1. Groupes : sous-groupes, morphismes, premiers exemples

Rappel : Sous-groupe
Un sous-ensemble non vide H d'un groupe G est un sous-groupe ssi H est stable par composition et passage au symétrique.

Exercice 1. Décrire tous les sous-groupes de $\mathbb{Z}$.

Exercice 2. Décrire tous les sous-groupes du groupe symétrique S_3.

Exercice 3. On note D_4 le groupe des isométries du carré pour la composition des applications (on l'appelle le quatrième groupe diédral, d'où la notation). Quel est l'ordre de ce groupe ? Quel est l'ordre de chacun de ses éléments ? Est-ce un groupe cyclique ? Est-ce un groupe commutatif ?

Exercice 4. Soit $\mathbb{H}_8$ le sous-groupe de $GL_2(\mathbb{C})$ engendré par les matrices

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

Calculer l'ordre de $\mathbb{H}_8$ et expliciter tous ses sous-groupes. Quel est son centre ?

Exercice 5. Montrer que le groupe $\mathrm{SL}(2,\mathbb{Z}/2\mathbb{Z})$ est isomorphes à un groupe symétriques S_n avec n que l'on déterminera. *Indication : combien y-a-t'il de sous-espaces vectoriels de dimension 1 dans le $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel* $(\mathbb{Z}/2\mathbb{Z})^2$ *?* Question subsidiaire : même question pour $\mathrm{PGL}(2,\mathbb{Z}/3\mathbb{Z})$...

Rappel : Morphisme de groupes
On dit qu'une application $f : G_1 \to G_2$ entre deux groupes est un morphisme si pour tous $x, y \in G_1$ on a $f(x.y) = f(x).f(y)$.

Exercice 6.

1. Soit $f : G_1 \to G_2$ un morphisme de groupes. Montrer que $f(e_1) = e_2$, et pour tout $x \in G_1$, on a $f(x^{-1}) = f(x)^{-1}$ (f envoie neutre sur neutre et symétrique sur symétrique).
2. Montrer que dans un groupe G il existe un unique élément neutre, et que tout $x \in G$ admet un unique symétrique.

Exercice 7.

1. Donner un exemple de morphisme de groupe de $(\mathbb{R},+)$ vers $(\mathbb{R}^*,.)$. Est-ce un isomorphisme ?
2. L'ensemble des bijections croissantes de $\mathbb{R}$ dans $\mathbb{R}$ est-il un groupe ? Et pour les décroissantes ?
3. Est-il possible de définir une loi $*$ sur l'ensemble des entiers positifs $\mathbb{N}$ de façon à ce que $(\mathbb{N},*)$ devienne un groupe ?

Exercice 8.

1. Donner deux exemples de groupes d'ordre 4 non isomorphes entre eux.
2. Donner deux exemples de groupes d'ordre 6 non isomorphes entre eux.
3. Donner cinq exemples de groupes d'ordre 8 non isomorphes entre eux.

> **Rappel : Groupe engendré**
> Soit G un groupe et S une partie de G. On note $\langle S\rangle$ le plus petit sous-groupe de G contenant S. On dit que $\langle S\rangle$ est le sous-groupe engendré par S. Si $\langle S\rangle = G$, on dit que S est une partie génératrice de G.

Exercice 9. Donner une partie génératrice la plus petite possible du groupe $\mathbb{Z}/6\mathbb{Z}$. Y a-t-il plusieurs choix possibles ? Mêmes questions pour les groupes S_3, $\mathbb{H}_8$ et $\mathbb{Z}^n$.

Exercice 10.

1. Donner un exemple de sous-groupe additif de $\mathbb{R}$ dense de type fini (c'est-à-dire engendré par un nombre fini d'éléments).
2. Tous les sous-groupes de $\mathbb{R}$ sont-ils de type fini ?
3. Montrer que les sous-groupes additifs de $\mathbb{R}$ sont soit monogènes soit denses.

> **Rappel : Ordre d'un groupe, ordre d'un élément**
> On dit qu'un groupe G est d'ordre n s'il contient n éléments.
> L'ordre d'un élément $x \in G$ est le plus petit entier strictement positif m tel que $x^m = 1$ (en notation multiplicative).

Exercice 11. Soit n un entier strictement positif.

1. Montrer que tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique. (On pourra pour cela utiliser le morphisme $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui a un entier k associe sa classe dans $\mathbb{Z}/n\mathbb{Z}$). En déduire que tout sous-groupe d'un groupe cyclique est cyclique.
2. Montrer que pour tout d divisant n, $\mathbb{Z}/n\mathbb{Z}$ possède un unique sous-groupe d'ordre d.
   Indication : considérer l'ensemble $H := \{\overline{k} \in \mathbb{Z}/n\mathbb{Z}; \overline{dk} = \overline{0}\}$.
3. L'indicatrice d'Euler $\varphi(m)$ est définie comme le nombre d'éléments inversibles dans $\mathbb{Z}/m\mathbb{Z}$. Montrer que le nombre d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $\varphi(d)$.
4. En déduire une démonstration de la relation $n = \sum_{d|n} \varphi(d)$.

Exercice 12.

1. Donner un exemple de groupe commutatif G et de deux éléments $a, b \in G$ tous deux d'ordre 4 tels que le produit ab soit d'ordre 1 ? d'ordre 2 ? d'ordre 4 ?
2. En général, montrer que dans un groupe commutatif G, si $\text{ordre}(a) = n$ et $\text{ordre}(b) = m$ alors $\text{ordre}(ab)$ divise $\text{PPCM}(\text{ordre}(a),\text{ordre}(b))$.
3. Est-il possible d'avoir un groupe G et deux éléments d'ordre 2 $x, y \in G$ tel que $x.y$ soit d'ordre infini (si oui, donner un exemple; si non, donner un court argument)?
4. Est-il possible d'avoir un groupe infini dont tous les éléments sont d'ordre fini ?

Exercice 13.

1. Soit G un groupe fini d'ordre n tel que pour tout diviseur d de n, il y ait au plus d éléments g de G vérifiant $g^d = 1$. Montrer que G est cyclique (indication : utiliser l'exercice 11)
2. Montrer que pour tout p premier, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.