

## 110. Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

**Introduction :** La transformée de Fourier discrète est un outil très utilisé en traitement du signal. Sa théorie sous-jacente repose sur la notion de caractère.

### 1 Dual d'un groupe abélien

Soit  $G$  un groupe fini, soit  $n = |G|$ .

#### 1.1 Généralités

**Proposition 1.** On note  $\mathcal{F}(G)$  l'ensemble des fonctions de  $G$  dans  $\mathbb{C}$ .

$\mathcal{F}(G)$  est un  $\mathbb{C}$ -espace vectoriel, que l'on munit du produit scalaire hermitien

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

**Proposition 2.** On note, pour  $g \in G$ ,  $\delta_g : h \mapsto \mathbb{1}_{h=g}$ .  $(\delta_g)_{g \in G}$  forme une base orthogonale de  $\mathcal{F}(G)$ , et  $\mathcal{F}(G)$  est un  $\mathbb{C}$ -ev de dimension  $n$ .

**Définition 3.** Soit  $G$  un groupe fini. Un caractère de  $G$  est un morphisme de groupes  $\chi : G \rightarrow \mathbb{C}^*$ . L'ensemble des caractères de  $G$  est appelé dual de  $G$ , et noté  $\widehat{G}$ .

**Exemple 4.** La signature  $\varepsilon$  est un caractère du groupe symétrique  $\mathcal{S}_p$ .

**Proposition 5.**  $(\widehat{G}, \times)$  est un groupe abélien.

**Proposition 6.** Tout caractère  $\chi \in \widehat{G}$  est constant sur les classes de conjugaison de  $G$ .

**Proposition 7.** Si  $n = |G|$ , alors tout caractère de  $G$  prend ses valeurs dans  $\mathbb{U}_n$ , l'ensemble des racines  $n$ -èmes de l'unité. En particulier,  $\widehat{G}$  est un groupe fini.

#### 1.2 Cas d'un groupe cyclique

**Définition 8.**  $G$  est dit cyclique s'il est monogène.

**Proposition 9.** Si  $G$  est cyclique, alors  $G$  est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$  et à  $\mathbb{U}_n$ .

**Théorème 10.** Supposons  $G$  cyclique, soit  $g$  générateur de  $G$ , soit  $\omega$  une racine primitive  $n$ -ème de l'unité. Alors  $\widehat{G} = \{\chi_0, \dots, \chi_{n-1}\}$  où pour  $j \in \llbracket 0, n-1 \rrbracket$ ,  $\chi_j : g^k \mapsto \omega^{jk}$ . En particulier,  $G$  et  $\widehat{G}$  sont isomorphes.

**Remarque 11.** L'isomorphisme n'est pas canonique, puisqu'il dépend du choix de  $\omega$ .

**Théorème 12.** Si  $G$  est cyclique, alors  $\widehat{G}$  forme une base orthonormée de  $\mathcal{F}(G)$ .

### 1.3 Cas général

On suppose désormais seulement  $G$  abélien.

**Proposition 13.** Si  $H, K$  sont deux groupes abéliens, alors  $\widehat{H \times K}$  est isomorphe à  $\widehat{H} \times \widehat{K}$ .

**Lemme 14.** Si  $H$  sous-groupe distingué de  $G$ , tout caractère de  $H$  se prolonge en un caractère de  $G$ .

**Théorème 15.** Il existe une unique suite  $d_1, \dots, d_k \in \mathbb{N}$  telle que  $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$  et  $d_1 | d_2 | \dots | d_k$ .

**Exemple 16.** Le groupe des bitranspositions de  $\mathcal{S}_4$  est isomorphe à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

**Corollaire 17.** On a alors encore  $G \simeq \widehat{G}$ .

**Théorème 18.** Si  $G$  abélien,  $\widehat{G}$  forme toujours une base orthonormée de  $\mathcal{F}(G)$ .

**Corollaire 19.** On a, pour tous  $g, h \in G$ ,  $\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g) \overline{\chi(h)} = \mathbb{1}_{g=h}$ .

