Le principe d'incertitude en combinatoire additive

Emma Weschler
Mémoire de Master 2 Mathématiques Fondamentales, Sorbonne Université

29 septembre 2023

Encadrante du stage : Gautami Bhowmik
Référent universitaire : Régis de La Brétèche

Table des matières

1 Remerciements **1**

2 Introduction **1**

3 Principe d'incertitude de Donoho et Stark et principe d'incertitude linéaire **3**

3.1 Transformée de Fourier sur les groupes abéliens finis 3

3.1.1 Premières définitions et principe d'incertitude de Donoho et Stark . 3

3.1.2 Principe d'incertitude sur $\mathbb{Z}/p\mathbb{Z}$ 10

3.2 Le théorème de Cauchy-Davenport 15

4 Des principes d'incertitudes sur un groupe abélien fini **16**

4.1 Un principe d'incertitude linéaire sur les groupes abéliens finis 16

4.1.1 Lemmes intermédiaires 18

4.1.2 Preuve du principe d'incertitude linéaire sur un groupe abélien fini . . 24

4.2 Un principe d'incertitude sur $(\mathbb{Z}/k\mathbb{Z})^n$ 25

4.2.1 Le principe d'incertitude 26

4.2.2 Une application pour la constante de Davenport 30

5 Généralisation du premier principe d'incertitude pour les groupes non abéliens, cas du groupe non abélien à pq éléments **33**

5.1 Définitions généralisées 33

5.2 Généralisation du premier principe d'incertitude 38

5.3 Cas du groupe non abélien à pq éléments 45

A Différentes démonstrations du théorème de Chebotarev **61**

A.1 La preuve de Tao 61

A.2 La preuve de Frenkel 62

A.3 La preuve de Chebotarev 67

B Preuve du théorème de Cauchy-Davenport par la transformée de Dyson **73**

1 Remerciements

Je tiens tout d'abord à remercier Gautami Bhowmik pour son encadrement bienveillant pour ce mémoire. Elle m'a été de bons conseils, sur le plan mathématique et humain.

Merci également au laboratoire Paul Painlevé de m'avoir accueillie à Lille très régulièrement. J'ai pu y découvrir notamment lors de la conférence Arithmétique en Plat Pays en juin 2023 des chercheurs et chercheuses passionné.e.s par leurs sujets d'étude.

Je remercie particulièrement la Fondation Sciences Mathématiques de Paris pour leur bourse pour mon mémoire de Master hors Île-de-France. Cette dernière m'a permise de voyager à Lille sereinement.

Enfin, je tiens à remercier mon compagnon, qui m'accompagne dans toutes les épreuves de ma vie. Tu as su écouter mes joies et mes frustrations pendant ces six mois à me consacrer à ce mémoire.

2 Introduction

En physique quantique, on vulgarise souvent le principe d'incertitude d'Heisenberg en affirmant qu'il est impossible de connaître simultanément et avec exactitude la vitesse et la position d'une particule. En effet, ces quantités sont liées par l'inégalité :

$$\sigma_x \sigma_v \geq \frac{\hbar}{2m},$$

où σ_x et σ_v représentent respectivement l'incertitude sur la position et sur la vitesse. Plus la position d'une particule est connue avec certitude, plus la quantité σ_x se rapproche de 0 et donc plus σ_v, l'incertitude sur la vitesse, augmente. Du fait de la dualité onde-corpuscule, ces propriétés physiques des particules peuvent être représentées par des fonctions d'ondes qui sont la transformée de Fourier l'une de l'autre. Ainsi, quand on parle de principe d'incertitude en mathématiques, on fait référence au fait qu'une fonction et sa transformée de Fourier ne peuvent être toutes deux concentrées en un endroit. Nous nous intéressons dans ce rapport à

une catégorie très particulière de principe d'incertitude : celle issue de la théorie de Fourier discrète. En effet, de manière analogue au cas continu, nous définissons une transformée de Fourier sur un groupe abélien fini, et plus loin dans le rapport nous généraliserons sa définition pour un groupe fini non abélien. Historiquement, Donoho et Stark [3] découvrirent un des premiers principes d'incertitude pour une fonction $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$, avec n est un entier naturel non nul :

$$|\text{supp}(f)||\text{supp}(\widehat{f})| \geq n,$$

et où $\text{supp}(f)$ désigne les éléments de $\mathbb{Z}/n\mathbb{Z}$ où f est non nulle. Tao a montré dans [15] une amélioration significative dans le cas où le groupe est $\mathbb{Z}/p\mathbb{Z}$ avec p premier. En effet, dans ce cas, Tao montre un principe d'incertitude non pas multiplicatif mais additif :

$$|\text{supp}(f)| + |\text{supp}(\widehat{f})| \geq p + 1,$$

pour toute fonction $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$. La clef de la démonstration de Tao est le théorème de Chebotarev. Ce dernier affirme que tous les mineurs de $(\omega^{ij})_{i,j\in\mathbb{Z}/p\mathbb{Z}}$ sont non nuls, pour p premier et ω une racine p-ième de l'unité, cette matrice étant la matrice de la transformation de Fourier dans certaines bases. Par la suite, Ram Murty et Peter Whang [10] démontrent une généralisation de ce théorème permettant une amélioration du principe d'incertitude pour certaines fonctions définies sur $\mathbb{Z}/m\mathbb{Z}$, pour un m quelconque. D'autres principes d'incertitude ont également vu le jour, comme par exemple la généralisation du principe d'incertitude de Tao à un groupe abélien fini quelconque par Meshulam [9].

Les principes d'incertitudes dans la théorie de Fourier discrètes connaissent des applications en combinatoire additive. Nous détaillerons dans ce rapport la nouvelle démonstration de Tao du théorème de Cauchy-Davenport, mais également comment l'analyse de Fourier discrète a permis à Meshulam [7] de donner une autre preuve d'une certaine majoration de la constante de Davenport. Cette dernière majoration a notamment permis de montrer qu'il existe une infinité de nombres de Carmichael [1].

Enfin, nous verrons une généralisation aux groupes non abéliens du principe d'incertitude de Donoho et Stark, la démonstration étant bien plus fastidieuse et complexe que dans

le cas où le groupe est abélien. Meshulam [8] donne également un exemple d'un autre principe d'incertitude pour le groupe non abélien à pq éléments, où p et q sont des nombres premiers vérifiant que p divise $q-1$.

3 Principe d'incertitude de Donoho et Stark et principe d'incertitude linéaire

3.1 Transformée de Fourier sur les groupes abéliens finis

3.1.1 Premières définitions et principe d'incertitude de Donoho et Stark

Soit G un groupe abélien fini. Afin de définir la transformée de Fourier d'une fonction de G dans $\mathbb{C}$, commençons par quelques rappels sur les caractères d'un groupe abélien fini. En effet, ces derniers forment une base orthonormale des fonctions de G dans $\mathbb{C}$ pour un certain produit scalaire, permettant d'avoir, comme dans le cas continu, une formule d'inversion de Fourier.

Définition 3.1.1.1 (Caractère)**.** *On appelle caractère de G un morphisme $\chi : G \to \mathbb{C}^*$. On note $\widehat{G}$ l'ensemble des caractères de G. Cet ensemble forme un groupe pour la multiplication.*

La proposition suivante donne une description des caractères d'un groupe cyclique.

Proposition 3.1.1.2 (Description des caractères d'un groupe cyclique)**.**

— *Soit $n \geq 2$ un entier. Le groupe des caractères de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au groupe U_n des racines n-ième de l'unité via l'application $\chi \mapsto \chi(1)$. Autrement dit :*

$$\forall \zeta \in U_n, \forall \chi \in \widehat{\mathbb{Z}/n\mathbb{Z}},\ \exists! k \in [\![0, p-1]\!], \chi(\cdot) = \zeta^{k\cdot}.$$

— *De plus, si $m \in \mathbb{N}^*$, $\widehat{(\mathbb{Z}/n\mathbb{Z})^m}$ est isomorphisme à $(\mathbb{Z}/n\mathbb{Z})^m$. Autrement dit :*

$$\forall \zeta \in U_n, \forall \chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^m},\ \exists! k \in [\![0, n-1]\!], \chi(\cdot) = \zeta^{k\cdot},$$

où . désigne le produit scalaire usuel de $(\mathbb{Z}/n\mathbb{Z})^m$.

— *Soit p premier. Les groupes* $\mathbb{Z}/p\mathbb{Z}$ *et* U_p *sont isomorphes de manière canonique par le morphisme qui envoie* 1 *sur* $e^{2i\pi/p}$*, et donc* $\widehat{\mathbb{Z}/p\mathbb{Z}}$ *est également isomorphe de manière canonique à* $\mathbb{Z}/p\mathbb{Z}$*. Autrement dit :*

$$\forall \chi \in \widehat{\mathbb{Z}/p\mathbb{Z}},\ \exists! k \in [\![0, p-1]\!], \chi(\cdot) = e^{2i\pi k \cdot /p}$$

.

Définition 3.1.1.3 (Transformée de Fourier)**.** *Soit* $f : G \to \mathbb{C}$*. On appelle transformée de Fourier discrète de* f *la fonction :*

$$\begin{aligned} \widehat{f} \colon \widehat{G} &\longrightarrow \mathbb{C} \\ \chi &\longmapsto \sum_{x \in G} f(x)\chi(-x) \end{aligned}$$

Remarque. *Cette définition est à mettre en parallèle avec celle de la transformée de Fourier continue. En effet, pour* $f : \mathbb{R} \to \mathbb{R}$ *intégrable sur* $\mathbb{R}$*, on définit la transformée de Fourier de* f *comme la fonction :*

$$\begin{aligned} \widehat{f} : \mathbb{R} &\longrightarrow \mathbb{R} \\ \xi &\longmapsto \int_{\mathbb{R}} f(x)e^{-i\xi x}. \end{aligned}$$

Cependant, contrairement au cas continu, la définition de la transformée de Fourier discrète, le théorème d'inversion de Fourier et la formule de Plancherel ne nécessitent pas d'hypothèse d'intégrabilité.

Comme dans le cas continu, les formules d'inversion de Fourier, Plancherel et Parseval sont vérifiées :

Proposition 3.1.1.4 (Inversion de Fourier et formule de Plancherel)**.** *La famille* $(\chi)_{\chi \in \widehat{G}}$ *est*

une base orthonormale de $\{f : G \to \mathbb{C}\}$ *pour le produit hermitien*

$$< f, g >= \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}, \text{ où } f, g : G \to \mathbb{C}.$$

On peut alors définir la norme de $f : G \to \mathbb{C}$ *comme étant :*

$$||f|| = \sqrt{< f, f >} = \left(\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 \right)^{1/2}.$$

On a la formule d'inversion de Fourier :

$$\forall f : G \to \mathbb{C}, f =< \widehat{f}, \chi >= \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi.$$

On a également la formule de Plancherel :

$$\forall f, g : G \to \mathbb{C}, \ < f, g >= \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)} = \frac{1}{|G|^2} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)} = \frac{1}{|G|} < \widehat{f}, \widehat{g} >,$$

et la formule de Parseval :

$$\forall f : G \to \mathbb{C}, \ ||f||^2 = \frac{1}{|G|} \sum_{x \in G} |f(x)|^2 = \frac{1}{|G|^2} \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2 = \frac{1}{|G|} ||\widehat{f}||^2.$$

On pourra trouver une preuve de ces formules dans [16].

Définition 3.1.1.5 (Support)**.** *Soit* $f : G \to \mathbb{C}$*. On appelle support de* f *l'ensemble*

$$supp(f) = \{x \in G, f(x) \neq 0\}.$$

Définition 3.1.1.6. *Soit* H *un sous-groupe de* G*. On appelle orthogonal de* H*, le sous-groupe* $H^\perp$ *de* $\widehat{G}$ *défini par :*

$$H^\perp = \{\chi \in \widehat{G}, H \subseteq \ker \chi\}.$$

En particulier $|H^\perp| = [G : H]$ *et donc* $(H^\perp)^\perp = H$.

Proposition 3.1.1.7. *Soit* H *un sous-groupe de* G. *On a :* $\widehat{\mathbb{1}_H} = |H|\mathbb{1}_{H^\perp}$.

Démonstration. Soit $\chi \in \widehat{G}$. On a :

$$\begin{aligned}\widehat{\mathbb{1}_H}(\chi) &= \sum_{x\in G} \mathbb{1}_H(x)\chi(-x) \\ &= \sum_{x\in H} \chi(-x).\end{aligned}$$

Si $\chi \in H^\perp$, alors $\widehat{\mathbb{1}_H}(\chi) = \sum_{x\in H} 1 = |H| = |H|\mathbb{1}_{H^\perp}(\chi)$.

Si $\chi \notin H^\perp$, alors il existe $h \in H$ tel que $\chi(h) \neq 1$. Alors en effectuant le changement de variable $x' = x + h$:

$$\begin{aligned}\widehat{\mathbb{1}_H}(\chi) &= \sum_{x'\in H} \chi(-(x' - h)) \\ &= \chi(h) \sum_{x\in H} \chi(-x) \\ &= \chi(h)\widehat{\mathbb{1}_H}(\chi).\end{aligned}$$

D'où comme $\chi(h) \neq 1$, $\widehat{\mathbb{1}_H}(\chi) = 0 = |H|\mathbb{1}_{H^\perp}(\chi)$. □

Proposition 3.1.1.8. *Soit* H *un sous-groupe de* G. *Posons le morphisme de restriction :*

$$\begin{aligned} q\colon \widehat{G} &\longrightarrow \widehat{H} \\ \chi &\longmapsto \chi|_H.\end{aligned}$$

On a :

$$\forall \eta \in \widehat{H}, \exists \tilde{\eta} \in \widehat{G}, q(\tilde{\eta}) = \eta,$$

ce $\tilde{\eta}$ *n'est pas nécessairement unique pour chaque* η, *mais on en fixe un pour chaque* η. *On a*

alors la décomposition suivante :

$$\widehat{G} = \{\tilde{\eta}\lambda, \eta \in \widehat{H}, \lambda \in H^{\perp}\},$$

et cette décomposition est unique.

Démonstration. Soit $\eta \in \widehat{H}$. On peut retrouver une preuve classique de l'existence d'un prolongement de η à $\widehat{G}$ dans [13].

Montrons tout d'abord que $q^{-1}(\eta) = \{\tilde{\eta}\lambda, \lambda \in H^{\perp}\}$. Soit $\chi \in q^{-1}(\eta)$, donc par définition de q, on a : $\chi|_H = \eta$. Soit $h \in H$, on a :

$$\chi(h)(\tilde{\eta}(h))^{-1} = \eta(h)(\eta(h))^{-1} = 1,$$

donc $\chi\tilde{\eta}^{-1} \in H^{\perp}$, autrement dit on a bien $\chi \in \{\tilde{\eta}\lambda, \lambda \in H^{\perp}\}$. Réciproquement, soit $\lambda \in H^{\perp}$. Soit $h \in H$, on a :

$$q(\tilde{\eta}\lambda)(h) = q(\tilde{\eta})(h)q(\lambda)(h) = \eta(h).$$

Nous pouvons maintenant montrer que $\widehat{G} = \{\tilde{\eta}\lambda, \eta \in \widehat{H}, \lambda \in H^{\perp}\}$. Soit $\chi \in \widehat{G}$, on a de manière évidente que $\chi \in q^{-1}\left(\chi|_H\right)$, et donc par ce qui précède $\chi \in \{\tilde{\eta}\lambda, \eta \in \widehat{H}, \lambda \in H^{\perp}\}$.

Enfin, montrons que cette décomposition est unique. Soit $\eta_1, \eta_2 \in \widehat{H}$, $\lambda_1, \lambda_2 \in H^{\perp}$ tels que $\tilde{\eta_1}\lambda_1 = \tilde{\eta_2}\lambda_2$. Alors pour tout $h \in H$, $\tilde{\eta_1}(h)\lambda_1(h) = \tilde{\eta_2}(h)\lambda_2(h)$ donc $\eta_1(h) = \eta_2(h)$. Alors $\tilde{\eta_1} = \tilde{\eta_2}$ (comme $\tilde{\eta}$ est fixé pour tout η), et donc $\lambda_1 = \lambda_2$. □

Proposition 3.1.1.9. *L'application suivante est un isomorphisme :*

$$\begin{aligned} \varphi\colon H^{\perp} &\longrightarrow \widehat{G/H} \\ \lambda &\longmapsto \lambda' : \begin{cases} G/H & \to \mathbb{C}^* \\ \overline{y} & \mapsto \lambda(y) \end{cases}, \end{aligned}$$

où $\overline{y}$ est l'image dans G/H de $y \in G$.

Démonstration. Tout d'abord, λ' est bien défini car $\lambda \in H^\perp$ donc ne dépend que de la classe de y dans G/H, pour tout $y \in G$. On peut vérifier immédiatement que φ est un morphisme. Montrons que φ est injective. Soit $\lambda \in H^\perp$ tel que $\varphi(\lambda) = 1$. Donc pour tout $\overline{y} \in G/H$, $\lambda'(\overline{y}) = 1$, d'où pour tout $y \in G$, $\lambda(y) = \lambda'(\overline{y}) = 1$, et donc on a $\lambda = 1$. Enfin, montrons que φ est surjective. Posons $m = [G : H]$, et soit $\chi \in \widehat{G/H}$. On partitionne G selon ses classes, en notant $y_1, \ldots, y_m$ des représentants de ces classes : $G = \bigsqcup_{i=1}^{m}(y_i + H)$.Comme pour tout $g \in G$, il existe un unique $i \in [\![1, m]\!]$, et un unique $h \in H$ tels que $g = y_i + h$, on pose $\lambda : g \mapsto \chi(\overline{y_i})$. Enfin $\lambda \in H^\perp$ car pour tout $h \in H$, $\lambda(h) = \chi(\overline{0}) = 1$. □

Nous pouvons maintenant énoncer et démontrer le premier principe d'incertitude. Ce dernier a été montré en premier lieu par Donoho et Stark [3] dans le cas d'un groupe cyclique, mais a pu rapidement être étendu aux groupes abéliens finis en général. La preuve proposée ici est issue de [15].

Proposition 3.1.1.10 (Principe d'incertitude de Donoho et Stark [3])**.**
Pour toute $f : G \to \mathbb{C}$ non nulle, on a :

$$|supp(f)||supp(\widehat{f})| \geq |G|.$$

Démonstration. Soit $f : G \to \mathbb{C}$ non nulle. On a :

$$\sup_{\chi \in \widehat{G}} |\widehat{f}(\chi)| \leq \sum_{x \in G} |f(x)| = \sum_{x \in G} |f(x)| \mathbb{1}_{\mathrm{supp}(f)}(x).$$

Par l'inégalité de Cauchy-Schwarz, on en déduit que :

$$\sup_{\chi \in \widehat{G}} |\widehat{f}(\chi)| \leq \left(\sum_{x \in G} |f(x)|^2 \right)^{1/2} \left(\sum_{x \in G} \mathbb{1}_{\mathrm{supp}(f)}(x) \right)^{1/2} = \frac{|\mathrm{supp}(f)|^{1/2}}{|G|^{1/2}} \left(|G| \sum_{x \in G} |f(x)|^2 \right)^{1/2}.$$

En appliquant la formule de Plancherel, on obtient :

$$\begin{aligned}\sup_{\chi\in\widehat{G}}|\widehat{f}(\chi)| &\leq \frac{|\mathrm{supp}(f)|^{1/2}}{|G|^{1/2}}\left(\sum_{\chi\in\widehat{G}}|\widehat{f}(\chi)|^2\right)^{1/2}\\ &\leq \frac{|\mathrm{supp}(f)|^{1/2}}{|G|^{1/2}}\sup_{\chi\in\widehat{G}}|\widehat{f}(\chi)|\left(\sum_{\chi\in\widehat{G}}\mathbb{1}_{\mathrm{supp}(\widehat{f})}(\chi)\right)^{1/2}.\end{aligned}$$

Au final, on a :

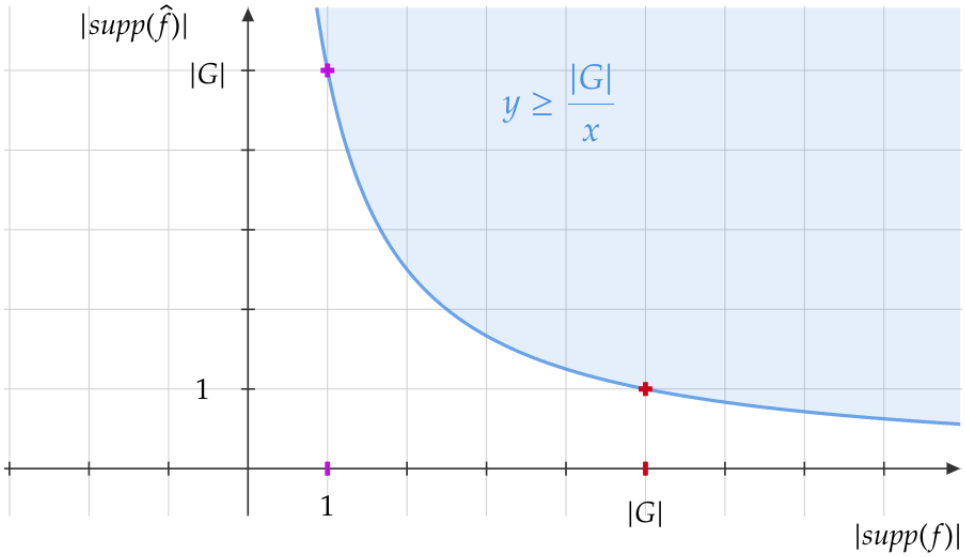
$$\sup_{\chi\in\widehat{G}}|\widehat{f}(\chi)| \leq \frac{|\mathrm{supp}(f)|^{1/2}|\mathrm{supp}(\widehat{f})|^{1/2}}{|G|^{1/2}}\sup_{\chi\in\widehat{G}}|\widehat{f}(\chi)|.$$

Comme $f\neq 0$, par le théorème d'inversion de Fourier on a $\widehat{f}\neq 0$, d'où

$$|G| \leq |\mathrm{supp}(f)||\mathrm{supp}(\widehat{f})|.$$

□

En d'autres termes, ce principe d'incertitude (Proposition 3.1.1.10) affirme que $|\mathrm{supp}(\widehat{f})|$ ne peut être qu'au dessus de l'hyperbole définit par $\frac{|G|}{|\mathrm{supp}(f)|}$:



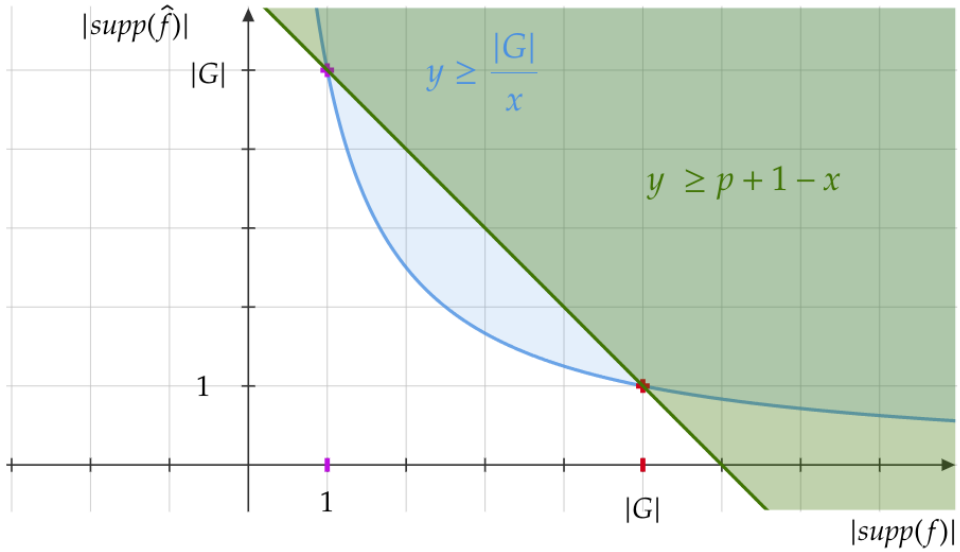
3.1.2 Principe d'incertitude sur $\mathbb{Z}/p\mathbb{Z}$

Le but de cette section est de montrer un raffinement de la proposition 3.1.1.10 dans le cas où $G = \mathbb{Z}/p\mathbb{Z}$ avec p premier. Grâce à la proposition 3.1.1.2, on peut écrire la transformée de Fourier de $f : G \to \mathbb{C}$ comme suit : $\widehat{f}(\xi) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} f(x)e^{-2i\pi x\xi/p}$ pour tout $\xi \in \mathbb{Z}/p\mathbb{Z}$. L'idée initiale de Tao dans [15] est de remarquer que les indicatrices de sous-groupe sont des fonctions qui vérifient l'égalité dans le principe d'incertitude de Donoho et Stark 3.1.1.10 (voir proposition 3.1.1.7), nous verrons au lemme 5.2.0.1 dans un cadre plus général des groupes non abéliens que ce sont "essentiellement" les seules. Si le groupe considéré est $\mathbb{Z}/p\mathbb{Z}$, étant donné que ce dernier n'a que des sous-groupes triviaux, il paraît raisonnable de pouvoir améliorer le principe d'incertitude en utilisant ce qui précède.

