110 STRUCTURE ET DUALITÉ DES GROUPES ABÉLIENS FINIS. APPLICATIONS.

Soit G un groupe abélien fini d'ordre n.

I. Caractères des groupes abéliens finis

I. A. Caractères et liens avec $\mathbb{C}^G$ [Pey04, Ch1, p2]

Définition des caractères, structure de groupe, $\widehat{G \times H} \simeq \hat{G} \times \hat{H}$
Exemples des caractères de $\mathbb{Z}/n\mathbb{Z}$, de $\mathfrak{S}_n$
χ est à valeurs dans $\mathbb{U}_n$, $\chi(g^{-1}) = \chi(g)^{-1}$, constant sur chaque classe de conjugaison
Prolongement d'un caractère de $H < G$ en un caractère de G
$|\hat{G}| = |G|$

Définition 1. Pour $f, g : G \longrightarrow \mathbb{C}$, on définit le produit scalaire :

$$\langle f \mid g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

Orthogonalité des caractères $\rightarrow$ base orthonormée, expression de f sur la base orthonormée

I. B. Théorème de structure des groupes abéliens finis [Col11, §I.2.4, p250–252] [Pey04, §I.2.2, p8]

Bidual
L'application $\iota : G \longrightarrow \hat{\hat{G}}, g \longmapsto (\chi \longmapsto \chi(g))$ est un isomorphisme de groupes.
En particulier $|\hat{\hat{G}}| = |G|$

Définition 2. On appelle exposant de G le plus petit $d \in \mathbb{N}^*$ tel que $g^d = 1$ pour tout $g \in G$.

Théorème 3. [Structure des groupes abéliens finis]
Il existe un unique entier ℓ et une unique suite $d_1 \geq d_2 \geq \cdots \geq d_\ell$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G, $d_{i+1} \mid d_i$ pour tout $i \leq \ell - 1$ et $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

Corollaire : $\hat{G} \simeq G$ (non canoniquement)
Exemple : il y a 6 groupes abéliens d'ordre 600 à isomorphisme près.

II. Transformée de Fourier discrète

II. A. Définitions et premiers résultats [Pey04, §II.3, p44]

Définition 4. [Transformée de Fourier discrète]
Soit $f : G \longrightarrow \mathbb{C}$. On définit le coefficient de Fourier associé à $\chi \in \widehat{G}$ par $c_f(\chi) = \langle f \mid \chi \rangle$ et la transformée de Fourier de f par $\widehat{f} : \chi \in \widehat{G} \longmapsto |G|\, c_f(\overline{\chi}) = \sum_{g \in G} f(g)\chi(g)$.

Proposition 5. [Propriétés de la transformée de Fourier]
- *La transformée de Fourier discrète $f \longmapsto \hat{f}$ est un isomorphisme de $\mathbb{C}^G$ dans $\mathbb{C}^{\hat{G}}$,*
- *Pour $f : G \longrightarrow \mathbb{C}$, on a $f = \sum_{\chi \in \widehat{G}} c_f(\chi)\chi = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi^{-1}$,*
- *formule de Fourier-Plancherel,*
- *$\widehat{f * g} = \hat{f}\hat{g}$.*

Définition 6. On définit $H^\# = \{\chi \in \widehat{G} \mid \forall h \in H, \chi(h) = 1\}$ l'orthogonal de H.

Lemme 7. *$H^\# \simeq \widehat{G/H}$ est de cardinal $|G| / |H|$.*

Proposition 8. [Formule de Poisson discrète]
Pour toute fonction $f : G \longrightarrow \mathbb{C}$, et pour tout $g \in G$, on a :

$$\sum_{h \in H} f(gh) = \frac{|H|}{|G|} \sum_{\chi \in H^\#} \widehat{f}(\overline{\chi})\chi(g)$$

En particulier ($g = 1$), on a $\displaystyle\sum_{h \in H} f(h) = \frac{|H|}{|G|} \sum_{\chi \in H^\#} \widehat{f}(\overline{\chi})$.

