Université Aix-Marseille 2021–2022

**Licence – Mathématiques**
**Algèbre 2**

TD2 : Groupes

# Généralités

**Exercice 1.**

1. L'addition munit-elle les ensembles ci-dessous d'une structure de groupe ?

$$\mathbb{N},\ \mathbb{N}^*,\ \mathbb{Z},\ \mathbb{Z}^*,\ \mathbb{Q},\ \mathbb{Q}^*,\ \mathbb{R},\ \mathbb{R}^*,\ \mathbb{C},\ \mathbb{C}^*,\ \{k \in \mathbb{Z} \mid k \text{ pair}\},\ \{k \in \mathbb{Z} \mid k \text{ impair}\}$$

2. Même question avec la multiplication.

**Exercice 2.** Montrer que les ensembles suivants, munis de l'opération indiquée, définissent des groupes, dont on précisera le caractère abélien ou non :

1. $\big(]-1,1[,*\big)$ avec $x * y := \frac{x+y}{1+x.y}$ ;
2. $\big(\mathbb{R}^2,*\big)$ avec $(x_1,x_2)*(y_1,y_2) := (x_1+y_1, x_2.e^{y_1}+y_2.e^{x_1})$ ;
3. $(L,\circ)$, où $L$ est l'ensemble des applications de la forme $\left\{\begin{array}{ccc} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & ax+b \end{array}\right.$ avec $a \in \mathbb{R}^*$ et $b \in \mathbb{R}$ ;
4. $\big(\mathcal{R}_{ABC},\circ\big)$ où $\mathcal{R}_{ABC}$ est l'ensemble des rotations laissant globalement invariant un triangle équilatéral $ABC$ du plan $\mathbb{R}^2$ ;
5. $\big(\mathrm{SL}_2(\mathbb{Z}),\times\big)$, où $\mathrm{SL}_2(\mathbb{Z})$ est l'ensemble des matrices $2\times 2$ à coefficient entiers et dont le déterminant vaut $1$ ;
6. $\big(\mathcal{P}(E),\Delta\big)$, où $E$ est un ensemble, $\mathcal{P}(E)$ l'ensemble des sous-ensembles de $E$, et $A\Delta B := (A\cup B)\setminus(A\cap B)$ la différence symétrique de $A, B \in \mathcal{P}(E)$.

**Exercice 3.** On pose

$$f_1 : \begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & z \end{array} \qquad f_2 : \begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & \frac{1}{z} \end{array} \qquad f_3 : \begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & -z \end{array} \qquad f_4 : \begin{array}{ccc} \mathbb{C}^* & \longrightarrow & \mathbb{C}^* \\ z & \longmapsto & -\frac{1}{z} \end{array}.$$

Montrer que $\big(\{f_1,f_2,f_3,f_4\},\circ\big)$ est un groupe abélien d'ordre 4.

**Exercice 4.** On note $\mathfrak{S}_3$ le groupe des bijections de l'ensemble $\{1,2,3\}$, muni de la composition. Expliciter les éléments du groupe $\mathfrak{S}_3$, donner son ordre, l'ordre de chacun de ses éléments, et écrire sa table de loi.

**Exercice 5.** Soit $G$ un groupe, $g_1, g_2 \in G$. Montrer que

1. $(g_1.g_2.g_1^{-1})^n = g_1.g_2^n.g_1^{-1}$ pour tout $n \in \mathbb{Z}$ ;
2. si $(g_1.g_2)^n = e$ avec $n \in \mathbb{N}^*$, alors $(g_2.g_1)^n = e$ ;
3. si $g_1^{-1}.g_2.g_1 = g_2^{-1}$ et $g_2^{-1}.g_1.g_2 = g_1^{-1}$, alors $g_1^2 = g_2^2$ et $g_1^4 = g_2^4 = e$.

**Exercice 6.** Soit $G$ un groupe.

1. Soit $x \in G$. Comparer l'ordre de $x$ et l'ordre de $x^{-1}$.
2. Soient $x, y \in G$. Comparer l'ordre de $xy$ et l'ordre de $yx$.
3. (a) On suppose que $G$ est abélien. Soient $x, y \in G$ des éléments d'ordre fini dont les ordres sont premiers entre eux. Déterminer l'ordre de $xy$.
   (b) Trouver un contre-exemple lorsque $G$ n'est pas abélien (on pourra penser au groupe $\mathfrak{S}_3$ de l'exercice 4).

