, being given $d-1$ arbitrary values in G for $d-1$ arbitrary unknowns from $(x_1, \ldots, x_d)$, there is exactly one solution to E_g.

Being given $(j_1, \ldots, j_c) \in \mathbb{N}^c$ such that $\sum_{k=1}^{c} j_k \leqslant d-1$ and a choice of j_k unknowns (for any $1 \leq k \leq c$), where no unknown is chosen twice, we have exactly

$$\left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-1-\sum_{k=1}^{c} j_k)}$$

solutions to E_g such that for k from 1 to c all values of the j_k unknowns are in A_k.

Then if we sum all these numbers of solutions for all possible choices of the unknowns, we get:

$$\binom{d}{j_1 \ \ldots \ j_c \ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-1-\sum_{k=1}^{c} j_k)}.$$

But in this last sum, some solutions of the equation are counted several times. More precisely, we can say that a solution that has i_k elements in A_k (for any k from 1 to c) has been counted exactly $\prod_{k=1}^{c} \binom{i_k}{j_k}$ times.

Rewriting this last statement using the linear form F_s, gives:

$$\binom{d}{j_1 \ \ldots \ j_c \ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-1-\sum_{k=1}^{c} j_k)} = F_s\left(\sum_{(i_1,\ldots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\ldots,i_c)}\right).$$

We can already notice that the left-hand term, say L, in this equality is a polynomial in the cardinalities of the colouring, while the right-hand term is a weighted sum of numbers of solutions.

We now simplify the left-hand term to have an expression using the linear form F_p:

$$\begin{aligned} L &= \binom{d}{j_1 \ \ldots \ j_c \ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-1-\sum_{k=1}^{c} j_k)} \\ &= \frac{1}{|G|} \binom{d}{j_1 \ \ldots \ j_c \ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) \left(\sum_{k=1}^{c} |A_k|\right)^{(d-\sum_{k=1}^{c} j_k)}, \end{aligned}$$

where $|G|$ has been rewritten as the sum of the $|A_k|$'s. We now can develop this last sum using the multinomial coefficients:

$$L = \frac{1}{|G|} \binom{d}{j_1 \ \ldots \ j_c \ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) \times \left(\sum_{\substack{(l_1,\ldots,l_c) \\ \in I_{c,(d-\sum_{k=1}^{c} j_k)}}} \binom{d-\sum_{k=1}^{c} j_k}{l_1 \ \ldots \ l_c} \left(\prod_{k=1}^{c} |A_k|^{l_k}\right)\right).$$

By replacing the indices l_k with $i_k - j_k$, we then obtain

$$L = \frac{1}{|G|}\binom{d}{j_1 \ \dots \ j_c \ (d-\sum_{k=1}^c j_k)}\left(\prod_{k=1}^c |A_k|^{j_k}\right) \times \left(\sum_{\substack{(i_1-j_1,\dots,i_c-j_c)\\ \in I_{c,(d-\sum_{k=1}^c j_k)}}} \binom{d-\sum_{k=1}^c j_k}{i_1-j_1 \ \dots \ i_c-j_c}\left(\prod_{k=1}^c |A_k|^{i_k-j_k}\right)\right),$$

and using the distributivity to express L, we get:

$$L = \frac{1}{|G|}\sum_{\substack{(i_1-j_1,\dots,i_c-j_c)\\ \in I_{c,(d-\sum_{k=1}^c j_k)}}} \binom{d}{j_1 \ \dots \ j_c \ (d-\sum_{k=1}^c j_k)}\binom{d-\sum_{k=1}^c j_k}{i_1-j_1 \ \dots \ i_c-j_c}\prod_{k=1}^c |A_k|^{i_k}.$$

Since the sum of all $i_k - j_k$'s is $d-\sum_{k=1}^c j_k$, the sum of all i_k's is d. Therefore we can write L as a sum indexed over $I_{c,d}$, but we need to add the conditions $i_k \geqslant j_k$ to have the exact same sum. We then develop the multinomial coefficients, and rearrange them to obtain

$$\begin{aligned} L =& \frac{1}{|G|}\sum_{\substack{(i_1,\dots,i_c)\in I_{c,d}\\ \forall k\in[1,c],\ j_k\leqslant i_k}} \frac{d!}{\prod_{k=1}^c j_k!\prod_{k=1}^c (i_k-j_k)!}\prod_{k=1}^c |A_k|^{i_k} \\ =& \frac{1}{|G|}\sum_{\substack{(i_1,\dots,i_c)\in I_{c,d}\\ \forall k\in[1,c],\ j_k\leqslant i_k}} \left(\prod_{k=1}^c \frac{i_k!}{j_k!(i_k-j_k)!}\right)\frac{d!}{\prod_{k=1}^c i_k!}\prod_{k=1}^c |A_k|^{i_k}. \end{aligned}$$

Indexing the sum over all elements in $I_{c,d}$, since all the new terms are equal to zero, we obtain

$$\begin{aligned} L =& \frac{1}{|G|}\sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^c \binom{i_k}{j_k}\right)\binom{d}{i_1\dots i_c}\prod_{k=1}^c |A_k|^{i_k} \\ =& \frac{1}{|G|}F_p\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}}\left(\prod_{k=1}^c \binom{i_k}{j_k}\right)e_{(i_1,\dots,i_c)}\right). \end{aligned}$$

Thus, for all $(j_1,\dots,j_c)\in\mathbb{N}^c$, such that $\sum_{k=1}^c j_k \leqslant d-1$, we have:

$$F_s\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}}\left(\prod_{k=1}^c \binom{i_k}{j_k}\right)e_{(i_1,\dots,i_c)}\right) = \frac{1}{|G|}F_p\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}}\left(\prod_{k=1}^c \binom{i_k}{j_k}\right)e_{(i_1,\dots,i_c)}\right).$$

Therefore for each index $(j_1,\dots,j_c)\in\mathbb{N}^c$, such that $\sum_{k=1}^c j_k \leqslant d-1$, there is a vector, namely $v_{(j_1,\dots,j_c)} = \sum_{(i_1,\dots,i_c)\in I_{c,d}}\left(\prod_{k=1}^c \binom{i_k}{j_k}\right)e_{(i_1,\dots,i_c)}$, on which the two linear forms F_s and $\frac{1}{|G|}F_p$ coincide. By linearity, F_s and $\frac{1}{|G|}F_p$ coincide on the vector subspace R generated by these $\binom{d+c-1}{d-1}$ vectors. □

Remark 1. *This result can be seen as a mean value result on all the elements of G. If we consider the set of all products that can be computed choosing for all k from 1 to c, i_k elements in A_k, for all elements in $I_{c,d}$ balanced by the coordinates*

of a vector $v_{(j_1,\dots,j_c)}$, there is equidistribution on all values of G. This explains the factor $1/|G|$.

Remark 2. *By similar computations, it can be checked that the $\binom{d+c-2}{d-1}$ vectors $v_{(j_1,\dots,j_c)}$, with $\sum_{k=1}^{c} j_k = d-1$ is a generating set of R, and that they are linearly independant, so $\dim_{\mathbb{Q}} R = \binom{d+c-2}{d-1}$. This will be proved in annex, section* **7**.

4. Symmetries in $\mathbb{Q}^{q_{c,d}}$

There is a natural action of the symmetric group $\mathfrak{S}_c$ on $I_{c,d}$, that can be extended to $\mathbb{Q}^{q_{c,d}}$, where the vector of index $(i_1,\dots,i_c) \in I_{c,d}$ is sent by $\sigma \in \mathfrak{S}_c$ to the vector of index $(i_{\sigma(1)},\dots,i_{\sigma(c)})$.

The dimension of the vector subspace P of the invariant vectors under the action of $\mathfrak{S}_c$ is $p_c(d)$, the number of partitions of d in at most c parts, it is the number of orbits of $I_{c,d}$ under the action of $\mathfrak{S}_c$.

We define

$$I'_{c,d} = \Big\{ (i_1,\dots,i_c) \in I_{c,d} \,/\, i_1 \geqslant i_2 \geqslant \dots \geqslant i_c \Big\}.$$

Since every orbit of $I_{c,d}$ has exactly one ordered writing, $I'_{c,d}$ is a set of representatives of all orbits of $I_{c,d}$. We will denote for each $(i_1,\dots,i_c) \in I'_{c,d}$

$$e'_{(i_1,\dots,i_c)} = \sum_{\substack{\exists \sigma \in \mathfrak{S}_c \\ \sigma.(i_1,\dots,i_c) = (i'_1,\dots,i'_c)}} e_{(i'_1,\dots,i'_c)}.$$

Therefore the set $(e'_{(i_1,\dots,i_c)})_{(i_1,\dots,i_c)\in I'_{c,d}}$ is a basis of P.

We observe that the set of vectors $\big\{ v_{(j_1,\dots,j_c)} / \sum_{k=1}^{c} j_k \leqslant d-1 \big\}$ is left invariant by any permutation of $\mathfrak{S}_c$. So the vector subspace R is globally invariant by the action of $\mathfrak{S}_c$.

The vectors in $R \cap P$ will be of particular interest. In the same way as for the vector basis, we can define for all $(j_1,\dots,j_c)$ such that $\sum_{k=1}^{c} j_k \leqslant d-1$ and $j_1 \geqslant j_2 \geqslant \dots \geqslant j_c$:

$$v'_{(j_1,\dots,j_c)} = \sum_{\substack{\exists \sigma \in \mathfrak{S}_c \\ \sigma.(j_1,\dots,j_c) = (j'_1,\dots,j'_c)}} v_{(j'_1,\dots,j'_c)}.$$

Consequently the vectors $v'_{(j_1,\dots,j_c)}$ span $R \cap P$. It can also be checked that the dimension of $R \cap P$ is $p_c(d-1)$.

Corollary 1. *Let G be a finite group, $g \in G$ and E_g be a regular equation in 3 unknowns $\lambda_1(x_1) \cdot \lambda_2(x_2) \cdot \lambda_3(x_3) = g$. If $(A_1,\dots,A_c)$ is a c-colouring of G, with $c \geq 3$, then the number of monochromatic solutions minus half the number of rainbow solutions to E_g is equal to:*

$$\frac{1}{|G|} \left(\sum_{k=1}^{c} |A_k|^3 - \frac{1}{2} \left(\sum_{\substack{(k,l,m)\in[1,c] \\ k\neq l\neq m \\ k\neq m}} 6|A_k||A_l||A_m| \right) \right).$$

Proof. From Theorem 1, this is equivalent to the fact that the vector $e'_{(3,0,\dots,0)} - \frac{1}{2} e'_{(1,1,1,0,\dots,0)}$ belongs to R. We just have to express $e'_{(3,0,\dots,0)} - \frac{1}{2} e'_{(1,1,1,0,\dots,0)}$ as a linear combination of the vectors $v'_{(j_1,\dots,j_c)}$, with $\sum_{k=1}^{c} j_k \leqslant 2$ and $j_1 \geqslant j_2 \geqslant \dots \geqslant j_c$. There are few such vectors, namely we have: $v'_{(2,0,\dots,0)}$, $v'_{(1,1,0,\dots,0)}$, $v'_{(1,0,\dots,0)}$ and $v'_{(0,\dots,0)}$. And not all these vectors are helpful, we will only need $v'_{(2,0,\dots,0)}$ and $v'_{(1,0,\dots,0)}$ that we express in the basis of P: $\{e'_{(3,0,\dots,0)}, e'_{(2,1,0,\dots,0)}, e'_{(1,1,1,0,\dots,0)}\}$.

We first write the vector $v_{(2,0,\dots,0)}$ in the basis of $\mathbb{Q}^{r_{c,3}}$:

$$\begin{aligned} v_{(2,0,\dots,0)} &= \binom{3}{2} e_{(3,0,\dots,0)} + \sum_{\substack{(i_2,\dots,i_c) \\ \sum_{k=2}^{c} i_k = 1}} \binom{2}{2}\binom{1}{0} e_{(2,i_2,\dots,i_c)} \\ &= 3e_{(3,0,\dots,0)} + \sum_{\substack{(i_2,\dots,i_c) \\ \sum_{k=2}^{c} i_k = 1}} e_{(2,i_2,\dots,i_c)}. \end{aligned}$$

Thus, we can state:

$$v'_{(2,0,\dots,0)} = 3e'_{(3,0,\dots,0)} + e'_{(2,1,0,\dots,0)}.$$

We now write the vector $v_{(1,0,\dots,0)}$ in the basis of $\mathbb{Q}^{r_{c,3}}$:

$$\begin{aligned} v_{(1,0,\dots,0)} &= \binom{3}{1} e_{(3,0,\dots,0)} + \sum_{\substack{(i_2,\dots,i_c) \\ \sum_{k=2}^{c} i_k = 1}} \binom{2}{1} e_{(2,i_2,\dots,i_c)} + \sum_{\substack{(i_2,\dots,i_c) \\ \sum_{k=2}^{c} i_k = 2}} \binom{1}{1} e_{(1,i_2,\dots,i_c)} \\ &= 3e_{(3,0,\dots,0)} + 2 \sum_{\substack{(i_2,\dots,i_c) \\ \sum_{k=2}^{c} i_k = 1}} e_{(2,i_2,\dots,i_c)} + \sum_{\substack{(i_2,\dots,i_c) \\ \sum_{k=2}^{c} i_k = 2}} e_{(1,i_2,\dots,i_c)}, \end{aligned}$$

which gives

$$\begin{aligned} v'_{(1,0,\dots,0)} &= 3e'_{(3,0,\dots,0)} + 2e'_{(2,1,0,\dots,0)} + (e'_{(2,1,0,\dots,0)} + 3e'_{(1,1,1,0,\dots,0)}) \\ &= 3e'_{(3,0,\dots,0)} + 3e'_{(2,1,0,\dots,0)} + 3e'_{(1,1,1,0,\dots,0)} \end{aligned}$$

and finally we have

$$\frac{1}{2} v'_{(2,0,\dots,0)} - \frac{1}{6} v'_{(1,0,\dots,0)} = e'_{(3,0,\dots,0)} - \frac{1}{2} e'_{(1,1,1,0,\dots,0)}$$

which implies that $e'_{(3,0,\dots,0)} - \frac{1}{2} e'_{(1,1,1,0,\dots,0)}$ belongs to R and concludes the proof. □

There is an interesting dual result for three-colourings.

Corollary 2. *Let G be a finite group and (A, B, C) be a three-colouring of G. Let $g \in G$ and E_g be a regular equation in d unknowns $\lambda_1(x_1) \cdot \ldots \cdot \lambda_d(x_d) = g$. Then*

- *If d is odd, the number of monochromatic solutions minus half the number of rainbow solutions is equal to:*

$$\frac{1}{|G|} \left(|A|^d + |B|^d + |C|^d - \frac{1}{2} \left(\sum_{\substack{(i,j,k) \in I_{3,d} \\ ijk \neq 0}} \binom{d}{i\ j\ k} |A|^i |B|^j |C|^k \right) \right).$$

- *If d is even, the number of rainbow solutions is equal to:*

$$\frac{1}{|G|} \sum_{\substack{(i,j,k) \in I_{3,d} \\ ijk \neq 0}} \binom{d}{i\ j\ k} |A|^i |B|^j |C|^k.$$

Proof. From Theorem 1, it suffices to prove that the vector $e'_{(d,0,0)} - \frac{1}{2} \sum_{\substack{(i,j,k) \in I'_{3,d} \\ ijk \neq 0}} e'_{(i,j,k)}$ is in R if d is odd, and that $\sum_{\substack{(i,j,k) \in I'_{3,d} \\ ijk \neq 0}} e'_{(i,j,k)}$ is in R if d is even. We will start by a first calculation:

$$\begin{aligned} w_1 = \sum_{i=0}^{d-1}(-1)^i v_{(i,0,0)} &= \sum_{i=0}^{d-1}(-1)^i \sum_{(i',j',k')\in I_{3,d}} \binom{i'}{i} e_{(i',j',k')} \\ &= \sum_{(i',j',k')\in I_{3,d}} \left(\sum_{i=0}^{d-1}(-1)^i \binom{i'}{i}\right) e_{(i',j',k')}. \end{aligned}$$

The coefficients in this last sum only depend on i' and can be computed:

- If $i'=0$ then $\sum_{i=0}^{d-1}(-1)^i\binom{i'}{i}=1$.
- If $i'\in[1,d-1]$, then:

$$\begin{aligned} \sum_{i=0}^{d-1}(-1)^i\binom{i'}{i} &= \sum_{i=0}^{i'}(-1)^i\binom{i'}{i} \\ &= (1-1)^{i'}=0. \end{aligned}$$

- If $i'=d$, then:

$$\begin{aligned} \sum_{i=0}^{d-1}(-1)^i\binom{i'}{i} &= \sum_{i=0}^{d}(-1)^i\binom{d}{i}-(-1)^d \\ &= (1-1)^d-(-1)^d \\ &= -(-1)^d. \end{aligned}$$

So we can write: $w_1 = -(-1)^d e_{(d,0,0)} + \sum_{(0,j',k')\in I_{3,d}} e_{(0,j',k')}$. By symmetry, we also have:

$$w_2 = \sum_{j=0}^{d-1}(-1)^j v_{(0,j,0)} = -(-1)^d e_{(0,d,0)} + \sum_{(i',0,k')\in I_{3,d}} e_{(i',0,k')},$$

$$w_3 = \sum_{k=0}^{d-1}(-1)^k v_{(0,0,k)} = -(-1)^d e_{(0,0,d)} + \sum_{(i',j',0)\in I_{3,d}} e_{(i',j',0)}.$$

The three vectors w_1, w_2 and w_3 are, as sums of vectors of R, also in R. We will need another vector from R, namely the vector $v_{(0,0,0)} = \sum_{(i',j',k')\in I_{3,d}} e_{(i',j',k')}$.

We can now compute the coordinates of the vector $u = w_1 + w_2 + w_3 - v_{(0,0,0)}$, which is in R by definition:

$$\begin{aligned} u &= (1-(-1)^d)(e_{(d,0,0)} + e_{(0,d,0)} + e_{(0,0,d)}) - \sum_{\substack{(i,j,k)\in I_{3,d}\\ ijk\neq 0}} e_{(i,j,k)} \\ &= (1-(-1)^d)e'_{(d,0,0)} - \sum_{\substack{(i,j,k)\in I'_{3,d}\\ ijk\neq 0}} e'_{(i,j,k)}. \end{aligned}$$

If d is even the coordinate of u on $e'_{(d,0,0)}$ vanishes, and $-u$, which is the vector we looked for, is in R.

If d is odd the coordinate of u on $e'_{(d,0,0)}$ is 2, and $\frac{1}{2}u$, which is the vector we looked for, is in R. □

5. Applications

5.1. **Three-term rainbow arithmetic progressions in a abelian group with an equinumerous three-colouring.** The first link between arithmetic progressions and colouring is the van der Waerden's Theorem [10]. In the past few years a

lot of new results have been established on rainbow three-term arithmetic progressions.

In 2003, Jungić and Radoičić [8] proved the existence of a rainbow three-term arithmetic progression in an equinumerous colouring of $[1, 3n]$. The same year, in [1], Axenovich and Fon-Der-Flaass proved the existence of a rainbow three-term arithmetic progression in a three-colouring of $[1, n]$ if each colour appears on at least $(n + 4)/6$ numbers. Among others results, Jungić, Licht, Mahdian, Nešetřil and Radoičić give in [6] a first result on the cyclic group $\mathbb{Z}_n$.

Most of the results in anti-Ramsey theory are obtained in a constructive way. The forthcoming proof is not constructive. In fact, it does not only establish the existence of one rainbow three-term arithmetic progression, but it provides a lower bound on the number of such solutions.

Proposition 1. *Let n be an odd integer, G be an abelian group of order $3n$, and (A, B, C) be a three-colouring of G such that $|A| = |B| = |C| = n$, then there are at least n three-term rainbow arithmetic progressions in G.*

Proof. If we consider the equation $x - 2y + z = 0$, the fact that n is odd implies that the map $x \mapsto -2x$ is bijective from G to G. So it follows from Corollary 1 or Corollary 2 since $d = c = 3$, that:

$$\begin{aligned} s_{(3,0,0)} + s_{(0,3,0)} + s_{(0,0,3)} - \frac{1}{2}s_{(1,1,1)} &= \frac{1}{3n}\left(|A|^3 + |B|^3 + |C|^3 - \frac{1}{2}6|A||B||C|\right) \\ &= \frac{1}{3n}(3n^3 - 3n^3) = 0. \end{aligned}$$

We can also notice that for every element $x \in G$, (x, x, x) is a monochromatic solution to the equation, therefore $s_{(3,0,0)} + s_{(0,3,0)} + s_{(0,0,3)} \geqslant 3n$ which implies $s_{1,1,1} \geqslant 6n$.

Since G is abelian, the equation $x - 2y + z = 0$ is characteristic of the three-term arithmetic progressions. Conversely, given a three-term arithmetic progression $(\alpha, \alpha + r, \alpha + 2r)$, if r has an order different from 3 in G, we have 2 solutions to $x - 2y + z = 0$ and if r has order 3 in G we have 6 solutions.

Therefore from $s_{(1,1,1)} \geqslant 6n$ we deduce that there are at least n three-term rainbow arithmetic progressions in G. □

Remark 3. *In annex* **8**, *we prove that this lower bound on the number of rainbow solutions is sharp in some groups, but can be improved in others.*

Remark 4. *For an equation like Sidon's one: $x + y - z - t = 0$ and a four-colouring of a group G, it would have been interesting to have such a relation as the one of Corollary 1, that links the numbers of monochromatic and rainbow solutions. Examples of groups of small cardinality can be found which prove that there is no such relation. However, we can, by the same process, find a (more complicated) relation, between the numbers of monochromatic, rainbow solutions and the number of solutions that count two colours and two elements in each colour. To be more precise, with $d = 4$ and $c = 4$, the vector:*

$$3e'_{(4,0,0,0)} - e'_{(2,2,0,0)} + e'_{(1,1,1,1)},$$

is in R.

5.2. **Points on a conic over a finite field.** In this part, we focus our attention on the equation $ax^2 + by^2 + cz^2 = 0$ in the finite field $\mathbb{F}_q$, where $abc \neq 0$. We want to determine the number S of solutions (x, y, z) of this equation such that $xyz \neq 0$. The value of this number is already known, and is usually established using character theory: for instance [5] presents this type of computations. What follows is a new computation of S, that relies only on combinatorial arguments.

Let us start with an obvious case, where $\mathbb{F}_q$ is a field of characteristic 2, the Frobenius map $x \mapsto x^2$ is then bijective, thus $S = q^2$. We will from now on, consider the case where $\mathbb{F}_q$ is a field of odd characteristic, we denote by $\mathbb{F}_q^2$ the subset of all squares from $\mathbb{F}_q$. We consider the three-colouring $A = \{0\}$, $B = \mathbb{F}_q^2 \setminus \{0\}$ and $C = \mathbb{F}_q \setminus \mathbb{F}_q^2$. It is known that $|A| = 1$, $|B| = |C| = \frac{q-1}{2}$.

Let us consider an arbitrary element μ in C. We first notice that all equations $ax^2 + by^2 + cz^2 = 0$ can be reduced to one of the following two: $x^2 + y^2 + z^2 = 0$ or $x^2 + y^2 + \mu z^2 = 0$, depending whether the coefficients are squares or not.

We will then consider the equation $x + y + \epsilon z = 0$, with $\epsilon \in \{1, \mu\}$ and the colouring (A, B, C) in the additive group of $\mathbb{F}_q$. Either Corollary 1 or Corollary 2 gives:

$$s_{(3,0,0)} + s_{(0,3,0)} + s_{(0,0,3)} - \frac{1}{2}s_{(1,1,1)} = \frac{1}{q}\left(1 + 2\left(\frac{q-1}{2}\right)^3 - \frac{1}{2}\left(6\left(\frac{q-1}{2}\right)^2\right)\right).$$

In this equality, we clearly see that $s_{(3,0,0)} = 1$ as $0 + 0 + 0 = 0$, $s_{(0,3,0)} = \frac{S}{2^3}$ because each square has exactly two squareroots and that $s_{(0,0,3)} = s_{(0,3,0)}$ because the map $(x, y, z) \mapsto (\mu x, \mu y, \mu z)$ sends bijectively the solutions from B^3 on the solutions from C^3. So, we have:

$$1 + \frac{S}{4} - \frac{1}{2}s_{(1,1,1)} = \frac{1}{4q}(q^3 - 6q^2 + 9q) = \frac{(q-3)^2}{4}.$$

What remains to be determined is $s_{(1,1,1)}$, the number of solutions that contain a zero, a square and a non-square. This can be reduced to the counting of the non-zero solutions of $X^2 = -\epsilon\mu Y^2$. This equation has $2(q-1)$ non-zero solutions if $-\epsilon\mu$ is a square and none if $-\epsilon\mu$ is not a square. Recalling that -1 is a square if and only if $q \equiv 1 \pmod 4$, we can conclude.

- If $q \equiv 1 \pmod 4$ then X is a square if and only if $-X$ is a square.

  Let us first consider the equation $x^2 + y^2 + z^2 = 0$, if one of the unknowns vanishes, the two others are both squares or both non-squares in the corresponding equation $x + y + z = 0$, so $s_{(1,1,1)} = 0$, and

  $$S = (q-3)^2 - 4 = q^2 - 6q + 5 = (q-1)(q-5).$$

  Let us consider now the equation $x^2 + y^2 + \mu z^2 = 0$, if z vanishes in $x + y + \mu z = 0$, x and y are both squares or both non-squares, if x or y vanishes the $q-1$ solutions of $x+y+\mu z = 0$ contain a square, a non-square and a zero, therefore $s_{(1,1,1)} = 2(q-1)$, and

  $$S = (q-3)^2 + 4(q-1) - 4 = q^2 - 2q + 1 = (q-1)^2.$$

- If $q \equiv 3 \pmod 4$ then X and $-X$ are never both squares or both non-squares.

  As in the first case, we will start with the equation $x^2 + y^2 + z^2 = 0$, if one of the unknowns vanishes then the two others are not both squares or both non-squares in $x + y + z = 0$, so $s_{(1,1,1)} = 3(q-1)$, and

  $$S = (q-3)^2 + 6(q-1) - 4 = q^2 - 1 = (q-1)(q+1).$$

  We consider now the equation $x^2 + y^2 + \mu z^2 = 0$, if x or y vanishes in $x + y + \mu z = 0$ then the two last are both squares or both non-squares and if z vanishes the two last are not both squares or both non-squares, thus finally $s_{(1,1,1)} = (q-1)$, and

  $$S = (q-3)^2 + 2(q-1) - 4 = q^2 - 4q + 3 = (q-1)(q-3).$$

Remark 5. *The general case of an equation $ax^n + by^n + cz^n = 0$ with $abc \neq 0$, will be discused in annex, section* **9**. *In this case, the number of solutions (x, y, z) such that $xyz \neq 0$ cannot be computed thanks to this method. Nevertheless it yields some information.*

6. System of equations

In this part, we will now consider not only an equation, but a system of equations:

$$\left\{\begin{array}{ccccc} \lambda_{1,1}(x_1) & \cdot \ldots \cdot & \lambda_{d,1}(x_d) & = & g_1 \\ \vdots & & \vdots & \vdots & \vdots \\ \lambda_{1,f}(x_1) & \cdot \ldots \cdot & \lambda_{d,f}(x_d) & = & g_f, \end{array}\right.$$

with $d \geq f$ and where $g_1, \ldots, g_f$ are parameters and the $\lambda_{l,m}$ are maps from G to G; the x_l's $(1 \leq l \leq d)$ being the unknowns.

In order to generalize our method, we need to fix a condition on the maps $\lambda_{l,m}$ to be allowed to choose some of the values of the unknowns, this condition will be similar to the inversibility of a matrix.

We will say that this system satisfies the Gaussian condition if $d \geq f$ and if given $d-f$ arbitrary values for $d-f$ arbitrary unknowns, there is exactly one solution of the system. It should be noticed that if $f = 1$, the Gaussian condition is equivalent to the bijectivity of all maps $\lambda_{l,1}$ that was supposed in Theorem 1.

We will now give the general theorem that holds for the systems that satisfy the Gaussian condition:

Theorem 2. *Let G be a finite group and*

$$\left\{\begin{array}{ccccc} \lambda_{1,1}(x_1) & \cdot \ldots \cdot & \lambda_{d,1}(x_d) & = & g_1 \\ \vdots & & \vdots & \vdots & \vdots \\ \lambda_{1,f}(x_1) & \cdot \ldots \cdot & \lambda_{d,f}(x_d) & = & g_f, \end{array}\right.$$

be a system of equations that satisfies the Gaussian condition.

If $(A_1, ..., A_c)$ is a c-colouring of G, then the two linear forms F_s and $\frac{1}{|G|^f} F_p$ coincide on the vector space R generated by the vectors:

$$v_{(j_1,\ldots,j_c)} = \sum_{(i_1,\ldots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\ldots,i_c)},$$

where $j_1, \ldots, j_c$ are nonnegative integers such that $\sum_{k=1}^{c} j_k \leqslant d - f$.

Proof. The Gaussian condition allowed us to choose $d-f$ arbitrary values in G for $d-f$ arbitrary unknowns from $(x_1, \ldots, x_d)$, then there is exactly one solution of the system. We will as before choose the first values in some of the coloured set.

Given $(j_1, \ldots, j_c) \in \mathbb{N}^c$, such that $\sum_{k=1}^{c} j_k \leqslant d-f$, and a choice of j_k unknowns for k from 1 to c, where no unknown is chosen twice. We have exactly

$$\left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-f-\sum_{k=1}^{c} j_k)}$$

solutions to the system such that for k from 1 to c all values of the j_k unknowns are in A_k. And if we sum all these solutions for all possible choices of the unknowns, we get as before:

$$\binom{d}{j_1 \ \ldots \ j_c \ (d - \sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-f-\sum_{k=1}^{c} j_k)}.$$

Again in this last sum, a solution that contains i_k elements in A_k for k from 1 to c is counted $\prod_{k=1}^{c} \binom{i_k}{j_k}$ times, and we can write:

$$\binom{d}{j_1\ \dots\ j_c\ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-f-\sum_{k=1}^{c} j_k)} = F_s\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\dots,i_c)}\right).$$

The result follows from exactly the same simple polynomial computation of the left-hand term L. Once factorized by the fraction $\frac{1}{|G|^f}$, we have exactly the same polynomial expression as in the proof of Theorem 1:

$$\begin{aligned} L =& \binom{d}{j_1\ \dots\ j_c\ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-f-\sum_{k=1}^{c} j_k)} \\ =& \frac{1}{|G|^f} \binom{d}{j_1\ \dots\ j_c\ (d-\sum_{k=1}^{c} j_k)} \left(\prod_{k=1}^{c} |A_k|^{j_k}\right) |G|^{(d-\sum_{k=1}^{c} j_k)} \\ =& \frac{1}{|G|^f} F_p\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\dots,i_c)}\right). \end{aligned}$$

So for all $(j_1,\dots,j_c)\in\mathbb{N}^c$, such that $\sum_{k=1}^{c} j_k \leqslant d-f$, we have:

$$F_s\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\dots,i_c)}\right) = \frac{1}{|G|^f} F_p\left(\sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\dots,i_c)}\right).$$

Then for each index $(j_1,\dots,j_c)\in\mathbb{N}^c$, such that $\sum_{k=1}^{c} j_k \leqslant d-f$, we have a vector $v_{(j_1,\dots,j_c)} = \sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\dots,i_c)}$ on which both linear forms F_s and $\frac{1}{|G|^f} F_p$ coincide. They will also by linearity coincide on the vector subspace R generated by this $\binom{d-f+c}{d-f}$ vectors. □

Remark 6. *It can be checked that the vector subspace R is generated by the $\binom{d-f+c-1}{d-f}$ vectors $v_{(j_1,\dots,j_c)}$ such that $\sum_{k=1}^{c} j_k = d-f$. It can also be checked that these vectors are linearly independent, this will be proved in annex, section* **7**, *so $\dim_{\mathbb{Q}} R = \binom{d-f+c-1}{d-f}$ and the dimension of $R\cap P$ is $p_c(d-f)$.*

Remark 7. *It seems natural that the more equations a system holds, the smaller the dimension of R is.*

As an exemple, we can see that if G is abelian, the following system,

$$\begin{cases} x-2y+z &= 0 \\ y-2z+t &= 0 \end{cases}$$

verifies the Gaussian condition if $|G|$ is divisible neither by 2 nor by 3 and is characteristic of the four-term arithmetic progressions.

For a four-colouring of G, as the system has at least $|G|$ monochromatic solutions (the trivial ones (x,x,x,x)), it would be interesting to have a relation that provides a link between monochromatic and rainbow solutions, but in this case, $c=4$, $d=4$ and $f=2$, $R\cap P$ has dimension 2 and is generated by:

$$v'_{(2,0,0,0)} = 6e'_{(4,0,0,0)} + 3e'_{(3,1,0,0)} + 2e'_{(2,2,0,0)} + e'_{(2,1,1,0)},$$

$$v'_{(1,1,0,0)} = 3e'_{(3,1,0,0)} + 4e'_{(2,2,0,0)} + 5e'_{(2,1,1,0)} + 6e'_{(1,1,1,1)}.$$

References

[1] M. Axenovich, D. Fon-Der-Flaass, *On rainbow arithmetic progressions*, Electronic Journal of Combinatorics **11** (2004), R1.

[2] P. Cameron, J. Cilleruelo, O. Serra, *On three-term arithmetic progressions in bicolored sets*, preprint, 2005.

[3] B.A. Datskovsky, *On the number of monochromatic Schur triples*, Adv. in Appl. Math. **31** (2003), 193-198.

[4] R. Graham, B. Rothschild, J.H. Spencer, *Ramsey theory*, John Wiley and sons, New-York, 1980.

[5] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Mathematics **84**, Springer-Verlag, 1990.

[6] V. Jungić, J. Licht, M. Mahdian, J. Nešetřil, R. Radoičić, *Rainbow Arithmetic Progressions and Anti-Ramsey Results*, Combinatorics, Probability and Computing **12** (2003), 599-620.

[7] V. Jungić, J. Nešetřil, R. Radoičić, *Rainbow Ramsey theory*, Integers **5(2)** (2005), A9.

[8] V. Jungić, R. Radoičić, *Rainbow 3-term arithmetic progressions*, Integers **3** (2003), A18.