Théorème 3.1.2.1 (Principe d'incertitude sur $\mathbb{Z}/p\mathbb{Z}$ [15])**.**

1. *Soit $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ non nulle. On a : $|supp(f)| + |supp(\widehat{f})| \geq p + 1$.*
2. *Réciproquement, soit $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ non vides. Si $|A| + |B| \geq p + 1$ alors il existe $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ telle que $supp(f) = A$ et $supp(\widehat{f}) = B$.*

En reprenant une vision "graphique" du principe d'incertitude, ce raffinement montre que pour les fonctions définies sur $\mathbb{Z}/p\mathbb{Z}$, $|\text{supp}(\widehat{f})|$ ne peut être qu'au dessus de la droite $p + 1 - |\text{supp}(f)|$:



Pour montrer ce théorème, Tao utilise le théorème suivant :

Théorème 3.1.2.2 (Théorème de Chebotarev)**.** *Soit p premier et $\omega \in \mathbb{C}$ une racine primitive p-ième de l'unité. Tous les mineurs de $(\omega^{ij})_{i,j\in\mathbb{Z}/p\mathbb{Z}}$ sont non nuls.*

L'intérêt du théorème de Chebotarev dans notre cas est de montrer l'inversibilité de la transformée de Fourier pour des fonctions dont le support et celui de leurs transformées de Fourier sont restreints.

En effet, les mineurs de la matrice précédente sont exactement dans des bases adaptées les matrices des applications suivantes (Proposition 3.1.2.3). Ces déterminants non nuls donnent alors l'inversibilité de ces applications. Nous proposons en annexe trois preuves différentes du théorème de Chebotarev.

Proposition 3.1.2.3. *Soit p premier. Soient $A, \tilde{A} \subseteq \mathbb{Z}/p\mathbb{Z}$ non vides tels que $|A| = |\tilde{A}|$. L'application suivante est inversible :*

$$\begin{aligned} T\colon l^2(A) &\longrightarrow l^2(\tilde{A}) \\ f &\longmapsto \widehat{f}|_{\tilde{A}}, \end{aligned}$$

où $l^2(A) = \{f : G \to \mathbb{C}, supp(f) \subseteq A\}$.

Démonstration. Posons $n = |A| = |\tilde{A}|$ et on écrit $A = \{x_1, \dots, x_n\}$, $\tilde{A} = \{\xi_1, \dots, \xi_n\}$. En particulier $\mathcal{B} = \left(\mathbb{1}_{\{x_1\}}, \dots, \mathbb{1}_{\{x_n\}}\right)$ est une base de $l^2(A)$ et de même $\mathcal{B}' = \left(\mathbb{1}_{\{\xi_1\}}, \dots, \mathbb{1}_{\{\xi_n\}}\right)$ est une base de $l^2(\tilde{A})$. Comme pour tout $i \in [\![1, n]\!]$:

$$\begin{aligned} T\mathbb{1}_{\{x_i\}} &= \widehat{\mathbb{1}}_{\{x_i\}}|_{\tilde{A}} \\ &= \sum_{x\in\mathbb{Z}/p\mathbb{Z}} \mathbb{1}_{\{x_i\}}(x) e^{-2i\pi x\cdot/p}|_{\tilde{A}} \\ &= e^{-2i\pi x_i\cdot/p}|_{\tilde{A}} \\ &= \sum_{j=1}^{n} e^{-2i\pi x_i\xi_j/p}\mathbb{1}_{\{\xi_j\}}, \end{aligned}$$

en posant $\omega = e^{-2i\pi/p}$, la matrice de T dans les bases $\mathcal{B}$ à $\mathcal{B}'$ est alors :

$$\mathcal{M}at_{\mathcal{B},\mathcal{B}'}T = \begin{pmatrix} \omega^{x_1\xi_1} & \dots & \omega^{x_n\xi_1} \\ \vdots & \ddots & \vdots \\ \omega^{x_1\xi_n} & \dots & \omega^{x_n\xi_n} \end{pmatrix}$$

qui est de déterminant non nul par le théorème de Chebotarev (Théorème 3.1.2.2).

□

Nous pouvons maintenant prouver le théorème 3.1.2.1.

Démonstration du théorème 3.1.2.1.

1. Supposons par l'absurde qu'il existe $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ non nulle telle que

$$|\mathrm{supp}(f)| + |\mathrm{supp}(\widehat{f})| \leq p.$$

Posons $A = \mathrm{supp}(f)$, et on a donc $|A| \leq p - |\mathrm{supp}(\widehat{f})| = |\mathbb{Z}/p\mathbb{Z} \setminus \mathrm{supp}(\widehat{f})|$. Alors il existe $\tilde{A} \subseteq \mathbb{Z}/p\mathbb{Z}$ tel que $\tilde{A} \cap \mathrm{supp}(\widehat{f}) = \emptyset$ et $|\tilde{A}| = |A|$. En effet, il suffit de prendre $\tilde{A} \subseteq \left(\mathbb{Z}/p\mathbb{Z} \setminus \mathrm{supp}(\widehat{f})\right)$ tel que $|\tilde{A}| = |A|$. Donc pour ce A et $\tilde{A}$, on a $Tf = 0$, ce qui est absurde car $f \neq 0$ et T bijective par le lemme 3.1.2.3.

2. La preuve de la réciproque se fait en deux étapes, en fonction de la valeur de $|A|+|B|$. On en déduira l'étape 2 de l'étape 1.

   Étape 1 : Soient $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, non vides, tels que $|A| + |B| = p + 1$. Montrons qu'il existe $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ telle que $\mathrm{supp}(f) = A$ et $\mathrm{supp}(\widehat{f}) = B$.
   Il existe $\tilde{A} \subseteq \mathbb{Z}/p\mathbb{Z}$ tel que $|\tilde{A}| = |A|$ et $|\tilde{A} \cap B| = 1$. En effet, posons

$$k = |A \cap B| = |A| + |B| - |A \cup B| = p + 1 - |A \cup B| \geq 1,$$

et notons $A \cap B = \{x_1, \dots, x_k\}$. Posons $\overline{A} = A \setminus \{x_2, \dots, x_k\}$, de telle sorte que $|\overline{A} \cap B| = 1$. Cependant $|\overline{A}| = |A| - (k-1)$, on cherche alors à rajouter $k-1$ éléments

qui ne sont pas dans B à $\overline{A}$ pour former $\tilde{A}$ tout en gardant $|\tilde{A} \cap B| = 1$ mais que $|\tilde{A}| = |A|$. Or $k - 1 = p - |A \cup B| = |(A \cup B)^C|$, donc au final $\tilde{A} = \overline{A} \cup (A \cup B)^C$ convient.

Notons $\tilde{A} \cap B = \{\xi\}$. Par la proposition 3.1.2.3, il existe $f \in l^2(A)$ non nulle telle que $Tf = \mathbb{1}_{\{\xi\}}$. Par définition on a $\text{supp}(f) \subseteq A$ et de plus,

$$|\tilde{A} \cup B| = |\tilde{A}| + |B| - |\tilde{A} \cap B| = |A| + |B| - |\tilde{A} \cap B| = p.$$

On en déduit que $\tilde{A} \cup B = \mathbb{Z}/p\mathbb{Z}$, et donc on peut décomposer $\mathbb{Z}/p\mathbb{Z} = (\tilde{A} \setminus \{\xi\}) \sqcup B$. Comme $\widehat{f}_{|_{\tilde{A}}}$, $\widehat{f}$ est nulle sur $\tilde{A} \setminus \{\xi\}$ donc $\text{supp}(\widehat{f}) \subseteq B$. Enfin, si par l'absurde $|\text{supp}(f)| < |A|$ ou $|\text{supp}(\widehat{f})| < |B|$ alors $|\text{supp}(f)| + |\text{supp}(\widehat{f})| < |A| + |B| = p+1$, ce qui est impossible par le sens direct du théorème, d'où $\text{supp}(f) = A$ et $\text{supp}(\widehat{f}) = B$.

Étape 2 : Soit $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, non vides, tels que $|A| + |B| > p + 1$. Posons

$$S = \{(A', B') \in (\mathcal{P}(\mathbb{Z}/p\mathbb{Z}))^2,\ A' \subseteq A,\ B' \subseteq B,\ |A'| + |B'| = p + 1\},$$

où $\mathcal{P}(\mathbb{Z}/p\mathbb{Z})$ est l'ensemble des parties de $\mathbb{Z}/p\mathbb{Z}$. S est fini, nous notons s son cardinal et $(A_1, B_1), \ldots, (A_s, B_s)$ ses élements. Par l'étape 1, il existe $f_1, \ldots, f_s : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ telles que $\text{supp}(f_i) = A_i$ et $\text{supp}(\widehat{f_i}) = B_i$ pour tout $i \in [\![1, s]\!]$. On cherche $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ tels que $\text{supp}(f) = A$ et $\text{supp}(\widehat{f}) = B$ où l'on pose $f = \sum_{i=1}^s \lambda_i f_i$. Or pour tout $\lambda_1, \ldots, \lambda_s \in \mathbb{C}, \text{supp}(f) \subseteq A$ et $\text{supp}(\widehat{f}) \subseteq B$. En effet, si $x \notin A$ alors pour tout $i \in [\![1, s]\!]$ $x \notin A_i$ donc $f_i(x) = 0$ et $f(x) = 0$. On applique le même raisonnement pour $\widehat{f}$.

Au final, on cherche $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ tels que

$$\begin{cases} \forall x \in A, \sum_{i=1}^s \lambda_i f_i(x) \neq 0 \\ \forall \xi \in B, \sum_{i=1}^s \lambda_i \widehat{f_i}(\xi) \neq 0. \end{cases}$$

Posons pour tout $x \in A, V_x = \{(\lambda_1, \ldots, \lambda_s) \in \mathbb{C}^s, \sum_{i=1}^s \lambda_i f_i(x) = 0\}$, qui est sous-espace vectoriel de $\mathbb{C}^s$ de dimension au plus $s - 1$. De même, posons pour tout $\xi \in B, W_\xi = \{(\lambda_1, \ldots, \lambda_s) \in \mathbb{C}^s, \sum_{i=1}^s \lambda_i \widehat{f_i}(\xi) = 0\}$, qui est aussi un sous-espace

vectoriel de $\mathbb{C}^s$ de dimension au plus $s-1$. Comme $\bigcup_{x\in A} V_x \cup \bigcup_{\xi\in B} W_\xi$ est une union finie de sous-espace vectoriels de dimensions strictement inférieures à s, on obtient que :

$$\bigcup_{x\in A} V_x \cup \bigcup_{\xi\in B} W_\xi \subsetneq \mathbb{C}^s,$$

autrement dit il existe $(\lambda_1,\dots,\lambda_s) \in \bigcap_{x\in A} V_x^C \cap \bigcap_{\xi\in B} W_\xi^C$. Pour ces λ_i, on a bien :

$$\begin{cases} \forall x \in A, f(x) \neq 0 \\ \forall \xi \in B, \widehat{f}(\xi) \neq 0. \end{cases}$$

□

Corollaire 3.1.2.4. *Soit $d \in \mathbb{N}$, $P = \sum_{j=0}^{d} c_j z^{n_j} \in \mathbb{C}[z]$, où chaque $c_j \in \mathbb{C}^*$ et $0 \leq n_0 < n_1 < \ldots < n_k < p$. Alors P admet au plus d racines parmi les racines p-ièmes de l'unité.*

L'élément central dans la démonstration de Tao est le théorème de Chebotarev, qui s'applique lorsque la taille de la matrice est un nombre premier. Ainsi, si l'on dispose d'une généralisation du théorème de Chebotarev au cas où la taille m de la matrice n'est pas un nombre premier, il sera possible d'adapter cette démonstration pour prouver un principe d'incertitude linéaire sur $\mathbb{Z}/m\mathbb{Z}$. C'est suivant cette idée que Ram Murty et Peter Whang [10] ont montré en utilisant la théorie des groupes de Lie sur le groupe unitaire la proposition suivante :

Proposition 3.1.2.5. *Soient $p_1,\dots,p_r$ les diviseurs premiers de m, $\omega_1,\dots,\omega_n$ des racines m-ièmes de l'unité deux à deux distinctes, et $\kappa_1,\dots,\kappa_n$ des entiers deux à deux distincts modulo m. Si*

$$\frac{\prod_{1\leq i<j\leq n} |\kappa_i - \kappa_j|}{\prod_{1\leq i<j\leq n} (j-i)} \notin \mathbb{N}p_1 + \ldots + \mathbb{N}p_r$$

alors $\det\left((w_i^{\kappa_j})_{1\leq i,j\leq n}\right) \neq 0$.

En posant $P(A)$ la condition sur $A = \{\kappa_1, \ldots, \kappa_n\} \subseteq \mathbb{Z}/m\mathbb{Z}$:

$$\frac{\prod\limits_{1\leq i<j\leq n} |\kappa_i - \kappa_j|}{\prod\limits_{1\leq i<j\leq n} (j-i)} \notin \mathbb{N}p_1 + \ldots + \mathbb{N}p_r,$$

ils en ont déduit le théorème :

Théorème 3.1.2.6. *Soit $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ non nulle. Si $P(supp(f))$ ou $P(supp(\widehat{f}))$, alors $|supp(f)| + |supp(\widehat{f})| \geq m + 1$.*

3.2 Le théorème de Cauchy-Davenport

Cette section est consacrée à une application du principe d'incertitude 3.1.2.1 à une autre démonstration du théorème de Cauchy-Davenport 3.2.0.1. Cette nouvelle preuve est issue de [15] et nous proposons une preuve plus classique en annexe.

Théorème 3.2.0.1 (Cauchy-Davenport)**.**
Soient $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, non vides. Posons $A + B = \{a + b, a \in A, b \in B\}$. Alors :

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

Démonstration. Soient $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, non vides.

Il existe $X, Y \subseteq \mathbb{Z}/p\mathbb{Z}$ tels que $|X| = p + 1 - |A|$, $|Y| = p + 1 - |B|$ et $|X \cap Y| = max(|X| + |Y| - p, 1)$. En effet, comme $A \neq \emptyset$, il existe $X \subseteq \mathbb{Z}/p\mathbb{Z}$ tel que $|X| = p + 1 - |A|$. Donc $|X^C| = |A| - 1$. On distingue deux cas :

Cas 1 : Si $|X| + 1 > |B|$, il existe $Y' \subseteq X$ tel que $|Y'| = |X| + \underbrace{1 - |B|}_{\leq 0}$. En posant $Y = Y' \cup X^C$, on a bien $|X| = |X| + 1 - |B| + |A| - 1 = p + 1 - |B|$.

Cas 2 : Si $|X| + 1 \leq |B|$, alors $p - |X| \geq p + 1 - |B|$. De plus, il existe $Y' \subseteq X$ singleton, et $Y'' \subseteq X^C$ tel que $|Y'| = p - |B|$. En posant $Y = Y' \sqcup Y''$, on a bien $|Y| = |Y'| + |Y''| = 1 + p - |B|$.

Dans tous les cas, $|X \cap Y| = |Y'| = max(|X| + 1 - |B|, 1) = max(|X| + |Y| - p, 1)$.

Par (ii) du théorème 3.1.2.1, il existe $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ telle que $\text{supp}(f) = A$ et $\text{supp}(\widehat{f}) = X$. De même, il existe $g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ telle que $\text{supp}(g) = B$ et $\text{supp}(\widehat{g}) = Y$. Alors la fonction

$$x \mapsto f * g(x) = \sum_{h \in \mathbb{Z}/p\mathbb{Z}} \underbrace{f(h)}_{\neq 0 \text{ si} h \in A} \underbrace{g(x-h)}_{\neq 0 \text{ si } x \in h+B} = \sum_{x \in A} f(h)g(x-h)$$

vérifie $\text{supp}(f * g) \subseteq A + B$. En effet, si $x \notin A + B$, on a $\forall h \in A, x \notin h + B$ i.e. $g(x-h) = 0$. Donc $f * g(x) = 0$.

De plus, $\widehat{f * g} = \widehat{f}\widehat{g}$, donc $\text{supp}(\widehat{f * g}) = X \cap Y \neq \emptyset$. En particulier, par inversion de Fourier, $f * g \neq 0$.

Par le sens direct du théorème 3.1.2.1, on a :

$$\underbrace{|\text{supp}(f * g)|}_{\leq |A+B|} + \underbrace{|\text{supp}(\widehat{f * g})|}_{= |X \cap Y|} \geq p + 1,$$

donc $|X \cap Y| \leq p + 1 - |A + B|$. On en conclut que :

$$\begin{aligned} |A + B| &\geq p + 1 - max(|X| + |Y| - p, 1) \\ &= p + 1 - max(p + 2 - |A| - |B|, 1) \\ &\geq min(|A| + |B| - 1, p). \end{aligned}$$

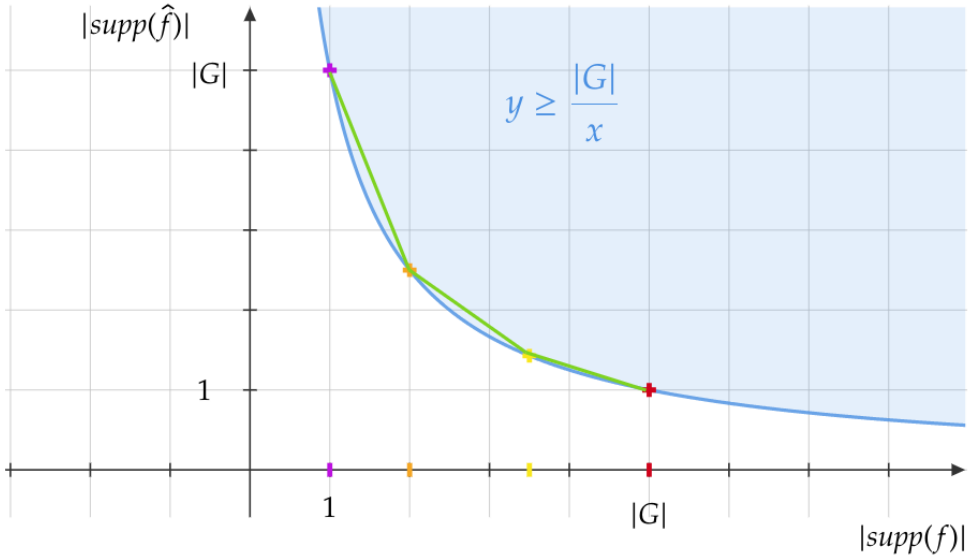
□

4 Des principes d'incertitudes sur un groupe abélien fini

4.1 Un principe d'incertitude linéaire sur les groupes abéliens finis

Comme nous avons pu l'observer pour le principe d'incertitude sur $\mathbb{Z}/p\mathbb{Z}$, l'idée que les indicatrices sont essentiellement les seules applications qui réalisent l'égalité dans le premier principe d'incertitude nous invite à améliorer ce dernier entre chaque diviseur du cardinal

du groupe. En effet, le groupe étant abélien, ces diviseurs correspondent exactement à un sous-groupe, par la réciproque au théorème de Lagrange. Nous ne pouvons pas espérer en général une droite, comme vu pour le principe d'incertitude sur $\mathbb{Z}/p\mathbb{Z}$, car $\mathbb{Z}/p\mathbb{Z}$ constitue un cas très particulier où il n'y a que des sous-groupes triviaux. Cependant, nous allons montrer qu'entre chaque paire de diviseurs successifs du cardinal du groupe, nous pourrons reproduire ce qu'il se passe pour $\mathbb{Z}/p\mathbb{Z}$. Cela nous donnera graphiquement un aspect de ligne brisée, où les sommets correspondent aux diviseurs du cardinal du groupe, comme illustré ici :



Définition 4.1.0.1. *Soit $n \in \mathbb{N}^*$, $k \in [1, n]$. On pose :*

- $d_1(n,k) = \max\{d|n,\ d \leq k\}$, $d_2(n,k) = \min\{d|n,\ d \geq k\}$. *Ces quantités sont les diviseurs successifs (ou égaux) de n tels que $k \in [\![d_1, d_2]\!]$.*
- $u(n,k) = \frac{n}{d_1 d_2}(d_1 + d_2 - k)$, *où $d_1 = d_1(n,k)$ et $d_2 = d_2(n,k)$. Si $k \in [d_1, d_2]$, $u(n,k)$ correspond au segment reliant $\left(d_1, \frac{n}{d_1}\right)$ et $\left(d_2, \frac{n}{d_2}\right)$.*
- $\forall k \in [1,n], \Theta(n,k) = \min\{|supp(\widehat{f})|, f : G \to \mathbb{C}$ *non nulle*, $|supp(f)| \leq k\}$.

L'objectif de cette section est de montrer le théorème de Meshulam [9] :

Théorème 4.1.0.2 (Principe d'incertitude linéaire sur un groupe abélien fini)**.**

Posons $n = |G|$. Soit $f : G \to \mathbb{C}$ non nulle. Alors :

$$|supp(\widehat{f})| \geq u(n, |supp(f)|).$$

Ce théorème nous donne une meilleure minoration que celle du théorème 3.1.1.10, mais elle n'est sûrement pas optimale, au vu par exemple du théorème 3.1.2.6.

Pour montrer ce théorème, nous allons le montrer par récurrence sur le cardinal de G. Voyons d'abord comment se comporte la fonction Θ (resp. u) en fonction d'un sous-groupe de G (resp. le cardinal d'un sous-groupe de G).

Remarque. *Donner des encadrements de Θ est un sujet encore étudié. Bonami et Ghobber ont donné dans [2], pour certains groupes, une description des fonctions dont le support vaut un certain k et celui de leur transformée de Fourier vaut $\Theta(n, k)$. Cela étend la description des cas d'égalités quand le groupe est $\mathbb{Z}/p\mathbb{Z}$, car dans ce cas $\Theta(n, k) = |G| - k + 1$.*

4.1.1 Lemmes intermédiaires

Posons $n = |G|$.

Proposition 4.1.1.1. *Soit H un sous-groupe de G, $k \in [1, n]$.*
Il existe $s \in [1, |H|]$ et $t \in [1, |G/H|]$ tels que $st \leq k$ et $\Theta(G, k) \geq \Theta(H, s)\Theta(G/H, t)$.

Dans la preuve de la proposition 4.1.1.1, nous allons vouloir qu'il est intéressant de poser les fonctions suivantes au vu de la définition de $\Theta(H, s)$ et de $\Theta(G/H, t)$.

Définition 4.1.1.2. *Soit $f : G \to \mathbb{C}$, et H un sous-groupe de G. On pose pour tout $y \in G$:*

$$\begin{aligned} f_y \colon H &\longrightarrow \mathbb{C} \\ h &\longmapsto f(h + y), \end{aligned}$$

et pour tout $\eta \in \widehat{H}$ *:*

$$\begin{aligned} F_\eta \colon G/H &\longrightarrow \mathbb{C} \\ \bar{y} &\longmapsto \widehat{f_y}(\eta)\tilde{\eta}(-y). \end{aligned}$$

Lemme 4.1.1.3. *Soit* $f : G \to \mathbb{C}$*, et* H *un sous-groupe de* G*. On a :*

$$\forall \eta \in \widehat{H}, \forall \lambda \in H^\perp, \widehat{f}(\tilde{\eta}\lambda) = \widehat{F_\eta}(\lambda'),$$

où λ' *est défini à la proposition 3.1.1.9.*

Démonstration. Soit $\eta \in \widehat{H}$ et $\lambda \in H^\perp$. Posons $m = [G : H]$, et on partitionne le groupe selon ses classes $G = \bigsqcup_{i=1}^m (y_i + H)$. On a :

$$\begin{aligned} \widehat{f}(\tilde{\eta}\lambda) &= \sum_{x \in G} f(x)(\tilde{\eta}\lambda)(-x) \\ &= \sum_{x \in G} f(x)\tilde{\eta}(-x)\lambda(-x) \\ &= \sum_{i=1}^m \sum_{h \in H} f(y_i + h)\tilde{\eta}(-y_i - h)\lambda(-y_i - h) \\ &= \sum_{i=1}^m \sum_{h \in H} f_{y_i}(h)\eta(-h)\tilde{\eta}(-y_i)\lambda(-y_i) \\ &= \sum_{i=1}^m \widehat{f_{y_i}}(\eta)\tilde{\eta}(-y_i)\lambda(-y_i) \\ &= \sum_{i=1}^m F_\eta(\bar{y_i}) \underbrace{\lambda(-y_i)}_{\lambda'(-\bar{y_i})} \\ &= \widehat{F_\eta}(\lambda'). \end{aligned}$$

□

Montrons maintenant la proposition 4.1.1.1.

Démonstration de la proposition 4.1.1.1.

Étape 1 : Montrons que $\forall f : G \to \mathbb{C}, f \neq 0, \exists s \in [1, |H|], \exists t \in [1, |G/H|], st = |\mathrm{supp}(f)|$ et $|\mathrm{supp}(\widehat{f})| \geq \Theta(H, s)\Theta(G/H, t)$.

Soit $f : G \to \mathbb{C}$ non nulle. Posons $k = |\mathrm{supp}(f)|$. On écrit encore $G = \bigsqcup_{i=1}^{m}(y_i + H)$, où $m = |G/H|$.