**Exercice 7.** Les ensembles suivants sont-ils des sous-groupes de $(\mathbb{R}^*, .)$ ?

$$\{-1,1\} \qquad \left\{1, \frac{1}{5}, 5\right\} \qquad \{3^k \mid k \in \mathbb{Z}\} \qquad \mathbb{N}^* \qquad \mathbb{Z}^* \qquad \mathbb{Q}^* \qquad \mathbb{R}_+^* \qquad \mathbb{R}_-^*$$

**Exercice 8.** On note $j = e^{\frac{2i\pi}{3}}$.

1. Déterminer le sous-groupe de $(\mathbb{C}, +)$ engendré par $i$ et $j$.
2. Déterminer le sous-groupe de $(\mathbb{C}^*, .)$ engendré par $i$ et $j$.

**Exercice 9.**

1. Soit $H \subset \mathbb{Z}$ un sous-groupe. Montrer qu'il existe $n \in \mathbb{N}$ tel que $H = n\mathbb{Z}$.
2. Soit $a, b \in \mathbb{Z}^*$. Déterminer les groupes $\langle a, b\rangle$ et $a\mathbb{Z} \cap b\mathbb{Z}$.
3. Soit $a_1, \dots, a_n \in \mathbb{Z}^*$. Déterminer les groupes $\langle a_1, \dots, a_n\rangle$ et $\cap_{1\leq i\leq n} a_i\mathbb{Z}$.

**Exercice 10.** Soit $G$ un groupe et $H_1, H_2 \subset G$ deux sous-groupes tels que $H_1 \cup H_2$ soit un sous-groupe. Montrer que parmi $H_1$ et $H_2$, il y en a un qui est inclu dans l'autre.

**Exercice 11.** Déterminer une famille génératrice du groupe multiplicatif $\mathbb{Q}^*$. Existe-t-il une famille génératrice finie ?

**Exercice 12.** Soit $G$ un groupe.

1. Soit $g \in G$. Montrer que $Z(g) := \{h \in G \mid g.h = h.g\}$ est un sous-groupe de $G$. C'est ce qu'on appelle le *centralisateur de $g$*.
2. Montrer que $Z(G) := \{g \in G \mid \forall h \in G, g.h = h.g\}$ est un sous-groupe de $G$. C'est ce qu'on appelle le *centre de $G$*.
3. Montrer que $Z(G) = \cap_{g\in G} Z(g)$.

**Exercice 13.** Soit $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On munit $G_1 \times G_2$ de la loi de composition interne

$$* : \begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2) & \longrightarrow & G_1 \times G_2 \\ \big((g_1, g_2), (h_1, h_2)\big) & \longmapsto & (g_1 *_1 h_1, g_2 *_2 h_2) \end{array}.$$

Montrer que $(G_1 \times G_2, *)$ est un groupe. C'est ce qu'on appelle la structure de *groupe produit*.

**Exercice 14.** Soit $G$ un groupe dont tous les éléments sont d'ordre 2.

1. Montrer que $G$ est abélien.
2. On suppose maintenant que $G$ est de plus fini.
   (a) Soit $H \subset G$ un sous-groupe et $g \in G \setminus H$. Montrer que $|\langle H \cup \{g\}\rangle| = 2|H|$.
   (b) En déduire que $|G|$ est une puissance de 2.

**Exercice 15.**

1. Montrer que les isométries du plan $\mathbb{R}^2$ forment un groupe pour la composition.
2. Soit $n \in \mathbb{N}^* \setminus \{1, 2\}$. On considère $A_1, \dots, A_n$ les sommets d'un polygone régulier à $n$ côtés.
   (a) Montrer que les isométries laissant l'ensemble $\{A_1, \dots, A_n\}$ globalement stable [1] est un sous-groupe des isométries du plan. Ce groupe est appelé *groupe diédral*, noté [2] $D_n$.
   (b) Montrer que $D_n$ contient un élément d'ordre $n$ et un élément d'ordre 2.
   (c) Montrer que tout élément de $D_n$ est entièrement déterminé par l'image de $A_1$ et $A_2$. En déduire que $|D_n| = 2n$.