[9] B. Landman, A. Robertson, *Ramsey theory on the integers*, Student Mathematical Library **24**, AMS, 2003.

[10] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Arch. Wisk. **15** (1927), 212-216.

COMPLÉMENTS À "COLOURED SOLUTIONS OF EQUATIONS IN FINITE GROUPS"

Nous allons ici développer trois points concernant l'article "*Coloured solutions of equations in finite groups*". Dans les remarques 2 et 6, il est affirmé que la dimension de l'espace vectoriel R des théorèmes 1 et 2 est $\binom{c+d-f-1}{d-f}$ (le théorème 1 correspond au cas particulier du théorème 2 où $f = 1$). La preuve de ce fait constitue le premier point de ces compléments.

Nous donnons dans une seconde partie quelques illustrations: la première montre la nécessité de la régularité de l'équation dans le théorème 1 et donc dans les corollaires 1 et 2; La seconde montre l'optimalité de la borne inférieure du nombre de solutions arc-en-ciel dans la proposition 1; la troisième et dernière illustration consiste à remarquer que cette borne peut être améliorée dans le cas d'un groupe cyclique d'ordre 9.

Le dernier point précise ce que l'on peut dire du nombre de points d'un ensemble défini par $ax^n + by^n + cz^n = 0$ avec $abc \neq 0$. La numérotation des sections prolonge celle de l'article.

7. Une base de l'espace vectoriel des relations R

On considère les $\binom{c+d-f}{d-f}$ vecteurs

$$v_{(j_1,\dots,j_c)} = \sum_{(i_1,\dots,i_c)\in I_{c,d}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right) e_{(i_1,\dots,i_c)},$$

où $(j_1,\dots,j_c) \in \mathbb{N}^c$, est tel que $\sum_{k=1}^{c} j_k \leqslant d-f$.
On note R l'espace vectoriel engendré par ces vecteurs.

Parmi ceux-la, on s'intéresse à la famille des vecteurs $v_{(j_1,\dots,j_c)}$, tels que $(j_1,\dots,j_c) \in I_{c,d-f}$.
Il y a exactement $q_{c,d-f} = \binom{c+d-f-1}{d-f}$ vecteurs dans cette famille.
Montrons qu'elle forme une base de R.

7.1. **Famille génératrice.** Soit $(j_1,\dots,j_c)$ tel que $\sum_{k=1}^{c} j_k \leqslant d-f$. On donne un calcul explicite donnant les coordonnées de $v_{(j_1,\dots,j_c)}$, ce calcul est assez intuitif. En effet, les vecteurs $v_{(l_1,\dots,l_c)}$, avec $(l_1,\dots,l_c) \in I_{c,d-f}$ correspondent aux choix les plus précis, les choix moins précis, correspondent à des choix intermédiaires.

On considère le vecteur:

$$w = \sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\prod_{k=1}^{c} \binom{l_k}{j_k}\right) v_{(l_1,\dots,l_c)}.$$

Ce vecteur est exprimé comme combinaison linéaire des vecteurs $v_{(l_1,\dots,l_c)}$, avec $(l_1,\dots,l_c) \in I_{c,d-f}$, dont nous connaissons les coordonnées dans la base $\{e_{(i_1,\dots,i_c)}/(i_1,\dots,i_c) \in I_{c,d}\}$. Nous pouvons alors exprimer w comme combinaison linéaire des vecteurs de cette base:

$$\begin{aligned} w &= \sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\left(\prod_{k=1}^{c} \binom{l_k}{j_k} \right) \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\prod_{k=1}^{c} \binom{i_k}{l_k} \right) e_{(i_1,\dots,i_c)} \right) \\ &= \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\prod_{k=1}^{c} \binom{i_k}{l_k} \binom{l_k}{j_k} \right) \right) e_{(i_1,\dots,i_c)}. \end{aligned}$$

Les coordonnées de w peuvent alors être simplifiées en développant et réarrangeant les coefficients binomiaux:

$$\begin{aligned} w &= \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}\\ j_k \leqslant l_k \leqslant i_k}} \left(\prod_{k=1}^{c} \frac{i_k!}{(i_k-l_k)!(l_k-j_k)!j_k!} \right) \right) e_{(i_1,\dots,i_c)} \\ &= \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\prod_{k=1}^{c} \binom{i_k-j_k}{i_k-l_k} \right) \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) \right) e_{(i_1,\dots,i_c)}. \end{aligned}$$

Seuls des termes nuls ont été ajoutés en indiçant cette dernière somme sur l'ensemble des $(l_1,\dots,l_c) \in I_{c,d-f}$. On peut alors factoriser par la quantité $\left(\prod_{k=1}^{c} \binom{i_k}{j_k}\right)$. On obtient alors:

$$w = \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) \left(\sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\prod_{k=1}^{c} \binom{i_k-j_k}{i_k-l_k} \right) \right) e_{(i_1,\dots,i_c)}.$$

La somme $\sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\prod_{k=1}^{c} \binom{i_k-j_k}{i_k-l_k}\right)$ n'est pas nulle si et seulement si pour tout $k \in [1,c]$, $j_k \leqslant i_k$. De plus chacun des termes de cette somme n'est pas nul si et seulement si pour tout $k \in [1,c]$, $j_k \leqslant l_k \leqslant i_k$. Comme cette somme est indicée sur tous les $(l_1,\dots,l_c) \in I_{c,d-f}$, elle peut se comprendre comme l'ensemble des choix de $\sum_{k=1}^{c} l_k - \sum_{k=1}^{c} j_k$ éléments parmi $\sum_{k=1}^{c} i_k - \sum_{k=1}^{c} j_k$, soit $\binom{d-\sum_{k=1}^{c} j_k}{d-f-\sum_{k=1}^{c} j_k}$. Donc:

$$\begin{aligned} w &= \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) \binom{d-\sum_{k=1}^{c} j_k}{d-f-\sum_{k=1}^{c} j_k} e_{(i_1,\dots,i_c)} \\ &= \binom{d-\sum_{k=1}^{c} j_k}{d-f-\sum_{k=1}^{c} j_k} v_{(j_1,\dots,j_c)}. \end{aligned}$$

De par la définition de w, on a:

$$v_{(j_1,\dots,j_c)} = \frac{1}{\binom{d-\sum_{k=1}^{c} j_k}{d-f-\sum_{k=1}^{c} j_k}} \sum_{\substack{(l_1,\dots,l_c)\\ \in I_{c,d-f}}} \left(\prod_{k=1}^{c} \binom{l_k}{j_k} \right) v_{(l_1,\dots,l_c)}.$$

Ainsi la famille des vecteurs $v_{(l_1,\dots,l_c)}$, avec $(l_1,\dots,l_c) \in I_{c,d-f}$, est bien une famille génératrice de R.

7.2. **Famille libre.** Soient $a_{(j_1,\dots,j_c)}$ tels que $(j_1,\dots,j_c) \in I_{c,d-f}$, une famille de rationnels telle que:

$$\sum_{\substack{(j_1,\dots,j_c)\\ \in I_{c,d-f}}} a_{(j_1,\dots,j_c)} v_{(j_1,\dots,j_c)} = 0.$$

On développe alors cette expression:

$$\begin{aligned}\sum_{\substack{(j_1,\dots,j_c)\\ \in I_{c,d-f}}} a_{(j_1,\dots,j_c)} \left(\sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) e_{(i_1,\dots,i_c)} \right) &= 0\\ \sum_{\substack{(i_1,\dots,i_c)\\ \in I_{c,d}}} \left(\sum_{\substack{(j_1,\dots,j_c)\\ \in I_{c,d-f}}} a_{(j_1,\dots,j_c)} \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) \right) e_{(i_1,\dots,i_c)} &= 0.\end{aligned}$$

Donc, pour tout $(i_1,\dots,i_c) \in I_{c,d}$, on a:

$$\sum_{\substack{(j_1,\dots,j_c)\\ \in I_{c,d-f}}} a_{(j_1,\dots,j_c)} \left(\prod_{k=1}^{c} \binom{i_k}{j_k} \right) = 0.$$

On raisonne par récurrence décroissante sur j_c:

Si $j_c = d-f$, alors $(j_1,\dots,j_c) = (0,\dots,0,d-f)$ et pour $(i_1,\dots,i_c) = (0,\dots,0,d) \in I_{c,d}$, on réécrit l'égalité précédente, on obtient alors:

$$\sum_{\substack{(j'_1,\dots,j'_c)\\ \in I_{c,d-f}}} a_{(j'_1,\dots,j'_c)} \left(\prod_{k=1}^{c} \binom{i_k}{j'_k} \right) = \binom{d}{d-f} a_{(0,\dots,0,d-f)} = 0.$$

Car si il existe $k \in [1, c-1]$ tel que $j'_k \neq 0$, on a $\binom{i_k}{j'_k} = 0$. Ainsi, $a_{(0,\dots,0,d-f)} = 0$.

Supposons que pour tout $(j_1,\dots,j_c) \in I_{c,d-f}$ tel que $j_c \geqslant l$, on ait $a_{(j_1,\dots,j_c)} = 0$. Soit $(j_1,\dots,j_k) \in I_{c,d-f}$ tel que $j_c = l-1$, on considère $(i_1,\dots,i_c) = (j_1,\dots,j_c+f)$, et on réécrit l'égalité précédente, on obtient:

$$\sum_{\substack{(j'_1,\dots,j'_c)\\ \in I_{c,d-f}}} a_{(j'_1,\dots,j'_c)} \left(\prod_{k=1}^{c} \binom{i_k}{j'_k} \right) = \binom{j_c+f}{j_c} a_{(j_1,\dots,j_c)} = 0,$$

car si $j'_c \geqslant l$, $a_{(j'_1,\dots,j'_c)} = 0$ d'après l'hypothèse de récurence, et si $j'_c < l$ et qu'il existe $k \in [1, c-1]$ tel que $j'_k > i_k$, on a $\binom{i_k}{j'_k} = 0$. Le seul cas restant à considérer est alors $a_{(j_1,\dots,j_c)}$. Donc on a $a_{(j_1,\dots,j_c)} = 0$.

Ainsi tous les $a_{(j_1,\dots,j_c)}$ sont nuls et la famille est libre.

8. Quelques illustrations

8.1. **Contre-exemple aux corollaires 1 et 2 lorsque l'équation n'est pas régulière.** Considérons le groupe $\mathbb{Z}/6\mathbb{Z}$ et la coloration équipotente suivante:

$$A = \{0,3\},\ B = \{1,5\},\ \text{et } C = \{2,4\}.$$

On considère aussi l'équation caractéristique des progressions arithmétiques à trois termes:

$$x - 2y + z = 0.$$

Cette équation n'est pas régulière dans $\mathbb{Z}/6\mathbb{Z}$, car la multiplication par 2 n'est pas une bijection.

On a une équation à trois inconnues et une trois-coloration, ainsi si les corollaires 1 et 2 ne nécessitaient pas la regularité de l'équation, le nombre de solutions monochromatiques moins la moitie du nombres de solutions arc-en-ciel serait exactement de:

$$\begin{aligned}\frac{1}{|G|}\left(|A|^3+|B|^3+|C|^3-\frac{1}{2}(6|A||B||C|)\right) &= \frac{1}{6}\left(2^3+2^3+2^3-\frac{1}{2}(6.2^3)\right)\\ &= 0.\end{aligned}$$

Or les solutions monochromatiques sont les six solutions triviales (x,x,x) et:

$$(0,3,0),\ (3,0,3).$$

Et les solutions arc-en-ciel sont:

$$(0,1,2),\ (2,1,0),\ (1,2,3),\ (3,2,1),\ (3,4,5),\ (5,4,3),\ (4,5,0),\ (0,5,4).$$

Le nombre de solutions monochromatiques moins la moitie du nombres de solutions arc-en-ciel est alors exactement de 4.

8.2. **Sur le nombre de progressions arithmétiques à trois termes arc-en-ciel.** La proposition 1 en application des corollaires 1 ou 2 affirme que pour un groupe G d'ordre impair et multiple de 3, $3n$ et une trois-coloration équipotente de G, il y a au moins n progressions arithmétiques à trois termes arc-en-ciel.

Nous allons voir que cette borne est optimale dans un premier exemple, puis qu'elle peut être améliorée si l'on précise la structure du groupe.

8.2.1. *Optimalité de la borne.* On considère le groupe $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, et la trois-coloration équipotente suivante:

$$A=\{(0,0),(1,0),(2,1)\},$$
$$B=\{(0,1),(1,1),(2,2)\},$$
$$C=\{(0,2),(1,2),(2,0)\}.$$

On s'intéresse aux solutions de l'équation régulière $x-2y+z=0$. On voit rapidemment que les seules solutions monochromatiques sont les solutions triviales $((x,x,x))$. On compte alors exactement 9 solutions monochromatiques. Ainsi d'après les corollaires 1 ou 2, on a exactement 18 solutions arc-en-ciel, correspondant à trois progressions arithmétiques à trois termes (chacune comptée 6 fois).

8.2.2. *Non-optimalité de la borne dans un groupe cyclique.* On considère le groupe cyclique $\mathbb{Z}/9\mathbb{Z}$ et une trois-coloration équipotente. La proposition 1 affirme qu'il y a au moins 3 progressions arithmétiques à trois termes arc-en-ciel. Nous allons montrer qu'il ne peut y en avoir que 3.

Supposons qu'il existe une trois-coloration équipotente (A,B,C) de $\mathbb{Z}/9\mathbb{Z}$, telle que l'on ait que 3 progressions arithmétiques à trois termes arc-en-ciel.

On considère l'équation régulière $x-2y+z=0$, elle admet au moins 9 solutions monochromatiques (les solutions (x,x,x)).

Ainsi d'après les corollaires 1 ou 2, il y a au moins 18 solutions arc-en-ciel. S'il n'y a que trois progressions arithmétiques à trois termes arc-en-ciel, c'est d'une part que les progressions arithmétiques à trois termes correspondent à six solutions chacune, donc sont toutes de raison 3, d'autre part qu'il n'y a pas d'autre solution monochromatique.

Comme il n'y a que trois progressions arithmetiques de raison 3, elles sont toutes arc-en-ciel. Quitte à renommer les couleurs, on considère que A contient 0, B contient 3 et C contient 6.

Si A contient 1 alors le troisième élément de A est 2, 5 ou 8, mais alors on aurait une nouvelle progression monochromatique respectivement $(0,1,2)$, $(1,5,0)$, ou $(8,0,1)$, ce qui est impossible. Ainsi A ne contient pas 1, de même symétriquement, on montre que A ne contient pas 8.

Si A contient 2 alors le troisième élément de A est 4 ou 7 (car 1 est exclu d'après ce qui précède), mais alors on aurait une nouvelle progression monochromatique respectivement $(0,2,4)$ ou $(7,0,2)$, ce qui est impossible. Ainsi A ne contient pas 2, de même symétriquement, on montre que A ne contient pas 7.

Il ne reste plus qu'une possibilité, c'est que $A = \{0,4,5\}$, mais là encore $(5,0,4)$ est une solution monochromatique, ce qui est impossible.

Ainsi, si l'on considère le groupe $\mathbb{Z}/9\mathbb{Z}$ et une trois-coloration équipotente, on peut affirmer qu'il y a au moins 4 progressions arithmétiques à trois termes arc-en-ciel.

En fait, on peut de la même manière montrer qu'il ne peut y en avoir ni 4, ni 5 et donc que le nombre minimal de progressions arithmétiques à trois termes dans une trois-coloration équipotente de $\mathbb{Z}/9\mathbb{Z}$ est de 6 comme par exemple dans cette configuration:

$$A = \{0,1,2\},$$

$$B = \{3,5,7\},$$

$$C = \{4,6,8\}.$$

9. Autour de l'équation $ax^n + by^n + cz^n = 0$ dans $\mathbb{F}_q$, avec $abc \neq 0$

9.1. **Le cas n=3.** On ne considère plus ici une équation $ax^2 + by^2 + cz^2 = 0$, mais l'équation de degré 3: $ax^3 + by^3 + cz^3 = 0$, avec $abc \neq 0$ sur un corps fini $\mathbb{F}_q$. De même, nous voudrions en connaitre le nombre de solutions. Les méthodes utilisant la théorie des caractères en donnent le compte exact. Nous verrons ici que les arguments combinatoires développés ne suffisent pas pour répondre à cette question, mais donnent néanmoins quelques informations.

Bien sûr, les cas où le corps est de cardinal q une puissance de 3, ou si $q \equiv 2 \pmod 3$ ne présentent aucune difficulté car l'application $x \mapsto x^3$ y est bijective, ainsi le nombre S de solutions est de q^2.

Nous considèrerons désormais que $q \equiv 1 \pmod 3$. On notera $\mathbb{F}_q^3$ le sous-ensemble des cubes dans $\mathbb{F}_q$, et $\mathbb{F}_q^{*3} = \mathbb{F}_q^3 \setminus \{0\}$, il s'agit d'un sous-groupe multiplicatif d'indice 3 dans $\mathbb{F}_q^*$. On considère j_0 un élément arbitraire de $\mathbb{F}_q \setminus \mathbb{F}_q^3$ et la quatre-coloration $A = \{0\}$, $B = \mathbb{F}_q^{*3}$, $C = j_0.\mathbb{F}_q^{*3}$ et $D = j_0^2.\mathbb{F}_q^{*3}$. On a $|A| = 1$, $|B| = |C| = |D| = \frac{q-1}{3}$.

On remarque que toutes les équations du type $ax^3 + by^3 + cz^3 = 0$, avec $abc \neq 0$ peuvent se ramener à une des quatre suivantes suivant les classes auxquelles appartiennent les éléments a, b et c modulo $\mathbb{F}_q^{*3}$.

$$x^3 + y^3 + z^3 = 0, \tag{1}$$

$$x^3 + y^3 + j_0 z^3 = 0, \tag{2}$$

$$x^3 + y^3 + j_0^2 z^3 = 0, \tag{3}$$

$$x^3 + j_0 y^3 + j_0^2 z^3 = 0. \tag{4}$$

Pour l'équation (i), on note S_i, le nombre de solutions (x,y,z) avec $xyz \neq 0$. En travaillant à l'aide des caractères cubiques de $\mathbb{F}_q$, on obtient:

$$\begin{aligned} S_1 &= (q-1)(q-8+A'),\\ S_2 &= (q-1)(q-2-\frac{1}{2}(A'-9B')),\\ S_3 &= (q-1)(q-2-\frac{1}{2}(A'+9B')),\\ S_4 &= (q-1)(q+1+A'), \end{aligned}$$

où A' et B' sont des entiers relatifs tels que $4q = A'^2 + 27B'^2$ et $A' \equiv 1 \pmod 3$. Le premier nombre A' est alors uniquement déterminé, B' est déterminé au signe près (cette indétermination est naturelle, elle est due au choix de j_0). Une preuve combinatoire de ce résultat donnerait une détermination combinatoire de A' et B', ce qui n'a jamais été vu.

On s'intéresse aux relations liant les nombres de solutions de l'équation régulière $X+Y+Z=0$ et la coloration (A,B,C,D). On applique donc le corollaire 1 avec $d=3$ impair, on obtient alors que le nombre de solutions monochromatiques moins la moitié du nombre de solutions arc-en-ciel est exactement de:

$$\begin{aligned} &\frac{1}{|G|}\left(|A|^3+|B|^3+|C|^3+|D|^3-\frac{6}{2}\big(|A||B||C|+|A||B||D|+|A||C||D|+|B||C||D|\big)\right)\\ &= \frac{1}{q}\left(1+3\left(\frac{q-1}{3}\right)^3-3\left(3\left(\frac{q-1}{3}\right)^2+\left(\frac{q-1}{3}\right)^3\right)\right)\\ &= \frac{1}{q}\left(1-9\left(\frac{q-1}{3}\right)^2\right)\\ &= \frac{1}{q}(1-(q-1)^2)\\ &= 2-q. \end{aligned}$$

On détermine maintenant le nombre de solutions monochromatiques ou arc-en-ciel en fonction des S_i.

Bien évidemment on a $s_{(3,0,0,0)} = 1$. De plus, on a $\frac{S_1}{27} = s_{(0,3,0,0)} = s_{(0,0,3,0)} = s_{(0,0,0,3)}$, car l'application $(x,y,z) \mapsto (j_0x, j_0y, j_0z)$ établit des bijections entre les solutions de B^3, de C^3 et de D^3. Ainsi, on a exactement $1+\frac{S_1}{9}$ solutions monochromatiques.

Une solution arc-en-ciel qui n'a pas d'élément dans A correspond, à une permutation près, à 27 solutions de l'équation (4). Ainsi $s_{(0,1,1,1)} = \frac{S_4}{27}$. Une solution arc-en-ciel qui a un élément dans A donne une égalité entre un élément d'une couleur et l'opposé d'une autre couleur. Or les couleurs sont symétriques (x et $-x$ sont de même couleur) car -1 est un cube. Il n'y a donc pas de solution arc-en-ciel avec un élément dans A. Ainsi on a $s_{(1,0,1,1)} = s_{(1,1,0,1)} = s_{(1,1,1,0)} = 0$. On a alors $6\frac{S_4}{27}$ solutions arc-en-ciel.

On en déduit alors l'égalité:

$$1+\frac{S_1}{9}-\frac{6}{2}\frac{S_4}{27} = 2-q.$$

Ce que l'on simplifie pour obtenir:

$$S_4 - S_1 = 9(q-1).$$

Cette relation est issue de l'application du corollaire 1, qui donne une relation entre des nombres de solutions, en distinguant un vecteur de l'espace $R \cap P$. Cet espace est, pour $d=3$ et $c=4$, de dimension 2. Une autre relation est donnée par

le compte de toutes les solutions (soit par le vecteur $v_{(0,0,0,0)}$ de R):

$$\begin{aligned}\sum_{(a,b,c,d)\in I_{4,3}} s_{(a,b,c,d)} &= \frac{1}{q}\sum_{(a,b,c,d)\in I_{4,3}} \binom{3}{a\ b\ c\ d}|A|^a|B|^b|C|^c|D|^d \\ &= \frac{1}{q}(|A|+|B|+|C|+|D|)^3 \\ &= q^2.\end{aligned}$$

On a deja donné des expressions des solutions monochromatiques et arc-en-ciel en fonction des S_i. On établit de même pour les autres nombres de solutions:

$$\begin{aligned}s_{(2,1,0,0)} = s_{(2,0,1,0)} = s_{(2,0,0,1)} &= 0,\\ s_{(1,2,0,0)} = s_{(1,0,2,0)} = s_{(1,0,0,2)} &= 3\frac{q-1}{3},\\ s_{(0,2,1,0)} = s_{(0,0,2,1)} = s_{(0,1,0,2)} &= 3\frac{S_2}{27},\\ s_{(0,1,2,0)} = s_{(0,0,1,2)} = s_{(0,2,0,1)} &= 3\frac{S_3}{27}.\end{aligned}$$

La relation $\sum_{(a,b,c,d)\in I_{4,3}} s_{(a,b,c,d)} = q^2$ donne alors:

$$1+3\frac{S_1}{27}+6\frac{S_4}{27}+3(q-1)+9\frac{S_2}{27}+9\frac{S_3}{27}=q^2.$$

Ce que l'on simplifie pour obtenir:

$$S_1+3(S_2+S_3)+2S_4 = 9(q-1)(q-2).$$

Les deux relations:

$$\left|\begin{array}{rcl} S_4-S_1 &=& 9(q-1)\\ S_1+3(S_2+S_3)+2S_4 &=& 9(q-1)(q-2).\end{array}\right.$$

permettent ainsi d'écrire toutes les relations entre les S_i indépendantes de A' et B'.

On peut aussi considérer le système équivalent suivant:

$$\left|\begin{array}{rcl} S_1+S_2+S_3 &=& 3(q-1)(q-4)\\ S_2+S_3+S_4 &=& 3(q-1)^2.\end{array}\right.$$

Que permettent aussi d'obtenir les deux vecteurs $v_{(0,2,0,0)}$ et $v_{(0,1,1,0)}$ de R.

9.2. **Autour de l'équation $ax^n+by^n+cz^n=0$ dans $\mathbb{F}_q$, avec $abc\neq 0$.** Pour tout $x\in\mathbb{F}_q$, on a $x^q=x$, ainsi, on peut se restreindre au cas où $n<q$. De plus lorsque $(q-1,n)=1$, $x\mapsto x^n$ est une bijection de $\mathbb{F}_q$ dans lui-même, ainsi le nombre S de solutions est de q^2.

On se ramène ainsi au cas où n divise $q-1$. On notera $\mathbb{F}_q^n$ le sous-ensemble des puissances $n^{\text{ièmes}}$ dans $\mathbb{F}_q$, et $\mathbb{F}_q^{*n}=\mathbb{F}_q^n\setminus\{0\}$, il s'agit d'un sous-groupe multiplicatif d'indice n dans $\mathbb{F}_q^*$. On considère j_0 un élément non nul d'ordre multiplicatif n de $\mathbb{F}_q\setminus\mathbb{F}_q^n$ et la $(n+1)$-coloration $A_\infty=\{0\}$, et pour $i\in[0,n-1]$, $A_i=j_0^i.\mathbb{F}_q^{*n}$. On a $|A_\infty|=1$, et pour $i\in[0,n-1]$, $|A_i|=\frac{q-1}{n}$.

On considère l'équation $ax^n+by^n+cz^n=0$, et on s'intéresse aux solutions (x,y,z) avec $xyz\neq 0$. On peut se ramener à une équation de la forme:

$$E_{(\alpha,\beta,\gamma)}: j_0^\alpha x^n+j_0^\beta y^n+j_0^\gamma z^n=0,$$

avec (α,β,γ) sont trois éléments de $\mathbb{Z}/n\mathbb{Z}$, suivant les classes auxquelles appartiennent a, b et c modulo $\mathbb{F}_q^{*n}$.

De plus pour un élément quelconque $\delta\in\mathbb{Z}/n\mathbb{Z}$, les équations $E_{(\alpha+\delta,\beta+\delta,\gamma+\delta)}$ et $E_{(\alpha,\beta,\gamma)}$, sont proportionnelles, elles ont donc les mêmes solutions. De même, pour une permutation σ de trois éléments, les équations $E_{(\alpha,\beta,\gamma)}$ et $E_{\sigma.(\alpha,\beta,\gamma)}$ admettent

autant de solutions (x,y,z) avec $xyz \neq 0$. Cela définit une action de $G = \mathfrak{S}_3 \times \mathbb{Z}/n\mathbb{Z}$ sur $(\mathbb{Z}/n\mathbb{Z})^3$.

On définit alors un type d'équation par une orbite de $(\mathbb{Z}/n\mathbb{Z})^3$ sous l'action de G. Toutes les équations d'un même type admettent alors un même nombre de solutions. On définit alors $S_{\overline{(\alpha,\beta,\gamma)}}$, où $\overline{(\alpha,\beta,\gamma)}$ désigne l'orbite de (α,β,γ) sous l'action de G, le nombre de solutions (x,y,z) avec $xyz \neq 0$, de chacune des l'équations $E_{(\alpha',\beta',\gamma')}$, avec (α',β',γ') dans $\overline{(\alpha,\beta,\gamma)}$.

On peut dénombrer le nombre T_n de types d'équation en fonction de la divisibilité de n par 3:

$$\text{Si} \quad 3 \mid n, \quad T_n = \left(\frac{\binom{n}{3}}{n} - \frac{1}{3} + 1 \right) + (n-1) + 1,$$

$$\text{et si} \quad 3 \not| n, \quad T_n = \left(\frac{\binom{n}{3}}{n} \right) + (n-1) + 1.$$

Où le premier terme correspond aux triplets (α,β,γ), où α, β et γ sont distincts deux à deux, le second correspond aux triplets où seulement deux parmi α, β et γ sont égaux et le dernier terme correspond au cas où $\alpha = \beta = \gamma$ (donc à l'équation $x^n + y^n + z^n = 0$).

Si l'on considère l'équation régulière $X + Y + Z = 0$ et la coloration $\{A_i,\ i \in [0, n-1] \cup \{\infty\}\}$. Chaque solution (x,y,z) avec $xyz \neq 0$ d'une coloration donnée $x \in A_\alpha$, $y \in A_\beta$ et $z \in A_\gamma$, correspond à n^3 solutions de l'équation $E_{(\alpha,\beta,\gamma)}$.

Les vecteurs $v_{(i_0,\ldots,i_{(n-1)},i_\infty)}$ avec $\sum_{k\in[0,n-1]\cup\{\infty\}} i_k = 2$ donne alors des relations liant les différents nombres de solutions $S_{\overline{(\alpha,\beta,\gamma)}}$ et les nombres de solutions avec $xyz = 0$. Ces derniers peuvent être déterminés connaissant la classe à laquelle appartient -1 modulo $\mathbb{F}_q^{*n}$. On remarque cependant qu'une relation issue d'un vecteur $v_{(i_0,\ldots,i_{(n-1)},i_\infty)}$ avec $i_\infty \neq 0$ ne peut faire intervenir aucun des nombres $S_{\overline{(\alpha,\beta,\gamma)}}$, car elle impose que l'une des valeurs des inconnues soit nulle.

On s'intéresse ainsi aux vecteurs $v_{(i_0,\ldots,i_{(n-1)},i_\infty)}$ avec $\sum_{k\in[0,n-1]} i_k = 2$ et $i_\infty = 0$. Un tel vecteur est déterminé par la donnée d'un couple de $(\mathbb{Z}/n\mathbb{Z})^2$, par $v_{(\alpha,\beta)} = v_{(i_0,\ldots,i_{(n-1)},i_\infty)}$, avec $i_\infty = 0$, $i_k = 0$, si $\beta \neq k \neq \alpha$ et $i_\alpha = i_\beta = 1$, si $\alpha \neq \beta$ et $i_\alpha = 2$ si $\alpha = \beta$.

De même que pour les nombres de solutions si $\delta \in \mathbb{Z}/n\mathbb{Z}$, on constate que les relations issues de $v_{(\alpha,\beta)}$ et $v_{(\alpha+\delta,\beta+\delta)}$ sont égales. De même, si $\sigma \in \mathfrak{S}_2$, les relations issues de $v_{(\alpha,\beta)}$ et $v_{\sigma.(\alpha,\beta)}$ sont égales. On obtient autant de relations distinctes que d'orbites dans $(\mathbb{Z}/n\mathbb{Z})^2$ sous l'action de $\mathfrak{S}_2 \times \mathbb{Z}/n\mathbb{Z}$.

On compte alors $\left\lceil \frac{n+1}{2} \right\rceil$ relations linéaires indépendantes entre les T_n nombres de solutions $S_{\overline{(\alpha,\beta,\gamma)}}$.

CHAPITRE 2

AUTOUR DE LA MÉTHODE ISOPÉRIMÉTRIQUE

Ce chapitre est constitué de deux articles "*Un nouveau point de vue isopérimétrique appliqué au théorème de Kneser*" et "*The Isoperimetric Method in non-abelian groups with an application to optimally small sumsets*" (tous les deux soumis pour publication) chacun immédiatement suivi d'un complément.

UN NOUVEAU POINT DE VUE ISOPÉRIMÉTRIQUE APPLIQUÉ AU THÉORÈME DE KNESER

par

Éric Balandraud

Résumé. — In additive number theory, Kneser's theorem is now a key element in a large number of proofs. Recently, Hamidoune developped a different approach, that he called the isoperimetric method, and that allowed him to provide news proofs and generalizations of classical results. However, it seems that this method cannot provide a new proof of Kneser's theorem itself. In this article, we present a new isoperimetric point-of-view that, among others, yields a second proof of Kneser's theorem.

En théorie additive des nombres, le théorème de Kneser joue aujourd'hui un rôle central dans un grand nombre de démonstrations. Récemment, Hamidoune a développé une approche alternative au théorème de Kneser, qu'il appela méthode isopérimétrique et qui lui permit de donner de nouvelles preuves et de nombreuses généralisations de résultats classiques. Cependant, il ne semble pas possible par cette méthode de prouver le théorème de Kneser lui-même. Dans cette article, nous proposons une nouvelle approche de type isopérimétrique, qui nous permet entre autres de donner une seconde preuve du théorème de Kneser.

Introduction

Soit $(G,+)$ un groupe (non nécessairement abélien). Soient A et B deux sous-ensembles de G et g un élément de G, on note $A+B=\{a+b|\ a\in A,\ b\in B\}$ et $g+B=\{g\}+B$. Par convention, on pose $\emptyset+B=\emptyset$.

Les premiers résultats sur l'addition d'ensembles sont dûs à Cauchy notamment ce qu'on appelle maintenant le théorème de Cauchy-Davenport (et ses applications). Démontré en premier lieu par Cauchy en 1813 [**3**], celui-ci l'utilisa pour démontrer que dans $\mathbb{Z}/p\mathbb{Z}$ tout élément est somme de k puissances k-ièmes. Le théorème fut redécouvert en 1935 par Davenport [**6**], mais ce n'est que douze ans plus tard qu'il réalisa qu'il avait été précédé [**7**].

Théorème 1. — *(Théorème de Cauchy-Davenport) Soient p un nombre premier, A et B deux sous-ensembles non vides de $\mathbb{Z}/p\mathbb{Z}$, on a :*

$$|A+B|\geqslant \min(p,|A|+|B|-1).$$

Le théorème de Vosper [**25, 26**] (qui date de 1956) précise la structure des ensembles intervenant dans le théorème de Cauchy-Davenport, lorsque la somme est de cardinal minimal, c'est-à-dire dans les cas d'égalité.

Théorème 2. — *(Théorème de Vosper) Soient p un nombre premier, A et B deux sous-ensembles de $\mathbb{Z}/p\mathbb{Z}$ contenant chacun au moins deux éléments et tels que $|A+B| < p-1$. Si $|A+B| = |A|+|B|-1$, A et B sont des progressions arithmétiques de même raison.*

Les applications de ces résultats sont extrêmement nombreuses en théorie additive des nombres. Certaines généralisations aux groupes abéliens sont bien connues, comme le théorème de Chowla dans les groupes cycliques [**4**], ou le théorème de Mann [**22**], qui est le premier à faire intervenir explicitement des sous-groupes :

Théorème 3. — *(Théorème de Mann) Soient G un groupe abélien fini, et A et B deux sous-ensembles non vides de G tels que $A+B \neq G$. Il existe un sous-groupe strict H de G (i.e. $H \neq G$), tel que :*

$$|A+B| \geqslant |A| + |H+B| - |H|.$$

Dans un groupe abélien G, on appelle période d'un sous-ensemble B de G, l'ensemble des $g \in G$, tel que $g+B = B$. Il est immédiat de constater que la période d'un sous-ensemble B est un sous-groupe de G. On dit qu'un ensemble est périodique si sa période n'est pas réduite au sous-groupe trivial.

