Abstract

Ce sujet traite de la théorie des représentations pour des groupes abéliens finis. Une application proposée d'une telle théorie est la définition d'une transformée de Fourier sur des groupes généralisant de nombreux résultats que vous avez pu observer en physique. C'est l'occasion d'introduire les bases de l'analyse harmonique.

Dans tout le sujet, $(G,+)$ désignera un groupe abélien de cardinal n. On définit également l'ensemble des morphismes de groupe $\widehat{G}$ de $(G,+)$ vers $(\mathbb{C}^{\times},\times)$ que l'on appelera *groupe dual*.
L'étude portera aussi sur le $\mathbb{C}$-espace vectoriel $E=\mathbb{C}^G$ que l'on appelera espace dual. Sur cet espace, nous définissons deux applications. La première, notée $\langle .,.\rangle : E\times E\to\mathbb{C}$, sera appelée produit hermitien et sera définie par

$$\langle f,g\rangle = \frac{1}{n}\sum_{x\in G} f(x)\overline{g(x)}.$$

La seconde, notée $\cdot\star\cdot : E\times E\to E$, sera appelée produit de convolution et sera définie par

$$\forall x\in G, (f\star g)(x) = \frac{1}{n}\sum_{y\in G} f(y)g(x-y).$$

1 Préliminaires

L'objectif de cette partie est de démontrer quelques propriétés essentielles. Un produit hermitien est une généralisation du produit scalaire appliqué à des espaces complexes. Soit F un espace vectoriel complexe, une application $\phi : F\times F\to\mathbb{C}$ est appelée produit hermitien si elle vérifie les propriétés suivantes pour tout $f,g,h\in F$ et pour tout $\lambda\in\mathbb{C}$:

- $\phi(f,g)=\overline{\langle g,f\rangle}$,
- $\phi(f+\lambda g,h)=\phi(f,h)+\lambda\phi(g,h)$,
- $\phi(f,f)\in\mathbb{R}_+$,
- $\phi(f,f)=0$ si et seulement si $f=0$.

On montre quelques résultats sur ces produits.

1. Soit ϕ un produit hermitien sur F, montrer que pour tout $f,g,h\in F$ et pour tout $\lambda\in\mathbb{C}$,

$$\phi(f,g+\lambda h)=\phi(f,g)+\overline{\lambda}\phi(f,h)$$

2. On dit qu'une famille $f_1,...,f_k$ est orthonormale si pour tout $i,j\in\{1,...,k\}$, $\langle f_i,f_j\rangle = \delta_{i,j}$. Montrer qu'une famille orthonormale est libre.

3. Montrer que $\langle \cdot, \cdot \rangle$ est un produit hermitien sur E.

   On admet que φ sur $\mathbb{C}^k \times \mathbb{C}^k$ défini par

$$\forall x, y \in \mathbb{C}^k, \varphi x y = \sum_{i=1}^{k} x_i \overline{y_i}$$

   est un produit hermitien.

4. Une matrice $U \in \mathcal{M}_k(\mathbb{C})$ est dite unitaire si les colonnes de U forment une base orthonormale de $\mathbb{C}^k$. Montrer qu'une matrice $U \in \mathcal{M}_k(\mathbb{C})$ est unitaire si et seulement si elle vérifie $\overline{U^T} U = I_k$.

5. Montrer que les vecteurs propres normalisés d'une matrice unitaire forment une famille orthonormale de $\mathbb{C}^k$.

Correction de la première partie

1. On applique les différents axiomes

$$\begin{aligned}
\phi(f, g + \lambda h) &= \overline{\phi(g + \lambda h, f)} \\
&= \overline{\phi(g, f) + \lambda \phi(h, f)} \\
&= \overline{\phi(g, f)} + \overline{\lambda} \overline{\phi(h, f)} \\
&= \phi(f, g) + \overline{\lambda} \phi(f, h).
\end{aligned}$$

   C'est ce qu'on appelle aussi la sesquilinéarité droite.