1. c'est-à-dire l'ensemble des isométries $f$ telle que $f(\{A_1, \dots, A_n\}) = \{A_1, \dots, A_n\}$
2. on le trouve aussi parfois noté $D_{2n}$, il faut donc toujours faire attention à la convention utilisée

## Morphismes de groupes

**Exercice 16.** Parmi les applications suivantes, dire lesquelles sont des morphismes de groupes.

- $\begin{array}{ccc} (\mathbb{C},+) & \longrightarrow & (\mathbb{C},+) \\ z & \longmapsto & \overline{z} \end{array}$ ;
- $\begin{array}{ccc} (\mathbb{C}^*,.) & \longrightarrow & (\mathbb{C}^*,.) \\ z & \longmapsto & \overline{z} \end{array}$ ;
- $\begin{array}{ccc} (\mathbb{C},+) & \longrightarrow & (\mathbb{R},+) \\ z & \longmapsto & |z| \end{array}$ ;
- $\begin{array}{ccc} (\mathbb{C}^*,.) & \longrightarrow & (\mathbb{R}^*,.) \\ z & \longmapsto & |z| \end{array}$ ;
- $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & (\{\pm 1\},.) \\ n & \longmapsto & \begin{cases} 1 & \text{si } n \text{ pair} \\ -1 & \text{si } n \text{ impair} \end{cases} \end{array}$ ;
- $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & (\{\pm 1\},.) \\ n & \longmapsto & \begin{cases} 1 & \text{si } n \text{ impair} \\ -1 & \text{si } n \text{ pair} \end{cases} \end{array}$ ;
- $\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & n^2 \end{array}$ ;
- $\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ \overline{n} & \longmapsto & \overline{n}^2 \end{array}$ ;
- $\det : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ ;
- $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$ ;
- $\mathrm{Tr} : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$ ;
- $\mathrm{Tr} : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}$ ;
- $\begin{array}{ccc} \big(C^\infty(\mathbb{R},\mathbb{R}),+\big) & \longrightarrow & \big(C^\infty(\mathbb{R},\mathbb{R}),+\big) \\ f & \longmapsto & f' \end{array}$ ;
- $\begin{array}{ccc} \big(C^\infty(\mathbb{R},\mathbb{R}^*),.\big) & \longrightarrow & \big(C^\infty(\mathbb{R},\mathbb{R}^*),.\big) \\ f & \longmapsto & f' \end{array}$

où $C^\infty(\mathbb{R},\mathbb{R}^{(*)})$ représente l'ensemble des fonctions infiniment dérivables de $\mathbb{R}$ dans $\mathbb{R}^{(*)}$.

**Exercice 17.** On considère l'application

$$f : \begin{array}{ccc} \mathbb{Z}/8\mathbb{Z} & \longrightarrow & \mathbb{Z}/12\mathbb{Z} \\ \overline{k} & \longmapsto & \overline{3k} \end{array}.$$

1. Montrer que $f$ est bien définie.
2. Montrer que $f$ est un morphisme de groupes.
3. Déterminer $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

**Exercice 18.** On considère $\mathcal{F}(\mathbb{R},\mathbb{R})$ l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$ et

$$\sigma : \begin{array}{ccc} \mathcal{F}(\mathbb{R},\mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R},\mathbb{R}) \\ f & \longmapsto & x \mapsto \frac{1}{2}\big(f(x)+f(-x)\big) \end{array}.$$

1. Montrer que $\big(\mathcal{F}(\mathbb{R},\mathbb{R}),+\big)$ est un groupe.
2. Montrer que $\sigma$ est un endomorphisme de groupe.
3. Caractériser l'image et le noyau de $\sigma$.

