Transformée de Fourier sur un groupe fini

Gabriel Peyré

Définition 0.1. DUAL D'UN GROUPE Soit G un groupe fini. Par définition, un caractère χ est un morphisme du groupe G dans le groupe multiplicatif $\mathbb{C}^*$. On note $\widehat{G}$ l'ensemble des caractères, et on l'appelle le dual de G. $\widehat{G}$ est un groupe pour la multiplication des applications, i.e. pour $(\chi_1, \chi_2) \in \widehat{G}^2$ on définit

$$(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x).$$

Proposition 0.1. *Soit G un groupe fini de cardinal n. Les éléments de $\widehat{G}$ sont en fait les morphismes de G dans le groupe des racines nièmes de l'unité.*

Définition 0.2. On note E l'ensemble des fonctions de G dans $\mathbb{C}$. C'est un espace vectoriel de dimension $n = Card(G)$ sur $\mathbb{C}$. Sur E on définit un produit scalaire hermitien, pour $(f, g) \in E^2$ par la formule :

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

Où $\overline{y}$ désigne le conjugué de y.

Proposition 0.2. DANS LE CAS CYCLIQUE *Soit $G = \mathbb{Z}/p\mathbb{Z}$. Soit $\omega = e^{\frac{2\imath\pi}{p}}$. Tous les éléments de $\widehat{G}$ sont alors de la forme, pour $i \in \{0, \dots, n-1\}$:*

$$\begin{array}{lll} \chi_i : G & \to \mathbb{C}^* \\ x & \mapsto (\omega^i)^x = e^{\frac{2\imath\pi i x}{p}} \end{array}$$

On a $G \simeq \widehat{G}$, et même plus fort, car $\widehat{G}$ forme une base orthogonale de E.

Proposition 0.3. CAS GÉNÉRAL *Soit G un groupe fini commutatif. Alors $\widehat{G}$ est une base orthogonale de E. On peut le voir via la décomposition des $\mathbb{Z}$-modules (i.e. des groupes abéliens) :*

$$G \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_r\mathbb{Z} \qquad (p_1, \dots, p_r) \in (\mathbb{N}^*)^r$$

ou alors en montrant que pour tout caractère sur un sous groupe $H \subset G$ peut être prolonger en un caractère de G, ce qui induit la suite exacte : $\{1\} \to \widehat{G/H} \hookrightarrow \widehat{G} \twoheadrightarrow \widehat{H} \to \{1\}$où la flèche $\widehat{G} \twoheadrightarrow \widehat{H}$ est le morphisme de restriction. Ceci montre que $\|\widehat{G}\| = \|\widehat{H}\|\|\widehat{G/H}\|$, et permet de démontrer par récurrence sur $\|G\|$ que $\|\widehat{G}\| = \|G\|$.

Remarque. Tout ceci est faux dans le cas non commutatif, comme le montre l'étude du groupe symétrique S_n. En effet, si on prend $f_1 = (a, b)$ et $f_2 = (c, d)$ deux transpositions, soit alors une permutation g dans S_n telle que : $g(a) = c$, $g(b) = d$. On a : $f_2 = gf_1g^{-1}$ d'où , si on note χ un caractère :

$$\chi(f_2) = \chi(gf_1g^{-1}) = \chi(g)\chi(f_1)\chi(g)^{-1} = \chi(f_1)$$

Donc χ est constante sur les transpositions, et comme $\chi(f_1^2) = \chi(f_1)^2 = 1$ on a $\chi(f_i) = +1$ ou $\chi(f_i) = -1$. Pour conclure, il suffit, si on prend une permutation quelconque f dans S_n, de la décomposer en produit de transpositions, et on a donc seulement deux caractères :

$$\forall f \in G, \quad \begin{array}{l} \chi_1(f) = 1 \quad \text{et} \\ \chi_2(f) = (-1)^{\varepsilon(f)} \end{array}$$

Où ε désigne la signature. La solution pour contourner ce problème de « manque » de caractère est de considérer des représentations de notre groupe ainsi que les caractères de ces représentations (le dual est composé uniquement des caractères des représentations de dimension 1).

Référence : [**?**, p.103][**?**, p.203][**?**, p.74][**?**, p.764][**?**, p.93]
Utilisation : (***,5) (**,2) (*,0)
Mots clefs : groupe fini, dualité, racines de l'unité, caractères, produit hermitien, transformée de Fourier, algorithmes, polynômes, racines de l'unité.

103	Sous-groupes distingués, groupes quotients. Exemples et applications.	***
104	Groupes finis. Exemples et applications.	***
108	Congruences dans $\mathbb{Z}/n\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.	***
114	Groupe des nombres complexes de module 1. Applications.	***
137	Exemples de parties génératrices d'un groupe.	***
126	Endomorphismes remarquables d'un espace vectoriel hermitien de dimension finie.	**
136	Formes linéaires sur un espace vectoriel de dimension finie. Espace dual, orthogonalité. Applications.	**