Chapitre 12

Structure usuelle

Hugo Salou MP2I

Dernière mise à jour le 22 mai 2022

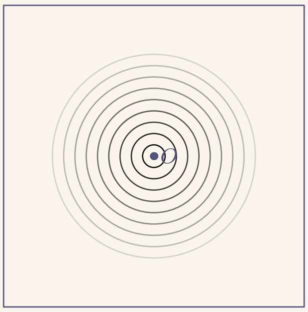
TABLE DES MATIÈRES

Première partie

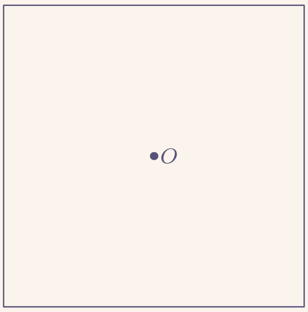
Groupes

Principe de symétrie (Pierre Curie)
La symétrie des causes se retrouvent dans les effets.

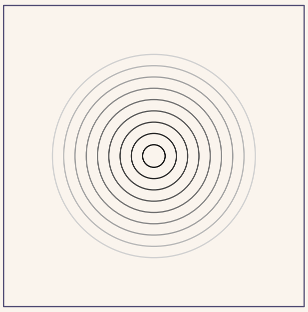
On fait tomber un caillou dans un plan d'eau ce qui crée une onde qui se propage.

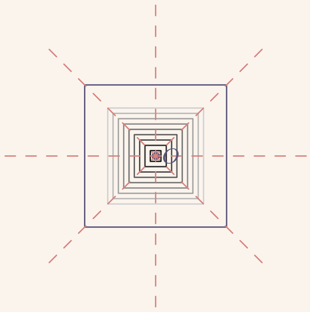


- Symétries des "causes"
  (conserver O en place)
  - translation de vecteur $\vec{0}$
  - rotations de centre O d'angle quelconque
  - symétries d'axe passant par O



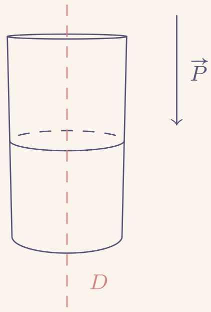
- Symétries des "effets"
  (conserver les ondes en place)
  - translation de vecteur $\vec{0}$
  - rotations de centre O d'angle quelconque
  - symétries d'axe passant par O



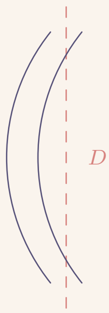


- translation de vecteur $\overrightarrow{0}$
- 4 rotations de centre O d'angle $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$
- 4 symétries axiales

- Causes
  - translations de vecteur $\vec{u} \in \overrightarrow{D}$
  - rotations d'axe D



- Effet



Définition: Soit G un ensemble, muni d'une loi de composition interne $\diamond$.
On dit que $(G, \diamond)$ est un groupe si :
- $\diamond$ est associative
- $\diamond$ a un neutre $e \in G$
- $\forall x \in G, \exists y \in G, x \diamond y = y \diamond x = e$

Exemple ((À connaître)):
1. E un ensemble. $S(E)$ l'ensemble des bijections de E dans E.
   $(S(E), \circ)$ est un groupe appelé groupe symétrique de E.
   Si, $E = [\![1, n]\!]$, alors noté $S(E)$ est noté S_n (ou parfois $\mathfrak{S}_n$)
2. $(\mathbb{Z}, +)$ est un groupe mais $(\mathbb{N}, +)$ n'est pas un groupe.
3. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sont des groupes
4. $(\mathbb{R}, \times)$ n'est pas un groupe car 0 n'a pas d'inverse.
   $(\mathbb{Q}_*, \times)$, $(\mathbb{R}_*, \times)$, $(\mathbb{C}_*, \times)$ sont des groupes.

$(\mathbb{Z}_*, \times)$ n'est pas un groupe.

