Théorème de structure des groupes abéliens finis

Notions utilisées : Groupes finis et cycliques, Racines de l'unité, ordre et exposant d'un groupe, représentations de groupes

Motivations :

Définition 1. *Soit G un groupe fini. On appelle exposant de G l'entier $N := \max\{o(g), g \in G\}$.*

Prérequis : si x et y d'ordre premiers entre eux alors l'ordre du produit est le produit des ordres.

Théorème 2. *Soit G un groupe abélien fini. Alors il existe un unique $r \in \mathbb{N}$ et un unique $r-$uplet $(d_1, \ldots, d_r)$ tel que $d_i | d_{i+1}$ et d_r soit l'exposant de G et que $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$.*

Lemme 3. *L'exposant N de G est le plus petit entier vérifiant $g^N = 1$ pour tout $g \in G$.*

Preuve. Idée : si pour tout $x \in G$ on arrive à prouver qu'il existe un élément y d'ordre $\alpha := ppcm(o(x), N)$, la preuve est finie. En effet, on remarque d'abord que $\alpha \geq N$ (c'est un *multiple* de N) et que α étant l'ordre d'un élément de G, par le théorème de Lagrange on a $\alpha \leq N$. Donc cet élément y convient.
Pour construire cet élément d'ordre $ppcm(o(x), N)$, l'idée est de prendre comme lors de la construction du ppcm de deux nombres le maximum des valuations $p-$adiques :
Si $x, y \in G$ d'ordres respectifs a et b, on considère $\mathscr{P}_a$ (resp. $\mathscr{P}_b$) l'ensemble des p premiers vérifiant $v_p(a) \neq 0$ et $v_p(a) \geq v_p(b)$ (resp. $v_p(b) \neq 0$ et $v_p(a) < v_p(b)$). On pose $k := \prod_{\mathscr{P}_1} p^{v_p(a)}$ et $l := \prod_{\mathscr{P}_1} p^{v_p(a)}$.
Par construction k et l sont premiers entre eux car les $\mathscr{P}_i$ sont disjoints, et donc $kl = ppcm(a, b)$. Or $k|a$ donc $x^{a/k}$ est d'ordre exactement k et $y^{b/l}$ d'ordre exactement l, qui sont premiers entre eux, d'où $x^{a/k}y^{b/l}$ d'ordre $kl = ppcm(a, b)$. □

Lemme 4. *Si G est abélien fini alors G et $\widehat{G}$ ont le même exposant. ($\widehat{G}$ = caractères de G vers $\mathbb{C}$).*

Preuve. On note $N(G) = N$ l'exposant de G. Pour $\chi \in \widehat{G}$, on a pour tout $x \in G$:

$$\chi^N(x) = \chi(x^N) = \chi(1) = 1$$

donc l'exposant de $\widehat{G}$ divise N. Or $\widehat{\widehat{G}} \simeq G$ donc $N(G) = N(\widehat{\widehat{G}}) \leq N(\widehat{G}) \leq N(G)$ d'où l'égalité. □

Preuve. Soit N l'exposant de G.

Etape 1 : Notre premier objectif est de trouver la partie en $\mathbb{Z}/N\mathbb{Z}$ de la décomposition. On espère qu'en chemin, on pourra lui trouver un supplémentaire "naturel" K tel que $G \simeq \mathbb{Z}/N\mathbb{Z} \times K$...

Etape 1.a : Utiliser les lemmes pour trouver un $\chi_1 \in \widehat{G}$ d'ordre exactement N.

On sait que l'exposant de $\widehat{G}$ est le même exposant N que G. En particulier on constate que tous les caractères χ de $\widehat{G}$ vérifient $\chi^N = 1$: ce sont des racines N-ièmres de l'unité. On déduit de cela que $\forall x \in G$, x est une racine N-ième de l'unité, et donc puisque $\chi : G \to \mathbb{C}$ est un morphisme, on en déduit que $\chi(G) \leq \mu_N(\mathbb{C})$.

Soit donc χ_1 d'ordre N dans $\widehat{G}$ (légitime car c'est le max des ordres de $\widehat{G}$, donc il est atteint). On a χ_1 racine N-ième de l'unité, en particulier χ_1 est un élément du groupe $\chi_1(G)$ qui par la remarque précédente est un sous-groupe cyclique inclus dans μ_N. Il est d'ordre N comme μ_N donc $\chi_1(G) = \mu_N$. Soit x_1 un générateur, c'est à dire $x_1 \in G$ tel que $\chi(x_1) = e^{2i\pi/n}$.

Etape 1.b : Exhibons nos candidats pour la somme directe (produit cartésien) $G = H \oplus K$.

On constate, par le lemme 3, que l'ordre de x divise N ($x^N = 1$). On en déduit que x est d'ordre N (sinon, la relation $\chi(x_1) = e^{2i\pi/n}$ entraînerait que χ serait d'rdre strictement plus petit que N). Nos candidats pour la récurrence sont donc $H := \langle x_1 \rangle \simeq \mathbb{Z}/N\mathbb{Z}$ (x_1 est d'ordre N dans G) ainsi que $K = \mathrm{Ker}(\chi_1)$.

Etape 2 : Maintenant que l'on a nos candidats, on peut procéder par récurrence en montrant que $G = \langle x_1 \rangle \times \mathrm{Ker}(\chi_1)$. On va tout simplement vérifier que $G = H \times K$ par caractérisation du produit direct.

- Montrons $G = HK$. On constate pour cela que χ_1 est bijectif. En effet, il est surjectif ($e^{2ik\pi/n} = \chi_1(x_1^k)$) et par égalité $N = N$ des cardinaux des ensembles de départ et d'arrivée il est bien bijectif. On note $\alpha : \mu_N \subset \mathbb{C} \to \chi_1(H) = \langle x_1 \rangle = H$ son inverse.

  Soit donc $x \in G$. On pose $a := \alpha(\chi_1(x_1)) \in H$. On a $b = a^{-1}x$ qui est dans K car $\chi_1(b) = \chi_1(a^{-1})\chi_1(x) = \chi_1(a)^{-1}\chi_1(x) = \chi_1(x)^{-1}\chi_1(x) = 1$ et donc b est bien dans le noyau. Ainsi, $G = HK$. (notation ensembliste)
- Enfin, si $x \in H \cap K$ alors d'une part $x = x_1^d$ et d'autre part $\chi(x) = 1$ et donc puisque χ_1 est bijectif **sur** H_1, en particulier il est injectif **sur** H_1 et donc $x = 1$.

Finalement, par hypothèse de récurrence, on a $K \simeq \prod \mathbb{Z}/d_i\mathbb{Z}$ et le théorème est ainsi prouvé. □

Références

[1] Colmez Pierre, Eléments d'analyse et d'algèbre