Structure des groupes abéliens finis

Lem : Soit G un groupe abélien fini. On pose $\exp(G) = \operatorname{ppcm}\{o(g),\ g \in G\}$.

(i) $\exp(G) = \max\{o(g),\ g \in G\}$

(ii) $\forall g \in G,\ o(g) \mid \exp(G)$. (iii) si $H \leq G$, $\exp(H) \mid \exp(G)$.

- Soit $x \in G$ d'ordre maximal n. Soit $y \in G$, d'ordre m.
On écrit $\operatorname{ppcm}(n,m) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$.
Pour $i \in \{1,\dots,r\}$, $p_i^{\alpha_i} \mid n$ ou $p_i^{\alpha_i} \mid m$. Dans le premier cas, $\langle x \rangle$ est cyclique d'ordre n donc il existe $z_i \in \langle x \rangle$ d'ordre $p_i^{\alpha_i}$, à savoir $x^{n/p_i^{\alpha_i}}$. (Dans le second cas, on considère y). Posons $z = z_1 \dots z_r$.
Puisque les p_i sont p.-à-p., z est d'ordre $p_1^{\alpha_1} \dots p_r^{\alpha_r} = \operatorname{ppcm}(m,n)$, donc par choix de n, $m \mid n$! Donc $\exp(G) \mid \max\{o(g),\ g \in G\}$. L'autre sens est clair.
- (ii) est immédiat. Soit h d'ordre $\exp(H)$. $h \in G$ donc $o(h) \mid \exp(G)$.

Lem : Si G est un groupe abélien fini, G et $\hat{G}$ ont même exposant.

Soit $\chi \in \hat{G}$. Soit $g \in G$.
$\chi^{\exp(G)}(g) = \chi(g)^{\exp(G)} = \chi(g^{\exp(G)}) = \chi(e) = 1$, donc $\exp(\hat{G}) \mid \exp(G)$.
Pour $\hat{G}$, on a donc $\exp(\hat{\hat{G}}) \mid \exp(\hat{G})$. Mais $\hat{\hat{G}} \simeq G$ via eV. Donc $\exp G = \exp \hat{G}$.

Thm : Soit G un groupe abélien fini. Il existe $n_1, \dots, n_r$ entiers, avec $n_1 = \exp G$, tels que $\forall i \in \{1,\dots,r-1\}$, $n_{i+1} \mid n_i$ et $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$.

Raisonnons par récurrence sur $|G|$.
* si $|G| = 1$, le résultat est immédiat avec $n_1 = 1$.
* Supposons le résultat vrai jusqu'au rang $|G|-1$. Posons $n = \exp(G)$.
Par lemme, $\hat{G}$ est aussi d'exposant n, donc par le premier lemme, $\exists \chi_1 \in \hat{G},\ o(\chi_1) = n$
Or $\chi_1(G)$ est un sous-groupe de U_n car $\forall g \in G,\ \chi_1(g)^n = \chi_1(g^n) = 1$, donc $\chi_1(G) = U_n$
Donc $\exists g_1 \in G,\ \chi_1(g_1) = \exp\left(\frac{2i\pi}{n}\right)$
Or $\begin{cases} \text{par définition de l'exposant, } o(g_1) \mid \exp(G) = n \\ \chi_1(g_1^{o(g_1)}) = \chi_1(g_1)^{o(g_1)} = \exp\left(\frac{2i\pi\, o(g_1)}{n}\right) \text{ et } \chi_1(g_1^{o(g_1)}) = 1 \end{cases}$ donc $o(g_1) = n$.

Ainsi, $H_1 = \langle g_1 \rangle \simeq \mathbb{Z}/n\mathbb{Z}$.
Le morphisme $\chi_1 : H_1 \to U_n$ est surjectif, donc bijectif car $|H_1| = n = |U_n|$.
Pour $g \in G$, posons $\begin{cases} a = \alpha(\chi_1(g)) \in H_1 \text{ avec } \alpha \text{ la bijection réciproque de } \chi_1 \\ b = a^{-1}g. \end{cases}$
$\chi_1(b) = \chi_1(a^{-1})\chi_1(g) = \chi_1(a)^{-1}\chi_1(g) = \chi_1(g)^{-1}\chi_1(g) = 1$ donc $b \in \ker \chi_1 = G_1$
Donc $g = ab \in H_1 G_1$, donc $G = H_1 G_1$.
De plus, $H_1 \cap G_1 = \{e\}$ car χ_1 injectif sur H_1. Donc $G = H_1 G_1 \simeq H_1 \times G_1$.
L'hypothèse de récurrence s'applique à G_1, d'exposant divisant $\exp(G)$.