Groupes abéliens finis

R. LOUBOUTIN

02/02/2017

Le but de ce problème est de prouver, en restant dans le cadre du prgramme de la filère MP, que tout groupe commutatif fini est isomorphe à un produit direct de groupes cycliques, avec une certaine unicité de l'écriture.

Notations

Si n est un entier non nul, on note $\frac{\mathbb{Z}}{n\mathbb{Z}}$ le groupe des entiers modulo n. Tout groupe cyclique d'ordre n est isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Si G est un groupe quelconque sa loi est notée mutiplicativement, s'il est commutatif additivement. Dans le premier cas l'élément neutre est noté e et l'itéré d'un élément x noté x^n ; dans le deuxième cas l'élément neutre est noté 0 et l'itéré de x noté $n.x$. On note toujours $< x >$ le sous-groupe engendré par un élément x.

La notation $G \sim G'$ signifie que les deux groupes G et G' sont isomorphes.

Si H et K sont deux parties du groupe G (en particulier deux sous-groupes) HK désigne $\{xy, x \in H\ y \in K\}$, $H + K$ désigne $\{x + y, x \in H\ y \in K\}$ (cas d'un groupe commutatif), $xH = \{xy, y \in H\}$, $x + H = \{x + y, y \in H\}$, $n.H = \{n.y, y \in H\}$.

On note $|H|$ le cardinal d'une partie finie (on parle d'ordre lorsqu'il s'agit d'un groupe ou d'un sous-groupe).

Si x et y sont deux entiers $x|y$ veut dire que x divise y, $x \wedge y$ désigne leur p.g.c.d. dans $\mathbb{N}$.

I : généralités sur les groupes finis

Soit G un groupe fini quelconque et H un sous-groupe de G

$I.1$) Montrer que la relation $xy^{-1} \in H$ définit une relation d'équivalence sur G dont toutes les classes d'équivalence ont pour cardinal le cardinal de H. En déduire que $|H|$ divise $|G|$ (théorème de Lagrange).

$I.2$) Soit a un élément de G et $< a >$ le sous-groupe engendré par G. Montrer que $< a >= \{e, a, \ldots, a^{n-1}\}$ où $n = \min\{p \in \mathbb{N}^*, a^p = e\}$. n s'appelle l'ordre de a.

$I.3$) Montrer que l'ordre de tout élément de G divise l'ordre de G. Montrer que s'il existe dans G un élément d'ordre n, il existe aussi un élément d'ordre d pour tout diviseur de n. On appelle exposant du groupe G le p.p.c.m. des ordres des éléments de G.

II : quelques résultats sur les groupes abéliens finis

Dans cette partie et les suivantes G est toujours un groupe commutatif.

Soit G un groupe commutatif, H et K deux sous-groupes de G. On dira que G est la somme directe de H et K et on écrira $G = H \oplus K$ si $G = H + K$ et $H \cap K = \{0\}$.

$II.1$) Montrer que si $G = H \oplus K$ alors G est isomorphe à $H \times K$, puis plus précisément que si H et K sont respectivement isomorphes à H' et K' alors G est isomorphe à $H' \times K'$.

Maintenant G est un groupe abélien fini.

$II.2$) On suppose maintenant que G est d'exposant mn avec $m \wedge n = 1$, c'est-à-dire $G = G_{mn}$. Montrer que G est isomorphe à $G_m \times G_n$.

Indication : Utilser l'identité de Bézout, pour chacune des propriétés à vérifier.

$II.3$) En déduire un résultat sur les groupes additifs $\frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$ et $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ si m et n sont des entiers non nuls premiers entre eux.

$II.4$) Soit d un entier, soit $G_d = \{x \in G, d.x = 0\}$. Montrer que G_d est un sous-groupe de G, formé des éléments dont l'ordre divise d.

$II.5$) On suppose que l'exposant n de G est de la forme $n = \prod_{k=1}^{s} p_k^{m_k}$ où les p_k sont des nombres premiers distincts et les m_k sont dans $\mathbb{N}^*$ (le cas $s = 0$ correspond par définition au cas $n = 1$ et $G = \{0\}$). Montrer que G est isomorphe au produit direct $\prod_{k=1}^{s} H_k$ où $H_k = G_{p_k^{m_k}}$.

III : p-groupes

Si p est un nombre premier, un p-groupe est un groupe (ici abélien) dans lequel tout élément à pour ordre une puissance de p. Par exemple, dans la partie précédente les H_k sont des p_k-groupes.

Dans cette partie G est un p-groupe abélien, p étant un nombr premier.

$III.1$) Montrer que tout sous-groupe de G est un p-groupe.

$III.2$) Rappeler comment et pourquoi $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps. On le notera $\mathbb{F}_p$

$III.3$) On suppose que tout élément du sous-groupe H est d'ordre au plus p. Montrer que $(\overline{m}, x) \mapsto \overline{m}.x = m.x$ permet de munir H d'une structure de $\mathbb{F}_p$-espace vectoriel. En déduire qu'il existe d tel que H soit isomorphe (en tant que groupe additif) à $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^d$.

$III.4$) On suppose que tout élément de G est d'ordre au plus p. Montrer que si H est un sous-groupe de G, il existe un sous-groupe K tel que $G = H \oplus K$.

$III.5$) On suppose G non réduit à $\{0\}$. Montrer qu'il existe $m \geq 1$ tel que $p^m.G = \{0\}$ et $H = p^{m-1}.G \neq \{0\}$. On notera $\tau(G)$ cet exposant m, avec la convention $\tau(\{0\}) = 0$.

