**UNIVERSITÉ DE NANTES**
**DÉPARTEMENT DE MATHÉMATIQUES**
**Année 2017-2018, Agrégation Externe**

# Thème N° I : Groupes abéliens

## Prérequis

- Ordre d'un élément.
- Théorème de Lagrange, indice d'un sous-groupe.

## Commentaires

Les groupes abéliens sont souvent les premiers groupes que vous avez étudiés, en particulier les groupes cycliques $\mathbb{Z}/n\mathbb{Z}$. Concernant ces derniers, le paragraphe A doit être compris et connu sur le bout des doigts !
La classification des groupes abéliens de type fini est au programme de l'agrégation et peut faire l'objet d'un développement à l'oral sous différentes formes. Le paragraphe B présente la classification des groupes abéliens finis à travers les composantes primaires.
Enfin, le paragraphe C vous propose l'étude d'un groupe un peu particulier : il pourra vous servir d'exemple ou de contre-exemple pour illustrer certaines leçons.

## Références

N'importe quel (bon) livre de théorie des groupes parle de groupes abéliens. Concernant les groupes cycliques, vous pouvez consulter l'index du livre de Ulmer (à « groupe cyclique »), [Tauvel, paragraphe 4.7 page 46] ou/et [Szpirglas, paragraphe VI.2 page 256]. Pour la notion de somme directe de groupes abéliens, vous pouvez regarder [Tauvel, paragraphe 4.9]. Enfin, vous trouverez dans [Combes, pages 66-67] une démonstration directe (sans passer par les composantes primaires) du théorème de classification par les facteurs invariants.

## A Groupes cycliques

Dans toute cette partie, $n$ est un entier naturel supérieur ou égal à 2.

**1)** Montrer que si $n$ est premier, alors tout groupe d'ordre $n$ est cyclique.

**2)** a) Montrer que l'ensemble des racines $n^{\text{èmes}}$ de l'unité dans $\mathbb{C}$ est cyclique d'ordre $n$.

b) Déterminer tous les sous-groupes finis du groupe multiplicatif $\mathbb{C}^*$.

**3)** Montrer qu'un groupe d'ordre $n$ est cyclique si, et seulement si, il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

**4)** Soit $d$ un diviseur de $n$. Montrer que $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous-groupe de cardinal $d$ et que celui-ci est cyclique.

**5)** a) Soit $a \in \mathbb{Z}^*$. Montrer l'équivalence des trois assertions suivantes :

*(i)* la classe de $a$ modulo $n$ engendre $\mathbb{Z}/n\mathbb{Z}$ ;
*(ii)* $a$ est premier avec $n$ ;
*(iii)* $a$ est inversible modulo $n$.

b) On note $\varphi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$. Calculer $\varphi(p^\alpha)$ pour $p$ premier et $\alpha \in \mathbb{N}^*$.

c) Montrer que $n = \sum_{d|n} \varphi(d)$.

**6)** Montrer qu'un groupe fini $G$ de cardinal $n$ est cyclique si, et seulement si, pour tout $d$ divisant $n$, il existe au plus un sous-groupe de cardinal $d$ dans $G$.

**7)** Soit $G$ un sous-groupe fini du groupe multiplicatif d'un corps. Montrer que $G$ est cyclique.

**8)** On note $(\mathbb{Z}/n\mathbb{Z})^{\times}$ le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Montrer que le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

**9)** Soit $m \in \mathbb{N}$, $m \geq 2$. Montrer que $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si, et seulement si, $m$ et $n$ sont premiers entre eux.

**10)** Soient $G$ et $G'$ deux groupes cycliques d'ordres respectifs $m$ et $n$. Montrer que le groupe des morphismes de groupes de $G$ vers $G'$ est un groupe cyclique dont on déterminera l'ordre.

## B Groupes abéliens finis

L'essentielle de cette partie est inspirée des exercices 4.1.3, 4.1.4, 4.1.6 et 4.1.7 de [Delcourt], sauf le **6)**, qui vient du [Combes, pages 65-66]. On peut également aller voir [Szpirglas, théorème 6.85 page 254] pour le **7)**.

Soit $G$ un groupe abélien fini dont la loi est notée additivement.

**1)** Pour $p$ nombre premier, on note $G(p) := \{x \in G \,/\, \exists n \in \mathbb{N},\ p^n x = 0\}$.
Montrer que $G(p)$ est un sous-groupe de $G$.

$G(p)$ est appelé *composante p-primaire* de $G$.

**2)** Soit $\mathscr{P}_G$ l'ensemble des diviseurs premiers du cardinal de $G$. Montrer que $G = \bigoplus_{p \in \mathscr{P}_G} G(p)$.

**3)** Montrer que si $G = H \times K$ ($H$ et $K$ sont deux groupes abéliens), alors, pour tout nombre premier $p$, $G(p)$ est isomorphe à $H(p) \times K(p)$.

**4)** Déterminer $(\mathbb{Z}/n\mathbb{Z})(p)$ pour tout nombre premier $p$ et tout $n \in \mathbb{N}$, $n \geq 2$.

**5)** Montrer que si $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ est la décomposition du cardinal de $G$ en facteurs premiers, alors, pour tout $i \in [\![1, k]\!]$, $G(p_i)$ est de cardinal $p_i^{\alpha_i}$.

