# Structure des groupes abéliens finis

Colas Bardavid

Ce développement a pour but de prouver que les groupes abéliens finis sont des produits directs de quotients cycliques de $\mathbb{Z}$.

## 1 Un lemme intéressant quant à l'obtention d'un supplémentaire

Un groupe abélien est un $\mathbb{Z}$-module. On peut donc parler à ce titre de somme directe, de supplémentaire pour les sous-groupes. Cependant, on n'a pas tous les résultats de la théorie des espaces vectoriels, notamment quant à l'existence de supplémentaires.

Voilà donc un cas particulier.

**Lemme 1** *Soient $G$ un groupe abélien et $H$ un sous-groupe de $G$. On suppose qu'il existe $\varphi \in Hom\,(G, K)$ tel que $\varphi$ induise un isomorphisme entre $H$ et $\varphi(G)$. Alors, $H \oplus ker\,\varphi = G$.*

*Démonstration :* Soit $x \in G$. Le but est de prouver qu'il existe un unique $x' \in H$ tel que $x - x' \in ker\,\varphi$, *ie* $\varphi(x) = \varphi(x')$. C'est le cas puisque $\varphi : H \to \varphi(G)$ est bijectif. ■

## 2 Exposant d'un groupe abélien

**Définition 1** *Soit $G$ un groupe fini. On appelle* exposant de $G$ *le $ppcm$ des ordres de $G$.*

On va montrer qu'il existe que si $G$ est abélien, il existe un élément dont l'ordre est l'exposant de $G$.

**Lemme 2** *Soit $(G, .)$ un groupe abélien fini. Si $a$ et $b$ sont deux éléments de $G$ d'ordre $n$ et $m$ premiers entre eux, alors $ab$ est d'ordre $nm$.*

*Démonstration :* On a d'abord $(ab)^{nm} = (a^n)^m(b^m)^n = e$. Donc $\omega(ab) \mid (nm)$. Par ailleurs, si $(ab)^p = e$, alors $x = a^p = b^{-p}$ appartient à $< a >$ et à $< b >$, groupes de cardinal respectif $n$ et $m$. Donc l'ordre de $x$, divisant $n$ et $m$, vaut 1. Donc $a^p = e$, et donc $n \mid p$. De même, $m \mid p$, et ainsi, $(nm) \mid p$. ■

**Proposition 1** *Soit $(G, .)$ un groupe abélien fini. Alors un élément de $G$ est d'ordre l'exposant de $G$.*

*Démonstration :* Notons $n = \prod_{i \leq n} p_i^{\alpha_i}$, où les $p_i$ sont distincts et premiers. Alors, par définition de $n$, il existe un élement $x_i$ de $G$ d'ordre $mp_i^{\alpha_i}$. On vérifie alors que $y_i = x^m$ est d'ordre $p_i^{\alpha_i}$. Enfin, d'après le lemme précédent, on sait que $\prod_{i \leq n} y_i$ est d'ordre $n$. ■

## 3 Caractères d'un groupe abélien

**Définition 2** *Soit $G$ un groupe abélien ; on appelle* caractère de $G$ *tout morphisme de $G$ dans le groupe $(\mathbb{U}, \times)$ des complexes de module 1.*

*On note $\widehat{G}$ et on appelle* groupe dual de $G$ *l'ensemble des caractères de $G$, muni de la multiplication des fonctions à valeurs dans $\mathbb{U}$.*

**Lemme 3 (Prolongement des caractères)** *Soient $(G, +)$ un groupe abélien fini, $H$ un sous-groupe de $G$ et $\varphi \in \widehat{H}$. Alors, il existe un élément de $\widehat{G}$ prolongeant $\varphi$.*

*Démonstration :* Si $H = G$, c'est fini. Sinon, on montre que l'on peut prolonger $\varphi$ à un sous-groupe de $G$ contenant strictement $H$ ; en répétant un nombre fini de fois ce processus, on obtient le résultat escompté. Soit donc $x \in G \backslash H$. Soit $K = \mathbb{Z}x + H$ le groupe engendré par $x$ et $H$.

On considère alors $E = \{k \in \mathbb{Z} \ / \ kx \in H\}$, qui un sous-groupe non-nul de $\mathbb{Z}$ ; en effet, $\omega(x)$ en est un élément.

On écrit donc $E = m\mathbb{Z}$, où $m \in \mathbb{N}^*$. Soit alors $\gamma \in \mathbb{U} \,/\, \gamma^m = \varphi(mx)$. Vérifions que $\psi \ : \begin{array}{c} K \to \mathbb{U} \\ kx + h \mapsto \gamma^k \varphi(h) \end{array}$ définit un caractère de $K$. Si $kx + h = k'x + h'$, alors on a $(k - k') = tm$ et $tmx = h' - h$. Et,

$$\frac{\gamma^k \varphi(h)}{\gamma^{k'} \varphi(h')} = \gamma^{k-k'} \varphi(h - h') = \gamma^{tm} \varphi(h - h') = \varphi(mx)^t \varphi(h - h') = \varphi(tmx - (h' - h)) = 1.$$

Il est ensuite clair que $\psi$ est à valeurs dans $\mathbb{U}$, est un morphisme et prolonge $\varphi$. ■

**Lemme 4** *Soient $(G, +)$ un groupe abélien fini, $x$ d'ordre l'exposant de $G$. Alors, il existe $H$ un sous-groupe de $G$ tel que $G = H \oplus \mathbb{Z}x$.*

*Démonstration :* Notons $n$ l'ordre de $x$. Soit $\varphi \in \widehat{(\mathbb{Z}x)}$ défini par $\varphi(x) = e^{i\pi/n}$ : c'est un isomorphisme. On prolonge $\varphi$ en $\psi \in \widehat{G}$. On a $\psi(nx) = 1 = \psi(x)^n$ par définition de $n$. Donc $\psi$ est à valeurs dans $\mathbb{U}_n = \psi(\mathbb{Z}x)$. On est alors dans le cadre du lemme 1.

On a donc $G = \mathbb{Z}x \oplus ker\, \psi$. ■

# 4 Structure des groupes abéliens finis

**Théorème 1 (Structure des groupes abéliens finis)** *Soit $G$ un groupe abélien fini non-nul. Alors, il existe $(n_i)_{i \leq n} \in (\mathbb{N}^* \setminus \{1\})^p$ tels que*

$$G \simeq \prod_{i}^{p} \mathbb{Z}/_{n_i\mathbb{Z}}.$$

*Démonstration :* On démontre le résultat par récurrence sur $n = |G|$.

$\underline{n = 2}$ : Alors, $G \simeq \mathbb{Z}/_{2\mathbb{Z}}$.

$\underline{HR_n \Longrightarrow HR_{n+1}}$ : Notons $d \geq 2$ l'exposant de $G$ et $x$ un élément d'ordre $d$. D'après le lemme précéde, soit $H$ un sous-groupe de $G$ tel que $G = \mathbb{Z}x \oplus H$. Alors, $\varphi \ : \begin{array}{c} G \to \mathbb{Z}/_{d\mathbb{Z}} \times H \\ px + h \mapsto (\chi_d(p), h) \end{array}$ est un isomorphisme de groupes. Comme $|H| \leq |G| - 1$, l'hypothèse de récurrence permet de conclure. ■