5. $(\mathscr{M}_n(\mathbb{C}), +)$ est un groupe
   $(\mathscr{M}_n(\mathbb{C}), \times)$ n'est pas un groupe

Définition: On dit que $(G, \diamond)$ est un groupe <u>commutatif</u> ou <u>abélien</u> si c'est un groupe et $\diamond$ est une loi commutative.

Définition: Soit $(G, \cdot)$ un groupe (d'élément neutre e) et $H \subset G$. On dit que H est un <u>sous groupe</u> de G si

1. $\forall (x, y) \in H^2, x \cdot y \in H$
2. $e \in H$
3. $\forall x \in H, x^{-1} \in H$

Proposition: Soit H un sous groupe de $(G, \cdot)$. Alors, $(H, \cdot)$ est un groupe. □

Proposition: Soit $(G, \cdot)$ un groupe et $H \subset G$.

$$H \text{ est un sous groupe de } G \iff \begin{cases} \forall (x, y) \in H, x \cdot y^{-1} \in H \\ H \neq \varnothing \end{cases}$$

Preuve: " $\implies$ " $e \in H$ donc $H \neq \varnothing$.
Soit $(x, y) \in H^2$.
$y \in H$ donc $y^{-1} \in H$.
$x \in H$ donc $x \cdot y^{-1} \in H$.

" $\impliedby$ " $H \neq \varnothing$.
Soit $a \in H$, $(a, a) \in H^2$ donc $a \cdot a^{-1} \in H$ donc $e \in H$.
Soit $x \in H$, $(e, x) \in H^2$ donc $e \cdot e^{-1} \in H$ donc $x^{-1} \in H$.
Soit $(x, y) \in H^2$. Comme $y \in H$, $y \in y^{-1} \in H$ donc $(x, y^{-1}) \in H^2$.
Donc, $x \cdot \left(y^{-1}\right)^{-1} \in H$.
Donc, $x \cdot y \in H$.

□

Exemple:
$2\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$.
En effet,

— $2 \in 2\mathbb{Z}$ donc $2\mathbb{Z} \neq \varnothing$

— Soit $(x, y) \in (2\mathbb{Z})^2$, $\begin{cases} x \equiv 0 \ [2] \\ y \equiv 0 \ [2] \end{cases}$

donc $x - y \equiv 0 \ [2]$ donc $x - y \in 2\mathbb{Z}$

Proposition: Soit $(G, \cdot)$ un groupe et $(H_i)_{i \in I}$ une famille non vide de sous groupes de G. Alors, $\bigcap\limits_{i \in I} H_i$ est un sous groupe de G.

Preuve:
On sait que $\forall i \in I, e \in H_i$ et $I \neq \varnothing$
Donc, $e \in \bigcap_{i \in I} H_i$ donc $\bigcap_{i \in I} H_i \neq \varnothing$
Soit $(x, y) \in \left(\bigcap_{i \in I} H_i\right)^2$.

$$\forall i \in I, \begin{cases} x \in H_i \\ y \in H_i \end{cases}$$

donc,

$$\forall i \in I, x \cdot y^{-1} \in H_i$$

donc

$$x \cdot y^{-1} \in \bigcap_{i \in I} H_i$$

□

Proposition: Soit $(G, \cdot)$ un groupe.
$\{e\}$ et G sont des sous groupes de G

Remarque:
Une réunion de sous groupes n'est pas nécessairement un sous groupe.

$$(G, \cdot) = (\mathbb{Z}, +)$$

$2\mathbb{Z} \cup 3\mathbb{Z} = A$
$2 \in A$ et $3 \in A$ mais $2 + 3 = 5 \notin A$.
Donc, A n'est pas un sous groupe de $\mathbb{Z}$

Proposition – Définition: Soit $(G, \cdot)$ un groupe et $A \subset G$. Alors,

$$\bigcap_{\substack{H \text{ sous groupe de } G \\ A \subset H}} H$$

est le plus petit (au sens de l'inclusion) sous groupe de G qui contient A. On dit que c'est le <u>sous groupe engendré</u> par A et on le note $\langle A \rangle$

