# Groupes

## Table des matières



À faire : regrouper dans un même paragraphe tous les exercices traitant de $\varphi : x \mapsto x^2$ ou de $A = \{g \in G \,/\, g^2 = e\}$ ou de groupes $G$ tels que $\forall g \in G,\ g^2 = g$.

## 1. Notations

1. On pose usuellement $\mathbb{U} = \{z \in \mathbb{C} \,/\, |z| = 1\}$ et $\mathbb{U}_n = \{z \in \mathbb{C} \,/\, z^n = 1\}$
   Muni de la multiplication, $\mathbb{U}_n$ est le *groupe des racines n-ièmes de l'unité*.
2. On note souvent $\langle g \rangle$ le sous-groupe de $G$ engendré par un certain $g \in G$, c'est-à-dire l'ensemble $\{g^k, k \in \mathbb{Z}\}$. Il peut être fini si $g$ est d'ordre fini.
   Autre façon de voir ça : soit $\varphi : \left\{ \begin{array}{c} \mathbb{Z} \to G \\ k \to g^k \end{array} \right.$ alors $\langle g \rangle = \operatorname{Im} \varphi$. (faire un exo à partir de ça).

## 2. Autour des groupes usuels

### 2.1. Groupes usuels isomorphes ou pas entre eux

1. Montrer que les groupes suivants ne sont pas isomorphes :
   a. $(\mathbb{Z}, +)$ et $(\mathbb{Z}^3, +)$ ;
   b. $(\mathbb{Z}, +)$ et $(\mathbb{Q}, +)$.

   Réponse : on regarde les générateurs.
   a. Soit $\varphi : \mathbb{Z} \to \mathbb{Z}^3$ alors $\varphi(1) = (a, b, c)$ qui ne peut en aucun cas engendrer $\mathbb{Z}^3$.
   b. Soit $\varphi : \mathbb{Z} \to \mathbb{Q}$ alors $\varphi(1) = \dfrac{a}{b}$ qui ne peut en aucun cas engendrer $\mathbb{Q}$ : de toutes manières, $\mathbb{Q}$ n'a pas de générateur.
2. Montrer que les groupes suivants ne sont pas isomorphes :
   a. $(\mathbb{R}, +)$ et $(\mathbb{R}^2, +)$ ;

   Réponse :
   a. Soit $\varphi : \mathbb{R}^2 \to \mathbb{R}$ un isomorphisme alors $\varphi(1, 0)$ et $\varphi(0, 1)$ sont non nuls donc il existe $a, b \in \mathbb{R}$ tels que $\varphi(a, 0) = \varphi(0, b)$.
3. Montrer que les groupes suivants ne sont pas isomorphes :
   a. $(\mathbb{Q}, +)$ et $(\mathbb{R}, +)$.

Réponse : les ensembles ne sont équipotents.

4. Montrer que les groupes suivants ne sont pas isomorphes :
   a. $(\mathbb{U}, \times)$ et $(\mathbb{R}, +)$ ;
   b. $(\mathbb{R}^*, \times)$ et $(\mathbb{R}, +)$.

   Réponse : on regarde les diviseurs du neutre.

5. Montrer que les groupes suivants sont isomorphes :
   a. $(\mathbb{R}^{+*}, \times)$ et $(\mathbb{R}, +)$ ;
   b. $(\mathbb{U}, \times)$ et $(\mathbb{R}/2\pi\mathbb{R}, +)$.

   Réponse : l'exponentielle donne l'isomorphisme.