On va montrer par récurrence sur $\tau(G)$, qu'il existe s dans $\mathbb{N}$ et $(m_1, \ldots, m_s)$ dans $(\mathbb{N}^*)^s$ tels que

$$G \sim \prod_{i=1}^{s} \frac{\mathbb{Z}}{p^{m_i}\mathbb{Z}}$$

(le cas $s = 0$ correspond par convention au cas $G = \{0\}$.)

$III.6$) Montrer que le résultat est vrai si $\tau(G) = 1$.

Soit m un entier non nul. On suppose maintenant le résultat vrai pour les p-groupes abéliens G' tels que $\tau(G') = m$. Soit G un p-groupe abélien tel que $\tau(G) = m + 1$.

$III.7$) Montrer que l'application $\phi : x \mapsto p.x$ est un morphisme de groupe de G vers G. Montrer que $\tau(\mathrm{Im}\,(\phi)) = m$.

On en déduit :

$$\mathrm{Im}\,(\phi) \sim \prod_{i=1}^{s} \frac{\mathbb{Z}}{p^{m_i}\mathbb{Z}} = \prod_{i=1}^{s} G'_i.$$

Soit θ l'application réalisant cet isomorphisme.

Pour j dans $[1, s]$ on pose $z_j = (z_{i,j}) \in \prod_{i=1}^{s} G'_i$, où $z_{i,j} = \overline{0}$ si $i \neq j$, $z_{i,i} = \overline{1}$ (où on note $\overline{x}$ la classe de x dans $\frac{\mathbb{Z}}{p^{m_i}\mathbb{Z}}$, pout tout i, la notation $\overline{x}^i$ étant vraiment lourde). On choisit alors y_j tel que $\theta(\phi(y_j)) = z_j$. Finalement on note $H =< y_1, \ldots, y_s >$ le sous groupe engendré par $\{y_1, \ldots, y_s\}$, c'est-à-dire le plus petit sous-groupe de G contenant $\{y_1, \ldots, y_s\}$

$III.8$) Montrer que :

$$H \sim \prod_{i=1}^{s} \frac{\mathbb{Z}}{p^{m_i+1}\mathbb{Z}}.$$

$III.9$) Soit $K = H \cap \mathrm{Ker}\ \phi$, montrer qu'il existe un sous groupe K' contenu dans Ker ϕ tel que $\mathrm{Ker}\,(\phi) = K \oplus K'$.

$III.10$) Montrer que $G = K' \oplus H$.

$III.11$) Conclure.

IV : synthèse

$IV.1$) En utilisant les résultats des parties précédentes montrer que tout groupe abélien fini est isomorphe à un produit direct de groupes cycliques.

V : questions d'unicité

$V.1$) Donner l'exemples de deux ensembles distincts $\{m_1, m_2\}$ et $\{m_3, m_4\}$ tels que :

$$\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \sim \frac{\mathbb{Z}}{m_3\mathbb{Z}} \times \frac{\mathbb{Z}}{m_4\mathbb{Z}}$$

$V.2$) Soit m et n deux entiers non nuls et $d = m \wedge n \in \mathbb{N}$. On écrit $m = m'd$, $n = n'd$. Montrer que :

$$m.\frac{\mathbb{Z}}{n\mathbb{Z}} \sim \frac{\mathbb{Z}}{n'\mathbb{Z}}$$

$V.3$) Soit m un entier, G et G' deux groupes commutatifs. Montrer que :

$$m.(G \times G') = m.G \times m.G'$$

V.4) En déduire que si $(p_1, \ldots, p_r)$ et $(p'_1, \ldots, p'_{r'})$ sont des suites croissantes de nombres premiers deux à deux distincts (dans chaque famille), $(m_{i,j})$ et $(m'_{i,j})$ deux familles d'entiers non nuls telles que à i fixé la suite $(m_{i,j})_{1\leq j\leq s_i}$ est croissante, et de même pour les suites $(m'_{i,j})_{1\leq j\leq s_i}$ et si

$$\prod_{i=1}^{r}\prod_{j=1}^{s_i}\frac{\mathbb{Z}}{p_i^{m_{i,j}}\mathbb{Z}} \sim \prod_{i=1}^{r'}\prod_{j=1}^{s'_i}\frac{\mathbb{Z}}{p'^{m'_{i,j}}_i\mathbb{Z}}$$

alors $r = r'$, puis pour tout i $p_i = p'_i$ et $s_i = s'_i$, et finalement $m_{i,j} = m'_{i,j}$ pour tout couple (i, j) envisageable.

Indication : Utiliser les deux question précédentes, en choisissant $m = p_1^{m_1}$, et en raisonnant par récurrence sur $\sum s_i + \sum s'_i$.

Indication : Utiliser les questions précédentes et raisonner par récurrence sur la somme des exposants.

V.5) Soit G un groupe abélien fini, montrer qu'il existe une suite $(d_1, \ldots, d_n)$ telle que $d_i | d_{i+1}$ si $1 \leq i < n$ et

$$G \sim \prod_{i=1}^{n}\frac{\mathbb{Z}}{d_i\mathbb{Z}}$$

(Décomposition de Frobénius)

V.6)

a) Montrer l'unicité de la décomposition obtenue dans la question précédente.

b) Donner la décomposition primaire et la décomposition de Frobénius du groupe

$$\frac{\mathbb{Z}}{72\mathbb{Z}} \times \frac{\mathbb{Z}}{30\mathbb{Z}} \times \frac{\mathbb{Z}}{75\mathbb{Z}}$$