Le théorème de structure des groupes abéliens finis.

On considère un groupe abélien fini G et on rappelle que son dual est le groupe des caractères $\widehat{G} = \mathrm{Hom}(V, \mathbf{C}^\times)$ muni de la multiplication sur les valeurs. On rappelle aussi que la terminologie *caractère* est un abus dans ce contexte.

Quelques prérequis.

Lemme. *Un groupe est fini si et seulement si toutes ses représentations irréductibles sont de dimension 1, c'est à dire que son groupe des caractères est égal à l'ensemble de ses caractères irréductibles.*

Lemme. *On a l'égalité des cardinaux* $|G| = |\widehat{G}|$.

Preuve. Il suffit d'écrire la suite d'égalités :

$$|G| = |\operatorname{Conj} G| = |\operatorname{Irr} G| = |\widehat{G}|.$$

On peut aussi utiliser le lemme de prolongement des caractères de G. Peyré. □

Lemme. *L'application de bidualité* $\mathrm{ev} : G \to \widehat{\widehat{G}}$ *défini par* $\mathrm{ev}(x)(\chi) = \chi(x)$ *est un isomorphisme de groupes.*

Preuve. On vérifie que ev est un morphisme et on montre sa bijectivité. On déduit du lemme précédent que $|G| = |\widehat{\widehat{G}}|$ et on montre l'injectivité de ev. Il suffit de prendre $g \in \operatorname{Ker} \mathrm{ev}$ et d'écrire :

$$\delta_g = \sum_{\chi \in \widehat{G}} \langle \delta_g, \chi \rangle \chi = \ldots = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi$$

de sorte que $\delta_g(e) = 1$ et $g = e$. □

Lemme. *Les groupes G et $\widehat{G}$ ont même exposant.*

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

$$\chi^{N(G)}(x) = \chi(x)^{N(G)} = \chi(x^{N(G)}) = \chi(1) = 1$$

donc $\chi^{N(G)} = 1$ et l'exposant de $\widehat{H}$ divise celui de H. En faisant pareil avec $\widehat{G}$ et $\widehat{\widehat{G}}$ et puisque $G \simeq \widehat{\widehat{G}}$, on a le résultat. □

Ce qu'on va montrer.

Théorème. *Soit G un groupe abélien fini. Il existe $r \in \mathbf{N}$ et des entiers $n_r | \ldots | n_1$ tels que*

$$G \simeq (\mathbf{Z}/n_1\mathbf{Z}) \times \ldots (\mathbf{Z}/n_r\mathbf{Z}).$$

Preuve. On procède par récurrence sur $|G|$. C'est bon avec $r = 0$ pour $|G| = 1$ et si $|G| > 1$ alors notons $n = n_1$ l'exposant de G.

(1) Pour tout $\chi \in \widehat{G}$ et tout $x \in G$, $\chi(x)$ est une racine n-ème de l'unité. De plus, comme n est aussi l'ordre de $\widehat{G}$, il existe[1] $\chi_1 \in \widehat{G}$ d'ordre n. Finalement, $\chi_1(G) \subset \mathbf{U}_n$ et il existe $x_1 \in G$ tel que

$$\chi_1(x_1) = e^{2i\pi/n}.$$

L'ordre de x_1 est aussi n et le sous-groupe de $H_1 \subset G$ engendré par x_1 est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

(2) On va montrer que $G \simeq H_1 \times G_1$ où $G_1 = \operatorname{Ker} \chi_1$. On commence par voir que χ_1 induit un isomorphisme $H_1 \to \mathbf{U}_n$. En effet, c'est un morphisme surjectif entre deux groupes de même cardinal . Son inverse sera noté

$$\alpha : \mathbf{U}_n \to H_1.$$

(3) Soit $x \in G$. On définit :

$$a = \alpha(\chi_1(x)) \quad \text{et} \quad b = a^{-1}x.$$

En particulier

$$\chi_1(b) = \chi_1(a)^{-1}\chi_1(x) = 1$$

donc $b \in G_1$ et tout élément de $x \in G$ peut s'écrire $x = ab$ où $a \in H_1$ et $b = G_1$.

(4) Par injectivité de χ_1, il est clair que $H_1 \cap G_1 = \{1\}$ et on peut conclure

$$G \simeq H_1 \times G_1.$$

(5) Puisque l'exposant d'un sous-groupe divise celui du groupe et que G_1 est isomorphe à un sous-groupe de G, la relation de divisibilité à lieu et on peut terminer la récurrence.

□

Références.

P. Colmez, *Éléments d'analyse et d'algèbre (et de théorie des nombres)*
G. Peyré, *L'Algèbre discrète de la Transformée de Fourier*

104 Groupes finis. Exemples et applications.
107 Représentations et caractères d'un groupe fini sur un C-espace vectoriel. Exemples.
110 Caractères d'un groupe abélien fini et transformée de Fourier discrète. Applications.

1. Dans un groupe **abélien** fini, il existe un élément d'ordre l'exposant du groupe. Pour le voir il suffit de montrer que si a est d'ordre m et b est d'ordre n alors il existe un élément d'ordre $m \vee n$. Lorsque $m \wedge n = 1$, ab convient. Dans le cas contraire, on considère $m' \wedge n' = 1$ tels que $m'|m$, $n'|n$ et $m'n' = m \vee n$. Ensuite on voit que $a^{\frac{m}{m'}} b^{\frac{n}{n'}}$ est d'ordre $m'n'$.