Le théorème suivant dû à Kneser [**20, 21**] s'est révélé être un outil extrêmement important en théorie additive des nombres :

Théorème 4. — *(Théorème de Kneser) Soient G un groupe abélien, A et B deux sous-ensembles finis non vides de G, si H désigne la période de $A+B$, alors on a :*

$$|A+B| \geqslant |A+H| + |B+H| - |H|.$$

On constate tout d'abord que le théorème de Kneser implique les théorèmes de Cauchy-Davenport et de Mann cités précédemment. De plus, les applications du théorème de Kneser sont elles aussi très nombreuses et dans des domaines assez divers, notamment pour les ensembles d'entiers de petite somme, ou pour les ensembles "sum-free" dans les groupes abéliens. Certaines de ces applications sont développées dans l'ouvrage de référence de Nathanson [**23**].

Dans [**19**], Kemperman exposa une méthode générale, généralisant le théorème de Vosper, basée sur des transformations des ensembles considérés. Plus récemment, Hamidoune [**11, 12, 13, 14, 16**], développa une méthode qu'il appela isopérimétrique, et qui permit de nombreuses généralisations des théorèmes sur l'addition d'ensembles comme par exemple une généralisation du théorème $3k-3$ de Freiman [**17, 18**], une amélioration de la détermination de la fonction X d'Erdős-Graham [**24**] ou la résolution du problème de Frobenius [**15**]. Cependant elle ne semblait pas en mesure de conduire facilement à une nouvelle preuve du théorème de Kneser.

Le propos de cet article est d'introduire une nouvelle approche de type isopérimétrique fortement inspirée de celle d'Hamidoune, mais plus adaptée à l'étude des ensembles de petites sommes. On pourra apprécier l'intérêt de cette nouvelle approche par le fait qu'elle nous permet de donner une seconde preuve du théorème de Kneser.

Parmi les différentes formulations du théorème de Kneser, nous nous intéresserons plus particulièrement à celle-ci, qui peut se comprendre comme une caractérisation des paires de petite somme :

Théorème 5. — *(Théorème de Kneser) Soient G un groupe abélien, A et B deux sous-ensembles finis non vides de G, tels que :*

$$|A+B| < |A| + |B| - 1,$$

alors $A+B$ est périodique et si H est la période de $A+B$, on a :

$$|A+B| = |A+H| + |B+H| - |H|.$$

L'équivalence entre les formulations des théorèmes 4 et 5 se démontre par un passage au quotient.

Pour l'étude des paires (A,B) de sous-ensembles d'un groupe G de petite somme (i.e : $|A+B| < |A| + |B| - 1$ et $A+B \neq G$), on est amené à s'intéresser pour un ensemble B donné aux valeurs de la fonction : $\Phi_B : X \mapsto |X+B| - |X|$. La méthode isopérimétrique d'Hamidoune caractérise déjà les ensembles A qui atteignent le minimum $\kappa_1(B)$ de cette fonction. Mais le théorème de Kneser est plus général et donne un résultat pour tous les ensembles qui atteignent les valeurs de cette fonction inférieures à $|B|-1$. Le principe de notre nouvelle approche isopérimétrique consiste précisément à considérer les valeurs successives prises par la Φ_B entre $\kappa_1(B)$ et $|B|-1$, et les ensembles pour lesquels la fonction Φ_B atteint ces valeurs.

Pour cela, nous étudierons dans la premiere partie les propriétés d'outils additifs purement ensemblistes relatifs à un ensemble B. Nous définirons alors une certaine famille de sous-ensembles dépendant de l'ensemble B. Le but principal de cette première partie est de restreindre l'étude de la fonction Φ_B à cette famille de sous-ensembles.

Nous développerons dans une deuxième partie le principe des idées isopérimétriques (reprenant celles de Hamidoune, généralisant certaines), qui s'exprimera sous la forme d'inégalités liées à cette fonction Φ_B. Ces propriétés forment la base de notre nouvelle approche isopérimétrique. Elles seront exposées dans un cadre général (dans un groupe non nécessairement abélien), car cette nouvelle formulation permet également d'envisager l'étude de problèmes dans un cadre non abélien [**27, 1**].

Nous donnons dans la partie 3.1 un premier résultat dû à Hamidoune, concernant les ensembles minimisant la fonction Φ_B dans un groupe abélien. Puis en 3.2, nous donnons un résultat original de structure concernant cette fois, tous les ensembles tels que leurs valeurs par Φ_B soient inférieures à $|B|-1$ dans le cas abélien. De ce résultat, on déduit rapidemment une nouvelle preuve du théorème de Kneser dans la partie 4.

1. Outils additifs de pivot $B \subset G$

Dans toute cette partie, on considère un groupe G non nécessairement abélien et un sous-ensemble B de G.

1.1. L'application $P_B : X \mapsto G \smallsetminus ((G \smallsetminus (X+B))-B)$. — On note $\mathbf{P}(G)$, l'ensemble des parties de G.

On s'intéresse aux propriétés de l'application :

$$P_B : \left| \begin{array}{ccc} \mathbf{P}(G) & \to & \mathbf{P}(G) \\ X & \mapsto & G \smallsetminus ((G \smallsetminus (X+B)) - B). \end{array} \right.$$

L'étude de cette application permet de remarquer que pour un ensemble X donné, l'ensemble $P_B(X)$ est caractéristique (au sens du corollaire 9) de la somme $X + B$. Cela nous permettra par la suite de limiter l'étude aux ensembles images de P_B.

Lemme 6. — *Pour tout sous-ensemble X de G, on a :*

$$X \subset P_B(X).$$

Démonstration. — Supposons qu'il existe $x \in X \smallsetminus P_B(X)$. Comme x n'est pas dans $P_B(X)$, il existe $x' \in G \smallsetminus (X + B)$ et $b \in B$, tels que $x = x' - b$. Cela implique que $x' = x + b$, ce qui est impossible car x' est par définition dans le complémentaire de $X + B$. On a donc l'inclusion $X \subset P_B(X)$. □

Proposition 7. — *Pour tout sous-ensemble X de G, on a :*

$$X + B = P_B(X) + B.$$

Démonstration. — D'après le lemme 6, on a $X \subset P_B(X)$ d'où l'inclusion $X + B \subset P_B(X)+B$. De plus, si $y \in (P_B(X)+B) \smallsetminus (X+B)$, alors d'une part il existe $z \in P_B(X)$ et $b \in B$ tels que $y = z + b$, et d'autre part $y \in G \smallsetminus (X + B)$. Cela implique que $z = y-b \in (G \smallsetminus (X+B))-B$, le complémentaire de $P_B(X)$, il y a donc contradiction. Donc $P_B(X) + B \subset X + B$, d'où l'égalité. □

Corollaire 8. — *L'application P_B vérifie $P_B^2 = P_B$.*

Démonstration. — Pour tout sous-ensemble X de G, on a d'après la proposition 7 :

$$\begin{aligned} P_B^2(X) &= G \smallsetminus ((G \smallsetminus (P_B(X) + B)) - B) \\ &= G \smallsetminus ((G \smallsetminus (X + B)) - B) \\ &= P_B(X). \end{aligned}$$

□

Corollaire 9. — *Pour tous sous-ensembles X et Y de G, on a $X + B = Y + B$ si et seulement si $P_B(X) = P_B(Y)$.*

Démonstration. — Si on a l'égalité $X + B = Y + B$, alors nécessairement, on a $G \smallsetminus ((G \smallsetminus (X + B)) - B) = G \smallsetminus ((G \smallsetminus (Y + B)) - B)$, c'est-à-dire $P_B(X) = P_B(Y)$.

Si $P_B(X) = P_B(Y)$, alors d'après la proposition 7,

$$X + B = P_B(X) + B = P_B(Y) + B = Y + B.$$

□

C'est cette dernière propriété qui fait de $P_B(X)$ un ensemble caractéristique de la somme $X + B$.

On peut aussi remarquer que l'ensemble $P_B(X)$ peut être défini comme l'ensemble maximal M tel que $M + B \subset X + B$.

1.2. Propriétés de l'image $\mathbf{C}_B$ de P_B. — On note $\mathbf{C}_B$ l'ensemble des images de $\mathbf{P}(G)$ par P_B,

$$\mathbf{C}_B = P_B(\mathbf{P}(G)).$$

Les éléments de $\mathbf{C}_B$ seront appelés les cellules pour B. Elles sont caractérisées naturellement comme étant les solutions de $P_B(X) = X$.

Ce sont ces cellules qui nous intéressent, car elles sont caractéristiques de leurs sommes avec B, nous allons donc pour les étudier, déterminer leurs propriétés notamment de translation par un élément du groupe ou d'intersection.

Remarque 1. — *On remarque que $P_B(\emptyset) = \emptyset$, ainsi $\emptyset \in \mathbf{C}_B$. De même, on a $P_B(G) = G$, ainsi $G \in \mathbf{C}_B$.*

Proposition 10. — *Pour tout sous-ensemble X de G, et tout $g \in G$, on a :*

$$P_B(g + X) = g + P_B(X).$$

Démonstration. — Par associativité, on a $(g+X)+B = g+(X+B)$. La fonction de translation de G dans G, qui à x associe $g + x$ étant bijective, quels que soient $g \in G$ et $X \subset G$, on a : $G \setminus (g + X) = g + (G \setminus X)$. On obtient :

$$\begin{aligned}(G \setminus ((g + X) + B)) - B &= (g + G \setminus (X + B)) - B \\ &= g + (G \setminus (X + B) - B).\end{aligned}$$

Il suffit alors de repasser au complémentaire pour obtenir $P_B(g + X) = g + G \setminus (G \setminus (X + B) - B) = g + P_B(X)$. □

Corollaire 11. — *L'ensemble $\mathbf{C}_B$ est stable par translation à gauche par un singleton.*

Dans la suite, on note $\pi(X)$ l'ensemble des $g \in G$ tels que $g + X = X$. Comme dans le cas abélien, il est immédiat de constater que $\pi(X)$ est un sous-groupe de G, qu'on appelle période à gauche de X.

Corollaire 12. — *Pour tout sous-ensemble X de G, on a l'inclusion :*

$$\pi(X) \subset \pi(P_B(X)).$$

Démonstration. — Si $g \in \pi(X)$, alors $g + X = X$, ainsi d'après la proposition 10 $g + P_B(X) = P_B(g + X) = P_B(X)$. Ce qui signifie que $g \in \pi(P_B(X))$. □

Proposition 13. — *L'application P_B est croissante : pour tous sous-ensembles X et Y de G, si $X \subset Y$ alors on a $P_B(X) \subset P_B(Y)$.*

Démonstration. — Comme $X \subset Y$, en additionnant B à droite et en passant au complémentaire, on a $G \smallsetminus (Y + B) \subset G \smallsetminus (X + B)$. Puis de façon similaire pour $-B$, on obtient : $G \smallsetminus ((G \smallsetminus (X + B)) - B) \subset G \smallsetminus ((G \smallsetminus (Y + B)) - B)$, c'est-à-dire $P_B(X) \subset P_B(Y)$. □

Corollaire 14. — *L'ensemble $\mathbf{C}_B$ est stable par intersection : si C_1 et C_2 sont deux éléments de $\mathbf{C}_B$, alors $C_1 \cap C_2 \in \mathbf{C}_B$.*

Démonstration. — Soit $Z = C_1 \cap C_2$. Comme $Z \subset C_1$, d'après la proposition 13 et le corollaire 8, on a $P_B(Z) \subset P_B(C_1) = C_1$. De même, on a $P_B(Z) \subset P_B(C_2) = C_2$. Ainsi $P_B(Z) \subset C_1 \cap C_2 = Z$. De plus, le lemme 6 nous donne $Z \subset P_B(Z)$, donc on a $Z = P_B(Z)$, ce qui signifie que $Z \in \mathbf{C}_B$. □

Notons bien que tout ce qui a été établi jusqu'ici l'a été dans un cadre général. Nous voyons maintenant une particularité du cas où le groupe est abélien.

Proposition 15. — *Si G est abélien, pour tout sous-ensemble X de G, on a :*

$$-P_B(X) = P_{-B}(-X).$$

Démonstration. — Puisque G est abélien, on peut en effet écrire $-(X+B) = -X-B$, d'où :

$$\begin{aligned} P_{-B}(-X) &= G \smallsetminus (G \smallsetminus (-X - B) + B) \\ &= G \smallsetminus (G \smallsetminus (-(X + B)) + B) \\ &= G \smallsetminus ((-(G \smallsetminus (X + B))) + B) \\ &= G \smallsetminus (-(G \smallsetminus (X + B) - B)) \\ &= -(G \smallsetminus (G \smallsetminus (X + B) - B)) \\ &= -P_B(X). \end{aligned}$$

□

Corollaire 16. — *Si G est abélien, $\mathbf{C}_B$ et $\mathbf{C}_{-B}$ sont symétriques : pour tout sous-ensemble X de G, $X \in \mathbf{C}_B$ si et seulement si $-X \in \mathbf{C}_{-B}$.*

Démonstration. — En effet, si $X \in \mathbf{C}_B$, d'après le corollaire 8, on a $X = P_B(X)$, ainsi d'après la proposition 15, on a $-X = P_{-B}(-X)$, et $-X$ est bien dans l'image de P_{-B}. On obtient la réciproque en échangeant les rôles de B et $-B$. □

1.3. Dualité additive $D_B : X \mapsto G \smallsetminus (X+B)$. — Parmi les propriétés des cellules qui nous seront utiles, il se trouve que celles pour B et celles pour $-B$ entretiennent des relations privilégiées que nous allons détailler maintenant.

On considère la fonction suivante :

$$D_B : \left| \begin{array}{ccc} \mathbf{P}(G) & \to & \mathbf{P}(G) \\ X & \mapsto & G \smallsetminus (X + B). \end{array} \right.$$

On remarque immédiatement que :

$$P_B = D_{-B} \circ D_B.$$

Lemme 17. — *Pour tout sous-ensemble X de G, on a :*

$$D_B(X) = D_B(P_B(X)).$$

Démonstration. — En effet, on remarque que $D_B(X)$ ne dépend que de la somme $X + B$, il suffit alors d'utiliser la proposition 7 :

$$D_B(X) = G \smallsetminus (X + B) = G \smallsetminus (P_B(X) + B) = D_B(P_B(X)).$$

□

L'étude de l'application D_B permet de remarquer qu'elle établit une bijection de $\mathbf{C}_B$ sur $\mathbf{C}_{-B}$, d'inverse D_{-B}. C'est cette propriété qui justifie l'appellation de dualité additive.

Proposition 18. — *L'image de la fonction D_B est $\mathbf{C}_{-B}$. De plus D_B est une bijection de $\mathbf{C}_B$ sur $\mathbf{C}_{-B}$, d'inverse D_{-B}.*

Démonstration. — Le lemme 17 permet de remarquer que pour $X \subset G$, on a $D_B(X) \in \mathbf{C}_{-B}$, en effet :

$$\begin{aligned} P_{-B}(D_B(X)) &= (D_B \circ D_{-B} \circ D_B)(X) \\ &= D_B(P_B(X)) \\ &= D_B(X). \end{aligned}$$

Ainsi D_B est à image dans $\mathbf{C}_{-B}$.

Comme P_B est une bijection de $\mathbf{C}_B$ sur lui-même (P_B est même trivial de $\mathbf{C}_B$ sur lui-même) et que $P_B = D_{-B} \circ D_B$, alors D_B est une injection de $\mathbf{C}_B$ sur $\mathbf{C}_{-B}$ et D_{-B} une surjection de $\mathbf{C}_{-B}$ sur $\mathbf{C}_B$. Il suffit d'échanger les rôles de B et $-B$ pour obtenir les propriétés inverses. Ainsi D_B et D_{-B} sont des bijections respectivement de $\mathbf{C}_B$ sur $\mathbf{C}_{-B}$ et de $\mathbf{C}_{-B}$ sur $\mathbf{C}_B$ et inverses l'une de l'autre. □

Proposition 19. — *Pour tout sous-ensemble X de G et tout $g \in G$, on a :*

$$D_B(g + X) = g + D_B(X).$$

Démonstration. — Par associativité, on a $(g+X)+B = g+(X+B)$, puis en passant au complémentaire, $G \smallsetminus ((g+X)+B) = g+G \smallsetminus (X+B)$, d'où $D_B(g+X) = g+D_B(X)$. □

Corollaire 20. — *On a l'inclusion :*

$$\pi(X) \subset \pi(D_B(X)).$$

De plus, pour tout $C \in \mathbf{C}_B$, on a l'égalité :

$$\pi(C) = \pi(D_B(C)).$$

Démonstration. — Si $g \in \pi(X)$, alors $g + X = X$, ainsi d'après la proposition 19, $g + D_B(X) = D_B(g+X) = D_B(X)$, donc $g \in \pi(D_B(X))$. On obtient alors l'inclusion $\pi(X) \subset \pi(D_B(X))$.

De plus, si $C \in \mathbf{C}_B$, l'inclusion précédente appliquée à $-B$, et $X = D_B(C)$, donne $\pi(D_B(C)) \subset \pi(D_{-B}(D_B(C)))$. Comme C est une cellule, on a $D_{-B}(D_B(C)) = C$. On obtient donc $\pi(C) = \pi(D_B(C))$. □

Proposition 21. — *L'application D_B est décroissante : pour tous sous-ensembles X et Y de G, si $X \subset Y$, alors on a $D_B(Y) \subset D_B(X)$.*

Démonstration. — Si $X \subset Y$, alors en additionnant B à droite, on a $X+B \subset Y+B$, puis en passant au complémentaire, on obtient $G \smallsetminus (Y+B) \subset G \smallsetminus (X+B)$, ce qui signifie $D_B(Y) \subset D_B(X)$. □

Proposition 22. — *Pour tous sous-ensembles X et Y de G, on a :*

$$P_B(X \cup Y) = D_{-B}(D_B(X) \cap D_B(Y)).$$

Démonstration. — On montre pour cela que $D_B(X) \cap D_B(Y) = D_B(X \cup Y)$, en écrivant la suite d'identités ensemblistes :

$$\begin{aligned} D_B(X) \cap D_B(Y) &= (G \smallsetminus (X+B)) \cap (G \smallsetminus (Y+B)) \\ &= G \smallsetminus ((X+B) \cup (Y+B)) \\ &= G \smallsetminus ((X \cup Y) + B) \\ &= D_B(X \cup Y). \end{aligned}$$

Ainsi, on obtient $D_{-B}(D_B(X) \cap D_B(Y)) = D_{-B}(D_B(X \cup Y))$, c'est à dire $P_B(X \cup Y) = D_{-B}(D_B(X) \cap D_B(Y))$. □

Toutes les propriétés précédentes de D_B sont établies sans aucune hypothèse sur G, nous allons maintenant voir une conséquence de la commutativité de G.

Proposition 23. — *Si G est abélien, pour tout sous-ensemble X de G, on a :*

$$D_B(-X) = -D_{-B}(X).$$

Démonstration. — Puisque G est abélien, on a $-(X+B) = -X - B$, ainsi :

$$\begin{aligned} D_B(-X) &= G \smallsetminus (-X + B) \\ &= G \smallsetminus (-(X - B)) \\ &= -(G \smallsetminus (X - B)) \\ &= -D_{-B}(X). \end{aligned}$$

□

1.4. Contributions de B. — Dans les parties précédentes, aucune supposition n'avait été faite sur l'ensemble B. Nous allons voir ici que des propriétés propres à l'ensemble B peuvent avoir des conséquences intéressantes pour l'études de ses cellules.

On note $\mathbf{P}_f(G)$ l'ensemble des parties finies de G.

Lemme 24. — *Soit G un groupe. Si B est un sous-ensemble fini et non vide de G, l'image de tout sous-ensemble fini de G par P_B est fini, autrement dit :*

$$P_B(\mathbf{P}_f(G)) \subset \mathbf{P}_f(G).$$

Démonstration. — Si G est fini, c'est évident. On ne s'intéresse donc qu'au cas où G est infini. Si X est un sous-ensemble fini de G, alors $X+B$ est aussi fini. De plus comme d'après le lemme 7, on a $X+B = P_B(X)+B$, alors $P_B(X)+B$ est fini lui aussi, ainsi $P_B(X)$ est fini. □

Lemme 25. — *Si G est un groupe infini et B est un sous-enemble fini de G, alors D_B est une bijection de l'ensemble des cellules finies de $\mathbf{C}_B$ sur l'ensemble des cellules de complémentaire fini de $\mathbf{C}_{-B}$.*

Démonstration. — La proposition 18 assure que D_B est à image dans $\mathbf{C}_{-B}$. Si C est une cellule finie pour B, alors $C+B$ est fini, et donc $D_B(C) = G \setminus (C+B)$ est de complémentaire fini.

De plus, si $D_B(C)$ est une cellule pour $-B$ de complémentaire fini alors $D_B(C)-B$ est aussi de complémentaire fini et $C = P_B(C) = G \setminus (D_B(C) - B)$ est fini. □

Lemme 26. — *Soit G un groupe. Si B est un sous-ensemble contenant 0 de G, alors pour tout $X \subset G$, les trois ensembles X, $(X+B)\setminus X$ et $D_B(X)$ forment une partition du groupe G.*

Démonstration. — Comme $0 \in B$, on a $X \subset (X+B)$, ainsi X et $(X+B)\setminus X$ forment une partition de $X+B$. Par définition, $D_B(X)$ est le complémentaire de $X+B$ dans G. Ainsi X, $(X+B)\setminus X$ et $D_B(X)$ forment une partition de G. □

Proposition 27. — *Soit G un groupe. Si B est un sous-ensemble contenant 0, alors pour tout cellule C pour B, on a :*

$$(C+B)\setminus C = (D_B(C) - B)\setminus D_B(C).$$

Démonstration. — D'après le lemme 26, C, $(C+B)\setminus C$ et $D_B(C)$ forment une partition de G. De même, $0 \in (-B)$, ainsi $D_B(C)$, $(D_B(C)-B)\setminus D_B(C)$ et $D_{-B}(D_B(C)) = C$ forment aussi une partition de G. Ces deux partitions comptent trois éléments chacune et ont deux éléments communs : C et $D_B(C)$. Ainsi il s'agit exactement de la même partition de G et donc $(C+B)\setminus C = (D_B(C) - B)\setminus D_B(C)$. □

Remarque 2. — *La notion de dualité additive apparaît implicitement dans l'énoncé du Théorème de Vosper. En effet, la condition $|A+B| < p-1$ est équivalente à $|D_B(A)| \geqslant 2$. On a alors dans les hypothèses du théorème à la fois $|A| \geqslant 2$ et $|D_B(A)| \geqslant 2$.*

2. Idées isopérimétriques

Dorénavant on considère un groupe G et B un sous-ensemble fini non vide de G.

2.1. Définition et premières propriétés. — On s'intéresse aux valeurs de l'application :

$$\Phi_B : \left| \begin{array}{ccc} \mathbf{P}_f(G) & \to & \mathbb{N} \\ X & \mapsto & |X+B| - |X|, \end{array} \right.$$

qui, lorsque $0 \in B$, donne le nombre d'éléments du périmètre de X dans le graphe de Cayley de (G, B), (graphe dont les sommets sont les éléments de G et les arêtes les paires (g_1, g_2), telles qu'il existe $b \in B$ tel que $g_1 + b = g_2$). Les graphes de Cayley occupent une place importante en théorie des graphes, voir le chapitre 6 de [**10**]. C'est à partir du point de vue de la théorie des graphes que la méthode a été qualifiée d'isopérimétrique par Hamidoune.

Cette fonction va nous permettre de classer les cellules pour B. Nous nous intéressons principalement aux ensembles de petit périmètre et donc aux cellules de petit périmètre. On établit dans cette partie les propriétés de Φ_B et ses relations avec les cellules pour B, en particulier le fait que Φ_B prend toujours une valeur moindre sur une cellule que sur un ensemble qui donne la même somme par B et le fait que Φ_B prend la même valeur sur une cellule que Φ_{-B} sur la cellule duale.

Lemme 28. — *Soient G un groupe et B un sous-ensemble fini non vide de G, alors pour tout $g \in G$, on a :*

$$\Phi_B = \Phi_{B+g}.$$

Démonstration. — En effet, quel que soit l'élément $g \in G$, et pour tout sous-ensemble fini X, les sous-ensembles $X + B$ et $X + B + g$ sont de même cardinal. On a alors $|X + B| - |X| = |X + B + g| - |X|$, donc $\Phi_B(X) = \Phi_{B+g}(X)$. □

Remarque 3. — *Si l'on choisit $g = -b$, avec $b \in B$, cela revient à considérer que 0 appartient à B. On peut alors considérer que pour tout X sous-ensemble de G, on a $X \subset (X + B)$ et donc on peut écrire :*

$$\Phi_B(X) = |(X + B) \smallsetminus X|.$$

Contrairement à la formulation initiale de Φ_B, cette formulation ne nécessite pas que l'ensemble X soit fini.

On peut ainsi sans aucune perte de généralité considérer que B contient 0 et étendre la fonction Φ_B à tout sous-ensemble X de G. Pour B un sous-ensemble fini de G contenant 0, on considèrera la fonction :

$$\Phi_B : \left| \begin{array}{ccc} \mathbf{P}(G) & \to & \mathbb{N} \cup \{\infty\} \\ X & \mapsto & |(X + B) \smallsetminus X|. \end{array} \right.$$

Lemme 29. — *(lemme de translation) Soient G un groupe et B un sous-ensemble fini non vide de G. Pour tout $g \in G$ et tout X sous-ensemble fini de G, on a :*

$$\Phi_B(X) = \Phi_B(g + X)$$

Démonstration. — Naturellement $|g + X| = |X|$. De même, $|g + X + B| = |X + B|$. On a alors $|g + X + B| - |g + X| = |X + B| - |X|$. □

Proposition 30. — *Soient G un groupe et B un sous-ensemble fini non vide de G. Pour tout sous-ensemble fini X de G, on a :*

$$\Phi_B(P_B(X)) \leqslant \Phi_B(X).$$

De plus, si $\Phi_B(P_B(X)) = \Phi_B(X)$, alors $P_B(X) = X$.

Démonstration. — On a vu au lemme 24 que si B et X sont finis, alors $P_B(X)$ l'est aussi. De plus, d'après le lemme 6, on a $X \subset P_B(X)$, donc $|X| \leqslant |P_B(X)|$ et d'après la proposition 7, on a $X + B = P_B(X) + B$, donc $|X + B| = |P_B(X) + B|$. Ainsi :

$$\begin{array}{rcl} \Phi_B(X) & = & |X + B| - |X| \\ & \geqslant & |P_B(X) + B| - |P_B(X)| \\ & = & \Phi_B(P_B(X)). \end{array}$$

De plus, si on a $\Phi_B(P_B(X)) = \Phi_B(X)$, on obtient naturellement $|P_B(X)| = |X|$. Et l'inclusion $X \subset P_B(X)$ de la proposition 6 impose alors $P_B(X) = X$. □

Proposition 31. — *Soient G un groupe et B un sous-ensemble fini contenant 0. Pour toute cellule finie ou de complémentaire fini C pour B, on a :*

$$\Phi_B(C) = \Phi_{-B}(D_B(C)).$$

Démonstration. — D'après la proposition 27, on a $(C + B) \smallsetminus C = (D_B(C) - B) \smallsetminus D_B(C)$, ainsi :

$$\begin{aligned} \Phi_B(C) &= |(C + B) \smallsetminus C| \\ &= |(D_B(C) - B) \smallsetminus D_B(C)| \\ &= \Phi_{-B}(D_B(C)). \end{aligned}$$

□

Le cas abélien présente une particularité que nous voyons maintenant :

Lemme 32. — *Si G est un groupe abélien et B un sous-ensemble fini de G contenant 0, alors pour tout sous-ensemble fini X de G, on a :*

$$\Phi_B(X) = \Phi_{-B}(-X).$$

Démonstration. — Par unicité de l'élément opposé, on a $|X| = |-X|$, et $|X + B| = |-B - X|$. De plus, par commutativité, on a $|-X - B| = |-B - X|$, ainsi $|X + B| - |X| = |-X - B| - |-X|$. □

2.2. Les k-cellules et k-noyaux. — On note $\mathbf{C}_B^0 = \{\emptyset, G\}$. D'après la remarque 1, on a $\mathbf{C}_B^0 \subset \mathbf{C}_B$. On note aussi $\lambda_0(B) = 0 = \Phi_B(\emptyset) = \Phi_B(G)$. On appelle 0-cellule, un élément de $\mathbf{C}_B^0$.

On introduit une notation des cellules finies ou de complémentaire fini qui vise à les classer en fonction de la taille de leurs périmètres. En particulier, on appelle l'ensemble des tailles de ces périmêtres la seconde suite isopérimétrique (en convenant d'appeler première suite isopérimétrique celle définie dans les travaux de Hamidoune [**11, 12, 13, 14, 16**]) :

On note $\mathbf{C}_{B,f}$ l'ensemble des cellules finies ou de complémentaire fini de B. Comme B est fini, naturellement ces cellules ont un périmètre fini.

Définition 1. — *On appelle seconde suite de nombres isopérimétriques, la suite ordonnée des valeurs prises par la fonction Φ_B sur l'ensemble des cellules finies ou de complémentaire fini $\mathbf{C}_{B,f} \smallsetminus \mathbf{C}_B^0$. On la notera :*

$$\Phi_B(\mathbf{C}_{B,f} \smallsetminus \mathbf{C}_B^0) = \{0 \leqslant \lambda_1(B) < \lambda_2(B) < \ldots\}.$$

La proposition 31 et la correspondance des cellules par dualité assure que cette suite est la même pour un ensemble B et pour son symétrique $-B$.

Définition 2. — *Pour k un entier naturel non nul, on appelle k-cellule, une cellule finie ou de complémentaire fini C, qui n'est pas une 0-cellule, telle que $\Phi_B(C) = \lambda_k(B)$. On note $\mathbf{C}_B^k$ l'ensemble des k-cellules.*

Si $\lambda_1(B) = 0$, on a :

$$\mathbf{C}_B^1 = (\mathbf{C}_{B,f} \smallsetminus \mathbf{C}_B^0) \cap \Phi_B^{-1}(\lambda_1(B)).$$

Pour $k > 1$, et pour tout $k \in \mathbb{N}$ si $\lambda_1(B) \neq 0$, on a :

$$\mathbf{C}_B^k = \mathbf{C}_{B,f} \cap \Phi_B^{-1}(\lambda_k(B)).$$

Parmi les k-cellules, lorsqu'il en existe de cardinal fini, certaines jouent un rôle privilégié : celles de cardinal minimal. On les distingue en donnant la définition suivante :

Définition 3. — *Soit k un entier naturel non nul. S'il existe des k-cellules de cardinal fini, on appelle k-noyau, une k-cellule de cardinal minimal. On note ce cardinal $\beta_k(B)$.*

Par définition, un noyau est toujours fini.

Remarque 4. — *Pour k un entier naturel non nul, s'il existe des k-cellules, au moins l'un des deux entiers $\beta_k(B)$ et $\beta_k(-B)$ est bien défini. En effet, si $\beta_k(B)$ n'est pas défini, toutes les k-cellules pour B sont infinies, donc par définition de complémentaire fini, ce qui impose que toutes les k-cellules pour $-B$ sont finies et ainsi que $\beta_k(-B)$ soit bien défini.*

Lemme 33. — *Pour tout entier naturel k non nul pour lequel $\beta_k(B)$ et $\beta_k(-B)$ sont définis, on a :*

$$\beta_k(B) + \lambda_k(B) + \beta_k(-B) \leqslant |G|.$$

Démonstration. — Si G est infini, tous les termes du membre de gauche étant finis, l'inégalité est assurée. Si G est fini, on considère un k-noyau N_k pour B, alors d'après la proposition 31, $D_B(N_k)$ est une k-cellule pour $-B$, ainsi, on a : $|D_B(N_k)| \geqslant \beta_k(-B)$. De plus, comme les trois ensembles N_k, $(N_k + B) \smallsetminus N_k$ et $D_B(N_k)$ forment, d'après le lemme 26, une partition de G, on obtient :

$$\begin{aligned} |G| &= |N_k| + |(N_k + B) \smallsetminus N_k| + |D_B(N_k)| \\ &= \beta_k(B) + \lambda_k(B) + |D_B(N_k)| \\ &\geqslant \beta_k(B) + \lambda_k(B) + \beta_k(-B). \end{aligned}$$

□

Remarque 5. — *Si G est abélien, d'après le lemme 32 et le corollaire 16, on a $\Phi_B(X) = \Phi_{-B}(-X)$, et $(X \in \mathbf{C}_B \Leftrightarrow -X \in \mathbf{C}_{-B})$, ainsi pour tout entier naturel k, $\beta_k(B)$ et $\beta_k(-B)$ sont toujours tous les deux définis et égaux :*

$$\lambda_k(B) = \lambda_k(-B), \text{ et } \beta_k(B) = \beta_k(-B).$$

Remarque 6. — *Bien que similaires, les outils de la méthode isopérimétrique développés par Y. ould Hamidoune, notamment dans* [**13**] *et* [**16**] *ne sont pas les mêmes que ceux qui viennent d'être définis, ainsi les k-cellules et les k-fragments des articles de Hamidoune ne sont pas tout à fait les mêmes objets, les k-noyaux ne sont pas les k-atomes et la première suite des nombres isopérimétriques $\kappa_k(B)$ est différente de*

celle des $\lambda_k(B)$. Cependant pour $k = 1$, et dans un groupe abélien, les 1-noyaux sont exactement les 1-atomes et les 1-cellules sont exactement les 1-fragments.

2.3. Inégalité fondamentale. — On établit ici une inégalité classique liant les périmètres des intersection et union de deux cellules en fonction de leur propre périmètre, on peut la retrouver dans le lemme 3.5 de [**14**]. Cette inégalité sera l'outil clef, qui nous permettra de donner les résultats de structure des cellules et noyaux.