Regardons les classes sur lesquelles f n'est pas nulle : on pose $I = \{i \in [\![1, m]\!], \mathrm{supp}(f) \cap (y_i + H) \neq \emptyset\}$, et $t = |I|$. Par définition, on a bien que $t \in [1, |G/H|]$. De plus, pour tout $\eta \in \widehat{H}, |\mathrm{supp}(F_\eta)| \leq t$ (en effet, si $j \notin I, f_{y_i} = 0$ donc par définition $F_\eta(\bar{y}_i) = 0$). Donc pour tout $\eta \in \widehat{H}$, si $F_\eta \neq 0$, alors par définition de Θ on a $|\mathrm{supp}(\widehat{F_\eta})| \geq \Theta(G/H, t)$.

Posons $s = \frac{k}{t}$. Comme $|\mathrm{supp}(f)| = k \leq |H|t$, on a bien $s \in [1, |H|]$. Montrons qu'il existe $i \in I$ tel que $0 < |\mathrm{supp}(f_{y_i})| \leq s$. Par l'absurde, supposons que pour tout $i \in I$, $|\mathrm{supp}(f_{y_i})| > \frac{k}{t}$ ou $|\mathrm{supp}(f_{y_i})| = 0$. On peut alors séparer les classes selon si f est nulle dessus ou pas :

$$\mathrm{supp}(f) = \underbrace{\bigsqcup_{i \in I}(y_i + H) \cap \mathrm{supp}(f)}_{\text{de cardinal } > |I|s = k} \bigsqcup \underbrace{\bigsqcup_{i \notin I}(y_i + H) \cap \mathrm{supp}(f)}_{= \emptyset},$$

et donc $|\mathrm{supp}(f)| > k$ ce qui est absurde. D'où il existe $i \in I$ tel que $0 < |\mathrm{supp}(f_{y_i})| \leq s$. Par définition de Θ, on a $|\mathrm{supp}(\widehat{f_{y_i}})| \geq \Theta(H, s)$.

Aussi remarquons que si $\eta \in \mathrm{supp}(\widehat{f_{y_i}}), F_\eta(\bar{y}_i) = \widehat{f_{y_i}}(\eta)\tilde{\eta}(-y_i) \neq 0$ donc F_η est non nulle.

Enfin, la proposition 3.1.1.8 nous permet avec le lemme 4.1.1.3 de compter les $\chi \in \mathrm{supp}(\widehat{f})$ en les décomposant (de manière unique) en $\tilde{\eta}\lambda$ avec $\eta \in \widehat{H}$ et $\lambda \in H^\perp$, et en regardant pour chaque $\eta \in \widehat{H}$ si $\lambda' \in \mathrm{supp}(\widehat{F_\eta})$.

Tout cela mis bout à bout nous permet d'écrire :

$$\begin{aligned}|\mathrm{supp}(\widehat{f})| &= \sum_{\eta\in\widehat{H}} |\mathrm{supp}(\widehat{F_\eta})| \\ &\geq \sum_{\eta\in\mathrm{supp}(\widehat{f_{y_i}})} |\mathrm{supp}(\widehat{F_\eta})| \\ &\geq |\mathrm{supp}(\widehat{F_\eta})|\Theta(G/H,t) \\ &\geq \Theta(H,s)\Theta(G/H,t).\end{aligned}$$

Étape 2 : montrons que $\forall k \in [1,n], \exists s \in [1,|H|], \exists t \in [1,|G/H|], st \leq k$ et $\Theta(G,k) \geq \Theta(H,s)\Theta(G/H,t)$. La différence avec l'étape 1 est que cette dernière nous donne l'existence de s et t à f fixée, on cherche maintenant s et k indépendants de f.
Soit $k \in [1,n]$. Posons $F = \{f : G \to \mathbb{C} \text{ non nulle}, |\mathrm{supp}(f)| \leq k\}$, qui est fini, de cardinal noté l. Écrivons $f_1, \ldots, f_l$ ses éléments. En appliquant l'étape 1 à chacune des ces fonctions, on obtient que pour tout $i \in [\![1,l]\!]$, il existe $s_i \in [1,|H|]$ et $t_i \in [1,|G/H|]$ tels que $s_i t_i = |\mathrm{supp}(f_i)|$ et $|\mathrm{supp}(\widehat{f_i})| \geq \Theta(H,s_i)\Theta(G/H,t_i)$. Posons $(s,t) \in \{(s_i,t_i), i \in [\![1,l]\!]\}$ tel que (s,t) réalise le $\min_{i\in[\![1,l]\!]} \Theta(H,s_i)\Theta(G/H,t_i)$. Alors $st \leq k$ et pour tout $f \in F$, $|\mathrm{supp}(\widehat{f})| \geq \Theta(H,s)\Theta(G/H,t)$. On en conclut que $\Theta(G,k) \geq \Theta(H,s)\Theta(G/H,t)$.

□

Proposition 4.1.1.4. *Soit $d|n$, $s \in [1,d]$ et $t \in [1,\frac{n}{d}]$. On a : $u(d,s)u(\frac{n}{d},t) \geq u(n,st)$.*

Démonstration. La preuve de la proposition 4.1.1.4 repose uniquement sur des inégalités de convexité. Posons $k = st$, $a_i = d_i(d,s)$, $b_i = d_i(\frac{n}{d},t)$ et $c_i = d_i(n,k)$ pour $i = 1,2$. Par définition de u, on a l'équivalence :

$$u(d,s)u(\frac{n}{d},t) \geq u(n,st) \iff \frac{(a_1+a_2-s)(b_1+b_2-t)}{a_1a_2b_1b_2} \geq \frac{c_1+c_2-k}{c_1c_2}.$$

Comme la dernière expression est symétrique en a_1, a_2, b_1, b_2, on peut supposer sans perte de généralités que $a_1b_1 \leq a_1b_2 \leq a_2b_1 \leq a_2b_2$. Or remarquons que comme $a_1 \leq s$ et $b_1 \leq t$

alors $a_1b_1 \leq k$, et de même comme $s \leq a_2$ et $t \leq b_2$ alors $k \leq a_2b_2$. Nous allons donc faire une disjonction de cas en fonctions de où se situe k par rapport à a_1b_2 et a_2b1. Posons $m_1 = \max(a_1, \frac{k}{b_2})$ et $m_2 = \min(a_2, \frac{k}{b_1})$. Par définition on a :

$$m_1 \leq s \leq m_2,$$

cela va nous servir dans un instant car nous allons vérifier des inégalités sur les valeurs extrêmes de s et conclure avec un argument de convexité. Supposons que $a_1b_1 \leq k \leq a_1b_2$

Or $a_1b_1|d \times \frac{n}{d} = n$ et de même $a_1b_2|n$, on a :

$$a_1b_1 \leq c_1 \leq k \leq c_2 \leq a_1b_2.$$

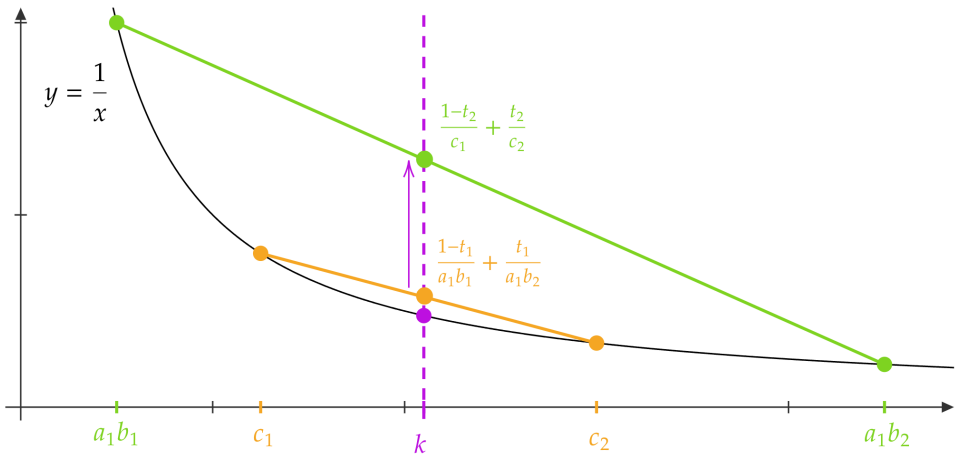
Montrons que $\frac{a_1b_1+a_1b_2-k}{(a_1b_1)(a_1b_2)} \geq \frac{c_1+c_2-k}{c_1c_2}$. On a :

$$\frac{a_1b_1 + a_1b_2 - k}{(a_1b_1)(a_1b_2)} \geq \frac{c_1 + c_2 - k}{c_1c_2} \iff \underbrace{\frac{1}{a_1b_1} + \frac{1}{a_1b_2} - \frac{k}{a_1b_1a_1b_2} \geq \frac{1}{c_1} + \frac{1}{c_2} - \frac{k}{c_1c_2}}_{(*)}$$

Écrivons k comme barycentre des autres points : $k = (1 - t_1)a_1b_1 + t_1a_1b_2$ et $k = (1 - t_2)c_1 + t_2c_2$, pour un certain $t_1, t_2 \in [0, 1]$. Alors :

$$\begin{aligned}(*) &\iff \frac{1}{a_1b_1} + \frac{1}{a_1b_2} - \left(\frac{1-t_1}{a_1b_2} + \frac{t_1}{a_1b_1}\right) \geq \frac{1}{c_1} + \frac{1}{c_2} - \left(\frac{1-t_2}{c_2} + \frac{t_2}{c_1}\right) \\ &\iff \frac{1-t_1}{a_1b_1} + \frac{t_1}{a_1b_2} \geq \frac{1-t_2}{c_1} + \frac{t_2}{c_2}\end{aligned}$$

Or la fonction $x \mapsto \frac{1}{x}$ est convexe sur $\mathbb{R}_+^*$, donc la dernière assertion est vraie, comme l'illustre le graphique suivant :



Il suffit donc de montrer que $\frac{(a_1+a_2-s)(b_1+b_2-t)}{a_1a_2b_1b_2} \geq \frac{a_1b_1+a_1b_2-k}{(a_1b_1)(a_1b_2)}$. Or :

$$\frac{(a_1+a_2-s)(b_1+b_2-t)}{a_1a_2b_1b_2} \geq \frac{a_1b_1+a_1b_2-k}{(a_1b_1)(a_1b_2)} \iff f(s) \geq d,$$

où on a posé $f(s) = a_1(a_1+a_2-s)(b_1+b_2-\frac{k}{s})$ et $d = a_2a_1b_1 + a_2a_1b_2 - ka_2$. On doit vérifier l'assertion précédente pour tout $s \in [m_1, m_2]$. Cependant, f est concave, pour montrer que $f(s) \geq d$, il suffit de montrer que la corde reliant $m_1, f(m_1))$ et $(m_2, f(m_2))$ est au dessus de la droite $y = d$. Cependant, comme le minimum de la corde est atteint en une des ces deux extrémités, il suffit de montrer que $f(m_1) \geq d$ et $f(m_2) \geq$. Or ici $m_1 = a_1$ et $m_2 = \frac{k}{b_1}$, de simples calculs donnent :

$$f(a_1) = d,$$

et

$$f\left(\frac{k}{b_1}\right) \geq d \iff (a_2b_1 - a_1b_2)(k - a_1b_1) \geq 0,$$

ce qui est vrai. D'où le résultat.

On raisonne exactement de la même manière pour les autres cas (si $a_1b_2 \leq k \leq a_2b_1$ ou si $a_2b_1 \leq k \leq a_2b_2$), que nous ne détaillerons pas. □

Enfin, terminons par une dernier lemme sur la décroissance de la fonction u suivant la variable k :

Lemme 4.1.1.5. *Soit $k, k' \in [1, n]$. Si $k' \leq k$ alors $u(n, k') \geq u(n, k)$.*

Démonstration. Posons $d_i = d_i(n, k)$ et $d'_i = d_i(n, k')$ pour $i = 1, 2$. Par définition : $d'_1 \leq d_1 \leq d_2$ et $d'_1 \leq d'_2 \leq d_2$. Nous allons donc faire une disjonction de cas en fonction de si $d_1 \leq d_2$ ou non.

Cas 1 : si $d'_1 \leq d'_2$ Comme $u(n, k')$ est la droite reliant $\left(d'_1, \frac{n}{d'_1}\right)$ et $\left(d'_2, \frac{n}{d'_2}\right)$ en fonction de $k' \in [d'_1, d'_2]$, et de même pour $u(n, k)$ pour $k \in [d_1, d_2]$, on a $u(n, k') \geq u(n, k)$.

Cas 2 : si $d'_1 \leq d'_2 \leq d_1 \leq d_2$ Comme d'_1 et d'_2 sont des diviseurs consécutifs ou égaux de n et de même pour d_1 et d_2, alors : ($d_1 = d'_1$ ou $d_1 = d'_2$) et ($d'_2 = d_1$ ou $d'_2 = d_2$). Dans chacun de ces quatre cas, on a $u(n, k') \geq u(n, k)$.

□

4.1.2 Preuve du principe d'incertitude linéaire sur un groupe abélien fini

Démonstration du théorème 4.1.0.2. On montre par récurrence sur $n = |G|$ que :

$$\forall k \in [1, n], \Theta(G, k) \geq u(n, k),$$

car ceci implique le théorème. En effet, supposons que $\forall k \in [1, n],\ \Theta(G, k) \geq u(n, k)$ et soit $f : G \to \mathbb{C}$ non nulle. Par définition de Θ, on a : $|\text{supp}(\widehat{f})| \geq \Theta(G, |\text{supp}(f)|) \geq u(n, |\text{supp}(f)|)$.

D'abord, supposons que $n = p$ premier et montrons que et montrons que $\forall k \in [1, p], \Theta(G, k) \geq u(p, k)$. Soit $k \in [1, p]$, et $f : G \to \mathbb{C}$ non nulle telle que $|\text{supp}(\widehat{f})| \leq k$. Comme p est premier, on a :

$$d_1(p, k) = \begin{cases} 1 & \text{si } k < p \\ p & \text{si } k = p \end{cases}$$

$$d_2(p, k) = \begin{cases} 1 & \text{si } k = 1 \\ p & \text{si } k > 1 \end{cases}$$

Si $k = 1$, alors $|\mathrm{supp}(f)| = 1$ d'où par le théorème 3.1.2.1 :

$$|\mathrm{supp}(\widehat{f})| \geq p + 1 - 1 = \frac{p}{1 \times 1}(1 + 1 - 1).$$

Si $k \in]1, p[$, alors $1 \leq |\mathrm{supp}(f)| \leq k < p$, d'où par le théorème 3.1.2.1 :

$$|\mathrm{supp}(\widehat{f})| \geq p + 1 - |\mathrm{supp}(f)| = \frac{p}{1 \times p}(1 + p - |\mathrm{supp}(f)|) \geq \frac{p}{1 \times p}(1 + p - k).$$

Si $k = p$, alors $1 \leq |\mathrm{supp}(f)| \leq p$, d'où par le théorème 3.1.2.1 :

$$|\mathrm{supp}(\widehat{f})| \geq p + 1 - |\mathrm{supp}(f)| \geq 1 = \frac{p}{p \times p}(p + p - p).$$

D'où $\forall k \in [1, p], \Theta(G, k) \geq u(p, k)$.

Supposons maintenant que n n'est pas premier et que pour tout groupe G' de cardinal $|G'| = n' < n$ on a que $\forall k' \in [1, n'],\ \Theta(G', k') \geq u(n', k')$. Soit $k \in [1, n]$. Comme n n'est pas premier, il existe d un diviseur de n tel que $d \neq 1, n$. Comme G est abélien, par la réciproque au théorème de Lagrange il existe H un sous-groupe de G de cardinal $|H| = d$. En appliquant la proposition 4.1.1.1, il existe $s \in [1, d]$ et $t \in [1, \frac{n}{d}]$ tels que $st \leq k$ et $\Theta(G, k) \geq \Theta(H, s)\Theta(G/H, t)$. Or par hypothèse de récurrence, $\Theta(H, s) \geq u(d, s)$ et $\Theta(G/H, t) \geq u(\frac{n}{d}, t)$. On en conclut que :

$$\begin{aligned}
\Theta(G, k) &\geq u(d, s)u(\frac{n}{d}, t) \\
&\geq u(n, st) && \text{par la proposition 4.1.1.4} \\
&\geq u(n, k) && \text{par le lemme 4.1.1.5.}
\end{aligned}$$

□

4.2 Un principe d'incertitude sur $(\mathbb{Z}/k\mathbb{Z})^n$

Dans cette section, nous allons voir un nouveau principe d'incertitude découvert par Meshulam [7] sur $(\mathbb{Z}/k\mathbb{Z})^n$ pour un type de fonction particulier. Nous appliquerons ce principe

d'incertitude restreint à l'indicatrice d'un certain sous-groupe, nous donnant une autre preuve d'une estimation de la constante de Davenport.

Soit $k \geq 2$ un entier. Grâce à la proposition 3.1.1.2, en fixant $\zeta \in U_k$, la transformée de Fourier sur $(\mathbb{Z}/k\mathbb{Z})^n$ peut s'écrire :

$$\begin{aligned} \widehat{f} \colon (\mathbb{Z}/k\mathbb{Z})^n &\longrightarrow \mathbb{C} \\ x &\longmapsto \sum_{y \in (\mathbb{Z}/k\mathbb{Z})^n} f(y)\zeta^{-y.x} \end{aligned}$$

4.2.1 Le principe d'incertitude

Définition 4.2.1.1. *Posons par récurrence :* $\begin{cases} \alpha(k,0) & = 1 \\ \alpha(k,s) & = \lceil \alpha(k,s-1)\frac{k}{k-1} \rceil \text{ si } s \in \mathbb{N}^* \end{cases}$

Théorème 4.2.1.2. *Soit $f : (\mathbb{Z}/k\mathbb{Z})^n \to \mathbb{C}$ telle que $f(0) = 1$ et $\forall \varepsilon \in \{0,1\}^n \setminus \{0\},\ f(\varepsilon) = 0$. On a :*

$$|supp(\widehat{f})| \geq \alpha(k,n).$$

Commençons d'abord par deux petits lemmes qui nous serviront pour prouver le théorème 4.2.1.2.

Lemme 4.2.1.3. *$f : \mathbb{Z}/k\mathbb{Z} \to \mathbb{C}$ telle que $|supp(\widehat{f})| \leq 1$. Alors il existe $x_0 \in \mathbb{Z}/k\mathbb{Z}$ tel que $f(0) = f(1)\zeta^{-x_0}$.*

Démonstration. Comme $|\mathrm{supp}(\widehat{f})| \leq 1$, il existe $x_0 \in \mathbb{Z}/k\mathbb{Z}$ et $C \in \mathbb{C}$ tels que $\widehat{f} = C\mathbb{1}_{\{x_0\}}$. Or par la formule d'inversion de Fourier (3.1.1.4), on peut écrire :

$$g(\cdot) = \frac{1}{k} \sum_{y \in \mathbb{Z}/k\mathbb{Z}} C\mathbb{1}_{\{x_0\}}(\cdot)\zeta^{y\cdot} = \frac{C}{k}\zeta^{x_0\cdot}.$$

En évaluant en 0 et en 1, on en déduit que $g(0) = g(1)\zeta^{-x_0}$. □

Lemme 4.2.1.4. *Soient X un ensemble $A_1, \ldots, A_k \subseteq X$, et $u \in \mathbb{N}$ tels que $|A_i| \geq u$ pour*

tout $i \in [\![1,k]\!]$. *On a :*

$$|\bigcup_{i=1}^{k} A_i| + |\bigcap_{i=1}^{k} A_i| \geq \frac{ku}{k-1}.$$

Démonstration. Posons $v = |\bigcap_{i=1}^{k} A_i|$ et pour tout $i \in [\![1,k]\!]$, $B_i = A_i \setminus (\bigcap_{i=1}^{k} A_i)$, de sorte que $\bigcap_{i=1}^{k} B_i = \emptyset$.

D'une part

$$|\{(x,i) \in X \times [\![1,k]\!], x \in B_i\}| \geq \min\{\underbrace{|B_i|}_{\geq u-v}, i \in [\![1,k]\!]\}k \geq (u-v)k,$$

et d'autre part si un $x \in B_i$ pour un certain i, alors il ne peut appartenir au maximum à $k-1$ B_j car $\bigcap_{i=1}^{k} B_i = \emptyset$, donc

$$|\{(x,i) \in X \times [\![1,k]\!], x \in B_i\}| \leq |\bigcup_{i=1}^{k} B_i|(k-1),$$

ce qui nous permet d'écrire :

$$\begin{aligned} |\bigcup_{i=1}^{k} A_i| + |\bigcap_{i=1}^{k} A_i| &= |\bigcup_{i=1}^{k} B_i| + 2v \\ &\geq \frac{(u-v)k}{k-1} + 2v \\ &= \frac{ku}{k-1} + \frac{v(k-2)}{k-1} \qquad \geq \frac{ku}{k-1} \text{ par le lemme 4.2.1.4} \end{aligned}$$

□

On peut maintenant prouver le principe d'incertitude.

Démonstration du théorème 4.2.1.2. Montrons le théorème par récurrence sur $n \in \mathbb{N}^*$.

Soit $f : \mathbb{Z}/k\mathbb{Z} \to \mathbb{C}$ telle que $f(0) = 1$ et $f(1) = 0$. Par le lemme 4.2.1.3, on a que $|\mathrm{supp}(\widehat{f})| \geq 2$. De plus, $\alpha(k,1) = \lceil \alpha(k,0)\frac{k}{k-1} \rceil = \lceil \frac{k}{k-1} \rceil = 2$, ce qui donne bien $|\mathrm{supp}(\widehat{f})| \geq$

$\alpha(k,1)$.

Soit $n \geq 2$ un entier. Supposons que :

$$\forall g : (\mathbb{Z}/k\mathbb{Z})^{n-1} \to \mathbb{C}, (g(0) = 1 \text{ et } \forall \varepsilon \in \{0,1\}^{n-1} \setminus \{0\}\ g(\varepsilon) = 0) \implies |\mathrm{supp}(\widehat{g})| \geq \alpha(k, n-1).$$

Soit $f : (\mathbb{Z}/k\mathbb{Z})^n \to \mathbb{C}$ telle que $f(0) = 1$ et $\forall \varepsilon \in \{0,1\}^n \setminus \{0\},\ f(\varepsilon) = 0$. On pose pour tout $y \in \mathbb{Z}/k\mathbb{Z}$:

$$\begin{aligned} f_y \colon (\mathbb{Z}/k\mathbb{Z})^{n-1} &\longrightarrow \mathbb{C} \\ x &\longmapsto f(x,y), \end{aligned}$$

et pour tout $a \in (\mathbb{Z}/k\mathbb{Z})^{n-1}$:

$$\begin{aligned} g_a \colon \mathbb{Z}/k\mathbb{Z} &\longrightarrow \mathbb{C} \\ y &\longmapsto \widehat{f_y}(a), \end{aligned}$$

de sorte que :

$$\begin{aligned} \forall (a,b) \in (\mathbb{Z}/k\mathbb{Z})^{n-1} \times \mathbb{Z}/k\mathbb{Z},\ \widehat{f}(a,b) &= \sum_{x \in (\mathbb{Z}/k\mathbb{Z})^{n-1}} \sum_{y \in \mathbb{Z}/k\mathbb{Z}} f(x,y) \zeta^{-(x,y).(a,b)} \\ &= \sum_{y \in \mathbb{Z}/k\mathbb{Z}} \left(\sum_{x \in (\mathbb{Z}/k\mathbb{Z})^{n-1}} f_y(x) \zeta^{-x.a} \right) \zeta^{-yb} \\ &= \sum_{y \in \mathbb{Z}/k\mathbb{Z}} \widehat{f_y}(a) \zeta^{-yb} \\ &= \widehat{g_a}(b) \end{aligned}$$

On en déduit que $|\mathrm{supp}(\widehat{f})| = \sum_{a \in (\mathbb{Z}/k\mathbb{Z})^{n-1}} |\mathrm{supp}(\widehat{g_a})|$.

Posons pour tout $i \in [\![0, k-1]\!]$:

$$\begin{aligned} h_i \colon (\mathbb{Z}/k\mathbb{Z})^{n-1} &\longrightarrow \mathbb{C} \\ x &\longmapsto f_0(x) - \zeta^i f_1(x). \end{aligned}$$

Par hypothèse sur f, on a pour tout $i \in [\![0, k-1]\!]$: $h_i(0) = 1$ et $\forall \varepsilon \in \{0,1\}^{n-1} \setminus \{0\}$ $h_i(\varepsilon) = 0$, et donc

$$\forall i \in [\![0, k-1]\!] \ |\mathrm{supp}(\widehat{h_i})| \geq \alpha(k, n-1).$$

Or par linéarité de la transformée de Fourier, on a :

$$\forall i \in [\![0, k-1]\!] \ \mathrm{supp}(\widehat{h_i}) = \{a \in (\mathbb{Z}/k\mathbb{Z})^{n-1}, g_a(0) \neq \zeta^i g_a(1)\}.$$

On remarque que pour un $a \in (\mathbb{Z}/k\mathbb{Z})^{n-1}$, s'il existe $i \in [\![0, k-1]\!]$ tel que $a \in \mathrm{supp}(\widehat{h_i})$ alors $g_a \neq 0$ et donc par la formule d'inversion de Fourier $|\mathrm{supp}(\widehat{g_a})| \geq 1$.

