# Théorie des groupes

## Rappel sur les diagrammes

$A, B, C, D$ ensembles

$f : A \to B$ $\quad h : A \to D$

$g : B \to C$ $\quad k : D \to C$

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] \arrow[dr, phantom, "\bullet"] & B \arrow[d, "g"] \\ D \arrow[r, "k"'] & C \end{tikzcd}$$

On dit que le diagramme $(A, B, C, D, f, g, h, k)$ est commutatif si $g \circ f = k \circ h$. ~~On~~ dénote un diagramme commutatif par un point au millieu.

On dénote par $1_A : A \to A$ l'identité $1_A(x) = x$.
Toute application qui est l'identité peut-etre ignorée dans un diagramme ~~en~~ identifiant sa source et son but :

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h"'] \arrow[dr, phantom, "\bullet"] & B \arrow[d, "g"] \\ C \arrow[r, "1_C"'] & C \end{tikzcd}$$ peut-être écrit $$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "h"'] & \bullet & B \arrow[dl, "g"] \\ & C & \end{tikzcd}$$

et la commutativité veut dire dans les deux cas : $g \circ f = h$

Suite :

$$\cdots \longrightarrow A_{-1} \longrightarrow A_0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow \cdots$$

## Les notions generales

**Def** Un <u>groupe</u> consiste en la donnée d'un ensemble $G \neq \emptyset$ et d'un application $\mu : G\times G \to G$, $(x,y) \mapsto x\cdot y$ appelée la multiplication, tels que :

(a) la multiplication est <u>associative</u>.

$$(xy)z = x(yz)$$

(b) $\exists\, e$ t.q. $e\cdot x = x\cdot e = x$

$e$ est appelé l'élément <u>neutre</u>

(c) $\forall\, x \in G$, $\exists\, x^{-1} \in G$ tel que $x\cdot x^{-1} = x^{-1}\cdot x = e$

$x^{-1}$ est appelé l'élément <u>inverse</u> du $x$.

### Exercices

1. L'élément neutre est unique
2. L'élément inverse de $x$ est unique.
3. Prendre l'inverse deux fois c'est l'identité :
   $(x^{-1})^{-1} = x$
4. $(x\cdot y)^{-1} = y^{-1}\cdot x^{-1}$

La definition du groupe en diagrammes :

a)
$$\begin{tikzcd}
G\times G\times G \arrow[r, "\mu\times 1_G"] \arrow[d, "1_G\times\mu"'] \arrow[dr, phantom, "\cdot"] & G\times G \arrow[d, "\mu"] \\
G\times G \arrow[r, "\mu"'] & G
\end{tikzcd}$$

b)
$$\begin{tikzcd}
G \arrow[r, "(c_e,1_G)"] \arrow[dr, "1_G"'] \arrow[r, phantom, shift right=4ex, "\cdot"] & G\times G \arrow[d, "\mu"] & G \arrow[l, "(1_G,c_e)"'] \arrow[dl, "1_G"] \arrow[l, phantom, shift right=4ex, "\cdot"] \\
& G &
\end{tikzcd}$$

où $c_e : G \to G$, $x \mapsto e$

c)
$$\begin{tikzcd}
G \arrow[r, "(1_G,r)"] \arrow[dr, "c_e"'] \arrow[r, phantom, shift right=4ex, "\cdot"] & G\times G \arrow[d, "\mu"] & G \arrow[l, "(r,1_G)"'] \arrow[dl, "c_e"] \arrow[l, phantom, shift right=4ex, "\cdot"] \\
& G &
\end{tikzcd}$$

$r : G \to G$, $x \mapsto x^{-1}$

Notations : • $(G, \mu)$ ou simplement $G$ pour le groupe
• le neutre est noté $1$.

<u>Def</u> On dit qu'un groupe est <u>commutatif</u> ou <u>abélien</u> si d) $\forall x, y \in G \quad x \cdot y = y \cdot x$

en diagramme : d)

$$\begin{tikzcd} G \times G \arrow[rr, "T"] \arrow[dr, "\mu"'] & & G \times G \arrow[dl, "\mu"] \\ & G & \end{tikzcd}$$

où $T : G \times G \longrightarrow G \times G$
$(x, y) \longmapsto (y, x)$

<u>Remarque</u> Si $(G, \mu)$ est abélien, on note souvent $\mu(x, y) = x + y$.