Preuve:
On pose $\mathscr{G} = \{H \in \mathscr{P}(G) \mid H \text{ sous groupe contenant } A\}$.
$G \in \mathscr{G}$ donc $\mathscr{G} \neq \varnothing$ donc $\bigcap_{H \in \mathscr{G}} H$ est un sous groupe de G.
Soit $a \in A$. Alors

$$\forall H \in \mathscr{G}, a \in A \subset H$$

et donc $a \in \bigcap_{H \in \mathscr{G}} H$.
Donc, $A \subset \bigcap_{H \in \mathscr{G}} H$.
Soit H un sous groupe de G qui contient A.

Alors, $H \in \mathscr{G}$ alors $H \supset \bigcap\limits_{H \in \mathscr{G}} H$ $\square$

Exemple:
$(G, \cdot) = (\mathbb{Z}, +)$
$A = 2\mathbb{Z} \cup 3\mathbb{Z}$
$\langle A \rangle = \mathbb{Z}$ (d'après le théorème de Bézout).
On généralise $\langle a\mathbb{Z} \cup b\mathbb{Z} \rangle = (a \wedge b)\mathbb{Z}$

Définition: Soit $(G, \cdot)$ un groupe et $A \subset G$.
On dit que A est une partie génératrice de G ou que A engendre G si $G = \langle A \rangle$

Exemple (Rubik's cube):

Exemple:
Soit $(G, \cdot)$ un groupe.

— $\langle \varnothing \rangle = \{e\}$
  $\langle G \rangle = G$
— Soit $a \in G \setminus \{e\}$.
  $\langle a \rangle = \langle \{a\} \rangle = \{a^n \mid n \in \mathbb{Z}\}$
— Soit $a \neq b$ deux éléments de $G \setminus \{e\}$

$$\begin{aligned}\langle \{a, b\} \rangle = \{x \in G \mid \exists n \in \mathbb{N}, \exists\, (a_1, a_2, \dots, a_n) \in \{a, b\}^n, \\ \exists\, (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \{-1, 1\}^n, x = a_1^{\varepsilon_1} \times a_2^{\varepsilon_2} \times \dots \times a_n^{\varepsilon_n}\}\end{aligned}$$

Remarque (Notation):
Soit $(G, \cdot)$ un groupe et $a \in G$.
Pour $n \in \mathbb{N}_*$, on pose $a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ fois}}$.
On pose $a^0 = e$ et pour $n \in Z_*^-$,

$$a^n = \left(a^{-1}\right)^{-n}$$

Remarque:
Si le groupe est noté additivement. On note na $(n \in \mathbb{Z}, a \in G)$ à la place de a^n

Définition: On dit qu'un groupe $(G, \cdot)$ est monogène s'il existe $a \in G$ tel que

$$G = \langle a \rangle$$

On dit alors que a est un générateur de G

Exemple:
$(\mathbb{Z}, +)$ est engendré par 1.
$(2\mathbb{Z}, +)$ est engendré par 2

Définition: Un groupe monogène fini est cyclique.

Proposition: Soit $(G, \cdot)$ un groupe monogène fini. Soit a un générateur de G. Il existe

$k \in \mathbb{N}$ tel que
$$G = \{e, a, a^2, \dots a^{k-1}\}$$

Preuve:
G est fini donc il existe $p < q$ tels que $a^p = a^q$. On a alors $e = a^{q-p}$.
On pose alors, $k = \min \{n \in \mathbb{N}_* \mid a^n = e\}$.
Soit $x \in G = \langle a \rangle$. Il existe $n \in \mathbb{Z}$ tel que $x = a^n$. On fait la division de n par k
$$\begin{cases} n = kq + r \\ q \in \mathbb{Z}, 0 \leqslant r < k \end{cases}$$
$$x = a^n = a^{kq+r} = \left(a^k\right)^q \times a^r = a^r$$
On a prouvé
$$G \subset \left\{e, a, \dots, e^{k-1}\right\}$$
On sait déjà que $\left\{e, a, \dots, a^{k-1}\right\} \subset G$. □

