Leçon 110 : Structure et dualité des groupes abéliens finis, applications.

1/ Structure des groupes abéliens finis :

1) Premières propriétés (Soit G un groupe abélien fini)

Prop 1 : • Le centre d'un groupe abélien est égal au groupe tout entier
• Le groupe dérivé d'un groupe abélien est réduit au neutre
• tout sous groupe d'un groupe abélien est distingué

Application 2 : Les quotients de groupes abéliens sont abéliens

Définition 3 : • Il existe un entier $n \geq 1$ vérifiant : $x^n = e, \forall x \in G$
• On note $\exp(G)$ le plus petit entier vérifiant la propriété précédente

Exemple 4 : L'exposant du groupe $\mathbb{Z}/n\mathbb{Z}$ est n pour tout $n \in \mathbb{N}^*$

Prop 5 : Si $x \in G$ est d'ordre n et que $d \mid n$, ~~il existe~~ $x^{n/d}$ est d'ordre d.

Prop 6 : Si $x, y \in G$ et que $o(x) = p$ et $o(y) = q$ avec $p \wedge q = 1$, alors $o(xy) = pq$

Prop 7 : L'exposant de G est égal au ppcm des ordres de ses éléments

Prop 8 : Il existe un élément de G d'ordre l'exposant de G

Application 9 : Les sous groupes finis du groupe multiplicatif d'un corps $\mathbb{K}$ sont cycliques.

2) Quelques résultats sur $\mathbb{Z}/n\mathbb{Z}$

Définitions 10 : Il existe un unique groupe d'ordre $n \in \mathbb{N}^*$ et monogène. De plus, celui-ci est donné par les définitions équivalentes à isomorphisme près suivantes :

(i) $\langle x \mid x^n \rangle$

(ii) Le quotient $\mathbb{Z}/\langle n \rangle$, noté $\mathbb{Z}/n\mathbb{Z}$

Théorème 11 : (Chinois) Soit $n \in \mathbb{N}^*$ et soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Alors : $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$

Exemple 12 : $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Propriété 13 : Soit $n \in \mathbb{N}^*$ et $d \mid n$.
• Il existe un unique sous groupe d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ et celui-ci est cyclique
• Réciproquement tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre un diviseur de n

Application 14 : Si p premier divise n, il existe un unique p-Sylow dans $\mathbb{Z}/n\mathbb{Z}$. Celui-ci est donné par le théorème chinois

Application 15 : • $\mathbb{Z}/n\mathbb{Z}$ est simple si n est premier

Déf 16 : Soit $n \in \mathbb{N}^*$, on dit qu'un élément de $\mathbb{Z}/n\mathbb{Z}$ est primitif si il est d'ordre n

Remarque 17 : $\bar{1}$ est toujours primitif dans $\mathbb{Z}/n\mathbb{Z}$

Prop 18 : • Les éléments primitifs de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ pour sa structure d'anneau
• Il y a $\varphi(n)$ éléments primitifs dans $\mathbb{Z}/n\mathbb{Z}$, où φ désigne l'indicatrice d'Euler

Exemple 19 : • $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\} \simeq \mathbb{Z}/2\mathbb{Z}$
• Si p est premier, $\varphi(p) = p-1$

Prop 20 : L'application $\begin{cases} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma \mapsto \sigma(\bar{1}) \end{cases}$ est un isomorphisme de groupe. En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Exemple 21 : Si $p \geq 2$, $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est cyclique d'ordre $p-1$

3) Caractères d'un groupe abélien

Soit G un groupe abélien fini

Définition 22 : On appelle caractère de G un élément $\chi \in \mathrm{Hom}(G, \mathbb{C}^*)$

Rem 23 : • Les caractères jouent un rôle similaire à celui des formes linéaires en algèbre linéaire, dans l'étude des groupes abéliens.
• On peut montrer via la théorie des représentations que l'ensemble des caractères de G est exactement l'ensemble des caractères irréductibles des représentations irréductibles de G, qui sont de dimension 1.