<u>Def</u> : Si $G$ est un ensemble infini, alors l'<u>ordre</u> de $G$ est $\# G$. Sinon on dit que $G$ a l'orde infini. ~~On~~ ~~dit~~ dit que $G$ est un groupe fini s'il a l'ordre fini et infini dans le cas contraire.

Exemples :

- groupe à deux éléments :

| | e | x |
|---|---|---|
| e | e | x |
| x | x | e |

- groupe de Klein (4 éléments)

| | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

<u>Question</u> : A) Comment reconnaître que $(G, \mu)$ est un groupe
B) Classer les groupes d'un type donné
- les groupe abeliens
- les p-groupes
- les groupes finis simples (15000 pages)

## Sous-groupe

Soit $(G, \mu)$ un groupe, Soit $H \neq \emptyset$ un sous-ensemble de $G$. On dit que $H$ est un sous-groupe de $G$ si $(H, \mu|_{H\times H})$ est un groupe.

Notations :

$$i : H \longrightarrow G \quad \text{l'inclusion}$$
$$x \longmapsto x$$

$$\begin{tikzcd} G\times G \arrow[r, "\mu"] & G \\ H\times H \arrow[u, "i\times i"] \arrow[ur, "\bar{\mu}"'] & H \arrow[u, "i"'] \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "r"] & G \\ H \arrow[u, "i"] \arrow[ur, "\bar{r}"'] & H \arrow[u, "i"'] \end{tikzcd}$$

$$\mu|_{H\times H} = \bar{\mu} \qquad r|_H = \bar{r}$$

Remarque :

Si $H$ est un sous-groupe de $G$ alors on a les diagrammes commutatifs suivants ;

$$\begin{tikzcd} G\times G \arrow[r, "\mu"] & G \\ H\times H \arrow[u, "i\times i"] \arrow[r, "\bar{\mu}"] \arrow[ur, phantom, "\bullet"] & H \arrow[u, "i"'] \end{tikzcd} \qquad \begin{tikzcd} G \arrow[r, "r"] & G \\ H \arrow[u, "i"] \arrow[r, "\bar{r}"'] \arrow[ur, phantom, "\bullet"] & H \arrow[u] \end{tikzcd}$$

Lemme Soit $H$ un sous-groupe de $G$, $e_H$ l'élément neutre de $H$ et $e_G$ l'element neutre de $G$. Alors $e_H = e_G$

Preuve :

En effet $\quad e_H \cdot e_H = e_H = e_H e_G$

Prenons $e_H^{-1}$ l'inverse de $e_H$ dans $G$. alors.

$$e_H^{-1} \cdot e_H \cdot e_H = e_H^{-1} \cdot e_H \cdot e_G$$

$$e_G \cdot e_H = e_G \cdot e_G \implies e_H = e_G \qquad \square$$

**Proposition** : Soit $(G;\mu)$ un groupe et $H$ un sous-ensemble non-vide de $G$.
On des equivalences entre est enoncés suivants:

a) $H$ est un sous-groupe de $G$.

b) i) pour tout $x, y \in H$ on a $x \cdot y \in H$

ii) pour tout $x \in H$ on a $x^{-1} \in H$

c) pour tout $x, y \in H$ on a $x y^{-1} \in H$.

**Preuve**

$$\begin{tikzcd} a) \arrow[rr, Rightarrow] & & c) \arrow[dl, Rightarrow] \\ & b) \arrow[ul, Rightarrow] & \end{tikzcd}$$

$\boxed{a) \Rightarrow c)}$ trivial car $H$ est un groupe.

$\boxed{c) \Rightarrow b)}$ Comme $H$ est non-vide on a ~~qu'il~~ il existe $x \in H$

$x, x \in H \Rightarrow x \cdot x^{-1} \in H \Rightarrow e_G \in H$

$e_G, x \in H \Rightarrow e_G \cdot x^{-1} = \underline{x^{-1} \in H} \Rightarrow$ i)

$x, y \in H \Rightarrow x, y^{-1} \in H \Rightarrow x \cdot (y^{-1})^{-1} \in H \Rightarrow x \cdot y \in H \Rightarrow$ ii)

