Caractères d'un GAF et TFD

Groupes abéliens finis et transformée de Fourier discrète

0.1 Les groupes abéliens finis

La théorie des groupes abéliens finis prend une place particulière au sein de la théorie des représentations. On peut déjà constater que si chaque classe de conjugaison est de cardinal 1 (donc si le groupe fini G est abélien), alors le groupe G est de même cardinal que $\mathrm{Irr}(G)$, et réciproquement. Mais le meilleur est à venir, car, comme nous allons le voir, $\mathrm{Irr}(G)$ a dans ce cas une structure de groupe abélien fini, de sorte que l'on voit apparaître une jolie dualité entre G et le groupe $\mathrm{Irr}(G)$, noté, dans ce contexte, $\widehat{G}$. Par dualité, on entend ici que les propriétés de $\mathrm{Irr}(G)$ vont se refléter dans G, et réciproquement. Voici donc une belle occasion de voir en oeuvre les miracles de la dualité dans un autre contexte que celui des espaces de dimension finie.

Cette dualité permet alors d'interpréter la forme hermitienne G-invariante sur $\mathbb{C}[G]$ comme un morphisme de $\mathbb{C}[G]$ vers $\mathbb{C}[\widehat{G}]$, selon un procédé bien connu dans le cadre des formes quadratiques/hermitiennes sur un espace vectoriel. Ce morphisme n'est rien d'autre que la *transformée de Fourier*, ou plutôt son analogue discret. La théorie des représentations des groupes abéliens finis devient un *toy model* qui permet d'y voir plus clair dans l'univers de l'analyse harmonique.

0.1.1 Caractères d'un groupe abélien fini

Dans la suite, on notera $(A, +)$ un groupe abélien fini (GAF), d'ordre n. On travaille toujours sur le corps des complexes, et donc par représentation, resp. caractère, on entend représentation, resp. caractère, complexe.

Notation. Si A est un GAF, on appelle dual de A, l'ensemble $\widehat{A}$ des caractères irréductibles de A.

Proposition. L'ensemble $\widehat{A}$ est de cardinal n. Une représentation de A est irréductible si et seulement si elle est de degré 1. En conséquence, l'ensemble $\widehat{A}$ s'identifie à l'ensemble des morphismes de $(A, +)$ dans $(\mathbb{C}^*, \times)$ et il possède une structure de groupe abélien pour la multiplication usuelle des fonctions de A dans $\mathbb{C}$. L'élément neutre de ce groupe est le caractère trivial χ_{triv}.

Démonstration. Comme A est abélien, ses classes de conjugaison sont singletonnes ; il y en a donc n. On en déduit l'existence de n représentations irréductibles de degré d_i, i de 1 à n, tels que $\sum_i d_i^2 = n$, ce qui force $d_i = 1$ pour tout i. Les représentations irréductibles vont donc de A vers $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^*$ et donc, les caractères irréductibles s'identifient à des morphismes de A vers $\mathbb{C}^*$. L'ensemble $\widehat{A}$ hérite donc bien de la structure de groupe (multiplicatif) de $\mathbb{C}^*$.

Remarque. Le fait que toute représentation irréductible d'un GAF A est de degré 1 peut aussi être vu comme une conséquence directe de la codiagonalisation. En effet, par Lagrange, toutes les matrices de représentation sont diagonalisables et, par commutativité, elles sont simultanément diagonalisables. Ceci implique que l'espace peut se décomposer en somme directe de droites propres communes pour l'action de tout élément de A.

La nomenclature change lorsque l'on passe des groupes quelconques aux groupes abéliens finis. Les morphismes de A vers $\mathbb{C}^*$ sont dans ce contexte appelés usuellement *caractères* de A, alors que dans le cadre des groupes en général, ce seraient plutôt les *caractères irréductibles*. Il est important de noter également qu'en degré 1, on peut identifier une représentation à son caractère (en fait, une matrice de taille 1 à sa trace), deux représentations irréductibles distinctes sont automatiquement non isomorphes [1].

Voici tout de suite un exemple fondamental :

Exemple 0.1 (L'aube de la dualité : le cas $\mathbb{Z}/n\mathbb{Z}$)**.**

Soit $A = \mathbb{Z}/n\mathbb{Z}$. Alors, $\widehat{A}$ est l'ensemble des morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{C}^*$. Or, par passage au quotient, un tel morphisme est entièrement déterminé par l'image de $\overline{1}$ dans l'ensemble U_n des racines n-ièmes de l'unité de $\mathbb{C}^*$. On voit donc que $\widehat{A}$ est naturellement isomorphe au groupe U_n, lui-même (non naturellement) isomorphe à $\mathbb{Z}/n\mathbb{Z}$. On commence à voir apparaître, comme dans la dualité des espaces vectoriels de dimension finie, un isomorphisme (non canonique) entre A et son dual $\widehat{A}$.

Exemple 0.2 (Table de caractères pour $\mathbb{Z}/n\mathbb{Z}$)**.**

Un isomorphisme entre $\mathbb{Z}/n\mathbb{Z}$ et U_n provient du choix d'un générateur de U_n, c'est-à-dire d'une racine primitive n-ième de l'unité. Si l'on fixe une telle racine ω, alors, on voit facilement que la table de caractères est donnée par $u_{ij} = \omega^{ij}$, pour $1 \leq i, j \leq n-1$. La matrice de la table de caractères est donc une matrice de Vandermonde.

1. Comme le caractère caractérise, une représentation de degré 1, qui est égale à son propre caractère, s'autocaractérise. Enorme !

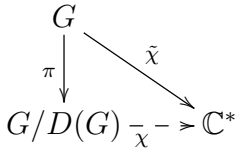
En fait, les propriétés des représentations des groupes abéliens finis concernent tous les groupes finis puisque ceux-ci possèdent des quotients abéliens. On rappelle que si G est un groupe alors on définit le sous-groupe $D(G)$ comme engendré par les commutateurs $ghg^{-1}h^{-1}$, $g, h \in G$, de G. Le sous-groupe $D(G)$ est distingué [2] et c'est le sous-groupe distingué minimal de G (pour l'inclusion) tel que le quotient soit abélien.

Remarque. Le groupe dérivé reprend ses droits en théorie des représentations de par son lien étroit avec les représentations de degré 1. En effet, une représentation de degré 1 est un morphisme de G dans le groupe abélien $\mathbb{C}^*$. Il en résulte que $D(G)$ s'envoie automatiquement vers 1. Et plus, généralement, si V est, en tant que représentation de G, somme directe de représentations de degré 1, alors l'image de $D(G)$ est réduite à l'identité.

On a le corollaire suivant :

Corollaire 0.3.
Soit G un groupe fini. Alors, le nombre de représentations irréductibles de G de degré 1 est égal à l'indice de $D(G)$ dans G. En particulier, G est abélien si et seulement si $\mathrm{Irr}(G) = |G|$.

