Structure des groupes abéliens finis

Notations :
- Pour tout $n \geq 1$, on désigne par $\mathcal{U}_n$ le groupe cyclique des racines n-ièmes de l'unité.
- On note $\mathcal{U}$ le groupe multiplicatif des nombres complexes de module 1.
- Dans ce problème, G désigne un groupe abélien fini d'ordre ≥ 2.
  La loi de G est notée par juxtaposition : $(a, b) \mapsto ab$. On note e le neutre de G.
- On appelle *caractère* de G tout morphisme de G dans $\mathcal{U}$.
  On note $\widehat{G}$ l'ensemble des caractères de G.

L'objet de ce problème est de prouver le théorème de structure des groupes abéliens finis :

Théorème

Soit G un groupe abélien d'ordre ≥ 2.
Il existe une unique suite $d_1, d_2, \ldots, d_r$ d'entiers supérieurs ou égaux à 2, tels que :
- Pour tout k de $\{1, \ldots, r-1\}$, l'entier d_k divise l'entier d_{k+1}.
- Le groupe G est isomorphe au groupe produit $\mathcal{U}_{d_1} \times \mathcal{U}_{d_2} \times \cdots \times \mathcal{U}_{d_r}$.

I. Prolongement d'un caractère d'un groupe abélien fini

Soit H un sous-groupe strict de G. On se donne un élément φ de $\widehat{H}$.
On se propose de montrer que φ se prolonge en un caractère ϕ de G.
Pour cela, on se donne un élément x de $G \setminus H$, et on note L le sous-groupe de G engendré par H et x, c'est-à-dire le plus petit sous-groupe de G (pour l'inclusion) contenant à la fois H et x.

1. Justifier l'existence de $n = \min\{m \geq 2, x^m \in H\}$ et de ω dans $\mathcal{U}$ tel que $\omega^n = \varphi(x^n)$. [S]
2. Montrer que tout y de L s'écrit de façon unique $y = x^k z$, avec $0 \leq k < n$ et $z \in H$. [S]
3. Avec les notations précédentes, on pose $\psi(y) = \omega^k \varphi(z)$.
   Montrer que ψ est un caractère de L, qui prolonge φ. [S]
4. Montrer finalement l'existence d'un caractère ϕ de G, qui prolonge φ. [S]

II. Exposant d'un groupe abélien fini

On rappelle que l'ordre d'un élément x de G est le plus petit entier $m \geq 1$ tel que $x^m = e$.
On note ici q le ppcm des ordres des différents éléments de G.
On dit que l'entier q est l'*exposant* du groupe G.
On se propose ici de montrer qu'il existe dans G un élément d'ordre q.
Pour cela, on note $q = \prod_{i=1}^{r} p_i^{\alpha_i}$ (les p_i sont premiers distincts deux à deux, les α_i sont dans $\mathbb{N}^*$.)

1. On se donne un entier j dans $\{1, \ldots, r\}$.
   Montrer qu'il existe x_j dans G dont l'ordre s'écrive $m_j\, p_j^{\alpha_j}$, avec $m_j \wedge p_j = 1$. [S]
2. Avec les notations précédentes, quel est l'ordre de $y_j = x_j^{m_j}$? [S]
3. Conclure en considérant l'élément $x = y_1 y_2 \cdots y_r$. [S]

III. Existence de la décomposition d'un groupe abélien fini

Avec les notations de II, on se donne un élément x de G d'ordre q.

1. Pour $0 \leq k < q$, on pose $\varphi(x^k) = \omega^k$, avec $\omega = \exp \frac{2i\pi}{q}$.
   Montrer que φ est un caractère de (x). [S]
2. On prolonge φ en un caractère ϕ de G (cf I.)
   Montrer que tout y de G s'écrit de façon unique $y = x^k z$, où $0 \leq k < q$ et $z \in \ker \phi$. [S]
3. En déduire que le groupe G est isomorphe à $\mathcal{U}_q \times \ker \phi$. [S]
4. En raisonnant par récurrence sur l'ordre de G, montrer l'existence de l'isomorphisme évoqué en préambule de l'énoncé. [S]

IV. Unicité de la décomposition d'un groupe abélien fini

On se propose ici de prouver l'unicité de la décomposition évoquée dans le théorème de l'énoncé.

Pour cela, on se donne les groupes $\begin{cases} H = \mathcal{U}_{d_1} \times \mathcal{U}_{d_2} \times \cdots \times \mathcal{U}_{d_r} \\ K = \mathcal{U}_{\delta_1} \times \mathcal{U}_{\delta_2} \times \cdots \times \mathcal{U}_{\delta_s} \end{cases}$ avec $\begin{cases} 2 \leq d_1 \mid d_2 \mid \cdots \mid d_r \\ 2 \leq \delta_1 \mid \delta_2 \mid \cdots \mid \delta_s \end{cases}$.

On notera indifféremment e l'élément neutre de H et celui de K.

On suppose que H et K sont isomorphes. Sans perdre de généralité, on peut supposer $r \leq s$.

Pour conclure, il faut donc établir $r = s$, et $d_j = \delta_j$ pour tout j de $\{1, \ldots, r\}$.

1. On se donne m et n dans $\mathbb{N}^*$. On note $m \wedge n$ le pgcd de m et de n.
   Montrer que dans $\mathcal{U}_n$ l'équation $x^m = 1$ possède $m \wedge n$ solutions distinctes. [S]
2. Pour tout $m \geq 1$, combien l'équation $x^m = e$ possède-t-elle de solutions distinctes dans H et dans K respectivement ? Pourquoi ces deux nombres sont-ils égaux ? [S]
3. En appliquant ce qui précède à l'entier $m = \delta_1$, prouver que $r = s$ et que $d_1 = \delta_1$. [S]
4. Conclure en appliquant ce qui précède aux entiers $m = \delta_2$, $m = \delta_3$, etc [S]

V. Applications

1. Donner (à un isomorphisme près) le nombre de groupes abéliens d'ordre 72. [S]
2. Dans cette question, on montre que les groupes G et $\widehat{G}$ sont isomorphes.
   (a) Pour $n \geq 1$, montrer que $\widehat{\mathcal{U}_n}$ est cyclique d'ordre n (donc isomorphe à $\mathcal{U}_n$.) [S]
   (b) Soient $H_1, H_2, \ldots, H_r$ des groupes abéliens, et $H = H_1 \times H_2 \ldots \times H_r$.
   Montrer que le groupe $\widehat{H}$ est isomorphe à $\widehat{H_1} \times \widehat{H_2} \ldots \times \widehat{H_r}$.
   Indication : Pour tous $\varphi_j \in \widehat{H_j}$, définir φ sur H par $\varphi(x_1, \ldots, x_n) = \prod_{j=1}^{r} \varphi_j(x_j)$. [S]
   (c) Conclure. [S]