Groupes abéliens de type fini

Exercice 1. —

a) Donner un exemple de groupe abélien qui n'est pas de type fini.

b) Si p est un nombre premier, quel est le groupe sous-jacent au corps $\mathbf{F}_{p^n}$?

c) Déterminer à isomorphisme près tous les groupes abéliens d'ordre 12 et 72.

d) Quels sont les facteurs invariants du groupe abélien $\mathbf{Z}/8 \times \mathbf{Z}/12 \times \mathbf{Z}/24$?

e) Déterminer le nombre de groupes abéliens d'ordre n en fonction de la décomposition de n en produit de facteurs premiers.

f) Soient $n, m \geqslant 1$ deux entiers. On note $\delta := \mathrm{pgcd}(n,m)$ et $\mu := \mathrm{ppcm}(n,m)$. Montrer l'isomorphisme de groupes

$$\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \approx \mathbf{Z}/\delta\mathbf{Z} \times \mathbf{Z}/\mu\mathbf{Z}.$$

g) Déterminer la structure des groupes abéliens de type fini suivants :

$$\mathbf{Z}^2/\langle (1;3),(2;0)\rangle \qquad \mathbf{Z}^2/\langle (1;1),(1;-1)\rangle.$$

h) Trouver une base du groupe suivant :

$$\left\{(x,y,z) \in \mathbf{Z}^3,\ \begin{array}{l} 2x+3y+5z=0 \\ 3x-6y+2z=0 \end{array}\right\}$$

i) A quelle condition nécessaire et suffisante sur $(b_1,b_2,b_3) \in \mathbf{Z}^3$ le système suivant admet-il au moins une solution (x,y,z) *entière* ?

$$\left\{\begin{array}{rcrcrl} 2x & - & y & + & z & = b_1 \\ -2x & + & 4y & + & 2z & = b_2 \\ -2x & + & 7y & + & 5z & = b_3 \end{array}\right.$$

j) Montrer que le sous-ensemble D de $\mathbf{Z}^n$ formés des n-uplets tels que $x_1^2 + \cdots + x_n^2$ est pair est un sous-groupe. Déterminer le groupe quotient $\mathbf{Z}^n/D$ et une base de D.

Exercice 2. — Soit n un entier naturel.

a) Soit G un groupe (quelconque). Etablir une bijection entre $\mathrm{Hom}_{\mathrm{gp}}(\mathbf{Z}^n, G)$ et le sous-ensemble de G^n formé des n-uplets d'éléments qui commutent deux à deux.

b) Soient A un groupe abélien et $\varphi : A \to \mathbf{Z}^n$ un morphisme de groupes surjectif. Montrer qu'il existe un morphisme $\psi : \mathbf{Z}^n \to A$ tel que $\varphi \circ \psi = \mathrm{id}_{\mathbf{Z}^n}$.

c) Montrer qu'un morphisme surjectif de $\mathbf{Z}^n$ dans $\mathbf{Z}^n$ est un isomorphisme.

Exercice 3. — Soient $n > 0$ un entier et $X_1 = \begin{bmatrix} x_{1,1} \\ \vdots \\ x_{n,1} \end{bmatrix}, \ldots, X_n = \begin{bmatrix} x_{1,n} \\ \vdots \\ x_{n,n} \end{bmatrix}$ des vecteurs de $\mathbf{Z}^n$.

a) Montrer que le sous-groupe H engendré par les X_i est libre de rang n ssi dét $(x_{i,j}) \neq 0$. Sous cette condition, montrer l'égalité $[G : H] = |\text{dét } (x_{i,j})|$.

b) A quelle condition la famille $\{X_i\}$ est-elle une base de $\mathbf{Z}^n$?

c) A quelle condition peut on compléter $\{X_1\}$ en une base de $\mathbf{Z}^n$?
Même question pour $\{X_1, \ldots, X_k\}$.

Exercice 4. — Soient L et M deux sous-groupes (libres) de $\mathbf{Z}^n$. Soit δ l'application :

$$\begin{aligned}\delta : L \times M &\to \mathbf{Z}^N \\ (\ell, m) &\mapsto \ell - m\end{aligned}$$

Montrer que $L \cap M$ est isomorphe au noyau de δ.
En pratique, étant données des bases $\{X_1, \ldots, X_k\}$ de L et $\{Y_1, \ldots, Y_\ell\}$ de M, comment calculer une base de $L \cap M$?