Également, pour un $a \in (\mathbb{Z}/k\mathbb{Z})^{n-1}$, si $a \in \bigcap_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})$ alors g_a n'est pas de la forme $C\zeta^{-\cdot y_0}$ pour un $C \in \mathbb{C}$ et $y_0 \in \mathbb{Z}/k\mathbb{Z}$. En effet, si c'était le cas, on aurait $g_a(0) = \zeta^{y_0} g_a(0)$ et donc $a \notin \mathrm{supp}(\widehat{h_{y_0}})$. Par le lemme 4.2.1.3, on a donc $|\mathrm{supp}(\widehat{g_a})| \geq 2$.

Au final :

$$\begin{aligned} |\mathrm{supp}(\widehat{f})| &= \sum_{a \in (\mathbb{Z}/k\mathbb{Z})^{n-1}} |\mathrm{supp}(\widehat{g_a})| \\ &\geq \sum_{a \in (\bigcup_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})) \setminus (\bigcap_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i}))} \underbrace{|\mathrm{supp}(\widehat{g_a})|}_{\geq 1} + \sum_{a \in \bigcap_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})} \underbrace{|\mathrm{supp}(\widehat{g_a})|}_{\geq 2} \\ &\geq |(\bigcup_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})) \setminus (\bigcap_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})| + 2|\bigcap_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})| \\ &\geq |\bigcup_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i}))| + |\bigcap_{i=0}^{k-1} \mathrm{supp}(\widehat{h_i})| \\ &\geq \frac{k\alpha(k, n-1)}{k-1}, \end{aligned}$$

et on en conclut que $|\mathrm{supp}(\widehat{f})| \geq \alpha(k, n)$. □

On termine avec un corollaire de ce principe d'incertitude.

Corollaire 4.2.1.5. *Soit $f : (\mathbb{Z}/k\mathbb{Z})^n \to \mathbb{C}$. Supposons que $n \geq k-1$ et que $f(0) = 1$ et $\forall \varepsilon \in \{0,1\}^n \setminus \{0\},\ f(\varepsilon) = 0$. On a :*

$$|supp(\widehat{f})| \geq \frac{k}{e}\left(\frac{k}{k-1}\right)^n.$$

Démonstration. Par le théorème 4.2.1.2 on a que : $|\mathrm{supp}(\widehat{f})| \geq \alpha(k,n)$. Or par définition de α, comme $n \geq k-1$, une rapide récurrence donne :

$$\alpha(k,n) \geq \alpha(k,k-1)\left(\frac{k}{k-1}\right)^{n-(k-1)}.$$

Montrons que $\alpha(k,k-1) = k$. Par définition, on a :

$$\alpha(k,k-1) = \left\lceil \left\lceil \left\lceil \dots \left\lceil \alpha(k,2)\frac{k}{k-1} \right\rceil \dots \right\rceil \frac{k}{k-1} \right\rceil \frac{k}{k-1} \right\rceil,$$

où il y a $k-2$ $\lceil\cdot\rceil$ dans l'expression précédente. Or à l'intérieur du crochet $j \in [\![1, k-2]\!]$, on a par récurrence $\left\lceil \frac{(j+1)k}{k-1} \right\rceil = j+2$ car $\frac{(j+1)k}{k-1} = j+1+\underbrace{\frac{j+1}{k-1}}_{\leq 1}$. Au final, on obtient que

$$|\mathrm{supp}(\widehat{f})| \geq k\left(\frac{k}{k-1}\right)^{n-(k-1)},$$

et comme $\ln\left(1+\frac{1}{k-1}\right) \leq \frac{1}{k-1}$ et donc $\left(\frac{k}{k-1}\right)^{k-1} \leq e$, on conclut que

$$|\mathrm{supp}(\widehat{f})| \geq \frac{k}{e}\left(\frac{k}{k-1}\right)^n.$$

□

4.2.2 Une application pour la constante de Davenport

Définition 4.2.2.1 (Constante de Davenport)**.** *Posons $s(G)$ le plus grand entier non nul tel qu'il existe une famille $(a_1, \dots, a_s) \in G^s$ vérifiant que toutes les sous-sommes de la famille*

soient non nulles, autrement dit :

$$\begin{aligned} s(G) &= \max\{s \in \mathbb{N}^*, \exists (a_1, \ldots, a_s) \in G^s, \forall I \subseteq [\![1, s]\!] \text{ non vide}, \sum_{i \in I} a_i \neq 0\} \\ &= \min\{s \in \mathbb{N}^*, \forall (a_1, \ldots, a_s) \in G^s, \exists I \subseteq [\![1, s]\!] \text{ non vide}, \sum_{i \in I} a_i = 0\} - 1, \end{aligned}$$

cette constante est appelée constante de Davenport.

Cette constante est connu dans certains cas particuliers. Par exemple, si G est un $p-groupe$, où ses invariants sont notés $p^{e_1}, \ldots, p^{e_r}$, Olson [12] a montré que $s(G) = \sum_{i=1}^{r}(p^{e_i}-1)$. Ici, nous donnons une majoration de $s(G)$ en utilisant la transformation de Fourier, pour G un groupe abélien fini quelconque. L'intérêt de cette preuve de la majoration suivante est la méthode utilisée, pour sa potentielle adaptabilité pour trouver une autre majoration de la constante de Davenport.

Théorème 4.2.2.2. *Posons $m = \max\{ord(x), x \in G\} = exp(G)$. On a la majoration :*

$$s(G) \leq m\left(1 + \ln\left(\frac{|G|}{m}\right)\right).$$

Cette estimation déjà obtenue en 1969 a permis notamment à Alford, Granville et Pomerance [1] de montrer qu'il existe une infinité de nombres de Carmichael, c'est-à-dire des entiers n non premiers vérifiant la propriété du petit théorème de Fermat : pour tout $a \in \mathbb{N}$, $a^n \equiv a[n]$.

Démonstration. L'idée est d'appliquer le corollaire 4.2.1.5 du principe d'incertitude à l'indicatrice de l'orthogonal d'un sous-groupe bien choisi (de cardinal inférieur à $|G|$) de $(\mathbb{Z}/m\mathbb{Z})^{s(G)}$. L'inégalité du corollaire 4.2.1.5 nous donnera le résultat.

Posons $s = s(G)$ pour simplifier les notations. Comme G est un groupe abélien fini, il existe $n \in \mathbb{N}^*$ et $m_1, \ldots, m_n \geq 2$ des entiers tels que :

$$G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z},$$

avec $m_{i+1}|m_i$ pour tout $i \in [\![1, n-1]\!]$, et $m_1 = m$. En particulier, pour tout $i \in [\![1, n]\!]$ $m_i|m$.

Par définition de s, il existe $(a_1, \ldots, a_s) \in G^s$ tel que :

$$\forall (\varepsilon_1, \ldots, \varepsilon_s) \in \{0,1\}^s \setminus \{0\} \ \sum_{i=1}^{s} \varepsilon_i a_i \neq 0.$$

On écrit pour chaque $i \in [\![1, s]\!]$ $a_i = (a_{i1}, \ldots, a_{in})$, où pour tout $j \in [\![1, n]\!]$ $a_{ij} \in [\![0, m_j - 1]\!]$.

Pour tout $j \in [\![1, n]\!]$, on pose $b_j = \frac{m}{m_j}(a_{1j}, \ldots, a_{sj}) \in (\mathbb{Z}/m\mathbb{Z})^s$. Posons $H =< b_1, \ldots, b_n >$ le sous-groupe de $(\mathbb{Z}/m\mathbb{Z})^s$ engendré par les b_j. Par définition, pour tout $j \in [\![1, n]\!]$, $ord(b_j) \leq m_j$, et donc $|H| \leq m_1 \ldots m_n = |G|$.

Décrivons les éléments de l'orthogonal de H :

$$\begin{aligned}
H^\perp &= \{(\varepsilon_1, \ldots, \varepsilon_s) \in (\mathbb{Z}/m\mathbb{Z})^s, \forall (h_1, \ldots, h_s) \in H \ \sum_{i=1}^{s} h_i \varepsilon_i = 0\} \\
&= \{(\varepsilon_1, \ldots, \varepsilon_s) \in (\mathbb{Z}/m\mathbb{Z})^s, \forall j \in [\![1, n]\!] \ \sum_{i=1}^{s} \frac{m}{m_j} a_{ij} \varepsilon_i = 0\} \\
&= \{(\varepsilon_1, \ldots, \varepsilon_s) \in (\mathbb{Z}/m\mathbb{Z})^s, \forall j \in [\![1, n]\!] \ \sum_{i=1}^{s} a_{ij} \varepsilon_i = 0\} \\
&= \{(\varepsilon_1, \ldots, \varepsilon_s) \in (\mathbb{Z}/m\mathbb{Z})^s, \ \sum_{i=1}^{s} a_i \varepsilon_i = 0\},
\end{aligned}$$

ce qui nous donne par choix de $(a_1, \ldots, a_s)$ que $H^\perp \cap \{0,1\}^s = \{0\}$. On en conclut que $\mathbb{1}_{H^\perp} : (\mathbb{Z}/m\mathbb{Z})^s \to \mathbb{C}$ vérifie bien les hypothèses du théorème 4.2.1.2.

Cependant pour appliquer le corollaire 4.2.1.5, il reste à vérifier que $s \geq m-1$. Comme $m = exp(G)$, il existe $a \in G$ d'ordre l'exposant de G. L'élément de $(a, \ldots, a) \in G^{m-1}$ vérifie que pour tout $I \subseteq [\![1, m-1]\!]$ non vide, $\sum_{i \in I} a = |I|a \neq 0$ car $1 \leq |I| \leq m-1 = ord(a) - 1$. On a donc bien que $m - 1 \leq s$.

On peut alors appliquer le corollaire 4.2.1.5 à $\mathbb{1}_{H^\perp}$, ce qui donne :

$$|\mathrm{supp}(\widehat{\mathbb{1}_{H^\perp}})| \geq \frac{m}{e}\left(\frac{m}{m-1}\right)^s.$$

Or la proposition 3.1.1.7 et le fait $H^{\perp\perp} = H$ (3.1.1.6) impliquent que

$$|\mathrm{supp}(\widehat{\mathbb{1}_{H^\perp}})| = |H| \leq |G|.$$

On en déduit que $\frac{m}{e}\left(\frac{m}{m-1}\right)^s \leq |G|$, et donc en réarrangeant que :

$$s \leq \frac{1+\ln(\frac{|G|}{m})}{\ln\left(\frac{m}{m-1}\right)}.$$

Enfin, on a l'inégalité de convexité $\forall x > 0$, $x < \ln(1+x)(1+x)$, ce qui donne en $x = \frac{1}{m-1}$ que $\ln\left(1+\frac{1}{m-1}\right) > \frac{1}{m}$ et donc $\frac{1}{\ln\left(\frac{m}{m-1}\right)} < m$. On en conclut finalement que

$$s \leq m\left(1+\ln\left(\frac{|G|}{m}\right)\right).$$

□

5 Généralisation du premier principe d'incertitude pour les groupes non abéliens, cas du groupe non abélien à pq éléments

5.1 Définitions généralisées

Soit G un groupe fini, potentiellement non abélien. Rappelons que la définition 3.1.1.3 de la transformée de Fourier d'une fonction définie sur un groupe abélien fait intervenir les caractères de ce groupe. Dans le cas d'un groupe abélien, les seules représentations irréductibles étant celles de degré 1, c'est-à-dire les caractères, une généralisation naturelle de la définition de la transformée de Fourier serait de définir cette dernière sur l'ensemble des représentations

complexes irréductibles (à isomorphisme près), noté $Irr(G)$. Le but de cette section est de voir comment Meshulam a montré dans [8] un équivalent du principe d'incertitude de Donoho et Stark 3.1.1.10 pour les groupes non abéliens.

Définition 5.1.0.1. *Soit $f : G \to \mathbb{C}$. On définit la transformée de Fourier de f pour toute représentation complexe irréductible $\rho : G \to GL(V)$, où V est l'espace vectoriel associé à la représentation, par :*

$$\widehat{f}(\rho) = \sum_{x \in G} f(x)\rho(x) \in \mathcal{L}(V).$$

Définition 5.1.0.2. *Soit $f : G \to \mathbb{C}$. On définit de la même manière que dans le cas abélien 3.1.1.5, le support de $\widehat{f}$ par :*

$$supp(\widehat{f}) = \{\rho \in Irr(G), \widehat{f}(\rho) \neq 0\}.$$

A la différence du cas abélien, nous n'utiliserons par le cardinal du support de la transformée de Fourier comme mesure sur le support de la transformée de Fourier, mais les quantités suivantes :

Définition 5.1.0.3. *Soit $f : G \to \mathbb{C}$. On pose :*

$$\mu(f) = \sum_{(\rho,V) \in Irr(G)} \dim(V) rg\left(\widehat{f}(\rho)\right),$$

$$\tilde{\mu}(f) = \sum_{(\rho,V) \in Irr(G)} \dim(V) \mathbb{1}_{supp(\widehat{f})}(\rho).$$

Pour plus d'explications sur cette nouvelle notion de support, on peut lire l'article de Wigderson et Wigderson [17]. Ces derniers montrent également le raffinement suivant du théorème 5.2.0.1 :

Théorème 5.1.0.4. *Pour toute fonction $f : G \to \mathbb{C}$ non nulle, on a :*

$$|supp(f)|\mu(f) \geq \frac{|G|}{4}.$$

Remarque. *Supposons G abélien. Dans ce cas, pour toute fonction $f : G \to \mathbb{C}$, on a $|supp\widehat{f}| = \mu(f) = \tilde{\mu}(f)$.*

Soit $f : G \to \mathbb{C}$. En effet, comme toute représentation irréductible de G est de degré 1, on a :

$$\mu(f) = \sum_{(\rho,V)\in Irr(G)} \underbrace{\dim(V)}_{=1} \underbrace{rg\left(\widehat{f}(\rho)\right)}_{=\begin{cases}1 \ si \ \widehat{f}(\rho) \neq 0\\ 0 \ si \ \widehat{f}(\rho) = 0\end{cases}} = |supp\widehat{f}|,$$

et de la même manière, $\tilde{\mu}(f) = |supp\widehat{f}|$.

Nous pouvons d'abord constater qu'on a l'encadrement suivant :

Lemme 5.1.0.5. *Pour toute $f : G \to \mathbb{C}$, on a : $\tilde{\mu}(f) \leq \mu(f) \leq (\tilde{\mu}(f))^2$.*

Démonstration. Soit $f : G \to \mathbb{C}$. D'une part,

$$\begin{aligned}\tilde{\mu}(f) &= \sum_{(\rho,V)\in Irr(G)} \dim(V) \underbrace{\mathbb{1}_{\mathrm{supp}(\widehat{f})}(\rho)}_{\leq\begin{cases}0 = \mathrm{rg}\widehat{f}(\rho) & \text{si } \widehat{f}(\rho) = 0\\ \mathrm{rg}\widehat{f}(\rho) & \text{si } \widehat{f}(\rho) \neq 0\end{cases}}\\ &\leq \sum_{(\rho,V)\in Irr(G)} \dim(V)\mathrm{rg}\left(\widehat{f}(\rho)\right)\\ &= \mu(f),\end{aligned}$$

et d'autre part,

$$\begin{aligned}
\mu(f) &= \sum_{(\rho,V)\in Irr(G)} \dim(V) \underbrace{\operatorname{rg}\left(\widehat{f}(\rho)\right)}_{\leq \dim V} \mathbb{1}_{\operatorname{supp}(\widehat{f})}(\rho) \\
&\leq \sum_{(\rho,V)\in Irr(G)} (\dim(V))^2 \mathbb{1}_{\operatorname{supp}(\widehat{f})}(\rho) \\
&\leq \left(\sum_{(\rho,V)\in Irr(G)} \dim(V) \mathbb{1}_{\operatorname{supp}(\widehat{f})}(\rho) \right)^2 \\
&= (\tilde{\mu}(f))^2.
\end{aligned}$$

□

Une manière alternative de comprendre $\mu(f)$ pour $f : G \to \mathbb{C}$ est de voir cette quantité comme le rang de l'application de multiplication par l'élément $\sum_{x\in G} f(x)x \in \mathbb{C}[G]$, la $\mathbb{C}$-algèbre de G.

Définition 5.1.0.6. *Pour toute $f : G \to \mathbb{C}$, posons $u = \sum_{x\in G} f(x)x \in \mathbb{C}[G]$. On définit l'application :*

$$\begin{aligned}
T_f \colon \mathbb{C}[G] &\longrightarrow \mathbb{C}[G] \\
v = \sum_{x\in G} v(x)x &\longmapsto uv = \sum_{x\in G} \left(\sum_{\substack{s,t\in G \\ st=x}} u(s)v(t) \right) x
\end{aligned}$$

Proposition 5.1.0.7. *Pour toute $f : G \to \mathbb{C}$, on a $\mu(f) = rg(T_f)$.*

Démonstration. Soit $f : G \to \mathbb{C}$. Notons $(\rho_1, V_1), \ldots, (\rho_m, V_m)$ les éléments de $Irr(G)$.

Posons

$$\begin{aligned}\varphi\colon \mathbb{C}[G] &\longrightarrow \mathcal{L}(V_1)\times\ldots\times\mathcal{L}(V_m)\\ \sum_{x\in G} h(x)x &\longmapsto (\widehat{h}(\rho_1),\ldots,\widehat{h}(\rho_m)),\end{aligned}$$

et

$$\begin{aligned}S\colon \mathcal{L}(V_1)\times\ldots\times\mathcal{L}(V_m) &\longrightarrow \mathcal{L}(V_1)\times\ldots\times\mathcal{L}(V_m)\\ (A_1,\ldots,A_m) &\longmapsto (\widehat{f}(\rho_1)\circ A_1,\ldots,\widehat{f}(\rho_m)\circ A_m).\end{aligned}$$

D'après [14], φ est un isomorphisme. En montrant que $S\circ\varphi=\varphi\circ T_f$, on en déduira que $\mathrm{rg}(S)=\mathrm{rg}(T_f)$. Enfin, nous verrons que $\mathrm{rg}(S)=\mu(f)$, ce qui nous permettra de conclure la proposition.

Montrons que $S\circ\varphi=\varphi\circ T_f$. Soit $h=\sum_{x\in G}h(x)x\in\mathbb{C}[G]$. On a d'un côté $\varphi(h)=(\widehat{h}(\rho_1),\ldots,\widehat{h}(\rho_m))$, donc $S(\varphi(h))=(\widehat{f}(\rho_1)\circ\widehat{h}(\rho_1),\ldots,\widehat{f}(\rho_m)\circ\widehat{h}(\rho_m))$. De l'autre côté, on a : $T_f(h)=\sum_{x\in G}\left(\sum_{\substack{s,t\in G\\ st=x}} f(s)h(t)\right)x=\sum_{x\in G}(f*h)(x)x$, donc :

$$\varphi(T_f(h))=(\widehat{f*h}(\rho_1),\ldots,\widehat{f*h}(\rho_m))=(\widehat{f}(\rho_1)\circ\widehat{h}(\rho_1),\ldots,\widehat{f}(\rho_m)\circ\widehat{h}(\rho_m))=S(\varphi(h)).$$

Comme φ est un isomorphisme, on en déduit que $\mathrm{rg}(S)=\mathrm{rg}(T_f)$.

Enfin, il reste à voir que $\mathrm{rg}(S) = \mu(f)$. On a :

$$\begin{aligned}
\mathrm{rg}(S) &= \dim Im(S) \\
&= \dim\{(\widehat{f}(\rho_1)\circ A_1, \ldots, \widehat{f}(\rho_m)\circ A_m), (A_1,\ldots,A_m) \in \mathcal{L}(V_1)\times\ldots\times\mathcal{L}(V_m)\} \\
&= \sum_{i=1}^{m} \dim \underbrace{\{\widehat{f}(\rho_i)\circ A_i, A_i \in \mathcal{L}(V_i)\}}_{\mathcal{L}(V_i, Im(\widehat{f}(\rho_i)))} \\
&= \sum_{i=1}^{m} \mathrm{rg}(\widehat{f}(\rho_i))\dim(V_i) \\
&= \mu(f).
\end{aligned}$$

Au final, on a bien montré que $\mathrm{rg}(T_f) = \mu(f)$.

□

5.2 Généralisation du premier principe d'incertitude

Nous pouvons maintenant voir une généralisation du premier principe d'incertitude 3.1.1.10 à un groupe non abélien.

Théorème 5.2.0.1 ([8])**.** *Pour toute $f : G \to \mathbb{C}$ non nulle, on a $|supp(f)|\mu(f) \geq |G|$. Si de plus on suppose $f(1) = 1$, alors sont équivalentes :*

- *$|supp(f)|\mu(f) = |G|$*
- *$supp(f)$ est un sous-groupe de G et il existe χ un caractère de $supp(f)$ tel que $f = \mathbb{1}_{supp(f)}\chi$.*

Démonstration. Pour simplifier les notations, posons $A = \mathrm{supp}(f)$.

Montrons d'abord que $\mu(f)|A| \geq |G|$. Posons t le plus grand entier tel qu'il existe un t-uplet $(g_1, \ldots, g_t)$ d'éléments de G vérifiant que chaque Ag_i n'est pas inclus dans l'union des

Ag_j précédents, c'est-à-dire :

$$t = \max\left\{ s \in [\![1, |G|]\!], \exists (g_1, \ldots, g_s) \in G^s, \forall i \in [\![2, s]\!], Ag_i \not\subseteq \bigcup_{j<i} Ag_j \right\}.$$

Par définition, il existe $(g_1, \ldots, g_t) \in G^t$ tel que pour tout $i \in [\![2, t]\!]$ $Ag_i \not\subseteq \bigcup_{j<i} Ag_j$.

Montrons que $(T_f(g_1), \ldots, T_f(g_t))$ est libre dans $\mathbb{C}[G]$. On a :

$$\forall i \in [\![1, t]\!], T_f(g_i) = \sum_{x \in G} \left(\sum_{\substack{s,t \in G \\ st = x}} f(s) \mathbb{1}_{\{g_i\}}(t) \right) x = \sum_{x \in G} f(x {g_i}^{-1}) x.$$

Soient $\lambda_1, \ldots, \lambda_t \in \mathbb{C}$ et supposons que $\sum_{i=1}^{t} \lambda_i T_f(g_i) = 0$. On a donc $\sum_{x \in G} (\lambda_1 f(x {g_1}^{-1}) + \ldots + \lambda_t f(x {g_t}^{-1}))x = 0$, autrement dit pour tout $x \in G$ $\lambda_1 f(x {g_1}^{-1}) + \ldots + \lambda_t f(x {g_t}^{-1}) = 0$. Or comme $Ag_t \not\subseteq \bigcup_{j<t} Ag_j$, il existe $x_t \in Ag_t$ tel que $x_t \notin \bigcup_{1 \leq i < t} Ag_i$. Par définition $A = \mathrm{supp}(f)$, donc on a $f(x_t g_t^{-1}) \neq 0$ et pour tout $i \in [\![1, t-1]\!]$ $f(x_t g_i^{-1}) = 0$. Au final, on obtient que :

$$\lambda_1 \underbrace{f(x_t {g_1}^{-1})}_{=0} + \ldots + \lambda_{t-1} \underbrace{f(x_t {g_{t-1}}^{-1})}_{=0} + \lambda_t \underbrace{f(x_t {g_t}^{-1})}_{\neq 0} = 0,$$

d'où $\lambda_t = 0$, et donc pour tout $x \in G$ avec $\lambda_1 f(x {g_1}^{-1}) + \ldots + \lambda_{t-1} f(x {g_{t-1}}^{-1}) = 0$. On réitère le processus en utilisant le fait $Ag_{t-1} \not\subseteq \bigcup_{1 \leq i < t-1} Ag_i$, ce qui implique que $\lambda_{t-1} = 0$. Par récurrence, on obtient que $\lambda_t = \ldots = \lambda_2 = 0$. Enfin, comme $A = \mathrm{supp}(f) \neq \emptyset$ alors $Ag_1 \neq \emptyset$ et donc $\lambda_1 = 0$. Au final, $\lambda_1 = \lambda_= \ldots = \lambda_t = 0$.

La famille $(T_f(g_1), \ldots, T_f(g_t))$ étant libre dans $\mathbb{C}[G]$, on en déduit que $\mathrm{rg}(T_f) \geq t$, d'où d'après la proposition 5.1.0.7, $\mu(f) = \mathrm{rg}(T_f) \geq t$.

Montrons maintenant que $\bigcup_{i=1}^{t} Ag_i = G$.

