Théorème de structure des groupes abéliens finis

Leçons : 102, 104, 107, 110

Définition 1

Si G est un groupe abélien fini, son groupe dual est $\hat{G}$, ensemble des morphismes de groupes de G dans $\mathbb{C}^*$, muni de la multiplication. Les éléments de $\hat{G}$ sont appelés caractères linéaires.

On sait que les caractères linéaires sont associés à des représentations de degré 1 de G donc sont des caractères irréductibles. De plus, il y a autant de caractères irréductibles de G que de classes de conjugaison de G, en l'occurrence $|G|$. D'où $\mathrm{Irr}(G) = \hat{G}$.

Définition 2

L'exposant d'un groupe fini G est le plus petit N tel que $\forall g \in G, g^N = e$.

Théorème 3

Si G est un groupe abélien fini, et N_1 est l'exposant de G, il existe $N_2 | \dots | N_r$ tels que

$$G \simeq \mathbb{Z}/N_1\mathbb{Z} \times \dots \mathbb{Z}/N_r\mathbb{Z}.$$

Lemme 4

L'exposant N de g est égal à $\mathrm{ppcm}_{g\in G} o(g)$. *De plus, il existe un élément d'ordre N dans g.*

Démonstration. Il suffit de montrer que si x et y ont pour ordres respectifs n et m, il existe $z \in G$ d'ordre $\mathrm{ppcm}(n,m)$. Une récurrence immédiate fournira le résultat de l'énoncé.

La preuve ne pose pas de difficultés si n et m sont premiers entre eux. Dans le cas général, soit $k = \prod_{p|n, v_p(n)\geqslant v_p(m)} p^{v_p(n)}$ et $l = \prod_{v_p(m)>v_p(n)} p^{v_p(m)}$. Alors k et l n'ont aucun facteur premier commun, donc sont premiers entre eux. De plus, pour tout p premier,

$$v_p(kl) = \begin{cases} v_p(n) & \text{si} \quad v_p(n) \geqslant v_p(m) \\ v_p(m) & \text{si} \quad v_p(m) > v_p(n) \end{cases},$$

donc $kl = \mathrm{ppcm}(n,m)$. Donc comme $k|a$, $x' = x^{n/k}$ est d'ordre k et $y' = y^{m/l}$ est d'ordre l. Ainsi, comme k et l sont premiers entre eux, $x'y'$ est d'ordre $kl = \mathrm{ppcm}(n,m)$.

□

Lemme 5

Si G est un groupe abélien fini, $i : \begin{array}{ccc} G & \longrightarrow & \hat{\hat{G}} \\ g & \longmapsto & \mathrm{ev}_g : \chi \mapsto \chi(g) \end{array}$ est un isomorphisme de groupes.

Démonstration. Comme G et $\hat{\hat{G}}$ ont meme cardinal, il suffit de montrer que i est injectif. Soit $g \in G$ tel que $i(g) = 1$. Alors $\forall \chi \in \hat{G}, \chi(g) = 1$.

On sait que les caractères irréductibles, c'est-à-dire ici les éléments de $\hat{G}$, forment une base orthonormée de l'espace des fonctions centrales de G dans $\mathbb{C}$.

En particulier, $\mathbb{1}_g = \sum_{\chi \in \hat{G}} \langle \mathbb{1}_g, \chi \rangle \chi$ et pour χ caractère,

$$\langle \mathbb{1}_g, \chi \rangle = \frac{1}{|G|} \sum_{h \in G} \overline{\mathbb{1}_g(h)} \chi(h) = \frac{\chi(g)}{|G|} = \frac{1}{|G|}$$

puisque $\chi(g) = 1$.

D'où, en évaluant en l'élément neutre, $\mathbb{1}_g(e) = \sum_{\chi \in \hat{G}} \frac{\chi(e)}{|G|} = 1$ donc $g = e$. □

Démonstration (du théorème)**.** Remarquons tout d'abord qu'en vertu du lemme précédent, G et $\hat{G}$ ont même exposant. En effet si $\forall \chi \in \hat{G}, \chi^M = 1$, alors $\forall g \in G, \forall \chi \in \hat{G}, \chi(g^M) = 1$ d'où $g^M = 1$ donc l'exposant de G divise M. Symétriquement, on obtient que M divise l'exposant de G ce qui donne l'égalité voulue.

Montrons le théorème de structure par récurrence sur $|G|$. Il est évident pour $|G| = 1$, on suppose donc $|G| \geqslant 2$

Notons N_1 l'exposant de G et prenons $\chi_1 \in N_1$ d'ordre N_1. Son image $\chi_1(G)$ est donc un sous-groupe du groupe $\mathbb{U}_{N_1}$ des racines N_1-èmes de l'unité, donc de la forme $\mathbb{U}_l$ où $l | N_1$. Comme χ_1 est d'ordre N_1, on a $l = N_1$. En particulier, on peut se donner $x_1 \in G$ tel que

$$\chi_1(x_1) = \exp\left(\frac{2i\pi}{N_1}\right).$$

L'ordre de x_1 est N_1 et donc $H = \langle x_1 \rangle$ est un sous-groupe cyclique d'ordre N_1 de G.

Montrons que $G \simeq H \times \ker \chi_1$.

- On a $\chi_1(H) = \chi_1(G)$ donc $\chi_{1|H}$ est injectif pour des raisons de cardinal. En d'autres termes, $H \cap \ker \chi_1 = \{e\}$.
- De plus, si $g \in G$, il existe $h \in H$ tel que $\chi_1(g) = \chi_1(h)$ donc $gh^{-1} \in \ker \chi_1$ ce qui assure que $G = H \ker \chi_1$.

Selon le théorème de factorisation en produit direct, on a $G \simeq H \times \ker \chi_1$.

Enfin, il est clair que l'exposant N_2 de $\ker \chi_1$ divise celui de G et par hypothèse de récurrence $\ker \chi_1 \simeq \mathbb{Z}/N_2\mathbb{Z} \times \ldots \mathbb{Z}/N_r\mathbb{Z}$ donc comme $H \simeq \mathbb{Z}/N_1\mathbb{Z}$, on a le résultat par récurrence. □

Référence : Pierre COLMEZ (2011). *Eléments d'analyse et d'algèbre (et de théorie des nombres)*. Ecole Polytechnique, p. 252.