21. Structure des groupes abéliens finis

[Col11, §I.2.4, p250–252]

ÉNONCÉ

Soit G un groupe abélien fini.

DÉFINITION. On appelle exposant de G le PPCM des ordres de ses éléments.

THÉORÈME. [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 $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$.

DÉVELOPPEMENT

La preuve nécessite plusieurs résultats préliminaires :

1. L'application $\iota : G \longrightarrow \hat{\hat{G}}, g \longmapsto (\chi \longmapsto \chi(g))$ est un isomorphisme de groupes.
   Pour $g \in G$, on vérifie que $\iota(g) \in \hat{\hat{G}}$. En effet pour $g \in G$, $\chi_1, \chi_2 \in \hat{G}$:
   $$\iota(g)(\chi_{\text{triv}}) = 1 \qquad \iota(g)(\chi_1\chi_2) = (\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \iota(g)(\chi_1)\iota(g)(\chi_2)$$
   Puis ι est bien un morphisme de groupes puisque pour $g, h \in G$, $\chi \in \hat{G}$:
   $$\iota(e)(\chi) = \chi(e) = 1 \qquad \iota(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = \iota(g)(\chi)\iota(h)(\chi)$$
   On sait que $G, \hat{G}$ puis $\hat{\hat{G}}$ ont même cardinal, donc il suffit de montrer l'injectivité de ι. Soit donc $g \in G$ tel que $\iota(g) = 1$. Comme les caractères de $\hat{G}$ forment une base de l'ensemble des fonctions centrales de G dans $\mathbb{C}$[1], écrivons :
   $$\mathbb{1}_g = \sum_{\chi \in \hat{G}} \langle \mathbb{1}_g \mid \chi \rangle \chi \quad \text{avec} \quad \langle \mathbb{1}_g \mid \chi \rangle = \frac{1}{|G|} \sum_{h \in G} \mathbb{1}_g(h)\overline{\chi(h)} = \frac{\overline{\chi(g)}}{|G|} = \frac{1}{|G|}$$
   Puis en évaluant en e, il vient $\mathbb{1}_g(e) = \sum_{\chi \in \hat{G}} \frac{1}{|G|}\chi(1) = \sum_{\chi \in \hat{G}} \frac{1}{|G|} = 1$, ou encore $g = e$.

2. Il existe $g \in G$ tel que g est d'ordre égal à l'exposant de G.
   En effet, vérifions que l'ensemble des ordres des éléments de G est stable par PPCM, puisqu'alors en un nombre fini d'itérations (G est fini), on trouvera un élément d'ordre l'exposant de G.
   Soient donc $x, y \in G$ d'ordre a et b. Montrons que l'on peut trouver un élément d'ordre $a \vee b$.
   Ecrivons $k = \prod_{p \in \mathcal{P} \mid v_p(a) > v_p(b)} p^{v_p(a)}$ et $\ell = \prod_{p \in \mathcal{P} \mid v_p(a) \leq v_p(b)} p^{v_p(b)}$. Alors $a \vee b = k\ell$ et k et ℓ sont premiers entre eux.
   Posons alors $x' = x^{a/k}$ et $y' = y^{b/\ell}$ qui sont d'ordre k et ℓ respectivement. Alors $x'y'$ est d'ordre $k\ell = a \vee b$.

3. G et $\hat{G}$ ont même exposant.
   Soit en effet H un groupe commutatif fini, d'exposant d. Alors si $\chi \in \hat{H}$, on a $\chi^d(h) = \chi(d)^h = \chi(d^h) = \chi(1) = 1$ pour tout $h \in H$ donc $\chi^d = 1$. Ainsi l'exposant de $\hat{H}$ est plus petit que celui de H. Appliquant à $H = G$ puis à $H = \hat{G}$, on a $d(\hat{\hat{G}}) \leq d(\hat{G}) \leq d(G)$ et puisque $G \simeq \hat{\hat{G}}$, on a en fait égalité.

4. Passons maintenant à la preuve du théorème. On procède par récurrence sur $|G|$:
   - Avec la convention $\prod_{i=1}^{0} = \{e\}$, le résultat est évident si $|G| = 1$ en prenant $\ell = 0$.
   - Supposons donc $|G| > 1$ et le résultat vrai pour tout groupe H tel que $|H| < |G|$.
     Soit d l'exposant de G. Pour $\chi \in \hat{G}$ et $g \in G$, $\chi(g)$ est une racine d-ième de l'unité et on sait que d est aussi l'exposant de $\hat{G}$, donc on peut trouver $\chi_1 \in \hat{G}$ tel que χ_1 est d'ordre d. $\chi_1(G)$ est alors un sous-groupe de $\mathbb{U}_d$.
     Par ailleurs, si $|\chi_1(G)| = d' < d$, alors $\chi_1^{d'}(g) = 1$ pour tout $g \in G$, donc $o(\chi_1) \leq d' < d$, ce qui est faux.
     Ainsi $\chi_1(G) = \mathbb{U}_d$. Soit alors $g_1 \in G$ tel que $\chi_1(g_1) = \mathrm{e}^{\frac{2i\pi}{d}}$. On sait alors que g_1 est d'ordre d (on savait déjà que $o(g_1) \mid d$) et ainsi $H_1 = \langle g_1 \rangle$ est cyclique d'ordre d, donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$.
     Vérifions que $G = G_1 \times H_1$ où $G_1 = \ker(\chi_1)$:
     - d'une part on a un isomorphisme $\chi_1(H_1) \simeq \mathbb{U}_d$, ce qui assure que $H_1 \cap \ker(\chi_1) = \{e\}$,
     - d'autre part si $g \in G$, on peut choisir $h \in H_1$ tel que $\chi_1(h) = \chi_1(g)$ et alors $gh^{-1} \in \ker(\chi_1) = G_1$, d'où $g = (gh^{-1})h \in G_1H_1$. Ainsi $G = G_1H_1$.

     On applique alors l'hypothèse de récurrence à G_1 de cardinal strictement inférieur à celui de G. On obtient que $G \simeq \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$ pour un ℓ et $d_2 \geq \cdots \geq d_\ell$. Il suffit de vérifier que $d = d_1 \mid d_2$, ou encore que d_2 l'exposant de G_1 divise d_1 l'exposant de G ce qui est bien le cas.
     D'où l'hypothèse de récurrence au rang $|G|$.

On conclut par principe de récurrence.

COMMENTAIRES

Le développement est un peu long. On peut admettre le premier point dans le plan.

Attention on ne fait que la preuve d'existence dans ce développement. On pourra trouver une preuve de l'unicité dans [Rom17, §1.9, p29–30].

1. en fait l'ensemble des fonctions de G dans $\mathbb{C}$ puisque G est abélien