Démonstration. Comme $G/D(G)$ est un groupe abélien, toutes ses représentations irréductibles sont de degré 1 et, par la proposition 0.1.1, il y en a exactement $k := |G/D(G)|$, c'est-à-dire l'indice de $D(G)$. Or, l'ensemble de ces représentations est en bijection avec l'ensemble des représentations (irréductibles) de degré 1 de G. En effet, soit π la surjection canonique de G sur $G/D(G)$, alors la bijection est donnée par l'application qui envoie le caractère χ de $G/D(G)$ sur la représentation $\tilde{\chi} := \chi \circ \pi$ de G. La bijection inverse est donnée par le passage au quotient, puisque si $\tilde{\chi}$ est un morphisme de G dans $\mathbb{C}^*$, alors, $\mathbb{C}^*$ étant abélien, tout commutateur de G s'envoie vers 1, et donc $D(G)$ est dans le noyau de ce morphisme :



Pour la dernière assertion, il suffit de voir la réciproque, car la proposition 0.1.1 assure l'implication directe.

2. Il est stable par tout automorphisme φ de G, puisque $\varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1}$. Donc, en particulier, il est stable par tout automorphisme intérieur.

Supposons donc $\mathrm{Irr}(G) = |G|$. Comme la somme des carrés des degrés des représentations irréductibles vaut $|G|$, elles sont toutes de degré 1. Le groupe dérivé $D(G)$ est donc d'indice $|G|$, ce qui implique que $D(G)$ est trivial ; G est abélien.

La proposition qui suit précise des isomorphismes naturels en dualité de GAF [3].

Proposition. Soit A et B deux GAF. On a les isomorphismes naturels de groupes

1. $\widehat{A} \times \widehat{B} \simeq \widehat{A \times B}$,
2. $A \simeq \widehat{\widehat{A}}$.

Démonstration. On va construire dans les deux cas un morphisme naturel, injectif. Par égalité des ordres, voir proposition 0.1.1, on obtiendra bien l'isomorphisme recherché.

1. On construit une application $\Delta : \widehat{A} \times \widehat{B} \simeq \widehat{A \times B}$, qui envoie (ϕ, ψ) sur l'application $\Delta_{\phi,\psi} : (a, b) \mapsto \phi(a)\psi(b)$. L'égalité $\phi(a + a')\psi(b + b') = \phi(a)\psi(b)\phi(a')\psi(b')$ prouve que l'application $\Delta_{\phi,\psi}$ est bien dans $\widehat{A \times B}$. L'égalité $(\phi\phi')(a)(\psi\psi')(b) = \phi(a)\psi(b)\phi'(a)\psi'(b)$ prouve que Δ est bien un morphisme de groupes. L'injectivité est claire : on retrouve ϕ et ψ à partir de $\Delta_{\phi,\psi}$ en posant respectivement $b = 0$ et $a = 0$ dans $\Delta_{\phi,\psi}(a, b)$.
2. Notons que $\widehat{\widehat{A}}$ a un sens puisque $\widehat{A}$ est un GAF. On construit une application $\iota : A \simeq \widehat{\widehat{A}}$ qui envoie a sur l'application $\iota_a : \phi \mapsto \phi(a)$. L'égalité $(\phi\phi')(a) = \phi(a)\phi'(a)$ prouve que ι_a est bien dans $\widehat{\widehat{A}}$, et l'égalité $\phi(a + a') = \phi(a)\phi(a')$ prouve que ι est un morphisme de groupes. L'injectivité est claire puisque ϕ peut être retrouvée à partir de la donnée des $\phi(a)$ pour tout a de A.

Exemple 0.4 (Table de caractères pour $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$)**.**

Pour construire la table de caractères de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, on doit trouver 6 caractères distincts. Comme $\widehat{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}} \simeq \widehat{\mathbb{Z}/2\mathbb{Z}} \times \widehat{\mathbb{Z}/3\mathbb{Z}}$, on se ramène aux caractères des groupes cycliques, étudiés ci-dessus. Voir la table de caractères en section 0.1.3.

3. La dualité des GAF ! Voilà un bon titre d'album de Gaston.

0.1.2 Théorème de relèvement des caractères et théorème de structure

Dans le cadre de l'analogie entre GAF et espaces vectoriels de dimension finie, le théorème de relèvement des caractères est au fond un théorème qui s'apparente au théorème de la base incomplète, dans le sens où ce dernier permet de voir que, si F est un sous-espace de E, alors le morphisme de restriction $E^* \to F^*$ est surjectif. Plus généralement, la belle dualité permet de voir que la transposée d'un morphisme injectif (l'injection naturelle de F dans E) est un morphisme surjectif (la restriction).

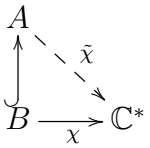
Théorème 0.5 (Relèvement des caractères)**.**
Soit A un GAF et B un sous-groupe. Alors, le morphisme de restriction de $\widehat{A}$ sur $\widehat{B}$ est surjectif. Dit autrement, tout caractère de B peut être relevé en un caractère de A.

Démonstration. Soit r ce morphisme. Son noyau est donc le sous-groupe des caractères χ de A tels que $\chi_{|B}$ est trivial. Par passage au quotient (tout sous-groupe est distingué dans le cas abélien), ce noyau s'identifie à $\widehat{A/B}$. On a donc

$$|\mathrm{Im}(r)| = \frac{\left|\widehat{A}\right|}{\left|\widehat{A/B}\right|} = \frac{|A|}{|A/B|} = |B| = \left|\widehat{B}\right|.$$

La surjectivité en découle.

Un petit dessin valant mieux qu'un long discours, on peut résumer schématiquement les choses avec un diagramme commutatif :



On va en déduire une preuve du théorème de structure des groupes abéliens finis. Unité et harmonie : avec l'approche des modules sur un anneau principal, c'est finalement équivalent au théorème de décomposition de Frobenius, [Tome 1 ed.2, Théorème 5.9]. C'est pourquoi on ne s'étonnera pas des similitudes entre les deux preuves.

Théorème 0.6 (Théorème de structure des groupes abéliens finis)**.**
Soit A un GAF. Il existe une unique famille d'entiers $a_i \geq 2$, i de 1 à s, telle que a_{i+1} divise a_i pour tout i de 1 à $s-1$, et telle que

$$A \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_s\mathbb{Z}.$$

Définition 0.7. Les a_i, de par leur unicité, sont appelés *facteurs invariants* du groupe abélien fini A.

Par l'exemple 0.1 et la proposition 0.1.1, le théorème de structure a pour corollaire immédiat :

Corollaire 0.8. Soit A un GAF. Alors A est isomorphe à son dual $\widehat{A}$.

Il va sans dire que l'isomorphisme est non canonique (il dépend du choix de racines primitives de l'unité [4]).