Proposition 34. — *Soient G un groupe, B un sous-ensemble fini non vide de G contenant 0 et X et Y deux sous-ensembles finis ou de complémentaire fini de G, alors on a :*

$$\Phi_B(X \cap Y) + \Phi_B(X \cup Y) \leqslant \Phi_B(X) + \Phi_B(Y).$$

Démonstration. — On considère les deux partitions $\{X, (X + B) \smallsetminus X, D_B(X)\}$ et $\{Y, (Y + B) \smallsetminus Y, D_B(Y)\}$ données par le lemme 26 et on construit la partition croisée :

$\cap$	X	$(X + B) \smallsetminus X$	$D_B(X)$
Y	R_{11}	R_{12}	R_{13}
$(Y + B) \smallsetminus Y$	R_{21}	R_{22}	R_{23}
$D_B(Y)$	R_{31}	R_{32}	R_{33}

On a alors les trois égalités et l'inclusion suivantes :

$$\begin{aligned}
(X + B) \smallsetminus X &= R_{12} \cup R_{22} \cup R_{32},\\
(Y + B) \smallsetminus Y &= R_{21} \cup R_{22} \cup R_{23},\\
((X \cup Y) + B) \smallsetminus (X \cup Y) &= R_{32} \cup R_{22} \cup R_{23},\\
((X \cap Y) + B) \smallsetminus (X \cap Y) &\subset R_{12} \cup R_{22} \cup R_{21}.
\end{aligned}$$

Comme B est fini et que X et Y sont chacun soit fini soit de complémentaire fini, les éléments R_{12}, R_{22}, R_{32}, R_{21} et R_{23} de cette partition sont tous finis. Ainsi, on déduit des égalités et de l'inclusion précédentes, trois nouvelles égalités et une inégalité :

$$\begin{aligned}
\Phi_B(X) &= |R_{12}| + |R_{22}| + |R_{32}|,\\
\Phi_B(Y) &= |R_{21}| + |R_{22}| + |R_{23}|,\\
\Phi_B(X \cup Y) &= |R_{32}| + |R_{22}| + |R_{23}|,\\
\Phi_B(X \cap Y) &\leqslant |R_{12}| + |R_{22}| + |R_{21}|.
\end{aligned}$$

En additionnant les deux premières lignes d'une part et les deux suivantes d'autre part, on a alors :

$$\begin{aligned}
\Phi_B(X) + \Phi_B(Y) &= |R_{12}| + |R_{21}| + 2|R_{22}| + |R_{32}| + |R_{23}|,\\
\Phi_B(X \cap Y) + \Phi_B(X \cup Y) &\leqslant |R_{12}| + |R_{21}| + 2|R_{22}| + |R_{32}| + |R_{23}|,
\end{aligned}$$

ce qui permet de conclure que :

$$\Phi_B(X \cap Y) + \Phi_B(X \cup Y) \leqslant \Phi_B(X) + \Phi_B(Y).$$

□

On en déduit le résultat fondamental suivant, qui sera souvent utilisé dans la suite de l'article :

Corollaire 35. — *Soient G un groupe et B un sous-ensemble fini contenant 0 de G, C_i une i-cellule et C_j une j-cellule pour B. Si k et l sont les entiers tels que $C_i \cap C_j$ soit une k-cellule et $P_B(C_i \cup C_j)$ soit une l-cellule pour B, alors :*

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_i(B) + \lambda_j(B).$$

De plus, si cette inégalité est une égalité, on a $P_B(C_i \cup C_j) = C_i \cup C_j$.

Démonstration. — Il suffit d'appliquer la proposition 34 avec $X = C_i$, et $Y = C_j$ pour obtenir l'inégalité :

$$\Phi_B(C_i \cap C_j) + \Phi_B(C_i \cup C_j) \leqslant \Phi_B(C_i) + \Phi_B(C_j),$$

donc

$$\lambda_k(B) + \Phi_B(C_i \cup C_j) \leqslant \lambda_i(B) + \lambda_j(B).$$

De plus, d'après la proposition 30, on a : $\lambda_l(B) = \Phi_B(P_B(C_i \cup C_j)) \leqslant \Phi_B(C_i \cup C_j)$, d'où l'inégalité.

Dans le cas d'égalité, on a nécessairement $\Phi_B(P_B(C_i \cup C_j)) = \Phi_B(C_i \cup C_j)$. La proposition 30 affirme alors que l'on a $P_B(C_i \cup C_j) = C_i \cup C_j$. □

Une autre inégalité un peu plus technique aura une grande importance par la suite pour s'assurer que les unions de cellules de petit périmètre ne puissent pas donner de cellules de trop petit périmètre. Il s'agit du généralisation de l'inégalité (5) du lemme 3.3 de [**16**].

Lemme 36. — *Soient G un groupe, B un sous-ensemble fini de G contenant 0, C_i une i-cellule finie et C_j une j-cellule pour B. Soit k l'entier tel que $C_i \cap C_j$ soit une k-cellule pour B. Si $k \geqslant j$, on a :*

$$\lambda_j(B) + |D_B(C_j) \smallsetminus D_B(C_i)| \leqslant \lambda_i(B) + |C_i \smallsetminus C_j|.$$

Démonstration. — La preuve se base aussi sur la partition croisée de la proposition 34 :

$\cap$	C_j	$(C_j + B) \smallsetminus C_j$	$D_B(C_j)$
C_i	R_{11}	R_{12}	R_{13}
$(C_i + B) \smallsetminus C_i$	R_{21}	R_{22}	R_{23}
$D_B(C_i)$	R_{31}	R_{32}	R_{33}

On note sur cette partition croisée l'égalité et l'inclusion suivantes :

$$\begin{aligned} (C_i + B) \smallsetminus C_i &= R_{21} \cup R_{22} \cup R_{23}, \\ ((C_i \cap C_j) + B) \smallsetminus (C_i \cap C_j) &\subset R_{21} \cup R_{22} \cup R_{12}. \end{aligned}$$

La cellule C_i est finie, ainsi $C_i + B$ est fini, donc les éléments $R_{1,1}$, $R_{1,2}$, $R_{1,3}$, $R_{2,1}$, $R_{2,2}$ et $R_{2,3}$ sont tous finis. De plus C_j est une j-cellule, donc de périmètre fini, ainsi $R_{3,2}$ est aussi fini. On en conclut que les deux seuls éléments de cette partition croisée qui peuvent éventuellement être infinis sont R_{31} et R_{33}.

Comme $C_i \cap C_j$ est une k-cellule et C_i une i-cellule, on a l'égalité et l'inégalité suivantes :

$$\begin{aligned}\lambda_i(B) &= |R_{21}| + |R_{22}| + |R_{23}|,\\ \lambda_k(B) &\leqslant |R_{21}| + |R_{22}| + |R_{12}|.\end{aligned}$$

De plus, on remarque sur la partition que : $|D_B(C_j) \smallsetminus D_B(C_i)| = |R_{13}| + |R_{23}|$ et $|C_i \smallsetminus C_j| = |R_{12}| + |R_{13}|$. Ainsi, on obtient :

$$\begin{aligned}\lambda_k(B) + |D_B(C_j) \smallsetminus D_B(C_i)| &\leqslant (|R_{21}| + |R_{22}| + |R_{12}|) + (|R_{13}| + |R_{23}|)\\ &\leqslant (|R_{21}| + |R_{22}| + |R_{23}|) + (|R_{12}| + |R_{13}|)\\ &\leqslant \lambda_i(B) + |C_i \smallsetminus C_j|.\end{aligned}$$

Enfin, l'inégalité $k \geqslant j$ impose $\lambda_k(B) \geqslant \lambda_j(B)$, ce qui nous donne :

$$\lambda_j(B) + |D_B(C_j) \smallsetminus D_B(C_i)| \leqslant \lambda_i(B) + |C_i \smallsetminus C_j|.$$

□

3. Structure dans le cas abélien

Dans toute cette partie, on considère un groupe abélien G et un sous ensemble B fini non vide.

3.1. Structure des 1-cellules et 1-noyaux. — On donne un premier résultat de structure pour les 1-cellules et 1-noyaux, représentatif du travail qui suit. Ce résultat est connu et dû à Hamidoune, proposition 4.2 de [**16**], ou [**12**]. Pour cela on considére les intersections non-vides des 1-noyaux avec les 1-cellules et on montre que ces intersections ne peuvent être quelconques. Le fait de pouvoir librement translater un 1-noyau en un autre permet de décrire la structure des 1-cellules.

3.1.1. Critère d'existence de 1-cellules. — Soient G un groupe et B un sous-ensemble fini de G. Si $B = G$, alors pour tout $X \subset G$ non vide, on a $X + B = G$. Ainsi les seules cellules sont $\emptyset$ et G et il n'y a pas de 1-cellule. Par contre, si B est différent de G, alors pour X réduit à un singleton quelconque, on a :

$$|X + B| - |X| = |B| - 1 \text{ et } X + B \neq G.$$

Ainsi, $X \neq \emptyset$ et $X + B \neq G$ donc $P_B(X)$ n'est pas une 0-cellule, il existe alors des 1-cellules et on a $\lambda_1(B) \leqslant |B| - 1$.

3.1.2. Structure des 1-cellules et 1-noyaux. — Soient G un groupe abélien et B un sous-ensemble fini non vide de G, différent de G. Si $\lambda_1(B) = |B| - 1$, alors les 1-noyaux sont exactement les singletons de G. Si nécessaire on pourra donc se restreindre au cas $\lambda_1(B) < |B| - 1$, qui impose donc que toutes les 1-cellules contiennent au moins deux éléments.

Définition 4. — *On appelle condition $E_1(B)$ pour une cellule C pour B, la condition :*

$$|G \smallsetminus C| \geqslant \lambda_1(B) + \beta_1(B).$$

D'après la remarque 5, $\lambda_1(B) + \beta_1(B)$ est toujours fini. Ainsi, si le groupe G est infini cette condition est remplie pour toute cellule finie.

Remarque 7. — *Si G est abélien, toutes les 1-cellules pour B vérifient la condition $E_1(B)$.*

Démonstration. — Si C_1 est une 1-cellule pour B, $D_B(C_1)$ est alors une 1-cellule pour $-B$ et est donc de cardinal supérieur à $\beta_1(-B) = \beta_1(B)$, ainsi :

$$|G \smallsetminus C_1| - \lambda_1(B) = |D_B(C_1)| \geqslant \beta_1(B)$$

et C_1 vérifie la condition $E_1(B)$. □

La proposition suivante met en lumière le rôle particulier des 1-noyaux. Il s'agit d'un cas particulier de la proposition 3.4 de [**16**].

Proposition 37. — *Soient G un groupe abélien, B un sous-ensemble fini contenant 0 de G, N_1 un 1-noyau et C_1 une 1-cellule pour B. Si $N_1 \cap C_1 \neq \emptyset$, alors $N_1 \subset C_1$.*

Démonstration. — D'après le corollaire 14, l'intersection $N_1 \cap C_1$ est une k-cellule, pour un certain $k \geqslant 1$. D'après le lemme 36, on a alors :

$$|D_B(C_1) \smallsetminus D_B(N_1)| \leqslant |N_1 \smallsetminus C_1|.$$

On s'intéresse maintenant à l'union $C_1 \cup N_1$, et à la cellule associée $P_B(C_1 \cup N_1)$. On va tout d'abord montrer qu'il s'agit d'une l-cellule pour un certain $l \geqslant 1$. Comme C_1 est une 1-cellule pour B, C_1 remplit la condition $E_1(B)$, ainsi on a :

$$|D_B(C_1)| \geqslant \beta_1(B) = |N_1|.$$

Or :

$$\begin{aligned} |D_B(C_1) \cap D_B(N_1)| &= |D_B(C_1)| - |D_B(C_1) \smallsetminus D_B(N_1)| \\ &\geqslant |D_B(C_1)| - |N_1 \smallsetminus C_1| \\ &\geqslant |N_1| - |N_1 \smallsetminus C_1| \\ &= |N_1 \cap C_1| > 0. \end{aligned}$$

Ainsi comme, d'après la proposition 22, $D_B(C_1 \cup N_1) = D_B(C_1) \cap D_B(N_1)$ et que cet ensemble n'est pas vide d'après l'inégalité ci-dessus, il s'agit d'une l-cellule pour B pour un certain $l \geqslant 1$.

Le corollaire 35 nous donne alors :

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_1(B) + \lambda_1(B).$$

Et ce, avec $k \geqslant 1$ et $l \geqslant 1$. Comme la suite des valeurs $\lambda_i(B)$ est strictement croissante à partir de $i = 1$, on a nécessairement $k = l = 1$.

De plus, N_1 est un 1-noyau, c'est une 1-cellule de cardinal minimal, ainsi l'égalité $k = 1$ impose l'inclusion $N_1 \subset C_1$. □

On retrouve alors un premier résultat de structure pour les 1-noyaux et les 1-cellules pour B, qui correspond à la proposition 4.2 de [**16**].

Théorème 38. — *Soient G un groupe abélien, B un sous-ensemble fini contenant 0 de G. Il existe un sous-groupe fini H tel que les 1-noyaux pour B soient les classes modulo H, et les 1-cellules soient périodiques modulo ce sous-groupe.*

Démonstration. — Si l'on a $\lambda_1(B) = |B|-1$, le sous-groupe trivial $H = \{0\}$ convient. On peut supposer désormais que $\lambda_1(B) < |B| - 1$. Si l'on considère deux 1-noyaux pour B, d'intersection non vide, d'après la proposition 37 précédente, ils sont inclus l'un dans l'autre, donc égaux. Ainsi deux 1-noyaux distincts sont disjoints.

Si N_1 est un 1-noyau pour B contenant 0 et si $x \in N_1$ avec $x \neq 0$, N_1 et $-x + N_1$ sont deux 1-noyaux pour B contenant 0 donc d'intersection non vide, ils sont donc égaux : $N_1 = -x + N_1$.

On a alors pour tout $x \in N_1$, $-x + N_1 = N_1$, ce qui signifie que N_1 est un sous-groupe fini de G. Par translation toutes les classes modulo N_1 sont des 1-noyaux. Et comme toutes les classes modulo N_1 forment une partition de G, il ne peut y avoir d'autres 1-noyaux.

Si C_1 est une 1-cellule pour B, la proposition 37 impose qu'elle contient tous les 1-noyaux qu'elle intersecte. Ainsi C_1 est une union de classes modulo N_1. Et donc $N_1 \subset \pi(C_1)$. □

Remarque 8. — *Comme Hamidoune le remarque dans le corollaire* 4.3 *de* **[16]**, *ce premier résultat nous permet d'ores et déjà de retrouver le théorème de Cauchy-Davenport, le théorème de Chowla dans les groupes cycliques et le théorème de Mann.*

3.2. Structure des i-cellules et i-noyaux (lorsque $\lambda_i(B) < |B| - 1$). — Dans cette partie, tous les résultats sont originaux. On veut montrer que toutes les i-cellules sont périodiques en généralisant les idées précédentes.

Le cas des i-cellules pour $i > 1$ est un peu plus délicat et nécessite quelques propositions préalables. L'idée consiste à mettre en place des conditions assurant que les unions de cellules de petits périmètres ne donnent pas des cellules de périmètre trop petit, puis de mettre en place des résultats assurant l'existence de i-cellules suffisamment petites. Cela nous permettra d'établir que les i-noyaux sont disjoints.

Définition 5. — *Pour un entier non nul i, on appelle condition $E_i(B)$ pour une cellule C pour B, la condition :*

$$|G \smallsetminus C| \geqslant \lambda_i(B) + \beta_i(B).$$

De même que pour la définition 4, on remarque que cette condition est remplie pour toute cellule finie pour B si G est infini.

Lemme 39. — *Soient G un groupe abélien, B un sous-ensemble fini contenant 0 de G, et i un entier non nul. Soit C_j une j-cellule pour B avec $j \geqslant i$. Si C_j ne vérifie pas la condition $E_i(B)$, alors $D_B(C_j)$ vérifie la condition $E_i(-B)$ et $|D_B(C_j)| < \beta_i(B) + \lambda_i(B) - \lambda_j(B)$.*

Démonstration. — Comme C_j ne vérifie pas la condition $E_i(B)$, $G \smallsetminus C_j$ est un ensemble fini et on a :

$$|G \smallsetminus C_j| < \lambda_i(B) + \beta_i(B).$$

Comme $D_B(C_j) \subset G \smallsetminus C_j$, $D_B(C_j)$ est aussi fini, et on peut alors écrire :

$$\begin{aligned} |D_B(C_j)| &= |D_B(C_j) - B| - \lambda_j(B) \\ &= |G \smallsetminus C_j| - \lambda_j(B) \\ &< \lambda_i(B) - \lambda_j(B) + \beta_i(B). \end{aligned}$$

De plus si G est infini, $D_B(C_j)$ est fini et vérifie donc la condition $E_i(-B)$. Si G est fini, on a vu au corollaire 33, que $\beta_i(B) + \lambda_i(B) + \beta_i(-B) \leqslant |G|$. Ainsi :

$$|D_B(C_j)| < \lambda_i(B) - \lambda_j(B) + \beta_i(B) \leqslant \beta_i(B) \leqslant |G| - \lambda_i(B) - \beta_i(-B).$$

On obtient finalement :

$$|G \smallsetminus D_B(C_j)| > \lambda_i(B) + \beta_i(-B) = \lambda_i(-B) + \beta_i(-B).$$

□

On donne maintenant une première implication de la condition $E_i(B)$.

Lemme 40. — *Soient G un groupe abélien et B un sous-ensemble fini de G contenant 0, N_i un i-noyau et C_j une j-cellule pour B avec $j \geqslant i$. Soit k l'entier tel que $N_i \cap C_j$ soit une k-cellule. Si $k \geqslant j$ et C_j vérifie $E_i(B)$, $P_B(N_i \cup C_j)$ est une l-cellule pour B avec $l > 0$.*

Démonstration. — L'intersection $N_i \cap C_j$ est une k-cellule finie, avec $k \geqslant j$, ainsi d'après le lemme 36, on a :

$$\lambda_j(B) + |D_B(C_j) \smallsetminus D_B(N_i)| \leqslant \lambda_i(B) + |N_i \smallsetminus C_j|.$$

On cherche maintenant à minorer $|D_B(C_j)|$. Comme C_j vérifie la condition $E_i(B)$, on a :

$$|G \smallsetminus C_j| \geqslant \lambda_i(B) + \beta_i(B).$$

Ainsi comme $G \smallsetminus C_j = D_B(C_j) \cup ((D_B(C_j) - B) \smallsetminus D_B(C_j))$, on obtient :

$$|D_B(C_j)| + \lambda_j(B) \geqslant \lambda_i(B) + \beta_i(B),$$

donc

$$|D_B(C_j)| \geqslant \lambda_i(B) + \beta_i(B) - \lambda_j(B).$$

Comme d'après la proposition 22, on a $P_B(N_i \cup C_j) = D_{-B}(D_B(C_j) \cap D_B(N_i))$, on peut écrire :

$$\begin{aligned} |D_B(C_j) \cap D_B(N_i)| &= |D_B(C_j)| - |D_B(C_j) \smallsetminus D_B(N_i)| \\ &\geqslant |D_B(C_j)| - \lambda_i(B) + \lambda_j(B) - |N_i \smallsetminus C_j| \\ &\geqslant (\beta_i(B) + \lambda_i(B) - \lambda_j(B)) - \lambda_i(B) + \lambda_j(B) - |N_i \smallsetminus C_j| \\ &= |N_i| - |N_i \smallsetminus C_j| \\ &= |N_i \cap C_j| > 0. \end{aligned}$$

Ainsi, $P_B(N_i \cup C_j)$ est une l-cellule pour B ou le dual d'une l-cellule pour $-B$ avec $l > 0$. □

Le lemme précédent a pour but de ramener l'étude des j-cellules pour $j \geqslant i$ à celles contenues dans un $(i-1)$-noyau. On définit maintenant une nouvelle condition adaptée aux j-cellules dans un $(i-1)$-noyau :

Définition 6. — *Pour un entier non nul tel que $1 < i$, on appelle condition $E'_i(B)$ pour une cellule C pour B incluse dans un $(i-1)$-noyau N_{i-1}, la condition :*

$$|C| \leqslant (\lambda_{i-1}(B) + \beta_{i-1}(B)) - (\lambda_i(B) + \beta_i(B)).$$

Lemme 41. — *Soient G un groupe abélien, B un sous-ensemble fini de G contenant 0, $i > 1$ un entier, N_i et N_{i-1} respectivement un i-noyau et un $(i-1)$-noyau et C_j une j-cellule. On suppose que $j \geqslant i$, $N_i \cap C_j \neq \emptyset$ et que $N_i \cup C_j \subset N_{i-1}$. Soit k l'entier tel que $N_i \cap C_j$ soit une k-cellule. Si $k \geqslant j$ et C_j vérifie la condition $E'_i(B)$, alors on a :*

$$|(N_{i-1} + B) \smallsetminus ((N_i \cup C_j) + B)| > 0.$$

Démonstration. — Dans un premier temps, on remarque que l'on peut minorer $|(N_{i-1}+B) \smallsetminus (C_j+B)| = |D_B(C_j) \smallsetminus D_B(N_{i-1})|$. En effet, comme C_j vérifie la condition $E'_i(B)$:

$$\begin{aligned}
|(N_{i-1} + B) \smallsetminus (C_j + B)| &= |N_{i-1} + B| - |C_j + B| \\
&= |N_{i-1} + B| - |C_j| - \lambda_j(B) \\
&\geqslant (\lambda_{i-1}(B) + \beta_{i-1}(B)) - (\lambda_{i-1}(B) + \beta_{i-1}(B)) \\
&\qquad + (\lambda_i(B) + \beta_i(B)) - \lambda_j(B) \\
&= \lambda_i(B) + \beta_i(B) - \lambda_j(B).
\end{aligned}$$

Ainsi en utilisant le lemme 36 et l'inégalité précédente, on obtient :

$$\begin{aligned}
|(N_{i-1} + B) \smallsetminus ((N_i \cup C_j) + B)| &= |(N_{i-1} + B) \smallsetminus (C_j + B)| \\
&\qquad - |(N_i + B) \smallsetminus (C_j + B)| \\
&= |(N_{i-1} + B) \smallsetminus (C_j + B)| - |D_B(C_j) \smallsetminus D_B(N_i)| \\
&\geqslant \lambda_i(B) + \beta_i(B) - \lambda_j(B) \\
&\qquad - (-\lambda_j(B) + \lambda_i(B) + |N_i \smallsetminus C_j|) \\
&= |N_i| - |N_i \smallsetminus C_j| \\
&= |N_i \cap C_j| > 0.
\end{aligned}$$

□

Ce lemme sera particulièrement utile pour montrer que l'union d'une cellule et d'un noyau ne peut être une cellule d'ordre trop petit.

Un dernier lemme sera nécessaire avant de donner un théorème de description finale :

Lemme 42. — *Soient G un groupe abélien, B un sous-ensemble fini de G contenant 0, i un entier tel que $1 < i$, N_i et N_{i-1} respectivement un i-noyau et un $(i-1)$-noyau et C_j une j-cellule pour B. On suppose que $j \geqslant i$, $N_i \cap C_j \neq \emptyset$, $N_i \cup C_j \subset N_{i-1}$ et que N_i vérifie la condition $E'_i(B)$. Si C_j ne vérifie pas la condition $E'_i(B)$, alors $D_B(C_j)$ vérifie la condition $E_i(-B)$ et $|(N_{i-1} + B) \smallsetminus (C_j + B)| < \beta_i(B)$.*

Démonstration. — Par contradiction de la condition $E_i'(B)$, on a $|C_j| > (\lambda_{i-1}(B) + \beta_{i-1}(B)) - (\lambda_i(B) + \beta_i(B))$, ce que l'on peut réécrire :

$$\beta_i(B) > (\lambda_{i-1}(B) + \beta_{i-1}(B)) - (\lambda_i(B) + |C_j|).$$

Ainsi, comme $j \geqslant i$, on a $\lambda_j(B) \geqslant \lambda_i(B)$ et donc :

$$\beta_i(B) > (\lambda_{i-1}(B) + \beta_{i-1}(B)) - (\lambda_j(B) + |C_j|) = |(N_{i-1} + B) \smallsetminus (C_j + B)|.$$

De plus, on a $G \smallsetminus D_B(C_j) = C_j + B$, ainsi l'inégalité précédente donne :

$$|G \smallsetminus D_B(C_j)| > (\lambda_{i-1}(B) + \beta_{i-1}(B)) - \beta_i(B).$$

Comme N_i vérifie la condition $E_i'(B)$, on a $\beta_i(B) \leqslant (\beta_{i-1}(B)+\lambda_{i-1}(B))-(\beta_i(B)+\lambda_i(B))$, ce dont on déduit l'inégalité $\beta_i(B) + \lambda_i(B) \leqslant (\beta_{i-1}(B) + \lambda_{i-1}(B)) - \beta_i(B)$. En combinant cette inégalité avec la précédente, on obtient :

$$|G \smallsetminus D_B(C_j)| > \beta_i(B) + \lambda_i(B) = \beta_i(-B) + \lambda_i(-B).$$

Ce qui prouve que $D_B(C_j)$ vérifie la condition $E_i(-B)$. □

Le théorème suivant donne un résultat de structure pour toutes les i-cellules telles que $\lambda_i(B) < |B| - 1$. Par récurrence, on établit pour tout i qu'il existe un i-noyau inclus dans un $(i-1)$-noyau, puis on ramène l'étude des i-cellules à l'intérieur d'un $(i-1)$-noyau et on montre que les intersections des i-noyaux et des i-cellules ne peuvent être quelconques.

Théorème 43. — *Soient G un groupe abélien et B un sous-ensemble non vide fini de G, et $n > 0$ un entier tel que $\lambda_n(B) < |B| - 1 \leqslant \lambda_{n+1}(B)$. Pour tout $i \leqslant n$, il existe un sous-groupe (fini et différent de $\{0\}$) N_i de G, qui est un i-noyau et pour toute i-cellule C_i, on a $N_i \subset \pi(C_i)$. De plus la suite de sous-groupes $(N_i)_{i=1,..,n}$ est une suite strictement décroissante pour l'inclusion.*

Démonstration. — Sans perte de généralité, on peut supposer que $0 \in B$ (quitte à effectuer une translation de B). On raisonne par récurrence sur $i < n$. Pour $i = 1$, le résultat est vrai d'après le théorème 38.

Supposons que l'énoncé du théorème soit vrai jusqu'à un certain rang $i < n$ et montrons le résultat au rang $i + 1 \leqslant n$.

Dans un souci de clarté, la preuve est décomposée en six assertions intermédiaires et une conclusion :

Assertion 1 *:* Pour tout $j \leqslant i$, N_j vérifie la condition $E_j'(B)$.

En effet, remarquons d'abord que N_j est bien inclus dans un $(j-1)$-noyau, à savoir N_{j-1}. De plus, pour toute j-cellule C_j (en particulier N_j) dans N_{j-1} avec $1 < j \leqslant i$, comme $C_j + B$ est N_j-périodique (d'après l'hypothèse de récurrence) et différent de $N_{j-1} + B$ (car C_j et N_{j-1} sont deux cellules distinstes), l'ensemble $(N_{j-1} + B) \smallsetminus (C_j + B)$ contient au moins une classe modulo N_j. Ainsi, on obtient l'inégalité :

$$2\beta_j(B) + \lambda_j(B) \leqslant \beta_{j-1}(B) + \lambda_{j-1}(B).$$

Cela signifie bien que N_j vérifie la condition $E_j'(B)$ (ce qui est une hypothèse du lemme 42, que nous utiliserons par la suite).

Assertion 2 *:* Une $(i+1)$-cellule ne peut pas être uniquement constituée de j-noyaux avec $j \leqslant i$.

En effet, comme on a :

$$|N_i + B| - |N_i| = \lambda_i(B) < |B| - 1 < |B| \leqslant |N_i + B|,$$

$|B| - 1$ est encadré par deux multiples consécutifs de $|N_i|$. Ainsi si A est une union de classes modulo N_i mais n'est pas une j-cellule avec $j \leqslant i$, l'entier $|A+B| - |A|$ est un multiple de $|N_i|$ supérieur ou égal à $|N_i + B|$ et donc $|A + B| > |A| + |B| - 1$.

Comme on a supposé que $\lambda_{i+1}(B) < |B| - 1$, une $(i+1)$-cellule ne peut donc pas être une union de classes modulo N_i. Pour $j \leqslant i$, comme N_i est un sous-groupe de N_j (d'après l'hypothèse de récurrence), une $(i+1)$-cellule ne peut donc pas être non plus une union de classes modulo les noyaux successifs de 1 à i.

Assertion 3 *:* Toute $(i+1)$-cellule ou sa duale est constituée d'une $(i+1)$-cellule incluse dans un 1-noyau et éventuellement de 1-noyaux.

Soit $\mathcal{N}_1$ l'ensemble des 1-noyaux pour B. D'après l'hypothèse de récurrence, il s'agit de l'ensemble des classes modulo N_1. L'ensemble $\mathcal{N}_1$ est donc une partition de G. Soit C_{i+1} une $(i+1)$-cellule, on a alors $C_{i+1} = \bigcup_{N \in \mathcal{N}_1} (C_{i+1} \cap N)$.

– Si C_{i+1} vérifie la condition $E_1(B)$, soient $N \in \mathcal{N}_1$, k l'entier tel que $C_{i+1} \cap N$ soit une k-cellule non vide et l tel que $P_B(N \cup C_{i+1})$ soit une l-cellule. On a d'après le corollaire 35 :

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_{i+1}(B) + \lambda_1(B).$$

Comme $l > 0$, d'après le lemme 40 (car C_{i+1} vérifie $E_1(B)$), ceci impose $k \leqslant i+1$. Mais comme C_{i+1} ne peut être uniquement constituée de k-cellules avec $k \leqslant i$ d'après l'assertion 2, cela implique qu'il existe $\widetilde{N} \in \mathcal{N}_1$ tel que $k = i+1$, ce qui impose que $l = 1$. La cellule C_{i+1} est alors constituée d'une $(i+1)$-cellule $C_{i+1} \cap \widetilde{N}$ incluse dans un 1-noyau, car $k = i+1$ et d'une éventuelle union de 1-noyaux à savoir $\bigcup_{N \in \mathcal{N}_1 \setminus \{\widetilde{N}\}} C_{i+1} \cap N$: en effet l'union $C_{i+1} \cup \widetilde{N} = P_B(C_{i+1} \cup \widetilde{N})$ est une 1-cellule car $l = 1$ (cas d'égalité du corollaire 35), donc est N_1-périodique. Il en est donc de même pour

$$(C_{i+1} \cup \widetilde{N}) \setminus \widetilde{N} = \bigcup_{N \in \mathcal{N}_1 \setminus \{\widetilde{N}\}} C_{i+1} \cap N.$$

– Si C_{i+1} ne vérifie pas la condition $E_1(B)$, d'après le lemme 39, c'est que $D_B(C_{i+1})$ vérifie la condition $E_1(-B)$ et $|D_B(C_{i+1})| < \beta_1(B)$. Ainsi on peut appliquer le raisonnement précédent à $D_B(C_{i+1})$ pour $-B$ ce qui donne le résultat.

En fait on peut même remarquer que comme $|D_B(C_{i+1})| < \beta_1(B)$, $D_B(C_{i+1})$ est une $(i+1)$-cellule pour $-B$ contenue dans un 1-noyau pour $-B$, qui est aussi un 1-noyau pour B.

Assertion 4 *:* Toute $(i+1)$-cellule incluse dans un $(j-1)$-noyau ou sa duale est composée d'une $(i+1)$-cellule incluse dans un j-noyau et éventuellement de j-noyaux.

Soit $\mathcal{N}_j$ l'ensemble des j-noyaux pour B. D'après l'hypothèse de récurrence, il s'agit de l'ensemble des classes modulo N_j. L'ensemble $\mathcal{N}_j$ est donc une partition de G. Soit C_{i+1} une $(i+1)$-cellule incluse dans un $(j-1)$-noyau $\widetilde{N}_{j-1}$. On a alors $C_{i+1} = \bigcup_{N\in\mathcal{N}_j}(C_{i+1}\cap N)$.

– Si C_{i+1} vérifie la condition $E'_j(B)$, soient $N \in \mathcal{N}_j$, k l'entier tel que $C_{i+1}\cap N$ soit une k-cellule et l tel que $P_B(N\cup C_{i+1})$ soit une l-cellule. On a d'après le corollaire 35 :

$$\lambda_k(B)+\lambda_l(B) \leqslant \lambda_{i+1}(B)+\lambda_j(B).$$

Avec $l > j-1$ d'après le lemme 41 (car C_{i+1} vérifie $E'_j(B)$), ce qui impose $k \leqslant i+1$. Mais comme C_{i+1} ne peut être uniquement constituée de k-cellules avec $1 \leqslant k \leqslant i$ d'après l'assertion 2, cela implique qu'il existe $\widetilde{N} \in \mathcal{N}_j$ tel que $k = i+1$, ce qui impose que $l = j$. La cellule C_{i+1} est alors constituée d'une $(i+1)$-cellule $C_{i+1}\cap\widetilde{N}$ incluse dans un j-noyau, car $k = i+1$ et d'une eventuelle union de j-noyaux à savoir $\bigcup_{N\in\mathcal{N}_j\smallsetminus\{\widetilde{N}\}} C_{i+1}\cap N$: en effet l'union $C_{i+1}\cup\widetilde{N} = P_B(C_{i+1}\cup\widetilde{N})$ est une j-cellule car $l = j$ (cas d'égalité du corollaire 35), donc est N_j-périodique. Il en est donc de même pour

$$(C_{i+1}\cup\widetilde{N})\smallsetminus\widetilde{N} = \bigcup_{N\in\mathcal{N}_j\smallsetminus\{\widetilde{N}\}} C_{i+1}\cap N.$$

– Si C_{i+1} ne vérifie pas la condition $E'_j(B)$, d'après le lemme 42, c'est que $D_B(C_{i+1})$ vérifie la condition $E_j(B)$ et $|D_B(C_{i+1})\smallsetminus D_B(\widetilde{N}_{j-1})| < \beta_j(B)$.