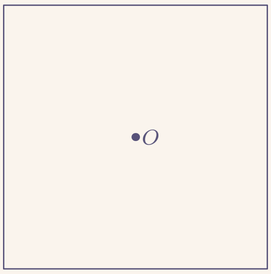
Exemple:
$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique :
$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{n-1}\}$$

Définition: Soit $(G, \cdot)$ un groupe et $a \in G$.
Si $\langle a \rangle$ est fini, le cardinal de $\langle a \rangle$ est appelé <u>ordre</u> de a : c'est le plus petit entier strictement positif n tel que $a^n = e$

Exemple:
$(S(\mathbb{C}_*), \circ)$ est un groupe
$z \mapsto \overline{z}$ est d'ordre de 2
$z \mapsto -z$ est d'ordre de 2
$z \mapsto \dfrac{1}{z}$ est d'ordre de 2

Exemple: — $G_1 = (\mathbb{U}_4, \times)$ où
$$\begin{aligned} \mathbb{U}_4 &= \{z \in \mathbb{C} \mid z^4 = 1\} \\ &= \{1, i, -1, -i\} \end{aligned}$$

$y \backslash x$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1



— G_2 l'ensemble des rotations planes qui laissent globalement invariant un carré.

$$G_2 = \left\{ id, \rho_{\frac{\pi}{2}}, \rho_\pi, \rho_{\frac{3\pi}{2}} \right\}$$

$y \backslash x$	id	$\rho_{\frac{\pi}{2}}$	ρ_π	$\rho_{\frac{3\pi}{2}}$
id	id	$\rho_{\frac{\pi}{2}}$	ρ_π	$\rho_{\frac{3\pi}{2}}$
$\rho_{\frac{\pi}{2}}$	$\rho_{\frac{\pi}{2}}$	ρ_π	$\rho_{\frac{3\pi}{2}}$	id
ρ_π	ρ_π	$\rho_{\frac{3\pi}{2}}$	id	$\rho_{\frac{\pi}{2}}$
$\rho_{\frac{3\pi}{2}}$	$\rho_{\frac{3\pi}{2}}$	id	$\rho_{\frac{\pi}{2}}$	ρ_π

—

$$G_3 = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$
$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{0})$	$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{0})$
$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{0})$	$(\overline{1}, \overline{1})$	$(\overline{0}, \overline{0})$	$(\overline{0}, \overline{1})$
$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{1})$	$(\overline{1}, \overline{0})$	$(\overline{0}, \overline{1})$	$(\overline{0}, \overline{0})$

Définition: Soient $(G_1, \cdot)$ et $(G_2, *)$ deux groupes et $f : G_1 \to G_2$. On dit que f est un (homo)morphisme de groupes si

$$\forall (x, y) \in G_1, f(x \cdot y) = f(x) * f(y)$$

EXEMPLE:
$\exp : (\mathbb{R}, +) \to (\mathbb{R}_*^+, \times)$ est un morphisme de groupes

Proposition: Avec les notations précédentes,
- l'image directe d'un sous groupe de G_1 est un sous groupe de G_2
- l'image réciproque d'un sous groupe de G_2 est un sous groupe de G_1

Preuve: — Soit H_1 un sous groupe de G_1.
$e_1 \in H_1$ donc $f(e_1) \in f(H_1)$ donc $H_1 \neq \varnothing$ Soients $x \in f(H_1)$ et $y \in f(H_2)$.
On pose $\begin{cases} x = f(u) \text{ avec } u \in H_1 \\ y = f(v) \text{ avec } v \in H_1 \end{cases}$

$$\begin{aligned} x * y^{-1} &= f(u) * f(v)^{-1} \\ &= f(u) * f\left(v^{-1}\right) \\ &= f\left(u \cdot v^{-1}\right) \end{aligned}$$

$\begin{cases} u \in H_1 \\ v \in H_1 \end{cases}$ donc $u \cdot v^{-1} \in H_1$ donc $x *^{-1} \in f(H_1)$