Démonstration. *Existence.*
Commençons par le lemme :

Lemme 0.9. Soit x_1 dans A d'ordre *maximal* a_1. Alors, l'ordre de tout élément de A divise a_1.

Preuve du lemme. Dire que a divise b revient à dire que pour tout p premier, $\nu_p(a) \leq \nu_p(b)$, où p désigne la p-valuation. Supposons donc, par l'absurde, qu'il existe x_1' dans A d'ordre a_1', et p premier fixé tel que $\alpha' := \nu_p(a_1') > \alpha := \nu_p(a_1)$. On a donc $a_1 = p^\alpha k$, resp. $a_1' = p^{\alpha'} k'$, où k est premier avec p^α, resp. k' premier avec $p^{\alpha'}$. On va construire un élément de A d'ordre $p^{\alpha'} k > a_1$, ce qui prouvera bien l'assertion par l'absurde. On a $y_1 := p^\alpha x_1$ d'ordre k et $y_1' := k' x_1'$ d'ordre $p^{\alpha'}$. Comme k et $p^{\alpha'}$ sont premiers entre eux, $y_1 + y_1'$ est bien d'ordre $p^{\alpha'} k$. En effet, d'une part $p^{\alpha'} k$ annule $y_1 + y_1'$, et d'autre part, si d annule $y_1 + y_1'$, alors $dy_1 = -dy_1' \in \langle y_1 \rangle \cap \langle y_1' \rangle = \{0\}$, par Lagrange, ce qui force $p^{\alpha'}$ et k à diviser d. ◇

Pour montrer l'existence, il suffit de montrer que le sous-groupe cyclique engendré par x_1 possède un supplémentaire B dans A, *i. e.* $A \simeq \langle x_1 \rangle \times B$, et d'appliquer une récurrence sur $|A|$. Montrons donc l'existence de ce supplémentaire. Soit ω_1 une racine primitive a_1-ième de l'unité et χ le caractère (comprendre ici morphisme) de $\langle x_1 \rangle$ qui envoie x_1 sur ω_1 ; χ est donc un isomorphisme de $\langle x_1 \rangle$ dans le groupe U_{a_1}. Par le théorème de relèvement, on peut prolonger χ en un morphisme $\tilde{\chi}$ de A vers $\mathbb{C}^*$. Or, comme l'ordre de tout élément de A divise a_1, l'image de $\tilde{\chi}$ reste dans U_{a_1}. On a donc une surjection $\tilde{\chi}$ de A vers U_{a_1}, munie d'une section, la réciproque χ^{-1}, de U_{a_1} vers $\langle x_1 \rangle \subset A$, ce qui prouve, par [Tome 1 ed.2, Chap. II, Corollaire 5.3.4], que A est un produit semi-direct $A \simeq \langle x_1 \rangle \rtimes \ker(\tilde{\chi})$. Comme A est abélien, le produit est en fait un produit direct.

Unicité. Montrons maintenant l'unicité des a_i. Pour cela, nous allons caractériser les a_i, en caractérisant, pour tout p premier, leur p-valuation $\nu_p(a_i)$.

4. Ça vous énerve pas les gens qui disent "ça va sans dire" et qui le disent quand même ? C'est insupportable !

Lemme 0.10. Soit n_p, resp. m_p, la p-valuation de $|A|$, resp. a_1. Soit A_j le sous-groupe $\{x \in A,\, p^j x = 0\}$ de A, et $\lambda_j := \nu_p\big(|A_j|\big) - \nu_p\big(|A_{j-1}|\big)$.

Alors, $(\lambda_1 \geq \lambda_2 \cdots \geq \lambda_{m_p}) \geq 0)$ est une partition de n_p. La famille $(\nu_p(a_i))$ forme la partition duale [5] de cette partition.

Preuve du lemme. Les sous-groupes A_i sont emboîtés, avec $\{0\} \subsetneq A_1$ par le lemme de Cauchy, et $A_{m_p} = A_k$ pour $m_p \leq k$, par la propriété de maximalité de a_1 du lemme 0.9. De plus, tous les éléments de A_j sont d'ordre divisant p^j, donc, encore par le lemme de Cauchy (ici, sa version contraposée), les A_j sont des p-groupes ; les λ_j sont bien des entiers.

La suite des $|A_i|$ s'essouffle, exactement comme dans [Tome 1 ed.2, Chap. III, Lemme 2.2.1], puisque la multiplication par p induit un morphisme de A_{i+1} dans A_i, puis, un morphisme de A_{i+1} dans A_i/A_{i-1} de noyau A_i. On a donc une injection de A_{i+1}/A_i dans A_i/A_{i-1}, ce qui donne bien les inégalités voulues sur les λ_i. Il vient donc que λ est une partition de $\sum_j \lambda_j = \nu_p(\big|A_{m_p}\big|)$.

Calculons maintenant précisément λ_i. On suppose dans un premier temps que $A = \mathbb{Z}/a\mathbb{Z}$, où a est un entier. Posons $k = \nu_p(a)$, c'est-à-dire, $a = p^k b$, avec b premier avec p. Si $i \leq k$, il y a exactement p^i classes x de $\mathbb{Z}/a\mathbb{Z}$ telles que $p^i x = 0$: ce sont les multiples de $p^{k-i}b$. Si $i > k$, alors il y a p^k classes x de $\mathbb{Z}/a\mathbb{Z}$ telles que $p^i x = 0$: ce sont les multiples de b. On en déduit dans ce cas que $|A_i| = p^{\min\{\nu_p(a),i\}}$. Dans le cas général, on obtient :

$$|A_i| = \prod_{j=1}^{s} p^{\min\{\nu_p(a_j),i\}}, \text{ et donc } \nu_p(|A_i|) = \sum_{j=1}^{s} \min\{\nu_p(a_j), i\}.$$

En particulier, comme m_p est le maximum des $\nu_p(a_j)$, il vient, d'une part

$$\nu_p(\big|A_{m_p}\big|) = \sum_{j=1}^{s} \nu_p(a_j) = n_p,$$

ce qui implique que λ est bien une partition de n_p.

D'autre part, il vient

$$\lambda_i := \nu_p(|A_i|) - \nu_p(|A_{i-1}|) = |\{j,\, i \leq \nu_p(a_j)\}|\,,$$

ce qui signifie que les partitions $(\nu_p(a_i))$ et (λ_j) sont en dualité.

5. La partition duale a été vue en Tome 1 ed.2, Chap. III, Annexe B, Définition 2.3] dans le passage, dans un tableau de Young, de la lecture horizontale à la lecture verticale, ou inversement. Autrement dit, si $\lambda = (\lambda_1 \geq \cdots \geq \lambda_s)$ est une partition de n, alors son dual $\lambda^* = (\lambda_1^* \geq \cdots \geq \lambda_{s^*}^*)$ est une partition de n donnée par $\lambda_i^* = |\{j,\, i \leq \lambda_j\}|$. On a $(\lambda^*)^* = \lambda$.

