3. Groupes (I)

Exercice 3.1 a) Montrer que tout sous-groupe additif de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un entier positif d. *[Utiliser la division euclidienne.]*

b) Soient m, n deux entiers strictement positifs. Décrire les sous-groupes additifs $m\mathbb{Z} + n\mathbb{Z}$ et $m\mathbb{Z} \cap n\mathbb{Z}$ de $\mathbb{Z}$.

Exercice 3.2 Soit $\mathbb{Q}$ l'ensemble des nombres rationnels muni de la loi de composition interne notée $*$ et définie par :

$$\begin{array}{lcl} \mathbb{Q} \times \mathbb{Q} & \to & \mathbb{Q} \\ (a,b) & \mapsto & a * b = a + b + ab \end{array}$$

$(\mathbb{Q}, *)$ est-il un groupe ? Même question pour $(\mathbb{Q} \setminus \{-1\}, *)$.

Exercice 3.3 a) Montrer que tout groupe monogène infini est isomorphe au groupe $(\mathbb{Z}, +)$.

b) Soit K un groupe fini de neutre 1_K et $x \in K$ un élément d'ordre $n \in \mathbb{N} \setminus \{0\}$. Montrer que pour un entier m on a $x^m = 1_K$ ssi $m \in n\mathbb{Z}$.

c) Soit $n \in \mathbb{N} \setminus \{0\}$. Donner un exemple de groupe cyclique d'ordre n. Est-il unique à isomorphisme près?

d) Soit $GL_2(\mathbb{C})$ le groupe des matrices complexes inversibles de type 2×2. Que peut-on dire du sous-groupe de $GL_2(\mathbb{C})$ engendré par $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ pour $z \in \mathbb{C}$ fixé? Par $\begin{pmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{\frac{-2\pi i}{n}} \end{pmatrix}$?

e) Trouver tous les éléments du sous-groupe engendré par la matrice : $\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$. Quel est son ordre ?

Exercice 3.4 Soit G un groupe fini et soit a un élément de G. On note $\mathrm{ord}(a) = m$, l'ordre de a. C'est le plus petit entier positif s tel que $a^s = 1_G$.

1. Montrer que si $a^k = 1_G$, alors m divise k.
2. Soit b un élément de G , posons $\mathrm{ord}(b) = n$ et supposons que a et b commutent, c'est-à-dire $ab = ba$. Montrer que $\mathrm{ord}(ab)$ est fini et divise $\mathrm{PPCM}(m, n)$. Montrer que $\mathrm{ord}(ab) = mn$ si et seulement si m et n sont premiers entre eux.
3. Soit $k \in \mathbb{Z}$, montrer que l'ordre de a^k est $m/\mathrm{PGCD}(m, k)$.
   Application. Trouver le nombre de générateurs d'un groupe cyclique d'ordre m.

Exercice 3.5 Le but de cet exercice est de démontrer que le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$, noté $\mathbb{F}_5^*$, est isomorphe au groupe additif $\mathbb{Z}/4\mathbb{Z}$.

1. Dresser la table d'addition de $\mathbb{Z}/4\mathbb{Z}$ et la table de multiplication de $\mathbb{F}_5^*$. Préciser le neutre et les ordres des éléments de chaque groupe.
2. Construire un isomorphisme entre $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{F}_5^*$.

Exercice 3.6 a) Soient K et K' deux groupes de neutres respectifs 1_K et $1_{K'}$. Définir une structure *naturelle* de groupe sur le produit cartésien $K \times K'$.

b) Montrer que tout morphisme injectif $f : K \to K'$ préserve l'ordre des éléments.

c) En déduire que les groupes $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ne sont pas isomorphes.

d) Donner deux exemples de groupes d'ordre 6 non isomorphes entre eux.

Exercice 3.7 Soit A une partie non vide d'un groupe G. Montrer que :

1. le normalisateur de A :
$$N(A) = \{g \in G \text{ tel que } gA = Ag\}$$
est un sous-groupe de G.

2. le centralisateur de A :
$$C(A) = \{c \in G \text{ tel que } ca = ac,\ \forall a \in A\}$$
est un sous-groupe distingué de $N(A)$. Montrer que si on prend $A = G$, alors $Z(G) = C_G(G)$, appelé le centre de G, est un sous-groupe abélien, invariant par chaque automorphisme de G.

Exercice 3.8 Soit G un groupe cyclique d'ordre n. En utilisant le théorème de factorisation des morphismes de groupes, démontrer que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Exercice 3.9 Montrer que $\mathbb{Z}$ et $\mathbb{Z}^2$ sont deux groupes non isomorphes.

Exercice 3.10 Montrer que tout sous-groupe et tout groupe quotient d'un groupe cyclique est cyclique.

Exercice 3.11 Soient G un groupe fini et H un sous-groupe de G.

1. Montrer que toutes les classes à gauche xH (resp. à droite Hx) ont le même cardinal.
2. On note $(G/H)_g$ (resp. $(G/H)_d$) l'ensemble des classes d'équivalence des éléments de G pour la relation à gauche (resp. à droite) modulo H. Montrer que les ensembles $(G/H)_d$ et $(G/H)_g$ ont le mme cardinal.