— Soit H_2 un sous groupe de G_2.

$$(x, y) \in f^{-1}(H_2)^2$$

$$\begin{aligned} x \cdot y^{-1} \in f^{-1}(H_2) &\iff f\left(x \cdot y^{-1}\right) \in H_2 \\ &\iff f(x) * f\left(y^{-1}\right) \in H_2 \\ &\iff f(x) * f(y)^{-1} \in H_2 \end{aligned}$$

Or, $\begin{cases} f(x) \in H_2 \\ f(y) \in H_2 \end{cases}$

Comme H_2 est un sous groupe de G_2,

$$f(x) * f(y)^{-1} \in H_2$$

et donc,

$$x \cdot y^{-1} \in f^{-1}(H_2)$$

□

Lemme:

$$\begin{cases} f(e_1) = e_2 \\ \forall u \in G_1, f\left(u^{-1}\right) = (f(u))^{-1} \end{cases}$$

Preuve:

$$f(e_1) = f(e_1 \cdot e_1) = f(e_1) * f(e_1)$$

On multiplie par $f(e_1)^{-1}$ (possible car G_2 est un groupe) et on trouve $f(e_1) = e_2$.
Soit $u \in G_1$.

$$f(u) * f(u^{-1}) = f(u \cdot u^{-1}) = f(e_1) = e_2 f(u^{-1}) * f(u) = f(u^{-1} \cdot u) = f(e_1) = e_2$$

Donc, $f\left(u^{-1}\right) = (f(u))^{-1}$ □

Corollaire: Soit $f : (G_1, \cdot) \to (G_2, *)$ un morphisme de groupes. Alors, $\mathrm{Im}(f)$ est un sous groupe de G_2.

$$\mathrm{Ker}(f) = \{x \in G_1 \mid f(x) = e_2\} = f^{-1}(\{e_2\})$$

est un sous groupe de G_1. □

Théorème: Avec les notations précédentes,

$$f \text{ injective} \iff \mathrm{Ker}(f) = \{e_1\}$$

Preuve: " $\implies$ " On suppose f injective.

$$\begin{aligned} f(e_1) = e_2 \text{ donc } & e_1 \in \mathrm{Ker}(f) \\ \text{donc } & \{e_1\} \subset \mathrm{Ker}(f) \end{aligned}$$

Soit $x \in \mathrm{Ker}(f)$. On a alors $f(x) = e_2 = f(e_1)$
Comme f injective, $x = e_1$.

" $\impliedby$ " On suppose $\mathrm{Ker}(f) = \{e_1\}$

Soient $\begin{cases} x \in G_1 \\ y \in G_1 \end{cases}$. On suppose $f(x) = f(y)$

$$\begin{aligned} f(x) = f(y) &\implies f(x) * f(y)^{-1} = e_2 \\ &\implies f(x) * f\left(y^{-1}\right) = e_2 \\ &\implies f\left(x \cdot y^{-1}\right) \qquad\qquad \implies x \cdot y^{-1} \in \mathrm{Ker}(f) = \{e_1\} \\ &\implies x \cdot y^{-1} = e_1 \\ &\implies x = y \end{aligned}$$

Donc, f est injective

□

Exemple ((équation diophantienne)):

$$\begin{cases} 2x + 5y = 1 \\ (x, y) \in \mathbb{Z}^2 \end{cases}$$

On trouve une solution particulière (Bézout) : $(-1, 1) = (x_0, y_0)$

$$\begin{aligned} 2x + 5y = 1 &\iff 2x + 5y = 2x_0 + 5y_0 \\ &\iff 2(x - x_0) + 5(y - y_0) = 0 \\ &\iff 2(x - x_0) = 5(y_0 - y) \end{aligned}$$

$$\vdots \quad \text{(Gauss)}$$

$$\begin{aligned} f : \mathbb{Z}^2 &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto 2x + 5y \end{aligned}$$