Définition 0.11. Le nombre a_1 est appelé *exposant* du groupe. C'est le plus petit commun multiple des ordres des éléments du groupe. C'est en quelque sorte l'équivalent du polynôme minimal pour un espace vectoriel E muni d'un endomorphisme.

Exemple 0.12. Par exemple, quels sont les facteurs invariants (a_i) du groupe $A = \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$?

Pour cela, il faut briser-rassembler (tout un programme !)
1) *briser* A en p-groupes, par le lemme chinois, puis
2) *rassembler* en p-valuations décroissantes.

1) $A \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}) \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z})$.
2) $A \simeq (\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/360\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Donc, les facteurs invariants de A sont $(360, 36, 2)$. Un groupe abélien fini sera isomorphe à A si et seulement s'il possède cette même famille de facteurs invariants.

Remarque. On peut montrer l'unicité de bien des manières, sans le langage des partitions. L'avantage de la méthode est qu'elle s'unifie joliment avec celle utilisée dans la réduction. On peut d'ailleurs se permettre, pour le plaisir et sans même aller plus loin, de faire un pont entre deux mondes : celui des groupes abéliens finis et celui des $\mathbb{C}-$espaces de dimension finie, munis d'un endomorphisme u. On fixera un diviseur premier p de $|A|$ et un diviseur $(X - \lambda)$ de χ_u, ce qui signifie que λ est valeur propre de u.

Groupe abélien fini A	$\mathbb{C}$-espace E muni d'un endomorphisme u
$A \simeq \widehat{\widehat{A}}$ (canonique)	$E \simeq E^{**}$ (canonique)
$A \simeq \widehat{A}$ (non canonique)	$E \simeq E^{*}$ (non canonique)
cardinal $\lvert A\rvert$	polynôme caractéristique χ_u
exposant a_1	polynôme minimal μ_u
facteurs invariants $a_1, \cdots, a_s$	polynômes invariants de similitude $P_1, \cdots, P_s$
ordre d'un élément	polynôme minimal $\mu_{u,x}$, pour $x \in E$, voir [Tome 1, Chap. III-5]
théorème de Lagrange	théorème de Cayley-Hamilton
lemme de Cauchy	existence d'un vecteur propre
lemme chinois	lemme des noyaux
sous-groupe cyclique	sous-espace cyclique, voir [Tome 1, Chap. III-5]
théorème de structure	décomposition de Frobenius

La comparaison Lagrange/Cayley-Hamilton est un peu osée ; elle est juste là pour marquer les esprits. Il faut le comprendre dans le sens où, d'une part,

l'ordre d'un élément divise l'ordre du groupe, et d'autre part, le polynôme minimal $\mu_{u,x}$ d'un élément x de E, voir [Tome 1, Chap. III-5], divise le polynôme caratéristique.

0.1.3 Tables de caractères

Voici, pour se fixer les idées, la table de caractères de $\mathbb{Z}/4\mathbb{Z}$ et celle du produit direct $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Table de caractères de $\mathbb{Z}/4\mathbb{Z}$, et au-delà

$\mathbb{Z}/4\mathbb{Z}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
χ_0	1	1	1	1
χ_1	1	i	-1	$-i$
χ_2	1	-1	1	-1
χ_3	1	$-i$	-1	i

Dans le tableau ci-dessus, on a fixé i comme racine primitive 4-ième de l'unité, et χ_k est le caractère qui envoie $\bar{1}$ sur i^k.

Plus généralement, on se fixe une racine primitive n-ième de l'unité ω, et on note χ_k le caractère (bien défini) de $\mathbb{Z}/n\mathbb{Z}$ tel que

$$\chi_k(\overline{a}) = \omega^{ka}.$$

Alors, la matrice de la table de caractères est donnée par

$$V_n := \big(\chi_i(\bar{j})\big)_{0\leq i,j\leq n-1} = (\omega^{ij})_{0\leq i,j\leq n-1}.$$

Table de caractères de $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, et au-delà

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1}\bar{2})$
$\chi_0 \otimes \chi_0$	1	1	1	1	1	1
$\chi_0 \otimes \chi_1$	1	j	j^2	1	j	j^2
$\chi_0 \otimes \chi_2$	1	j^2	j	1	j^2	j
$\chi_1 \otimes \chi_0$	1	1	1	-1	-1	-1
$\chi_1 \otimes \chi_1$	1	j	j^2	-1	$-j$	$-j^2$
$\chi_1 \otimes \chi_2$	1	j^2	j	-1	$-j^2$	$-j$

Le lecteur reconnaîtra en un clin d'oeil que cette matrice de taille 6 est constituée de 4 blocs de taille 3 : V_3, V_3, V_3, $-V_3$, et que les scalaires devant la matrice V_3 sont les coefficients 1, 1, 1, -1 de la matrice V_2. Ceci appelle une définition *ad hoc* :

Définition 0.13 (Produit tensoriel de deux matrices)**.** Soient n et p deux entiers naturels non nuls et soient U une matrice $n \times n$ et V une matrice $p \times p$, toutes deux à coefficients complexes. On définit le *produit tensoriel* de U et V comme la matrice $np \times np$ décrite par blocs de la façon suivante :

$$U \otimes V = \begin{pmatrix} u_{11}V & u_{12}V & \cdots & u_{1n}V \\ u_{21}V & u_{22}V & \cdots & u_{2n}V \\ \vdots & & & \vdots \\ u_{n1}V & u_{n2}V & \cdots & u_{nn}V \end{pmatrix} \in \mathcal{M}_{np}(\mathbb{C}).$$

Proposition. Soit A, resp. B, un GAF, que l'on suppose ordonné (comme ensemble), et soit $\widehat{A}$, resp. $\widehat{B}$, son dual, supposé ordonné également. Soit U, resp. V, la matrice de la table de caractères de A, resp. B. Alors, en ordonnant $A \times B$ et $\widehat{A \times B} \simeq \widehat{A} \times \widehat{B}$ par l'ordre lexicographique, la matrice de la table de caractères de $A \times B$ est le produit tensoriel $U \otimes V$.

Démonstration. Tout d'abord, on voit que si ϕ est un caractère de A et ψ un caractère de B, alors $\phi \otimes \psi(a, b) = \phi(a)\psi(b)$ définit un caractère (un morphisme de groupes) du produit direct $A \times B$. On obtient donc bien $|A \times B|$ caractères distincts, et on laisse le soin au lecteur de vérifier que la matrice $\big((\phi \otimes \psi)(a, b)\big)$ de taille $|A \times B|$ est bien égale à la matrice voulue.

Cette proposition permet donc de construire la table des caractères de tout GAF dont on connaît les facteurs invariants.