Pour $N \in \mathcal{N}_j$ intersectant $D_B(C_{i+1})\smallsetminus D_B(\widetilde{N}_{j-1})$, soit k est l'entier tel que $D_B(C_{i+1})\cap N$ soit une k-cellule pour $-B$ et l tel que $P_{-B}(D_B(C_{i+1})\cup N)$ soit une l-cellule pour $-B$, on a d'après le corollaire 35 :

$$\lambda_k(-B)+\lambda_l(-B) \leqslant \lambda_{i+1}(-B)+\lambda_j(-B).$$

Avec $l > j-1$, d'après le lemme 40 (car $D_B(C_{i+1})$ vérifie la condition $E_j(-B)$ et que $P_{-B}(D_B(C_{i+1})\cup N_j)$ contient strictement $D_B(\widetilde{N}_{j-1})$), ce ne peut donc pas être une j'-cellule pour $-B$ avec $j' < j$. On a alors $l \geqslant j$, ceci impose $k \leqslant i+1$. Mais comme $|D_B(C_{i+1})\smallsetminus D_B(\widetilde{N}_{j-1})| < \beta_j(B)$ et que $D_B(C_{i+1})$ ne peut être uniquement constituée de k-noyaux avec $1 \leqslant k \leqslant i$, il existe un $\widetilde{N} \in \mathcal{N}_j$ tel que $k = i+1$, ce qui impose $l = j$. La cellule duale de C_{i+1}, $D_B(C_{i+1})$, est alors constituée d'une $(i+1)$-cellule incluse dans un j-noyau $D_B(C_{i+1})\cap\widetilde{N}$, car $k = i+1$ et d'une union de j-noyaux, $D_B(\widetilde{N}_{j-1})$.

Assertion 5 *:* Toute $(i+1)$-cellule incluse dans un i-noyau vérifie nécessairement la condition $E'_{i+1}(B)$.

On considère une $(i+1)$-cellule C_{i+1} incluse dans un i-noyau $\widetilde{N}_i$.

Montrons que $D_B(C_{i+1})$ vérifie la condition $E_{i+1}(-B)$. Si tel n'est pas le cas, d'après le lemme 39, C_{i+1} vérifie la condition $E_{i+1}(B)$ et $|C_{i+1}| < \beta_{i+1}(-B)$, ce qui est impossible, car $\beta_{i+1}(-B) = \beta_{i+1}(B)$.

Considérons alors un $(i+1)$-noyau N_{i+1} pour $-B$ intersectant $D_B(C_{i+1})\smallsetminus D_B(\widetilde{N}_i)$. Si k et l sont les entiers tels que $D_B(C_{i+1})\cap N_{i+1}$ soit une k-cellule pour $-B$ et

$P_{-B}(D_B(C_{i+1}) \cup N_{i+1})$ soit une l-cellule pour $-B$, on a d'après le corollaire 35 :

$$\lambda_k(-B) + \lambda_l(-B) \leqslant \lambda_{i+1}(-B) + \lambda_{i+1}(-B).$$

Avec $l \geqslant i+1$, car $D_B(C_{i+1})$ vérifie la condition $E_{i+1}(-B)$ et que $P_{-B}(D_B(C_{i+1}) \cup N_{i+1})$ contient strictement $D_B(\widetilde{N}_i)$ (ce ne peut donc pas être une j-cellule pour $-B$ avec $j < i+1$). Ainsi, on a $l \geqslant i+1$, ce qui impose $k \leqslant i+1$. Mais pour tout j, tel que $1 \leqslant j \leqslant i$, N_j est de cardinal strictement supérieur à $\beta_{i+1}(B)$, donc on a $k = i+1$, ce qui implique aussi $l = i+1$. Ainsi $D_B(C_{i+1}) \smallsetminus D_B(\widetilde{N}_i)$ contient au moins un $(i+1)$-noyau pour $-B$. On a alors $\beta_{i+1}(-B) \leqslant |D_B(C_{i+1}) \smallsetminus D_B(\widetilde{N}_i)|$, ce qui peut se réécrire $\beta_{i+1}(B) \leqslant (\lambda_i(B) + \beta_i(B)) - (\lambda_{i+1}(B) + |C_{i+1}|)$. Il suffit d'échanger les termes $|C_{i+1}|$ et $\beta_{i+1}(B)$ pour obtenir :

$$|C_{i+1}| \leqslant (\lambda_i(B) + \beta_i(B)) - (\lambda_{i+1}(B) + \beta_{i+1}(B)).$$

Ce qui signifie que C_{i+1} vérifie la condition $E'_{i+1}(B)$.

Assertion 6 *:* Il existe un sous-groupe de N_i qui est un $(i+1)$-noyau et tel que toutes les $(i+1)$-cellules incluses dans N_i soient périodiques modulo ce sous-groupe.

On considère alors une $(i+1)$-cellule C_{i+1} et un $(i+1)$-noyau N_{i+1} inclus dans N_i. Soient k l'entier tel que l'intersection de C_{i+1} et N_{i+1} soit une k-cellule et l l'entier tel que $P_B(N_{i+1} \cup C_{i+1})$ soit une l-cellule. On a d'après le corollaire 35 :

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_{i+1}(B) + \lambda_{i+1}(B).$$

Avec $l \geqslant i+1$ d'après le lemme 41 (car C_{i+1} vérifie $E'_{i+1}(B)$ d'après l'assertion 5), ceci impose $k \leqslant i+1$. Mais tous les j-noyaux avec $j \leqslant i$ sont de cardinaux strictement supérieurs à $\beta_{i+1}(B)$, donc $N_{i+1} \cap C_{i+1}$, qui est de cardinal inférieur à $\beta_{i+1}(B)$, ne peut être une j-cellule avec $j \leqslant i$. C'est donc que $k = i+1$ et $l = i+1$. Ainsi si un $(i+1)$-noyau et une $(i+1)$-cellule sont inclus dans N_i, et que leur intersection n'est pas vide, le $(i+1)$-noyau est inclus dans la $(i+1)$-cellule.

Pour un $(i+1)$-noyau contenant 0, N_{i+1}, il contient au moins deux éléments car $\lambda_{i+1}(B) < |B| - 1$. On obtient que pour tout $x \in N_{i+1}$, N_{i+1} et $x + N_{i+1}$ sont d'intersection non vide, ainsi $N_{i+1} = x + N_{i+1}$, ce qui signifie que N_{i+1} est un sous-groupe strict de N_i, (différent de $\{0\}$, car $\lambda_{i+1}(B) < |B|-1$) et que toute $(i+1)$-cellule est une union de classes modulo N_{i+1}, donc périodique de période contenant N_{i+1}.

Conclusion : L'assertion 6 a établi l'existence d'un sous-groupe strict N_{i+1} de N_i qui est un $(i+1)$-noyau. Pour démontrer l'hypothèse de récurrence au rang $i+1$, il ne reste plus qu'à prouver que toutes les $(i+1)$-cellules sont N_{i+1}-périodiques.

On montre par récurrence descendante sur j allant de i à 1 que toutes les $(i+1)$-cellules incluses dans un j-noyau sont N_{i+1}-périodiques. L'assertion 6 établit déjà cette périodicité pour toutes les $(i+1)$-cellules incluses dans N_i et donc par translation à toutes les $(i+1)$-cellules incluses dans un i-noyau.

Supposons que pour un certain rang j, toutes les $(i+1)$-cellules incluses dans un j-noyau sont N_{i+1}-périodiques. Si l'on considère une $(i+1)$-cellule C_{i+1} incluse dans un $(j-1)$-noyau, d'après l'assertion 4, elle ou sa duale est composée d'une $(i+1)$-cellule incluse dans un j-noyau et d'une union éventuelle de j-noyaux. Comme tout

j-noyau est N_{i+1}-périodique, car $N_{i+1} \subset N_j$, d'après l'hypothèse de récurrence C_{i+1} ou $D_B(C_{i+1})$ est N_{i+1}-périodique.

De plus, d'après la proposition 20, toute cellule a la même période que sa duale. Ainsi, C_{i+1} est nécessairement N_{i+1}-périodique. On a donc montré que toute $(i+1)$-cellule incluse dans un $(j-1)$-noyau est N_{i+1}-périodique, ce qui est l'hypothèse au rang $j-1$.

Cette récurrence vient d'établir que toute $(i+1)$-cellule incluse dans un 1-noyau est N_{i+1}-périodique.

Finalement, si l'on considère une $(i+1)$-cellule dans G, d'après l'assertion 3, C_{i+1} ou sa duale est composée d'une $(i+1)$-cellule incluse dans un 1-noyau et d'une union éventuelle de 1-noyaux. Comme tout 1-noyau est N_{i+1}-périodique, car $N_{i+1} \subset N_1$, C_{i+1} ou $D_B(C_{i+1})$ est N_{i+1}-périodique. Or d'après la proposition 20 toute cellule a la même période que sa duale. Ainsi, toute $(i+1)$-cellule est N_{i+1}-périodique.

Cela prouve l'hypothèse de récurrence au rang $i+1$ et clôt la preuve du théorème. □

Remarque 9. — *Comme pour tout $1 \leqslant i \leqslant n$, N_i est un i-noyau, et que la suite des $(N_i)_{i=1,..,n}$ est décroissante pour l'inclusion, on a :*

$$|N_1 + B| - |N_1| < ... < |N_n + B| - |N_n| < |B| - 1 < |N_n + B| < ... < |N_1 + B|.$$

Cela peut se comprendre comme une approximation de l'ensemble B par les ensembles $N_i + B$. On retrouve dans cette approximation un des éléments de la décomposition récursive de Kemperman [**19**].

4. Théorème de Kneser

À l'aide des éléments mis en place dans les parties précédentes, et principalement du théorème 43, nous pouvons désormais démontrer le théorème 5 énoncé en introduction :

Démonstration. — Lorsque G est fini, le cas où $A + B = G$ est trivial, en effet $A + B$ est G-périodique, et on a bien $|A + B| = |G| = |G| + |G| - |G|$.

On considère désormais le cas où $A + B \neq G$. On considère la cellule $P_B(A)$ pour B, on a $P_B(A) + B = A + B$ d'après la proposition 7. Par ailleurs $P_B(A)$ est fini (d'après le lemme 24). De plus, d'après la proposition 30 :

$$|P_B(A) + B| - |P_B(A)| \leqslant |A + B| - |A| < |B| - 1.$$

Ainsi $P_B(A)$ est une i-cellule avec $\lambda_i(B) < |B| - 1$ pour un certain entier i. D'après le théorème 43, il existe un sous-groupe fini $N_i \neq \{0\}$, qui est un i-noyau pour B, et $P_B(A)$ est périodique, avec $N_i \subset \pi(P_B(A))$. La somme $P_B(A) + B$ est alors aussi périodique, et comme il s'agit aussi de la somme $A + B$, on a montré que $A + B$ est périodique.

De plus si H est la période de $A + B$, pour $X \subset G$ on note $\overline{X}$ l'image de X dans le groupe quotient G/H par le morphisme canonique. La somme $A + B$ étant maximalement H-périodique, la somme $\overline{A + B}$ n'est plus périodique. Par la contraposée du théorème 43, on a donc l'inégalité $|\overline{A + B}| \geqslant |\overline{A}| + |\overline{B}| - 1$.

Comme $A+B$ est H-périodique, on a $|A+B| = |H|.|\overline{A+B}|$. De plus $|\overline{A}| = |A+H|/|H|$ et $|\overline{B}| = |B+H|/|H|$. En multipliant par $|H|$ l'inégalité $|\overline{A+B}| \geqslant |\overline{A}|+|\overline{B}|-1$, on obtient donc $|A+B| \geqslant |A+H|+|B+H|-|H|$.

Or la première inégalité donne $|A+B| < |A+H|+|B+H|-1$. Comme $|A+B|$ est divisible par $|H|$, on en déduit $|A+B| \leqslant |A+H|+|B+H|-|H|$, ce qui conclut la preuve. □

Remarque 10. — *La méthode se base sur des outils de pivot B, elle désymétrise la paire (A,B). Notons que si $|A+B| < |A|+|B|-1$, $P_B(A)$ est une i-cellule pour B avec $\lambda_i(B) < |B|-1$ alors, si N_i est le i-noyau contenant 0 pour B, $P_A(N_i)$ est aussi une j-cellule pour A avec $\lambda_j(A) < |A|-1$.*

De plus, si N_j est le j-noyau contenant 0 pour A, on a : $N_i \subset N_j$ ou $N_j \subset N_i$.

Démonstration. — Si $|A+B| < |A|+|B|-1$, alors $P_B(A)$ est une i-cellule avec $\lambda_i(B) < |B|-1$, donc si N_i est le i-noyau pour B contenant 0, on a $A+N_i \subset P_B(A)$. De plus, si $A+N_i \neq P_B(A)$, alors on a $|A+N_i|+|N_i| \leqslant |P_B(A)|$, ce qui impose :

$$\begin{aligned} |A+B| &\geqslant |P_B(A)|+\lambda_i(B) \\ &\geqslant |A+N_i|+|N_i|+|B+N_i|-|N_i| \\ &= |A+N_i|+|B+N_i| \\ &> |A|+|B|-1, \end{aligned}$$

ce qui est contraire à l'hypothèse, ainsi $A+N_i = P_B(A)$. On déduit alors de $|A+B|-|P_B(A)| = \lambda_i(B)$, l'inégalité :

$$|A+B| = |A+N_i|+|B+N_i|-|N_i|.$$

De l'inégalité $|A+N_i|+|B+N_i|-|N_i| < |A|+|B|-1$, on déduit :

$$\begin{aligned} |A+N_i|-|N_i| &< |A|-1+(|B|-|B+N_i|) \\ &\leqslant |A|-1. \end{aligned}$$

Ainsi $P_A(N_i)$ est aussi une j-cellule pour A avec $\lambda_j(A) < |A|-1$. D'après le théorème 43, j-noyau pour A contenant 0, N_j est un sous-groupe de G. On a alors aussi similairement $P_A(N_i) = N_i+N_j$ et $|A+N_i| = |N_i+N_j|+|A+N_j|-|N_j|$.

Des deux égalités : $|A+B| = |A+N_i|+|B+N_i|-|N_i|$ et $|A+N_i| = |N_i+N_j|+|A+N_j|-|N_j|$, on obtient :

$$|A+B| = |A+N_j|+|B+N_i|+|N_i+N_j|-|N_j|-|N_i|.$$

On peut maintenant, à partir de l'inégalité $|A+B| < |A|+|B|-1$, donner une majoration de $|N_i+N_j|$:

$$\begin{aligned} |N_i+N_j| &= |A+B|-|A+N_j|-|B+N_i|+|N_j|+|N_i| \\ &< |N_j|+|N_i|+(|A|-|A+N_j|)+(|B|-|B+N_i|)-1 \\ &\leqslant |N_j|+|N_i|-1. \end{aligned}$$

Or N_i et N_j sont deux sous-groupes finis de G, on sait alors que :

$$|N_i+N_j| = \frac{|N_i||N_j|}{|N_i \cap N_j|}.$$

Si l'on suppose que $N_i \not\subset N_j$ et $N_j \not\subset N_i$, on a alors :

$$\begin{aligned} |N_i + N_j| &= \max(|N_i|, |N_j|) \frac{\min(|N_i|, |N_j|)}{|N_i \cap N_j|} \\ &\geqslant 2\max(|N_i|, |N_j|). \end{aligned}$$

Ce qui contredit l'inégalité $|N_i + N_j| < |N_j| + |N_i| - 1$. □

Références

[1] E. Balandraud, thèse en préparation à l'université Bordeaux 1.

[2] L. V. Brailovsky et G. A. Freiman, *On a product of finite subsets in a torsion-free group*, J. Algebra **130** (1990), 462-476.

[3] A.-L. Cauchy, *Recherches sur les nombres*, J. Ecole Polytech. **9** (1813), 99-116.

[4] I. Chowla, *A theorem on the additions of residue classes : application to the number* $\Lambda(k)$ *in the Waring's problem*, Proc. Indian Acad. Sci. **2** (1937), 242-245.

[5] I. Chowla, H. B. Mann et E. G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh. (Trondheim) **32** (1959), 74-80.

[6] H. Davenport, *On the addition of residue classes*, J. Lond. Math. Soc. **10** (1935), 30-32.

[7] H. Davenport, *A historical note*, J. Lond. Math. Soc. **22** (1947), 100-101.

[8] G. T. Diderrich, *On Kneser's addition theorem in groups*, Proc. Amer. Math. Soc. **38** (1973), 443-451.

[9] G. A. Freiman, *On the addition of finite sets. I*, Izv. Vysš. Učebn. Zaved. Matematika **6** (13) (1959), 202-213.

[10] J. L. Gross et J. Yellen (Éditeurs), *Handbook of Graph Theory*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, 2004.

[11] Y. ould Hamidoune, *Sur les atomes d'un graphe orienté*, C.R. Acad. Sci. Paris **284** (1977), 1253-1256.

[12] Y. ould Hamidoune, *On the connectivity of Cayley digraphs*, Europ. J. Combin. **5** (1984), 309-312.

[13] Y. ould Hamidoune, *An isoperimetric method in additive Theory*, J. Algebra **179** (1996), 622-630.

[14] Y. ould Hamidoune, *Subsets with small sums in abelian groups I : the Vosper property*, Europ. J. Combin. **18** (1997), 541-556.

[15] Y. ould Hamidoune, *On the diophantine Frobenius problem*, Portugal. Math. **55** (1998), no.4, 425-449.

[16] Y. ould Hamidoune, *Some results in additive number theory I : the critical pair theory*, Acta arith. **96.2** (2000), 97-119.

[17] Y. ould Hamidoune et A. Plagne, *A generalization of Freiman's 3k-3 Theorem*, Acta arith. **103.2** (2002), 147-155.

[18] Y. ould Hamidoune et A. Plagne, *A multiple set version of the 3k-3 Theorem*, Rev. Mat. Iberoam. **21** (2005), no.1, 133-161.

[19] J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. **103** (1960), 63-88.

[20] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. **58** (1953), 459-484.

[21] M. Kneser, *Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429-434.

[22] H. B. Mann, *An addition theorem for sets of elements of an abelian group*, Proc. Amer. Math. Soc. **4** (1953), 423.

[23] M. B. Nathanson, *Additive number theory : inverse problems and the geometry of sumsets*, GTM **165**, Springer-Verlag, 1996.

[24] A. Plagne, *À propos de la fonction X d'Erdős et Graham*, Ann. Inst. Fourier (Grenoble) **54** (2004), no.6, 1717-1767.

[25] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. Lond. Math. Soc. **31** (1956), 200-205.

[26] G. Vosper, *Addendum to "The critical pairs of subsets of a group of prime order"*, J. Lond. Math. Soc. **31** (1956), 280-282.

[27] G. Zémor, *A generalisation to noncommutative groups of a theorem of Mann*, Discrete Math. **126** (1994), 365-372.

Éric Balandraud, A2X, 351 cours de la Libération, 33405 TALENCE
E-mail : eric.balandraud@math.u-bordeaux1.fr, eric.balandraud@math.polytechnique.fr

COMPLÈMENT À "UN NOUVEAU POINT DE VUE ISOPÉRIMÉTRIQUE APPLIQUÉ AU THÉORÈME DE KNESER"

Nous allons ici développer un point concernant l'article "*Un nouveau point de vue isopérimétrique appliqué au théorème de Kneser*", concernant la fonction P_B. La numérotation reprend celle de l'article.

5. Autour de la question: $A + B = P_B(A) + P_A(B)$?

Soit G un groupe abélien et A et B deux sous-ensembles finis de G. Les fonctions P_B et P_A sont définies dans deux cadres d'étude bien distincts, chacune étant définie pour l'étude spécifique des sommes par B ou par A. Elles ont donc a priori peu de relation. Cependant on a:

$$P_B(A) + B = A + B = A + P_A(B).$$

Il est alors naturel de se poser la question:

A-t-on l'égalité $P_B(A) + P_A(B) = A + B$?

L'inclusion $A+B \subset P_B(A)+P_A(B)$ est évidente, car $A \subset P_B(A)$ et $B \subset P_A(B)$. Cependant, en toute généralité, l'inclusion inverse est fausse. On peut en donner un premier exemple dans $\mathbb{Z}$:

Exemple 1. *Dans le groupe $\mathbb{Z}$, soient $A = \{-2, -1, 1, 2\}$ et $B = \{-4, -3, 3, 4\}$, on a $A + B = [-6, -1] \cup [1, 6]$. On détermine aisément que $P_B(A) = [-2, 2] = A \cup \{0\}$ et que $P_A(B) = \{-4, -3, 0, 3, 4\} = B \cup \{0\}$. D'où, $P_B(A) + P_A(B) = [-6, 6] = (A + B) \cup \{0\}$. Ainsi $P_B(A) + P_A(B) \neq A + B$.*

Dans le cas particulier des ensembles de petite somme, on peut par contre établir cette égalité:

Proposition 44. *Soient G un groupe abélien, A et B deux sous-ensembles finis de G. Si $|A + B| \leqslant |A| + |B| - 1$ alors $P_B(A) + P_A(B) = A + B$.*

Démonstration. On a par définition, les égalités $P_B(A)+B = A+B = A+P_A(B)$, ainsi si $P_A(B) = B$ ou $P_B(A) = A$, la proposition est vraie.

Supposons que $P_A(B) \neq B$ et $P_B(A) \neq A$, soient $p \in P_A(B) \smallsetminus B$ et $q \in P_B(A) \smallsetminus A$. On pose $A' = A \cup \{q\}$ et $B' = B \cup \{p\}$. On peut alors déterminer la somme $A' + B' = (A + B) \cup (A + p) \cup (q + B) \cup \{p + q\}$. Or comme $p \in P_A(B)$, on a $p + A \subset A + B$, de même $q + B \subset A + B$. Ainsi, on a:

$$A' + B' = (A + B) \cup \{p + q\}.$$

On en déduit la majoration de $A' + B'$:

$$\begin{aligned} |A' + B'| &\leqslant |A + B| + 1 \\ &\leqslant |A| + |B| \\ &= |A'| + |B'| - 2. \end{aligned}$$

On peut alors utiliser le théorème de Scherk, qui affirme ici que dans la somme $A' + B'$ tous les éléments ont au moins deux écritures, comme somme d'un élément de A' et d'un élément de B'.

Théorème 45. *(Scherk)*[1] *Soit G un groupe abélien. Si A et B sont deux sous-ensembles finis de G tels que: $|A+B| = |A| + |B| - \rho$, alors tout élément s de la somme $A+B$ admet au moins ρ écritures distinctes $s = a+b$, avec $a \in A$ et $b \in B$.*

En particulier, l'élément $p+q$ admet une seconde écriture. Il existe $a \in A'$ et $b \in B'$ tels que $a+b = p+q$ et $(a,b) \neq (q,p)$. Nécessairement, on a $a \in A$ et $b \in B$, ainsi $p+q = a+b \in A+B$. On a alors $P_B(A) + P_A(B) = A+B$. □

Cette proposition ne peut par contre pas s'étendre au cas de somme plus large comme le montre l'exemple suivant:

Exemple 2. *On considère le groupe $\mathbb{Z}/5\mathbb{Z}$ et les deux sous-ensembles $A = \{1,4\}$, $B = \{2,3\}$. On a alors $A+B = \{1,2,3,4\}$. La somme vérifie ainsi:*

$$|A+B| = |A| + |B|.$$

On détermine $P_B(A) = \{0,1,4\} = A \cup \{0\}$ et $P_A(B) = \{0,2,3\} = B \cup \{0\}$. On a alors $P_B(A) + P_A(B) = \{0,1,2,3,4\} = (A+B) \cup \{0\}$. Ainsi:

$$P_B(A) + P_A(B) \neq A+B.$$

References

[1] P. Scherk et J.H.B. Kemperman, *Complexes in abelian groups*, Can. J. Math., **6** (1954), 230-237.

THE ISOPERIMETRIC METHOD IN NON-ABELIAN GROUPS WITH AN APPLICATION TO OPTIMALLY SMALL SUMSETS

ÉRIC BALANDRAUD

Abstract. Set addition theory was born a few decades ago from additive number theory. Several difficult issues, more combinatorial in nature than algebraic, have been revealed. In particular, computing the values taken by the function:

$$\mu_G : \left| \begin{array}{ccc} [1,|G|]^2 & \to & \mathbb{N}^* \\ (r,s) & \mapsto & \min\{|A.B||A \subset G,\ |A|=r,\ B \subset G,\ |B|=s\}, \end{array} \right.$$

where G is a given group does not seem easy in general. Some successive results, using Kneser's Theorem, allowed the determination of the values of this function, provided that the group G is abelian.

Recently, a method called isoperimetric, has been developed by Hamidoune and allowed new proofs and generalisations of the classical theorems in additive number theory. For instance, a new interpretation of the isoperimetric method has been able to give a new proof of Kneser's Theorem.

The purpose of this article is to adapt this last proof in a non abelian group, in order to give new values of the function μ_G, for some solvable groups and symmetric groups. These values allow us in particular to answer negatively a question asked in the litterature on the μ_G functions.

1. Introduction

Let $(G,.)$ be a group. Let A and B be two subsets of G and g an element of G, we denote $A.B = \{a.b|a \in A,\ b \in B\}$, $g.B = \{g\}.B$ and $B^{-1} = \{b^{-1}|b \in B\}$. By convention, we denote $\emptyset.B = \emptyset$.

Considering a finite group G, we define the function:

$$\mu_G : \left| \begin{array}{ccc} [1,|G|]^2 & \to & \mathbb{N}^* \\ (r,s) & \mapsto & \min\{|A.B||A \subset G,\ |A|=r,\ B \subset G,\ |B|=s\}. \end{array} \right.$$

The so-called prehistorical lemma (folklore) asserts that if A and B are two subsets of a finite group such that $|A|+|B| > |G|$, then $A.B = G$. It gives a first easy result on the function μ_G: if $r+s > |G|$, then $\mu_G(r,s) = |G|$. This lemma can also be stated as follows: for A subset of a left-coset $a.H$ and B subset of a right-coset $H.b$ modulo a same finite subgroup H of G, if $|A|+|B| > |H|$ then $A.B = a.H.b$. This seems to point out that the values of the function μ_G are related with the cardinalities of the finite subgroups of G.

In the case of cyclic groups of prime order, $\mathbb{Z}/p\mathbb{Z}$, the Cauchy-Davenport Theorem [3, 4, 5] gives the expression:

$$\mu_{\mathbb{Z}/p\mathbb{Z}}(r,s) = \min\{r+s-1, p\}.$$

In 1981, Yuzvinsky [22] showed, for groups of the form $(\mathbb{Z}/2\mathbb{Z})^n$, the equality between the μ_G function and the Hopf-Stiefel-Pfister function, well known in topology and quadratic form theory. Then, Bollobás and Leader [2] proved that the μ_G function for p-groups depends only on $|G|$ and not on the structure of the group. They also study the case of any abelian finite p-group. Eliahou and Kervaire [8]

2000 Mathematics Subject Classification: 11P70.

gave a formula for p-groups of the form $(\mathbb{Z}/p\mathbb{Z})^n$. In 2003, Plagne [19] gave for all cyclic groups the following formula:

$$\mu_{\mathbb{Z}/n\mathbb{Z}}(r,s) = \min_{d|n} \left\{ \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \right\}.$$

This result was then extended to finite abelian groups by Eliahou, Kervaire and Plagne [9]:

Theorem 1. *Let G be a finite abelian group, r and s two integers satisfying $1 \leqslant r, s \leqslant |G|$, then:*

$$\mu_G(r,s) = \min_{d||G|} \left\{ \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \right\}.$$

Moreover the authors of [9] asked if the following generalization holds:

Conjecture 2. *Let G be a finite group, r and s two integers from $[1, |G|]$, then:*

$$\mu_G(r,s) = \min_{H \leqslant G} \left\{ \left(\left\lceil \frac{r}{|H|} \right\rceil + \left\lceil \frac{s}{|H|} \right\rceil - 1 \right) |H| \right\}.$$

In parts 2 and 3, we give the recapitulation of the definitions and basic properties of the isoperimetric interpretation of [1], without proofs. These proofs do not contain any difficult point. They are based only on elementary set-theoretical considerations. In part 4, we give a first structural result, on 1-kernels and 1-cells, that is a new proof in our language of a result of Zémor, [23]. The new interpretation allows us to give a new structural result for the j-cells for some value of j well fitted for our purpose in part 5.

In the sixth and last part, we show how to deduce from this last structural result some new exact values for the μ_G function. These new values are in contradiction with conjecture 2 for solvable groups and for symmetric groups.

Another question asked in [9] is the inverse problem of characterizing the pairs of subsets A and B of G with the prescribed cardinalities $|A| = r$ and $|B| = s$ which realize the minimal sumset size $|A+B| = \mu_G(r,s)$. In abelian groups, the answer of the inverse problem is a consequence of Kemperman theorem [17]. In non-abelian groups, there is no similar theorem. However the method used to compute $\mu_G(r,s)$ in Part 6 gives also a characterisation of the subsets that realize the minimal sumset size and thus it answers the associated inverse problem too.

2. ADDITIVE TOOLS OF PIVOT $B \subset G$

In this whole part, we consider a group G and a subset B of G. The proofs of all the properties of this section are in [1].

2.1. The Application $P_B : X \mapsto G \smallsetminus ((G \smallsetminus (X.B)).B^{-1})$.

We denote $\mathbf{P}(G)$ the set of all subsets of G.

We study the properties of the application:

$$P_B : \left| \begin{array}{ccc} \mathbf{P}(G) & \to & \mathbf{P}(G) \\ X & \mapsto & G \smallsetminus ((G \smallsetminus (X.B)).B^{-1}). \end{array} \right.$$

The study of this application allows us to notice that for a given subset X, the set $P_B(X)$ is characteristic (in the meaning of the equivalence (3)) of the product $X.B$.

Among the properties of this application, studied in [1], we recall that for all subsets X of G, we have:

$$X \subset P_B(X), \tag{1}$$

and

$$X.B = P_B(X).B. \tag{2}$$

We can easily establish the following fundamental properties:

- The application P_B verifies $P_B^2 = P_B$.
- For any subsets X and Y of G, we have:

$$X.B = Y.B \text{ if and only if } P_B(X) = P_B(Y). \tag{3}$$

The proofs of these properties are based on elementary set-theoretical considerations and are not difficult. The set $P_B(X)$ can also be expressed by the following formula: $P_B(X) = \{g \in G | g.B \subset X.B\}$.

2.2. **Properties of $\mathbf{C}_B$, the set of images of P_B.** We denote by $\mathbf{C}_B$ the set:

$$\mathbf{C}_B = P_B(\mathbf{P}(G)).$$

The elements of $\mathbf{C}_B$ will be called the cells for B.

Among the cells, we notice that $P_B(\emptyset) = \emptyset$, therefore $\emptyset \in \mathbf{C}_B$. Similarly, we have $P_B(G) = G$, and thus $G \in \mathbf{C}_B$.

The set $\mathbf{C}_B$ of cells for B has some interesting properties that we mention now.

- It can easily be checked that for any subset X of G, and any $g \in G$, we have: $P_B(g.X) = g.P_B(X)$. We deduce from this that the set $\mathbf{C}_B$ is stable by translation on the left.
- Set-theoretical considerations prove that the P_B function is increasing: for any subsets X and Y of G, if $X \subset Y$ then $P_B(X) \subset P_B(Y)$. An interesting consequence of this fact is that for any cells C_1 and C_2 for B, $C_1 \cap C_2$ is also a cell for B. This statement means that the set $\mathbf{C}_B$ is stable by intersection.

In the particular case of abelian groups, it can also be checked that for any subset X of G we have: $(P_B(X))^{-1} = P_{B^{-1}}(X^{-1})$. We deduce from this that the two sets $\mathbf{C}_B$ and $\mathbf{C}_{B^{-1}}$ are symmetric: for any subset X of G, $X \in \mathbf{C}_B$ if and only if $X^{-1} \in \mathbf{C}_{B^{-1}}$.

2.3. **Additive duality $D_B : X \mapsto G \smallsetminus (X.B)$.** We now consider the following function:

$$D_B : \left| \begin{array}{ccc} \mathbf{P}(G) & \to & \mathbf{P}(G) \\ X & \mapsto & G \smallsetminus (X.B). \end{array} \right.$$

We may immediately notice that: $P_B = D_{B^{-1}} \circ D_B$. Moreover, since the expression of $D_B(X)$ depends uniquely on $X.B$, we have: $D_B(X) = D_B(P_B(X))$. We can deduce from this that the image of the function D_B is $\mathbf{C}_{B^{-1}}$ and that D_B is a bijection from $\mathbf{C}_B$ to $\mathbf{C}_{B^{-1}}$. Its reciprocal map is $D_{B^{-1}}$.

The additive duality has the following properties:

- For any subset X of G and any $g \in G$, we have: $D_B(g.X) = g.D_B(X)$.
- The map D_B is decreasing: for any subsets X and Y of G, if $X \subset Y$ then $D_B(Y) \subset D_B(X)$. From this fact, we deduce:

$$P_B(X \cup Y) = D_{B^{-1}}(D_B(X) \cap D_B(Y)). \tag{4}$$

In the case where the group G is abelian, for any subset X of G, we have the symmetry: $D_B(X^{-1}) = (D_{B^{-1}}(X))^{-1}$.

2.4. **Contributions from B.** Until now, no assumption has been made on B. If some assumption on B is made, we may deduce some interesting additional properties.

- If G is infinite and B is a non-empty finite set, then the image of a finite subset by P_B is finite. Therfore the duality D_B is a bijection from the subset of finite cells of $\mathbf{C}_B$ on the set of cells of finite complement of $\mathbf{C}_{B^{-1}}$.

- If B is a subset containing 1, then for any subset $X \subset G$, the three sets X, $(X.B) \smallsetminus X$ and $D_B(X)$ form together a partition of G. Moreover for any cell C for B, we have:

$$(C.B) \smallsetminus C = (D_B(C).B^{-1}) \smallsetminus D_B(C). \tag{5}$$

This equality will be of great importance in the sequel. We will see that the condition that $1 \in B$ can be assumed without loss of generality.

3. Isoperimetric ideas

In this part, we consider a group G and a non-empty finite subset B of G. The proofs of all the properties of this section are in [1].

3.1. **Definitions and first properties.** We are interested in the first values of the application:

$$\Phi_B : \left| \begin{array}{ccc} \mathbf{P}_f(G) & \to & \mathbb{N} \\ X & \mapsto & |X.B| - |X|, \end{array} \right.$$

that gives, when $1 \in B$, the number of elements of the perimeter of X in the Cayley graph of (G, B), (the graph whose vertices are the elements of G and whose edges are the couples (g_1, g_2) such that $g_1^{-1}.g_2 \in B$). Cayley graphs are a popular topic in graph theory, as can be read in chapter 6 of [10]. This is after this graph theoretical point-of-view that Hamidoune called his method isoperimetric.

