Structure des groupes abéliens finis

Proposition 1. *L'application suivante est un isomorphisme de groupe :*

$$\iota : \left| \begin{array}{ccc} G & \longrightarrow & \widehat{\widehat{G}} \\ g & \longmapsto & (\chi \mapsto \chi(g)) \end{array} \right.$$

Démonstration.
Pour $g \in G$, vérifions que $\iota(g) \in \widehat{\widehat{G}}$. En effet, pour $g \in G$, et $\chi_1, \chi_2 \in \widehat{G}$, on a :

$$\iota(g)(\chi_{triv}) = 1 \quad \text{et} \quad \iota(g)(\chi_1\chi_2) = (\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) = \iota(g)(\chi_1)\iota(g)(\chi_1)$$

Puis ι est bien un morphisme de groupe, puisque pour $g, h \in G$ et $\chi \in \widehat{G}$ on a :

$$\iota(e)(\chi) = \chi(e) = 1 \quad \text{et} \quad \iota(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = \iota(g)(\chi)\iota(h)(\chi)$$

Puisque G est abélien, G, $\widehat{G}$ et $\widehat{\widehat{G}}$ 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 $\widehat{G}$ forment une base des fonctions centrales de G dans $\mathbb{C}^\star$, écrivons :

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

Puis, en évaluant en e, il vient que $\mathbb{1}_g(e) = \sum_{\chi \in \widehat{G}} \frac{1}{|G|} \mathbb{1}_g \chi(e) = 1$, donc que $g = e$, d'où l'injectivité de ι. Ainsi, ι est un isomorphisme. $\square$

Lemme 2. *Il existe un élément de G d'ordre l'exposant de G.*

Démonstration.
Vérifions que l'ensemble des ordres des éléments de G est stable par ppcm, puisqu'alors on trouvera un élément d'ordre l'exposant de G en un nombre fini d'itérations. Soient donc $x, y \in G$ d'ordres a et b. Montrons que l'on peut trouver un élément d'ordre $\text{ppcm}(a, b)$. Écrivons :

$$k = \prod_{\substack{p \in \mathcal{P} \\ v_p(a) > v_p(b)}} p^{v_p(a)} \qquad \text{et} \qquad \ell = \prod_{\substack{p \in \mathcal{P} \\ v_p(a) \leqslant v_p(b)}} p^{v_p(b)}$$

Alors $\text{ppcm}(a, b) = k\ell$, et k et ℓ sont premiers entre eux. Posons alors $x' = x^{\frac{a}{k}}$ et $y' = y^{\frac{b}{\ell}}$ qui sont d'ordre k et ℓ respectivement. Alors $x'y'$ est d'ordre $k\ell = \text{ppcm}(a, b)$. $\square$

Proposition 3. *G et $\widehat{G}$ ont même exposant.*

Démonstration.
Soit H un groupe commutatif fini d'exposant d. Si $\chi \in \widehat{H}$, on a alors, pour tout $h \in H$:

$$\chi^d(h) = \chi(h)^d = \chi(h^d) = \chi(e) = 1 \quad \text{donc} \quad \chi^d = 1$$

Ainsi l'exposant de $\widehat{H}$ est plus petit que celui de H. En appliquant à $H = G$ puis à $H = \widehat{G}$, on a $d(\widehat{\widehat{G}}) \leqslant d(\widehat{G}) \leqslant d(G)$. Mais on a en fait égalité puisque $G \cong \widehat{\widehat{G}}$. $\square$

Théorème 4. *Il existe un unique entier ℓ et une unique suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2 tels que d_1 est l'exposant de G et :*

$$G \cong \prod_{i=1}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$$

Démonstration.
On va raisonner 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 $\chi \in \widehat{G}$ et $g \in G$, $\chi(g)$ est une racine d-ième de l'unité. De plus, on sait que d est l'exposant de $\widehat{G}$, on peut donc trouver $\chi_1 \in \widehat{G}$ tel que χ_1 est d'ordre d. $\chi_1(G)$ est alors un sous-groupe de μ_d, le groupe des racines d-ièmes de l'unité. Par ailleurs, si $|\chi_1(G)| = d' < d$, alors $\chi_1^{d'}(g) = 1$ pour tout $g \in G$, donc χ_1 serait d'ordre $d' < d$, ce qui est faux. Ainsi $\chi_1(G) = \mu_d$.
Soit alors $g_1 \in G$ tel que $\chi_1(g_1) = e^{\frac{2i\pi}{d}}$. On sait alors que g_1 est d'ordre d, et ainsi $H_1 = \langle g_1 \rangle$ est cyclique d'ordre d, donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$.
Vérifions que $G \cong H_1 \times G_1$, où $G_1 = \mathrm{Ker}(\chi_1)$:

— D'une part, on a $\chi(H_1) = \mu_d$, ce qui assure que $\mathrm{Ker}(\chi_1) \cap H_1 = \{e\}$.

— D'autre part, si $g \in G$, il existe $h \in H_1$ tel que $\chi_1(h) = \chi_1(g)$, et alors $gh^{-1} \in \mathrm{Ker}(\chi_1)$, d'où $g = (gh^{-1})h \in G_1H_1$. Ainsi, $G = G_1H_1$.

On applique alors l'hypothèse de récurrence à $\mathrm{Ker}(\chi_1)$ de cardinal strictement inférieur à celui de G. On obtient que $G_1 \cong \prod_{i=2}^{\ell} \mathbb{Z}/d_i\mathbb{Z}$ pour un entier ℓ et une suite $d_\ell | \cdots | d_2 | d_1$ d'entiers supérieurs à 2. Il suffit que vérifier que $d_2 | d_1 = d$. Or d_2 est l'exposant de G_1 et divise d l'exposant de G. $\square$

Références

[Col09] P. Colmez. *Éléments d'analyse et d'algèbre.* Les éditions de l'École Polytechnique