**Exercice 19.** Soit $n, m \in \mathbb{N}^*$ et $n', m'$ tels que $n = n'.\mathrm{pgcd}(n,m)$ et $m = m'.\mathrm{pgcd}(n,m)$. On considère l'application

$$\mathrm{mult}_m^n : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ \overline{k} & \longmapsto & \overline{m}.\overline{k} \end{array}.$$

1. Montrer que $\mathrm{mult}_m^n$ est un endomorphisme de groupe.
2. Soit $k \in \mathbb{N}^*$ tel que $\overline{k} \in \mathrm{Ker}(\mathrm{mult}_m^n)$. Montrer que $n' \mid k$.
3. En déduire que $\mathrm{Ker}(\mathrm{mult}_m^n)$ est engendré par la classe de $\frac{n}{\mathrm{pgcd}(n,m)}$ dans $\mathbb{Z}/n\mathbb{Z}$.

**Exercice 20.**

1. Montrer qu'un endomorphisme de groupe $f : \mathbb{Z} \to \mathbb{Z}$ est entièrement déterminé par $f(1)$. En déduire tous les endomorphismes, puis tous les automorphismes de $\mathbb{Z}$.
2. Déterminer tous les endomorphismes, puis tous les automorphismes de $\mathbb{Q}$.
3. Déterminer tous les endomorphismes continus de $\mathbb{R}$.

**Exercice 21.** Soit $G$ un groupe. Montrer que l'application

$$\begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & g^{-1} \end{array}$$

est un morphisme de groupe si et seulement si $G$ est abélien.

**Exercice 22.** Soit $f : G_1 \to G_2$ un morphisme de groupes.

1. Soit $g \in G_1$ un élément d'ordre fini. Montrer que $|f(g)|$ est fini et qu'il divise $|g|$.
2. Soit $H \subset G_1$ un sous-groupe fini. Montrer que $f(H) \subset G_2$ est fini et que $|f(H)|$ divise $|H|$.

**Exercice 23.** Soit $f : G_1 \to G_2$ un morphisme de groupes. Montrer que si $g_1 \in G_1$ et $g_2 \in G_2$ vérifient $g_2 = f(g_1)$, alors $f^{-1}(g_2) = g_1.\mathrm{Ker}(f) := \{g_1.h \mid h \in \mathrm{Ker}(f)\}$.

**Exercice 24.**

1. Montrer que $\left(\mathbb{Z}/2\mathbb{Z}, +\right)$ et $\left(\{\pm 1\}, \,.\,\right)$ sont isomorphes.
2. Soit $n \in \mathbb{N}^*$. On considère $\mathbb{U}_n \subset \mathbb{C}$ l'ensemble des racines $n^{\text{ièmes}}$ de l'unité.
   (a) Montrer que $(\mathbb{U}_n, \,.\,)$ est un groupe.
   (b) Montrer que $(\mathbb{U}_n, \,.\,)$ est isomorphe à $\left(\mathbb{Z}/n\mathbb{Z}, +\right)$.

**Exercice 25.**

1. Montrer que $\mathbb{Z}$ et $\mathbb{Z}/100\mathbb{Z}$ ne sont pas isomorphes.
2. Montrer que $D_3$ et $\mathbb{Z}/6\mathbb{Z}$ ne sont pas isomorphes.
3. Montrer que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.

**Exercice 26.** Soit $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes. On se donne un morphisme de groupe $\varphi : G_2 \to \mathrm{Aut}(G_1)$ et on munit $G_1 \times G_2$ de la loi de composition interne

$$*_\varphi : \begin{array}{ccc} (G_1 \times G_2) \times (G_1 \times G_2) & \longrightarrow & G_1 \times G_2 \\ \big((g_1, g_2), (h_1, h_2)\big) & \longmapsto & \Big(g_1 *_1 \big(\varphi(g_2)\big)(h_1)\ ,\ g_2 *_2 h_2\Big) \end{array}.$$

Montrer que $(G_1 \times G_2, *_\varphi)$ est un groupe. C'est ce qu'on appelle le *produit semi-direct* associé à $\varphi$. On le note $G_1 \rtimes_\varphi G_2$, ou seulement $G_1 \rtimes G_2$ lorsqu'il n'y a pas d'ambiguité sur $\varphi$.

