Classification des groupes abéliens finis par les caractères

Lemme . Soit G un groupe abélien fini. On définit son exposant comme le ppcm des ordres de ses éléments. Alors

(i) L'exposant de G est le maximum des ordres des éléments de G. En particulier, il existe un élément d'ordre l'exposant de G.

(ii) L'ordre de tout élément divise l'exposant du groupe.

(iii) L'exposant d'un sous-groupe divise l'exposant du groupe.

Preuve :
Soit $x \in G$ un élément d'ordre maximal n. Soit y un élément d'ordre m. Alors il existe $p_1, \dots, p_r$ des nombres premiers et $\alpha_1, \dots, \alpha_r \in \mathbb{N}$ tels que

$$\text{ppcm}(n,m) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$$

avec $p_i^{\alpha_i}$ divise n ou divise m. Soit $i \in [\![1,r]\!]$ et supposons par exemple que $p_i^{\alpha_i}$ divise n. Alors comme $\langle x \rangle$ est cyclique d'ordre n,

$$\text{il existe } z_i \in \langle x \rangle \text{ d'ordre } p_i^{\alpha_i}.$$

On pose $z = z_1 \dots z_r$. Alors z est d'ordre ppcm(n,m), qui est donc plus petit que n par hypothèse et plus grand que n par définition du ppcm. Donc ppcm$(m,n) = n$, c'est-à-dire m divise n, ce qui établit le premier point. Le deuxième est immédiat au vu de la définition.

Pour le troisième, soit H un sous-groupe de G. Alors il existe $h \in H$ tel que l'ordre de h soit l'exposant de H. Or l'ordre de $h \in G$ divise l'ordre de G, d'où le résultat.

□

Lemme . Si G est un groupe abélien fini, alors G et $\widehat{G}$ ont même exposant.

Preuve :
On note $n(G)$ l'exposant du groupe G. Soit $\chi \in \widehat{G}$. Alors

$$\forall g \in G, \quad \chi^{n(G)}(g) = \chi(g)^{n(G)} = \chi\left(g^{n(G)}\right) = \chi(1) = 1,$$

donc $n(\widehat{G})$ divise $n(G)$. En appliquant ce résultat avec $G = \widehat{G}$, on a $n(\widehat{\widehat{G}})$ divise $n(\widehat{G})$. Or un groupe abélien fini est isomorphe à son bidual, donc $n(G)$ divise $n(\widehat{G})$, d'où l'égalité.

□

Théorème . Soit G un groupe abélien fini. Alors il existe $n_1, \ldots, n_r$ des entiers, avec n_1 l'exposant de G et $n_{i+1}|n_i$ pour $i \in [\![1, r-1]\!]$, tels que

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}.$$

Preuve :
On raisone par récurrence sur le cardinal de G, le résultat étant vrai pour $|G| = 1$ avec $n_1 = 1$. On note $|G| > 1$ et on suppose le résultat vrai pour les groupes de cardinal inférieur.
Soit n l'exposant du groupe. Alors

$$\forall g \in G, \forall \chi \in \widehat{G}, \quad \chi(g)^n = 1.$$

D'après le lemme, $\widehat{G}$ est aussi d'exposant n, donc il existe $\chi_1 \in \widehat{G}$ d'ordre n. Or $\chi_1(G)$ est un sous-groupe du groupe $\mathbb{U}_n$ des racines n-ième de l'unité, donc $\chi_1(G) = \mathbb{U}_n$. En particulier, il existe $g_1 \in G$ tel que

$$\chi_1(g_1) = e^{\frac{2i\pi}{n}}.$$

Or par définition de l'exposant, l'ordre de g_1 divise n, donc g_1 est d'ordre n. On a donc trouvé un sous-groupe $H_1 := \langle g_1 \rangle$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Il reste alors à montrer que $G \simeq H_1 \times G_1$ avec $G_1 := \ker(\chi_1)$ et on pourra appliquer la récurrence à G_1, l'exposant d'un sous-groupe divisant l'exposant du groupe.

On sait que $\chi_1 : H_1 \to \mathbb{U}_n$ est surjectif et $|H_1| = |\mathbb{U}_n|$, donc χ_1 est bijectif. Soit $\alpha : \mathbb{U}_n \to H_1$ sa bijection réciproque. Pour $g \in G$, on pose $a = \alpha(\chi_1(g)) \in H_1$ et $b = a^{-1}g$. Alors

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

donc $b \in G_1$ et ainsi $H_1G_1 = G$. Enfin, $H_1 \cap G_1 = \{1\}$ car $G_1 = \ker(\chi_1)$ et χ_1 est injective sur H_1. Donc $G \simeq H_1 \times G_1$.

□