II. B. Transformée de Fourier rapide [Per96, §III.2, p65]

Notons $G_a = \mathbb{Z}/N\mathbb{Z}$ où $N = 2^p$ pour $p \in \mathbb{N}^*$. Soit $f \in \mathbb{C}^G$. On veut calculer efficacement $\hat{f}$.
Note : ne considérer que les groupes de la forme G_p reste intéressant, par rapport à la transformée de Fourier discrète en analyse de signaux.
On adopte justement des notations de transformée de Fourier en traitement du signal … c'est équivalent avec la formulation de la TFD sur un groupe. On verra donc f comme une fonction de $\mathbb{C}^N$. On note $\omega_N = \mathrm{e}^{2i\pi/N}$.
Remarque : l'algorithme naïf calcule $\hat{f}$ en $\mathcal{O}(N^2)$.
Idée : on sépare le vecteur f en 2 vecteurs et la TFD de f se sépare en deux sommes sur ses

vecteurs de taille $n/2$.
Définition : si $f \in \mathbb{C}^N$, on définit $f_{\text{paire}}, f_{\text{impaire}} \in \mathbb{C}^{N/2}$ par $f_{\text{paire}}(a) = f(2a)$ et $f_{\text{impaire}}(a) = \ldots$
On a $\hat{f}(k) = \widehat{f_{\text{paire}}}(k) + \omega_N^{-k}\widehat{f_{\text{impaire}}}(k)$
On obtient une complexité en $\mathcal{O}(N\ln(N))$.
Application : calcul du produit de convolution en passant en FOURIER, multiplication rapide de polynômes

III. Caractères des corps finis

[Per96, ChII, p27]

Soit p un nombre premier, $q = p^r$ une puissance de p (avec $r \in \mathbb{N}^*$).
Caractères additifs et multiplicatifs
Exemple : $x \longmapsto \zeta^x$ est un caractère additif de $\mathbb{F}_q$, pour tout ζ. Le symbole de LEGENDRE est un caractère multiplicatif sur $\mathbb{F}_p$
ζ générateur de $\mathbb{F}_q^*$. Permet d'obtenir un isomorphisme $\mathbb{F}_q^* \simeq \widehat{\mathbb{F}_q^*}$
Application trace : forme linéaire sur $\mathbb{F}_q$ (en tant que $\mathbb{F}_p$-espace vectoriel)
Caractère additif canonique, générateur de $\widehat{\mathbb{F}_q}$
Sommes de GAUSS. TDF additive, multiplicative associée ...
On retrouve la loi de réciprocité quadratique en travaillant notamment avec $G\left(\left(\frac{\cdot}{p}\right), \Psi_1\right)$

SPEECH

L'intérêt de la dernière partie est de voir $\mathbb{F}_q$ da manière additive (comme $\mathbb{F}_p$-espace vectoriel) mais aussi de manière multiplicative ($\mathbb{F}_q^*$). Cela permet de combiner deux types de caractères.

QUESTIONS

Q Appliquer le théorème de structure à $(\mathbb{Z}/56\mathbb{Z})^\times$ et $(\mathbb{Z}/35\mathbb{Z})^\times$.

R C'est bien un groupe abélien (groupe fini d'inversibles). On a $\varphi(56) = \varphi(2^3 \times 7) = \varphi(8)\varphi(7) = 4 \times 6 = 24$ donc le groupe est d'ordre 24.
On a $24 = 3 \times 2^3$ et le théorème chinois donne :

$$(\mathbb{Z}/56\mathbb{Z})^\times \simeq (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z})^\times \simeq (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/8\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Puis de même :

$$(\mathbb{Z}/35\mathbb{Z})^\times \simeq (\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Si $p \neq 2$:

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^* = \mathbb{Z}/(p^\alpha - p^{\alpha-1})\mathbb{Z}$$

Et

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \begin{cases} \{1\} & \text{si } \alpha = 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{si } \alpha = 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z} & \text{si } \alpha \geq 3 \end{cases}$$

BIBLIOGRAPHIE

[Col11] P. COLMEZ : *Éléments d'analyse et d'algèbre*. Les éditions de l'École Polytechnique, 2 ème édition, 2011.

[Per96] D. PERRIN : *Cours d'algèbre*. Ellipses, 1996.

[Pey04] G. PEYRÉ : *L'algèbre discrète de la transformée de* FOURIER. Ellipses, 2004.