0.1.4 Décomposition d'une fonction sur A en somme de caractères

Soit A un GAF. On rappelle que l'algèbre $\mathbb{C}[A]$ des fonctions de A dans $\mathbb{C}$ possède deux bases : celle, naturelle, des $(\delta_a)_{a \in A}$, et celle des caractères $(\chi)_{\chi \in \widehat{A}}$. On a également doté $\mathbb{C}[A]$ d'un produit hermitien

$$\langle f, g \rangle = \langle f, g \rangle_A = \frac{1}{|A|} \sum_{a \in A} \overline{f(a)} g(a).$$

On sait que la base des caractères est une base unitaire. De plus, il est immédiat de voir que la base légèrement modifiée $\sqrt{|A|}\delta_a)_{a \in A}$ est également unitaire.

La décomposition d'une fonction f de $\mathbb{C}[A]$ dans la première base est claire :

$$f = \sum_{a \in A} f(a)\delta_a$$

La base des caractères fera tout de même l'objet d'un intérêt particulier. En effet, on peut voir une fonction $k \mapsto \omega^k$ sur le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ comme une version discrète de la fonction $t \mapsto e^{it}$ sur le groupe $\mathbb{R}$ des réels. La décomposition d'une fonction f de $\mathbb{C}[A]$ dans la base des caractères peut être donc vue comme une *décomposition de Fourier discrète*.

Comme la base des caractères est unitaire, on trouve immédiatement la décomposition de tout f de $\mathbb{C}[A]$:

$$f = \sum_{\chi \in \widehat{A}} \langle \chi, f \rangle \chi.$$

On pose donc, naturellement

$$c_f(\chi) = \langle \chi, f \rangle_A = \frac{1}{|A|} \sum_{a \in A} \chi(a)^{-1} f(a),$$

de sorte à avoir

$$f = \sum_{\chi \in \widehat{A}} c_f(\chi) \chi. \tag{1}$$

Les coefficients $c_f(\chi)$ peuvent être vus comme des coefficients de Fourier, et si l'on pense à la forme intégrale des coefficients de Fourier en analyse harmonique, la somme ci-dessus, donnant $c_f(\chi)$, peut être vue comme une *méthode des rectangles* pour un calcul d'intégrale.

0.1.5 Transformée de Fourier discrète

On rappelle le résultat utile et bien connu, voir [Tome 1 ed.2, Chap V, annexe A-1], qu'une forme bilinéaire non dégénérée sur un espace E de dimension finie fournit un isomorphisme entre E et son dual E^* ; plus précisément, à x dans E, on associe $\hat{x}$ dans E^* tel que $\hat{x}(y) = \langle x, y \rangle$. C'est à peu de choses près [6] ce qu'il va se passer ici dans le contexte des formes hermitiennes et des GAF. L'isomorphisme s'appelle ici *transformée de Fourier discrète*.

Définition 0.14. Soit $\mathcal{F}$ l'application de $\mathbb{C}[A]$ dans $\mathbb{C}[\widehat{A}]$ qui envoie la fonction f sur la fonction $\widehat{f} = \mathcal{F}(f)$ telle que

$$\widehat{f}(\chi) = \sum_{a \in A} f(a) \chi(a).$$

L'application $\mathcal{F}$ est appelée transformée de Fourier discrète.

6. En fait, on va avoir une variante : $\hat{f}(\chi) = |A| \, \langle \overline{\chi}, f \rangle_A$.

Voici un résumé des propriétés de la transformée de Fourier discrète, dont on connaît déjà les analogues en analyse harmonique :

Théorème 0.15. La transformée de Fourier $\mathcal{F}$ possède les propriétés suivantes :

1. elle établit un isomorphisme entre $\mathbb{C}[A]$ et $\mathbb{C}[\widehat{A}]$,
2. c'est (presque) une isométrie :
$$\langle f, g\rangle_A = \frac{1}{|A|}\langle \widehat{f}, \widehat{g}\rangle_{\widehat{A}},$$
3. sa réciproque est donnée par
$$f = \frac{1}{|A|}\sum_{\chi\in\widehat{A}} \widehat{f}(\overline{\chi})\chi,$$
4. si on munit $\mathbb{C}[A]$ d'une structure de $\mathbb{C}$-algèbre en ajoutant le *produit de convolution*, défini par
$$(f * g)(a) = \sum_{x+y=a} f(x)g(y),$$
alors $\widehat{f * g} = \widehat{f} \times \widehat{g}$, c'est-à-dire que $\mathcal{F}$ fournit un isomorphisme d'algèbres entre $(\mathbb{C}[A], +, \cdot, *)$ et $(\mathbb{C}[A], +, \cdot, \times)$.

Démonstration. Il est clair que $\mathcal{F}$ est une application $\mathbb{C}$-linéaire. Calculons en premier lieu $\langle \widehat{f}, \widehat{g}\rangle_{\widehat{A}}$:

$$\begin{aligned}\langle \widehat{f}, \widehat{g}\rangle_{\widehat{A}} &= \frac{1}{\left|\widehat{A}\right|}\sum_{\chi\in\widehat{A}} \overline{\widehat{f}(\chi)}\widehat{g}(\chi) = \frac{1}{|A|}\sum_{a,b\in A,\,\chi\in\widehat{A}} \overline{f(a)\chi(a)}g(b)\chi(b)\\ &= \frac{1}{|A|}\sum_{a,b\in A,\,\chi\in\widehat{A}} \overline{f(a)}g(b)\chi(b-a) = \frac{1}{|A|}\sum_{a,b\in A} \overline{f(a)}g(b)\sum_{\chi\in\widehat{A}}\chi(b-a)\end{aligned}$$

Or, si on identifie A à son bidual $\widehat{\widehat{A}}$, on peut identifier naturellement a et b à leurs caractères respectifs $\widehat{\widehat{a}}$ et $\widehat{\widehat{b}}$ sur $\widehat{A}$, ce qui donne, par orthonormalité des caractères :

$$\sum_{\chi\in\widehat{A}}\chi(b-a) = \sum_{\chi\in\widehat{A}}\overline{\chi(a)}\chi(b) = \sum_{\chi\in\widehat{A}}\overline{\widehat{\widehat{a}}(\chi)}\widehat{\widehat{b}}(\chi) = |A|\,\delta_{a,b}.$$

On obtient donc au final :

$$\langle \widehat{f}, \widehat{g} \rangle_{\widehat{A}} = \sum_{a \in A} \overline{f(a)} g(a) = |A| \, \langle f, g \rangle_A .$$

Donc, $\mathcal{F}$ est le produit d'une isométrie par une homothétie (non nulle), ce qui implique que $\mathcal{F}$ est injective. C'est donc bien un isomorphisme, par égalité des dimensions.