2. On suppose que $\sum_{i=1}^k \lambda_i f_i = 0$ où $\lambda_i \in \mathbb{C}$. On a

$$\begin{aligned}
0 &= \langle \sum_{i=1}^{k} \lambda_i f_i, f_j \rangle \\
&= \sum_{i=1}^{k} \lambda_i \langle f_i, f_j \rangle \\
&= \lambda_j.
\end{aligned}$$

3. On vérifie les propriétés.

4. Il suffit de faire les calculs.

$$\begin{aligned}
(\overline{U^T} U)_{i,j} &= \sum_{l=1}^{k} \overline{U_{l,i}} U_{l,j} \\
&= \langle U_j, U_i \rangle \\
&= \delta_{i,j}.
\end{aligned}$$

   On a donc bien $\overline{U^T} U = I_k$. La réciproque est immédiate.

5. Soit λ une valeur propre de U et v un vecteur propre normalisé associé. $\langle Ux, Uy\rangle = \overline{(Uy)}^T Ux = \overline{y}^T \overline{U}^T Ux = \langle x, y\rangle$. En particulier, $\langle Uv, Uv\rangle = \langle v, v\rangle = |\lambda|^2 \langle v, v\rangle$. Donc $|\lambda|^2 = 1$.

6. Soit λ, μ deux valeurs propres distinctes de U associées à v, w. On a
$$\begin{aligned}\langle v, w\rangle &= \langle Uv, Uw\rangle \\ &= \lambda\overline{\mu}\langle v, w\rangle.\end{aligned}$$
Si $\langle v, w\rangle \neq 0$, alors $\lambda = \overline{\mu}^{-1}$. Or, $|\lambda| = 1$, donc $\mu = \overline{\overline{\mu}} = \lambda$.

2 Convolutions de fonctions

1. Montrer que $\star$ est une loi commutative, associative et bilinéaire sur E.
2.

3 Caractères et groupe dual

L'objectif de cette partie est de déterminer une base orthonormale de E pour le produit hermitien. Cela se fera via l'étude de l'endormorphisme de translation $\tau_y : E \to E$ avec $y \in G$ défini par
$$\forall x \in G, \tau_y(f)(x) = f(x - y).$$

1. Montrer que $y \mapsto \tau_y$ est un morphisme de groupe de G dans $\mathcal{GL}(E)$.
2. Montrer que T_y est unitaire pour tout $y \in G$.
3. Montrer que si $\chi \in \widehat{G}$, i.e. χ est un morphisme de groupe de G dans $\mathbb{C}^\times$, alors χ est un vecteur propre de τ_y.
4. Montrer que τ_y est diagonalisable.
5. En déduire qu'il existe $\chi_1, \dots, \chi_n \in \widehat{G}$ distincts tels que
$$\forall y \in G, \mathrm{mat}_{\chi_1,\dots,\chi_n}(T_y) = \begin{pmatrix} \chi_1(y) & 0 & \dots & 0 \\ 0 & \chi_2(y) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \chi_n(y) \end{pmatrix}.$$
6. Montrer que $\widehat{G} = \{\chi_1, \dots, \chi_n\}$ et que $(\widehat{G}, \times)$ forme un groupe abélien. En déduire que $(\widehat{G}, \times)$ est isomorphe à $(G, +)$.
7. Montrer que $\chi_1, \dots, \chi_n$ forment une base orthonormale de E.
8. Montrer que pour tout
$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} n & \text{si } x = 0 \\ 0 & \text{sinon.} \end{cases}$$

3.1 Caractères de $\mathbb{Z}/n\mathbb{Z}$

1. Montrer que l'endormorphisme τ_1 peut-être représenté par la matrice

$$T = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

2. Montrer que les valeurs propres de T sont les racines n-ièmes de l'unité. En déduire l'ensemble des caractères de $\mathbb{Z}/n\mathbb{Z}$.

3. En déduire qu'on peut indexer les caractères χ_i de $\mathbb{Z}/n\mathbb{Z}$ par des $l \in \mathbb{Z}/n\mathbb{Z}$ de sorte que

$$\forall k \in \mathbb{Z}/n\mathbb{Z}, \chi_l \chi_{-l'} = \chi_{l-l'}.$$

En conclure que $\widehat{\mathbb{Z}/n\mathbb{Z}}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

3.2 Caractère d'un produit de groupes

Dans cette partie, on considère un groupe $G = G_1 \times \dots G_k$ tel que $\mathrm{card}(G) = n$.

