Théorème de structure des groupes abéliens finis

Références : Colmez, *Éléments d'analyse et d'algèbre (et de théorie des nombres)*, p 250-252

On rappelle que l'exposant d'un groupe G est le plus petit entier n tel que pour tout $g \in G$, $g^n = e$. Comme pour tous $g, h \in G$, gh est un élément d'ordre $\mathrm{ppcm}(o(g), o(h))$ **car G est abélien**, l'exposant est donc le ppcm des ordres des éléments du groupe, et aussi le plus grand des ordres des éléments du groupe.

Théorème.

Si G est un groupe abélien fini, alors il existe $r \in \mathbb{N}$ et des entiers N_1, ..., N_r, où N_1 est l'exposant de G et $N_{i+1}|N_i$ tels que

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

Comme G est un groupe abélien fini, les classes de conjugaisons n'ont qu'un élément. On a donc $n = |G|$ représentations irréductibles de degré 1 par Burnside.
Puis on remarque que les caractères irréductibles sont des morphismes. Ce sont donc des éléments de $\widehat{G}$, le groupe abélien des morphismes de G dans $\mathbb{C}^*$.
Réciproquement, tout élément de $\widehat{G}$ fournit une représentation irréductible, donc un caractère irréductible.
$\widehat{G}$ est donc le groupe des caractères irréductibles de G.

Lemme.

On pose l'application

$$i : \begin{array}{ccc} G & \to & \widehat{\widehat{G}} \\ g & \mapsto & (\chi \mapsto \chi(g)) \end{array},$$

alors i est un isomorphisme de groupes.

Démonstration. i est bien un morphisme de groupes car les caractères sont des morphismes.
En effet,

$$i(gh)(\chi) = \chi(gh) = \chi(g)\chi(h) = i(g)(\chi)i(h)(\chi).$$

On a vu que $\widehat{G}$ est l'ensemble des caractères irréductibles. Il est donc de même cardinal que G. On a $\left|\widehat{G}\right| = \left|\widehat{\widehat{G}}\right|$, en appliquant le même raisonnement aux éléments de $\widehat{\widehat{G}}$, qui sont les caractères irréductibles sur $\widehat{G}$ **car $\widehat{G}$ est abélien**.
D'où $|G| = \left|\widehat{\widehat{G}}\right|$.
Il suffit de montrer que i est injectif.

Soit $g \in G$ tel que $i(g)(\chi) = 1 = i(e)(\chi)$. Alors $\forall \chi \in \widehat{G}$, $\chi(g) = \chi(e) = 1$.
On décompose $\mathbb{1}_{\{g\}}$ dans la base des caractères.

$$\begin{aligned}
\mathbb{1}_{\{g\}} &= \sum_{\chi \in \widehat{G}} \langle \mathbb{1}_{\{g\}}, \chi \rangle \chi \\
&= \sum_{\chi \in \widehat{G}} \frac{1}{G} \sum_{h \in G} \overline{\mathbb{1}_{\{g\}}(h)} \chi(h) \chi \\
&= \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi(g) \chi \\
&= \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi
\end{aligned}$$

On a donc en évaluant en e :

$$\mathbb{1}_{\{g\}}(e) = \frac{1}{G} \sum_{\chi \in \widehat{G}} \chi(e) = 1.$$

D'où $g = e$ et i est bien injective. □

Lemme.

G et $\widehat{G}$ ont même exposant.

Démonstration. Soit N l'exposant de G, on a $\forall \chi \in \widehat{G}$, $\forall g \in G$,

$$\chi^N(g) = \chi(g)^N = \chi(g^N) = \chi(1) = 1.$$

L'exposant de $\widehat{G}$ est inférieur ou égal à N.
On peut appliquer le même raisonnement à $\widehat{G}$ pour obtenir que N est inférieur ou égal à l'exposant de $\widehat{G}$ (car G et $\widehat{\widehat{G}}$ ont même exposant par le lemme précédent).
Cela donne le résultat. □

Passons à la preuve du théorème.

Démonstration. Démontrons le théorème par récurrence sur $n = |G|$.
Pour $n = 1$, le résultat est évident.
On suppose $n > 1$, notons N_1 l'exposant de G.

• Par le lemme précédent, il existe un élément $\chi_1 \in \widehat{G}$ d'ordre N_1. On a donc $\forall g \in G$, $\chi_1(g)^{N_1} = 1$.
Donc $\chi_1(G)$ est un sous-groupe des racines N_1-ièmes de l'unité et on a égalité car χ_1 est d'ordre exactement N_1.

Soit $x_1 \in G$ tel que $\chi_1(x_1) = \exp\left(\frac{2i\pi}{N_1}\right)$ et soit p l'ordre de x_1.
On sait que p divise N_1. Puis $\chi_1(x_1^p) = 1 = \exp\left(\frac{2ip\pi}{N_1}\right)$, donc N_1 divise p et finalement x_1 est d'ordre N_1.

• On pose $H_1 = \langle x_1 \rangle$. Montrons que $G \simeq H_1 \times \mathrm{Ker}(\chi_1)$. Comme $H_1 \simeq \mathbb{Z}/N_1\mathbb{Z}$ et $|\mathrm{Ker}(\chi_1)| < n$, on aura le résultat en appliquant l'hypothèse de récurrence.
En effet, si on décompose $\mathrm{Ker}(\chi_1)$ en $\prod_{i=2}^{r} \mathbb{Z}/N_i\mathbb{Z}$ avec $N_{i+1}|N_i$, alors comme les éléments de G sont d'ordre divisant N_1, on aura $G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}$ avec $N_{i+1}|N_i$.

χ_1 induit un morphisme surjectif α de H_1 sur $\mathbb{U}_{N_1}$, puis par égalité des cardinaux, α est un isomorphisme.
Soit $x \in G$, alors

$$x = \alpha^{-1}(\chi_1(x)) \left(\alpha^{-1}(\chi_1(x))\right)^{-1} x.$$

Par définition de α, $\alpha^{-1}(\chi_1(x)) \in H_1$.
Puis

$$\chi_1\left(\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x\right) = \chi_1\left(\left(\alpha^{-1}(\chi_1(x))\right)^{-1}\right) \chi_1(x) = (\chi_1(x))^{-1}\chi_1(x) = 1,$$

donc $\left(\alpha^{-1}(\chi_1(x))\right)^{-1} x \in \mathrm{Ker}(\chi_1)$.
On a donc bien $G = H_1 \,\mathrm{Ker}(\chi_1)$.
On a aussi $H_1 \cap \mathrm{Ker}(\chi_1) = \{e\}$ car χ_1 est injectif sur H_1.
Il vient donc que $G \simeq H_1 \times \mathrm{Ker}(\chi_1)$, ce qui termine la preuve. □

Remarques : • On peut déduire de ce résultat le théorème de structure des groupes abéliens de type fini.
On applique le théorème précédent au sous-groupe de torsion T, puis on peut prouver qu'on peut écrire $G \simeq T \times L$ avec L sans torsion. On montre en se donnant une base que L est isomorphe à $\mathbb{Z}^d$. Cela donne le résultat.
• Ce résultat peut être généralisé en le théorème de structure des modules de type fini sur les anneaux principaux.

Adapté du travail de Alexandre Bailleul.