L'égalité (iii) est quasiment tautologique puisque, par construction, voir 1, $f = \sum_{\chi \in \widehat{A}} c_\chi(f)\chi$, avec $c_\chi(f) = \frac{1}{|A|}\widehat{f}(\overline{\chi})$.

Il reste à montrer (iv). Tout d'abord, il n'est pas difficile de voir que $(\mathbb{C}[A], +, *)$ est bien un anneau unitaire. En effet, la convolution $*$ est visiblement distributive sur l'addition, son élément neutre est δ_0, et l'associativité vient de

$$\big((f * g) * h\big)(a) = \sum_{x+y+z=a} f(x)g(y)h(z) = \big(f * (g * h)\big)(a).$$

Il ne reste donc plus qu'à développer $\widehat{f} \times \widehat{g}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi)$:

$$\begin{aligned}
\widehat{f}(\chi)\widehat{g}(\chi) &= \big(\sum_{a \in A} f(a)\chi(a)\big)\big(\sum_{b \in A} g(b)\chi(b)\big) = \sum_{a,b \in A} f(a)g(b)\chi(a+b) \\
&= \sum_{x \in A} \sum_{a+b=x} f(a)g(b)\chi(x) = \sum_{x \in A} f * g(x)\chi(x) \\
&= \widehat{f * g}(\chi).
\end{aligned}$$

L'égalité (ii) est l'analogue discret de l'égalité de Parseval de l'analyse harmonique. La propriété (iii) n'est finalement rien d'autre que le reflet de la propriété du bidual, proposition 0.1.1. On peut se demander pourquoi on n'a pas défini la transformée de Fourier comme une vraie isométrie. La réponse est simple : pour qu'elle le soit, il aurait fallu qu'on mette des $\sqrt{|A|}$ dans les formules, et on a préféré garder des formules avec des entiers pour des raisons purement arithmétiques que l'on peut imaginer.

Remarque. On pourra trouver, dans l'exercice 0.17, une incroyable application de ce théorème à un algorithme de calcul pour la multiplication de grands nombres entiers. Pour résumer, on peut se demander si, en terme de complexité de calculs, la transformée de Fourier discrète est suffisamment économique pour être utilisée lorsque l'on veut calculer un produit de convolution, par exemple, quand on veut multiplier des entiers écrits sous forme décimale. La réponse vient de Cooley et Tukey en 1965 [7], c'est oui, et pas qu'un peu !

7. En fait, Gauss avait déjà utilisé leur algorithme en 1805. Et oui, rien de nouveau en ce monde depuis Carl Friedrich !

0.1.6 Transformée de Fourier discrète-Version matricielle

Il serait dommage de passer à côté de la version matricielle de la transformée de Fourier car celle-ci éclaire, d'une part, sa connexion avec la théorie des représentations, et d'autre part, le lien (originel) avec la décomposition d'une fonction en somme de caractères.

Soit donc A un groupe abélien. On munit $\mathbb{C}[A]$ de la base $(\delta_a)_{a\in A}$ des fonctions caractéristiques d'éléments de A, et, de même, on munit $\mathbb{C}[\widehat{A}]$ de la base $(\delta_\chi)_{\chi\in\widehat{A}}$ des fonctions caractéristiques d'éléments de $\widehat{A}$. Comme

$$\hat{\delta}_a(\chi) = \sum_b \chi(b)\delta_a(b) = \chi(a),$$

l'isomorphisme $\mathcal{F}$ entre les espaces $\mathbb{C}[A]$ et $\mathbb{C}[\widehat{A}]$ s'écrit matriciellement dans ces deux bases :

$$V := \mathrm{mat}(\mathcal{F}) = (\chi(a))_{\chi,a}$$

On reconnaît la matrice de la table de caractères de A. Cela signifie, par la proposition **??**, que, si l'on connaît la décomposition de A en sous-groupes cycliques, théorème **??**, la matrice de $\mathcal{F}$ se calcule facilement comme produit tensoriel de matrices de Vandermonde de la forme $(\omega_m^{ij})_{0\leq i,j\leq m}$, où ω_m est une racine primitive m-ième de l'unité. On obtient également les égalités

$$VV^* = V^*V = n\mathrm{I}_n, \text{ où } n = |A|\,.$$

D'autre part, comme $\chi = \sum_a \chi(a)\delta_a$, la matrice V est égale à la transposée de la matrice de passage de la base (δ_a) vers la base (χ) de $\mathbb{C}[A]$. Or, décomposer une fonction f en somme de caractères revient à passer du vecteur de coordonnées $v_f = (f(a))_a$ de f dans la base (δ_a) au vecteur de coordonnées $c_f := (c_\chi(f))_\chi$ dans la base (χ). On a donc, par les formules de changement de base (les vecteurs sont en colonnes) :

$$c_f = V^{-1}\cdot v_f = \frac{1}{n}V^*\cdot v_f$$

Exercice 0.16. [Transformée de Walsh]

On considère le groupe abélien $G_n = (\mathbb{Z}/2\mathbb{Z})^n$. A tout élément $g := (\bar{g}_1,\ldots,\bar{g}_n)$ de G_n, on associe le nombre $b_g \in \mathbb{N}$ dont l'écriture binaire est $\overline{g_1\ldots g_n}$, avec $g_i = 0, 1$.

1. Montrer que $g \mapsto b_g$ définit une bijection entre G_n et $\{0, 1, \ldots, 2^n - 1\}$. On notera $b \mapsto g_b$ la bijection inverse. De même on construit, à l'aide de la proposition 0.1.1, la bijection naturelle [8], voir

$$\widehat{G}_n \simeq \widehat{\mathbb{Z}/2\mathbb{Z}} \times \ldots \times \widehat{\mathbb{Z}/2\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z} \simeq \{0, 1, \ldots, 2^n - 1\}.$$

On notera χ_a le caractère associé au nombre a.

2. On note $W_n = (\chi_a(g_b))_{a,b}$. Montrer

$$W_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; W_n = \begin{pmatrix} W_{n-1} & W_{n-1} \\ W_{n-1} & -W_{n-1} \end{pmatrix}$$

3. On associe à tout χ de $\widehat{G_n}$ sa "fréquence" $\omega_n(\chi)$, égale au nombre de changements de signe le long de la ligne correspondant à χ dans W_n. Dit autrement :

$$\omega_n(\chi) := \#\{b, \, \chi(g_b)\chi(g_{b+1}) < 0, \, 0 \leq b \leq 2^n - 2\}.$$

Calculer les fréquences pour les caractères dans les cas $n = 1$ et 2. Puis, montrer les formules de récurrence suivantes :

$$\omega_n(\chi_{\overline{0g_2\cdots g_n}}) = \begin{cases} 2\omega_{n-1}(\chi_{\overline{g_2\cdots g_n}}) & \text{si } g_2 + \cdots + g_n \text{ est pair,} \\ 2\omega_{n-1}(\chi_{\overline{g_2\cdots g_n}}) + 1 & \text{si } g_2 + \cdots + g_n \text{ est impair} \end{cases}$$

$$\omega_n(\chi_{\overline{1g_2\cdots g_n}}) = \begin{cases} 2\omega_{n-1}(\chi_{\overline{g_2\cdots g_n}}) + 1 & \text{si } g_2 + \cdots + g_n \text{ est pair,} \\ 2\omega_{n-1}(\chi_{\overline{g_2\cdots g_n}}) & \text{si } g_2 + \cdots + g_n \text{ est impair.} \end{cases}$$

En déduire que ω_n établit une bijection de $\widehat{G_n}$ sur $\{0, 1, \ldots, 2^n - 1\}$.