## 2.2. Sous-groupes des groupes usuels

1. Déterminer les sous-groupes de $(\mathbb{Z}, +)$.
2. Montrer que les sous-groupes de $(\mathbb{R}, +)$ sont soit denses soit des échelles (isomorphes à $\mathbb{Z}$).
   Réponse : pour $G$ sous-groupe de $(\mathbb{R}, +)$, on considère $\delta = \inf G \cap \mathbb{R}_*^+$, et on distingue les cas $\delta > 0$ et $\delta = 0$.
3. Sous-groupes de $(]0; +\infty[, \times)$ :
   a. Montrer que $H = \left\{x + y\sqrt{3} / x \in \mathbb{N}, y \in \mathbb{Z}, x^2 - 3y^2 = 1\right\}$ en est un.
4. Sous-groupes de $\mathbb{Z}^2$ (c'est-à-dire de $(\mathbb{Z}, +) \times (\mathbb{Z}, +)$)
   a. Ces sous-groupes sont-ils de la forme $(a\,\mathbb{Z}, +) \times (b\,\mathbb{Z}, +)$ ?
      Non pas forcément : prendre $H = \{(x, y) \in \mathbb{Z}^2 / y - x \equiv 0 (\mathrm{mod}\, 2)\}$, autrement dit le sous-groupe de $\mathbb{Z}^2$ engendré par $(2, 0)$ et $(1, 1)$. Faire un dessin.
5. Déterminer tous les sous-groupes finis de $(\mathbb{C}^*, \times)$.

## 2.3. Groupes classés par ordre

### 2.3.1. ordre 4

1. Soit $(G, +)$ abélien d'ordre 4, prouver que $G$ est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   Réponse : .
   - si $G$ ne contient que des éléments d'ordre 2, alors si $a \neq b \in G$, il est facile d'établir un isomorphisme entre $(G, +)$ et $(\mathbb{Z}/2\mathbb{Z}, +)$ ;
   - si $G$ contient un élément $a$ d'ordre 4, alors $G = <a>$ isomorphe à $\mathbb{Z}/4\mathbb{Z} = <\dot{1}>$.
2. Applications :
   a. Quelle est la structure de groupe de $(\mathbb{F}_5^*, \times)$ (c'est-à-dire du groupe multiplicatif du corps $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$) ?
   b. Quelle est la structure du groupe des éléments inversibles de l'anneau $(\mathbb{Z}/12\mathbb{Z}, +, \times)$ ?

### 2.3.2. ordre 12

1. Soit $G = \mathbb{Z}/12\mathbb{Z}$, montrer que $G$ possède un sous-groupe $T$ d'ordre 3 et un sous-groupe $Q$ d'ordre 4, et que $G = T \oplus Q$ (tout intervalle est somme de tierces mineures et de tierces majeures).

## 2.4. Groupes cycliques

1. Montrer que deux groupes cycliques de même ordre $n$ sont isomorphes.
   Conséquences :
   a. Si $n \wedge m = 1$, alors $\mathbb{Z}/n\,m\mathbb{Z} \sim \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (chinois, montrer que $\varphi$ est injective).

b. $(\mathbb{Z}/p\mathbb{Z}^*, \times) \sim (\mathbb{Z}/(p-1)\mathbb{Z}, +)$ pour $p$ premier.

c. Pour tout $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +) \sim (\mathbb{U}_n, \times)$.

2. Sous-groupes :

a. Montrer qu'un sous-groupe d'un groupe cyclique est cyclique.

b. Montrer que si $d|n$, alors il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal $d$.

c. Déterminer tous les sous-groupes de $\mathbb{U}_6$.

3. Soit $G$ un groupe abélien de cardinal $pq$, où $p$ et $q$ sont deux nombres premiers distincts. Montrer que $G$ est un groupe cyclique.
Réponse : Il suffit de prouver qu'il y a un élément d'ordre $pq$ dans $G$. Supposons que ce ne soit pas le cas, alors tout élement de $G$ autre que $e$ est soit d'ordre $p$ soit d'ordre $q$.
Soit $a$ d'ordre $p$, et soit $b \notin \langle a \rangle$.
* Supposons $b$ d'ordre $p$ aussi ; alors :

- $\langle a \rangle \cap \langle b \rangle = \{e\}$ car $\langle a \rangle \cap \langle b \rangle$ est un sous-groupe de $\langle a \rangle$ donc d'ordre $p$ ou 1.
- D'autre part $\langle a \rangle \cup \langle b \rangle = \{a^u b^v, u, v \in \{0, ..., p-1\}\}$ contient $p^2$ éléments (car il y a $p$ valeurs possibles pour $u$ et idem pour $v$ et deux $a^u b^v$ ne peuvent être égaux sinon en simplifiant cela contredirait $\langle a \rangle \cap \langle b \rangle = \{e\}$.

