Réf : Colmez Elts d'analyse et d'algèbre
Beyer L'algèbre discrète de la transformée de Fourier (Pas dans la bibliothèque de l'agrég)

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

110

I. Caractères d'un groupe

1. Représentations linéaires

Définition 1 : Soit G un groupe, et soit k un corps.
On appelle représentation de G la donnée d'un k-espace vectoriel V et d'un morphisme $\rho : G \to GL(V)$.
Si $\dim(V) < \infty$, on note $\chi : g \in G \mapsto \mathrm{Tr}(\rho(g)) \in k$ le caractère de (V, ρ).

Définition 2 : Soient (V,ρ) et (V',ρ') deux k-représentations de G.
On pose $\rho \otimes \rho'(g)$ l'unique isomorphisme de $V \otimes V'$ se restreignant à $\rho(g)$ sur V et à $\rho'(g)$ sur V'. La représentation obtenue est notée $(V \otimes V', \rho \otimes \rho')$.

Théorème 3 : Soit G un groupe abélien fini, et soit k un corps de caractéristique ne divisant pas $|G|$, algébriquement clos.
Alors toute représentation de G est somme de représentations de dimension 1 (de dimension finie).

Remarque : dans la suite on supposera $k = \mathbb{C}$, G fini abélien, et on s'intéressera à la dimension 1. On a alors $\rho(g) = \chi(g) \cdot \mathrm{Id}_V$ donc l'étude des caractères suffit.

2. Dual d'un groupe abélien fini

Proposition 4 : Les caractères de représentations de dimension 1 de G sont les morphismes de G dans $(\mathbb{C}^*, \cdot)$. Ils forment un groupe $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^*)$

Proposition 5 : Si G est d'exposant n, $\hat{G} = \mathrm{Hom}(G, U_n)$ où $(U_n, \cdot)$ est le groupe des racines n-èmes de l'unité.

Corollaire 6 : $\hat{G}$ est aussi un groupe abélien fini.

Corollaire 7 : $\overline{\chi} = \chi^{-1}$ pour tout $\chi \in \hat{G}$.

Définition 8 : On note $\mathbb{C}[G]$ le $\mathbb{C}$-espace vectoriel des fonctions $G \to \mathbb{C}$.
On le munit du produit hermitien $\langle f ; g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$

Théorème 9 : Si G est cyclique, $\hat{G} \simeq G$ et $\hat{G}$ est une base orthonormée de $\mathbb{C}[G]$.
Remarque : l'isomorphisme $G \simeq \hat{G}$ n'est pas canonique

Lemme 10 : Soit $H \leq G$ et $\chi \in \hat{H}$. Alors χ se prolonge à G.

Lemme 11 : On a alors la suite exacte courte $1 \to G/H \to \hat{G} \to \hat{H} \to 1$ où $G/H \to \hat{G}$ est la composition par $G \to G/H$ et $\hat{G} \to \hat{H}$ la restriction.

Corollaire 12 : $\hat{G}$ et G ont même ordre.

DVT 1.

3. Bidual et théorème de structure

Définition 13 : Le bidual de G est le dual $\hat{\hat{G}}$ de $\hat{G}$.
On dispose de $\Phi : \left[g \mapsto (\chi \in \hat{G} \mapsto \chi(g) \in \mathbb{C}) \right] \in \hat{\hat{G}}$

Proposition 14 : Φ est un isomorphisme de G sur $\hat{\hat{G}}$.

Corollaire 15 : G et $\hat{G}$ ont même exposant.

Théorème 16 (structure) : Il existe une unique suite $n_r | n_{r-1} | \cdots | n_1 \neq 0$ d'entiers > 0 telle que : $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$.

DVT 2.

4. L'algèbre $\mathbb{C}[G]$

Proposition 17 : $\hat{G}$ est une base orthonormée de $\mathbb{C}[G]$.

Fin du DVT1

Proposition-Définition 18 : Pour f et g dans $\mathbb{C}[G]$, on pose $f * g \in \mathbb{C}[G]$ la fonction : $f * g : \left[x \mapsto \sum_{h \in G} f(h)\, g(xh^{-1}) \right]$. On définit ainsi sur $\mathbb{C}[G]$ une structure d'algèbre associative, commutative, et unitaire.

Proposition 19 : $\left[g \mapsto 1_g \right] : (G, \cdot) \to (\mathbb{C}[G]^\times, *)$ est un morphisme de groupes injectif.
On identifie G à son image.

Proposition 19 : Si $\rho \in \hat{G}$, il existe un unique morphisme d'algèbres $\tilde{\rho} : \mathbb{C}[G] \to \mathbb{C}$ tel que $\tilde{\rho}(1_g) = \rho(g)$.