Soluce. 1. C'est le théorème classique de décomposition d'un nombre en base b, ici $b = 2$. Cela provient essentiellement de la série géométrique, et du fait que $1 + 2 + 2^2 + \cdots + 2^{n-1} < 2^n$.

2. Pour $n = 1$,

$$W_1 = \begin{pmatrix} \chi_0(0) & \chi_0(1) \\ \chi_1(0) & \chi_1(1) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Pour $n = 2$, l'ordre total $0 < 1 < 2 < 3$ devient $(0,0) < (0,1) < (1,0) < (1,1)$. Comme, par construction, $\chi_{\overline{ij}}(\overline{kl}) = \chi_i(k)\chi_j(l)$, il vient :

8. On n'a qu'une seule racine primitive deuxième de l'unité ! Donc, $\widehat{Z/2\mathbb{Z}}$ et $\mathbb{Z}/2\mathbb{Z}$ sont naturellement isomorphes.

$$W_2 = \begin{pmatrix} \chi_0(0)\chi_0(0) & \chi_0(0)\chi_0(1) & \chi_0(1)\chi_0(0) & \chi_0(1)\chi_0(1) \\ \chi_0(0)\chi_1(0) & \chi_0(0)\chi_1(1) & \chi_0(1)\chi_1(0) & \chi_0(1)\chi_1(1) \\ \chi_1(0)\chi_0(0) & \chi_1(0)\chi_0(1) & \chi_1(1)\chi_0(0) & \chi_1(1)\chi_0(1) \\ \chi_1(0)\chi_1(0) & \chi_1(0)\chi_1(1) & \chi_1(1)\chi_1(0) & \chi_1(1)\chi_1(1) \end{pmatrix} = \begin{pmatrix} W_1 & W_1 \\ W_1 & -W_1 \end{pmatrix}$$

Pour n fixé, l'ordre total $0 < 1 < \cdots < 2^n - 1$ devient $(0, \overline{g}) < (1, \overline{g})$, où les $\overline{g} \in \mathbb{Z}/2^{n-1}\mathbb{Z}$ ont été ordonnés par récurrence. Comme, par construction, $\chi_{\overline{ig}}(\overline{kh}) = \chi_i(k)\chi_{\overline{g}}(\overline{h})$, avec $i, k = 0, 1$, on a la formule annoncée :

$$W_n = \begin{pmatrix} W_{n-1} & W_{n-1} \\ W_{n-1} & -W_{n-1} \end{pmatrix}$$

3. Pour $n = 1$, on constate, en comptant le nombre de changements de signes sur les lignes de W_1, W_2 :

$$\omega_1(0) = 0,\ \omega_1(1) = 1;\ \omega_2(0) = 0,\ \omega_2(1) = 3, \omega_2(2) = 1,\ \omega_2(3) = 2,$$

Pour le cas général, on remarque que le nombre de changements de signe sur une ligne de W_{n-1} est égal au nombre de changements de signe sur la même ligne de $-W_{n-1}$. Donc, pour chaque ligne $\overline{ig_2 \cdots g_n}$ de W_n, $i = 0, 1$, le nombre de changements de signe est égal à deux fois le nombre de changements de signe de ligne $\overline{g_2 \cdots g_n}$ de W_{n-1} plus 1 ou 0 selon s'il y a un changement de signe ou non entre les deux blocs matriciels.
Le passage entre les deux blocs de W_n se fait entre la colonne $\overline{011\cdots1}$ et la colonne $\overline{100\cdots0}$. Le changement de signe entre deux blocs dépend donc du signe de :

$$\begin{aligned} \chi_{\overline{ig_2\cdots g_n}}(\overline{011\cdots1})\chi_{\overline{ig_2\cdots g_n}}(\overline{100\cdots0}) &= \chi_i(0)\chi_{\overline{g_2\cdots g_n}}(\overline{11\cdots1})\chi_i(1)\chi_{\overline{g_2\cdots g_n}}(\overline{00\cdots0}) \\ &= \chi_{g_2}(1)\cdots\chi_{g_n}(1)\chi_i(1). \end{aligned}$$

Ceci fournit directement le résultat demandé.
Montrons maintenant que ω_n établit une bijection entre les ensembles $\widehat{G_n}$ et $\{0, 1, \ldots, 2^n - 1\}$. Comme ils ont même cardinal, il suffit de montrer que ω_n est surjectif. Montrons-le par récurrence. On l'a vu pour $n = 1$ et 2. Supposons que ce soit vrai à l'ordre $n-1$ et montrons-le à l'ordre n. Soit k_n un entier de $[0, 2^n - 1]$. La division euclidienne de k_n par 2 donne $k_n = 2k_{n-1} + r$, où k_{n-1} est un entier dans $[0, 2^{n-1} - 1]$, et $r = 0$ ou 1. Par récurrence, k_{n-1} a un antécédent par ω_{n-1}, soit g_{n-1} cet antécédent. Supposons que $\mathrm{ht}(g_{n-1})$ soit paire, et $r = 0$, alors, $\omega(\overline{0g_{n-1}})$ est un antécédent de k_n pour ω_n. Si on suppose maintenant que $\mathrm{ht}(g_{n-1})$ soit impaire, et $r = 0$, alors, $\omega(\overline{1g_{n-1}})$ est un antécédent de k_n pour ω_n. De même, on trouve un antécédent à k_n si $r = 1$ en faisant deux cas.

Remarque. On n'a pas vraiment parlé de transformées dans cet exercice. Disons qu'à normalisation près la transformée de Fourier discrète dans le cas du groupe G_n est la transformée de Walsh-Hadamard qui a pour matrice la matrice W_n, à normalisation près. On trouvera deux avantages non négligeables : d'une part, la matrice W_n se calcule de façon quasi-instantanée par récurrence, et d'autre part, on a un ordre total sur les caractères, qui s'apparentent ici à des fréquences. On peut donc compresser un signal de la façon suivante : on part d'une fonction discrétisée que l'on considère comme une fonction de $\mathbb{Z}/2^n\mathbb{Z}$ dans $\mathbb{C}$, puis, on calcule ses coefficients de Fourier dans la base des caractères, à l'aide de la matrice de W_n, et enfin, on compresse le signal en annulant les coefficients des caractères à partir d'un certain ordre. On peut voir de jolis exemples d'applications à la compression d'image dans [Peyré].