Cas 1 : si $t < |G|$. Supposons par l'absurde qu'il existe $g \in G$ tel que $g \notin \bigcup_{i=1}^{t} Ag_i$. On cherche un $g_{t+1} \in G$ tel que $Ag_{t+1} \not\subseteq \bigcup_{i=1}^{t} Ag_i$, de sorte de contredire la maximalité de t. Comme $A \neq \emptyset$, il existe $x \in A$, et donc en posant $g_{t+1} = x^{-1}g$, on a bien $xg_{t+1} =$

$g \notin \bigcup_{i=1}^{t} Ag_i$. La famille $(g_1, \ldots, g_t, g_{t+1})$ vérifie alors que pour tout $i \in [\![2, t+1]\!]$ $Ag_i \not\subseteq \bigcup_{j<i} Ag_j$, ce qui contredit la maximalité de t.

Cas 2 : si $t = |G|$. Premièrement, comme A est non vide, on a $|Ag_1| \geq 1$. Or comme $Ag_2 \not\subseteq Ag_1$, on voit que $|Ag_1 \cup Ag_2| \geq |Ag_1| + 1 \geq 2$. De la même manière, comme $Ag_3 \not\subseteq Ag_2 \cup Ag_1$, on a $|Ag_1 \cup Ag_2 \cup Ag_3| \geq |Ag_1 \cup Ag_2| + 1 \geq 3$. Par récurrence, comme $Ag_t \not\subseteq Ag_1 \cup \ldots \cup Ag_{t-1}$, on en conclut que $|\bigcup_{i=1}^{t} Ag_i| \geq t = |G|$. Or comme $\bigcup_{i=1}^{t} Ag_i \subseteq G$, on en conclut par cardinalité que $\bigcup_{i=1}^{t} Ag_i = G$.

Dans tous les cas $\bigcup_{i=1}^{t} Ag_i = G$.

Enfin, $|G| = |\bigcup_{i=1}^{t} Ag_i| \leq \sum_{i=1}^{t} |Ag_i| = |A|t$, et donc en combinant avec le fait que $\mu(f) \geq t$, on en conclut que $\mu(f) \geq \frac{|G|}{|A|}$, autrement dit $\mu(f)|\mathrm{supp}(f)| \geq |G|$.

Supposons maintenant que $f(1) = 1$.

Dans un sens, posons $H = \mathrm{supp}(f)$ puis supposons que H est un sous-groupe de $|G|$ et qu'il existe $\chi \in \widehat{H}$ tel que $f = \mathbb{1}_H \chi$. Posons $l = [G : H]$, et écrivons $G = \bigsqcup_{i=1}^{l} Hg_i$, avec $(g_1, \ldots, g_l) \in G^l$. Il suffit de montrer que $(T_f(g_1), \ldots, T_f(g_l))$ forme une base de $Im(T_f) \subseteq \mathbb{C}[G]$. En effet, on aura alors par la proposition 5.1.0.7, $\mu(f) = \mathrm{rg}(T_f) = l = \frac{|G|}{|H|}$, d'où $|\mathrm{supp}(f)|\mu(f) = |G|$.

Montrons que $(T_f(g_1), \ldots, T_f(g_l))$ est libre. Comme $G = \bigsqcup_{i=1}^{l} Hg_i$, en particulier on a pour tout $i \in [\![2, l]\!]$ $Hg_i \not\subseteq \bigcup_{j<i} Hg_j$, et donc par le même raisonnement que précédemment, on conclut que la famille est libre.

Montrons que $(T_f(g_1), \ldots, T_f(g_l))$ est une famille génératrice $Im(T_f)$. Soit $v = \sum_{x \in G} v(x)x \in Im(T_f) \subseteq \mathbb{C}[G]$. On cherche $\lambda_1, \ldots, \lambda_l \in \mathbb{C}$ tels que $v = \sum_{i=1}^{l} \lambda_i T_f(g_i)$ i.e. tels que

$$\forall x \in G, v(x) = \sum_{i=0}^{l} \lambda_i f(x g_i^{-1}).$$

On raisonne par analyse-synthèse pour trouver $\lambda_1, \ldots, \lambda_l$.

Analyse : Supposons qu'il existe de tels $\lambda_1, \ldots, \lambda_l$. Soit $i \in [\![1, l]\!]$. Comme $1 \in H$, on a $g_i \in Hg_i$, et donc :

$$v(g_i) = \sum_{j=1}^{l} \lambda_j f(g_i g_j^{-1}) = \lambda_i f(1) + \sum_{\substack{j=1 \\ j \neq i}}^{l} \lambda_j f(g_i g_j^{-1}).$$

Comme $f(1) = 1$ et que pour tout $j \neq i$, $f(g_i g_j^{-1}) = \mathbb{1}_H(g_i g_j^{-1})\chi(g_i g_j^{-1}) = 0$ (car les classes sont disjointes), on obtient que $v(g_i) = \lambda_i$.

Synthèse : Montrons que $\forall x \in G, v(x) = \sum_{i=1}^{l} v(g_i) f(x g_i^{-1})$. Soit $x \in G$. Comme $G = \bigsqcup_{i=1}^{l} Hg_i$, il existe un unique $i \in [\![1, l]\!]$ tel que $x \in Hg_i$, et donc il existe $h \in H$ tel que x s'écrive comme $x = hg_i$. Or comme $v \in \mathrm{Im}(T_f)$, il existe $v_0 \in \mathbb{C}[G]$ tel que $v = uv_0$. On a :

$$\sum_{j=1}^{l} v(g_j) f(x g_j^{-1}) = \sum_{i=j}^{l} v(g_j) f(h g_i g_j^{-1}) = v(g_i) f(h) + \sum_{\substack{j=1 \\ j \neq i}}^{l} v(g_j) \underbrace{f(h g_i g_j^{-1})}_{=0},$$

et comme $f = \mathbb{1}_H \chi$,

$$\sum_{j=1}^{l} v(g_j) f(x g_j^{-1}) = v(g_i)\chi(h).$$

Pour montrer le résultat, il suffit donc de montrer que $v(hg_i) = v(g_i)\chi(h)$. Or comme $v = uv_0$, on a $v(x) = \sum_{\substack{s,t \in G \\ st = x}} f(s) v_0(t) = \sum_{\substack{s,t \in G \\ st = x}} \mathbb{1}_H(s)\chi(s) v_0(t)$. Il suffit alors de montrer que $\sum_{\substack{s,t \in G \\ st = hg_i}} \mathbb{1}_H(s)\chi(s) v_0(t) = \sum_{\substack{s,t \in G \\ st = g_i}} \mathbb{1}_H(s)\chi(s) v_0(t) \times \chi(h)$. Et effectivement, on a :

$$\begin{aligned}
\sum_{\substack{s,t \in G \\ st = hg_i}} \mathbb{1}_H(s)\chi(s) v_0(t) &= \sum_{s \in G} \mathbb{1}_H(s)\chi(s) v_0(s^{-1} h g_i) \\
&= \sum_{s \in G} \underbrace{\mathbb{1}_H(hs)}_{hs \in H \iff s \in H} \chi(hs) v_0(s^{-1} g_i) \\
&= \sum_{s \in G} \mathbb{1}_H(s)\chi(h)\chi(s) v_0(s^{-1} g_i) \\
&= \sum_{\substack{s,t \in G \\ st = g_i}} \mathbb{1}_H(s)\chi(s) v_0(t) \times \chi(h).
\end{aligned}$$

On a bien montré que $(T_f(g_1), \ldots, T_f(g_l))$ est une famille génératrice $Im(T_f)$.

Réciproquement, posons $A = \text{supp}(f)$ et supposons que $\mu(f) = \frac{|G|}{|A|}$. Montrons que A est un sous-groupe de G et que pour tous $x, y \in A, f(xy) = f(x)f(y)$.

Reposons comme précédemment

$$t = \max\left\{ s \in [\![1, |G|]\!], \exists (g_1, \ldots, g_s) \in G^s, \forall i \in [\![2, s]\!], Ag_i \not\subseteq \bigcup_{j<i} Ag_j \right\}.$$

On a montré que $\mu(f) \geq t \geq \frac{|G|}{|A|}$, et donc combiné avec notre hypothèse on en déduit que $t = \frac{|G|}{|A|}$.

Montrons d'abord que pour tout $g \in G$, ou bien $Ag = A$ ou bien $Ag \cap A = \emptyset$. Supposons par l'absurde qu'il existe $g \in G$ tel que $Ag \cap A \neq \emptyset$ et tel que $Ag \neq A$. On a alors $0 < |Ag \cap A| < A$. Posons

$$r = \max\left\{ s \in [\![2, |G|]\!], \exists (g'_1, \ldots, g'_s) \in G^s, g'_1 = 1, g'_2 = g, \forall i \in [\![2, s]\!], Ag'_i \not\subseteq \bigcup_{j<i} Ag'_j \right\}.$$

L'ensemble sous-jacent est bien non vide car $(1, g)$ vérifie $Ag \not\subseteq A$ (en effet sinon $Ag \cap A = Ag$ d'où $|Ag \cap A| = |A|$ ce qui serait absurde). Par définition de r, on a $t \geq r$ et $r \geq 2$. Posons $(g'_1, \ldots, g'_r) \in G^r$ tel que $g'_1 = 1, g'_2 = g$ et pour tout $i \in [\![2, r]\!], Ag'_i \not\subseteq \bigcup_{j<i} Ag'_j$. Par la même preuve qu'on a fait précédemment, on a $\bigcup_{i=1}^{r} Ag'_i = G$. On en déduit que :

$$\begin{aligned}
|G| &\leq \underbrace{|A \cup Ag|}_{=|A|+|Ag|-|A\cap Ag|} + |\bigcup_{i=3}^{r} Ag'_i| \\
&\leq 2|A| - |A \cap Ag| + (r-2)|A| \\
&= r|A| - |A \cap Ag| \\
&< r|A| \text{ car } 0 < |Ag \cap A|.
\end{aligned}$$

On en conclut que $t \geq r > \frac{|G|}{|A|}$, ce qui est absurde.

Déduisons-en que A est un sous-groupe de G. Soient $a, b \in A$. On a $a \in Ab^{-1}a \cap A$,

donc par ce qui précède $Ab^{-1}a = A$. Or $1 \in A$ (car $f(1) = 1$), donc $b^{-1}a \in A$, ce qui prouve que A est bien un sous-groupe de G.

Montrons maintenant la deuxième partie de l'assertion. Comme on a montré que A est un sous-groupe de G, il existe $(g_1 = 1, g_2, \ldots, g_l) \in G^l$ tel que $G = \bigsqcup_{i=1}^{l} Ag_i$. Posons pour tout $i \in [\![1, l]\!]$:

$$\mathcal{U}_i = \mathbb{C}[A].g_i = \{ug_i, u = \sum_{x \in A} u(x)x \in \mathbb{C}[A]\}.$$

Vérifions d'abord que pour tout $i \in [\![1, l]\!]$ $\mathcal{U}_i$ est stable sous T_f. Soit $i \in [\![1, l]\!]$ et $v \in \mathbb{C}[A]$. On a

$$T_f(vg_i) = \left(\sum_{x \in G} f(x)x\right)\left(\sum_{x \in A} v(x)x\right) g_i = \sum_{x \in G} \left(\underbrace{\sum_{\substack{s,t \in G \\ st = x}} f(s)v(t)\mathbb{1}_A(t)}_{:= h(x)} \right) xg_i.$$

Or si $x \notin A$, $h(x) = \sum_{t \in A} \underbrace{f(xt^{-1})}_{=0 \text{ car } At = A} v(t) = 0$, et on a bien que $T_f(vg_i) \in \mathcal{U}_i$.

Montrons maintenant que $\mathbb{C}[G] = \bigoplus_{i=1}^{l} \mathcal{U}_i$. Soit $v \in \mathbb{C}[G]$. D'une part, on a :

$$v = \sum_{x \in G} v(x)x = \sum_{i=1}^{l} \underbrace{\left(\sum_{a \in A} v(ag_i)a\right)}_{\in \mathbb{C}[A]} g_i \in \mathcal{U}_i.$$

D'autre part, supposons qu'il existe $v_1, \ldots, v_l, v'_1, \ldots, v'_l \in \mathbb{C}[A]$ tels que $v = \sum_{i=1}^{l} v_i g_i =$

$\sum_{i=1}^{l} v_i' g_i$. On a donc :

$$\begin{aligned}\sum_{x\in G} v(x)x &= \sum_{i=1}^{l}\sum_{x\in A} v_i(x)xg_i \\ &= \sum_{i=1}^{l}\sum_{x\in G} v_i(x)\mathbb{1}_A(x)xg_i \\ &= \sum_{i=1}^{l}\sum_{x\in G} v_i(xg_i^{-1})\mathbb{1}_A(xg_i^{-1})x,\end{aligned}$$

d'où

$$\forall i[\![1,l]\!], \forall a\in A, v(ag_i) = v_i(a).$$

De même, on a :

$$\forall i[\![1,l]\!], \forall a\in A, v(ag_i) = v_i'(a).$$

On en conclut que pour tout $i\in[\![1,l]\!]$ $v_i = v_i'$.

Montrons que pour tout $i\in[\![1,l]\!]$, $\mathrm{rg}(T_f)|_{\mathcal{U}_i} = 1$. On sait que $l = \frac{|G|}{|A|} = \mu(f) = \mathrm{rg}(T_f)$ et par les deux points qui précèdent $\mathrm{rg}(T_f) = \sum_{i=1}^{l}\mathrm{rg}(T_f|_{\mathcal{U}_i})$. On en déduit que si pour tout $i\in[\![1,l]\!], \mathrm{rg}(T_f|_{\mathcal{U}_i})\geq 1$ alors pour tout $i\in[\![1,l]\!], \mathrm{rg}(T_f|_{\mathcal{U}_i}) = 1$. Supposons donc par l'absurde qu'il existe $i\in[\![1,l]\!]$ tel que $\mathrm{rg}(T_f|_{\mathcal{U}_i}) = 0$. Alors on a : $\forall v\in\mathbb{C}[A], uvg_i = 0$. Or :

$$\begin{aligned}\forall v\in\mathbb{C}[A], uvg_i &= \sum_{x\in G}\left(\sum_{s\in A} f(s)v(s^{-1}x)\mathbb{1}_A(s^{-1}x)\right)xg_i \\ &= \sum_{x\in G}\left(\sum_{s\in A} f(s)v(s^{-1}xg_i^{-1})\mathbb{1}_A(xg_i^{-1})\right)x,\end{aligned}$$

ce qui donne :

$$\forall v\in\mathbb{C}[A], \forall x\in G, \sum_{s\in A} f(s)v(s^{-1}xg_i^{-1})\mathbb{1}_A(xg_i^{-1}) = 0.$$

En particulier, on a

$$\forall v\in\mathbb{C}[A], \forall a\in A, \sum_{s\in A} f(s)v(s^{-1}a) = 0.$$

En prenant en particulier $v = \sum_{x \in A} \mathbb{1}_{\{1\}}(x)x = 1$, on obtient :

$$\forall a \in A, \sum_{s \in A} f(s)\mathbb{1}_{\{1\}}(s^{-1}a) = 0,$$

d'où : $\forall a \in A, f(a) = 0$, ce qui est absurde car $A = \text{supp}(f) \neq \emptyset$.

En particulier, on vient de montrer que $\text{rg}\left(T_f|_{\mathcal{U}_1}\right) = 1$, et comme par définition $\mathcal{U}_1 = \mathbb{C}[A]$, on a :

$$\forall y \in A, \exists h_y \in \mathbb{C}, T_f(y) = h_y T_f(1),$$

autrement dit :

$$\forall y \in A, \sum_{x \in A} f(x)xy = T_f(y) = h_y T_f(1) = h_y \sum_{x \in A} f(x)x = \sum_{x \in A} h_y f(x)x.$$

On a donc :

$$\forall y \in A, \forall x \in A, f(xy^{-1}) = h_y f(x),$$

ce qui donne :

$$\forall y \in A, \forall x \in A, f(xy) = h_{y^{-1}} f(x) = f(y)f(x).$$

Au final, en posant $\chi : \begin{cases} A & \to \mathbb{C}^* \\ a & \mapsto f(a) \end{cases}$, on a bien $\chi \in \widehat{A}$ et $f = \mathbb{1}_A \chi$. □

5.3 Cas du groupe non abélien à pq éléments

Après avoir généralisé le premier principe d'incertitude à des groupes non abéliens, nous allons maintenant exposer comment Meshulam [8] a découvert un principe d'incertitude pour un groupe non abélien particulier, qui est $D_{p,q}$, le groupe non abélien à pq éléments tel que $p|q-1$.

Commençons par rappeler sa définition.

Définition 5.3.0.1. *Soient p, q des premiers tels que $p|q-1$. Soit ζ un générateur de $(\mathbb{Z}/q\mathbb{Z})^*$.*

Posons $r = \frac{q-1}{p}$ *et* $\alpha = \zeta^r$. *Notons* $C_p =< a >$ *le groupe cyclique d'ordre* p *et* $C_q =< b >$ *le groupe cyclique d'ordre* q. *On a une action* φ *non triviale de* C_p *sur* C_q *donnée par :*

$$\begin{aligned} \varphi : C_p \times C_q &\to C_q \\ (a^n, b^m) &\mapsto b^{m\alpha^n} \end{aligned}$$

On pose le produit semi-direct $D_{p,q} = C_q \rtimes_\varphi C_p$, *qui est bien non-abélien. Ce dernier est donc défini par :*

$$(a^n, b^m).(a^{n'}, b^{m'}) = (a^{n+n'}, b^{m+m'\alpha^n})$$

Si on pose la multiplication ba *donnée par :* $ba = (a, 1).(1, b)$, *on :*

$$ba = (a, b^\alpha) = (1, b^\alpha).(a, 1) = ab^\alpha$$

Au final, $D_{p,q}$ *peut être défini par :*

$$D_{p,q} =< \{a, b \text{ } t.q. \text{ } a^p = b^q = 1 \text{ } et \text{ } a^{-1}ba = b^\alpha\} >$$

Définition 5.3.0.2. *On pose pour* $x = a^k b^l \in D_{p,q}$, $\pi(x) = a^k$.

Définition 5.3.0.3. *Pour* $k = (k_1, \ldots, k_N) \in (\mathbb{Z}/p\mathbb{Z})^N$, $l = (l_1, \ldots, l_N) \in (\mathbb{Z}/q\mathbb{Z})^N$, *on pose* $a^k b^l = \prod_{i=1}^{N} a^{k_i} b^{l_i}$.

Nous allons maintenant donner les représentations complexes irréductibles de degré 1 et p de $D_{p,q}$, dont nous pouvons trouver une preuve dans pour cadre plus général dans [6].

Proposition 5.3.0.4.

— $D_{p,q}$ *a* p *représentations complexes de degré* 1, *notées* $\varphi_0, \ldots, \varphi_{p-1}$, *où pour chaque*

$j \in [\![0, p-1]\!]$, *on a :*

$$\begin{aligned} \varphi_j : D_{p,q} &\to \mathbb{C}^* \\ a^k b^l &\mapsto e_p(jk), \end{aligned}$$

où $e_p = e^{2i\pi \cdot / p}$.

— $D_{p,q}$ *a* $\frac{q-1}{p}$ *représentations complexes irréductibles de degré* p. *Premièrement,* C_q *a* q *représentations complexes irréductibles de degré* 1, *notées* $\psi_0, \ldots, \psi_{q-1}$ *définies pour chaque* $j \in [\![0, q-1]\!]$ *par :* $\psi_j(b^l) = e_q(jl)$. *Ensuite en posant*

$$W = Vect_{\mathbb{C}}(\{w_t, t \in \mathbb{Z}/p\mathbb{Z}\}),$$

qui est de dimension p, *on définit pour chaque* $j \in [\![0, q-1]\!]$ *:*

$$\begin{aligned} \rho_j : D_{p,q} &\to GL(W) \\ a^k b^l &\mapsto \left(w_t \mapsto e_q(jl\alpha^t) w_{t+k} = \psi_j(b^{l\alpha^t}) w_{t+k} \right). \end{aligned}$$

Les ρ_j, $j \in (\mathbb{Z}/q\mathbb{Z})^*$ *sont irréductibles et* ρ_j *est isomorphe à* $\rho_{j'}$ *si* $j' = \alpha^n j$ *pour un certain* n. *Au final, l'ensemble des représentations irréductibles de degré* p *de* $D_{p,q}$ *est :*

$$\Lambda = \{\rho_j, j = \zeta^m, m \in [\![0, \frac{q-1}{p} - 1]\!]\}.$$

Ce sont les seules représentations irréductibles de $D_{p,q}$.

Pour énoncer le nouveau principe d'incertitude que nous allons montrer pour $D_{p,q}$, nous avons besoin des définitions suivantes.

Définition 5.3.0.5. *Soit* G *un groupe fini. On pose pour* $c \in G, N \in \mathbb{N}^*$ *l'ensemble suivant :*

$$A_N(G, c) = \{(x_1, \ldots, x_N) \in G^N, x_1 \ldots x_N = c\}.$$

On pose de plus :

$$\lambda(G,N) = \min\{\mu(f), f : G^N \to \mathbb{C}, f \neq 0, \exists c \in G, supp(f) \subseteq A_N(G,c)\}.$$

On définit de la même manière $\tilde{\lambda}(G,N)$*, en remplacant* μ *par* $\tilde{\mu}$*. On a donc*

$$\tilde{\lambda}(G,N) \leq \lambda(G,N) \leq \tilde{\lambda}^2(G,N).$$

Remarque. *Si* G *est abélien,* $\lambda(G,N) = |G|$*. En effet, posons* $H = A_N(G,1)$*, qui est un sous-groupe de* G^N*. Soit* $c \in G$*, et posons* $K = A_N(G,1)$*. Alors* K *est une classe à gauche de* G^N *suivant* H *car* $K = yH$*, où* $y = (1,\ldots,1,c)$*. Or* $\mathbb{1}_H(1) = 1$ *donc par le théorème 5.2.0.1 on a*

$$\mu(\mathbb{1}_H) = \frac{|G^N|}{|H|} = |G|.$$

Or $\mathbb{1}_K = \mathbb{1}_{yH} = \mathbb{1}_H \circ t_{y^{-1}}$*, où* $t_{y^{-1}}$ *est la translation à gauche sur* G^N *par* y^{-1}*, et un calcul donne que pour* $\rho \in Irr(G^N)$ *:* $\widehat{\mathbb{1}_K}(\rho) = \rho(y) \circ \widehat{\mathbb{1}_H}$*. On obtient alors que* $rg(\widehat{\mathbb{1}_K}(\rho)) = rg(\widehat{\mathbb{1}_H}(\rho))$*, et donc* $\mu(\mathbb{1}_K) = \mu(\mathbb{1}_H) = |G|$*. En particulier,* $\lambda(G,N) \leq |G|$*.*

Or par le théorème 5.2.0.1, pour toute fonction $f : G^N \to \mathbb{C}$ *non nulle telle qu'il existe* $c \in G$ *vérifiant* $supp(f) \subseteq A_N(G,c)$*, on a* $\mu(f) \geq \frac{|G^N|}{|supp(f)|} \geq |G|$ *car* $|supp(f)| \leq |H| = |G|^{N-1}$*. On en déduit que* $\lambda(G,N) \geq |G|$*, et donc que* $\lambda(G,N) = |G|$*.*

Le théorème suivant nous donne un encadrement de $\lambda(D_{p,q},N)$, pour $N \in \mathbb{N}^*$.

Théorème 5.3.0.6. *Soit* $N \in \mathbb{N}^*$*. On a :*

$$q^{1/2}p^{(N-1)/2} \leq \tilde{\lambda}(D_{p,q},N) \leq \lambda(D_{p,q},N) \leq qp^N.$$

Démonstration. (Début) La deuxième inégalité est vraie comme on l'a vu à la définition 5.3.0.5.

Montrons la troisième. Posons $H = \{(b^{l_1},\ldots,b^{l_N}) \in D_{p,q}^N, \sum_{i=1}^{N} l_i \equiv 0[q]\}$. On a de manière évidente que $H \subseteq A_N(D_{p,q},1)$ et H est un sous-groupe de $D_{p,q}^N$. Par le théorème 5.2.0.1 on

obtient :

$$\lambda(D_{p,q}, N) \leq \mu(\mathbb{1}_H) = \frac{|D_{p,q}^N|}{|H|} = \frac{(pq)^N}{q^{N-1}} = qp^N.$$

□

Pour montrer la première inégalité du théorème, nous allons avoir besoin de deux propositions.

Proposition 5.3.0.7. *Soit $f : D_{p,q}^N \to \mathbb{C}$ non nulle. Supposons que :*

— *$supp(f) \subseteq A_N(D_{p,q}, 1)$*

— *$\forall (a^{k_1}b^{k_1}, \ldots, a^{k_N}b^{k_N}) \in D_{p,q}^N$ t.q. $\prod_{i=1}^{N} a^{k_i}b^{k_i} = 1$, $f(a^{k_1}b^{k_1}, \ldots, a^{k_N}b^{k_N}) = f(a^{k_1}, \ldots, a^{k_N})$*

alors $\mu(f) \geq (q-1)p^N$ et $\tilde{\mu}(f) \geq (q-1)p^{N-1}$.