$(\mathbb{Z}^2, +)$ est un groupe avec $+$ qui est l'addition composante par composante.
f est un morphisme de groupes.

$$\begin{aligned} f(x, y) = 1 = f(x_0, y_0) &\iff f(x, y) - f(x_0, y_0) = 0 \\ &\iff f(x - x_0, y - y_0) = 0 \\ &\iff (x - x_0, y - y_0) \in \mathrm{Ker}(f) \end{aligned}$$

Théorème: Soit $f : (G_1, \cdot) \to (G_2, *)$ un morphisme de groupes, $y \in G_2$ et $(\mathscr{E})$ l'équation

$$f(x) = y$$

d'inconnue $x \in G_1$.
Si $y \notin \mathrm{Im}(f)$, alors $(\mathscr{E})$ n'a pas de solution.
Sinon, soit $x_0 \in G_1$ tel que $f(x_0) = y$ (x_0 est une solution particulière de $(\mathscr{E})$)

$$f(x) = y \iff \exists h \in \mathrm{Ker}(f), x = x_0 \cdot h$$

Preuve:

$$\begin{aligned} f(x) = y &\iff f(x) = f(x_0) \\ &\iff f(x_0)^{-1} * f(x) = e_2 \\ &\iff f\left(x_0^{-1}\right) * f(x) = e_2 \\ &\iff f\left(x_0^{-1} \cdot x\right) = e_2 \\ &\iff x_0^{-1} \cdot x \in \mathrm{Ker}(f) \\ &\iff \exists h \in \mathrm{Ker}(f), x_0^{-1} \cdot x = h \\ &\iff \exists h \in \mathrm{Ker}(f), x = x_0 \cdot h \end{aligned}$$

□

Proposition: Soient $f : G_1 \to G_2$ et $g : G_2 \to G_3$ deux morphisme de groupes. Alors, $g \circ f$ est un morphisme de groupes.

Preuve:
Soient $x \in G_1$ et $y \in G_2$.

$$\begin{aligned} g \circ f(x \cdot y) &= g(f(x) * f(y)) = g(f(x)) \times g(f(y)) \\ &= g \circ f(x) \times g \circ f(y) \end{aligned}$$

□

Définition: Soit G un groupe.

- Un <u>endomorphisme</u> de G est un morphisme de groupes de G dans G.
- Un <u>isomorphisme</u> de G dans H un morphisme de groupes $f : G \to H$ bijectif.
- Un <u>automorphisme</u> de G est un endomorphisme de G bijectif.

Proposition: Soit $f : G \to H$ un isomorphisme de groupes.
Alors, $f^{-1} : H \to G$ est aussi un isomorphisme.

Preuve:

Soit $(x,y) \in H^2$. On pose $\begin{cases} f(u) = x, u \in G \\ f(v) = y, v \in G \end{cases}$

$$\begin{aligned} f\left(f^{-1}\left(x \cdot y^{-1}\right)\right) &= x \cdot y^{-1} \\ &= f(u) \cdot f(v)^{-1} \\ &= f\left(u \cdot v^{-1}\right) \end{aligned}$$

Comme f injective,

$$f^{-1}\left(x \cdot y^{-1}\right) = u \cdot v^{-1} = f^{-1}(x)\left(f^{-1}(y)\right)^{-1}$$

□

Corollaire: On note $\mathrm{Aut}(G)$ l'ensemble des automorphismes de G.
$\mathrm{Aut}(G)$ est un sous groupe de $(S(G), \circ)$.

Définition: Soit $(G, \cdot)$ un groupe et $g \in G$. L'application

$$\begin{aligned} c_g : G &\longrightarrow G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est appelée conjugaison par g. On dit aussi que c'est un automorphisme intérieur.

Proposition: Avec les notations précédentes,

$$c_g \in \mathrm{Aut}(G)$$

Preuve:
Soient $x \in G$ et $y \in G$.

$$c_g(xy) = g \cdot xy \cdot g^{-1}$$
$$c_g(x) \cdot c_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = c_g(xy)$$

Donc, c_g est un morphisme de groupes.

