3. Groupes : exemples, sous-groupes et ordres

Exercice 1. Soit $\mathbb{Q}$ l'ensemble des nombres rationnels muni de la loi de composition interne

$$* \ : \ \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, \ (a,b) \mapsto a * b = a + b + ab.$$

Cette loi fait-elle de $\mathbb{Q}$ un groupe ? Reprendre la question avec $(\mathbb{Q} - \{-1\}, *)$.

Exercice 2. Soit G un ensemble *fini* muni d'une loi de composition interne $\mathrm{G} \times \mathrm{G} \to \mathrm{G}, \ (a,b) \mapsto a \cdot b.$
On fait les hypothèses suivantes :
- cette loi est associative ;
- quels que soient les éléments a, b et c de G,

$$(a \cdot b = a \cdot c \implies b = c) \quad \text{et} \quad (b \cdot a = c \cdot a \implies b = c).$$

(On dit que tout élément de G est *simplifiable* à gauche et à droite.)
1. Étant donné un élément a de G, démontrer qu'il existe un et un seul un élément e_a de G tel que $a \cdot e_a = e_a \cdot a = a$.
2. Vérifier que l'on a $e_a = e_b$ pour tous éléments a et b de G.
3. En conclure que G est un groupe.

Exercice 3. Soit G un groupe d'élément neutre e. Démontrer que, si $g^2 = e$ pour tout élément g de G, alors G est abélien. (*Indication : calculer l'inverse du produit gh de deux éléments g, h de* G.)

Exercice 4. (*Le groupe des quaternions*) Soit $\mathbb{H}_8$ l'ensemble des huit matrices complexes suivantes :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

1. Vérifier que $\mathbb{H}_8$ est un sous-groupe du groupe $\mathrm{SL}(2, \mathbb{C})$ et déterminer l'ordre de chacun de ses éléments.
2. Le groupe $\mathbb{H}_8$ est-il abélien ?
3. Posons

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ \text{et} \ b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Vérifier que le groupe $\mathbb{H}_8$ est engendré par les éléments a et b.

Exercice 5. Démontrer que les groupes $\mathbb{Z}$ et $\mathbb{Z}^2$ ne sont pas isomorphes.

Exercice 6. Soit G un groupe d'ordre 4.
1. Quelles sont les valeurs possibles pour l'ordre d'un élément g de G ?
2. S'il existe un élément $g \in \mathrm{G}$ d'ordre 4, démontrer que G est cyclique et engendré par g.
3. Si $g^2 = e$ pour tout élément $g \in \mathrm{G}$, démontrer que G est isomorphe au groupe produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
4. En déduire que tout groupe d'ordre 4 est isomorphe au groupe $\mathbb{Z}/4\mathbb{Z}$ ou au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et justifier que ces deux groupes ne sont pas isomorphes.

Exercice 7. Vérifier que l'ensemble

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ ; \ a, b \in \mathbb{R} \ \text{ et } \ a^2 + b^2 \neq 0 \right\}$$

est un sous-groupe du groupe $\mathrm{GL}(2, \mathbb{R})$ puis démontrer qu'il est isomorphe au groupe multiplicatif $\mathbb{C}^\times$. (Écrire un isomorphisme explicite.)

Exercice 8. Soit p un nombre premier. Démontrer que tout groupe fini d'ordre p est cyclique.

Exercice 9. Soit k un corps. Démontrer que tout groupe fini est isomorphe à un sous-groupe du groupe linéaire $\mathrm{GL}(\mathrm{N}, k)$ pour un entier N convenable. (*Indication : utiliser le théorème de Cayley...*)

Exercice 10. Soient a et b des éléments d'ordre p et q dans un groupe G. On suppose que p et q sont premiers entre eux.

1. Si a et b commutent, démontrer que ab est d'ordre pq.

2. Donner un exemple mettant ce résultat en défaut si a et b ne commutent pas. (*Indication : on pourra chercher parmi les groupes d'ordre* 6...)

3. Soit G un groupe abélien fini et soit d le ppcm des ordres des éléments de G. Démontrer que G contient un élément d'ordre d.

Exercice 11. (*Groupes cycliques finis*) Soit G un groupe cyclique fini d'ordre n.

1. Soit g un générateur de G et soit H un sous-groupe de G. Démontrer que H est cyclique et engendré par g^k, où k est le plus petit nombre entier strictement positif tel que $g^k \in \mathrm{H}$.