Démonstration. Premièrement, on peut montrer par récurrence sur $N \in \mathbb{N}^*$ en utilisant la relation définissant $D_{p,q}$ (5.3.0.1), que pour tout $k = (k_1, \ldots, k_N) \in (\mathbb{Z}/p\mathbb{Z})^N$ et $(l_1, \ldots, l_N) \in (\mathbb{Z}/q\mathbb{Z})^N$, on a $a^k b^l = a^A b^B$ où $A = \sum_{i=1}^{N} k_i$ et $B = \sum_{i=1}^{N} l_i \alpha^{\sum_{s=i+1}^{N} k_s}$.

Posons $K = \{(k_1, \ldots, k_N) \in (\mathbb{Z}/p\mathbb{Z})^N, \sum_{i=1}^{N} k_i = 0\}$, et pour tout $k \in K$ posons également $L(k) = \{l \in (\mathbb{Z}/q\mathbb{Z})^N, a^k b^l = 1\}$. On a alors, pour $k \in K$ et $l \in (\mathbb{Z}/q\mathbb{Z})^N$, les équivalences suivantes :

$$l \in L(k) \iff a^k b^l = 1 \iff a^A b^B = 1 \iff b^B = 1 \iff l_N = -\sum_{i=1}^{N-1} l_i \alpha^{\sum_{s=i+1}^{N} k_s}.$$

L'idée de la démonstration est de trouver une minoration du rang de $\widehat{(}f)\left(\bigotimes_{i=1}^{N} \rho\right)$, pour des représentations complexes irréductibles ρ particulières (celles de dimension p), ce qui nous permettra de minorer $\mu(f)$ et $\tilde{\mu}(f)$ en utilisant leurs définitions.

Posons pour $\rho_j \in \Lambda$:

$$F_j(k) = \sum_{l \in L(k)} \bigotimes_{i=1}^{N} \rho_j(b^{l_i}) \in \mathcal{L}(W^{\otimes N}).$$

Soit $t_1, \dots, t_N \in \mathbb{Z}/p\mathbb{Z}$ et $k \in K$. On a :

$$\begin{aligned} F_j(k)\left(\bigotimes_{i=1}^{N} w_{t_i}\right) &= \sum_{l\in L(k)} \bigotimes_{i=1}^{N} \rho_j(b^{l_i}) \left(\bigotimes_{i=1}^{N} w_{t_i}\right) \\ &= \sum_{l\in L(k)} \bigotimes_{i=1}^{N} \rho_j(b^{l_i}) w_{t_i} \\ &= \sum_{l\in L(k)} \bigotimes_{i=1}^{N} e_q(jl_i\alpha^{t_i}) w_{t_i} \\ &= \sum_{l\in L(k)} \prod_{i=1}^{N} e_q(jl_i\alpha^{t_i}) \bigotimes_{i=1}^{N} w_{t_i} \\ &= \sum_{l\in L(k)} e_q\left(j\sum_{i=1}^{N} l_i\alpha^{t_i}\right) \bigotimes_{i=1}^{N} w_{t_i}. \end{aligned}$$

Or comme $\sum_{i=1}^{N} k_i = 0$, on a :

$$\begin{aligned} \sum_{l\in L(k)} e_q\left(j\sum_{i=1}^{N} l_i\alpha^{t_i}\right) &= \sum_{l_1\in\mathbb{Z}/q\mathbb{Z}} \dots \sum_{l_{N-1}\in\mathbb{Z}/q\mathbb{Z}} e_q\left(j\left(\sum_{i=1}^{N-1} l_i\alpha^{t_i} - \left(\sum_{i=1}^{N-1} l_i\alpha^{-\sum_{s=1}^{i} k_s}\right)\alpha^{t_N}\right)\right) \\ &= \sum_{l_1\in\mathbb{Z}/q\mathbb{Z}} \dots \sum_{l_{N-1}\in\mathbb{Z}/q\mathbb{Z}} e_q\left(j\sum_{i=1}^{N-1} l_i\left(\alpha^{t_i} - \alpha^{t_N-\sum_{s=1}^{i} k_s}\right)\right) \\ &= \prod_{i=1}^{N-1} \sum_{l_i\in\mathbb{Z}/q\mathbb{Z}} e_q\left(jl_i\left(\alpha^{t_i} - \alpha^{t_N-\sum_{s=1}^{i} k_s}\right)\right). \end{aligned}$$

Donc si pour tout $i \in [\![1, N]\!]$, $t_i = t_N - \sum_{s=1}^{i} k_s$ (l'égalité pour $i = N$ est toujours vraie), alors :

$$F_j(k)\left(\bigotimes_{i=1}^{N} w_{t_i}\right) = \left(\prod_{i=1}^{N-1} \sum_{l_i\in\mathbb{Z}/q\mathbb{Z}} 1\right) \bigotimes_{i=1}^{N} w_{t_i} = q^{N-1} \bigotimes_{i=1}^{N} w_{t_i}.$$

Au contraire, s'il existe $i_0 \in [\![1, N]\!]$ tel que $t_{i_0} \neq t_N - \sum_{s=1}^{i_0} k_s$, on a :

$$\sum_{l_{i_0} \in \mathbb{Z}/q\mathbb{Z}} e_q \left(jl_{i_0} \underbrace{\left(\alpha^{t_{i_0}} - \alpha^{t_N - \sum_{s=1}^{i_0} k_s} \right)}_{:=x \neq 0} \right) = \sum_{l_{i_0} \in \mathbb{Z}/q\mathbb{Z}} e^{2i\pi j l_{i_0} x/q} = 0,$$

et donc

$$F_j(k) \left(\bigotimes_{i=1}^{N} w_{t_i} \right) = 0.$$

En isolant les k_i, on obtient l'équivalence des deux conditions suivantes :

1. $\forall i \in [\![1, N]\!], t_i = t_n - \sum_{s=1}^{i} k_s$
2. $k_1 = t_N - t_1$ et $\forall i \in [\![2, N]\!], k_i = t_{i-1} - t_i$.

Maintenant, calculons $\widehat{f}(\bigotimes_{i=1}^{N} \rho_j)$ pour $\rho_j \in \Lambda$. On a :

$$\begin{aligned} \widehat{f}(\bigotimes_{i=1}^{N} \rho_j) &= \sum_{x \in D_{p,q}^N} f(x) \bigotimes_{i=1}^{N} \rho_j(x) \\ &= \sum_{(k_1,\ldots,k_N) \in (\mathbb{Z}/p\mathbb{Z})^N} \sum_{(l_1,\ldots,l_N) \in (\mathbb{Z}/q\mathbb{Z})^N} f(a^{k_1} b^{l_1}, \ldots, a^{k_N} b^{l_N}) \bigotimes_{i=1}^{N} \rho_j(a^{k_i} b^{l_i}). \end{aligned}$$

Or comme $\mathrm{supp}(f) \subseteq A_N(D_{p,q}, 1)$, on en déduit que :

$$\begin{aligned} \widehat{f} \left(\bigotimes_{i=1}^{N} \rho_j \right) &= \sum_{k \in K} \sum_{l \in L(k)} f(a^{k_1} b^{l_1}, \ldots, a^{k_N} b^{l_N}) \bigotimes_{i=1}^{N} \rho_j(a^{k_i} b^{l_i}) \\ &= \sum_{k \in K} \sum_{l \in L(k)} f(a^{k_1}, \ldots, a^{k_N}) \bigotimes_{i=1}^{N} \rho_j(a^{k_i} b^{l_i}) \end{aligned}$$

Exprimons cela en fonction de $F_j(k)$:

$$\begin{aligned}\sum_{l\in L(k)}\bigotimes_{i=1}^{N}\rho_j(a^{k_i}b^{l_i}) &= \sum_{l\in L(k)}\bigotimes_{i=1}^{N}\rho_j(a^{k_i})\circ\rho_j(b^{l_i})\\ &= \sum_{l\in L(k)}\left(\bigotimes_{i=1}^{N}\rho_j(a^{k_i})\right)\circ\left(\bigotimes_{i=1}^{N}\rho_j(b^{l_i})\right)\\ &= \left(\bigotimes_{i=1}^{N}\rho_j(a^{k_i})\right)\circ F_j(k),\end{aligned}$$

d'où :

$$\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right) = \sum_{k\in K} f(a^{k_1},\dots,a^{k_N})\left(\bigotimes_{i=1}^{N}\rho_j(a^{k_i})\right)\circ F_j(k).$$

En combinant tout ce qui précède, on obtient alors le résultat suivant :

$$\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)\left(\bigotimes_{i=1}^{N}w_{t_i}\right) = \sum_{k\in K} f(a^{k_1},\dots,a^{k_N})\left(\bigotimes_{i=1}^{N}\rho_j(a^{k_i})\right)\underbrace{F_j(k)\left(\bigotimes_{i=1}^{N}w_{t_i}\right)}_{\begin{cases} q^{N-1}\bigotimes_{i=1}^{N}w_{t_i} \text{ si (1)}\\ 0 \text{ sinon}\end{cases}}.$$

En utilisant la définition 5.3.0.4 des ρ_j et la condition 1, on en déduit que :

$$\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)\left(\bigotimes_{i=1}^{N}w_{t_i}\right) = q^{N-1}f(a^{t_N-t_1},a^{t_1-t_2},\dots,a^{t_{N-1}-t_N})\left(w_{t_N}\otimes w_{t_1}\otimes\ldots\otimes w_{t_{N-1}}\right).$$

Comme $\mathrm{supp}(f)\neq\emptyset$, il existe $(a^{k_1}b^{l_1},\dots,a^{k_N}b^{l_N})\in\mathrm{supp}(f)\subseteq A_N(D_{p,q},1)$. On a alors $f((a^{k_1}b^{l_1},\dots,a^{k_N}b^{l_N})) = f(a^{k_1},\dots,a^{k_N})\neq 0$, d'où $(a^{k_1},\dots,a^{k_N})\in A_N(D_{p,q},1)$, et donc $\sum_{i=1}^{n}k_i = 0$, i.e. $(k_1,\dots,k_N)\in K$.

En reprenant le calcul de $\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)$, on obtient que pour tout $k\in\mathbb{Z}/p\mathbb{Z}$:

$$\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)\left(\bigotimes_{i=1}^{N}w_{k-\sum_{s=1}^{i}k_s}\right)=q^{N-1}f(a^{k_1},\ldots,a^{k_N})w_k\otimes w_{k-k_1}\otimes\ldots\otimes w_{k-\sum_{s=1}^{N-1}k_s}.$$

Enfin, nous allons pouvoir montrer que $\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)$ est injective sur

$$V=Vect\left(\bigotimes_{i=1}^{N}w_{k-\sum_{s=1}^{i}k_s},k\in\mathbb{Z}/p\mathbb{Z}\right).$$

Pour montrer cela, il faut et il suffit de montrer que

$$\left(\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)\left(\bigotimes_{i=1}^{N}w_{k-\sum_{s=1}^{i}k_s},k\in\mathbb{Z}/p\mathbb{Z}\right)\right)_{k\in\mathbb{Z}/p\mathbb{Z}}$$

est libre, c'est-à-dire grâce au calcul que nous venon de faire il faut et il suffit de montrer que $\left(w_k\otimes w_{k-k_1}\otimes\ldots\otimes w_{k-\sum_{s=1}^{N-1}k_s}\right)_{k\in\mathbb{Z}/p\mathbb{Z}}$ est libre. Or par définition de W, $(w_t)_{t\in\mathbb{Z}/p\mathbb{Z}}$ est une base de W donc $(w_{t_1}\otimes\ldots\otimes w_{t_N})_{(t_1,\ldots,t_N)\in(\mathbb{Z}/p\mathbb{Z})^N}$ est une base de $W^{\otimes N}$. Donc $\left(\bigotimes_{i=1}^{N}w_{k-\sum_{s=1}^{i}k_s}\right)_{k\in\mathbb{Z}/p\mathbb{Z}}$ est libre et V est de dimension p. De même, $\left(\bigotimes_{i=1}^{N}w_{k-\sum_{s=1}^{i-1}k_s}\right)$ est libre et on a bien montré que $\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)$ est injective sur V.

Ainsi, $\mathrm{rg}\left(\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_j\right)\right)) \geq p$, et donc on obtient une minoration de $\mu(f)$:

$$\begin{aligned}
\mu(f) &= \sum_{\rho\in Irr(D_{p,q}^N)} \deg(\rho)\mathrm{rg}\left(\widehat{f}(\rho)\right) \\
&\geq \sum_{\rho\in\Lambda} p^N \mathrm{rg}\left(\widehat{f}\left(\bigotimes_{i=1}^{N}\rho\right)\right)) \\
&= \sum_{m=0}^{\frac{q-1}{p}-1} p^N \underbrace{\mathrm{rg}\left(\widehat{f}\left(\bigotimes_{i=1}^{N}\rho_{\lambda^m}\right)\right)}_{\geq p} \\
&\geq p^{N+1}\frac{q-1}{p} = p^N(q-1).
\end{aligned}$$

On obtient de la même manière une minoration de $\tilde{\mu}(f)$:

$$\tilde{\mu}(f) \geq \sum_{m=0}^{\frac{q-1}{p}-1} p^N \underbrace{\mathbb{1}_{\mathrm{supp}(\widehat{f})}\left(\bigotimes_{i=1}^{N}\rho_{\lambda^m}\right)}_{=1} \geq p^{N-1}(q-1).$$

□

Définition 5.3.0.8. *Pour tout $f : D_{p,q}^N \to \mathbb{C}$, $x, y \in D_{p,q}$, on pose :*

$$\begin{aligned}
f_{x,y} \colon D_{p,q}^{N-2} &\longrightarrow \mathbb{C} \\
(x_1, \ldots, x_{N-2}) &\longmapsto f(x_1, \ldots, x_{N-2}, x, y).
\end{aligned}$$

Proposition 5.3.0.9. *Soit $f : D_{p,q}^N \to \mathbb{C}$.*

Supposons qu'il existe $c \in D_{p,q}$ tel que $supp(f) \subseteq A_N(D_{p,q}, c)$. Supposons de plus qu'il existe $u_1, u_2, v_1, v_2 \in D_{p,q}$ tels que :

1. *$u_1u_2 = v_1v_2$ et $\forall i = 1, 2, \pi(u_i) = \pi(v_i)$*
2. *$f_{u_1,u_2} \neq f_{v_1,v_2}$*

Alors $\tilde{\mu}(f) \geq p\tilde{\lambda}(D_{p,q}, N-2)$.

Démonstration. Posons

$$\begin{aligned} g\colon D_{p,q}^{N-2} &\to \mathbb{C} \\ (x_1, \ldots, x_{N-2}) &\mapsto f_{u_1,u_2}(x_1, \ldots, x_{N-2}) - f_{v_1,v_2}(x_1, \ldots, x_{N-2}), \end{aligned}$$

et $E = \mathrm{supp}(\widehat{g}) = \{\bar{\eta} \in Irr(D_{p,q}^{N-2}), \widehat{g}(\bar{\eta}) \neq 0\}$. Posons également $c' = u_1u_2 = v_1v_2$.

Montrons tout d'abord que

$$\mathrm{supp}(g) \subseteq A_{N-2}(D_{p,q}, c(c')^{-1}).$$

Soit $(x_1, \ldots, x_{N-2}) \notin A_{N-2}(D_{p,q}, c(c')^{-1})$. Alors par définition

$$x_1 \ldots x_{N-2}u_1u_2 = x_1 \ldots x_{N-2}c' \neq c,$$

donc $(x_1, \ldots, x_{N-2}, u_1, u_2) \notin A_N(D_{p,q}, c)$ et donc par supposition $(x_1, \ldots, x_{N-2}, u_1, u_2) \notin \mathrm{supp}(f)$. On en déduit que $f_{u_1,u_2}(x_1, \ldots, x_{N-2}) = 0$ et de même $f_{v_1,v_2}(x_1, \ldots, x_{N-2}) = 0$, d'où $g(x_1, \ldots, x_{N-2}) = 0$.

De plus, $g \neq 0$ par hypothèse donc :

$$\tilde{\mu}(f)(g) = \sum_{\bar{\eta} \in E} \deg(\bar{\eta}) \geq \tilde{\lambda}(D_{p,q}, N-2).$$

Soit $\bar{\eta} : D_{p,q}^{N-2} \to GL(U)$ tel que $\bar{\eta} \in E$. Il existe alors $\eta_1, \ldots, \eta_{N-2}$ des représentations complexes irréductibles de $D_{p,q}$ telles qu'on puisse écrire $\bar{\eta} = \eta_1 \otimes \ldots \otimes \eta_{N-2}$. Posons :

$$\begin{aligned} h : D_{p,q}^2 &\to \mathcal{L}(U) \\ (x, y) &\mapsto \widehat{f_{x,y}}(\bar{\eta}). \end{aligned}$$

On a donc pour tout $\eta_{N-1} \otimes \eta_N \in Irr(D_{p,q}^2)$:

$$\begin{aligned}
\widehat{f}\left(\bigotimes_{i=1}^{N} \eta_i\right) &= \sum_{x,y \in D_{p,q}} \sum_{x_1,\ldots,x_{N-2} \in D_{p,q}} f(x_1,\ldots,x_{N-2},x,y) \bigotimes_{i=1}^{N} \eta_i(x_1,\ldots,x_{N-2},x,y) \\
&= \sum_{x,y \in D_{p,q}} \sum_{x_1,\ldots,x_{N-2} \in D_{p,q}} f(x_1,\ldots,x_{N-2},x,y) \bigotimes_{i=1}^{N-2} \eta_i(x_i) \otimes \eta_{N-1}(x) \otimes \eta_N(y) \\
&= \sum_{x,y \in D_{p,q}} \widehat{f_{x,y}}\left(\bigotimes_{i=1}^{N-2} \eta_i\right) \otimes \eta_{N-1}(x) \otimes \eta_N(y)
\end{aligned}$$

En posant $h : (x,y) \mapsto \widehat{f_{x,y}}\left(\bigotimes_{i=1}^{N-2} \eta_i\right)$, et en étendant la définition de la transformée de Fourier aux fonctions $a : G \to \mathcal{L}(U)$, où U est un $\mathbb{C}$-espace vectoriel, de la manière suivante :

$$\forall \rho \in Irr(G), \widehat{a}(\rho) = \sum_{x \in G} a(x) \otimes \rho(x) \in \mathcal{L}(U \otimes V),$$

où V est l'espace vectoriel associé à la représentation, ρ, on obtient que :

$$\widehat{f}\left(\bigotimes_{i=1}^{N} \eta_i\right) = \widehat{h}(\eta_{N-1} \otimes \eta_N).$$

Maintenant nous allons montrer qu'il existe $\eta_{N-1} \otimes \eta_N \in Irr(D_{p,q}^2)$ tel que $\deg(\eta_{N-1} \otimes \eta_N) \geq p$ et $\widehat{h}(\eta_{N-1} \otimes \eta_N) \neq 0$. Pour cela, supposons par l'absurde que :

$$\forall \eta_{N-1} \otimes \eta_N \in Irr(D_{p,q}^2), \deg(\eta_{N-1} \otimes \eta_N) < p \text{ ou } \widehat{h}(\eta_{N-1} \otimes \eta_N) = 0.$$

On a alors :

$$\forall \eta_{N-1} \otimes \eta_N \in \mathrm{supp}(\widehat{h}), \deg(\eta_{N-1}) \deg(\eta_N) = \deg(\eta_{N-1} \otimes \eta_N) < p.$$

Or par la description des représentations complexes irréductibles de $D_{p,q}$ (5.3.0.4), cela nous donne que :

$$\mathrm{supp}(\widehat{h}) \subseteq \{\varphi_i \otimes \varphi_j, 0 \leq i,j \leq p-1\}.$$

Par le théorème d'inversion de Fourier, il existe alors pour tout $i, j \in [\![0, p-1]\!]$, $A_{i,j} \in \mathcal{L}(U)$ tel que pour tout $x, y \in D_{p,q}$:

$$h(x,y) = \sum_{i,j=0}^{p-1} \varphi_i(x) \circ \varphi_j(y) \circ A_{i,j}.$$

Par définition, pour tout $i = 1, 2$ et pour tout $j \in [\![0, p-1]\!]$,

$$\varphi_j(u_i) = e_p(j\pi(u_i)) = e_p(j\pi(v_i)) = \varphi_j(v_i).$$

On a alors :

$$\begin{aligned}
\widehat{f_{u_1,u_2}}(\bar{\eta}) &= h(u_1, u_2) \\
&= \sum_{i,j=0}^{p-1} \varphi_i(u_1) \circ \varphi_j(u_2) \circ A_{i,j} \\
&= \sum_{i,j=0}^{p-1} \varphi_i(v_1) \circ \varphi_j(v_2) \circ A_{i,j} \\
&= h(v_1, v_2) \\
&= \widehat{f_{v_1,v_2}}(\bar{\eta}),
\end{aligned}$$

et donc $\widehat{g}(\bar{\eta}) = 0$ ce qui est absurde car $\bar{\eta} \in E = \mathrm{supp}(\widehat{g})$.

Au final, il existe donc $\eta_{N-1} \otimes \eta_N \in Irr(D_{p,q}^2)$ tel que $\deg(\eta_{N-1} \otimes \eta_N) \geq p$ et $\widehat{h}(\eta_{N-1} \otimes \eta_N) \neq 0$, et cela nous permet de donner la minoration de $\tilde{\mu}$ suivante :

$$\begin{aligned}
\tilde{\mu}(f) &= \sum_{\eta'_1,\ldots,\eta'_N \in Irr(D_{p,q})} \deg\left(\bigotimes_{i=1}^{N} \eta'_i\right) \mathbb{1}_{\mathrm{supp}(\widehat{f})}\left(\bigotimes_{i=1}^{N} \eta'_i\right) \\
&\geq \sum_{\bar{\eta} \in E} \deg(\bar{\eta}) \deg(\eta_{N-1} \otimes \eta_N) \mathbb{1}_{\mathrm{supp}(\widehat{f})}(\bar{\eta} \otimes \eta_{N-1} \otimes \eta_N),
\end{aligned}$$

Comme $\deg(\eta_{N-1} \otimes \eta_N) \geq p$ et $\widehat{f}(\bar{\eta} \otimes \eta_{N-1} \otimes \eta_N) = \widehat{h}(\eta_{N-1} \otimes \eta_N) \neq 0$, on conclut que :

$$\tilde{\mu}(f) \geq \sum_{\bar{\eta} \in E} \deg(\bar{\eta}) p \geq p\tilde{\lambda}(D_{p,q}, N-2).$$

□

Nous pouvons, maintenant munis des deux propositions précédentes, terminer la preuve du théorème 5.3.0.6.

Démonstration. (Fin)

Il reste à montrer que

$$q^{1/2} p^{(N-1)/2} \leq \tilde{\lambda}(D_{p,q}, N).$$

On raisonne par récurrence sur $N \in \mathbb{N}^*$.

Pour montrer que l'assertion est vraie au rang 1 et 2, nous allons utiliser le théorème 5.3.0.6. Soit $N \in \mathbb{N}^*$. Par définition de $\lambda(D_{p,q}, N)$, il existe $f : D_{p,q}^N \to \mathbb{C}$ non nulle telle qu'il existe $c \in D_{p,q}$ vérifiant $\mathrm{supp}(f) \subseteq A_N(D_{p,q}, c)$ et $\mu(f) = \lambda(D_{p,q}, N)$. Comme $|A_N(D_{p,q}, c)| = (pq)^{N-1}$, on a alors :

$$\lambda(D_{p,q}, N) = \mu(f) \geq \frac{|D_{p,q}^N|}{|\mathrm{supp}(f)|} \geq \frac{(pq)^N}{|A_N(D_{p,q}, c)|} = pq,$$

ce qui implique que $\tilde{\lambda}(D_{p,q}, N) \geq \sqrt{\lambda(D_{p,q}, N)} \geq \sqrt{pq}$. En particulier, on a donc

$$\tilde{\lambda}(D_{p,q}, 1) \geq \sqrt{pq} \geq p^{(1-1)/2} q^{1/2},$$

et

$$\tilde{\lambda}(D_{p,q}, 1) \geq \sqrt{pq} = q^{1/2} p^{(2-1)/2}.$$

Soit $N \geq 3$. Supposons que pour tout $N' < N, \tilde{\lambda}(D_{p,q}, N') \geq q^{1/2} p^{(N'-1)/2}$. Soit $f : D_{p,q} \to \mathbb{C}$ non nulle telle qu'il existe $c \in D_{p,q}$ vérifiant $\mathrm{supp}(f) \subseteq A_N(D_{p,q}, c)$. Montrons que

$\tilde{\mu}(f) \geq q^{1/2}p^{(N-1)/2}$.

Déjà montrons qu'il suffit de supposer que $c = 1$. Posons

$$g : D_{p,q}^N \to \mathbb{C}$$
$$(x_1, \ldots, x_N) \mapsto f(x_1, \ldots, x_{N-1}, x_N c),$$

on a alors $\mathrm{supp}(f) \subseteq A_N(D_{p,q}, 1)$. De plus, comme pour tout $\rho \in Irr(D_{p,q})$, $\widehat{g}(\rho) = \widehat{f}(\rho) \circ f((1, \ldots, 1, c^{-1}))$, $\rho \in \mathrm{supp}(\widehat{f})$, on obtient que $\mathrm{supp}(\widehat{f}) = \mathrm{supp}(\widehat{g})$, et donc par définition $\tilde{\mu}(f) = \tilde{\mu}(g)$.