. Conclusion : $p^2$ diviserait $pq$ ce qui est impossible.
* Supposons $b$ d'ordre $q$ ; alors :

-

4. Soit $p$ premier et $G = (\mathbb{Z}/p\mathbb{Z}^*, \times)$. Montrer que tout élément est d'ordre$(p-1)$ en déduire le petit théorème de Fermat.

## 3. Groupes, exercices divers

### 3.1. Ordre d'un élément

$G$ un groupe de neutre $e$. On appelle *ordre* de $g \in G$ le plus petit $n \in \mathbb{N}^*$, s'il en existe, tel que $g^n = e$.

1. Soit $g$ d'ordre $n$ et soit $m > n$ tel que $g^m = e$, montrer que $n|m$.
Réponse : si $m = kn + r$ avec $r < n$ on a rapidement $g^r = e$...

2. Soient $g, h \in G$ deux éléments du groupe. Les questions suivantes sont indépendantes :

a. on suppose que $g, h, gh$ sont d'ordre 2, montrer que $gh = hg$ ;
$g^{-1} = g$ et $h^{-1} = h$ et $(gh)^{-1} = gh$ par hypothèse ;
par ailleurs $(gh)^{-1} = h^{-1} g^{-1}$.

b. on suppose maintenant simplement que $gh$ est d'ordre fini, montrer qu'alors $gh$ et $hg$ sont de même ordre.
$(hg)^{n+1} = h(gh)^n g = hg$ donc $(hg)^n = e$.

3. Soit $g \in G$ d'ordre fini $n$ :

a. montrer que $g^{-1}$ a aussi un ordre fini et que $g$ et $g^{-1}$ ont le même ordre ;

b. montrer que pour tout $h \in G$, $g$ et $h^{-1}gh$ sont de même ordre fini $n$ ;
$(h^{-1}gh)^k = h^{-1} g^k h$ donc $(h^{-1}gh)^k = e \Leftrightarrow h^{-1} g^k h = e$.

4. Pouvez-vous imaginer un groupe $G$ dans lequel il existe au moins un élément d'ordre fini et au moins un élément d'ordre infini ?
Réponse : par produit cartésien : $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}, +)$.

5. Soit $G$ commutatif d'ordre $n$ et $g \in G$, alors l'ordre de $g$ divise $n$.
Réponse : on regarde $\pi_g = \prod_{h \in G}(gh)$ et l'on a $\pi_g = g^n \prod_{h \in G}(h)$ or, vu que $h \to gh$ est une bijection, les deux produits sont les mêmes d'où $g^n = e$ d'où l'ordre de $g$ divise $n$ d'après un exercice ci-dessus.

## 3.2. Sous-groupes

1. Si $H, K$ sont deux sous-groupes d'un groupe $(G, \times)$, montrer que $H \cup K$ est un sous-groupe de $G$ ssi l'un des deux est inclus dans l'autre.
   Réponse : si $\begin{cases} h_0 \in H \setminus K \\ k_0 \in K \setminus H \end{cases}$ alors $h_0 k_0 \in H \cup K$ d'où la contradiction.
2. Si $H$ est un sous-groupe de $G$ alors les $\{gH\}$ forment une partition de $G$.
3. Montrer que tout sous-groupe d'indice 2 est distingué.
4. Un groupe peut-il être isomorphe à l'un de ses sous-groupes stricts ?
   Réponse : oui, prendre $(\mathbb{Z}, +)$ et $(2\mathbb{Z}, +)$.
5. $H$ une partie finie d'un groupe $(G, \times)$, stable par la loi $\times$, montrer que $H$ est un sous-groupe.
   soit $h \in H$, regarder l'ordre de $h$.
6. **Exercices où il faut raisonner sur le cardinal d'un (sous)-groupe**
   a. Soit $(G, \cdot)$ un groupe fini et $A \subset G$ une partie de $G$ telle que $|A| > |G|/2$. Montrer que tout $g \in G$ est le produit de deux éléments de $A$.
      Réponse : on considère l'ensemble $A(g) = \{g\, a^{-1}, a \in A\}$. Alors $|A(g)| = |A| > |G|/2$ donc $A(g) \cap A \neq \emptyset$ et c'est gagné.
   b. Soit $G$ un groupe fini d'ordre pair. Montrer qu'un existe un $g \in G$ vérifiant $g^2 = e$.
      Réponse : étudier le cardinal de $\{g \in G / g^2 \neq e\}$ et montrer que c'est un nombre pair.
7. On appelle *centre* d'un groupe $G$ l'ensemble $Z(G) = \{z \in G / \forall g \in G, z\, g = g\, z\}$. Montrer que $Z(G)$ est toujours un sous-groupe de $G$.