Prop 24 : • Soit $\chi \in \mathrm{Hom}(G, \mathbb{C}^*)$, alors $\chi^{-1} = \bar{\chi}$
• Si N est l'exposant de G, les caractères de G sont à valeurs dans $\mu_N(\mathbb{C}^*)$

Théorème 25 : (prolongement des caractères) Soit $H \leq G$ et $\chi_0 \in \mathrm{Hom}(H, \mathbb{C}^*)$ un caractère de H. Alors χ_0 admet un prolongement χ à G :
$\exists \chi \in \mathrm{Hom}(G, \mathbb{C}^*)$ tq $\chi_{|H} = \chi_0$

Exemple 26 : Un prolongement de $\chi_0 : \langle \bar{2} \rangle \subset \mathbb{Z}/6\mathbb{Z} \to \mathbb{C}^*$ défini par $\chi(\bar{2}) = j$ est donné par $\chi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{C}^*$ l'unique caractère vérifiant $\chi_{|\langle \bar{2} \rangle} = \chi_0$ et $\chi(\bar{3}) = -1$. On a alors :

	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
χ	$-j^2$	j	-1	j^2	$-j$	1

Rem 27 : • Ce théorème est l'équivalent du théorème de Hahn-Banach dans le cadre de la dualité dans les groupes abéliens
• La démonstration de ce théorème est constructive, elle donne une méthode pour construire le prolongement

Théorème 28 : (Structure des groupes abéliens finis) Soit G gp abélien fini
Il existe une suite d'entiers $d_1, \dots, d_s$ supérieur à 2 et vérifiant :
• $d_1 | d_2 | \dots | d_s$
• $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$
De plus, la suite $(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G.

Exemple 29 : • $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ et $\mathbb{Z}/18\mathbb{Z}$ ne sont pas isomorphes et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ n'est donc pas cyclique
• D'après le théorème chinois, si p et q sont premiers entre eux, $\mathbb{Z}/pq\mathbb{Z}$ est l'écriture de $\mathbb{Z}/p\mathbb{Z} * \mathbb{Z}/q\mathbb{Z}$ sous la forme ci-dessus

II/ Dualité :

1) Définitions :

Définition 30 : Soit $(G, \cdot)$ un groupe.
On appelle dual de G, l'ensemble $\hat{G} := \mathrm{Hom}(G, \mathbb{C}^\times)$

31 Le bidual de G est le dual du dual de G :
$$\hat{\hat{G}} = \mathrm{Hom}(\hat{G}, \mathbb{C}^\times).$$

Def 31 : pour $(G, \cdot)$ un groupe : on notera :
$\mathbb{C}[G] := \mathcal{F}(G, \mathbb{C})$ fonction de $G \to \mathbb{C}$.

Def 32 : on peut définir le produit (hermitien) suivant : $\langle \cdot, \cdot \rangle : \mathbb{C}[G]^2 \longrightarrow \mathbb{C}$ $\boxed{G \text{ fini}}$
$$(\varphi, \psi) \longmapsto \frac{1}{|G|} \sum \overline{\varphi(g)} \psi(g)$$

2) Propriétés : a) L'ev $\mathbb{C}[G]$

Proposition 33 :
1) $\mathbb{C}[G]$ est un $\mathbb{C}$-ev.
2) $\left\{ g \longmapsto \begin{cases} 1 & \text{si } g = k \\ 0 & \text{sinon} \end{cases} \text{ pour } k \in G \right\}$ Base de $\mathbb{C}[G]$

$[\Rightarrow \mathbb{C}[G]$ de dimension $< \infty$ et $= |G|]$.

3) $\langle \cdot, \cdot \rangle$ est un produit hermitien sur $\mathbb{C}[G]$:
4) $\hat{G} = \mathrm{Hom}(G, \mathbb{C})$ est une BON pour $(\mathbb{C}[G], \langle , \rangle)$

b) Structure du dual, bidual.