**Exercice 27.** Soit $n \in \mathbb{N}^* \setminus \{1, 2\}$.

1. Montrer que l'application

$$\varphi : \begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathrm{Aut}\left(\mathbb{Z}/n\mathbb{Z}\right) \\ \overline{k} & \longmapsto & \begin{cases} g \mapsto g & \text{si k=0} \\ g \mapsto -g & \text{si k=1} \end{cases} \end{array}$$

   est un morphisme de groupe bien défini.
2. Montrer que le groupe diédral $D_n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$.

**Exercice 28.** On considère l'ensemble $M$ des morphismes de groupes allant de $\mathbb{Z}/20\mathbb{Z}$ dans $\mathbb{Z}/10\mathbb{Z}$.

1. Montrer que tout élément $f \in M$ est entièrement déterminé par $f(\overline{1})$.
2. Déterminer le cardinal de $M$.
3. Déterminer le nombre d'épimorphismes de groupes dans $M$.

**Exercice 29.** Montrer que tout groupe d'ordre 4 est isomorphe soit à $\mathbb{Z}/4\mathbb{Z}$, soit à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

**Exercice 30.** Soit $G$ un sous-groupe de $\mathbb{R}$ non réduit à $\{0\}$. On note $e = \inf G \cap \mathbb{R}_+^*$.

1. On suppose dans cette question que $e > 0$. Montrer que $G$ est isomorphe à $\mathbb{Z}$.
2. On suppose dans cette question que $e = 0$. Montrer que $G$ est dense dans $\mathbb{R}$, c'est-à-dire que pour tout $x \in \mathbb{R}$ et tout $\varepsilon > 0$, il existe $g \in G$ tel que $|x - g| < \varepsilon$.

## Groupes quotients

**Exercice 31.** Déterminer les classes à gauche de $\mathfrak{S}_3$ modulo $\langle (13) \rangle$.

**Exercice 32.** Soient $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ et $H = \langle (\overline{3}, \overline{2}) \rangle \subset G$.

1. Donner l'ordre de $H$ et son indice dans $G$.
2. Écrire les classes à gauche de $G$ modulo $H$.
3. Justifier que le sous-groupe $H$ est distingué dans $G$. Décrire le quotient $G/H$.

**Exercice 33.** Déterminer tous les sous-groupes distingués de $\mathfrak{S}_3$.

**Exercice 34.** Pour les sous-groupes $H \subset G$ suivants, dire si $H$ est distingué dans $G$. Si oui, identifier le quotient $G/H$.

$$\mathbb{R}_+^* \subset \mathbb{R}^* \qquad\qquad \mathbb{R} \subset \mathbb{C} \qquad\qquad \mathrm{SL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{R})$$

**Exercice 35.** On note $O$ l'origine du plan euclidien $\mathbb{R}^2$. Montrer que $\{$rotations autour de $O\}$ est un sous-groupe non distingué des isométries du plan.

**Exercice 36.** Soit $T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a, c \in \mathbb{R}^*, b \in \mathbb{R} \right\}$ et $U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathbb{R} \right\}$.

1. Montrer que $T$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$. Est-il distingué ?
2. Montrer que $U$ est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$. Est-il distingué ?
3. Montrer que $U$ est un sous-groupe de $T$. Est-il distingué ?

**Exercice 37.** Soit $G$ un groupe et $H \subset G$ un sous-groupe. Pour tout $g \in G$, on note $g.H := \{g.h \mid h \in H\}$ et $H.g := \{h.g \mid h \in H\}$. Montrer que $H$ est distingué si et seulement si, pour tout $g \in G$, $g.H = H.g$.

**Exercice 38.** Soit $G$ un groupe.

1. Montrer que $Z(G)$ est distingué.
2. On note $[G, G] := \langle \{g_1.g_2.g_1^{-1}.g_2^{-1} \mid g_1, g_2 \in G\} \rangle$.
   (a) Montrer que $[G, G]$ un sous-groupe distingué de $G$.
   (b) Montrer que le groupe $G/[G, G]$ est abélien.
   (c) Soit $H \subset G$ un sous-groupe distingué tel que $G/H$ soit abélien. Montrer que $[G, G] \subset H$.