## 3.3. Lois variées sur un même ensemble.

1. Loi construite à partir d'une autre loi
   a. Soit $(G, \cdot)$ un groupe et soit $\varphi\colon G \to G$ une bijection sur $G$ (pas forcément un isomorphisme).
      On définit la loi $*$ par : $g * g' = \varphi^{-1}(\varphi(g) \cdot \varphi(g'))$.
      Montrer que $(G, *)$ est un groupe aussi.
   b. Applications : expliciter les lois obtenues avec $(\mathbb{R}, +)$ et les $\varphi$ suivants, puis donner le sous-groupe engendré par 1.
      i. $\varphi\colon \begin{cases} \mathbb{Z} \to \mathbb{Z} \\ p \to p+1 \end{cases}$
      ii. $\varphi\colon \begin{cases} \mathbb{Z} & \to & \mathbb{Z} \\ 2p & \to & 2p+1 \\ 2p+1 & \to & 2p \end{cases}$
      iii. $\varphi\colon \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ 0 & \mapsto & 0 \\ x \neq 0 & \mapsto & \frac{1}{x} \end{cases}$
      On a $x * y = \dfrac{x\,y}{x+y}$ si $x, y \neq 0$ et $0 * y = y$ et $0 * 0 = 0$.
      En écrivant bien les choses, on a $x * (-x) = 0$.
      Alors, $\langle 1 \rangle = \left\{\dfrac{1}{n}, n \in \mathbb{Z}^*\right\} \cup \{0\}$.
      iv. $\varphi\colon \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^3 \end{cases}$
      On a $x * y = \sqrt[3]{x^3 + y^3}$ et $\langle 1 \rangle = \{\sqrt[3]{z}, z \in \mathbb{Z}\}$.
      v. $\varphi\colon \begin{cases} \mathbb{R} & \to & \mathbb{R} \\ x & \to & \operatorname{sh} x \end{cases}$

2. On considère un ensemble $E$ et l'ensemble $\mathcal{P}(E)$ de ses parties. $A$ et $B$ étant deux éléments de $\mathcal{P}(E)$, on considère les lois suivantes :
   - l'union $A \cup B$ ;
   - l'intersection $A \cap B$ ;
   - la différence symétrique : $A \Delta B = (A \cup B) \backslash (A \cap B)$ ;
   - la réunion des complémentaires : $A * B = A^C \cup B^C$ ;
   - l'intersection des complémentaires : $A \% B = A^C \cap B^C$.