(a) Soient $\chi^{(1)}, \dots, \chi^{(k)}$ des caractères de $G_1, \dots, G_k$. Montrer que $\chi^{(1)} \times \dots \times \chi^{(k)}$ est un caractère de G.

(b) Montrer alors que

$$\widehat{G} = \{\chi^{(1)} \times \dots \times \chi^{(k)}, \ \ \chi^{(1)} \in \widehat{G_1}, \dots, \chi^{(k)} \in \widehat{G_k}\}.$$

(c) En déduire que $\widehat{G}$ est isomorphe à G.

(d) On considère le groupe $G = (\mathbb{Z}/2\mathbb{Z})^n$, montrer que les caractères de G sont de la forme

$$\chi_x(y) = (-1)^{\sum_{i=1}^n x_i y_i}.$$

On admettra désormais que le groupe dual $\widehat{G}$ est toujours isomorphe à G dans le cas des groupes abéliens finis. On notera χ_x le caractère associé à $x \in G$.

Correction de la troisième partie

1. On vérifie les propriétés.

2. On peut le vérifier de plusieurs manières. La première est de vérifier que l'image de d'une base orthonormale est encore une base orthonormale. On prend, par exemple, la base des $\{\delta_x, x \in G\}$.

$$\langle \tau_y \delta_x, \tau_y \delta_z \rangle = \langle \delta_{x-y}, \delta_{z-y} \rangle = \delta_{x-y,z-y} = \delta_{x,z}.$$

Ce qui permet de conclure que τ_y sera unitaire. Sinon, on peut aussi vérifier que l'inverse de T_y est $\overline{T_y^T}$. On a $T_y^{-1} = T_{-y}$. On ensuite vérifier pour chaque δ_x que $\overline{T_y^T} = T_{-y}$.

3. On considère un morphisme χ. On a par définition

$$\forall x \in G,\ \tau_y(\chi)(x) = \chi(x+y) = \chi(y)\chi(x).$$

Donc χ est un vecteur propre de τ_y associé à la valeur propre $\chi(y)$.

4. On utilise le fait que $\tau_y^n = \tau_{ny} = \tau_0 = \mathrm{id}$. On en déduit que $X^n - 1$ est annulateur de τ_y. Donc τ_y est diagonalisable car il est annulé par un polynôme scindé à racines simples.

5. On sait qu'il existe alors une base commune de diagonalisation pour tous les y de $\mathbb{C}^G$ formée de vecteurs propres de τ_y, on les note $\chi_1, \ldots, \chi_n$. On vérifie que $\chi_i \in \widehat{G}$ simplement.

6. On a vu qu'il y a au moins autant de valeur propres distinctes que de morphismes de groupe. Le résultat précédent montre que l'ensemble des valeurs propres est inclus dans $\widehat{G}$. On en déduit que $\widehat{G} = \{\chi_1, \ldots, \chi_n\}$. On montre simplement la structure de groupe de $\widehat{G}$.

7. Les χ_i forment une base car ce sont des vecteurs propres. Et d'après la partie préliminaire, ces vecteurs sont orthogonaux. Il reste à montrer que ces vecteurs sont de norme 1.

$$\begin{aligned}\langle \chi_i, \chi_i \rangle &= \frac{1}{n} \sum_{x \in G} \chi_i(x)\overline{\chi_i(x)} \\ &= \frac{1}{n} \sum_{x \in G} |\chi(x)|^2 \\ &= 1.\end{aligned}$$

car les $\chi_i(x)$ sont les valeurs propres de τ_x qui est unitaire (donc les valeurs propres sont de module 1).