**Théorème 20.**  $G$  et  $\widehat{\widehat{G}}$  sont canoniquement isomorphes via  $g \mapsto (\chi \mapsto \chi(g))$ .

### 1.4 Application : tables de groupes non abéliens

**Lemme 21.** Soient  $H$  distingué dans  $G$  et  $\bar{\rho} : G/H \rightarrow GL(V)$  une représentation de  $G/H$ . Alors  $\rho = \bar{\rho} \circ \pi$  définit une représentation de  $G$ , irréductible si et seulement si  $\bar{\rho}$  est irréductible.

**Proposition 22.** Les caractères irréductibles de  $G/D(G)$  sont en bijection avec les caractères de degré 1 de  $G$ .

**Application 23.**  $D(\mathbb{H}_8) = \{-1, 1\}$  et  $\mathbb{H}_8/\{-1, 1\}$  est isomorphe à  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . On en déduit la table de caractères de  $\mathbb{H}_8$ .

**Application 24.** Si on note  $V_4$  le sous-groupe de  $\mathcal{A}_4$  engendré par les bitranspositions,  $\mathcal{A}_4/V_4$  est isomorphe à  $\mathbb{Z}/3\mathbb{Z}$ , et on déduit de la table de  $\mathbb{Z}/3\mathbb{Z}$  celle de  $\mathcal{A}_4$ .

## 2 Transformation de Fourier

### 2.1 Convolution dans les groupes abéliens

**Définition 25.** Soient  $f_1, f_2 \in \mathcal{F}(G)$ . On définit leur produit de convolution par  $f_1 * f_2(g) = \sum_{h \in G} f_1(h)f_2(gh^{-1})$ .

**Proposition 26.** Le produit de convolution est associatif, commutatif et  $(f_1, f_2) \mapsto f_1 * f_2$  est bilinéaire.

**Corollaire 27.**  $(\mathcal{F}(G), +, *, \cdot)$  a une structure de  $\mathbb{C}$ -algèbre.

**Remarque 28.** On a, pour  $g, h \in G, f \in \mathcal{F}(G), (f * \delta_g)(h) = f(gh^{-1})$ .

### 2.2 Transformation de Fourier dans les groupes abéliens

**Remarque 29.**  $\widehat{G}$  formant une base orthonormée de  $\mathcal{F}(G)$ , toute fonction  $f \in \mathcal{F}(G)$  peut s'écrire  $f = \sum_{\chi \in \widehat{G}} c_\chi(f)\chi$  avec  $c_\chi(f) = \langle f, \chi \rangle$ .

**Définition 30.** On appelle alors la transformée de Fourier de  $f$  l'application  $\widehat{f} : \widehat{G} \rightarrow \mathbb{C}, \chi \mapsto |G|c_\chi(f) = \sum_{g \in G} f(g)\overline{\chi}(g)$ .

**Proposition 31** (Inversion). On a alors  $f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi$ .

**Proposition 32** (Parseval). On a, pour  $f, h \in \mathcal{F}(G), \langle f, h \rangle = \frac{1}{|G|} \langle \widehat{f}, \widehat{h} \rangle$ .

**Proposition 33.** Pour  $f, h \in \mathcal{F}(G)$ , on a  $\widehat{f * h} = \widehat{f}\widehat{h}$ .

### 2.3 Transformée de Fourier discrète

On se place désormais sur le groupe cyclique  $G = \mathbb{Z}/N\mathbb{Z}$ . On note  $\omega_N = e^{2i\pi/N}$ , et on rappelle que les caractères de  $G$  sont les  $\chi_k : n \mapsto e^{2ikn\pi/N} = \omega_N^{kn}, 0 \leq k \leq n-1$ . On notera  $\widehat{f}(k) = \widehat{f}(\chi_k)$ .

**Définition 34.** On appelle transformée de Fourier de  $f = (f(n))_{0 \leq n \leq N}$  le vecteur  $(\widehat{f}(n))_{n \in \mathbb{N}}$ . On définit ainsi la transformée de Fourier comme une application  $\mathbb{C}^N \rightarrow \mathbb{C}^N$ .