Exercice 5. — Soit $q = p^n$ une puissance d'un nombre premier et $\mathbf{F}_q$ « le » corps fini à q éléments.

a) Montrer que $\mathbf{F}_q^*$ est cyclique.
[**Indication:** Soit $d_1 | \ldots | d_r$ les facteurs invariants de $\mathbf{F}_q^*$. Considérer les racines dans $\mathbf{F}_q$ du polynôme $X^{d_r} - 1$.]

b) Donner tous les générateurs des groupes $(\mathbf{Z}/5)^\times$, $(\mathbf{Z}/7)^\times$ et $(\mathbf{Z}/11)^\times$.

Exercice 6. — Soient p un nombre premier *impair* et $k > 0$ un entier. On va montrer que le groupe $(\mathbf{Z}/p^k)^\times$ est cyclique.
Soit $\varphi : \mathbf{Z}/p^k \to \mathbf{Z}/p$ le morphisme de "réduction modulo p", *i.e.* : $\varphi(x \mod p^k) = x \mod p$.

a) Vérifier que φ est un morphisme d'anneaux bien défini.

b) Vérifier que φ induit (par restriction) un morphisme de groupes $\psi : (\mathbf{Z}/p^k)^\times \to (\mathbf{Z}/p)^\times$. Montrer que ψ est surjectif.

c) En utilisant l'exercice *5*, montrer qu'il existe un élément g d'ordre $p-1$ dans $(\mathbf{Z}/p^k)^\times$.
[**Indication:** Soit x un générateur de $(\mathbf{Z}/p)^\times$, montrer qu'un élément y tel que $\psi(y) = x$ est d'ordre multiple de $p-1$ et considérer les puissances de y.]

d) Soit $\langle g \rangle$ le sous-groupe engendré par g et soit Γ le noyau de ψ. Montrer que l'application

$$\begin{aligned}\langle g \rangle \times \Gamma &\to (\mathbf{Z}/p^k)^\times \\ (a, b) &\mapsto a \cdot b\end{aligned}$$

est un isomorphisme de groupes.

e) Montrer que pour tout entier $\ell \geqslant 0$, on a $(1+p)^{p^\ell} \equiv 1 + p^{\ell+1}\ [p^{\ell+2}]$.

f) Déduire de la question précédente que $\overline{1+p}$ engendre Γ.

g) En déduire que $(\mathbf{Z}/p^k)^\times$ est cyclique et même que l'élément $g \cdot \overline{(1+p)}$ en est un générateur.

h) Pour $k \geqslant 2$, montrer qu'un $x \in (\mathbf{Z}/p^k)^\times$ est générateur ssi sa réduction $\overline{x} \in (\mathbf{Z}/p^2)^\times$ est un générateur.
[**Indication:** Considérer les cardinaux des ensembles de générateurs de ces groupes.]

i) Soit $x \in \mathbf{Z}$ tel que $\overline{x}$ soit un générateur de $(\mathbf{Z}/p)^\times$. Montrer qu'on a l'alternative suivante : soit $\overline{x}$ soit $\overline{x+p}$ est un générateur de $(\mathbf{Z}/p^2)^\times$ et de tous les $(\mathbf{Z}/p^k)^\times$ pour tout $k \geqslant 2$.

j) Déterminer un générateur pour les groupes $(\mathbf{Z}/5^3)^\times$, $(\mathbf{Z}/7^2)^\times$ et $(\mathbf{Z}/11^{2014})^\times$.

Exercice 7. — **a)** Déterminer les groupes $(\mathbf{Z}/2)^\times$, $(\mathbf{Z}/4)^\times$ et $(\mathbf{Z}/8)^\times$. Sont-ils cycliques ?

b) Où la démonstration de l'exercice *6* ne marche-t-elle plus pour $p = 2$?

c) Montrer que pour $n \geqslant 2$ on a :

$$(\mathbf{Z}/2^n)^\times \cong (\mathbf{Z}/2) \times (\mathbf{Z}/2^{n-2})$$

Exercice 8. — Pour quels entiers n le groupe $(\mathbf{Z}/n)^\times$ est-il cyclique ?