A first look allows to notice that for any $g \in G$, we have: $\Phi_B = \Phi_{B.g}$. If we choose $g = b^{-1}$, with $b \in B$, this means that we can here consider that 1 belongs to B without loss of generality. Therefore we can notice that for any subset X of G, we have $X \subset (X.B)$ and we can write: $\Phi_B(X) = |(X.B) \smallsetminus X|$. The function Φ_B can thus be extended to all subsets of G.

Thus, for B a finite subset of G containing 1, we consider the function:

$$\Phi_B : \left| \begin{array}{ccc} \mathbf{P}(G) & \to & \mathbb{N} \cup \{\infty\} \\ X & \mapsto & |(X.B) \smallsetminus X|. \end{array} \right.$$

This function has the following properties:

- For any $g \in G$ and any subset X of G, we have: $\Phi_B(X) = \Phi_B(g.X)$.
- For any subset X of G, we have: $\Phi_B(P_B(X)) \leqslant \Phi_B(X)$. Moreover the equality case, $\Phi_B(P_B(X)) = \Phi_B(X)$ implies that $X \in \mathbf{C}_B$.
- for any cell C for B that is either finite or has a finite complement, we have:

$$\Phi_B(C) = \Phi_{B^{-1}}(D_B(C)). \tag{6}$$

- In the case where G is an abelian group and B is a finite subset of G containing 1, we have for any subset X of G: $\Phi_B(X) = \Phi_{B^{-1}}(X^{-1})$.

These properties will allow us to limit the study of sets of small product with B to the cells for B. In order to study the cells for B, we will use the properties of additive duality, of translation, and in the abelian case of symmetry.

3.2. **k-cells and k-kernels.** We denote $\mathbf{C}_B^0 = \{\emptyset,\ G\}$. From what has been shown in part 2, we have $\mathbf{C}_B^0 \subset \mathbf{C}_B$. We also denote $\lambda_0(B) = 0 = \Phi_B(\emptyset) = \Phi_B(G)$. We call any element from $\mathbf{C}_B^0$ a 0-cell.

We now introduce a notation for cells that are either finite or have a finite complement. This notation consists to order them according to the size of their perimeters. The set of these perimeters will be called the second isoperimetric sequence (where the first one is the sequence defined in Hamidoune's articles, [11, 12, 14, 15, 16]):

Definition 1. *We call second sequence of isoperimetric numbers, the increasing (possibly finite) sequence of values taken by the function Φ_B on the set of cells for B of $\mathbf{C}_{B,f} \setminus \mathbf{C}_B^0$, that are either finite or have a finite complement, we denote this sequence:*

$$\Phi_B(\mathbf{C}_{B,f} \setminus \mathbf{C}_B^0) = \{0 \leqslant \lambda_1(B) < \lambda_2(B) < \ldots\}.$$

Property (6) ensures that this sequence is the same for the set B and for its symmetric B^{-1}.

Definition 2. *For any non zero integer k, we call k-cell, a cell C that is either finite or has a finite complement, that is not a 0-cell and such that $\Phi_B(C) = \lambda_k(B)$. We denote $\mathbf{C}_B^k$ the set of k-cells.*

In other words: If $\lambda_1(B) = 0$, we have:

$$\mathbf{C}_B^1 = (\mathbf{C}_{B,f} \setminus \mathbf{C}_B^0) \cap \Phi_B^{-1}(\lambda_1(B)).$$

For $k > 1$, and for any $k \in \mathbb{N}$ if $\lambda_1(B) \neq 0$, we have:

$$\mathbf{C}_B^k = \mathbf{C}_{B,f} \cap \Phi_B^{-1}(\lambda_k(B)).$$

Among k-cells, when there are some that are finite, the ones of minimal cardinality will have a specific role. We state the following definition to distinguish them.

Definition 3. *For a non zero integer k, we call k-kernel, a k-cell of finite minimal cardinality, if there is any. We denote this cardinality $\beta_k(B)$.*

It follows from this definition, that a k-kernel, when it exists, is always finite.

Remark 1. *At least one from the two values, $\beta_k(B)$ or $\beta_k(B^{-1})$, exists.*

Lemma 3. *For any non zero integer k such that $\beta_k(B)$ and $\beta_k(B^{-1})$ both exist, we have:*

$$\beta_k(B) + \lambda_k(B) + \beta_k(B^{-1}) \leqslant |G|.$$

In the abelian case, since we have $\Phi_B(X) = \Phi_{B^{-1}}(X^{-1})$ and $(X \in \mathbf{C}_B \Leftrightarrow X^{-1} \in \mathbf{C}_{B^{-1}})$, we deduce that for any non zero integer:

$$\lambda_k(B) = \lambda_k(B^{-1}), \text{ and } \beta_k(B) = \beta_k(B^{-1}).$$

Remark 2. *The first isoperimetric tools have been developed by Y. ould Hamidoune, mostly in* [14] *and* [16]. *The tools that have been defined previously in this article are not the same as Hamidoune's ones. However for $k = 1$, or in finite groups, the 1-kernels are exactly the 1-atoms defined by Hamidoune and the 1-cells are the 1-fragments of Hamidoune.*

3.3. **Fundamental inequality.** We consider a group G and a subset B of G containing 1. As has already been noticed in part 2.4, for X a subset of G, the three sets X, $(X.B) \setminus X$ and $D_B(X)$, form a partition of G. We state now a fundamental inequality that will be of great use. This inequality is a classical one, it can be found in lemma 3.5 of [16].

Proposition 4. *Let G be a group, B a finite subset of G containing 1, X and Y two subsets that are either finite or have a finite complement of G. We have:*

$$\Phi_B(X \cap Y) + \Phi_B(X \cup Y) \leqslant \Phi_B(X) + \Phi_B(Y).$$

We can deduce from this last proposition the following fundamental result, that will be used a lot in this article:

Corollary 5. *Let C_i be a i-cell for B and C_j a j-cell for B, k the integer such that $C_i \cap C_j$ is a k-cell for B, and l such that $P_B(C_i \cup C_j)$ is a l-cell for B, then we have the inequality:*

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_i(B) + \lambda_j(B).$$

Moreover, if this inequality is an equality, then $P_B(C_i \cup C_j) = C_i \cup C_j$.

Another more technical inequality will be of great use. It is a generalization of the inequality (5) of [16].

Lemma 6. *Let C_i be a finite i-cell for B and C_j a j-cell for B, k the integer such that $C_i \cap C_j$ is a k-cell for B. If $k \geqslant j$, we have:*

$$\lambda_j(B) + |D_B(C_j) \smallsetminus D_B(C_i)| \leqslant \lambda_i(B) + |C_i \smallsetminus C_j|.$$

4. Structure of the 1-cells and 1-kernels

This section gives a structural result on 1-kernels and 1-cells, which paraphrases, in our language, a work by Zémor, [23].

4.1. **Existence condition of 1-cells.** Let G be a group and B a finite subset of G. If $B = G$, then for any non empty $X \subset G$, we have $X.B = G$. Therefore the only cells are $\emptyset$ and G and there is no 1-cell.

Otherwise, if B is different from G, then for X reduced to a single element, we have:

$$|X.B| - |X| = |B| - 1 \text{ and } X.B \neq G.$$

This implies that $X \neq \emptyset$ and $X.B \neq G$, therefore $P_B(X)$ is not a 0-cell. Thus 1-cells for B do exist. Consequently, at least one from the two numbers $\beta_1(B)$ and $\beta_1(B^{-1})$ exists and $\lambda_1(B) \leqslant |B| - 1$.

4.2. **Structure of the 1-cells and 1-kernels.** Let G be a group and B a subset of G, B different from G. If $\lambda_1(B) = |B| - 1$, then a 1-kernel is naturally composed of a unique element. Therefore we will consider the case $\lambda_1(B) < |B| - 1$, which implies that the 1-kernels contain strictly more than one element.

Definition 4. *If $\beta_1(B)$ exists, we call condition $E_1(B)$ for a cell C for B, the condition:*

$$|G \smallsetminus C| \geqslant \lambda_1(B) + \beta_1(B).$$

Remark 3. *If $\beta_1(B) \leqslant \beta_1(B^{-1})$, any 1-cell for B satisfies the condition $E_1(B)$.*

Proof. If C_1 is a 1-cell for B, $D_B(C_1)$ is a 1-cell for B^{-1} and is then of cardinality greater than $\beta_1(B^{-1})$, therefore we have:

$$|G \smallsetminus C_1| - \lambda_1(B) = |D_B(C_1)| \geqslant \beta_1(B^{-1}) \geqslant \beta_1(B),$$

and C_1 satisfies the condition $E_1(B)$. □

We show now some consequence on the 1-cells that satisfy the condition $E_1(B)$.

Proposition 7. *Let G be a group, B a finite subset of G containing 1 and such that $\beta_1(B)$ exists. Let N_1 be a 1-kernel and C_1 a 1-cell for B such that C_1 satisfies the condition $E_1(B)$. If $N_1 \cap C_1 \neq \emptyset$, then $N_1 \subset C_1$.*

Proof. The 1-kernel N_1 is by definition finite, of cardinality $\beta_1(B)$. The intersection $C_1 \cap N_1$ is a finite k-cell, with $k \geqslant 1$.

We are now considering the union $C_1 \cup N_1$. Let l be the integer such that $P_B(C_1 \cup N_1)$ is a l-cell. We will show that $l \geqslant 1$.

By lemma 6, we have:

$$|D_B(C_1) \smallsetminus D_B(N_1)| \leqslant |N_1 \smallsetminus C_1|.$$

Moreover, since C_1 satisfies the condition $E_1(B)$, we can write:

$$|D_B(C_1)| \geqslant \beta_1(B) = |N_1|.$$

Thus we can show that $D_B(C_1) \cap D_B(N_1) \neq \emptyset$. Indeed, we have:

$$\begin{aligned} |D_B(C_1) \cap D_B(N_1)| &= |D_B(C_1)| - |D_B(C_1) \smallsetminus D_B(N_1)| \\ &\geqslant |D_B(C_1)| - |N_1 \smallsetminus C_1| \\ &\geqslant |N_1| - |N_1 \smallsetminus C_1| \\ &= |N_1 \cap C_1| > 0. \end{aligned}$$

Since $D_B(C_1 \cup N_1) = D_B(C_1) \cap D_B(N_1)$ from (4) and because we just showed that this set is non empty, it is a l-cell for B with $l \geqslant 1$.

Then corollary 5 gives:

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_1(B) + \lambda_1(B).$$

This inequality holds with $k \geqslant 1$ and $l \geqslant 1$. Since the sequence of values $\lambda_i(B)$, with $i \geqslant 1$ is strictly increasing, we necessarily have $k = l = 1$.

Moreover, N_1 is a 1-kernel, which is a 1-cell of minimal cardinality, therefore the equality $k = 1$ implies the inclusion $N_1 \subset C_1$. □

With the help of proposition 7, we can give a first structural result for 1-kernels for B, and for all the 1-cells that satisfy the condition $E_1(B)$. This result is contained in theorem 1.2 of [23], we give here a new proof in our language.

Theorem 8. *Let G be a group, B a finite subset of G containing 1. There exists a finite subgroup N_1 of G, that is a 1-kernel for B or for B^{-1} such that for any 1-cell C_1, C_1 or $C_1.B$ is right-periodic modulo N_1.*

Proof. If $\lambda_1(B) = |B| - 1$, the subgroup $N_1 = \{0\}$ fits. We can hence consider that $\lambda_1(B) < |B| - 1$. If there is a 1-cell that satisfies the condition $E_1(B)$, then a 1-kernel also satisfies the condition $E_1(B)$. If we consider two 1-kernels for B, that are of non empty intersection, by proposition 7 they are included the one in the other, then they are equals. Consequently two distinct 1-kernels are disjoint.

If N_1 is a 1-kernel for B containing 1 and if $x \in N_1$ with $x \neq 1$, N_1 and $x^{-1}.N_1$ are two 1-kernels for B that contain 1 therefore their intersection is non empty, they are therefore equal: $N_1 = x^{-1}.N_1$.

Thus we have for any $x \in N_1$, $x^{-1}.N_1 = N_1$, which means that N_1 is a finite subgroup of G. By translation all left-cosets modulo N_1 are 1-kernels. And since all left-cosets modulo N_1 form a partition of G, there cannot be another 1-kernel.

If C_1 is a 1-cell for B that satisfies the condition $E_1(B)$, proposition 7 asserts that it contains all the 1-kernels it meets. Then C_1 is a union of left-cosets modulo N_1 and therefore $C_1.N_1 = C_1$.

If $\beta_1(B) \leqslant \beta_1(B^{-1})$, by remark 3 every 1-cell satisfies the condition $E_1(B)$, and the theorem is proved.

If $\beta_1(B) > \beta_1(B^{-1})$, there exists a finite subgroup N_1 that is a 1-kernel for B^{-1} and all 1-cells for B^{-1} satisfies the condition $E_1(B^{-1})$ and are therefore right-periodic modulo N_1. If C_1 is a 1-cell for B, then $C_1.B$ is the complement of a right-periodic set modulo N_1, therefore it is also right-periodic modulo N_1. □

Corollary 9. *Let G be a group, B a finite subset of G containing 1. There exists a finite subgroup N_1 such that $\lambda_1(B) = \left(\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1\right)|N_1|$. Moreover for any finite 1-cell C_1, $|C_1|$ and $|C_1.B|$ are multiples of $|N_1|$.*

Proof. From theorem 8, if $\beta_1(B) \leqslant \beta_1(B^{-1})$, then a 1-kernel N_1 for B containing 1, is a finite subgroup of G and we have:

$$\lambda_1(B) = |N_1.B| - |N_1| < |B| - 1 < |N_1.B|.$$

That means that $\lambda_1(B)$ is the greatest multiple of $\beta_1(B)$ strictly less than $|B|$, this can be written:

$$\lambda_1(B) = \left(\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1 \right) |N_1|.$$

Moreover, for any finite 1-cell C_1, C_1 is right-periodic modulo N_1, thus $|C_1|$ is a multiple of $|N_1|$. For the product $C_1.B$, we have $|C_1.B| = \lambda_1(B) + |C_1|$, thus $|C_1.B|$ is also a multiple of $|N_1|$.

If $\beta_1(B) \geqslant \beta_1(B^{-1})$, then a 1-kernel N_1 for B^{-1} containing 1 is a finite subgroup of G. Thus we have for B^{-1}:

$$\lambda_1(B) = \lambda_1(B^{-1}) = \left(\left\lceil \frac{|B^{-1}|}{|N_1|} \right\rceil - 1 \right) |N_1| = \left(\left\lceil \frac{|B|}{|N_1|} \right\rceil - 1 \right) |N_1|.$$

Moreover for any finite 1-cell C_1 for B, its dual $D_B(C_1)$ is right-periodic modulo N_1, thus its complement $C_1.B$ is also right-periodic modulo N_1. Therefore $|C_1.B|$ is a multiple of $|N_1|$, and $|C_1| = |C_1.B| - \lambda_1(B)$ also. □

4.3. **Non-abelian specificities.** In an abelian group, we have $\beta_1(B) = \beta_1(B^{-1})$ and a 1-kernel for B is also a 1-kernel for B^{-1} as it is stated in theorem 38 in [1]. In a non-abelian group, such equalities do not hold in general, nevertheless we can prove the following propositions:

Proposition 10. *Let G be a group and B a finite subset of G, if $\beta_1(B)$ and $\beta_1(B^{-1})$ both exist and are such that $\beta_1(B) < \beta_1(B^{-1})$, then $\beta_1(B)$ divides $\beta_1(B^{-1})$.*

Proof. Indeed, if we consider N_1 a 1-kernel for B that contains 1, it is a finite subgroup of G and we have $\lambda_1(B) = |N_1.B| - |N_1|$, where $N_1.B$ is a union of right-cosets modulo N_1. Thus $\beta_1(B)$ divides $\lambda_1(B)$.

Moreover, by remark 3, if N_1' is a 1-kernel for B^{-1} then $D_{B^{-1}}(N_1')$ is a 1-cell for B that satisfies the condition $E_1(B)$. Therefore by theorem 8, $D_{B^{-1}}(N_1')$ is a union of left-cosets modulo N_1. Consequently $\beta_1(B)$ divides $|G \setminus (D_{B^{-1}}(N_1'))| = \lambda_1(B) + \beta_1(B^{-1})$. □

Even when a 1-kernel does not satisfy the condition $E_1(B)$, we can give a structural description of the 1-kernel in the way of the following proposition.

Proposition 11. *Let G be a finite group and B a subset of G containing 1. Suppose that there is not any 1-cell for B that satisfies the condition $E_1(B)$. For N_1 a 1-kernel for B, then $N_1.B$ is the complement of a left-coset modulo a subgroup of G.*

It is enough to use a similar argument, based not on the minimality of the kernels, but on the maximality of the dual of N_1. This will be proved in annex section 7.

5. Relations with the following cells and kernels

We will now focus our interest on the relations between the 1-cells and the following ones. In the case of a set B such that $\beta_1(B) \leqslant \beta_1(B^{-1})$, we denote by a_2 the least index, such that there exists a a_2-cell strictly included in a 1-kernel or a a_2-cell that does not satisfy the condition $E_1(B)$. From remark 3 and proposition 7, we have $a_2 > 1$. The purpose of this section is to give a structural result about a_2-cells similar to theorem 8 about 1-cells.

Lemma 12. *Let G be a group, B a finite subset that contains 1, such that $\beta_1(B) \leqslant \beta_1(B^{-1})$. Every j-cell, that satisfies the condition $E_1(B)$, is a disjoint union of 1-kernels and k-cells, each included in a 1-kernels, with $k \leqslant j$.*

Moreover, any a_2-cell, that satisfies the condition $E_1(B)$, is a disjoint union of 1-kernels and at most one a_2-cell included in an 1-kernel.

Proof. By remark 1, necessarily, $\beta_1(B)$ exists. We consider C_j a j-cell for B, that satisfies the condition $E_1(B)$ and a 1-kernel N_1 that intersects C_j. Let k be the non zero integer such that $C_j \cap N_1$ is a k-cell.

Suppose that $k \geqslant j$, by lemma 6, we have: $\lambda_j(B)+|D_B(C_j) \smallsetminus D_B(N_1)| \leqslant \lambda_1(B)+|N_1 \smallsetminus C_j|$, which can be written $|D_B(C_j) \smallsetminus D_B(N_1)| \leqslant \lambda_1(B) - \lambda_j(B) + |N_1 \smallsetminus C_j|$.

Since C_j satisfies the condition $E_1(B)$, we have $|G \smallsetminus C_j| \geqslant \lambda_1(B)+\beta_1(B)$, which can be written $|D_B(C_j)| \geqslant \beta_1(B) + \lambda_1(B) - \lambda_j(B)$.

We can with the use of these two last inequalities give a lower bound for $|D_B(C_j) \cap D_B(N_1)|$:

$$\begin{aligned} |D_B(C_j) \cap D_B(N_1)| &= |D_B(C_j)| - |D_B(C_j) \smallsetminus D_B(N_1)| \\ &\geqslant |D_B(C_j)| - \lambda_1(B) + \lambda_j(B) - |N_1 \smallsetminus C_j| \\ &\geqslant (\beta_1(B) + \lambda_1(B) - \lambda_j(B)) - \lambda_1(B) + \lambda_j(B) - |N_1 \smallsetminus C_j| \\ &= |N_1| - |N_1 \smallsetminus C_j| \\ &= |N_1 \cap C_j| > 0. \end{aligned}$$

This last statement implies that $P_B(C_j \cup N_1)$ is a l-cell with $l \geqslant 1$.

If we consider the inequality of corollary 5, we have:

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_1(B) + \lambda_j(B).$$

But this inequality is false with the assumptions $k > j$ and $l \geqslant 1$. Therefore we necessarily have $k \leqslant j$.

Moreover, if we consider a a_2-cell C_{a_2}, that satisfies the condition $E_1(B)$ and that is not a union of 1-kernels and N_1 a 1-kernel such that, $N_1 \cap C_{a_2} \neq \emptyset$ and $N_1 \not\subset C_{a_2}$. Let k and l be the integers such that $N_1 \cap C_{a_2}$ is a k-cell, and $P_B(N_1 \cup C_{a_2})$ is a l-cell. By corollary 5, we have:

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_1(B) + \lambda_{a_2}(B).$$

This equality holds with $k \leqslant a_2$ and $l \geqslant 1$. Since the k-cell $N_1 \cap C_{a_2}$ is stricly included in N_1, we also have by the definition of a_2, $k \geqslant a_2$. Thus necessarily $k = a_2$ and $l = 1$, and the previous inequality is an equality. Therefore Corollary 5 asserts that $P_B(N_1 \cup C_{a_2}) = N_1 \cup C_{a_2}$ is a 1-cell, consequently it is a union of 1-kernels, which proves the unicity of N_1. □

Consequently, the j-cells with $1 \leqslant j < a_2$ have a similar structure as the 1-cells:

Proposition 13. *Let G be a group and B a finite subset of G containing 1. There is a finite subgroup N_1 such that for any j-cell C_j with $1 \leqslant j < a_2$, C_j or $C_j.B$ is a union of left-cosets modulo N_1.*

Proof. If we have $\beta_1(B) \leqslant \beta_1(B^{-1})$, then considering a j-cell, C_j with $1 \leqslant j < a_2$, by definition of a_2, it satisfies the condition $E_1(B)$. Theorem 8 asserts that a 1-kernel N_1 containing 1 is a subgroup. Moreover, if N_1' is a 1-kernel that intersects C_j, by lemma 12, the intersection is a k-cell included in a 1-kernel with $k \leqslant j$ and therefore $k < a_2$. By definition of a_2, we necessarily have $k = 1$, thus C_j is a union of 1-kernels and therefore is right-periodic modulo the 1-kernel N_1.

If we have $\beta_1(B) > \beta_1(B^{-1})$, then when we consider a j-cell C_j, from what has been proved in the previous case, its dual $D_B(C_j.B)$ is a union of left-cosets modulo N_1, the 1-kernel for B^{-1} containing 1. Therefore the complement of the dual, $C_j.B$, is also a union of left-cosets modulo N_1. □

In order to go further, we want to study the a_2-cells. If there exists a finite a_2-cell, then we define the condition:

Definition 5. *If $\beta_{a_2}(B)$ exists, we call condition $E_{a_2}(B)$ for a cell C for B, the condition:*

$$|G \smallsetminus C| \geqslant \lambda_{a_2}(B) + \beta_{a_2}(B).$$

This condition will be useful to prove that the union of a a_2-cell with a a_2-kernel will not give a 0-cell (the entire group G), as proves the following lemma:

Lemma 14. *Let G be a group, B a finite subset that contains 1. Let C be a 1-cell or a a_2-cell and N_{a_2} be a a_2-kernel. Let k be the integer such that $C \cap N_{a_2}$ is a k-cell. If $k \geqslant a_2$ and C satisfies the condition $E_{a_2}(B)$ then we have $P_B(C \cup N_{a_2}) \neq G$.*

Proof. Since $k \geqslant a_2$, by lemma 6, we have: $|D_B(C) \smallsetminus D_B(N_{a_2})| \leqslant |N_{a_2} \smallsetminus C|$. Moreover, C satisfies the condition $E_{a_2}(B)$, which implies that $|D_B(C)| \geqslant \beta_{a_2}(B)$. Thus we can give a lower bound of $|D_B(C) \cap D_B(N_{a_2})|$, if it is finite, as follows:

$$\begin{aligned} |D_B(C) \cap D_B(N_{a_2})| &= |D_B(C)| - |D_B(C) \smallsetminus D_B(N_{a_2})| \\ &\geqslant \beta_{a_2}(B) - |N_{a_2} \smallsetminus C| \\ &= |N_{a_2} \cap C| > 0. \end{aligned}$$

□

Some other definitions and conditions will be necessary to avoid that a union of a_2-cells gives a 1-cell.

If there exists a a_2-cell strictly included in a 1-kernel, we define the two following conditions:

Definition 6. *If B is such that $\beta_1(B)$ exists, and if there exists a a_2-cell C_{a_2} included in a 1-kernel N_1, we denote:*

$$\beta'_{1,a_2}(B) = \min\{|(N_1.B) \smallsetminus (C_{a_2}.B)|/C_{a_2} \subset N_1\}.$$

Remark 4. *From this definition, we see that in this situation, we have:*

$$\beta_{a_2}(B) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B) \leqslant \lambda_1(B) + \beta_1(B).$$

Definition 7. *If B is such that $\beta_1(B)$ exists and if a a_2-kernel N_{a_2} and a j-cell C_j for B are both included in the 1-kernel N_1 for B, we call condition $F_{1,a_2}(B)$ for C_j, the condition:*

$$|C_j| \leqslant (\lambda_1(B) + \beta_1(B)) - (\lambda_{a_2}(B) + \beta_{a_2}(B)).$$

Definition 8. *If B is such that $\beta_1(B)$ exists, and if a a_2-kernel N_{a_2} and a j-cell C_j for B are both included in the 1-kernel N_1 for B, we call condition $F'_{1,a_2}(B)$ for C_j, the condition:*

$$|C_j| \geqslant \beta'_{1,a_2}(B).$$

We focus our interest on the relations between the two conditions $F_{1,a_2}(B)$ and $F'_{1,a_2}(B)$ for some j-cell C_j included in a 1-kernel.

Lemma 15. *Let G be a group and B a finite subset of G containing 1 such that $\beta_1(B)$ exists. Suppose that a a_2-kernel N_{a_2} and a j-cell C_j for B are both included in the 1-kernel N_1 for B. If C_j does not satisfy the condition $F_{1,a_2}(B)$, then C_j satisfies the condition $F'_{1,a_2}(B)$.*

Proof. Indeed, if C_j does not satisfy the condition $F_{1,a_2}(B)$, we have:

$$\begin{aligned} |C_j| &> (\lambda_1(B) + \beta_1(B)) - (\lambda_{a_2}(B) + \beta_{a_2}(B))) \\ &= |(N_1.B) \smallsetminus (N_{a_2}.B)| \\ &\geqslant \min\{|(N_1.B) \smallsetminus (C_{a_2}.B)|/C_{a_2} \subset N_1\} \\ &= \beta'_{1,a_2}(B). \end{aligned}$$

□

Remark 5. *If $\beta_{a_2}(B) \leqslant \beta'_{1,a_2}(B)$, then every a_2-cell included in a 1-kernel N_1 satisfies the condition $F_{1,a_2}(B)$.*

If $\beta_{a_2}(B) > \beta'_{1,a_2}(B)$, then every a_2-cell included in a 1-kernel N_1 satisfies the condition $F'_{1,a_2}(B)$.

We will now see in the following lemmas what can be deduced from conditions $F_{1,a_2}(B)$ or $F'_{1,a_2}(B)$.

Lemma 16. *Let G be a group and B a finite subset of G containing 1 such that $\beta_1(B)$ exists. Let N_{a_2} be a a_2-kernel and C_j be a j-cell for B, both included in the 1-kernel N_1 for B. Let k be the integer such that $N_{a_2} \cap C_j$ is a k-cell. If C_j satisfies the condition $F_{1,a_2}(B)$ and $k \geqslant j$, then $P_B(N_{a_2} \cup C_j) \neq N_1$.*

Proof. We will show that $N_{a_2} \cup C_j$ and N_1 do not give the same product with B, more precisely we show that the set $|(N_1.B) \smallsetminus ((N_{a_2} \cup C_j).B)|$ is not empty.

In a first step, we give a lower bound for $|(N_1.B) \smallsetminus (C_j.B)| = |D_B(C_j) \smallsetminus D_B(N_1)|$, arguing that C_j satisfies the condition $F_{1,a_2}(B)$:

$$\begin{aligned} |(N_1.B) \smallsetminus (C_j.B)| &= |N_1.B| - |C_j.B| \\ &= |N_1.B| - |C_j| - \lambda_j(B) \\ &\geqslant (\lambda_1(B) + \beta_1(B)) - (\lambda_1(B) + \beta_1(B)) \\ &\qquad + (\lambda_{a_2}(B) + \beta_{a_2}(B)) - \lambda_j(B) \\ &= \lambda_{a_2}(B) + \beta_{a_2}(B) - \lambda_j(B). \end{aligned}$$

By lemma 6 and the last inequality we have:

$$\begin{aligned} |(N_1.B) \smallsetminus ((N_{a_2} \cup C_j).B)| &= |(N_1.B) \smallsetminus (C_j.B)| - |(N_{a_2}.B) \smallsetminus (C_j.B)| \\ &= |(N_1.B) \smallsetminus (C_j.B)| - |D_B(C_j) \smallsetminus D_B(N_{a_2})| \\ &\geqslant \lambda_{a_2}(B) + \beta_{a_2}(B) - \lambda_j(B) \\ &\qquad - (-\lambda_j(B) + \lambda_{a_2}(B) + |N_{a_2} \smallsetminus C_j|) \\ &= \beta_{a_2}(B) - |N_{a_2} \smallsetminus C_j| \\ &= |N_{a_2} \cap C_j| > 0. \end{aligned}$$

Thus this proves that $(N_{a_2} \cup C_j).B \neq N_1.B$. Therefore equivalence (3) implies that $P_B(N_{a_2} \cup C_j) \neq N_1$. □

We show now a consequence of the condition $F'_{1,a_2}(B)$.

Lemma 17. *Let G be a group, B a finite subset of G containing 1 such that $\beta_1(B) \leqslant \beta_1(B^{-1})$, N_1 the 1-kernel for B that contains 1. We denote B_k, for $1 \leqslant k \leqslant l$, the sets $B \cap (N_1.b_k)$ for $b_k \in B$ such that B is the disjoint union of these l sets. Suppose that there is a a_2-cell in N_1 that satisfies the condition $F'_{1,a_2}(B)$. There exists an index k_0 such that if a j-cell C_j included in N_1 satisfies the condition $F'_{1,a_2}(B)$, $C_j.B_{k_0} \neq N_1.b_{k_0}$ and, if $k \neq k_0$, $C_j.B_k = N_1.b_k$.*

Moreover, we have $|B| \leqslant \lambda_{a_2}(B) + \beta'_{1,a_2}(B)$.

Proof. Let N'_{a_2} be a a_2-cell included in N_1 such that $\beta'_{1,a_2}(B) = |(N_1.B) \smallsetminus (N'_{a_2}.B)|$. The a_2-cell N'_{a_2} is therefore a a_2-cell of maximal size in N_1. Since there exists a a_2-cell satisfying the condition $F'_{1,a_2}(B)$ in N_1, N'_{a_2} satisfies the condition $F'_{1,a_2}(B)$. The two cells N_1 and N'_{a_2} being different, they cannot give the same product by B, $N_1.B \neq N'_{a_2}.B$. This implies that there exists a k_0 such that $N'_{a_2}.B_{k_0} \neq N_1.b_{k_0}$.

Suppose that there exist two distinct integers k_1 and k_2 such that: $N'_{a_2}.B_{k_1} \neq N_1.b_{k_1}$ and $N'_{a_2}.B_{k_2} \neq N_1.b_{k_2}$. By the prehistorical lemma, we have $|B_{k_1}| \leqslant |N_1| - |N'_{a_2}|$ and $|B_{k_2}| \leqslant |N_1| - |N'_{a_2}|$. Therefore we can majorize $|B|$ by $(l-2)|N_1| +$

$2(|N_1|-|N'_{a_2}|) = l|N_1|-2|N'_{a_2}|$. But since N'_{a_2} is a a_2-cell, we have $|N'_{a_2}.B|-|N'_{a_2}| < |B|-1$. Therefore we deduce the inequality:

$$1+|N'_{a_2}.B|-|N'_{a_2}| < l|N_1|-2|N'_{a_2}|.$$

But $l|N_1| = |N_1.B|$, thus the previous inequality leads to $|N'_{a_2}|+1 < |(N_1.B) \smallsetminus (N'_{a_2}.B)|$. This can be rewritten $|N'_{a_2}|+1 < \beta'_{1,a_2}(B)$, but this is in contradiction with the hypothesis that N'_{a_2} satisfies the condition $F'_{1,a_2}(B)$. This proves the unicity of k_0.

Moreover, since $|B|-1 > \lambda_{a_2}(B)$, we have:

$$\begin{aligned}
\sum_{k\neq k_0}|B_k| &> \lambda_{a_2}(B)-|B_{k_0}|+1\\
&= |N'_{a_2}.B|-|N'_{a_2}|-|B_{k_0}|+1\\
&= |N_1.B|-|(N_1.B)\smallsetminus(N'_{a_2}.B)|-|N'_{a_2}|-|B_{k_0}|+1\\
&= l|N_1|-\beta'_{1,a_2}(B)-|N'_{a_2}|-|B_{k_0}|+1\\
&= (l-1)|N_1|-\beta'_{1,a_2}(B)+(|N_1|-|N'_{a_2}|-|B_{k_0}|+1)\\
&> (l-1)|N_1|-\beta'_{1,a_2}(B).
\end{aligned}$$

However for a j-cell C_j included in N_1 and that satisfies the condition $F'_{1,a_2}(B)$, we have by definition $|C_j| \geqslant \beta'_{1,a_2}(B)$. Therefore the inequality $|C_j|+\sum_{k\neq k_0}|B_k| > (l-1)|N_1|$ implies $C_j.\bigcup_{k\neq k_0}B_k = N_1.\bigcup_{k\neq k_0}B_k = \bigcup_{k\neq k_0}N_1.b_k$.

Moreover, the inequality $|N'_{a_2}|+|B_{k_0}| \leqslant |N_1|$ implies:

$$\begin{aligned}
|B_{k_0}| &\leqslant |N_1|-|N'_{a_2}|\\
&= |(N_1.B_{k_0})\smallsetminus(N'_{a_2}.B_{k_0})|+|N'_{a_2}.B_{k_0}|-|N'_{a_2}|\\
&= \beta'_{1,a_2}(B)+(\lambda_{a_2}(B)-\lambda_1(B)).
\end{aligned}$$

Since the inclusion $\bigcup_{k\neq k_0}B_k \subset \bigcup_{k\neq k_0}N_1.b_k$ gives $\sum_{k\neq k_0}|B_k| \leqslant (l-1)|N_1| = \lambda_1(B)$, we finally have the inequality:

$$\begin{aligned}
|B| &= |B_{k_0}|+\sum_{k\neq k_0}|B_k|\\
&\leqslant (\lambda_{a_2}(B)-\lambda_1(B)+\beta'_{1,a_2}(B))+\lambda_1(B)\\
&= \lambda_{a_2}(B)+\beta'_{1,a_2}(B).
\end{aligned}$$

□

We show now a structural result on a_2-cells under the assumption that there exists a a_2-cell that is not a union of 1-kernels and satisfies $E_1(B)$.