**Exercice 39.**

1. Soit $f : G_1 \to G_2$ un morphisme de groupes, et $H \subset G_2$ un sous-groupe distingué. Montrer que $f^{-1}(H)$ est distingué.
2. Montrer que l'image directe d'un sous-groupe distingué $H \subset G_1$ par un morphisme de groupes $f : G_1 \to G_2$ n'est pas forcément un sous-groupe distingué de $G_2$.

**Exercice 40.** Soit $G$ un groupe et $H \subset G$ un sous-groupe d'indice 2.

1. Montrer que $H$ est distingué.
2. Déterminer à quel groupe classique $G/H$ est isomorphe.

**Exercice 41.** On fixe $n \in \mathbb{N}^*$ et on considère les ensembles

$$\mathbb{U} := \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\} \qquad \mathbb{U}_n := \left\{ z \in \mathbb{C} \;\middle|\; z^n = 1 \right\} \qquad \mathbb{U}_\infty := \left\{ z \in \mathbb{C} \;\middle|\; \exists k \in \mathbb{N}^*, z^k = 1 \right\}.$$

1. Montrer que, pour la multiplication, $\mathbb{U}$, $\mathbb{U}_n$ et $\mathbb{U}_\infty$ sous des sous-groupes distingués de $\mathbb{C}^*$, et que $\mathbb{U}_n \subset \mathbb{U}_\infty \subset \mathbb{U}$.
2. Montrer que les groupes $\mathbb{R}/\mathbb{Z}$, $\mathbb{C}^*/\mathbb{R}_+^*$, $\mathbb{C}^*/\mathbb{R}^*$ et $\mathbb{U}/\mathbb{U}_n$ sont tous isomorphes à $\mathbb{U}$.
3. Montrer que $\mathbb{C}^*/\mathbb{U}_n$ est isomorphe à $\mathbb{C}^*$.
4. Montrer que $\mathbb{U}_\infty$ est isomorphe à $\mathbb{Q}/\mathbb{Z}$.

**Exercice 42.**

1. Montrer que $\mathbb{Z}$ est un sous-groupe distingué de $\mathbb{Q}$.
2. Montrer que, pour tout $n \in \mathbb{N}^*$, il existe un élément d'ordre $n$ dans $\mathbb{Q}/\mathbb{Z}$.
3. Montrer que tout élément de $\mathbb{Q}/\mathbb{Z}$ est d'ordre fini.

**Exercice 43.**

1. Montrer que la relation "être un sous-groupe" est une relation d'ordre sur les groupes.
2. Montrer que la relation "être un sous-groupe distingué" n'est pas une relation d'ordre sur les groupes.

**Exercice 44.** Soit $n_1, \dots, n_k \in \mathbb{N}^*$ des entiers deux à deux premiers entre eux. On considère l'application

$$\varphi\colon \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ n & \longmapsto & \big(n\ [n_1], n\ [n_2], \dots, n\ [n_k]\big) \end{array}.$$

1. Montrer que $\varphi$ est un morphisme de groupes.
2. Déterminer le noyau de $\varphi$.
3. Redémontrer le théorème des restes chinois.

# Groupes de permutations

**Exercice 45.**

1. Ecrire les permutations suivantes comme produits de cycles à supports disjoints :
   - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 6 & 2 & 3 & 5 \end{pmatrix}$ ;
   - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 8 & 9 & 7 & 3 & 2 & 4 & 6 \end{pmatrix}$ ;
   - $(624) \circ (361) \circ (12)$.
2. Ecrire les permutations suivantes comme produits de transpositions élémentaires :
   - $(142)(3576)$ ;
   - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$.
3. Calculer la signatures des permutations suivantes :
   - $(316)(24)$ ;
   - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 6 & 4 \end{pmatrix}$.

**Exercice 46.**

1. Décrire les éléments des groupes $\mathfrak{S}_4$ et $\mathcal{A}_4$.
2. Le groupe $\mathcal{A}_4$ a-t-il un sous-groupe d'ordre 4 ?
3. Le groupe $\mathcal{A}_4$ est-il monogène ?
4. Donner une famille génératrice minimale de $\mathcal{A}_4$.