Corollaire 20 : $\hat{G} = \mathrm{Hom}_{gr}(G, \mathbb{C}^*) = \mathrm{Hom}_{\mathbb{C}\text{-Alg}}(\mathbb{C}[G], \mathbb{C})$

Rappel :

II. Transformée de Fourier dans $\mathbb{C}[G]$

G désigne toujours un groupe abélien fini.

Définition 21 : Pour $f \in \mathbb{C}[G]$, on pose $c_f : \left\{ \begin{array}{ccc} \widehat{G} & \longrightarrow & \mathbb{C} \\ \chi & \longmapsto & \langle f, \chi \rangle \end{array} \right.$. Les $c_f(\chi)$ sont les coefficients de Fourier de f.

Définition 22 : Pour $f \in \mathbb{C}[G]$, on note $\widehat{f}(\chi) = |G| \, c_f(\overline{\chi})$ et on pose $\mathcal{F} : \left\{ \begin{array}{ccc} \mathbb{C}[G] & \longrightarrow & \mathbb{C}[\widehat{G}] \\ f & \longmapsto & \widehat{f} \end{array} \right.$ la transformation de Fourier.

Proposition 23 : On a la formule d'inversion : $f = \sum_{\chi \in \widehat{G}} c_f(\chi) \chi = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \overline{\chi}$

Corollaire 24 : $\mathcal{F}$ est un isomorphisme d'espaces vectoriels de $\mathbb{C}[G]$ sur $\mathbb{C}[\widehat{G}]$

Proposition 25 : (Plancherel) Pour $(f, g) \in \mathbb{C}[G]^2$, on a :

$$\sum_{s \in G} f(s) \overline{g(s)} = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \overline{\widehat{g}(\chi)}$$

Proposition 26 : Pour f, g dans $\mathbb{C}[G]$, on a : $\widehat{f * g} = \widehat{f} \cdot \widehat{g}$

Corollaire 27 : $\mathcal{F}$ est un isomorphisme d'algèbres de $(\mathbb{C}[G], +, \cdot, *)$ dans $(\mathbb{C}[\widehat{G}], +, \cdot, \times)$ où $\times$ est la multiplication usuelle.

III. Application aux corps finis

Dans la suite q est une puissance p^r d'un nombre premier p impair.

1. Caractères additifs et multiplicatifs de $\mathbb{F}_q$

Définition 28 : Un élément de $\widehat{\mathbb{F}_q}$ est appelé caractère additif. Un élément de $\widehat{\mathbb{F}_q^*}$ est appelé caractère multiplicatif.

Théorème 29 : $\mathbb{F}_q^*$ est cyclique.

Proposition 30 : Soit ζ un générateur de $\mathbb{F}_q^*$, et soit $\omega = e^{\frac{2i\pi}{q-1}}$. On note $\chi_1 : \left\{ \begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \mathbb{C}^* \\ \zeta^k & \longmapsto & \omega^k \end{array} \right.$. χ_1 est un caractère multiplicatif, et les caractères multiplicatifs sont exactement les $\chi_j = \chi_1^j$ pour $j \in \{0, \dots, q-2\}$

Proposition 31 : On a $\chi_{\frac{q-1}{2}}(x) = \begin{cases} 1 & \text{si } x \text{ est un carré de } \mathbb{F}_q \\ -1 & \text{sinon} \end{cases}$ pour tout $x \in \mathbb{F}_q^*$

On note ce caractère η, et on le nomme caractère quadratique de $\mathbb{F}_q$.

Définition 32 : Pour $a \in \mathbb{F}_q$, on note $\mathrm{Tr}(a) = a + a^p + \dots + a^{p^{r-1}}$.

Proposition 33 : Tr est une forme $\mathbb{F}_p$-linéaire non nulle de $\mathbb{F}_q$.

Définition 34 : On appelle caractère additif canonique de $\mathbb{F}_q$ le caractère $\psi_1 : \left\{ \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & \exp\left(\frac{2i\pi}{p} \mathrm{Tr}(x)\right) \end{array} \right.$

Proposition 35 : Les caractères additifs sont les $\psi_a = \psi_1(a \cdot)$ pour $a \in \mathbb{F}_q$.

2. Sommes de Gauss

Notation : Dans la suite si χ est un caractère multiplicatif, on le prolongera à $\mathbb{F}_q$ en $\widetilde{\chi}$ avec $\widetilde{\chi}(0) = 0$.

Définition 36 : Soient ψ un caractère additif et χ un caractère multiplicatif. On appelle somme de Gauss de χ et ψ la somme : $G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi(x)$

Proposition 37 : $G(\chi, \psi) = \mathcal{F}_{\text{mult}}(\psi_{|\mathbb{F}_q^*})(\chi) = \mathcal{F}_{\text{add}}(\widetilde{\chi})(\psi)$.