8. Notons $S(x) = \sum_{\chi \in \widehat{G}} \chi(x)$. Si $x = 0$, on a facilement $S(0) = n$. Sinon, on peut utiliser le fait que $\chi \mapsto \chi'\chi$ soit une bijection de $\widehat{G}$ sur lui-même. On a

$$\begin{aligned}S(x) &= \sum_{\chi \in \widehat{G}} \chi(x) \\ &= \sum_{\chi \in \widehat{G}} \chi'(x)\chi(x) \\ &= \chi'(x) \sum_{\chi \in \widehat{G}} \chi(x) \\ &= \chi'(x) S(x).\end{aligned}$$

Or, pour tout $x \neq 0$, il existe un χ' tel $\chi'(x) \neq 1$. On en conclut que $S(x) = 0$.

Correction des questions sur $\mathbb{Z}/n\mathbb{Z}$

1. Si on considère à la base $\{\delta_i\}$, on a $\tau_1(\delta_i) = \delta_{i-1}$ pour i différent de 0, et pour $i = 0$ on a $\tau_1(\delta_0) = \delta_{n-1}$. On a donc

$$\mathrm{mat}_{\delta_0,\ldots,\delta_{n-1}}(\tau_1) = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \end{pmatrix}.$$

2. Un calcul de valeur propre...
3. Il suffit d'associer à chaque $l \in \mathbb{Z}/n\mathbb{Z}$ le caractère χ_l défini par

$$\forall k \in \mathbb{Z}/n\mathbb{Z}, \chi_l(k) = \exp\left(\frac{2i\pi lk}{n}\right).$$

On vérifie alors que $\chi_l\chi_{-l'} = \chi_{l-l'}$. $\chi(l) = 1$ si et seulement si $l = 0$, donc $l \mapsto \chi_l$ est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ vers $\widehat{\mathbb{Z}/n\mathbb{Z}}$.

Correction des questions sur les groupes produits

1. On vérifie les propriétés. On considère $(0, ..., 0) \in G$, on a

$$\chi^{(1)} \times \cdots \times \chi^{(k)}(0, ..., 0) = \chi^{(1)}(0) \times \cdots \times \chi^{(k)}(0) = 1.$$

$$\begin{aligned} \chi^{(1)} \times \cdots \times \chi^{(k)}((x_1, ..., x_k) - (y_1, ..., y_k)) &= \chi^{(1)}(x_1 - y_1) \times \cdots \times \chi^{(k)}(x_k - y_k) \\ &= \chi^{(1)}(x_1) \times \cdots \times \chi^{(k)}(x_k)\chi^{(1)}(-y_1) \times \cdots \times \chi^{(k)}(-y_k) \\ &= \chi^{(1)}(x_1) \times \cdots \times \chi^{(k)}(x_k)\chi^{(1)}(y_1)^{-1} \times \cdots \times \chi^{(k)}(y_k)^{-1} \end{aligned}$$

Donc $\chi^{(1)} \times \cdots \times \chi^{(k)}$ est un caractère de G.

2. $\chi^{(1)} \times \cdots \times \chi^{(k)}(x_1, \ldots, x_k) = \rho^{(1)} \times \cdots \times \rho^{(k)}(x_1, \ldots, x_k)$. On peut appliquer, on note n_i le cardinal de G_i, et on a pour tout j

$$\chi^{(1)}\times\cdots\times\chi^{(k)}(n_1x_1, \ldots, x_j, \ldots, n_kx_k) = \rho^{(1)}\times\cdots\times\rho^{(k)}(n_1x_1, \ldots, x_j, \ldots, n_kx_k).$$

On en déduit que $\chi_j(x_j) = \rho_j(x_j)$. Autrement dit, $\prod_j \chi^{(j)} = \prod_j \rho^{(j)}$ si et seulement si $\chi^{(j)} = \rho^{(j)}$. Ainsi, les $\prod_j \chi^{(j)}$ sont distincts et forment $n_1 \ldots n_k = n$ morphismes de G, donc $\widehat{G} = \{\chi^{(1)} \times \cdots \times \chi^{(k)}, \quad \chi^{(1)} \in \widehat{G_1}, \ldots, \chi^{(k)} \in \widehat{G_k}\}$