De plus,

$$\forall x \in G, c_{g^{-1}} \circ c_g(x) = g^{-1}\left(gxg^{-1}g\right) = x$$

Donc, $c_{g^{-1}} \circ c_g = id_G$.
De même, $c_g \circ c_{g^{-1}} = id_G$
Donc, c_g bijective et $(c_g)^{-1} = c_{g^{-1}}$ □

Corollaire:

$$\forall x \in G, \forall n \in \mathbb{Z}, c_g(x^n) = (c_g(x))^n$$

□

Proposition: L'application

$$\begin{aligned} G &\longrightarrow \mathrm{Aut}(G) \\ g &\longmapsto c_g \end{aligned}$$

est un morphisme de groupes.

Preuve:
Soient $(g, h) \in G^2$.

$$\begin{aligned} \forall x \in G, c_g \circ c_h(x) &= g\left(hxh^{-1}\right)g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= c_{gh}(x) \end{aligned}$$

Donc, $c_g \circ c_h = c_{gh}$ □

Proposition (Rappel)**:**

$$\forall g, h \in G, (gh)^{-1} = h^{-1}g^{-1}$$

Preuve:

$$\begin{aligned} (gh)\left(h^{-1}g^{-1}\right) &= e \\ \left(h^{-1}g^{-1}\right)(gh) &= e \end{aligned}$$

□

Proposition – Définition: Soient $(G_1, *)$ et $(G_2, *)$ deux groupes. On définit une loi sur $G_1 \times G_2$ en posant

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1y_1, x_2y_2)$$

Alors, $G_1 \times G_2$ est un groupe pour cette loi appelée groupe produit.

Preuve: — Soient $(x_1, y_1) \in {G_1}^2$ et $(x_2, y_2) \in {G_2}^2$.
On sait que $x_1 * y_1 \in G_1$ et que $x_2 * y_2 \in G_2$.
Donc, $(x_1, x_2) \cdot (y_1, y_2) = (x_1x_2, y_1y_2) \in G_1 \times G_2$

□

Deuxième partie

Anneaux

Définition: Un anneau $(A, +, \times)$ est un ensemble A muni de deux lois de compositions internes notées $+$ et $\times$ vérifiant

1. $(A, +)$ est un groupe commutatif (son neutre est noté 0_A)
2. $(A, \times)$ est un monoïde
   (a) $\times$ est associative
   (b) $\times$ a un neutre $1_A \in A$
3. distributivité à gauche et à droite :

$$\forall (a,b,c) \in A^3, \begin{cases} a \times (b+c) = (a \times b) + (a \times c) \\ (b+c) \times a = (b \times a) + (c \times a) \end{cases}$$

Remarque (Convention):
Soit $(A, +, \times)$ un anneau.
On convient que la multiplication est prioritaire sur l'addition.

$$(a \times b) + (a \times c) = a \times b + a \times c$$

et l'exponentiation est prioritaire sur la multiplication ($n \in \mathbb{N}$)

$$\begin{aligned} a \times b^n &= a \times (\underbrace{b \times b \times \cdots \times b}_{n \text{ fois}}) \\ &\neq (a \times b)^n \end{aligned}$$

Proposition: Soit $(A, +, \times)$ un anneau. Alors, 0_A est absorbant

$$\forall a \in A, a \times 0_A = 0_A \times a = 0_A$$

Preuve:
Soit $a \in A$. On pose $b = a \times 0_A \in A$.

$$\begin{aligned} b = a \times 0_A &= a \times (0_A + 0_A) = a \times 0_A + a \times 0_A \\ &= b + b \ (= 2b) \end{aligned}$$

Donc,

$$-b + b = -b + b + b$$

donc $0_A = b$
De même, $0_A \times a = 0_A$. $\square$

Remarque:

On peut imaginer $\begin{cases} a \times b = 0_A \\ a \neq 0_A \\ b \neq 0_A \end{cases}$

