$\mathbf{Z}$ et $\mathbf{Z}/n$

Exercice 1. — **[Morphismes de groupes]**

a) Montrer qu'un morphisme de groupes qui est bijectif est un isomorphisme de groupes.

b) Montrer qu'un morphisme de groupes injectif entre deux groupes finis de même cardinal est un isomorphisme de groupes.

c) Montrer que l'image par un morphisme d'un groupe monogène est monogène.

d) Soient G un groupe quelconque et H un groupe abélien. Montrer que $\mathrm{Hom}_{\mathrm{gp}}(G,H)$ est un sous-groupe de l'ensemble des fonctions $\mathcal{F}(G,H)$.

Soient $\varphi : G \to H$ et $\psi : H \to K$ des morphismes de groupes.

e) Montrer que si φ est injectif alors G est isomorphe à $\mathrm{Im}\,\varphi$.

f) Montrer que si $\psi \circ \varphi$ est injective (resp. surjective) alors φ aussi (resp. ψ aussi).

g) Pour $K = G$ quelconque, donner un exemple où $\psi \circ \varphi = \mathrm{id}_G$ mais $\varphi \circ \psi \neq \mathrm{id}_H$.

Exercice 2. — **[$(\mathbf{Z},+)$]**

a) Montrer que les sous-groupes de $\mathbf{Z}$ sont exactement les $n\mathbf{Z}$ pour $n \in \mathbf{N}$.

b) A quelle condition a-t-on $n\mathbf{Z} \subset m\mathbf{Z}$?

c) Expliciter les sous-groupes $n\mathbf{Z} \cap m\mathbf{Z}$ et $n\mathbf{Z} + m\mathbf{Z}$ (sous-groupe engendré).

d) Quels sont les morphismes de groupes de $\mathbf{Z}$ dans lui-même ?
Plus généralement, pour tout groupe G, montrer que l'on a une bijection

$$\mathrm{Hom}_{\mathrm{gp}}(\mathbf{Z}, G) \cong G.$$

Lorsque G est abélien, montrer qu'il s'agit d'un isomorphisme de groupes.

Exercice 3. — **[$(\mathbf{Z}/n\mathbf{Z},+)$]**

a) Déterminer les sous-groupes de $\mathbf{Z}/n$.

b) Quel est l'ensemble des générateurs de $\mathbf{Z}/n$?

c) Déterminer les ensembles de morphismes suivants :

$$\mathrm{Hom}_{\mathrm{gp}}(\mathbf{Z}/n, \mathbf{Z}), \qquad \mathrm{Hom}_{\mathrm{gp}}(\mathbf{Z}/n, \mathbf{Z}/n), \qquad \mathrm{Aut}(\mathbf{Z}/n), \qquad \mathrm{Hom}_{\mathrm{gp}}(\mathbf{Z}/n, \mathbf{Z}/m).$$

Plus généralement, expliciter une bijection entre $\mathrm{Hom}_{\mathrm{gp}}(\mathbf{Z}/n, G)$ et l'ensemble des éléments de G d'ordre divisant n.

d) Soit d un diviseur de n. Montrer que le morphisme *de réduction*

$$\begin{array}{ccc} \mathbf{Z}/n & \to & \mathbf{Z}/d \\ x[n] & \mapsto & x[d] \end{array}$$

est (bien défini et) surjectif. Quel est son noyau ?

e) Quel est le noyau du morphisme de réduction $\mathbf{Z}/mn \to \mathbf{Z}/m \times \mathbf{Z}/n$? Montrer que son image est isomorphe à $Z/\mathrm{ppcm}(m,n)$.
Montrer qu'un élément $(x \mod m, y \mod n)$ est dans son image ssi l'on a $x \equiv y[\mathrm{pgcd}(n,m)]$.

f) Les groupes $\mathbf{Z}/mn$ et $\mathbf{Z}/n \times \mathbf{Z}/m$ sont-ils isomorphes si m et n ne sont pas premiers entre eux.

g) Déterminer tous les sous-groupes de $\mathbf{Z}/2 \times \mathbf{Z}/2$.

Exercice 4. — Soit p un nombre premier. Montrer qu'un groupe d'ordre p est isomorphe à $\mathbf{Z}/p$.

Exercice 5. — Montrer que les groupes $(\mathbf{R}^{+*}, \times)$ et $(\mathbf{R}, +)$ sont isomorphes.

Exercice 6. — **[Où l'on parle de Q]**

a) Montrer qu'un sous-groupe de $(\mathbf{Q}, +)$ engendré par un nombre fini d'éléments est monogène.

b) Soit p un nombre premier. Montrer que les ensembles suivants sont des sous-groupes de $(\mathbf{Q}, +)$ qui ne sont pas de type fini :

(*i*) $\mathbf{Z}_{(p)} := \left\{\frac{a}{b},\ a \in \mathbf{Z} \text{ et } b \text{ premier à } p\right\}$

(*ii*) $p^n\mathbf{Z}_{(p)}$

(*iii*) $\mathbf{Z}\left[\frac{1}{p}\right] := \left\{\frac{a}{p^k},\ a \in \mathbf{Z}, k \in \mathbf{N}\right\}$

(*iv*) $n\mathbf{Z}\left[\frac{1}{p}\right]$, pour n un entier premier à p

c) Plus généralement, soit $\mathcal{P}$ l'ensemble des nombres premiers. A toute fonction $h : \mathcal{P} \to \mathbf{Z} \cup \{-\infty\}$ qui est presque partout négative, on associe

$$\mathbf{Z}_h := \{x \in \mathbf{Q}, \forall p \in \mathcal{P},\ v_p(x) \geqslant h(p)\}$$

Montrer que $\mathbf{Z}_h$ est un sous-groupe de $\mathbf{Q}$ et que les quatre exemples précédents sont de cette forme.

d) Montrer que tous les sous-groupes de $(\mathbf{Q}, +)$ sont de la forme $\mathbf{Z}_h$.
[**Indication:** Commencer par traiter le cas des sous-groupes qui contiennent 1. Montrer qie si un tel sous-groupe contient une fraction $\frac{a}{p^k}$ alors il contient $\frac{1}{p^k}$. Quel est l'analogue de la décomposition en éléments simples dans $\mathbf{Q}$?]