2. Démontrer que, pour tout diviseur d de n, G possède un unique sous-groupe d'ordre d.

3. Démontrer que, pour tout diviseur d de n, G possède exactement $\varphi(d)$ éléments d'ordre d. En déduire une nouvelle démonstration de l'identité suivante (établie à l'exercice 5 de la fiche 2) :

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

Exercice 12. (*Groupes cycliques finis, suite*) Soit G un groupe fini d'ordre n satisfaisant à la condition suivante :

pour tout diviseur d de n, il existe au plus d éléments $g \in \mathrm{G}$ tels que $g^d = e$.

1. Étant donné un diviseur d de n, démontrer qu'il existe au plus $\varphi(d)$ éléments d'ordre d dans G. (*Indication : si* G *possède un élément g d'ordre d, comparer $\{h \in \mathrm{G} \mid h^d = e\}$ et le sous-groupe de* G *engendré par g...*)

2. En conclure que le groupe G est cyclique. (*Indication : utiliser la dernière question de l'exercice précédent.*)

3. Soit p un nombre premier. Démontrer que le groupe multiplicatif $\mathbb{F}_p^\times = \mathbb{F}_p - \{0\}$ du corps fini $\mathbb{F}_p$ est cyclique.

4. Déterminer un générateur explicite de $\mathbb{F}_p^\times$ pour tout nombre premier $p \leq 11$ ainsi que pour $p = 43$ et $p = 71$. (*Indication : utiliser l'exercice 8*)

Exercice 13. Combien y a-t-il d'homomorphismes du groupe $(\mathbb{Z}/8\mathbb{Z})^\times$ dans le groupe $\mathfrak{S}_3$?

Exercice 14. Soit G un groupe et soit H un sous-groupe de G. On note G/H l'ensemble des classes à droite modulo H et on désigne par $p : \mathrm{G} \to \mathrm{G}/\mathrm{H}$ l'application définie par $p(g) = g\mathrm{H}$.

Démontrer que les assertions suivantes sont équivalentes :

(i) il existe une structure de groupe sur G/H telle que p soit un homomorphisme de groupes ;

(ii) H est un sous-groupe distingué.

En guise d'application, en déduire que tout sous-groupe de G d'indice 2 est distingué.

Exercice 15. Le *centre* d'un groupe G est l'ensemble $\mathrm{Z} = \{g \in \mathrm{G} \mid gh = hg \text{ pour tout } h \in \mathrm{G}\}$.

1. Vérifier que Z est un sous-groupe distingué de G. À quelle condition a-t-on Z = G ?

2. Déterminer le centre des groupes suivants : $\mathfrak{S}_n$, $\mathrm{GL}(\mathrm{N}, \mathbb{Q})$, $\mathbb{H}_8$ (cf. exercice 4).

3. Démontrer que le groupe G est abélien si et seulement si le groupe quotient G/Z est cyclique.

Exercice 16. 1. Vérifier que le groupe symétrique $\mathfrak{S}_3$ est engendré par les permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

2. Déterminer les classes à droite et à gauche de $\mathfrak{S}_3$ modulo le sous-groupe $\{1, \tau\}$.

Exercice 17. Soient H et K deux sous-groupes d'un groupe G tels que $\mathrm{K} \subset \mathrm{H}$. On suppose que H est d'indice fini dans G et que K est d'indice fini dans H. Démontrer que K est d'indice fini dans G et que l'on a

$$(\mathrm{G} : \mathrm{K}) = (\mathrm{G} : \mathrm{H})(\mathrm{H} : \mathrm{K}).$$

Exercice 18. Soit G le sous-groupe de $\mathrm{GL}(2, \mathbb{Q})$ engendré par les matrices $\mathrm{A} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\mathrm{B} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.

Vérifier que l'on a $\mathrm{A}^2 = \mathrm{B}^2 = 1$ puis démontrer que tout élément de $\mathrm{G} - \{1\}$ s'écrit d'une manière et d'une seule sous la forme $\mathrm{X}_1\mathrm{X}_2 \ldots \mathrm{X}_n$ avec $\mathrm{X}_i \in \{\mathrm{A}, \mathrm{B}\}$ et $\mathrm{X}_{i+1} \neq \mathrm{X}_i$; en particulier, le groupe G est *infini*. Vérifier également que G contient un élément $g \in \mathrm{G}$ tel que $g^n \neq 1$ pour tout $n \geq 1$.