On peut donc supposer que $\mathrm{supp}(f) \subseteq A_N(D_{p,q}, 1)$. Raisonnons par disjonction de cas.

Cas 1 : Supposons que pour tout $j \in [\![1, N-1]\!]$ et pour tout $u_1, u_2, v_1, v_2 \in D_{p,q}$, si $u_1u_2 = v_1v_2$ et $\pi(u_i) = \pi(v_i)$ pour $i \in \{1, 2\}$, alors pour tout $(x_i)_{\substack{1 \leq i \leq N \\ i \neq j, j+1}} \in D_{p,q}^{N-2}$

$$f(x_1, \ldots, x_{j-1}, u_1, u_2, x_{j+2}, \ldots, x_N) = f(x_1, \ldots, x_{j-1}, v_1, v_2, x_{j+2}, \ldots, x_N).$$

Cherchons maintenant à appliquer la proposition 5.3.0.7, vérifions donc les hypothèses en question. Soit $(a^{k_1}b^{l_1}, \ldots, a^{k_N}b^{k_N}) \in D_{p,q}^N$ tel que $\prod_{i=1}^N a^{k_i}b^{l_i} = 1$. Comme $a^{k_1}b^{l_1} \times a^{k_2}b^{l_2} = ak_1 \times a^{k_2}b^{l_1\alpha^{k_2}+l_2}$, on a par supposition :

$$f(a^{k_1}b^{l_1}, a^{k_2}b^{l_2}, \ldots, a^{k_N}b^{l_N}) = f(a^{k_1}, a^{k_2}b^{l_1\alpha^{k_2}+l_2}, a^{k_3}b^{l_3}, \ldots, a^{k_N}b^{l_N}).$$

En réitérant, le processus, on obtient

$$f(a^{k_1}b^{l_1}, a^{k_2}b^{l_2}, \ldots, a^{k_N}b^{l_N}) = f(a^{k_1}, \ldots, a^{k_{N-1}}, a^{k_N}b^{e}),$$

où l'on a posé $e = \sum_{i=1}^{N} l_i\alpha^{\sum_{s=i+1}^N k_s}$. Or on a vu au début de la preuve de la proposition 5.3.0.7, que comme $\prod_{i=1}^N a^{k_i}b^{l_i} = 1$, alors $e = 0$. Nous avons donc grâce à la proposition 5.3.0.7 :

$$\tilde{\mu}(f) \geq (q-1)p^{N-1}.$$

Enfin un calcul nous donne que $(q-1)p^{N-1} > q^{1/2}p^{(N-1)/2}$ car $p^{(N-1)/2} > 1$ et $q \geq 3$, et donc on conclut que :

$$\tilde{\mu}(f) \geq q^{1/2}p^{(N-1)/2}.$$

Cas 2 : Supposons qu'il existe $j \in [\![1, N-1]\!]$ et $u_1, u_2, v_1, v_2 \in D_{p,q}$ tels que $u_1v_1 = u_2v_2$, et vérifiant pour tout $i \in \{1, 2\}$, $\pi(u_i) = \pi(v_i)$. Supposons de plus qu'il existe $(x_i)_{\substack{1\leq i\leq N \\ i\neq j, j+1}} \in D_{p,q}^{N-2}$ tel que :

$$f(x_1, \ldots, x_{j-1}, u_1, u_2, x_{j+2}, \ldots, x_N) \neq f(x_1, \ldots, x_{j-1}, v_1, v_2, x_{j+2}, \ldots, x_N).$$

Appliquons la proposition 5.3.0.9 à la fonction suivante :

$$\begin{aligned} g : D_{p,q}^N &\to \mathbb{C} \\ (z_1, \ldots, z_N) &\mapsto f(z_{N-j}, \ldots, z_N, z_1, \ldots, z_{N-j-1}). \end{aligned}$$

On a par supposition sur f que $\mathrm{supp}(g) \subseteq A_N(D_{p,q}, 1)$ et que

$$g(x_{j+2}, \ldots, x_N, x_1, \ldots, x_{j-1}, u_1, u_2) \neq g(x_{j+2}, \ldots, x_N, x_1, \ldots, x_{j-1}, v_1, v_2),$$

ce qui donne en particulier que $g_{u_1,u_2} \neq g_{v_1,v_2}$. Par la proposition 5.3.0.9 appliquée à g, nous obtenons donc la minoration suivante :

$$\tilde{\mu}(g) \geq p\tilde{\lambda}(D_{p,q}, N-2).$$

Or par hypothèse de récurrence, $\tilde{\lambda}(D_{p,q}, N-2) \geq q^{1/2}p^{(N-3)/2}$, donc $\tilde{\mu}(g) \geq q^{1/2}p^{(N-1)/2}$. Enfin, un changement de variable nous donne que $\tilde{\mu}(g) = \tilde{\mu}(f)$, et au final

$$\tilde{\mu}(f) \geq q^{1/2}p^{(N-1)/2}.$$

□

Annexe A Différentes démonstrations du théorème de Chebotarev

A.1 La preuve de Tao

Cette preuve est issue de [15].

Lemme A.1.1. *Soit p premier, $n \in \mathbb{N}^*$. Soit $P(z_1, \dots, z_n) \in \mathbb{Z}[z_1, \dots, z_n]$. S'il existe n racines p-ième de l'unité $\omega_1, \dots, \omega_n$ telles que $P(\omega_1, \dots, \omega_n) = 0$, alors $P(1, \dots, 1) \in p\mathbb{Z}$.*

Démonstration. Soit $P(z_1, \dots, z_n) \in \mathbb{Z}[z_1, \dots, z_n]$. Supposons qu'il existe $\omega_1, \dots, \omega_n$ des racines p-ième de l'unité telles que $P(\omega_1, \dots, \omega_n) = 0$. En posant $\omega = e^{2i\pi/p}$, pour tout $j \in [\![1, n]\!]$, il existe $k_j \in [\![1, p-1]\!]$ t.q. $\omega_i = \omega^{k_j}$.
Posons $Q(z) = P(z^{k_1}, \dots, z^{k_n}) \bmod z^p - 1$, on a donc $Q \in {}^{\mathbb{Z}[z]}\!/_{(z^p-1)}$. Par définition $Q(\omega) = 0$ et $Q(1) = P(1, \dots, 1)$. Or le polynôme minimal de ω est le p-ième polynôme cyclotomique $\phi_p(z) = 1 + z + \ldots + z^{p-1}$ et $deg(Q) \leq p - 1$, donc il existe $a \in \mathbb{Z}$ t.q. $Q = a\phi_p \bmod z^p - 1$. Donc $P(1, \dots, 1) = ap \in p\mathbb{Z}$. □

Démonstration du théorème 3.1.2.2. Soit $n \in [\![1, p]\!]$ la taille d'un mineur de la matrice en question. Soient $x_1, \dots, x_n \in \mathbb{Z}/p\mathbb{Z}$ deux à deux distincts, et $\xi_1, \dots, \xi_n \in \mathbb{Z}/p\mathbb{Z}$ deux à deux distincts. On cherche donc à montrer que $det\left((e^{2i\pi x_j \xi_k/p})_{1\leq j,k\leq n}\right) \neq 0$. Posons $\forall j \in [\![1, n]\!], \omega_j = e^{2i\pi x_j/p}$. Montrons que $det\left((\omega_j^{\xi_k/p})_{1\leq j,k\leq n}\right) \neq 0$. Posons $D(z_1, \dots, z_n) = det\left((z_j^{\xi_k/p})_{1\leq j,k\leq n}\right) \in \mathbb{Z}[z_1, \dots, z_n]$. Si on avait $D(1, \dots, 1) \notin p\mathbb{Z}$ alors par le lemme A.1.1, $D(\omega_1, \dots, \omega_n) \neq 0$. Le problème est que $D(1, \dots, 1) = det\left((1)_{1\leq j,k\leq n}\right) = 0 \in p\mathbb{Z}$. Or on remarque que si $z_j = z_{j'}$ pour $j \neq j' \in [\![1, n]\!]$ alors $D(z_1, \dots, z_n) = 0$. L'idée est donc de factoriser D par les facteurs linéaires $(z_j - z_{j'})$: il existe $P \in \mathbb{Z}[z_1, \dots, z_n]$ t.q. $D(z_1, \dots, z_n) = P(z_1, \dots, z_n) \underbrace{\prod_{1\leq j<j'\leq n} (z_j - z'_j)}_{\frac{n(n-1)}{2}\text{facteurs}}$. Il suffit donc de montrer que $P(1, \dots, 1) \notin p\mathbb{Z}$, car par le lemme A.1.1 $P(\omega_1, \dots, \omega_n) \neq 0$. Comme les ω_j sont deux à deux distincts, on en conclut que $D(\omega_1, \dots, \omega_n) \neq 0$.

On considère l'expression suivante :

$$E(z_1,\dots,z_n)=\underbrace{\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\dots\left(z_n\frac{d}{dz_n}\right)^{n-1}}_{\frac{n(n-1)}{2}\text{dérivations}}D(z_1,\dots,z_n).$$

Par la règle de Leibniz, quand on applique un $z_j\frac{d}{dz_j}$, soit on élimine un facteur linéaire $z_j-z_{j'}$ et on le remplace par z_j, soit on dérive d'autres termes. Quand on évalue $E(z_1,\dots,z_n)$ en des $z_1=\dots=z_n\neq 0$, les seuls termes qui ne s'annulent pas sont ceux pour lesquels chaque $z_j\frac{d}{dz_j}$ a éliminé et remplacé par z_j un facteur $z_j-z_{j'}$. Les $n-1$ opérateurs $z_n\frac{d}{dz_n}$ ne peuvent donc qu'éliminer les $n-1$ facteurs $z_j-z_n, j\in[\![1,n-1]\!]$, et chaque $z_n\frac{d}{dz_n}$ doit éliminer exactement un z_j-z_n. IL y $(n-1)!$ manières de le faire. On raisonne de la même manière pour les autres $z_j\frac{d}{dz_j}$. Au final :

$$E(1,\dots,1)=\underbrace{(n-1)!(n-2)!\dots 0!}_{\notin p\mathbb{Z}}P(1,\dots,1).$$

Enfin, il suffit donc de montrer que $E(1,\dots,1)\notin p\mathbb{Z}$. Or $\forall j\in[\![1,n]\!]$, $\left(z_j\frac{d}{dz_j}\right)^{j-1}z_j^\xi=\xi^{j-1}z_j^\xi$, donc par multilinéarité du déterminant :

$$E(1,\dots,1)=det\left((\xi_k^{j-1})_{1\leq j,k\leq n}\right).$$

On reconnaît un déterminant de Vandermonde, d'où :

$$E(1,\dots,1)=\prod_{1\leq j,k\leq n}\underbrace{(\xi_k-\xi_{k'})}_{\notin p\mathbb{Z}}.$$

D'où $E(1,\dots,1)\notin p\mathbb{Z}$. □

A.2 La preuve de Frenkel

Cette preuve est issue de [4].

Soit $I,J\subseteq\mathbb{Z}/p\mathbb{Z}$ de même cardinal. Nous allons montrer que $det((\omega^{ij})_{i\in I,j\in J})\neq 0$.

Le lemme 3.1.2.2 est équivalent au fait que les colonnes de la matrice (qui sont des

éléments de $(\mathbb{Q}(\omega))^{|I|}$) soient libres, autrement dit :

$$\forall (a_j)_{j\in J} \in (\mathbb{Q}(\omega))^{|J|},\ (\forall i \in I,\ \sum_{j\in J} a_j \omega^{ij} = 0) \implies \forall j \in J, a_j = 0.$$

On verra qu'on pourra remplacer $\mathbb{Q}(\omega)$ par $\mathbb{Z}[\omega]$ dans l'assertion précédente.

En remarquant (lemme A.2.1) que $\mathbb{Z}[\omega]/(1-\omega) = \mathbb{F}_p$, on va montrer que le polynôme $g(X) = \sum_{j\in J} a_j X^j$ a pour image dans $\mathbb{Z}[\omega]/(1-\omega)$ un polynôme dont la multiplicité de 1 est supérieure à $|I|$. D'où vient la question : est-ce qu'il existe un lien entre la multiplicité d'une racine non nulle d'un polynôme non nul à coefficients dans $\mathbb{F}_p$ et son nombre de coefficients non nuls ? La réponse est oui, voir lemme A.2.2. On en déduira que $\bar{g}$ est nul dans $\mathbb{F}_p[X]$, et donc par un argument d'itération que $g = 0$.

Lemme A.2.1. *On a :* $\mathbb{Z}[\omega]/(1-\omega) \simeq \mathbb{F}_p$.

Démonstration. Notons $\Phi_p(X) = 1 + X + \ldots + X^{p-1}$ le p-ième polynôme cyclotomique, qui est le polynôme minimal de ω. Posons :

$$\begin{aligned} \varphi_1 \colon \mathbb{Z}[X] &\longrightarrow \mathbb{Z}[X]/(\Phi_p(X)) = \mathbb{Z}[\omega] \\ X &\longmapsto \omega \end{aligned}$$

$$\begin{aligned} \varphi_2 \colon \mathbb{Z}[X] &\longrightarrow \mathbb{Z}[X]/(1-X, p) = \mathbb{F}_p \\ X &\longmapsto 1, \end{aligned}$$

qui sont toutes deux surjectives.

De plus, $\ker(\varphi_1) \subseteq \ker(\varphi_2)$. En effet, soit $P \in \ker(\varphi_1) \subseteq \mathbb{Z}[X]$. Alors il existe $Q \in \mathbb{Z}[X]$ tel que $P = \Phi_p Q$. En évaluant en 1 on obtient que : $P(1) = \underbrace{\Phi_p(1)}_{=p} Q(1) = 0 \mod p$. D'où $P \in \ker \varphi_2$.

Par le théorème de factorisation, on peut factoriser φ_2 comme suit :

$$\begin{array}{ccc} \mathbb{Z}[X] & \xrightarrow{\quad\varphi_2\quad} & \mathbb{Z}[X]/(1-X,p) = \mathbb{F}_p \\ \Big\downarrow \pi & \nearrow_{\bar{\varphi}_2} & \\ \mathbb{Z}[\omega] = \mathbb{Z}[X]/\ker(\varphi_1) & & \end{array}$$

où $\bar{\varphi}_2$ vérifie $\varphi_2 = \bar{\varphi}_2 \circ \pi$.

Enfin, montrons que $\ker(\bar{\varphi}_2) = (1-\omega)$.

Tout d'abord, vérifions que $\ker(\bar{\varphi}_2) = (1-X,p)/(\Phi_p(X))$. Soit $\bar{P} \in \ker(\bar{\varphi}_2)$,où $\bar{P} = \pi(P)$ avec $P \in \mathbb{Z}[X]$. Par définition $\varphi_2(P) = \bar{\varphi}_2(\pi(P)) = \bar{\varphi}_2(\bar{P}) = 0$ donc $P \in (1-X,p)$, d'où $\bar{P} \in (1-X,p)/(\Phi_p(X))$. Réciproquement, soit $\overline{(P)} \in (1-X,p)/(\Phi_p(X))$, où $P \in (1-X,p) \subseteq \mathbb{Z}[X]$ et $\bar{P} = \pi(P)$. Donc $\bar{\varphi}_2(\bar{P}) = \bar{\varphi}_2(\pi(P)) = \varphi_2(P) = 0$.

Or

$$\begin{aligned} (1-X,p)/(\Phi_p(X)) &= (1-X/\Phi_p(X),p) \\ &= (1-\omega,p) \\ &= (1-\omega) \text{ car } p = \Phi_p(1) = \Phi_p(\omega) \bmod 1-\omega \\ &= 0 \bmod 1-\omega. \end{aligned}$$

D'où $\mathbb{Z}[\omega]/(1-\omega) = \mathbb{F}_p$ □

Lemme A.2.2. *Soit $g(X) = \sum_{i=0}^{p-1} a_i X^i \in \mathbb{F}_p[X]$ non nul. Soit $a \in \mathbb{F}_p \setminus \{0\}$ une racine de g. Notons $m_g(a)$ la multiplicité de a. Alors : $m_g(a) < |\{i \in [\![0,p-1]\!], a_i \neq 0\}|$.*

Démonstration. Montrons par récurrence sur $k \in [\![0,p-1]\!]$, $H(k) : \forall g(X) = \sum_{i=0}^{k} a_i X^i \in \mathbb{F}_p[X], \forall a \in \mathbb{F}_p \setminus \{0\}, g(a) = 0 \implies m_g(a) < |\{i \in [\![0,k]\!], a_i \neq 0\}|$.

Soit $g \in \mathbb{F}_p[X]$ non nul tel que $deg(g) \leq 0$. Donc g n'a pas de racine non nulle, la propriété est donc vraie.

Soit $k \in [\![1, p-1]\!]$. Supposons que $\forall k' \in [\![0, k-1]\!]$, $H(k')$ est vraie. Soit $g(X) = \sum_{i=0}^{k} a_i X^i \in \mathbb{F}_p[X]$. Soit $a \in \mathbb{F}_p \setminus \{0\}$ tel que $g(a) = 0$. Distinguons deux cas.

Cas 1 : si $g(0) = 0$.

Alors $\frac{g(X)}{X} = \sum_{i=0}^{k-1} a_{i+1} X^i$. Alors d'une part $|\{i \in [\![0, k]\!], a_i \neq 0\}| = |\{i \in [\![0, k-1]\!], a_{i+1} \neq 0\}|$. D'autre part, en écrivant $g(X) = (X-a)^{m_g(a)} \tilde{g}(X)$, où $\tilde{g}(a) \neq 0$, et comme $X | g(X)$ et $X \nmid (X-a)$, on a que $X | \tilde{g}(X)$. D'où $\frac{g(X)}{X} = (X-a)^{m_g(a)} \frac{\tilde{g}(X)}{X}$ avec $\frac{\tilde{g}(a)}{a} \neq 0$, donc $m_g(a) = m_{\frac{g(X)}{X}}(a)$. Par hypothèse de récurrence sur $\frac{g(X)}{X}$:

$$m_{\frac{g(X)}{X}}(a) < |\{i \in [\![0, k-1]\!], a_{i+1} \neq 0\}|,$$

d'où

$$m_g(a) < |\{i \in [\![0, k]\!], a_i \neq 0\}|.$$

Cas 2 : si $g(0) \neq 0$.

Comme $g'(X) = \sum_{i=1}^{k} i a_i X^{i-1}$, on a que $g' \neq 0$. En effet, $g \neq 0$ et $deg(g) \geq 1$ donc il existe $j \in [\![1, k]\!]$ tel que $a_j \neq 0$ donc $j a_j \neq 0$.

D'une part $|\{i \in [\![0, k]\!], a_i \neq 0\}| = |\{i \in [\![1, k]\!], i a_i \neq 0\}| + 1$.

D'autre part, en écrivant $g(X) = (X-a)^{m_g(a)} \tilde{g}(X)$ avec $\tilde{g}(a) \neq 0$, on a que

$$g'(X) = (X-a)^{m_g(a)-1} \underbrace{(m_g(a)\tilde{g}(X) + (X-a)\tilde{g}'(X))}_{\text{évaluation en a : } m_g(a)\tilde{g}(a) \neq 0 \text{ car } 1 \leq m_g(a) \leq k \text{ et } 0 < k < p},$$

donc,

$$m_{g'}(a) = m_g(a) - 1.$$

Par hypothèse de récurrence sur g' :

$$m_{g'}(a) < |\{i \in [\![1, k]\!], i a_i \neq 0\}|,$$

d'où :

$$m_g(a) < |\{i \in [\![0, k]\!], a_i \neq 0\}|.$$

□

Démonstration du théorème 3.1.2.2. Notons $C_j,\ j \in J$ les colonnes de $(\omega^{ij})_{i\in I,\ j\in J}$, qui sont donc des éléments de $(\mathbb{Q}(\omega))^{|I|}$. On a donc les équivalences suivantes :

$$\begin{aligned}
\det((\omega^{ij})_{i\in I,\ j\in J}) \neq 0 &\iff (C_j)_{j\in J} \text{ est libre} \\
&\iff \forall (a_j)_{j\in J} \in (\mathbb{Q}(\omega))^{|J|}, \sum_{j\in J} a_j C_j = 0 \implies \forall j \in J, a_j = 0 \\
&\iff \forall (a_j)_{j\in J} \in (\mathbb{Q}(\omega))^{|J|}, \left(\forall i \in I, \sum_{j\in J} a_j \omega^{ij} = 0\right) \implies \forall j \in J, a_j = 0 \\
&\iff \forall (a_j)_{j\in J} \in (\mathbb{Z}[\omega])^{|J|}, \left(\forall i \in I, \sum_{j\in J} a_j \omega^{ij} = 0\right) \implies \forall j \in J, a_j = 0
\end{aligned}$$

Justifions la dernière équivalence. Un sens est évident. Pour l'autre, soit $(a_j)_{j\in J} \in (\mathbb{Q}(\omega))^{|J|}$. Posons $d \in \mathbb{Z}[\omega]$ le produit des dénominateurs des $a_j, j \in J$. En particulier $d \neq 0$. Supposons que $\forall i \in I, \sum_{j\in J} a_j \omega^{ij} = 0$. Alors $\forall i \in I, \sum_{j\in J} \underbrace{d a_j}_{\in \mathbb{Z}[\omega]} \omega^{ij} = 0$. On en conclut que $\forall j \in J,\ d a_j = 0$, et donc que $\forall j \in J,\ a_j = 0$.

Pour montrer le théorème, nous allons donc montrer la dernière assertion. Soit $(a_j)_{j\in J} \in (\mathbb{Z}[\omega])^{|J|}$, et supposons que $\forall i \in I, \sum_{j\in J} a_j \omega^{ij} = 0$. On va montrer que $\forall j \in J \forall n \in \mathbb{N},\ (1-\omega)^n | a_j$, ce qui implique que $\forall j \in J\ a_j = 0$.

Posons $g(X) = \sum_{j\in J} a_j X^j \in \mathbb{Z}[\omega][X]$. Par supposition on a que $\forall i \in I,\ (\omega^i) = 0$, autrement dit il existe $f \in \mathbb{Z}[\omega][X]$ tel que $g(X) = \prod_{i\in I}(X - \omega^i) f(X)$.

Posons

$$\begin{aligned}
\varphi \colon \mathbb{Z}[\omega] &\longrightarrow \mathbb{Z}[\omega]/(1-\omega) = \mathbb{F}_p \\
X &\longmapsto 1,
\end{aligned}$$

définie au lemme A.2.1, qui est un morphisme d'anneau. On peut donc étendre φ de la manière suivante :

$$\tilde{\varphi}\colon \mathbb{Z}[\omega][X] \longrightarrow \mathbb{Z}[\omega]/(1-\omega)[X] = \mathbb{F}_p[X]$$
$$\sum_{j=0}^{m} q_j X^j \longmapsto \sum_{j=0}^{m} \varphi(q_j) X^j,$$

où $\forall P, Q \in \mathbb{Z}[\omega][X],\ \tilde{\varphi}(PQ) = \tilde{\varphi}(P)\tilde{\varphi}(Q)$.

Posons $\bar{g}(X) = \tilde{\varphi}(g) \in \mathbb{F}_p[X]$. Par ce qui précède :

$$\bar{g}(X) = \prod_{i \in I} \underbrace{\tilde{\varphi}(X - \omega^i)}_{=X-1} \tilde{\varphi}(f(X)) = (X-1)^{|I|} \tilde{\varphi}(f(X)),$$

d'où $m_{\bar{g}}(1) \geq |I|$.

Or $\bar{g}$ a par définition $|J|$ coefficients non nuls (car g aussi). Si par l'absurde $\bar{g} \neq 0$, on aurait par le lemme A.2.2 $|I| \leq m_{\bar{g}}(1) < |\{j \in J, \varphi(a_j) \neq 0\}| \leq |J|$, ce qui est absurde. On en déduit que $\forall j \in J,\ 1 - \omega | a_j$.

On peut réitérer l'argument sur le polynôme $h(X) = \sum_{j \in J} \frac{a_j}{1-\omega} X^j$. Par récurrence :

$$\forall j \in J, \forall n \in \mathbb{N},\ (1-\omega)^n | a_j,$$

ce qui est possible que si $\forall j \in J\ a_j = 0$. □

A.3 La preuve de Chebotarev

Cette preuve est issue de [5].

