Structure des groupes abéliens finis

Lemme 1. Soit G un groupe abélien fini. On définit $\exp G = \mathrm{ppcm}\{o(g),\ g \in G\}$.
D'une part, $\exp G = \max\{o(g),\ g \in G\}$ et d'autre part, si $H \leqslant G$, alors $\exp(H) | \exp(G)$.

Démonstration. Soit $x \in G$ d'ordre maximal n. Soit $y \in G$ d'ordre m. On écrit $\mathrm{ppcm}(m,n) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Pour $i \in \{1, \dots, r\}$, on a $p_i^{\alpha_i}$ divise n ou m. Dans le premier cas, puisque $\langle x \rangle$ est cyclique, il existe z_i (explicitement $x^{n/p_i^{\alpha_i}}$) d'ordre $p_i^{\alpha_i}$. Dans le second cas, on pose $z_i = y$. Soit $z = z_1 \dots z_r$. Puisque les p_i sont premiers entre eux, z est d'ordre $\mathrm{ppcm}(m,n)$, donc par maximalité, m divise n, donc $\exp G$ divise n. Ce qui donne le premier point du lemme.
Pour le second point, si $h \in H$ est d'ordre $\exp H$, alors $o(h)$ divise $\exp G$ car $h \in G$, ce qui conclut. □

Lemme 2. Si G est un groupe abélien fini, alors G et $\hat{G}$ ont même exposant.

Démonstration. Soit $\chi \in \hat{G}$. Soit $g \in G$.

$$\chi^{\exp(G)}(g) = \chi\left(g^{\exp G}\right) = \chi(e) = 1.$$

donc $\exp \hat{G}$ divise $\exp G$. Puisque G et son bidual sont isomorphes, ils ont même exposant, et le raisonnement précédent appliqué à $\hat{G}$ assure $\exp G = \exp \hat{G}$. □

Théorème 3. Soit G un groupe abélien fini. Il existe $n_1, \dots, n_r$ entiers, avec $n_1 = \exp G$, tels que :

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \quad \text{et} \quad \forall i \in \{1, \dots, r-1\},\ n_{i+1} | n_i.$$

Démonstration. Posons $n = \exp G$. Le lemme précédent assure que $\hat{G}$ est aussi d'exposant n. Par le premier lemme, il existe $\chi_1 \in \hat{G}$ d'ordre n. Or, $\chi_1(G)$ est un sous-groupe de $\mathbb{U}_n$ puisque :

$$\chi_1(g)^n = \chi_1(g^n) = 1.$$

Par égalité des ordres, $\chi_1(G) = \mathbb{U}_n$. En particulier, il existe $g_1 \in G$ tel que $\chi_1(g_1) = \exp(2\mathrm{i}\pi/n)$. Par définition de l'exposant, l'ordre de g_1 divise $\exp G = n$ et d'autre part :

$$1 = \chi_1(g_1^{o(g_1)}) = \chi_1(g_1)^{o(g_1)} = \exp\left(\frac{2\mathrm{i}\pi\, o(g_1)}{n}\right).$$

Cela entraîne que $o(g_1) = n$. Ainsi, $H_1 = \langle g_1 \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.
Considérons α la bijection réciproque de $\chi_1 : H_1 \to \mathbb{U}_n$ (surjective, donc bijective par égalité des cardinaux). Pour $g \in G$, si l'on pose $a = \alpha(\chi_1(g))$ 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 $b \in \ker \chi_1 = G_1$, puis $g = ab \in H_1G_1$, ce qui assure que $G = H_1G_1 \simeq H_1 \times G_1$ car par injectivité de χ_1, l'intersection de H_1 et G_1 est triviale. En itérant le raisonnement sur G_1, d'exposant divisant $\exp G$ par le premier lemme, on conclut. □