Proposition 18. *Let G be a group, B a finite subset of G containing 1, such that $\beta_1(B) \leqslant \beta_1(B^{-1})$ and $\lambda_{a_2}(B) < |B|-1$. Suppose that there exists a a_2-cell that satisfies the condition $E_1(B)$ and that is not a union of 1-kernels. There exists a proper subgroup N_{a_2} of N_1 such that if C_2 is a a_2-cell included in N_1, C_2 or $C_2.B$ is a disjoint union of cosets modulo some conjugates of N_{a_2} and of N_1.*

Moreover, we have $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|}\right\rceil - 1\right)|N_{a_2}|$.

Proof. If there exists a a_2-cell C_{a_2} that satisfies the condition $E_1(B)$, that is not a union of 1-kernels, then there exists a 1-kernel such that its intersection with C_{a_2} is neither empty nor the entire 1-kernel. By lemma 12, the intersection is necessarily a a_2-cell included in the 1-kernel and the union is therefore a 1-cell.

Thus we consider the a_2-cells included in the 1-kernel N_1. Again, two cases appear:

- *(Direct case)* If $\beta_{a_2}(B) \leqslant \beta'_{1,a_2}(B)$, then every a_2-cell included in N_1 satisfies the condition $F_{1,a_2}(B)$. If we consider a a_2-kernel N_{a_2} and a a_2-cell C_{a_2} included in N_1, such that $N_{a_2} \cap C_{a_2}$ is a k-cell with $k \geqslant 1$ and that $P_B(N_{a_2} \cap C_{a_2})$ is a l-cell, we have by corollary 5:

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_{a_2}(B) + \lambda_{a_2}(B).$$

  By definition of a_2, we have $k \geqslant a_2$. By lemma 16, we have $P_B(N_{a_2} \cup C_{a_2}) \neq N_1$, therefore $l \geqslant a_2$. We deduce from it that $k = l = a_2$. Moreover if the intersection is a a_2-cell, we have $N_{a_2} \subset C_{a_2}$.

  In particular if we consider the a_2-kernel N_{a_2} that contains 1, then for every $x \in N_{a_2}$, we have: $x^{-1}.N_{a_2} \cap N_{a_2} \neq \emptyset$. Thus we deduce that $x^{-1}.N_{a_2} = N_{a_2}$. This means that N_{a_2} is a subgroup of N_1. Any a_2-kernel is therefore a left-coset modulo N_{a_2} and every a_2-cells that satisfies $E_1(B)$ is then right-periodic modulo N_{a_2}.

  Moreover, we have:

$$\lambda_{a_2}(B) = |N_{a_2}.B| - |N_{a_2}| < |B| - 1 < |N_{a_2}.B|.$$

  Since N_{a_2} is a subgroup, $|N_{a_2}.B| - |N_{a_2}|$ and $|N_{a_2}.B|$ are two consecutive multiples of $|N_{a_2}|$. This last statement can be written: $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}|$.
- *(Reverse case)* If $\beta_{a_2}(B) > \beta'_{1,a_2}(B)$, then any a_2-cell included in N_1 satisfies the condition $F'_{1,a_2}(B)$. Let us denote B_k, for $1 \leqslant k \leqslant l$, the sets $B \cap (N_1.b_k)$ for $b_k \in B$ such that B is the disjoint union of these l sets. By lemma 17, there exists an index k_0 such that for any a_2-cell C_{a_2} included in N_1, $C_{a_2}.B_{k_0} \neq N_1.b_{k_0}$ and if $k \neq k_0$, $C_{a_2}.B_k = N_1.b_k$.

  We consider then the set $B_{k_0}.b_{k_0}^{-1}$ in the finite group N_1, we have then for any a_2-cell C_{a_2} included in N_1:

$$\begin{aligned} |C_{a_2}.B_{k_0}.b_{k_0}^{-1}| - |C_{a_2}| &= |C_{a_2}.B| - |C_{a_2}| - \Big|\bigcup_{k\neq k_0} N_1.B_k\Big| \\ &< |B| - 1 - \Big|\bigcup_{k\neq k_0} B_k\Big| \\ &= |B_{k_0}| - 1. \end{aligned}$$

  Then C_{a_2} gives a small product for $B_{k_0}.b_{k_0}^{-1}$ in N_1. If C'_1 is a 1-cell for $B_{k_0}.b_{k_0}^{-1}$ in N_1, we have:

$$\begin{aligned} |C'_1.B| - |C'_1| &\leqslant |C'_1.B_{k_0}| - |C'_1| + \Big|\bigcup_{k\neq k_0} N_1.B_k\Big| \\ &\leqslant |C_{a_2}.B_{k_0}.b_{k_0}^{-1}| - |C_{a_2}| + \lambda_1(B) \\ &= \lambda_{a_2}(B) - \lambda_1(B) + \lambda_1(B) \\ &= \lambda_{a_2}(B). \end{aligned}$$

  Since there is no j-cell for B with $j < a_2$ in N_1, it means that the a_2-cells for B included in N_1 are exactly the 1-cells for $B_{k_0}.b_{k_0}^{-1}$. We have then $\beta_1(b_{k_0}.B_{k_0}^{-1}) = \beta'_{1,a_2}(B)$. The condition $\beta_{a_2}(B) > \beta'_{1,a_2}(B)$ then corresponds to the condition $\beta_1(B_{k_0}.b_{k_0}^{-1}) > \beta_1(b_{k_0}.B_{k_0}^{-1})$. Thus by theorem 8 there exists a subgroup of N_1, N_{a_2} of cardinality $\beta'_{1,a_2}(B)$ that is a 1-kernel for $b_{k_0}.B_{k_0}^{-1}$ and such that every 1-cell for $b_{k_0}.B_{k_0}^{-1}$ is right-periodic modulo N_{a_2}.

Finally for any a_2-cell C_{a_2} for B included in N_1, the product $C_{a_2}.B$ is a union of right-cosets modulo N_1: $\bigcup_{k\neq k_0} N_1.B_k$, and in a union of left-cosets modulo the conjugate $b_{k_0}^{-1}.N_{a_2}.b_{k_0}$ of N_{a_2}: $C_{a_2}.B_{k_0}$. Thus $|C_{a_2}.B|$ is a multiple of $|N_{a_2}|$ and $\lambda_{a_2}(B)$ also.

Lemma 17 gives another information on the cardinality of $|B|$: $|B| \leqslant \lambda_{a_2}(B) + \beta'_{1,a_2}(B)$. Therefore we have the double inequality:

$$\lambda_{a_2}(B) < |B| \leqslant \lambda_{a_2}(B) + \beta'_{1,a_2}(B),$$

from which we deduce the equality: $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right) |N_{a_2}|$.

□

Corollary 19. *In the conditions of proposition 18, for any finite a_2-cell C_{a_2} that satisfies the condition $E_1(B)$, the two integers $|C_{a_2}|$ and $|C_{a_2}.B|$ are multiples of $|N_{a_2}|$.*

Proof. Indeed, proposition 18 proves the existence of a subgroup N_{a_2} of N_1 such that $\lambda_{a_2}(B)$ is a multiple of $|N_{a_2}|$. For a a_2-cell C_{a_2} that satisfies the condition $E_1(B)$, lemma 12 asserts that it is a disjoint union of 1-kernels and at most one a_2-cell included in a 1-kernel. Therefore, it is enough to prove the corollary for the a_2-cell included in a 1-kernel.

Proposition 18 proves also that for any a_2-cell C_{a_2} included in a 1-kernel, C_{a_2} or $D_B(C_{a_2})$ is a disjoint union of cosets modulo conjugates of N_1 and N_{a_2}. Therefore one from the two numbers $|C_{a_2}|$ and $|C_{a_2}.B|$ is a multiple of $|N_{a_2}|$.

Moreover since C_{a_2} is a a_2-cell, we have $|C_{a_2}.B| - |C_{a_2}| = \lambda_{a_2}(B)$ which is a multiple of $|N_{a_2}|$, then the numbers $|C_{a_2}|$ and $|C_{a_2}.B|$ are both multiples of $|N_{a_2}|$. □

We show now a second structural result on a_2-cells under the assumption that there is a a_2-cell that does not satisfy $E_1(B)$.

Proposition 20. *Let G be a group, B a finite subset of G that contains 1, such that $\beta_1(B) < \beta_1(B^{-1})$ and $\lambda_{a_2}(B) < |B| - 1$. Suppose that there is a a_2-cell for B that does not satisfy the condition $E_1(B)$. There exists a proper subgroup N_{a_2} of G, that is a_2-kernel for B^{-1}. Moreover any 1-cell for B^{-1} and any a_2-cell for B^{-1} whose dual does not satisfy the condition $E_1(B)$ is right-periodic modulo N_{a_2}.*

Moreover, we have:

$$\lambda_{a_2}(B^{-1}) + 2\beta_{a_2}(B^{-1}) \leqslant \lambda_1(B) + \beta_1(B),$$

$$\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right) |N_{a_2}|.$$

Proof. Since there exists a a_2-cell for B that does not satisfy the condition $E_1(B)$, let us consider a a_2-cell C_{a_2} for B^{-1} whose dual does not satisfy the condition $E_1(B)$. From its definition, we have: $|G \smallsetminus D_{B^{-1}}(C_{a_2})| < \lambda_1(B) + \beta_1(B)$, therefore C_{a_2} is finite, and:

$$|C_{a_2}| < \beta_1(B) + \lambda_1(B) - \lambda_{a_2}(B).$$

Therefore we deduce that $\beta_{a_2}(B^{-1}) < \beta_1(B) + \lambda_1(B) - \lambda_{a_2}(B) < \beta_1(B)$. Since proposition 10 explains that $\beta_1(B)$ divides $\beta_1(B^{-1})$, we have $\beta_1(B^{-1}) \geqslant 2\beta_1(B)$ and $\beta_{a_2}(B^{-1}) + |C_{a_2}| < \beta_1(B^{-1}) + \lambda_1(B) - \lambda_{a_2}(B)$.

Let us consider a a_2-kernel for B^{-1} N_{a_2} and a a_2-cell C_{a_2} for B^{-1} whose dual does not satisfy the condition $E_1(B)$. Suppose that their intersection is not empty. Their intersection is then a k-cell with $k \geqslant a_2$. By lemma 6, we have:

$$|D_B(N_{a_2}) \smallsetminus D_B(C_{a_2})| \leqslant |C_{a_2} \smallsetminus N_{a_2}|.$$

Thus, we can majorize the size of $(C_{a_2} \cup N_{a_2}).B^{-1}$, as follows:

$$\begin{aligned}|(C_{a_2} \cup N_{a_2}).B^{-1}| &= |N_{a_2}.B^{-1}| + |(C_{a_2}.B^{-1}) \smallsetminus (N_{a_2}.B^{-1})| \\ &= \lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}) + |D_{B^{-1}}(N_{a_2}) \smallsetminus D_{B^{-1}}(C_{a_2})| \\ &\leqslant \lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}) + |C_{a_2} \smallsetminus N_{a_2}| \\ &< \lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}) + |C_{a_2}| \\ &< \beta_1(B^{-1}) + \lambda_1(B).\end{aligned}$$

Thus $P_{B^{-1}}(N'_{a_2} \cup N_{a_2})$ cannot be a j-cell for B^{-1} with $j < a_2$, it is then a l-cell, with $l \geqslant a_2$.

If we consider the inequality of corollary 5 taken between the two a_2-cells N_{a_2} and C_{a_2} for B^{-1}, we obtain:

$$\lambda_k(B^{-1}) + \lambda_l(B^{-1}) \leqslant \lambda_{a_2}(B^{-1}) + \lambda_{a_2}(B^{-1}).$$

This inequality holds with the condition proven above: $k \geqslant a_2$ and $l \geqslant a_2$. Then we have $k = l = a_2$. The fact that $k = a_2$ implies that $N_{a_2} \subset C_{a_2}$. In particular two a_2-kernels are either disjoint or equal.

Let us consider the particular a_2-kernel N_{a_2} for B^{-1} that contains 1. For any $x \in N_{a_2}$, we have $1 \in N_{a_2} \cap (x^{-1}.N_{a_2})$, then $N_{a_2} = x^{-1}.N_{a_2}$ which means that N_{a_2} is a subgroup of G. All the a_2-kernels for B^{-1} are exactly the left-cosets modulo N_{a_2}, and all the a_2-cells for B^{-1} whose dual does not satisfy the condition $E_1(B)$ are right-periodic modulo N_{a_2}.

If we consider now a 1-cell C_1 for B^{-1}, and any a_2-kernel N'_{a_2} for B^{-1} that intersects it. Since $D_{B^{-1}}(C_1)$ is a 1-cell for B, we have:

$$\begin{aligned}|G \smallsetminus C_1| &\geqslant \lambda_1(B) + \beta_1(B) \\ &> \lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}),\end{aligned}$$

This means that C_1 satisfies the condition $E_{a_2}(B^{-1})$.

Let k and l be the integers such that $C_1 \cap N'_{a_2}$ is a k-cell and $P_{B^{-1}}(C_1 \cup N'_{a_2})$ is a l-cell for B^{-1}. By corollary 5, we have:

$$\lambda_k(B^{-1}) + \lambda_l(B^{-1}) \leqslant \lambda_1(B^{-1}) + \lambda_{a_2}(B^{-1}).$$

This inequality holds with $k \geqslant a_2$ and since C_1 satisfies the condition $E_{a_2}(B^{-1})$ by lemma 14, we have $l > 0$. This implies that $k = a_2$ and $l = 1$. Therefore $N'_{a_2} \subset C_1$. Thus every 1-cell for B^{-1} is right-periodic modulo N_{a_2}.

In particular, if we consider a 1-kernel N_1 for B, the 1-cell $D_B(N_1)$ for B^{-1} is right-periodic modulo N_{a_2}, therefore, its complement $N_1.B$ is also right periodic modulo N_{a_2}. Thus the integer $\lambda_1(B) + \beta_1(B)$ is a multiple of $\beta_{a_2}(B^{-1})$. The fact that $D_{B^{-1}}(N_{a_2})$ does not satisfy the condition $E_1(B)$ means that $\lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}) < \lambda_1(B) + \beta_1(B)$. Therefore, we have:

$$\lambda_{a_2}(B^{-1}) + 2\beta_{a_2}(B^{-1}) \leqslant \lambda_1(B) + \beta_1(B).$$

Finally, since N_{a_2} is a subgroup, $|N_{a_2}.B^{-1}| - |N_{a_2}|$ and $|N_{a_2}.B^{-1}|$ are two consecutive multiples of $|N_{a_2}|$. This last statement can be written:

$$\lambda_{a_2}(B) = \lambda_{a_2}(B^{-1}) = \left(\left\lceil \frac{|B^{-1}|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}| = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}|.$$

□

Propositions 18 and 20 both give some structural results for the a_2-cells when $\lambda_{a_2}(B) < |B| - 1$ under some different assumptions. We will see that these two structural results are compatible when both assumptions are made.

Theorem 21. *Let G be a group, B a finite subset of G containing 1 such that $\lambda_{a_2}(B) < |B| - 1$, then there exists a finite proper subgroup N_{a_2} of G such that $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}|$. Moreover for any finite a_2-cell C_{a_2}, $|C_{a_2}|$ and $|C_{a_2}.B|$ are multiples of $|N_{a_2}|$.*

Proof. We will consider the case where $\beta_1(B) \leqslant \beta_1(B^{-1})$ and show that the result holds for all finite a_2-cell for B and for B^{-1}. By the definition of a_2, there exists a a_2-cell, C_{a_2}, such that C_{a_2} is not a union of 1-kernels or such that it does not satisfy the condition $E_1(B)$.

We will consider three exclusive cases, where all the a_2-cells satisfy a same assumption. Three mixed cases will follow, where there coexist a_2-cells that satisfy the condition $E_1(B)$ and a_2-cells that do not.

First exclusive case:

If all a_2-cells for B satisfy the condition $E_1(B)$, lemma 12 proves that any a_2-cell is a disjoint union of one a_2-cell included in a 1-kernel and some 1-kernels. Proposition 18 proves that there exists a subgroup N_{a_2} of N_1 such that $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}|$. Moreover corollary 19 precises that for any a_2-cell C_{a_2} included in a 1-kernel $|C_{a_2}|$ is a multiple of $|N_{a_2}|$. Therefore for any finite a_2-cell C_{a_2}, the number $|C_{a_2}|$ is also a multiple of $|N_{a_2}|$, and $|C_{a_2}.B| = \lambda_{a_2}(B) + |C_{a_2}|$ also.

Moreover for any finite C_{a_2} a_2-cell for B^{-1}, $D_{B^{-1}}(C_{a_2})$ is a a_2-cell for B, thus it is the union of 1-kernels for B and of a a_2-cell included in a 1-kernel. Therefore the complement $C_{a_2}.B^{-1}$ of $D_{B^{-1}}(C_{a_2})$ has cardinality multiple of $|N_{a_2}|$. Thus the number $|C_{a_2}| = |C_{a_2}.B^{-1}| - \lambda_{a_2}(B^{-1})$ is also a multiple of $|N_{a_2}|$.

Second exclusive case:

If all a_2-cells for B do not satisfy the condition $E_1(B)$ and $\beta_1(B) < \beta_1(B^{-1})$, it implies that they are all finite. Proposition 20 proves that all the a_2-cells for B^{-1} are right-periodic modulo a subgroup N_{a_2} that is a a_2-kernel for B^{-1}. Proposition 20 also give the equality $\lambda_{a_2}(B) = \left(\left\lceil \frac{|B|}{|N_{a_2}|} \right\rceil - 1\right)|N_{a_2}|$. Moreover for any finite a_2-cell C_{a_2} for B, $D_B(C_{a_2})$ is right-periodic modulo N_{a_2} then its complement $C_{a_2}.B$ also, then $|C_{a_2}.B|$ is a multiple of $|N_{a_2}|$, and $|C_{a_2}| = |C_{a_2}.B| - \lambda_{a_2}(B)$ also.

Moreover if there is any finite C_{a_2} a_2-cell for B^{-1}, since its dual $D_{B^{-1}}(C_{a_2})$ is a a_2-cell for B, it is also finite and this implies that G is a finite group. Then the two numbers $|C_{a_2}| = |G| - |D_B(C_{a_2}).B|$ and $|C_{a_2}.B^{-1}| = |G| - |C_{a_2}|$ are also mutliples of $|N_{a_2}|$.

Third exclusive case:

If all a_2-cells for B do not satisfy the condition $E_1(B)$ and $\beta_1(B) = \beta_1(B^{-1})$, it means that all a_2-cells for B^{-1} are included in a 1-kernel for B^{-1}. Since we also have $\beta_1(B^{-1}) \geqslant \beta_1(B)$, we are reduce to the first exclusive case.

It remains to prove that the theorem is true in a general case, where there coexist a_2-cells that satisfy the condition $E_1(B)$ and a_2-cells that do not. Then the three values $\beta_{a_2}(B)$, $\beta'_{1,a_2}(B)$ and $\beta_{a_2}(B^{-1})$ are all defined. We will consider three different cases depending on which of these values is minimal.

First mixed case: if $\min\{\beta_{a_2}(B), \beta'_{1,a_2}(B), \beta_{a_2}(B^{-1})\} = \beta_{a_2}(B)$.

This case is similar to the abelian situation. The direct case of proposition 18 proves that there exists a subgroup N_{a_2} of N_1 that is a a_2-kernel for B, and that any a_2-cell that satisfies the condition $E_1(B)$ is right-periodic modulo N_{a_2}.

Moreover if we consider a a_2-cell C_{a_2} for B that does not satisfy $E_1(B)$. Its dual $D_B(C_{a_2})$ is a a_2-cell for B^{-1} which implies that $|D_B(C_{a_2})| \geqslant \beta_{a_2}(B^{-1}) \geqslant \beta_{a_2}(B)$.

Therefore $|G \smallsetminus C_{a_2}| \geqslant \lambda_{a_2}(B)+\beta_{a_2}(B)$, which means that C_{a_2} satisfies nevertheless $E_{a_2}(B)$.

Let us consider now a a_2-kernel N'_{a_2} for B that intersects C_{a_2}, let k and l be the integers such that $N'_{a_2} \cap C_{a_2}$ is a k-cell and $P_B(N'_{a_2} \cup C_{a_2})$ is a l-cell for B, by corollary 5, we have:

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_{a_2}(B) + \lambda_{a_2}(B).$$

This inequality holds with $k \geqslant a_2$, because the intersection is a subset of N'_{a_2}. Moreover C_{a_2} satisfies $E_{a_2}(B)$, therefore by lemma 14 we have $l \neq 0$. Moreover C_{a_2} does not satisfy $E_1(B)$, thus $D_B(C_2)$ is of cardinality lower than $\beta_1(B)$. Thus $D_B(C_{a_2} \cup N'_{a_2})$ is a l-cell with $l \geqslant a_2$. This implies that $k = l = a_2$ and that $N'_{a_2} \subset C_{a_2}$.

Therefore C_{a_2} is also right-periodic modulo N_{a_2}. If C_{a_2} is finite, it implies that $|C_{a_2}|$ is a multiple of $|N_{a_2}|$ and the number $|C_{a_2}.B| = |C_{a_2}| + \lambda_{a_2}(B)$ also.

If a a_2-cell C_{a_2} for B^{-1} is finite, its dual $D_{B^{-1}}(C_{a_2})$ is a a_2-cell for B, thus it is right-periodic modulo N_{a_2}. The complement $C_{a_2}.B^{-1}$ of $D_{B^{-1}}(C_{a_2})$ is therefore also right-periodic modulo N_{a_2}, thus $|C_{a_2}.B^{-1}|$ is a multiple of $|N_{a_2}|$ and the number $|C_{a_2}| = |C_{a_2}.B^{-1}| - \lambda_{a_2}(B)$ also.

Second mixed case: if $\min\{\beta_{a_2}(B), \beta'_{1,a_2}(B), \beta_{a_2}(B^{-1})\} = \beta_{a_2}(B^{-1})$ and $\beta_1(B) < \beta_1(B^{-1})$.

Proposition 20 shows that there exists a subgroup N_{a_2} of G that is a a_2-kernel for B^{-1} such that any 1-cell for B^{-1} and any a_2-cell for B^{-1} whose dual does not satisfy the condition $E_1(B)$ is a right-periodic modulo N_{a_2}.

Let us first consider a a_2-cell C_{a_2} for B included in a 1-kernel N_1. Since $|C_{a_2}| \geqslant \beta_{a_2}(B) \geqslant \beta_{a_2}(B^{-1})$, we have $|G \smallsetminus D_B(C_{a_2})| = \lambda_{a_2}(B)+|C_{a_2}| \geqslant \lambda_{a_2}(B)+\beta_{a_2}(B^{-1})$, which means that $D_B(C_{a_2})$ satisfies the condition $E_{a_2}(B^{-1})$.

Let us consider a a_2-kernel for B^{-1} N'_{a_2}, that intersects $D_B(C_{a_2}) \smallsetminus D_B(N_1)$, let k and l be the integers such that $N'_{a_2} \cap D_B(C_{a_2})$ is a k-cell and $P_B(N'_{a_2} \cup D_B(C_{a_2}))$ is a l-cell, by corollary 5, we have:

$$\lambda_k(B^{-1}) + \lambda_l(B^{-1}) \leqslant \lambda_{a_2}(B^{-1}) + \lambda_{a_2}(B^{-1}).$$

This inequality holds with $k \geqslant a_2$, because the intersection is a subset of N'_{a_2}. Since $D_B(C_{a_2})$ satisfies the condition $E_{a_2}(B^{-1})$, by lemma 14, we have $l \neq 0$. Moreover by (4), we have $D_{B^{-1}}(N'_{a_2} \cup D_B(C_{a_2})) = C_{a_2} \cap D_{B^{-1}}(N_{a_2})$, this is a subset of C_{a_2} and is strictly included in a 1-kernel for B. Therefore it is a l-cell with $l \geqslant a_2$. Therefore we have $k = l = a_2$, and this implies $N'_{a_2} \subset D_B(C_{a_2})$. It follows that $D_B(C_{a_2})$ is right-periodic modulo N_{a_2}.

If we consider now a a_2-cell C_{a_2} for B that satisfies the condition $E_1(B)$, lemma 12 proves that it is the disjoint union of 1-kernels and at most one a_2-cell included in a 1-kernel. Thus $D_B(C_{a_2})$ is the intersection of the duals of these 1-kernels and of the dual of at most one a_2-cell included in a 1-kernel. But all these duals are right-periodic modulo N_{a_2}, therefore $D_B(C_{a_2})$ is also right-periodic modulo N_{a_2}.

Therefore all a_2-cells for B^{-1} are right-periodic modulo N_{a_2}.

If C_{a_2} is a finite a_2-cell for B^{-1}, then $|C_{a_2}|$ is a multiple of $|N_{a_2}|$, and consequently $|C_{a_2}.B^{-1}| = |C_{a_2}| + \lambda_{a_2}(B)$ also.

If C_{a_2} is a finite a_2-cell for B, then its dual $D_B(C_{a_2})$ is a a_2-cell for B^{-1}, it is right-periodic modulo N_{a_2}. The complement $C_{a_2}.B$ of $D_B(C_{a_2})$ is therefore also right-periodic modulo N_{a_2}, and thus $|C_{a_2}.B|$ is a multiple of $|N_{a_2}|$. The number $|C_{a_2}| = |C_{a_2}.B| - \lambda_{a_2}(B)$ is also a multiple of N_{a_2}.

Third mixed case: if $\min\{\beta_{a_2}(B), \beta'_{1,a_2}(B), \beta_{a_2}(B^{-1})\} = \beta'_{1,a_2}(B)$.

If we have $\beta'_{1,a_2}(B) = \beta_{a_2}(B)$, we are in the case of the mixed case 1, thus we can suppose that $\beta'_{1,a_2}(B) < \beta_{a_2}(B)$.

If we have $\beta'_{1,a_2}(B) = \beta_{a_2}(B^{-1})$ and $\beta_1(B) < \beta_1(B^{-1})$, we are in the case of the mixed case 2, thus we can suppose that either $\Big(\beta'_{1,a_2}(B) < \beta_{a_2}(B^{-1})$ and $\beta_1(B) = \beta_1(B^{-1})\Big)$ or $\beta_1(B) = \beta_1(B^{-1})$.

- Let us first consider the sub-case where $\beta'_{1,a_2}(B) < \beta_{a_2}(B^{-1})$ and $\beta_1(B) < \beta_1(B^{-1})$.

  Let us consider N'_{a_2} a a_2-cell for B included in a 1-kernel N_1 for B such that $|(N_1.B) \smallsetminus (N'_{a_2}.B)| = \beta'_{1,a_2}(B) = |D_B(N'_{a_2}) \smallsetminus D_B(N_1)|$. Proposition 20 proves the existence of a a_2-kernel N_{a_2} for B^{-1} that is a subgroup of G and that any 1-cell for B^{-1} is right-periodic modulo N_{a_2}. It also asserts the inequality:

$$\lambda_{a_2}(B^{-1}) + 2\beta_{a_2}(B^{-1}) \leqslant \lambda_1(B) + \beta_1(B).$$

  From this inequality, we deduce that $\lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}) + \beta'_{1,a_2}(B) < \lambda_1(B) + \beta_1(B)$, what can be rewritten:

$$\lambda_{a_2}(B^{-1}) + \beta_{a_2}(B^{-1}) < \lambda_1(B) + \beta_1(B) - \beta'_{1,a_2}(B) = |G \smallsetminus D_B(N'_{a_2})|.$$

  This proves that $D_B(N'_{a_2})$ satisfies the condition $E_{a_2}(B^{-1})$.

  As we noticed before, the 1-cell $D_B(N_1)$ is right-periodic modulo N_{a_2}. We can now consider a a_2-kernel N''_{a_2} for B^{-1} that intersects $D_B(N'_{a_2}) \smallsetminus D_B(N_1)$. By corollary 5, we have:

$$\lambda_k(B^{-1}) + \lambda_l(B^{-1}) \leqslant \lambda_{a_2}(B^{-1}) + \lambda_{a_2}(B^{-1}).$$

  This inequality holds with $k \geqslant a_2$, because the intersection is a subset of N''_{a_2}. Moreover since $D_B(N'_{a_2})$ satisfies $E_{a_2}(B^{-1})$, by lemma 14 we have $l \neq 0$ and $D_{B^{-1}}(D_B(N'_{a_2}) \cup N''_{a_2})$ is stricly contained in N_1, therefore we have $l \neq 1$. This implies that $k = l = a_2$ and that $N''_{a_2} \subset (D_B(N'_{a_2}) \smallsetminus D_B(N_1))$. But this last inclusion proves that $\beta'_{1,a_2}(B) \geqslant \beta_{a_2}(B^{-1})$ and contradicts the hypothesis.
- Let us now consider the sub-case where $\beta_1(B) = \beta_1(B^{-1})$. Then the four numbers $\beta_{a_2}(B)$, $\beta'_{1,a_2}(B)$, $\beta_{a_2}(B^{-1})$ and $\beta'_{1,a_2}(B)$ are defined. Their definitions imply the two inequality:

$$\begin{aligned} \beta_{a_2}(B) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B) &\leqslant \lambda_1(B) + \beta_1(B), \\ \text{and } \beta_{a_2}(B^{-1}) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B^{-1}) &\leqslant \lambda_1(B) + \beta_1(B). \end{aligned}$$

  Then at least one of the two following inequalities holds:

$$\begin{aligned} \beta_{a_2}(B) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B^{-1}) &\leqslant \lambda_1(B) + \beta_1(B), \\ \text{or } \beta_{a_2}(B^{-1}) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B) &\leqslant \lambda_1(B) + \beta_1(B). \end{aligned}$$

  Since these two inequalities are symmetric, we can consider without loss of generality that the second holds:

  Let us consider N'_{a_2} a a_2-cell for B included in a 1-kernel N_1 for B such that $|(N_1.B) \smallsetminus (N'_{a_2}.B)| = \beta'_{1,a_2}(B) = |D_B(N'_{a_2}) \smallsetminus D_B(N_1)|$. We can then minimize the quantity:

$$|G \smallsetminus D_B(N'_{a_2})| = \lambda_1(B) + \beta_1(B) - \beta'_{1,a_2}(B) \geqslant \lambda_{a_2}(B) + \beta_{a_2}(B^{-1}).$$

  This means that $D_B(N'_{a_2})$ satisfies the condition $E_{a_2}(B^{-1})$.

  We can now consider a a_2-kernel N''_{a_2} for B^{-1} that intersects $D_B(N'_{a_2}) \smallsetminus D_B(N_1)$. By corollary 5, we have:

$$\lambda_k(B^{-1}) + \lambda_l(B^{-1}) \leqslant \lambda_{a_2}(B^{-1}) + \lambda_{a_2}(B^{-1}).$$

This inequality holds with $k \geqslant a_2$, because the intersection is a subset of N''_{a_2}. Moreover $D_B(N'_{a_2})$ satisfies $E_{a_2}(B^{-1})$, therefore by lemma 14 we have $l \neq 0$. Furthermore $D_{B^{-1}}(D_B(N'_{a_2}) \cup N''_{a_2})$ is stricly contained in N_1, therefore we have $l \neq 1$. This implies that $k = l = a_2$. Since the a_2-kernel for B^{-1} is stricly included in a 1-kernel for B^{-1} and that $D_B(N_1)$ is a union of 1-kernels for B^{-1}, $k = a_2$ implies $N''_{a_2} \subset (D_B(N'_{a_2}) \smallsetminus D_B(N_1))$. This last inclusion proves that $\beta'_{1,a_2}(B) \geqslant \beta_{a_2}(B^{-1})$.

We consider now three sub-sub-cases:

- If $\beta_{a_2}(B) \leqslant \beta_{a_2}(B^{-1})$ then $\min\{\beta_{a_2}(B), \beta'_{1,a_2}(B), \beta_{a_2}(B^{-1})\} = \beta_{a_2}(B)$ which means that we are in the mixed case 1 for B.
- If we have $\beta_{a_2}(B) > \beta_{a_2}(B^{-1})$ and $\beta_{a_2}(B^{-1}) \leqslant \beta'_{1,a_2}(B^{-1})$, we have: $\min\{\beta_{a_2}(B), \beta'_{1,a_2}(B^{-1}), \beta_{a_2}(B^{-1})\} = \beta_{a_2}(B^{-1})$ and we are in the mixed case 1 for B^{-1}.
- Finally, if $\beta_{a_2}(B) > \beta_{a_2}(B^{-1})$ and $\beta_{a_2}(B^{-1}) > \beta'_{1,a_2}(B^{-1})$, we have: $\beta'_{1,a_2}(B) > \beta_{1,a_2}(B^{-1})$.
  Therefore the inequality: $\beta_{a_2}(B) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B) \leqslant \lambda_1(B) + \beta_1(B)$ proves that the other inequality holds too: $\beta_{a_2}(B) + \lambda_{a_2}(B) + \beta'_{1,a_2}(B^{-1}) < \lambda_1(B) + \beta_1(B)$, and consequently we have: $\beta'_{1,a_2}(B^{-1}) \geqslant \beta_{a_2}(B)$, which is a contradiction, this case is thus impossible.

What concluded the proof. □

6. Applications to the function $\mu_G(r, s)$

In [9], the authors ask if for any finite group G, the following equality holds:

$$\mu_G(r,s) = \min_{H \leqslant G} \left\{ \left(\left\lceil \frac{r}{|H|} \right\rceil + \left\lceil \frac{s}{|H|} \right\rceil - 1 \right) |H| \right\}.$$

The next two subsections show that this is not true in general.

