Groupes abéliens finis
L3–Mathématiques
2019–2020

Paul LESCOT
Université de Rouen
paul.lescot@univ-rouen.fr

1. Groupes abéliens finis

THÉORÈME 1.1. *Soit G un groupe fini abélien ; alors il existe un entier $r \in \mathbf{N}$ et des entiers $a_1, ..., a_r$ avec $a_1 \geq 2$ et*

$$a_1|a_2|...|a_r$$

tels que

$$G \simeq \frac{\mathbf{Z}}{a_1\mathbf{Z}} \times ... \times \frac{\mathbf{Z}}{a_r\mathbf{Z}}.$$

DÉMONSTRATION. On procède par récurrence sur $|G|$, le résultat étant clair pour $|G| = 1$. Soit donc G d'ordre $|G| > 1$, et supposons que chaque groupe d'ordre $< |G|$ satisfasse à la conclusion du Théorème. Posons

$$e(G) := ppcm(\omega(x)|x \in G)$$

(**exposant** de G) ; on a vu en cours qu'il existait $x \in G$ tel que $\omega(x) = e(G)$.

Il existe au moins un sous–groupe T de G tel que $T \cap < x >= \{e\}$: le sous–groupe $\{e\}$. Choisissons un de ces sous–groupes d'ordre maximal : H. On a $H \cap < x >= \{e\}$, donc le sous–groupe $H < x >$ est un produit direct :

$$H < x >= H \times < x > .$$

Supposons pour le moment $G \neq H < x >$, et soit alors $y \in G \setminus H < x >$ d'ordre minimal.

Alors $y \neq e$ d'où $\omega(y) \geq 2$. Ecrivons

$$\omega(y) = q_1^{\alpha_1}...q_m^{\alpha_m}$$

avec les q_i premiers et deux à deux distincts et les $\alpha_i \geq 1$.

Si $m \geq 2$, on peut écrire

$$y = y_1...y_m$$

où les y_i sont des puissances de y et

$$\forall i \in \{1, ..., m\}\ \omega(y_i) = q_i^{\alpha_i}.$$

Si l'on avait $m \geq 2$, on aurait, pour chaque i, $\omega(y_i) < \omega(y)$, d'où, par définition de y, $y_i \in H < x >$ et $y = y_1...y_m \in H < x >$, une contradiction. Donc $m = 1$ et $\omega(y) = q_1^{\alpha_1}$, que nous noterons plus simplement $\omega(y) = q^\alpha$ (q premier, $\alpha > 1$).

On a

$$\omega(y^q) = \frac{\omega(y)}{pgcd(\omega(y), q)} = \frac{q^\alpha}{pgcd(q^\alpha, q)} = \frac{q^\alpha}{q} = q^{\alpha-1} < q^\alpha = \omega(y),$$

donc, encore une fois par définition de y, $y^q \in H < x >$. Ecrivons donc

$$y^q = hx^s (h \in H, s \in \mathbf{Z}).$$

Il apparaît que

$$\begin{aligned} e &= y^{q^\beta} \\ &= (y^q)^{q^{\beta-1}} \\ &= (hx^s)^{q^{\beta-1}} \\ &= h^{q^{\beta-1}} x^{sq^{\beta-1}} \end{aligned}$$

d'où

$$(h^{q^{\beta-1}})^{-1} = x^{sq^{\beta-1}} \in H \cap < x >= \{e\}$$

et

$$x^{sq^{\beta-1}} = e,$$

soit $\omega(x)|sq^{\beta-1}$.

Mais $q^\beta = \omega(y)$ divise $e(G) = \omega(x)$, donc q^β divise $sq^{\beta-1}$: q divise s. Nous pouvons donc écrire $s = qt(t \in \mathbf{Z})$; soit $z := yx^{-t}$. Du fait que $y \notin H < x >$, on a $z \notin H < x >$; de plus

$$\begin{aligned} z^q &= (yx^{-t})^q \\ &= y^q x^{-qt} \\ &= hx^s x^{-s} \\ &= h. \end{aligned}$$

Soit maintenant $H^{'} = H < z >$; $H^{'}$ est un sous–groupe de G, $H^{'}$ contient H, et $H^{'} \neq H$ vu que $z \in H^{'}$ et $z \notin H$; on a donc $|H^{'}| > |H|$. Par définition, $H^{'} \cap < x > \neq \{e\}$; soit donc $w \in H^{'} \cap < x >$, $w \neq e$. On peut écrire $w = h_1 z^n (h_1 \in H$, $n \in \mathbf{Z})$.

Si q divisait n, on pourrait écrire $n = qu$ $(u \in \mathbf{Z})$ et

$$w = h_1 z^{qu} = h_1 (z^q)^u = h_1 h^u \in H$$

d'où

$$e \neq w \in H \cap < x >= \{e\},$$

une contradiction. Donc q ne divise pas n ; il en résulte que q et n sont premiers entre eux. D'après le Théorème de Bachet–Bezout, il existe $(\lambda, \mu) \in \mathbf{Z}^2$ tel que $\lambda q + \mu n = 1$. Mais alors

$$\begin{aligned} z &= z^{\lambda q + \mu n} \\ &= (z^q)^\lambda (z^n)^\mu \\ &= h^\lambda (h_1^{-1} w)^\mu \\ &= h^\lambda h_1^{-\mu} w^\mu. \end{aligned}$$

Vu que $h \in H \subset H < x >$, $h_1 \in H \subset H < x >$ et $w \in < x > \subset H < x >$, on trouve $z \in H < x >$, une contradiction.

On a donc $G = H < x >= H \times < x >$.

Par hypothèse de récurrence, vu que $|H| = \dfrac{|G|}{| < x > |} = \dfrac{|G|}{\omega(x)} < |G|$, on peut écrire

$$H \simeq \frac{\mathbf{Z}}{a_1 \mathbf{Z}} \times ... \times \frac{\mathbf{Z}}{a_r \mathbf{Z}}$$

pour $r \in \mathbf{N}$ et des entiers $a_1, ..., a_r$ tels que $a_1 \geq 2$ et

$$a_1 | a_2 | ... | a_r.$$

Mais alors H contient un sous–groupe isomorphe à $\dfrac{\mathbf{Z}}{a_r \mathbf{Z}}$, donc il contient un élément d'ordre a_r ; G contient donc un élément d'ordre a_r. En particulier, a_r divise $e(G) = \omega(x)$. Posons $a_{r+1} = \omega(x)$; alors

$$a_1 | a_2 | ... | a_r | a_{r+1}$$

2

et

$$\begin{aligned} G &= H\times < x > \\ &\simeq \frac{\mathbf{Z}}{a_1\mathbf{Z}} \times ... \times \frac{\mathbf{Z}}{a_r\mathbf{Z}} \times < x > \\ &\simeq \frac{\mathbf{Z}}{a_1\mathbf{Z}} \times ... \times \frac{\mathbf{Z}}{a_r\mathbf{Z}} \times \frac{\mathbf{Z}}{\omega(x)\mathbf{Z}} \\ &= \frac{\mathbf{Z}}{a_1\mathbf{Z}} \times ... \times \frac{\mathbf{Z}}{a_r\mathbf{Z}} \times \frac{\mathbf{Z}}{a_{r+1}\mathbf{Z}}. \end{aligned}$$

□