4 Transformée de Fourier

Pour une fonction $f \in E$, on définit sa transformée de Fourier $\hat{f}$ par

$$\forall x \in G, \hat{f}(x) = n\langle f, \chi_x \rangle = \sum_{y \in G} f(y)\overline{\chi_x(y)}.$$

On définit également la transformée de Fourier inverse par

$$\forall x \in G, \tilde{f}(x) = \frac{1}{n} \sum_{y \in G} f(y)\chi_y(x).$$

1. Montrer que $f \mapsto \hat{f}$ est une application linéaire de E dans E.
2. Montrer que pour tout $f \in E$, on a $\tilde{\hat{f}} = f$.
3. Montrer que pour tout $f \in E$,

$$\sum_{x \in G} |\hat{f}(x)|^2 = n \sum_{x \in G} |f(x)|^2.$$

4. Montrer que pour tout $f, g \in E$, on a

$$\widehat{f \star g} = \hat{f}\hat{g}.$$

Correction de la quatrième partie

1.

5 Marche aléatoire

On considère $(X^{(k)})_{k \in \mathbb{N}^*}$ une suite de variables aléatoires indépendantes et indentiquement distribuées sur G. On définit la marche aléatoire S_k par

$$S_k = \sum_{l=1}^{k} X^{(l)}.$$

On notera $p^{(k)}(x) = \mathbb{P}(S_k = x)$.

1. Montrer que pour tout $k \in \mathbb{N}^*$, on a

$$\overbrace{p \star \cdots \star p}^{k} = p^{(k)}.$$

   Une première question qu'on se posera sera de savoir si S_k se rapproche de la loi uniforme υ sur G pour la norme ℓ^1, i.e. étudier la quantité suivante

$$\|p^{(k)} - \upsilon\|_1 = \sum_{x \in G} \left| p^{(k)}(x) - \frac{1}{n} \right|.$$

(a) Montrer que pour tout $k \in \mathbb{N}^*$, on a

$$\|p^{(k)} - \upsilon\|_1 \leq \sqrt{n}\|p - \upsilon\|_2.$$

En déduire que pour tout $k \in \mathbb{N}^*$, on a

$$\|p^{(k)} - \upsilon\|_1 \leq \left\|\hat{p}^k - \widehat{\upsilon}\right\|_2$$

(b) Montrer que pour tout $k \in \mathbb{N}^*$, on a

$$\left\|\hat{p}^k - \widehat{\upsilon}\right\|_2^2 = \sum_{x \in G \setminus \{0\}} |\hat{p}(x)|^{2k}.$$

(c) On considère désormais que $G = \mathbb{Z}/n\mathbb{Z}$ avec n impair et $p(X = -1) = p(X = 1) = \frac{1}{2}$. Montrer que pour tout $z \in [0, \pi/2[$, on a

$$\cos\left(\frac{2z\pi}{n}\right) \leq e^{-\frac{z^2}{2}}$$

(d) Pour tout $k \in \mathbb{N}^*$, montrer que

$$\sum_{x=1}^{n-1} \cos\left(\frac{2\pi x}{n}\right)^{2k} = 2\sum_{x=1}^{\frac{n-1}{2}} \cos\left(\frac{2\pi x}{n}\right)^{2k} = 2\sum_{x=1}^{\frac{n-1}{2}} \cos\left(\frac{\pi x}{n}\right)^{2k}$$

En déduire l'inégalité suivante

$$\|p^{(k)} - \upsilon\|_1^2 \leq 2e^{-\frac{k\pi^2}{n^2}} \sum_{x=1}^{\frac{n-1}{2}} e^{-\frac{\pi^2(x^2-1)k}{n^2}}$$

(e) Montrer que pour $x \in \{1, \ldots, n-1\}$, $(x^2 - 1) \geq 3(x - 1)$, et en déduire que

$$\|p^{(k)} - \upsilon\|_1^2 \leq 2\frac{e^{-\frac{k\pi^2}{n^2}}}{1 - e^{-\frac{3k\pi^2}{n^2}}}$$

5.1 Retour à l'origine

On s'intéresse désormais à la probabilité de retour à l'origine dans $(\mathbb{Z}/2\mathbb{Z})^n$, i.e.

$$\mathbb{P}(S_k = 0).$$

On suppose de plus que $p(e_i) = \frac{1}{n+1}$ où $e_0 = 0$ et e_i correspond au n-uplet de 0 sauf en la i-ième position où il vaut 1. Pour tout $x \in (\mathbb{Z}/2\mathbb{Z})^n$, on note $w(x)$ le nombre de 1 dans x.