On a ainsi  $\widehat{f}(k) = \sum_{n=0}^N f(n)\omega_N^{-nk}$ .

**Lemme 35.**

Pour  $x \in \mathbb{C}$ , on définit la matrice de Vandermonde

$$V(x) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & x & \cdots & x^{(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x^{(N-1)} & \cdots & x^{(N-1)(N-1)} \end{pmatrix}. \text{ Alors } V(\omega_N^{-1}) \text{ a pour inverse } \frac{1}{N}V(\omega_N).$$

**Remarque 36.** Le calcul de la transformée de Fourier d'un échantillon  $(f(k))_{0 \leq k \leq N-1}$  revient à faire le produit par  $V(\omega_N^{-1})$ . Ce calcul nécessite donc  $O(N^2)$  opérations. L'inversion est donc également possible en le même nombre d'opérations.

## 3 Utilisation de la transformée de Fourier discrète

### 3.1 Transformée de Fourier rapide

On suppose que  $N = 2^p, p \in \mathbb{N}^*$ .

On a  $\widehat{f}(k) = \sum_{n=0}^{N/2-1} f(2n)\omega_N^{-2nk} + \sum_{n=0}^{N/2-1} f(2n+1)\omega_N^{-(2n+1)k}$ . Ainsi, si on définit

$f_p = (f(0), f(2), \dots, f(N-2))$  et  $f_i = (f(1), f(3), \dots, f(N-1))$ , on a :

Pour  $k \in \llbracket 0, \frac{N}{2} - 1 \rrbracket, \widehat{f}(k) = \widehat{f}_p(k) + \omega_N^{-k}\widehat{f}_i(k)$ .

Pour  $k \in \llbracket \frac{N}{2}, N \rrbracket, \widehat{f}(k) = \widehat{f}_p(k - \frac{N}{2}) - \omega_N^{k-N/2}\widehat{f}_i(k - \frac{N}{2})$ .

On a ainsi un algorithme de calcul récursif qui permet le calcul de la transformée de Fourier en  $O(N \log_2(N))$  opérations.

**Remarque 37.** Cet algorithme permet aussi le calcul de la transformée inverse, en remplaçant  $\omega_N^{-1}$  par  $\omega_N$  et en divisant le résultat final par  $N$ .

### 3.2 Application : multiplication de polynômes

**Remarque 38.** Le calcul de la transformée de Fourier de  $(f(0), \dots, f(N-1))$  revient aussi à évaluer le polynôme  $P = f(0) + f(1)X + \dots + f(N-1)X^{N-1}$  en  $1, \omega_N^{-1}, \dots, \omega_N^{-(N-1)}$ . La transformée de Fourier inverse revient alors à interpoler le polynôme prenant les valeurs  $\widehat{f}(0), \dots, \widehat{f}(N-1)$  en  $1, \omega_N^{-1}, \dots, \omega_N^{-(N-1)}$ .

Ainsi, si  $P, Q$  sont deux polynômes de degré  $N$ , on peut calculer les coefficients de leur produit  $PQ$  via l'algorithme suivant :

1. Les évaluer en  $1, \omega_{2N}^{-1}, \dots, \omega_{2N}^{-(2N-1)}$ .

2. Effectuer le produit terme à terme  $PQ(1) = P(1)Q(1), \dots, PQ(\omega_{2N}^{-(2N-1)}) = P(\omega_{2N}^{-(2N-1)})Q(\omega_{2N}^{-(2N-1)})$ .
3. Interpoler le polynôme  $PQ$  par transformée de Fourier inverse.

## Développements

- Théorème de structure des groupes abéliens finis.
- Table de caractères de  $\mathcal{A}_4$  et  $\mathbb{H}_8$ .

## Références

- [1] G. Peyré, L'ALGÈBRE DISCRÈTE DE LA TRANSFORMÉE DE FOURIER, Ellipses.
- [2] G. Rauch, LES GROUPES FINIS ET LEURS REPRÉSENTATIONS, Ellipses.