Théorème 34 : Soit G gp ; $\ell : G \longrightarrow \hat{\hat{G}}$
$$x \longmapsto [\varphi \mapsto \varphi(x)]$$
est un morphisme de gp.
• si G abélien fini : c'est un isomorphisme.

Rq : 35 : On retrouve, comme pour E K-ev ~~dual~~ la canonicité de l'isomorphisme entre E et son bidual.

Théorème 36 : $G \simeq \hat{G}$

Nécessite le lemme 37 :

Lemme 37 : Soit H, G deux gp abélien :
$$\widehat{G \times H} \longrightarrow \hat{G} \times \hat{H}$$
$$\chi \longmapsto (\chi|_{\bar{G}}, \chi|_{\bar{H}})$$
où $\bar{G} = G \times \{1\}$, $\bar{H} = \{1\} \times H$ isomorphisme.

VI. Transformée de Fourier et Application.

1) Définition et formule d'inversion :

Cadre : $(G, \cdot)$ Abélien fini :

Définition 38 : Soit $\phi \in \mathbb{C}[G]$: La transformée de Fourier est : $\hat{\phi} : \hat{G} \longrightarrow \mathbb{C} \in \mathbb{C}[\hat{G}]$.

$$\chi \longmapsto \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}\, \phi(g).$$

Proposition 39 : Formule d'inversion :

$\forall \phi \in \mathbb{C}[G] : \quad \forall g \in G : \phi(g) = \sum_{\chi \in \hat{G}} \overline{\chi(g)}\, \hat{f}(\chi)$

Rq. 40 : On retrouve la formule d'inversion de $L^1 \cap L^2$ de la TF usuelle (d'analyse).

2) Algèbre $(\mathbb{C}[G], \star, +)$, $(\mathbb{C}[\hat{G}], \cdot, +)$:

Def 41 : Soit G un groupe fini. Sur $\mathbb{C}[G]$, on définit le produit : $\star : \mathbb{C}[G]^2 \to \mathbb{C}[G]$;

$\forall \varphi, \phi \in \mathbb{C}[G], \quad \varphi \star \phi := \sum_{h, g \in G} \phi(h)\, \varphi(h^{-1}g)\, \delta_g.$

• On appelle $\circledast$ produit de convolution.

Proposition 42 : 1) $\star$ est l'unique produit sur $\mathbb{C}[G]$; $\star$ prolonge la multiplication sur G.

2) $(\mathbb{C}[G], \star, +)$ est une $\mathbb{C}$-algèbre.

3) $\mathcal{F} : \mathbb{C}[G] \longrightarrow (\mathbb{C}[\hat{G}], \cdot, +)$
$\phi \longmapsto \hat{\phi}$ est un morphisme d'algèbre bijectif.

3) Des applications : a) incertitude :

Théorème : Inégalité 43 : Principe d'incertitude :

$\forall f \in \mathbb{C}[G] : \quad |G| \leqslant \operatorname{supp}(f) \operatorname{supp}(\hat{f})$.

Rq (44) Rappel le principe d'incertitude d'Eisenberg.

b) Transformée de Fourier discrète et multiplication de polynômes :

Définition (45) : Pour un signal $f : [a ; b] \longrightarrow \mathbb{C}$. On appelle, pour une partition $\sigma = (a_0, \dots, a_{N-1})$ de $[a ; b]$, l'application : $f_! : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{C}$
$k \longmapsto f[k] := f(ak)$.

Théorème (46) : Multiplication de polynômes :

L'algorithme FFT donne un moyen de calculer des polynômes de pdt de degré $N-1$ ($\mathbb{C}[X^N - 1]$) avec un coût de $O(N \log(N))$

Autre applications : Théorème de progression arithmétique Dirichlet.