# Leçon 110 : Structure et dualité des groupes abéliens finis. Applications.

## Développements :

Thm de structure des groupes abéliens finis. Dualité et bidualité pour un groupe fini abélien

## Bibliographie :

Peyré, Ulmer,

## Plan

Soit $G$ un groupe fini quelconque

## 1 Dualité des groupes abéliens finis

**Proposition 1** (Ulm p.149)**.** *Un sous groupe abélien fini $G$ de $\mathrm{GL}_n(\mathbb{C})$ peut être mis simultanément sous forme diagonale, en particulier, toutes les représentations irréductibles de $G$ sont de degré 1.*

Cela donne une importance particulière aux représentations de degré 1.

### 1.1 Caractères linéaires et groupe dual

**Définition 2** (Pey p.2)**.** On appelle caractère linéaire de $G$, un morphisme de groupes $G \to \mathbb{C}^*$.

*Remarque* 3. L'usage du mot caractère est un abus dans ce contexte, l'abus est légitimé par le fait que le caractère de la représentation est clairement égal à $\chi$.

**Définition 4** (Pey p.2)**.** On appelle groupe dual $\hat{G}$, l'ensemble des caractères linéaires de $G$.

**Proposition 5** (Pey p.2)**.** *$\hat{G}$ est un groupe muni de la multiplication sur les valeurs : $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$.*

On a une réciproque :

**Proposition 6** (réécriture de Ulmer p.157)**.** *$G$ abélien ssi toutes ses représentations irréductibles sont de degré 1.*

Ainsi $\hat{G}$ est l'ensemble des caractères irréductibles. Or les caractères irréductibles forment une bon de l'espace des fonctions centrales.

**Proposition 7** (Pey p.2)**.** *Si $|G| = n$, les éléments de $\hat{G}$ sont les morphismes de $G \to \mathbb{U}_n$. En particulier, $\forall g \in G, |\chi(g)| = 1$ et $\chi(g^{-1}) = \bar{\chi(g)}$.*

*Remarque* 8 (Pey p.2). $\hat{G}$ est donc un groupe fini et commutatif.

### 1.2 Cas d'un groupe cyclique

Ici $G$ est un groupe cyclique de cardinal $n$

**Proposition 9** (Pey p.4)**.** *Eléments de $\hat{G}$, l'isomorphisme entre $G$ et son dual*

*Remarque* 10 (Pey p.4). Isomorphisme non canonique

**Corollaire 11.** *Dual de $\mathbb{Z}/n\mathbb{Z}$.*

### 1.3 Cas d'un groupe abélien fini quelconque

Ici $G$ est un groupe abélien fini

**Proposition 12** (Pey p.6)**.** *Prolongement d'un caractère de $H$ à un caractère de $G$.*

**Corollaire 13.** $|G| = |\hat{G}|$

**Définition 14** (Pey p.8)**.** Bidual

**Proposition 15** (Pey p.9)**.** *Isomorphisme entre $G$ et son bidual*

**Théorème 16** (Pey p.8)**.** *Thm de structure des groupes abéliens*

**Application 17.** les groupes abéliens d'ordre 8.

**Corollaire 18** (Pey p.8)**.** *Isomorphisme entre $G$ et son dual*

*Remarque* 19 (Pey p.8). Isomorphisme non canonique

## 2 Algèbre $\mathbb{C}[G]$ et transformée de Fourier discrète

### 2.1 Structure de $\mathbb{C}[G]$

**Définition 20** (Pey p.3)**.** On note $\mathbb{C}[G]$ l'ensemble des fonctions de $G$ dans $\mathbb{C}$. C'est un ev. sur $\mathbb{C}$, muni d'un produit scalaire hermitien : FORMULE +norme

**Proposition 21** (Pey p.3)**.** *Fonction indicatrice, base de $\mathbb{C}[G]$ et dimension*

*Remarque* 22 (Pey p.3). Ecriture d'un élément dans cette base

*Remarque* 23. Pas facile à utiliser en calcul, on verra une meilleure base au paragraphe suivant.

### 2.2 Relations d'orthogonalité

**Lemme 24** (Pey p.9)**.** *Valeur de* $\sum_{g\in G}\chi(g)$.

Rajouter le cas d'un groupe cyclique : p.6 prop 1.10

**Théorème 25** (Pey p.10)**.** *Orthogonalité des caractères*

**Corollaire 26** (Pey p.10)**.** *Base orthonormale de* $\mathbb{C}[G]$.

**Proposition 27** (Pey p.10)**.** *Valeur de* $\sum_{\chi\in\hat{G}}\chi(g)\chi(\bar{h})$.

*Remarque* 28 (Pey p.10). Table de caractères

**Application 29** ( ? ? ?)**.** Déterminant de Vandermonde des racines de l'unité

### 2.3 Transformée de Fourier

Ici $G$ est un groupe abélien fini.

**Définition 30** (Pey p.14)**.** Transformée de Fourier

**Proposition 31** (Pey p.15)**.** *Formule d'inversion*

**Proposition 32** (Pey p.15)**.** *Isomorphisme d'ev*

*Remarque* 33. Parallèle avec la transformée de Fourier sur $L^2$.

**Proposition 34** (Pey p.15)**.** *Formule de Plancherel*

*Remarque* 35. Parallèle avec la transformée de Fourier sur $L^2$.

**Application 36.** Multiplication rapide des polynômes

## 3 Applications sur les corps finis

Soit $p$ un nombre premier et soit $q = p^r$.

### 3.1 Caractères additifs et multiplicatifs

**Définition 37** (Pey p.29)**.** Caractères additifs
Caractères multiplicatifs

*Remarque* 38 (Pey p.29). Les plus simples à déterminer sont les multiplicatifs
// $\mathbb{F}_q^*$ est cyclique. On connait donc le groupe dual de $\mathbb{F}_q^*$.

**Définition 39** (Pey p.30)**.** Application trace

**Proposition 40** (Pey p.30)**.** *c'est une forme k-linéaire non nulle*

**Définition 41** (Pey p.31)**.** Caractère additif canonique

**Proposition 42** (Pey p.31)**.** *Les caractères additifs*

### 3.2 Somme de Gauss : lien entre caractères additifs et multiplicatifs

Les sommes de Gauss servent à démontrer la loi de la réciprocité quadratique.

**Définition 43** (Pey p.32)**.** Somme de Gauss

*Remarque* 44 (Pey p.33). Lien avec la transformée de Fourier

**Proposition 45** (Pey p.33)**.** *Décomposition de* $\chi$

## 4 Alternative au 3 : Applications à la transformée de Fourier discrète et algo FFT

Tout est dans le Peyré