Corollaire 38 : $\chi = \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} G(\chi, \overline{\psi}) \, \psi$

Propriétés 39 :

- $\forall a, b \in \mathbb{F}_q$, $G(\chi, \psi_{ab}) = \overline{\chi(a)} \, G(\chi, \psi_b)$
- $G(\chi, \overline{\psi}) = \chi(-1) \, G(\chi, \psi)$
- $G(\overline{\chi}, \psi) = \chi(-1) \, \overline{G(\chi, \psi)}$

Proposition 40 : $G(\chi,\psi) = \begin{cases} q-1 \text{ si } \chi=\chi_0, \psi=\psi_0 \\ -1 \text{ si } \chi=\chi_0, \psi\neq\psi_0 \\ 0 \text{ si } \chi\neq\chi_0, \psi=\psi_0 \end{cases}$

Sinon $(\chi\neq\chi_0, \psi\neq\psi_0)$, $|G(\chi,\psi)|^2 = q$, et $G(\chi,\psi)G(\overline{\chi},\psi) = q\chi(-1)$

Proposition 41 : Soit m l'ordre de χ dans $\mathbb{F}_q^*$.

Alors $\chi(-1) = \begin{cases} -1 \text{ si } m \text{ pair } \frac{q-1}{m} \text{ impair} \\ +1 \text{ sinon} \end{cases}$

3. Réciprocité quadratique

Dans la suite $q=p$ est premier. η se note alors $\left(\frac{\cdot}{p}\right)$ via le symbole de Legendre.

Définition 42 : On notera $T : \mathbb{C}[\mathbb{F}_p^*] \longrightarrow \mathbb{C}[\mathbb{F}_p^q]$

$$f \longmapsto Tf : \left| \begin{array}{ccc} \mathbb{F}_p^q & \to & \mathbb{C}^q \\ a & \mapsto & \sum_{x\in\mathbb{F}_p^q} f(x)\, e^{2i\frac{ax}{p}\pi} \end{array} \right.$$

Proposition 43 : $\det(T) = (-1)^{\frac{p-1}{2}} i^{\frac{(p-1)(p-3)}{4}} p^{\frac{p-3}{2}} G(\eta,\psi_1)$

Proposition 44 : $G(\eta,\psi_1) = \begin{cases} \sqrt{p} \text{ si } p\equiv 1[4] \\ i\sqrt{p} \text{ si } p\equiv 3[4] \end{cases}$

Théorème 45 : Si p et r sont deux entiers premiers impairs distincts, alors $\left(\frac{p}{r}\right)\left(\frac{r}{p}\right) = (-1)^{\frac{(p-1)(r-1)}{4}}$

IV Transformée de Fourier discrète

Définition 46 : Soit $N\geq 1$, et $f=(f[n])\in\mathbb{C}^N$. On appelle transformée de Fourier discrète le vecteur $\hat{f}=(\hat{f}[k])\in\mathbb{C}^N$ tel que

$$\hat{f}[k] = \sum_{n=0}^{N-1} f[n] \exp\left[\frac{2i\pi}{N}\times(-nk)\right]$$

Proposition 47 : Si on note $f_i : \underline{\mathbb{Z}/N\mathbb{Z}} \to \mathbb{C}$, $i \mapsto f[i]$, et $\chi_k : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^*$, $\ell \to \exp\left(\frac{2i\pi}{N}\ell k\right)$

on a $\hat{f}[k] = \mathcal{F}(f_i)(\chi_k)$

Corollaire 48 : On a : $\forall n\in\{0,\dots,N-1\}$, $f[n] = \frac{1}{N}\sum_{k=0}^{N-1} \hat{f}[k]\exp\left(\frac{+2i\pi nk}{N}\right)$

Corollaire 49 : $\mathbb{C}^N \to \mathbb{C}^N$, $f \to \hat{f}$ est un isomorphisme d'espaces vectoriels.

Corollaire 50 (Plancherel) : $\sum_{i=0}^{N-1} f[i]g[i] = \frac{1}{N}\sum_{i=0}^{N-1} \hat{f}[i]\hat{g}[i]$

Proposition 51 : Soit $f\in\mathbb{C}^N$. On note :

$\hat{f}_g = \{\hat{f}[0],\dots,\hat{f}[\frac{N}{2}-1]\}$, $\hat{f}_d = \{\hat{f}[\frac{N}{2}],\dots,\hat{f}[N]\}$

$f_0 = \{f[0], f[2],\dots,f[N-2]\}$, $f_1 = \{f[1], f[3],\dots,f[N-1]\}$

$S : \{x_i\} \to \{x_i \exp(\frac{2i\pi}{2^p}i)\}$

Alors $\hat{f}_g = \hat{f}_0 + S\hat{f}_1$ et $\hat{f}_d = \hat{f}_0 - S\hat{f}_1$

Remarque : La TFD d'un vecteur de taille 2^p se calcule donc à partir de celles de 2 vecteurs de taille 2^{p-1}, de deux additions, de N coordonnées, et de N produits.

On obtient un algorithme en $O(n\log n)$, dit algorithme de transformée de Fourier rapide (FFT).