Exercice 0.17 (La transformée de Fourier rapide (FFT))**.**

Soit f dans $\mathbb{C}[G]$, on suppose pour simplifier $G = G_a = \mathbb{Z}/n\mathbb{Z}$, avec $n = 2^a$. On veut un algorithme efficace pour calculer la transformée de Fourier discrète. Soit ω une racine n-ième de l'unité et χ_ω le caractère associé à ω.

$$\hat{f}(\chi_\omega) = \sum_{k=0}^{n-1} f(k)\omega^k.$$

1. Quelle est la complexité du calcul naïf [9] ?
2. On considère la fonction f_{pair}, resp. f_{imp}, dans $\mathbb{C}[G_{a-1}]$, telle que $f_{\text{pair}}(p) = f(2p)$, resp. $f_{\text{imp}}(p) = f(2p+1)$. Montrer
$$\hat{f}(\chi_\omega) = \widehat{f_{\text{pair}}}(\omega^2) + \omega\widehat{f_{\text{imp}}}(\omega^2).$$
On notera au passage que $\chi_{\omega^2} \in \widehat{G_{a-1}}$, puisque ω^2 est une racine 2^{a-1}-ième de l'unité.
3. Montrer que l'on peut alors calculer $\hat{f}(\chi_\omega)$ par récurrence sur a et que la complexité d_a du calcul vérifie la récurrence $d_a = 2d_{a-1} + 2^{a+1}$.
4. Montrer l'égalité $d_a = a2^{a+1}$, puis, que ce nouvel algorithme est de complexité $n\log(n)$.
5. Est-il rentable de calculer la transformée de Fourier de deux fonctions f et g de $\mathbb{C}[G]$ dans le but de calculer $f * g$?

Soluce. 1. Pour chaque χ dans $\widehat{G}$, on a n multiplications et $n-1$ additions. Comme $\left|\widehat{G}\right| = n$, cela nous fait en tout $(2n-1)n$ opérations.

9. Curieux, plus un calcul est naïf, plus il est complexe...

2. On décompose la somme en une partie où k est pair, et une autre où k est impair :

$$\widehat{f}(\chi_\omega) = \sum_{p=0}^{\frac{n}{2}-1} f(2p)\omega^{2p} + \omega \sum_{k=0}^{n/2-1} f(2p+1)\omega^{2p},$$

ce qui fournit directement le résultat voulu.

3. On calcule $\hat{f}(\chi)$, pour $f \in \mathbb{C}[G_a]$, $\chi \in \widehat{G_a}$, par récurrence sur a.
Si $a = 0$. $\hat{f}(\chi_{\text{triv}}) = f(0)$. Puis, par récurrence par la formule ci-dessus : pour chaque χ dans $\widehat{G_a}$, on doit calculer 2 transformées de Fourier à l'ordre $a-1$, une multiplication (par ω), et une addition. On a donc bien $d_a = 2d_{a-1} + 2n = 2d_{a-1} + 2^{a+1}$.

4. L'égalité $d_a = a2^{a+1}$ vérifie bien $d_0 = 0$ (0 calcul pour $a = 0$), et

$$2d_{a-1} + 2^{a+1} = 2(a-1)2^a + 2^{a+1} = a2^{a+1} = d_a,$$

comme désiré. La complexité du calcul est donc

$$d_a = a2^{a+1} = \frac{2n\log(n)}{\log(2)}.$$

En bref, on est passé d'un algorithme naïf en n^2 en un algorithme (rusé !) en $n\log(n)$.

5. Le calcul de $(f * g)(k) = \sum_{l=0}^{n-1} f(l)g(k-l)$ nécessite $2n-1$ opérations pour chaque k, c'est-à-dire $(2n-1)n$ opérations en tout. Puisque $\widehat{f * g} = \hat{f}\hat{g}$, calculer la transformée de Fourier permet de se ramener à une seule opération pour chaque élément de $\widehat{G}$, soit n opérations en tout. Mais, il faut également calculer le prix du voyage aller-retour ! On prend deux transformées de Fourier (de f et de g, donc, en $n\log(n)$), et une transformée de Fourier inverse (qui est encore une transformée de Fourier). Comme n est négligeable devant $n\log(n)$, on trouve un algorithme en $n\log(n)$. La réponse est clairement oui !

Remarque. On note que la multiplication de deux polynômes $P = \sum_{i=0}^{n-1} a_i X^i$ et $Q = \sum_{j=0}^{n-1} b_j X^j$ se fait à l'aide d'une convolution : $PQ = \sum_k c_k X^k$, avec $c_k = \sum_{i+j=k} a_i b_j$. Effectivement, on peut interpréter P comme une fonction $i \mapsto a_i$, Q comme une fonction $j \mapsto b_j$, et donc, la fonction $k \mapsto c_k$ peut se voir comme une convolution des deux premières. La transformée de Fourier rapide devient un outil essentiel pour la multiplication polynomiale, à partir d'un certain degré. En particulier (prendre $X = 10$), c'est aussi vrai pour la multiplication des entiers en écriture décimale.

Remarque. Quel tour de magie tout de même ! Mais où est passé le lapin ? Comment a-t-on pu subtiliser tant de complexité pour passer de n^2 à $n\log(n)$? [10] Toute l'idée consiste à remarquer que, lorsque l'on calcule $\hat{f}(\chi)$ pour tout χ, on effectue plusieurs fois les mêmes opérations. Par exemple, pour $a = 2$ (et donc, $n = 4$), si on doit effectuer les quatre calculs $a_0 + a_1 + a_2 + a_3$, $a_0 + ia_1 - a_2 - ia_3$, $a_0 - a_1 + a_2 - a_3$, $a_0 - ia_1 - a_2 + ia_3$, il suffit de calculer dans un premier temps $\alpha = a_0 + a_2$, $\beta = a_1 + a_3$, $\gamma = a_0 - a_2$ et $\delta = a_1 - a_3$, puis $\alpha + \beta$, $\gamma + i\delta$, $\alpha - \beta$, $\gamma - i\delta$. On est déjà passés de 16 à 10 opérations !

10. Imaginons un peu que l'on modélise (pixellise) un cube d'un mètre de côté en petits cubes d'un centimètre. Il faudra donc $n = 10^6$ cubes pour faire de l'analyse de Fourier discrète d'une fonction sur ce cube : on passe de $n^2 = 10^{12}$ opérations à $n\log(n) \simeq 6.000.000$, c'est-à-dire environ 1000 secondes contre 6 millièmes de secondes. Ça fait quand même beaucoup de lapins !