**Exercice 47.**

1. Dire si le sous-groupe $H := \langle (12) \rangle \subset \mathfrak{S}_n$ est distingué dans $\mathfrak{S}_n$. Si oui, identifier le quotient $\mathfrak{S}_n/H$.
2. Même question avec $H := \mathcal{A}_n$.

**Exercice 48.** Soit $n \in \mathbb{N}^*$.

1. Soit $c = (k_1 k_2 \cdots k_\ell) \in \mathfrak{S}_n$ un cycle de longueur $\ell \geq 2$.
   (a) Donner explicitement l'inverse de $c$.
   (b) Déteminer $|c|$.
   (c) Déterminer $\operatorname{sign}(c)$.
2. On note $c_1 \circ \cdots \circ c_r$ la décomposition d'une permutation $\sigma \in \mathfrak{S}_n$ en cycles à supports disjoints.
   (a) Montrer que, pour tout $k \in \mathbb{N}^*$, $\sigma^k = c_1^k \circ \cdots \circ c_r^k$.
   (b) Montrer que l'ordre de $\sigma$ est égal au plus petit multiple commun des longueurs des $c_i$.
   (c) Montrer que $\operatorname{sign}(\sigma) = \prod_{i=1}^r (-1)^{|c_i|+1}$, et en déduire que $\operatorname{sign}(\sigma) = (-1)^{p_\sigma}$, où $p_\sigma \in \mathbb{N}$ est le nombre de cycles de longueur paire dans la décomposition de $\sigma$.
3. Décomposer $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 6 & 4 & 9 & 10 & 2 & 5 & 8 & 1 & 7 \end{pmatrix}$ en produit de cycles à supports disjoints, puis calculer son ordre et sa signature.

**Exercice 49.** Soit $n \in \mathbb{N}^*$.

1. Soit $c := (k_1 k_2 \cdots k_s) \in \mathfrak{S}_n$ un cycle. Montrer que, pour tout $\sigma \in \mathfrak{S}_n$,
$$\sigma \circ c \circ \sigma^{-1} = \big(\sigma(k_1)\sigma(k_2) \cdots \sigma(k_s)\big).$$
2. En déduire que deux cycles de $\mathfrak{S}_n$ ayant même longueur sont toujours conjugués.
3. Montrer que deux permutations dans $\mathfrak{S}_n$ dont les décompositions en cycles à supports disjoints possèdent le même nombre de cycles de longueur $\ell$ pour tout $\ell \in [\![1, n]\!]$ sont conjugués.
4. Soit $\sigma_1 := (327)(19)(485)$ et $\sigma_2 := (48)(129)(365)$. Trouver $\sigma \in \mathfrak{S}_9$ telle que $\sigma_2 = \sigma \circ \sigma_1 \circ \sigma^{-1}$.

**Exercice 50.** Soit $n \in \mathbb{N}^*$. Déterminer les $m \in \mathbb{N}^*$ tels qu'il existe un morphisme de groupe non trivial $f : \mathfrak{S}_n \to \mathbb{Z}/m\mathbb{Z}$.

**Exercice 51.** Le but de l'exercice est de montrer que, pour $n \geq 3$, le centre $Z(\mathfrak{S}_n)$ du groupe $\mathfrak{S}_n$ est réduit à l'identité.

1. Soit $i \in \{1 \dots n\}$, donner un exemple de permutation $s$ fixant $i$ et seulement $i$.
2. Soit $\sigma \in Z(\mathfrak{S}_n)$, en utilisant le fait que $s \circ \sigma = \sigma \circ s$, montrer que $\sigma(i) = i$.
3. Conclure que le centre de $\mathfrak{S}_n$ est réduit à l'identité.

**Exercice 52.** (l'acmé "Reservoir dogs") Dans un moment critique, $n$ individus, disposés dans une pièce (on supposera qu'ils sont tous à des distances différentes les uns des autres), pointent chacun leur arme vers la personne la plus proche. Soudain, un ballon éclate et tous tirent. Montrer que, si $n$ est impair, alors il y a au moins un survivant.