Soit $n \in [\![1, p]\!]$ la taille d'un mineur M de la matrice. L'idée pour cette dernière preuve est non plus de voir les entrées de la matrice comme éléments de $\mathbb{Q}(\omega)$ mais comme éléments de $\mathbb{Q}_p(\omega)$, où $\mathbb{Q}_p$ est la complétion de $\mathbb{Q}$ pour la valuation p-adique. Ce dernier corps, muni de sa valuation, est non-archimédien, et a pour uniformisante $\pi = \omega - 1$. Nous noterons v_π sa valuation. A l'image du lemme de Hensel, nous allons pouvoir développer chaque entrée

de la matrice en sommes suivant π. On aura donc

$$M = \sum_{k_1,\ldots,k_n \geq 0} D_{k_1,\ldots,k_n} \pi^{k_1+\ldots+k_n},$$

où l'on explicitera $D_{k_1,\ldots,k_n}$, faisant de la somme précédente en fait une somme finie. Nous montrerons alors ces trois faits sur les $D_{k_1,\ldots,k_n}$:

— Si $k_1 + \ldots + k_n < 0 + 1 + \ldots + (n-1)$, alors $D_{k_1,\ldots,k_n} = 0$.
— Si $k_1+\ldots+k_n = 0+1+\ldots+(n-1)$, alors $(D_{k_1,\ldots,k_n} \neq 0 \implies \{k_1,\ldots,k_n\} = \{0,\ldots,n-1\})$.
— Si $\{k_1,\ldots,k_n\} = \{0,\ldots,n-1\}$, alors $D_{k_1,\ldots,k_n}$ est premier à p, donc $v_\pi(D_{k_1,\ldots,k_n}) = 0$.

Grâce à cela, nous on concluront que $v_\pi(M) = \frac{n(n-1)}{2} \neq -\infty$, d'où $M \neq 0$.

Démonstration du théorème 3.1.2.2. Tout d'abord, vérifions que $\omega - 1$ est une uniformisante de $\mathbb{Q}_p(\omega)$ pour l'unique valeur absolue $|N_{\mathbb{Q}_p(\omega)/\mathbb{Q}_p}(\cdot)|_p^{1/(p-1)}$. La norme vaut :

$$N_{\mathbb{Q}_p(\omega)/\mathbb{Q}_p}(\omega - 1) = \begin{vmatrix} -1 & 0 & 0 & \cdots & 1 \\ 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{vmatrix} = (-1)^{p+1}.$$

Donc $|N_{\mathbb{Q}_p(\omega)/\mathbb{Q}_p}(\omega - 1)|_p = 0$, d'où $\omega - 1$ est de valuation égale à 1. Notons $\pi = \omega - 1$ cette uniformisante et v_π la valuation de $\mathbb{Q}_p(\omega)$.

Développons chaque entrée de la matrice en l'uniformisante :

$$\forall x, \xi \ [\![0, p-1]\!], \omega^{x\xi} = (\pi + 1)^{x\xi} = \sum_{k=0}^{x\xi} \binom{x\xi}{k} \pi^k.$$

Soit $M = \det(\omega^{x_i \xi_j})_{1 \leq i,j \leq n}$ un mineur la matrice $(\omega^{ij})_{i,j \in [\![0,p-1]\!]}$ où $x_i, \xi_j \in [\![0, p-1]\!]$ pour tout

$i, j \in [\![1, n]\!]$. Par multilinéarité du déterminant par rapport aux colonnes, développons M :

$$M = \begin{vmatrix} \sum_{k_1=0}^{x_1\xi_1} \binom{x_1\xi_1}{k_1}\pi^{k_1} & \cdots & \sum_{k_n=0}^{x_1\xi_n} \binom{x_1\xi_n}{k_n}\pi^{k_n} \\ \vdots & \ddots & \vdots \\ \sum_{k_1=0}^{x_n\xi_1} \binom{x_n\xi_1}{k_1}\pi^{k_1} & \cdots & \sum_{k_n=0}^{x_n\xi_n} \binom{x_n\xi_n}{k_n}\pi^{k_n} \end{vmatrix}$$

$$= \sum_{k_1,\ldots,k_n \geq 0} \underbrace{\begin{vmatrix} \binom{x_1\xi_1}{k_1} & \cdots & \binom{x_1\xi_n}{k_n} \\ \vdots & \ddots & \vdots \\ \binom{x_n\xi_1}{k_1} & \cdots & \binom{x_n\xi_n}{k_n} \end{vmatrix}}_{=D_{k_1,\ldots,k_n}} \pi^{k_1+\ldots+k_n}.$$

Ces dernières sommes étant en fait finies.

Nous allons maintenant estimer la valeur des $D_{k_1,\ldots,k_n}$.

Premièrement, supposons qu'il existe $d \in [\![1, n-1]\!]$ tel que $d+1$ entiers parmi $\{k_1, \ldots, k_n\}$ sont strictement inférieurs à d et montrons que $D_{k_1,\ldots,k_n} = 0$. Posons

$$\forall j \in [\![1, n]\!], P_j(X) = \frac{\prod_{s=0}^{k_j-1}(\xi_j X - s)}{k_j!} \in \mathbb{Q}[X]$$

qui est de degré k_j, de telle sorte que :

$$D_{k_1,\ldots,k_n} = \begin{vmatrix} P_1(x_1) & P_2(x_1) & \cdots & P_n(x_1) \\ \vdots & \vdots & & \vdots \\ P_1(x_n) & P_2(x_n) & \cdots & P_n(x_n) \end{vmatrix}.$$

Or $d+1$ polynômes de degrés strictement inférieurs à d sont linéairement dépendants, donc par supposition $P_1, \ldots, P_n$ sont linéairement dépendants. On en conclut que les colonnes sont liées et $D_{k_1,\ldots,k_n} = 0$.

Deuxièmement, montrons grâce à ce qui précède que si $k_1 + \ldots + k_n < 0 + \ldots + (n-1)$ alors $D_{k_1,\ldots,k_n} = 0$. Il suffit alors de montrer que :

$$k_1+\ldots+k_n < 0+\ldots+(n-1) \implies (\exists d \in [\![1, n-1]\!], \exists A \subseteq \{k_1, \ldots, k_n\}\ |A| \geq d+1, \forall k \in A, k < d).$$

Trions sans perte de généralités les $k_1, \ldots, k_n$ de telle sorte que $k_1 \leq \ldots \leq k_n$ (ce tri ne change rien à la nullité du déterminant ni à la somme des $k_1 \leq \ldots \leq k_n$). Par contraposée, supposons que : $\forall d \in [\![1, n-1]\!], \forall A \subseteq \{k_1, \ldots, k_n\}\ |A| \geq d+1, \exists k \in A, k \geq d$. Appliqué en $d = 1$, cela donne que parmi les $k_1, \ldots, k_n$, tous sauf au plus un sont supérieurs ou égaux à 1. Comme ils sont triés, on a que $k_i \geq 1$ pour tout $i \geq 2$. On peut répéter ce raisonnement pour tout les $d \in [\![1, n-1]\!]$, ce que donne :

$$\forall i \geq d, k_i \geq d-1.$$

En sommant les k_i, et comme $k_1 \geq 0$, on obtient que :

$$k_1 + \ldots + k_n \geq 0 + 1 + \ldots n - 1.$$

Troisièmement, supposons que $k_1 + \ldots + k_n = 0 + 1 + \ldots n - 1$ et montrons que si $D_{k_1,\ldots,k_n} \neq 0$ alors $\{k_1, \ldots, k_n\} = \{0, \ldots, n-1\}$. Supposons encore les $k_1, \ldots, k_n$ encore triés et que $D_{k_1,\ldots,k_n} \neq 0$, ce qui implique par le premier point que :

$$\forall d \in [\![1, n-1]\!], \forall A \subseteq \{k_1, \ldots, k_n\}\ |A| \geq d+1, \exists k \in A, k \geq d.$$

Avec le raisonnement donné au point précédent, on obtient que $\forall i \in [\![1, n]\!], k_i \geq i-1$ et $k_1 + \ldots + k_n \geq 0 + 1 + \ldots n - 1$. Or si par l'absurde il existe $i \in [\![1, n]\!], k_i > i-1$, alors $k_1 + \ldots + k_n > 0 + 1 + \ldots n - 1$ ce qui est absurde. D'où $\forall i \in [\![1, n]\!], k_i = i-1$. Enfin si les $k_1, \ldots, k_n$ ne sont plus supposés triés, on conclut que $\{k_1, \ldots, k_n\} = \{0, \ldots, n-1\}$.

Quatrièmement, supposons que $\{k_1, \ldots, k_n\} = \{0, \ldots, n-1\}$ et calculons $D_{k_1,\ldots,k_n}$. Pour simplifier, distinguons deux cas :

Cas 1 : si $\forall i \in [\![1,n]\!], k_i = i-1$, alors :

$$
\begin{aligned}
D_{k_1,\dots,k_n} &= \begin{vmatrix} \binom{x_1\xi_1}{0} & \binom{x_1\xi_2}{1} & \cdots & \binom{x_1\xi_n}{n-1} \\ \vdots & \vdots & & \vdots \\ \binom{x_n\xi_1}{0} & \binom{x_n\xi_2}{1} & \cdots & \binom{x_n\xi_n}{n-1} \end{vmatrix} \\
&= \begin{vmatrix} 1 & x_1\xi_2 & \cdots & \frac{\prod_{s=0}^{(n-1)-1}(x_1\xi_n - s)}{(n-1)!} \\ \vdots & \vdots & & \vdots \\ 1 & x_n\xi_2 & \cdots & \frac{\prod_{s=0}^{(n-1)-1}(x_n\xi_n - s)}{(n-1)!} \end{vmatrix} \\
&= \frac{\xi_2}{0!1!2!\dots(n-1)!} \begin{vmatrix} 1 & x_1 & (x_1\xi_3)^2 - x_1\xi_3 & \cdots & \prod_{s=0}^{n-2}(x_1\xi_n - s) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & (x_n\xi_3)^2 - x_n\xi_3 & \cdots & \prod_{s=0}^{n-2}(x_n\xi_n - s) \end{vmatrix} \\
&= \frac{\xi_1^0\xi_2^1\xi_3^1}{0!1!2!\dots(n-1)!} \begin{vmatrix} 1 & x_1 & x_1^2\xi_3 - x_1 & \cdots & \prod_{s=0}^{n-2}(x_1\xi_n - s) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2\xi_3 - x_n & \cdots & \prod_{s=0}^{n-2}(x_n\xi_n - s) \end{vmatrix} \\
&= \frac{\xi_1^0\xi_2^1\xi_3^1}{0!1!2!\dots(n-1)!} \begin{vmatrix} 1 & x_1 & x_1^2\xi_3 & \cdots & \prod_{s=0}^{n-2}(x_1\xi_n - s) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2\xi_3 & \cdots & \prod_{s=0}^{n-2}(x_n\xi_n - s) \end{vmatrix} \\
&= \frac{\xi_1^0\xi_2^1\xi_3^2}{0!1!2!\dots(n-1)!} \begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & \prod_{s=0}^{n-2}(x_1\xi_n - s) \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & \prod_{s=0}^{n-2}(x_n\xi_n - s) \end{vmatrix} \\
&\overset{\text{récurrence}}{=} \frac{\xi_1^0\xi_2^1\xi_3^2\dots\xi_n^{n-1}}{0!1!2!\dots(n-1)!} \underbrace{\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}}_{\text{on reconnaît un déterminant de Vandermonde}} \\
&= \frac{\xi_1^0\xi_2^1\xi_3^2\dots\xi_n^{n-1}}{0!1!2!\dots(n-1)!} \prod_{1\le i<j\le n}(x_j - x_i).
\end{aligned}
$$

Cas 2 : si $\{k_1,\dots,k_n\} = \{0,\dots,n-1\}$ alors il y a autant de manière pour les $k_1,\dots,k_n$ d'avoir $\{k_1,\dots,k_n\} = \{0,\dots,n-1\}$ que de permutations de $\{0,\dots,n-1\}$. Notons

$\mathfrak{S}'_n$ les permutations de $\{0,\dots,n-1\}$, et ε' la signature d'un élément de $\mathfrak{S}'_n$. Alors :

$$D_{k_1,\dots,k_n} = \sum_{\sigma'\in\mathfrak{S}'_n} \varepsilon'(\sigma') \frac{\xi_1^{\sigma'(0)}\xi_2^{\sigma'(1)}\xi_3^{\sigma'(2)}\dots\xi_n^{\sigma'(n-1)}}{0!1!2!\dots(n-1)!} \prod_{1\le i<j\le n}(x_j - x_i).$$

Or en effectuant le changement de variable

$$\sigma' \to \sigma : (j \in [\![1,n]\!] \mapsto \sigma(j) = \sigma'(j-1)+1),$$

on obtient :

$$D_{k_1,\dots,k_n} = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \frac{\prod_{j=1}^n \xi_j^{\sigma(j)-1}}{0!1!2!\dots(n-1)!} \prod_{1\le i<j\le n}(x_j - x_i).$$

On reconnaît de nouveau un déterminant de Vandermonde :

$$\sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^n \xi_j^{\sigma(j)-1} = \begin{vmatrix} 1 & \xi_1 & \xi_1^2 & \cdots & \xi_1^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi_n & \xi_n^2 & \cdots & \xi_n^{n-1} \end{vmatrix},$$

d'où :

$$D_{k_1,\dots,k_n} = \frac{\prod_{1\le i<j\le n}(\xi_j-\xi_i)\prod_{1\le i<j\le n}(x_j-x_i)}{0!1!2!\dots(n-1)!}.$$

Notons C cette dernière constante.

Au final, en combinant toutes ces informations on obtient que :

$$M = C\pi^{\frac{n(n-1)}{2}} + \pi^{\frac{n(n-1)}{2}+1} \underbrace{(\dots)}_{v_\pi(\dots)\ge 0}.$$

Or on remarque que $C \in \mathbb{N}^*$ (car c'est un déterminant d'une matrice à entrées entières), et que C est premier à p car p ne divise pas $\prod_{1\le i<j\le n}(\xi_j-\xi_i)\prod_{1\le i<j\le n}(x_j-x_i)$ et

$$\prod_{1\le i<j\le n}(\xi_j-\xi_i)\prod_{1\le i<j\le n}(x_j-x_i) = C0!1!2!\dots(n-1)!,$$

donc p ne divise pas C. D'où $v_\pi(C) = v_p(C) = 0$, et donc :

$$v_\pi(M) = \min\left(\frac{n(n-1)}{2}, \frac{n(n-1)}{2} + 1 + \underbrace{v_\pi(\ldots)}_{\geq 0}\right) = \frac{n(n-1)}{2} \neq -\infty.$$

En particulier, M est non nul. □

Annexe B Preuve du théorème de Cauchy-Davenport par la transformée de Dyson

Cette preuve est issue du livre [11].

Lemme B.0.0.1. *Soit G un groupe abélien fini, et $A, B \subseteq G$. S'il existe $t \in \mathbb{N}$ tel que $|A| + |B| \geq |G| + t$, alors :*

$$\forall g \in G, r_{A,B}(g) \geq t,$$

où l'on a posé $r_{A,B}(g) = |\{(a,b) \in A \times B, g = a + b\}|$.

Démonstration. Soit $g \in G$. Notons $g - B = g - b, b \in B$. On a :

$$\begin{aligned} |G| &\geq |A \cup (g - B)| \\ &= |A| + |g - B| - |A \cap (g - B)| \\ &= |A| + |B| - |A \cap (g - B)| \end{aligned}$$

D'où $|A \cap (g - B)| \geq |A| + |B| - |G| \geq t$. Autrement dit, il existe $a_1, \ldots, a_t \in A \cap (g - B)$ distincts. Donc il existe $b_1, \ldots, b_t \in B$ distincts tels que $a_i = g - b_i \forall i \in [\![1, t]\!]$. D'où $g = a_i + b_i \ \forall i \in [\![1, t]\!]$, et donc $r_{A,B}(g) \geq t$. □

Définition B.0.0.2 (Transformée de Dyson)**.** *Soit G un groupe abélien et $A, B \subseteq G$ non vides. Soit $e \in G$. Posons :*

$$A(e) = A \cup (B + e)$$

$$B(e) = B \cap (A - e)$$

La paire $(A(e), B(e))$ est appelée la transformée de Dyson en e de (A, B).

Voyons quelques propriétés des transformées de Dyson.

Lemme B.0.0.3. *Soit G un groupe abélien et $A, B \subseteq G$ non vides. Soit $e \in G$. On a :*

(i) $A(e) + B(e) \subseteq A + B$

(ii) $A(e) \setminus A = e + (B \setminus B(e))$

(iii) Si A et B sont finis, alors $|A(e)| + |B(e)| = |A| + |B|$

(iv) Si $e \in A$ et $0 \in B$ alors $e \in A(e)$ et $0 \in B(e)$

Démonstration. (i) Soit $x \in A(e) = A \cup (B + e)$ et $y \in B(e) = B \cap (A - e)$. Il existe $a \in A$ tel que $y = a - e$. Si $x \in A$, alors $x + y \in A + B$. Si $x \in (B + e)$, il existe $b \in B$ tel que $x = b + e$. Alors $x + y = b + e + a - e = a + b \in A + B$.

(ii)

$$\begin{aligned} A(e) \setminus A &= (B + e) \setminus A \\ &= \{b + e, b \in B, b + e \notin A\} \\ &= e + \{b \in B, b \notin A - e\} \\ &= e + \{b \in B, b \notin B(e)\} \\ &= e + (B \setminus B(e)) \end{aligned}$$

(iii) Comme $A \subseteq A(e)$ et $B(e) \subseteq B$, on a :

$$|A(e)| - |A| = |A(e) \setminus A| = |B \setminus B(e)| = |B| - |B(e)| \text{ par (ii).}$$

(iv) Supposons que $e \in A(e)$ et $0 \in B$. Alors $e \in A(e)$ et $0 = e - e \in A - e$. D'où $0 \in B \cap (A - e) = B(e)$.

□

Lemme B.0.0.4. *Soit $m \geq 2$ un entier, et $A, B \subseteq \mathbb{Z}/m\mathbb{Z}$. Si $0 \in B$ et pgcd$(b, m) = 1$ pour*

tout $b \in B \setminus \{0\}$*, alors :*

$$|A+B| \geq \min(m, |A|+|B|-1).$$

Démonstration. Supposons que $0 \in B$ et $\text{pgcd}(b,m) = 1$ pour tout $b \in B \setminus \{0\}$.

Si $|A|+|B| \geq m+1$, par le lemme B.0.0.1 appliqué à $t = 1$, on a $\forall x \in \mathbb{Z}/m\mathbb{Z},\ r_{A,B}(x) \geq 1$. Donc $A + B = \mathbb{Z}/m\mathbb{Z}$, d'où $|A+B| = m \geq \min(m, |A|+|B|-1)$.

Supposons donc que $|A|+|B| \leq m$. Alors $\min(m, |A|+|B|-1) = |A|+|B|-1 \leq m-1$. Distinguons deux cas.

Cas 1 : si $|A| = 1$ ou $|B| = 1$. Alors :

$$\begin{aligned} |A+B| &= \begin{cases} |A| & \text{si } |B| = 1 \\ |B| & \text{si } |A| = 1 \end{cases} \\ &= |A| + |B| - 1 \end{aligned}$$

Cas 2 : si $|A| \geq 2$ et $|B| \geq 2$.

Supposons par l'absurde qu'il existe $A, B \subseteq \mathbb{Z}/m\mathbb{Z}$ tels que :

$$|A|,\ |B| \geq 2,\ 0 \in B \text{ et } \forall b \in B \setminus \{0\},\ \text{pgcd}(b,m) = 1$$

mais vérifiant :

$$|A+B| < \min(m, |A|+|B|-1) = |A|+|B|-1.$$

Prenons (A, B) tel que B soit de cardinal minimal pour cette propriété.

L'idée est de montrer qu'il existe $e \in \mathbb{Z}/m\mathbb{Z}$ tel que la transformée de Dyson en e $(A(e), B(e))$ vérifie également la propriété mais $|B(e)| < |B|$.

Montrons tout d'abord que $A \neq \mathbb{Z}/m\mathbb{Z}$. En effet par l'absurde si $A = \mathbb{Z}/m\mathbb{Z}$ alors $A \subseteq A + B$ (car $0 \in B$) d'où $m \leq |A+B|$ ce qui est absurde car

$$|A+B| < |A|+|B|-1 \leq m-1.$$

Comme $|B| \geq 2$, il existe $b^* \in B \setminus \{0\}$. Montrons qu'il existe $e \in A$ tel que $e+b^* \notin A$. Supposons par l'absurde que : $\forall e \in A,\ e + b^* \in A$. Alors par récurrence :

$$\forall e \in A,\ \forall j \in [\![0, m-1]\!],\ e + jb^* \in A.$$

Comme A est non vide, il existe $e \in A$. On a donc $\{e+jb^*, j \in [\![0, m-1]\!]\} \subseteq \mathbb{Z}/m\mathbb{Z}$. Or comme $\text{pgcd}(b^*, m) = 1$, b^* est inversible dans $\mathbb{Z}/m\mathbb{Z}$, et donc si $e+jb^* = e+j'b^*$ pour $j, j' \in [\![0, m-1]\!]$, alors $j = j'$. D'où $|\{e + jb^*, j \in [\![0, m-1]\!]\}| = m$ et

$$\mathbb{Z}/m\mathbb{Z} = \{e + jb^*, j \in [\![0, m-1]\!]\}.$$

Or :

$$\{e + jb^*, j \in [\![0, m-1]\!]\} \subseteq A \subseteq \mathbb{Z}/m\mathbb{Z},$$

donc $A = \mathbb{Z}/m\mathbb{Z}$, ce qui est absurde. D'où il existe $e \in A$ tel que $e + b^* \notin A$.
Par le lemme B.0.0.3, on a :

$$\begin{aligned} |A(e) + B(e)| &\overset{(i)}{\leq} |A + B| \\ &< |A| + |B| - 1 \\ &\overset{(iii)}{=} |A(e)| + |B(e)| - 1. \end{aligned}$$

De plus, comme $e \in A$ et $0 \in B$, par (iv) du lemme B.0.0.3, on a que $0 \in B(e)$. Comme $B(e) \subseteq B$, on a : $\forall b \in B(e) \setminus \{0\}, \text{pgcd}(b, m) = 1$.
Par l'absurde si $|A(e)| \leq 1$ ou $|B(e) \leq 1|$, alors par le cas 1 $|A(e) + B(e)| = |A(e)| + |B(e)| - 1$.
Enfin, comme $b^* \in B$ et $b^* \notin B(e)$ (car $b^* \notin A - e$) on obtient $|B(e)| < B$.
D'où $(A(e), B(e))$ vérifie aussi la proposition, ce qui est absurde par minimalité du cardinal de B.

□

Démonstration de théorème de Cauchy-Davenport 3.2.0.1. On aimerait appliquer lemme B.0.0.4,

mais 0 n'appartient pas forcément à B. On va alors translater B pour qu'il contienne 0. Comme $B \neq \emptyset$, il existe $b_0 \in B$, et posons $B' = B - b_0$. Ce dernier vérifie donc $|B'| = |B|$ et $|A + B'| = |A + B|$. Maintenant $0 \in B'$, et on a encore : $\forall b \in B' \setminus \{0\},\ \text{pgcd}(b, p) = 1$. Le lemme B.0.0.4 appliqué à (A, B') donne :

$$|A + B| = |A + B'| \geq \min(p, |A| + |B'| - 1) = \min(p, |A| + |B| - 1).$$

□

Références

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Annals of mathematics*, 139(3) :703–722, 1994.

[2] A. Bonami and S. Ghobber. Equality cases for the uncertainty principle in finite abelian groups. *Acta Scientiarum Mathematicarum*, 79(3) :507–528, 2013.

[3] D. L. Donoho and P. B. Stark. Uncertainty principles and signal recovery. *SIAM journal on applied mathematics*, 49(3) :906–931, 1989.

[4] P. E. Frenkel. Simple proof of Chebotarev's theorem on roots of unity. *preprint.*, page math.AC/0312398, 2004.

[5] H. W. Lenstra and P. Stevenhagen. Chebotarëv and his density theorem. *Math. Intelligencer*, 18 :26–37, 1996.

[6] I. I. Martin. *Character theory of finite groups.* Pure and applied mathematics, a series of monographs and textbooks. Academic Press, 1976.

[7] R. Meshulam. An uncertainty inequality and zero subsums. *Discrete mathematics*, 84(2) :197–200, 1990.

[8] R. Meshulam. An uncertainty inequality for groups of order pq. *European journal of combinatorics*, 13(5) :401–407, 1992.

[9] R. Meshulam. An uncertainty inequality for finite abelian groups. *European journal of combinatorics*, 27(1) :63–67, 2006.

[10] M. R. Murty and J. P. Whang. The uncertainty principle and a generalization of a theorem of Tao. *Linear algebra and its applications*, 437(1) :214–220, 2012.

[11] M. B. Nathanson. *Additive number theory : inverse problems and the geometry of sumsets.* Graduate texts in mathematics. Springer, 1996.

[12] J. E. Olson. A combinatorial problem on finite abelian groups, i. *Journal of number theory*, 1(1) :8–10, 1969.

[13] J.-E. Rombaldi. *Mathématiques pour l'agrégation : algèbre et géométrie.* De Boeck Supérieur, 2e édition edition, 2021.

[14] J.-P. Serre and L. L. Scott. *Linear Representations of Finite Groups*. Springer International Publishing, 1977.

[15] T. Tao. An uncertainty principle for cyclic groups of prime order. *Mathematical Research Letters*, 12 :342–351, 2005.

[16] A. Terras. *Fourier analysis on finite groups and applications*. London Mathematical Society student texts. Cambridge University Press, 1999.

[17] A. Wigderson and Y. Wigderson. The uncertainty principle : Variations on a theme. *Bulletin (new series) of the American Mathematical Society*, 58(2) :225–261, 2021.