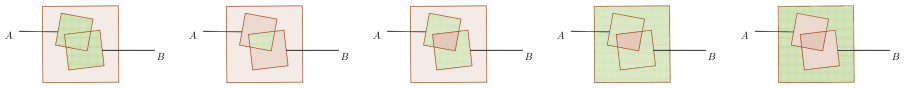


**Figure 1.** de gauche à droite :
$A \cup B$ $A \cap B$ $A \Delta B$ $A * B$ $A \% B$

Pour laquelle(s) de ces lois $\mathcal{P}(E)$ est-il un groupe ?
Réponse :

- Pour $\cup$ (neutre $\emptyset$) et $\cap$ (neutre $E$), pas d'inverse.
- Pour $\Delta$ c'est bon, demander l'associativité sur un schéma :

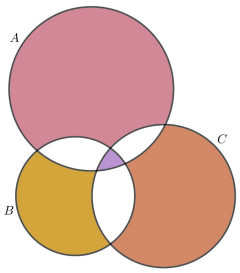


**Figure 2.** Illustration de $A \Delta B \Delta C$.

Pour une rédaction formelle on a :

$$x \in A\Delta(B\Delta C) \Leftrightarrow \left[ \begin{cases} x \in A \\ x \notin B \\ x \notin C \end{cases} \text{ ou } \begin{cases} x \notin A \\ x \in B \\ x \notin C \end{cases} \text{ ou } \begin{cases} x \notin A \\ x \notin B \\ x \in C \end{cases} \text{ ou } \begin{cases} x \in A \\ x \in B \\ x \in C \end{cases} \right].$$

- Pour $*$, le neutre est $\emptyset$, pas d'inverse.
- Pour $\%$, il n'y a pas de neutre.

## 3.4. Divers

1. Soit $\varphi : \begin{cases} G \to G \\ g \mapsto g^2 \end{cases}$. Montrer que :
   a. $\varphi$ morphisme $\Leftrightarrow$ $G$ abélien ;
   b. si $|G|$ premier $\neq 2$ alors $\varphi$ bijective ;
   c. si $|G|$ pair alors $\varphi$ non injective.
2. **Propriété d'un groupe entraînant une propriété sur son ordre**
   a. Soit $G$ un groupe tel que $\forall g \in G, g^2 = e$.
      i. Montrer que $G$ est commutatif.

Réponse : pour tous $a, b \in G$, on a : $a\,b\,a\,b = e$ mais aussi $a\,b\,b\,a = e$.
autre réponse : tout $a \in G$ est son propre inverse, regarder alors $(a\,b)^{-1}$.

ii. Soit H un sous-groupe de $G$ et soit $x \notin H$ et soit $K$ le sous-groupe de $G$ engendré par $H \cup \{x\}$. Montrer que $|K| = 2 \times |H|$.

iii. Montrer que $|G|$ est de la forme $2^n$ avec $n \in \mathbb{N}$.

iv. Exemple : $(\mathbb{Z}/12\mathbb{Z}^*, \times)$.

b. Soit $G$ un groupe n'ayant pas de sous-groupe en dehors de $\{e\}$ et de lui-même.

i. Montrer que chaque $g \in G$ différent de $e$ engendre $G$.
(On dit que $G$ est *monogène*).

ii. Montrer que $G$ est fini.

iii. Montrer que $|G|$ est un nombre premier.

3. Montrer que, si $a, b$ sont deux éléments d'un groupe $G$ :

a. si $a^2 = b^2 = (a\,b)^2 = e$ alors $a\,b = b\,a$.

b. si $a$ est d'ordre fini $n$, alors $a^{-1}$ aussi.

c. si $a$ est d'ordre fini $n$, alors $b\,a\,b^{-1}$ aussi.

d. si $a\,b$ est d'ordre $n$ alors $b\,a$ aussi.

**4. Groupes abéliens : quelques caractérisations**
Soit $(G, \cdot)$ un groupe.

a. Montrer que les propriétés suivantes sont équivalentes :

i. $G$ commutatif ;

ii. $\varphi : g \to g^2$ est un endomorphisme de $G$ ;

iii. $\psi : g \to g^{-1}$ est un endomorphisme de $G$ ;

b. Montrer que les propriétés suivantes sont suffisantes pour affirmer que $G$ abélien. Sont-elles nécessaires ?

i. $\forall g \in G, g^2 = e$.

## 4. GROUPES D'ISOMÉTRIES

1. Le groupe des isométries du triangle équilatéral est-il isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$ ?
non car par les chinois il serait isomorphe à $\mathbb{Z}/6\mathbb{Z}$ et serait commutatif