Exercice 3.12 Montrer qu'un sous-groupe d'indice 2 est toujours distingué.

Exercice 3.13 Deux éléments x, y d'un groupe G sont conjugués s'il existe $g \in G$ tel que $x = g\,y\,g^{-1}$.

1. Montrer que la conjugaison est une relation d'équivalence.
2. Quelle est la classe de l'élément neutre e ?
3. Montrer que deux éléments d'une mme classe ont le même ordre.

Exercice 3.14 Soit H le sous-ensemble de $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ définit par

$$H = \{(0,0),(1,2),(2,0),(3,2)\}\,.$$

Montrer que H est un sous-groupe distingué, puis que

$$(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})/H \simeq \mathbb{Z}/4\mathbb{Z}.$$

Donner un générateur du quotient.

Exercice 3.15 Soit G un groupe d'ordre 6.

1. On suppose que G est abélien. Montrer que $G \simeq \mathbb{Z}/6\mathbb{Z}$
2. On suppose que G est non abélien. Montrer que $G \simeq S_6$.

Exercice 3.16

1. Est-ce que le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est isomorphe au groupe $\mathbb{Z}/8\mathbb{Z}$? au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?
2. Est-ce que le groupe $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ est isomorphe au groupe $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/36\mathbb{Z}$? Trouver toutes les manières de décomposer $\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ comme produit de groupes cycliques.

Exercice 3.17 On désigne par $GL_n(K)$ le groupe des matrices inversibles de taille n à coefficients dans le corps K et par $SL_n(K) \subset GL_n(K)$ l'ensemble des matrices de determinant 1_K.

a) Montrer que $Sl_n(K)$ est un sous-groupe distingué de $Gl_n(K)$.

b) Montrer que l'application $\rho : GL_n(K) \longrightarrow K^\times \times SL_n(K)$

$$A \mapsto \big(Det(A), \begin{pmatrix} \frac{1}{Det(A)} & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} A\big)$$

est une bijection. En déduire une structure de groupe sur $K^\times \times SL_n(K)$ telle que ρ soit un isomorphisme de groupes.
(On dit que $GL_n(K)$ est le *produit semi-direct* de $K^\times$ par $SL_n(K)$.)

On suppose à présent $K = \mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{N}$ premier.

c) Déterminer le cardinal de $GL_n(K)$. En déduire le cardinal de $SL_n(K)$. Que peut-on dire lorsque $n = 2$?

d) Faire la liste des éléments de $GL_2(\mathbb{Z}/2\mathbb{Z})$ et dresser sa table de composition. Conclure que $GL_2(\mathbb{Z}/2\mathbb{Z})$ est isomorphe au groupe de permutations S_3.

Exercice 3.18 (Quaternions de Hamilton.)

On considère les quaternions

$$H = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \quad a, b \in \mathbb{C} \right\}.$$

Pour $h = (h_{ij}) \in H$ on note $h^\star = (\overline{h_{ji}})$.

a) Montrer que la sphère unité

$$S^3 = \left\{ h \in H \mid hh^\star = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

est un groupe pour la multiplication matricielle.

b) Déterminer le sous-groupe $H_8 =< K, I >$ de la sphère S^3 engendré par

$$K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

c) Expliciter tous les sous-groupes de H_8. Quel est son centre?

Exercice 3.19 (Les réflexions engendrent le groupe orthogonal.)

On désigne par $O(V)$ le groupe des transformations orthogonales d'un espace euclidien $(V, (\,|\,))$. Soit $s : V \to V$ une symétrie (i.e. $s : V \to V$ est linéaire et $s \circ s = \mathrm{Id}_V$) et $V = V_+^s \oplus V_-^s$ la décomposition de V en sous-espaces propres $V_\pm^s = \{v \in V,\, s(v) = \pm v\}$.

1) Montrer que $s \in O(V)$ ssi $V_-^s = (V_+^s)^\perp$.

2) On appelle *réflexion* toute symétrie orthogonale $s \in O(V)$ pour laquelle $\dim V_+^s = \dim V - 1$. On se propose de montrer, par une récurrence sur $n = \dim V$, le résultat d'engendrement suivant:
"*quel que soit* $f \in O(V)$ *il existe* $p\,(\leq n)$ *réflexions* $s_1, \ldots, s_p \in O(V)$ *telles que* $f = s_1 \circ s_2 \circ \cdots \circ s_p$."

Après avoir vérifié le cas trivial ($n = 1$), on procède comme suit:

- On suppose $n \geq 2$ et $f \in O(V) \setminus \{\mathrm{Id}_V\}$. Soit $v \in V$ tel que $f(v) \neq v$ et soit s la réflexion d'hyperplan fixe $V_+^s = \langle v - f(v) \rangle^\perp$.
- Montrer que $(s \circ f)(v) = v$ et en déduire que $(s \circ f)(\langle v \rangle^\perp) = \langle v \rangle^\perp$.
- Etablir le pas de récurrence ($n \Rightarrow n + 1$) en considérant la somme directe

$$V = \langle v \rangle \oplus \langle v \rangle^\perp$$

et en appliquant l'hypothèse de récurrence à la restriction $(s \circ f)_{|_{\langle v \rangle^\perp}} \in O(\langle v \rangle^\perp)$.