(a) On note $\mathcal{B}_m = \{x \in (\mathbb{Z}/2\mathbb{Z})^n, w(x) = m\}$. Montrer que

$$\operatorname{card}(\mathcal{B}_m) = \binom{n}{m}.$$

(b) Montrer que pour tout $(x_1, \dots, x_n)$, on a

$$\hat{p}(x) = \frac{1+n-2w(x)}{n+1} = 1 - \frac{2w(x)}{n+1}.$$

(c) En déduire que pour tout $k \in \mathbb{N}^*$, on a

$$p^{(k)}(0) = \frac{1}{2^n} \sum_{m=0}^{n} \binom{n}{m} \left(1 - \frac{2m}{n+1}\right)^k.$$

$$\begin{aligned} \frac{1}{2^n} \sum_{m=0}^{n} \binom{n}{m} \left(1 - \frac{2m}{n+1}\right)^{2k} &\leq \left(1 - \frac{2}{n+1}\right)^k \frac{1}{2^n} \sum_{m=0}^{n} \binom{n}{m} \\ &= \left(1 - \frac{2}{n+1}\right)^k. \end{aligned}$$

Correction de la cinquième partie

1. Généralement, on considère deux variables aléatoires indépendantes X et Y. La loi de $X+Y$ sera donné par la convolution des lois de X et Y. On a

$$\begin{aligned} \mathbb{P}(X+Y=x) &= \sum_{y \in G} \mathbb{P}(X+Y=x, Y=y) \\ &= \sum_{y \in G} \mathbb{P}(X=x-y, Y=y) \\ &= \sum_{y \in G} \mathbb{P}(X=x-y)\mathbb{P}(Y=y). \end{aligned}$$

On fait ensuite la preuve par récurrence. $p^{(1)} = p$. On suppose que $\overbrace{p \star \cdots \star p}^{k} = p^{(k)}$. On a $S_{k+1} = S_k + X^{(k+1)}$ avec S_k et $X^{(k+1)}$ indépendants. On a donc

$$p^{(k+1)} = p^{(k)} \star p = \overbrace{p \star \cdots \star p}^{k+1}.$$

(a) On utilise l'inégalité de Cauchy-Schwarz pour passer de la norme 1 à la norme 2. On utilise ensuite l'égalité de Plancherel.

(b) On remarque que $\upsilon = \chi_0$ et $\hat{p^{(k)}}(0) = n$

$$\begin{aligned} \left\|\hat{p}^k - \widehat{\upsilon}\right\|_2^2 &= \sum_{x \in G} |\hat{p}^k(x) - \widehat{\upsilon}(x)|^2 \\ &= \sum_{x \in G} \left|\hat{p^{(k)}}(x) - n\langle \chi_0, \chi_x \rangle\right|^2 \\ &= \sum_{x \in G \setminus \{0\}} |\hat{p}(x)|^{2k}. \end{aligned}$$

(c) On commmence par calculer $\hat{p}(x)$. On a

$$\begin{aligned}
\hat{p}(x) &= \sum_{y \in G} p(y)\overline{\chi_x(y)} \\
&= \frac{1}{2}\left(\chi_{-1}(x) + \chi_1(x)\right) \\
&= \frac{1}{2}\left(e^{-\frac{2x\pi}{n}} + e^{\frac{2x\pi}{n}}\right) \\
&= \cos\left(\frac{2\pi x}{n}\right)
\end{aligned}$$

On a donc

$$\|p^{(k)} - \upsilon\|^2 \leq \sum_{x=1}^{n-1} \cos\left(\frac{2\pi x}{n}\right)^{2k}.$$