$\boxed{b) \Rightarrow a)}$

i) $\Longleftrightarrow$
$$\begin{tikzcd} G \times G \arrow[r, "\mu"] & G \\ H \times H \arrow[u, "i \times i"] \arrow[r, "\bar{\mu}"'] \arrow[ur, phantom, "\bullet"] & H \arrow[u, "i"'] \end{tikzcd}$$

ii) $\Longleftrightarrow$
$$\begin{tikzcd} G \arrow[r, "r"] & G \\ H \arrow[u, "i"] \arrow[r, "\bar{r}"'] \arrow[ur, phantom, "\bullet"] & H \arrow[u, "i"'] \end{tikzcd}$$

En utilisant ces diagrammes commutatifs et le fait que $G$ est un groupe on demontre pour $H$ les propriétés a) b) c) dans la definition de groupe.

a) l'associativité est équivalente avec la commutativité du diagramme central dans :

$$\begin{tikzcd}
G\times G\times G \arrow[rrr, "\mu\times 1_G"] \arrow[ddd, "1_G\times\mu"'] & & & G\times G \arrow[ddd, "\mu"] \\
& H\times H\times H \arrow[ul, "i\times i\times i"'] \arrow[r, "\bar{\mu}\times 1_H"] \arrow[d, "1_H\times\bar{\mu}"] & H\times H \arrow[ur, "i\times i"] \arrow[d, "\bar{\mu}"] & \\
& H\times H \arrow[dl, "i\times i"'] \arrow[r, "\bar{\mu}"] & H \arrow[dr, "i"] & \\
G\times G \arrow[rrr, "\mu"'] & & & G
\end{tikzcd}$$

Comme tous les diagrammes-trapèze et le diagramme-carré extérieur sont commutatifs, et $i$ est injectif, on déduit, en utilisant l'Exercice 4 / Série 1 que le carré intérieur est commutatif.

Par des procédés analogues on démontre l'existence d'un élément neutre et un inverse pour chaque élément dans $H$. $\square$

<u>Remarques</u>

1. b) i) n'est pas suffisant en general pour dire que $H$ est un groupe. Exemple $(\mathbb{N},+)\subseteq(\mathbb{Z},+)$ satisfait b) i) mais $(\mathbb{N},+)$ n'est pas un groupe car on n'a pas d'inverse.

2. Si $G$ est fini, alors b) i) $\Rightarrow$ b) ii)
   $x\in H \Rightarrow \exists\, p\geq 1,\ p\in\mathbb{Z}$ tel que $x^n=1$.
   On pose $x^{-1}=x^{n-1}$.

3. Il y a toujours au moins deux sous-groupes d'un groupe $G$ : $\{1\}$, $G$. $\{1\}$ et $G$ sont appelés les sous-groupes triviaux de $G$.
   Les autres sous-groupes sont les sous-groupes propres.

## Morphismes de groupes.

Soit $(G, \mu)$, $(H, \nu)$ deux groupes.

Def : On dit que $f : G \to H$ est un morphisme de groupes si $f(x \cdot y) = f(x) \cdot f(y)$

$$\begin{tikzcd} G \times G \arrow[r, "f \times f"] \arrow[d, "\mu"'] \arrow[dr, phantom, "\circ"] & H \times H \arrow[d, "\nu"] \\ G \arrow[r, "f"] & H \end{tikzcd} \qquad f(\mu(x,y)) = \nu(f(x), f(y))$$

Remarques : • $f(1) = 1$
• $f(x^{-1}) = f(x)^{-1}$

$f : G \to H$, $p : H \to K$ alors $p \circ f$ est un morphisme de groupes. $1_G : G \to G$ est un morphisme de groupes.

Les groupes et les morphismes de groupes forment une catégorie Gr.

De même les groupes abéliens et les morphismes de groupes abéliens forment une catégorie Ab.

On dit qu'un morphisme de groupes $f : G \to H$ est un isomorphisme s'il existe un morphisme $e : H \to G$ t.q. $f \circ e = 1_H$ et $e \circ f = 1_G$.

Rem : Si $e$ existe, il est unique et on le dénote par $f^{-1}$.

Def : $\mathrm{Ker}(f) := \{ x \in G \mid f(x) = 1_H \}$
$\mathrm{Im}(f) := \{ y \in H \mid \exists x \in G,\ f(x) = y \}$

Lemme : On a $\mathrm{Ker}\, f \leq G$ et $\mathrm{Im}\, f \leq H$.