6.1. **An application to solvable groups.**

Let us consider two odd prime numbers p and q, such that $q \equiv 1 \pmod{p}$, and the semidirect product $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. We recall that this semidirect product is unique up to a unique isomorphism. We also recall that such a semidirect product contains a unique subgroup of cardinality q that is therefore normal. This results are proved in [18], chapter I.6. It is obviously a solvable group:

$$\{0\} \triangleleft (\mathbb{Z}/q\mathbb{Z}) \triangleleft (\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}).$$

The fact, that for a given prime number p there are infinitely many primes q such that $q \equiv 1 \pmod{p}$, is a weak version of Dirichlet's Theorem, that can be proved by elementary arguments. Consequently there are infinitely many such groups $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ with p and q both odd prime and $q \equiv 1 \pmod{p}$.

Proposition 22. *Let p and q be two odd prime numbers such that $q \equiv 1 \pmod{p}$, then in the group $G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$, we have:*

$$\mu_G(q+p-1, q-1) = 2q,$$

$$\text{and } \min_{H \leqslant G} \left\{ \left(\left\lceil \frac{q+p-1}{|H|} \right\rceil + \left\lceil \frac{q-1}{|H|} \right\rceil - 1 \right) |H| \right\} = 2q-2.$$

Proof. The subgroups of G have a cardinality belonging to $\{1, p, q, pq\}$, therefore the minimum in the second equality is

$$\min_{d \in \{1,p,q,pq\}} \left\{ \left(\left\lceil \frac{q+p-1}{d} \right\rceil + \left\lceil \frac{q-1}{d} \right\rceil - 1 \right) d \right\}.$$

These four values can easily be computed thanks to the fact that p divides $q-1$, thus the minimum is the minimum of $\{2q+p-3, 2q-2, 2q, pq\}$, that is $2q-2$.

We now want to prove that $\mu_G(q+p-1, q-1) = 2q$. In order to do this, we establish with two opposite inequalities that $\mu_G(q+p-1, q-1)$ is lower and greater than $2q$.

First inequality: $\mu_G(q+p-1, q-1) \leqslant 2q$**.**

To prove this inequality, it is enough to exhibit a couple (A, B) such that $|A| = q+p-1$, $|B| = q-1$ and $|A.B| = 2q$.

In the semidirect product G, we denote H_q the unique subgroup of cardinality q. Let us consider a subset B of H_q of cardinality $q-1$, and for any $a \notin H_q$, a subset A of $H_q \cup a.H_q$ of cardinality $p+q-1$. It follows that the product $A.B$ is a subset of $(H_q \cup a.H_q).H_q = H_q \cup a.H_q$ of cardinality $2q$. A simple application of the pigeonhole principle shows that both cosets H_q and $a.H_q$ contain at least 2 elements from A. Thus by the prehistorical lemma $(A \cap H_q).B = H_q$ and $(A \cap a.H_q) = a.H_q$. Then we have $A.B = H_q \cup a.H_q$, and $|A.B| = 2q$.

Second inequality: $\mu_G(q+p-1, q-1) \geqslant 2q$**.**

Imagine that A', B' are such that $|A'| = q+p-1$, $|B'| = q-1$ and $|A'.B'| < 2q$. Then we have $|A'.B'| - |A'| < q-p+1 \leqslant |B'| - 1 = q-2$. It follows from corollary 9 that there exists a proper subgroup N_1 that is a 1-kernel for B' or B'^{-1} and such that $\lambda_1(B') = \left(\left\lceil \frac{q-1}{|N_1|} \right\rceil - 1\right)|N_1| < q-p+1$.

Since we know all the cardinalities of the subgroups of G, we can calculate the possible values of $\lambda_1(B')$. There are only two possibilities for the cardinality of $|N_1|$, either $|N_1| = q$ or $|N_1| = p$.

First case: In the case where $|N_1| = q$, the 1-kernel N_1 is the normal subgroup H_q. Therefore it is a 1-kernel for B' and for B'^{-1}. We have $\lambda_1(B') = \left(\left\lceil \frac{q-1}{q} \right\rceil - 1\right) q = 0$, which means that B' is included in a coset modulo H_q. Thus we can consider A' as the disjoint union $\bigcup_{i=1}^{p} A'_i$ of its intersections with all cosets modulo H_q. Since the cardinality of A' is $p+q-1$, at least two of the sets A'_i are non empty.

Consequently the product $A'.B'$ is the disjoint union $\bigcup_{i=1}^{p} A'_i.B'$. If three of the A'_i are non empty then $A'.B'$ would be of cardinality more than $3|B'| = 3q-3$ which gives a contradiction with $|A'.B'| < 2q$. Thus exactly two of the A'_i are non empty. By the pigeonhole principle, these two sets contain at least two elements each. The two non empty sets $A'_i.B'$ are each a complete coset modulo H_q. This implies that $|A'.B'| = 2q$. This gives a contradiction for this case.

Second case: In the case where $|N_1| = p$, we have $\lambda_1(B') = \left(\left\lceil \frac{q-1}{p} \right\rceil - 1\right) p = q-1-p$. Moreover there cannot be any a_2-cells with $\lambda_{a_2}(B') < |B'|-1$ for the only possible value would be $\lambda_{a_2}(B') = \left(\left\lceil \frac{q-1}{q} \right\rceil - 1\right) q = 0$. The cell $P_B(A')$ is therefore a j-cell with $1 \leqslant j < a_2$.

The subgroup N_1 is a 1-kernel, either for B' or B'^{-1}, we will now show that it can be considered as a 1-kernel for B'.

Indeed, if N_1 is a 1-kernel for B'^{-1}, then $D_{B'}(A')$ is a union of left-cosets modulo N_1. Thus $|D_{B'}(A')|$ is a multiple of p. Since $|D_{B'}(A')| = |G| - |A'.B'| > pq - 2q$, we have:

$$|D_{B'}(A')| \geqslant \left\lceil \frac{pq-2q}{p} \right\rceil p = pq - 2(q-1).$$

But this implies that $|A'.B'| \leqslant 2(q-1)$, and therefore $|A'.B'| - |A'| \leqslant q-1-p = \lambda_1(B')$. Then A' is an 1-cell for B'. Moreover since A' satisfies the condition $E_1(B')$,

any 1-kernel for B' will also satisfy the condition $E_1(B')$ and the 1-kernel for B' that contains 1 will be a subgroup of cardinality p.

We will now consider that N_1 is the 1-kernel for B' that contains 1. Since $|N_1.B'| - |N_1| = q - 1 - p$ and $|B'| = q - 1$, $|N_1| = p$, we deduce that $N_1.B' = B'$.

The group $G = \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$ can be parametrized as $H_q \rtimes N_1$ in the following way: There exists $\alpha \in \mathbb{Z}/q\mathbb{Z}$ of multiplicative order p such that:

$$G = \{(x, y) | x \in \mathbb{Z}/q\mathbb{Z},\ y \in \mathbb{Z}/p\mathbb{Z}\},$$
$$(a, b).(c, d) = (a + c.\alpha^b, b + d)$$

and

$$H_q = \{(x, 0) | x \in \mathbb{Z}/q\mathbb{Z}\},\ N_1 = \{(0, y) | y \in \mathbb{Z}/p\mathbb{Z}\}.$$

Since B' is left-periodic modulo N_1, it is completely determined by a set $B_0 \subset \mathbb{Z}/q\mathbb{Z}$ of cardinality $\frac{q-1}{p}$:

$$B' = \{(b_0.\alpha^x, x) | b_0 \in B_0,\ x \in \mathbb{Z}/p\mathbb{Z}\},$$

(This follows from the product $(0, y).(b_0.\alpha^x, x) = (b_0.\alpha^{x+y}, x + y)$.)

Similarly, we have seen that $P_{B'}(A')$ is a j-cell, with $1 \leqslant j < a_2$, thus it is a right-periodic set modulo N_1. Therefore $|P_{B'}(A')|$ is a multiple of p. Moreover, since we have seen that $|A'.B'| - |A'| < q + 1 - p$ and $\lambda_1(B') = q - 1 - p$, we have $0 \leqslant |P_{B'}(A')| - |A'| < 2$. Since $|A'| = q - 1 + p$ is also a multiple of p, it proves that $|P_{B'}(A')| - |A'| = 0$ and that $P_{B'}(A') = A'$. Thus A' is completely determined by a set $A_0 \subset \mathbb{Z}/q\mathbb{Z}$ of cardinality $\frac{q-1}{p} + 1$:

$$A' = \{(a_0, x) | a_0 \in A_0,\ x \in \mathbb{Z}/p\mathbb{Z}\}.$$

In these conditions, we can compute the product:

$$\begin{aligned} A'.B' &= \left\{(a_0, x).(b_0.\alpha^y, y) | a_0 \in A_0,\ b_0 \in B_0,\ (x, y) \in (\mathbb{Z}/p\mathbb{Z})^2\right\} \\ &= \left\{(a_0 + b_0.\alpha^{x+y}, x + y) | a_0 \in A_0,\ b_0 \in B_0,\ (x, y) \in (\mathbb{Z}/p\mathbb{Z})^2\right\} \\ &= \{(s, x) | x \in \mathbb{Z}/p\mathbb{Z},\ s \in (A_0 + B_0.\alpha^x)\}. \end{aligned}$$

From Cauchy-Davenport Theorem [3, 4, 5], for any $x \in \mathbb{Z}/p\mathbb{Z}$, we have $|A_0 + B_0.\alpha^x| \geqslant |A_0| + |B_0| - 1 = 2\frac{q-1}{p}$. If there exist two values x_1 and x_2 from $\mathbb{Z}/p\mathbb{Z}$ such that $|A_0 + B_0.\alpha^{x_1}| > 2\frac{q-1}{p}$ and $|A_0 + B_0.\alpha^{x_2}| > 2\frac{q-1}{p}$, we would have:

$$\begin{aligned} |A'.B'| &= |A_0 + B_0.\alpha^{x_1}| + |A_0 + B_0.\alpha^{x_2}| + \sum_{\substack{x \neq x_1 \\ x \neq x_2}} |A_0 + B_0.\alpha^x| \\ &\geqslant \left(2\frac{q-1}{p} + 1\right) + \left(2\frac{q-1}{p} + 1\right) + (p - 2)\left(2\frac{q-1}{p}\right) \\ &= 2q, \end{aligned}$$

which is a contradiction.

Then at most one value x_0 from $\mathbb{Z}/p\mathbb{Z}$ can give $|A_0 + B_0.\alpha^{x_0}| > 2\frac{q-1}{p}$. And for any $x \in (\mathbb{Z}/p\mathbb{Z} \setminus \{x_0\})$ we have:

$$|A_0 + B_0.\alpha^x| = 2\frac{q-1}{p} = |A_0| + |B_0.\alpha^x| - 1.$$

Then Vosper Theorem [20, 21] asserts that A_0 and $B_0.\alpha^x$ are two arithmetical progressions of same difference.

But it is a well known fact that for an arithmetical progression of length less than $\frac{q-1}{2}$ the difference is uniquely determined up to opposition. Indeed let us consider an arithmetical progression P of first term a and difference r, $\{a + k.r / k \in [0, l-1]\}$

with $l \leqslant \frac{q-1}{2}$. If P is also an arithmetical progression of difference $r' \neq \pm r$, it can also be denoted $\{a' + k.r'/k \in [0, l-1]\}$. Thus there exists two integers i and j in $[0, l-1]$ with $(i,j) \neq (0,1)$ and $(i,j) \neq (l-1, l-2)$ such that $a' = a + i.r$ et $a' + r' = a + j.r$. This gives $r' = (j-i).r$, which implies that there exists in P a term of the form $a + k.r$ with $k \in ([-(l+1), 2l-2] \setminus [0, l-1])$. Since $l \leqslant \frac{q-1}{2}$, such an element cannot be in $\{a + k.r/k \in [0, l-1]\}$.

Let us denote r the difference of the arithmetical progression A_0. It has to be noticed that $r \neq 0$.

Since p is an odd prime number, we can consider x_1 and x_2 different and both different from x_0 in $\mathbb{Z}/p\mathbb{Z}$. The set B_0 is then an arithmetical progression of difference $r.\alpha^{-x_1}$ and also of difference $r.\alpha^{-x_2}$.

If $r.\alpha^{-x_1} = r.\alpha^{-x_2}$, we obtain $\alpha^{x_2 - x_1} = 1$, therefore $x_1 = x_2$ which is a contradiction.

If $r.\alpha^{-x_1} = -r.\alpha^{-x_2}$, we obtain $\alpha^{x_2 - x_1} = -1$, but this implies that the multiplicative order of α is even, and this contradicts the fact that its order is the odd prime p.

This gives a contradiction for this case and concludes the proof. □

Remark 6. *If we consider two subsets A and B such that $|A| = q+p-1$, $|B| = q-1$ and $|A.B| = \mu_G(q+p-1, q-1) = 2q$. It is possible to prove that B is a subset of cardinality $q-1$ of a coset $H_q.b$, and A is a subset of cardinality $p+q-1$ of $H_q \cup a.H_q$ for some $a \notin H_q$. To prove this it suffices to consider the equality case in the proof of the second inequality. This solves the associated inverse problem.*

Remark 7. *Exactly the same arguments and computations show that for two integers x and y such that $1 \leqslant x < y \leqslant p-1$, we have:*

$$\mu_G(q-x, q+y) = 2q,$$

$$\text{and } \min_{H \leqslant G} \left\{ \left(\left\lceil \frac{q-x}{|H|} \right\rceil + \left\lceil \frac{q+y}{|H|} \right\rceil - 1 \right) |H| \right\} = 2q - 2.$$

Remark 8. *The fact that p is odd, is crucial in the argument. For groups of the type $\mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, it is possible to construct two sets A' and B' such that $|A'| = q-1$, $|B'| = q+1$ and $|A'.B'| = |A'| + |B'| - 2 = 2q - 2$. This can also be done for other even values of $|A'|$ and $|B'|$ and gives a proof that in these groups, we have:*

$$\mu_G(r,s) = \min_{H \leqslant G} \left(\left\lceil \frac{r}{|H|} \right\rceil + \left\lceil \frac{s}{|H|} \right\rceil - 1 \right) |H|.$$

6.2. **An application to symmetric groups.** In the symmetric groups $\mathfrak{A}_n$, with $n \leqslant 4$, the values of the function $\mu_{\mathfrak{A}_n}$ have been computed in [9] and we have the equality:

$$\mu_G(r,s) = \min_{H \leqslant \mathfrak{A}_n} \left\{ \left(\left\lceil \frac{r}{|H|} \right\rceil + \left\lceil \frac{s}{|H|} \right\rceil - 1 \right) |H| \right\}.$$

Nevertheless, this result is certainly not true in general symmetric groups. We may apply the method developed in this article to symmetric groups $\mathfrak{A}_n$, with $n \geqslant 9$. For this purpose, we will need the following corollary of theorem 5.2*A* of [7]:

Corollary 23. *In $\mathfrak{A}_n$, with $n \geqslant 9$, if H is a proper subgroup of $\mathfrak{A}_n$ of index strictly less than $\frac{n(n-1)}{2}$, then there exists $i \in \{1..n\}$ such that H is the stabilizer of i, (and then H has cardinality $\frac{(n-1)!}{2}$ and index n).*

Here is our result:

Proposition 24. *In the alternate group $\mathfrak{A}_n$, with $n \geqslant 9$, we have:*

$$\mu_{\mathfrak{A}_n}((n-1)!, (n-1)!) = 2(n-1)! - (n-2)!,$$

$$\textit{and } \min_{H \leqslant \mathfrak{A}_n} \left\{ \left(\left\lceil \frac{(n-1)!}{|H|} \right\rceil + \left\lceil \frac{(n-1)!}{|H|} \right\rceil - 1 \right) |H| \right\} = \frac{3}{2}(n-1)!.$$

Proof. The second equality is just a numeric one, that requires only to know the maximal cardinality of the subgroups of $\mathfrak{A}_n$. It is an application of the corollary 23.Indeed, for every proper subgroup H of $\mathfrak{A}_n$, we have: $\left\lceil \frac{(n-1)!}{|H|} \right\rceil |H| \geqslant (n-1)!$. Therefore, we have:

$$\begin{aligned} \min_{H < \mathfrak{A}_n} \left\{ \left(\left\lceil \frac{(n-1)!}{|H|} \right\rceil + \left\lceil \frac{(n-1)!}{|H|} \right\rceil - 1 \right) |H| \right\} &\geqslant 2(n-1)! - \sup_{H < \mathfrak{A}_n} |H| \\ &= 2(n-1)! - \frac{(n-1)!}{2} \\ &= 3\frac{(n-1)!}{2}. \end{aligned}$$

We notice that this inequality is an equality, by considering a proper subgroup of maximal cardinality, thanks to the fact that $\frac{(n-1)!}{2}$ divides $(n-1)!$.

We want now to prove that $\mu_{\mathfrak{A}_n}((n-1)!, (n-1)!) = 2(n-1)! - (n-2)!$. In order to do this, we establish with two opposite inequalities that $\mu_{\mathfrak{A}_n}((n-1)!, (n-1)!)$ is lower and greater than $2(n-1)! - (n-2)!$.

First inequality: $\mu_{\mathfrak{A}_n}((n-1)!, (n-1)!) \leqslant 2(n-1)! - (n-2)!$**.**

It is enough to build a couple (A, B) such that $|A| = |B| = (n-1)!$ and $|A.B| = 2(n-1)! - (n-2)!$.

Let us consider the proper subgroup H isomorphic to $\mathfrak{A}_{n-1}$ stabilizer of n and the sets $A = H \cup a.H$ and $B = H \cup H.b$, with $a \notin H$ and $b \notin H$. So, we have $|H| = \frac{(n-1)!}{2}$ and $|A| = |B| = (n-1)!$.

We can characterize the elements from A by $\sigma \in A$ if and only if $\sigma(n) = a(n) \neq n$ or $\sigma(n) = n$, and the elements from B by $\sigma \in B$ if and only if $\sigma^{-1}(n) = b^{-1}(n) \neq n$ or $\sigma^{-1}(n) = n$.

We can now determine the product $A.B = H \cup a.H \cup H.b \cup a.H.b$. Since we have $H \cap a.H = \emptyset$, $H \cap H.b = \emptyset$, $a.H \cap a.H.b = \emptyset$ and $H.b \cap a.H.b = \emptyset$, the only possible non-empty intersections are $H \cap a.H.b$ and $a.H \cap H.b$.

To determine the cardinality of these intersections, we see that $\sigma \in H \cap a.H.b$ is equivalent to $\sigma(n) = n$ and $\sigma(b^{-1}(n)) = a(n)$.

- In the case where $a(n) = b^{-1}(n)$, this two equalities are $\sigma(n) = n$ and $\sigma(a(n)) = a(n)$. Since $a(n) \neq n$, there is exactly $\frac{(n-2)!}{2}$ even permutations that fulfill these conditions.
- In the case where $a(n) \neq b^{-1}(n)$, this two equalities are equivalent to $\Big(\sigma \circ \big(a(n), b^{-1}(n)\big)\Big)(n) = n$ and $\Big(\sigma \circ \big(a(n), b^{-1}(n)\big)\Big)(a(n)) = a(n)$. Since $a(n) \neq n$, there is exactly $\frac{(n-2)!}{2}$ odd permutations $\Big(\sigma \circ \big(a(n), b^{-1}(n)\big)\Big)$ that fulfill these conditions, so there is exactly $\frac{(n-2)!}{2}$ even permutations $\sigma \in H \cap a.H.b$.

Thus we have $|H \cap a.H.b| = \frac{(n-2)!}{2}$. Similarly, $\sigma \in a.H \cap H.b$ is equivalent to $\sigma(n) = a(n)$ and $\sigma^{-1}(n) = b^{-1}(n)$. Exactly $\frac{(n-2)!}{2}$ even permutations fulfill these conditions, therefore $|a.H \cap H.b| = \frac{(n-2)!}{2}$. We deduce from this that $|A.B| = 2(n-1)! - (n-2)!$.

We now show that this product is of minimal size.

Second inequality: $\mu_{\mathfrak{A}_n}((n-1)!, (n-1)!) \geqslant 2(n-1)! - (n-2)!$**.**

Suppose that we have a couple (A', B') of subsets of $\mathfrak{A}_n$, with $|A'| = |B'| = (n-1)!$ and $|A'.B'| < 2(n-1)! - (n-2)!$. Then we have $|A'.B'| - |A'| < (n-1)! - (n-2)!$,

which is strictly less than $|B'|-1=(n-1)!-1$. For all subgroups of $\mathfrak{A}_n$, we can compute the potential values of $\lambda_i(B')<|B'|-1$, because there exists a subgroup H such that $\lambda_i(B')=\left(\left\lceil\frac{|B'|}{|H|}\right\rceil-1\right)|H|$, for $i=1$ and $i=a_2$ by corollary 9 and theorem 21.

But the inequality $\lambda_i(B')\leqslant|A'.B'|-|A'|$ implies $|H|>(n-2)!$ therefore H has index strictly less than $\frac{n(n-1)}{2}$. Then corollary 23 proves that only one of these values is non zero and less than $(n-1)!-(n-2)!$. This value is given by $|H|=\frac{(n-1)!}{2}$. Therefore only a subgroup of cardinality $\frac{(n-1)!}{2}$ can be a 1-kernel for B' or B'^{-1} and we have $\lambda_1(B')=\frac{(n-1)!}{2}$. Moreover, necessarily $\lambda_{a_2}(B')\geqslant(n-1)!-(n-2)!$, then the i-cell $P_{B'}(A')$ is such that $1\leqslant i<a_2$.

- If $\beta_1(B')\geqslant\beta_1(B'^{-1})$, the 1-kernel for B' that contains 1 is a subgroup H and $|H.B'|-|H|=\frac{(n-1)!}{2}$ implies that B' is in the type $B'=H.b_1\cup H.b_2$, with $b_2.b_1^{-1}\notin H$.

  Since $P_{B'}(A')$ is a i-cell with $\lambda_i(B')$ less to all potential values of $\lambda_{a_2}(B')$, $P_{B'}(A')$ is a union of left-cosets modulo H.

  If $P_{B'}(A')\neq A'$, then $|P_{B'}(A')|\geqslant 3\frac{(n-1)!}{2}$ and consequently

$$\begin{aligned}|P_{B'}(A').B'|-|P_{B'}(A')| &= |A'.B'|-|P_{B'}(A')|\\ &< 2(n-1)!-(n-2)!-3\frac{(n-1)!}{2}\\ &= \frac{(n-1)!}{2}-(n-2)!\\ &< \lambda_1(B'),\end{aligned}$$

  which is impossible. Therefore $P_{B'}(A')=A'$ and A' is in the type $A'=a_1.H\cup a_2.H$, with $a_1.a_2^{-1}\notin H$. Thus we have two sets A' and B' of the previous types. Finally we have $|A'.B'|=2(n-1)!-(n-2)!$, which is a contradiction.
- If $\beta_1(B')>\beta_1(B'^{-1})$, the 1-kernel for B'^{-1} that contains 1 is a subgroup H and $|H.B'^{-1}|-|H|=\frac{(n-1)!}{2}$. The i-cell $D_{B'}(A')$ for B'^{-1} with $1\leqslant i<a_2$ is then a union of left-cosets modulo H. Moreover:

$$\begin{aligned}|D_{B'}(A')| &= \frac{n!}{2}-|A'.B'|\\ &> \frac{n!}{2}-2(n-1)!+(n-2)!\\ &= \frac{(n-1)!}{2}\left(n-4+\frac{2}{n-1}\right).\end{aligned}$$

  Since $D_{B'}(A')$ is a union of left-cosets modulo H, its cardinality is a multiple of $\frac{(n-1)!}{2}$. Thus we have: $|D_{B'}(A')|\geqslant\frac{(n-1)!}{2}(n-3)$. Consequently we can give a upper bound for the size of its complement, the product $|A'.B'|\leqslant 3\frac{(n-1)!}{2}$, which gives $|A'.B'|-|A'|\leqslant\frac{(n-1)!}{2}$. It means that A' is a 1-cell for B'.

  Thus we have $\beta_1(B')\leqslant|A'|=(n-1)!$ and $\beta_1(B')$ is a strict multiple of $\beta_1(B'^{-1})=\frac{(n-1)!}{2}$. Therefore $\beta_1(B')=|A'|=(n-1)!$ and A' is a 1-kernel for B'. We can easily check that A' satisfies the condition $E_1(B')$, because $|\mathfrak{A}_n\smallsetminus A'|=(n-2)\frac{(n-1)!}{2}$, $\beta_1(B')+\lambda_1(B')=3\frac{(n-1)!}{2}$ and $n>4$. Thus by theorem 8, the 1-kernel that contains 1 is a subgroup of $\mathfrak{A}_n$. But corollary 23 asserts that there is no subgroup of this cardinality. It gives a contradiction and there are no such sets as A' and B' in this situation.

□

Remark 9. *Theorem* 5.2*A of* [7] *gives also a more complicated structural result for the symmetric groups* $\mathfrak{A}_n$ *with* $5 \leqslant n \leqslant 8$. *This can be used to prove similarly that:*

$$\mu_{\mathfrak{A}_5}(4!, 4!) = 2.4! - 3! = 42 \text{ and } \mu_{\mathfrak{A}_7}(6!, 6!) = 2.6! - 5! = 1320.$$

These values give also a contradiction with conjecture 2, since:

$$\min_{H \leqslant \mathfrak{A}_5} \left\{ \left(\left\lceil \frac{4!}{|H|} \right\rceil + \left\lceil \frac{4!}{|H|} \right\rceil - 1 \right) |H| \right\} = \frac{3}{2} 4! = 36,$$

$$\min_{H \leqslant \mathfrak{A}_7} \left\{ \left(\left\lceil \frac{6!}{|H|} \right\rceil + \left\lceil \frac{6!}{|H|} \right\rceil - 1 \right) |H| \right\} = \frac{3}{2} 6! = 1080.$$

Remark 10. *If we consider two subsets* A *and* B *such that* $|A| = |B| = (n-1)!$ *and* $|A.B| = \mu_G((n-1)!, (n-1)!) = 2(n-1)! - (n-2)!$. *It is possible to prove that* $A = a_1.H \cup a_2.H$ *with* $a_1.a_2^{-1} \notin H$ *and* $B = H.b_1 \cup H.b_2$, *with* $b_2.b_1^{-1} \notin H$, *where* H *is a subgroup isomorphic to* $\mathfrak{A}_{n-1}$. *To prove this it suffices to consider the equality case in the proof of the second inequality. Some other cases have to be excluded. This solves the associated inverse problem.*

Remark 11. *In the previous case, the set* B *is also right-periodic modulo the subgroup* $H' = \left\{ \sigma \in \mathfrak{A}_n | \{\sigma(n), \sigma(b^{-1}(n))\} = \{n, b^{-1}(n)\} \right\}$ *of cardinality* $(n-2)!$. *This subgroup is then also a* a_2*-kernel for* B^{-1}. *However, when* n *is an even number,* $(n-2)!$ *does not divide* $\frac{(n-1)!}{2}$, *therefore* $\beta_{a_2}(B^{-1})$ *does not divide* $\beta_1(B)$.

References

[1] E. Balandraud, *Un nouveau point de vue isopérimétrique appliqué au théorème de Kneser*, submitted for publication.
[2] B. Bollobás, I. Leader, *Sums in the grid*, Discrete Math. **162** (1996), 31-48.
[3] A. Cauchy, *Recherches sur les nombres*, J. Ecole Polytech. **9** (1813), 99-116.
[4] H. Davenport, *On the addition of residue classes*, J. Lond. Math. Soc. **10** (1935), 30-32.
[5] H. Davenport, *A historical note*, J. Lond. Math. Soc. **22** (1947), 100-101.
[6] G. T. Diderrich, *On Kneser's addition theorem in groups*, Proc. Amer. Math. Soc. **38** (1973), 443-451.
[7] J.D. Dixon, B. Mortimer, *Permutation groups*, GTM **163**, Springer-Verlag, 1996.
[8] S. Eliahou, M. Kervaire, *Sumsets in vector spaces over finite fields*, J. Number Theory **71** (1998), 12-39.
[9] S. Eliahou, M. Kervaire, A. Plagne, *Optimally small sumsets in finite abelian groups*, J. Number Theory **101** (2003), 338-348.
[10] J. L. Gross, J. Yellen (Éditors), *Handbook of Graph Theory*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, 2004.
[11] Y. ould Hamidoune, *Sur les atomes d'un graphe orienté*, C.R. Acad. Sci. Paris **284** (1977), 1253-1256.
[12] Y. ould Hamidoune, *On the connectivity of Cayley digraphs*, Europ. J. Combin. **5** (1984), 309-312.
[13] Y. ould Hamidoune, *On a subgroup contained in some words with a bounded length*, Discrete Math. **103**(1992), 171-176.
[14] Y. ould Hamidoune, *An isoperimetric method in additive Theory*, J. Algebra **179** (1996), 622-630.
[15] Y. ould Hamidoune, *Subsets with small sums in abelian groups I: the Vosper property*, Europ. J. of Combinatorics **18** (1997), 541-556.
[16] Y. ould Hamidoune, *Some results in additive number theory I: the critical pair theory*, Acta arith. **96.2** (2000), 97-119.
[17] J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. **103** (1960), 63-88.
[18] D. Perrin, *Cours d'algèbre*, Ellipses, Paris (1996).
[19] A. Plagne, *Additive number theory sheds extra light on the Hopf-Stiefel* $\circ$ *fonction*, L'enseignement Math. **49** (2003), 109-116.
[20] G. Vosper, *The critical pairs of subsets of a group of prime order*, J. Lond. Math. Soc. **31** (1956), 200-205.
[21] G. Vosper, *Addendum to "The critical pairs of subsets of a group of prime order"*, J. Lond. Math. Soc. **31** (1956), 280-282.
[22] S. Yuzvinsky, *Orthogonal pairings of Euclidean spaces*, Michigan Math. J. **28** (1981), 109-119.

[23] G. Zémor, *A generalisation to noncommutative groups of a theorem of Mann*, Discrete Math. **126** (1994), 365-372.

Éric Balandraud, A2X, 351 cours de la Libération, 33405 TALENCE
E-mail address: eric.balandraud@math.u-bordeaux1.fr, eric.balandraud@math.polytechnique.fr

COMPLÉMENT À "THE ISOPERIMETRIC METHOD IN NON-ABELIAN GROUPS WITH AN APPLICATION TO OPTIMALLY SMALL SUMSETS"

Nous allons ici développer un point concernant l'article "*The Isoperimetric Method in non-abelian groups with an application to optimally small sumsets*". Dans la section 4.3 de cet article, il est affirmé que pour G un groupe fini et B un sous-ensemble de G, si aucune 1-cellule pour B ne vérifie la condition $E_1(B)$, alors le dual d'un 1-noyau est une classe à gauche modulo un sous-groupe de G. Ce complément en donne la preuve. La numérotation reprend celle de l'article.

7. Structure d'une 1-cellule maximale lorsque un noyau pour B^{-1} ne vérifie pas $E_1(B^{-1})$

Proposition 25. *Soit G un groupe fini et B un sous-ensemble non vide de G. Soit M_1 une 1-cellule pour B de taille maximale. Si $D_B(M_1)$ ne vérifie pas la condition $E_1(B^{-1})$, alors pour toute 1-cellule C_1 pour B, si $M_1 \cap C_1 \neq \emptyset$ alors $C_1 \subset M_1$.*

Démonstration. Comme M_1 est une 1-cellule pour B de taille maximale, $D_B(M_1)$ est un 1-noyau pour B^{-1}. Ainsi, on a $|D_B(M_1)| = \beta_1(B^{-1})$. Que le 1-noyau $D_B(M_1)$ ne vérifie pas la condition $E_1(B^{-1})$ signifie que:

$$|G \smallsetminus D_B(M_1)| < \lambda_1(B^{-1}) + \beta_1(B^{-1}).$$

Ce que l'on peut récrire: $|G| - \beta_1(B^{-1}) < \lambda_1(B^{-1}) + \beta_1(B^{-1})$, soit $|G| < \lambda_1(B^{-1}) + 2\beta_1(B^{-1})$.

On en déduit que $2|M_1| + \lambda_1(B) < |G|$, en effet:

$$\begin{aligned} 2|M_1| + \lambda_1(B) &= 2(|G| - \lambda_1(B) - \beta_1(B^{-1})) + \lambda_1(B) \\ &= 2|G| - \lambda_1(B) - 2\beta_1(B^{-1}) \\ &= |G| + (|G| - \lambda_1(B) - 2\beta_1(B^{-1})) \\ &< |G|. \end{aligned}$$

On a alors nécessairement $|M_1| < \beta_1(B^{-1})$.

Ainsi si l'on considère une 1-cellule pour B, C_1 telle que $M_1 \cap C_1 \neq \emptyset$, on a aussi $|C_1| < \beta_1(B^{-1})$. De plus, $M_1 \cap C_1$ est une k-cellule avec $k \geqslant 1$. Ainsi d'après le lemme 7, on a $|D_B(M_1) \smallsetminus D_B(C_1)| \leqslant |C_1 \smallsetminus M_1|$.

Ainsi, on a:

$$\begin{aligned} |D_B(M_1) \cap D_B(C_1)| &= |D_B(M_1)| - |D_B(M_1) \smallsetminus D_B(C_1)| \\ &\geqslant |C_1| - |C_1 \smallsetminus M_1| \\ &= |C_1 \cap M_1| > 0. \end{aligned}$$

Ce qui impose que $P_B(D_B(M_1) \cup D_B(C_1))$ est une l-cellule avec $l \geqslant 1$.

Or le corollaire 6 affirme que:

$$\lambda_k(B) + \lambda_l(B) \leqslant \lambda_1(B) + \lambda_1(B).$$

Ainsi, on a $k = l = 1$. En particulier, $l = 1$ impose que $C_1 \subset M_1$, car M_1 est une 1-cellule de taille maximale. □

Corollaire 26. *Soit G un groupe fini et B un sous-ensemble non vide de G. Soit M_1 une 1-cellule pour B de taille maximale contenant 1. Alors M_1 est un sous-groupe de G.*

Démonstration. En effet, pour tout $x \in M_1$, les deux 1-cellules M_1 et $x^{-1}.M_1$ contiennent toutes les deux 1. Ainsi $M_1 \cap (x^{-1}.M_1) \neq \emptyset$, donc d'après le lemme précédent, on a $M_1 \subset x^{-1}.M_1$ et par cardinalité $M_1 = x^{-1}.M_1$. Ainsi M_1 est un sous-groupe de G.

□