**6)** Soit $g \in G$ un élément d'ordre maximal et $\pi : G \to G/\langle g \rangle$ la surjection canonique. Le but de cette question est de démontrer que tout $\xi \in G/\langle g \rangle$ admet un représentant $x_0$ dans $G$ dont l'ordre coïncide avec celui de $\xi$. Considérons $x \in G$ tel que $\pi(x) = \xi$.

a) Si $s$ désigne l'ordre de $\xi$, montrer qu'il existe $k \in \mathbb{Z}$ tel que $sx = kg$.

b) Soit $(q, r) \in \mathbb{Z}^2$ tel que $k = sq + r$ et $0 \leq r < s$, et $x_0 := x - qg$. Pourquoi $s$ divise-t-il l'ordre de $x_0$ ?

c) Montrer que $s$ divise $k$ (on pourra supposer que $r \neq 0$ et mettre en défaut le fait que $g$ est un élément d'ordre maximal dans $G$).

d) En déduire que $x_0$ est bien un représentant de $\xi$ d'ordre $s = \omega(\xi)$.

**7)** Soit $p$ un nombre premier, $n \in \mathbb{N}^*$ et $H$ un groupe abélien de cardinal $p^n$.

a) Montrer par récurrence sur $n$ qu'il existe $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ tel que $G$ soit isomorphe à

$$\mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}.$$

b) Montrer que si $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ et $(m_1, \ldots, m_l) \in (\mathbb{N}^*)^l$ sont tels que

- $n_1 \leq \cdots \leq n_k$ et $m_1 \leq \cdots \leq m_l$,
- $\mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{n_k}\mathbb{Z}$ et $\mathbb{Z}/p^{m_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{m_l}\mathbb{Z}$ sont isomorphes,

alors $k = l$ et, pour tout $i \in [\![1, k]\!]$, $n_i = m_i$.

**8)** Donner la décomposition en composantes primaires des deux groupes $G_1$ et $G_2$ suivants :

$$G_1 = \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/56\mathbb{Z} \quad \text{et} \quad G_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

Ces deux groupes sont-ils isomorphes ?

**9)** a) Déterminer pour le groupe $G_1$ précédent une famille $(d_1, \dots, d_k)$ d'entiers naturels vérifiant :

*i)* $2 \leq d_1$ et $d_1 | d_2 | \cdots | d_k$ ;
*ii)* $G_1$ est isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}$.

b) Établir ce résultat général pour $G$ et montrer qu'une telle décomposition est unique.

Les entiers $d_1, \dots, d_k$ sont appelés *facteurs invariants* du groupe $G$. La suite $(p_1^{\alpha_1^1}, \dots, p_1^{\alpha_{t_1}^1}, \dots, p_k^{\alpha_1^k}, \dots, p_k^{\alpha_{t_k}^k})$ telle que

$$G \approx \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{t_i} \mathbb{Z}/p_i^{\alpha_j^i}\mathbb{Z}$$

(résultats des questions **2)** et **5)**) est appelée *suite des diviseurs élémentaires* de $G$.

**10)** Combien existe-t-il, à isomorphisme près, de groupes abéliens de cardinal 600 ? Donner pour chaque classe d'isomorphisme les composantes primaires et les facteurs invariants.

# C Un exemple un peu particulier

Voir [Delcourt, problème 2.5.2 pages 56-57 et 175-176], [Francinou *et al.* , exercice 2.16 page 54], [Calais, exercice 34 p.171]ou [Schwartz, exercices 3, 4 et 6 page 45].

On note $G$ l'ensemble des racines de l'unité de $\mathbb{C}$ :

$$G = \left\{ z \in \mathbb{C} \,/\, \exists n \in \mathbb{N}^*, \ z^n = 1 \right\} = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$$

où $\mathbb{U}_n$ désigne le groupe des racines $n^{\text{èmes}}$ de l'unité.

**1)** Montrer que $G$ est un sous-groupe de $S^1$ coïncidant avec $\left\{ e^{2i\pi x} \,/\, x \in \mathbb{Q} \right\}$.

**2)** Montrer que $G$ est isomorphe au groupe quotient $\mathbb{Q}/\mathbb{Z}$.

**3)** Montrer que tout élément de $G$ est fini mais que $G$ est infini.

**4)** Montrer qu'il existe dans $G$ des éléments d'ordre arbitraire.

**5)** Soit $n \in \mathbb{N}^*$. Montrer qu'il existe dans $G$ un unique sous-groupe de cardinal $n$ et qu'il est cyclique.

**6)** Montrer que $G$ est *divisible*, c'est-à-dire que pour tout élément $g$ de $G$ et tout entier naturel non nul $n$, il existe $h \in G$ tel que $g = h^n$.

**7)** Soit $n \in \mathbb{N}^*$ et $H_n$ l'unique sous-groupe de cardinal $n$ de $G$. Montrer que le groupe quotient $G/H_n$ est isomorphe à $G$.

**8)** Dans cette question, $p$ est un nombre premier et on définit $\mathbb{U}_{p^\infty}$ par $\mathbb{U}_{p^\infty} = \bigcup_{k \in \mathbb{N}} \mathbb{U}_{p^k}$

a) Montrer que $\mathbb{U}_{p^\infty}$ est un sous-groupe infini de $G$.

b) Montrer que $\mathbb{U}_{p^\infty}$ n'est pas de type fini.

c) Montrer que tous les sous-groupes de $\mathbb{U}_{p^\infty}$ sont finis cycliques.

# Bibliographie


Calais, Josette. 1984. *Élément de théorie des groupes.* PUF.

Combes, François. 1998. *Algèbre et géométrie.* Bréal.

Delcourt, Jean. 2007. *Théorie des groupes.* Dunod.

Francinou, Serge, Gianella, Hervé, & Nicolas, Serge. 2001. *Exercices de mathématiques. Oraux-XENS, algèbre 1.* Cassini.

Schwartz, Lionel. 1998. *Algèbre.* Dunod.

Szpirglas, Aviva. 2009. *Mathématiques L3 : Algèbre.* Pearson.

Tauvel, Patrice. 2005. *Algèbre : agrégation, licence 3e année, master.* Dunod.