Preuve : (easy) exercice.

**Lemme** : • $f : G \to H$ est un morphisme injectif.
ssi $\operatorname{Ker}(f) = 1$.

**Preuve** "$\Rightarrow$" $f(1_G) = 1_H$
et si $x \neq 1_G$ $f(x) \neq f(1_G) = 1_H$
$\Rightarrow \operatorname{Ker}(f) = \{1_G\}$.

"$\Leftarrow$" Supp $f(x_1) = f(x_2) \Rightarrow f(x_1 x_2^{-1}) = 1_H$
$\Rightarrow x_1 x_2^{-1} = 1_G \Rightarrow x_1 = x_2$. $\square$

**Remarque** • $f : G \to H$ est un morphisme surj
ssi $\operatorname{Im} f = H$

## Suites exactes de morphismes de groupe

**Def** Une suite $\cdots \to A_{k-1} \xrightarrow{f_{k-1}} A_k \xrightarrow{f_k} A_{k+1} \to \cdots$
est exacte à $A_k$ si $\operatorname{Im} f_{k-1} = \ker f_k$.

On dit qu'une suite est exacte si elle est exacte partout.

$$A \xrightarrow{u} B \xrightarrow{v} C$$

**Lemme**

$$\operatorname{Ker}(v) = \operatorname{Im}(u) \iff \begin{cases} \operatorname{Ker}(v) \subseteq \operatorname{Im}(u) \\ \operatorname{Im}(u) \subseteq \operatorname{Ker}(v) \end{cases} \iff \begin{cases} \operatorname{Ker}(v) \subseteq \operatorname{Im}(u) \\ v \circ u = 0 \end{cases}$$

**Def** : Une suite exacte courte est une suite exacte de la forme :

$$1 \to A \xrightarrow{u} B \xrightarrow{v} C \to 1 \iff \begin{cases} \ker u = 1 \\ \operatorname{Im} v = C \\ \operatorname{Ker} v = \operatorname{Im} u \end{cases} \iff \begin{cases} u \text{ inj} \\ v \text{ surj} \\ \operatorname{Ker} v = \operatorname{Im} u \end{cases}$$

Ex ; 1) Tout morphisme donne une suite exacte

$$1 \longrightarrow \mathrm{Ker}(f) \longrightarrow G \xrightarrow{\ f\ } \mathrm{Im}(f) \longrightarrow 1.$$

2) $$1 \longrightarrow \{-1,1\} \longrightarrow (\mathbb{R}^*, \cdot) \longrightarrow (\mathbb{R}^*_+, \cdot) \longrightarrow 1$$
$$x \longmapsto |x|$$

3) $$1 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{R} \longrightarrow (S^1, \cdot)$$
$$1 \longmapsto 0 \qquad t \longmapsto e^{2\pi i t}$$

## Ordre d'un élément

Soit $G$ un groupe et $g \in G$.

$$g^m = \begin{cases} \underbrace{g \cdot g \cdot \cdots \cdot g}_{m} & \text{si } m > 0 \\ 1_G & \text{si } m = 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot \cdots \cdot g^{-1}}_{|m| \text{ fois}} & \text{si } m < 0 \end{cases}$$

$\langle g \rangle = \{ g^m \mid m \in \mathbb{Z} \}$ est un sous groupe de $G$ (appelé le sous-groupe monogène engendré par $G$).

**Def** Si $\langle g \rangle$ est fini alors $\underline{\text{ordre}(g)} = \text{ordre}(\langle g \rangle)$
Autrement on dit que $g$ est d'ordre infini.

Notation : pour ordre de $g$ : $|g|$, $o(g)$.

**Lemme** $G$ un groupe $g \in G$

1) $|g| = \infty \iff \forall\, m \in \mathbb{Z}_{>0}$ $g^m \neq 1$ ds $\mathbb{Z}_{>0}$
2) $|g| = m < \infty \implies m$ est le plus petit t.q. $g^m = 1$
3) $g^k = 1 \implies k \mid |g|$.

Preuve (exercice)

Remarques 1) $1$ est le seul élément d'ordre $1$.
2) Notation ; additivement $mg = \begin{cases} g + g + \cdots + g \\ (-g) + (-g) + \cdots + (-g) \end{cases}$