Exemple: — $(\mathbb{Z}/4\mathbb{Z}, +, \times)$ est un anneau

$$\begin{cases} \overline{2} \times \overline{2} = \overline{0} & \text{car } 4 \equiv 0 \ [4] \\ \overline{2} \neq \overline{0} & \text{car } 2 \not\equiv 0 \ [4] \end{cases}$$

— $(\mathscr{M}_2(\mathbb{C}), +, \times)$ est un anneau (non commutatif)

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_A$$
$$A^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Définition: On dit qu'un anneau $(A, +, \times)$ est intègre si

$$\forall (a, b) \in A^2, (a \times b = 0_A \implies a = 0_A \text{ ou } b = 0_A)$$

Exemple: — $(\mathbb{Z}, +, \times)$ est intègre

— $\forall p$ premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est intègre (car tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible donc simplifiable)

Exemple:
Soit $(A, +, \times)$ un anneau et $(a, b) \in A^2$.

$$\begin{aligned}(a+b)^2 &= (a+b) \times (a+b) \\ &= (a+b) \times a + (a+b) \times b \\ &= a^2 + b \times a + a \times b + b^2\end{aligned}$$

Si a et b commutent, alors, $a \times b = b \times a$ et donc $(a+b)^2 = a^2 + b^2 + 2ab$

$$\begin{aligned}(a+b)^3 &= (a+b) \times (a+b) \times (a+b) \\ &= a^3 + a^2 \times b + a \times b \times a + b \times a^2 \\ &+ b^2 \times a + b \times a \times b + a \times b^2 + b^3\end{aligned}$$

Si a et b commutent,
$$(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$$

Proposition: Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{Z}$. Alors,

$$n(a \times b) = (na) \times b = a \times (nb)$$

Preuve: — Évident si $n = 0$

— On suppose $n > 0$.

$$\begin{aligned}(n(a \times b) &= \underbrace{a \times b + \cdots + a \times b}_{n \text{ fois}} \\ &= \sum_{k=1}^{n} (a \times b) \\ &= a \times \sum_{k=1}^{n} = a \times (nb) \\ &= \left(\sum_{k=1}^{n} a\right) \times b = (na) \times b\end{aligned}$$

— On suppose $n < 0$. On pose $n = -p$ avec $p = \mathbb{N}_*$.

$$\begin{aligned}n(a \times b) &= (-p)(a \times b) = -\left(p(a \times b)\right) \\ &= -\left((pa) \times b\right) = (-p)a \times b = (na) \times b \\ &= -\left(a \times (pb)\right) = a \times (-pb) = a \times (nb)\end{aligned}$$

En effet,

$$\forall (a', b') \in A^2 (-a') \times b' + a' \times b' = (-a' + a') \times b' = 0_A \times b' = 0_A$$

donc $-\left(a' \times b'\right) = \left(-a'\right) \times b'$

□

Théorème (Formule du binôme de Newton)**:** Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$, $n \in \mathbb{N}$.
Si a et b commutent alors

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Preuve (par récurrence sur n)*:*

□

Proposition: Soient $(A, +, \times)$ un anneau, $(a, b) \in A^2$ et $n \in \mathbb{N}_*$.
Si a et b commutent, alors

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

□

Proposition: On note $A^\times$ l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$.
$(A^\times, \times)$ est un groupe. □

Exemple: — $\mathbb{Z}^\times = \{-1, 1\}$

- $\mathscr{M}_n(\mathbb{C})^\times = GL_n(\mathbb{C})$
- $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$

Définition: Soit $(A, +, \times)$ un anneau commutatif.

1. Soient $(a, b) \in A^2$. On dit que a divise b s'il existe $k \in A$ tel que $b = a \times k$. On dit aussi que a est un diviseur de b et que b est un multiple de a.
2. On dit que a et b sont associés s'il existe $k \in A^\times$ tel que $ak = b$ (dans ce cas, $a \mid b$ et $b \mid a$)

Remarque:
Le théorème des deux carrés peut se démontrer en exploitant les propriétés arithmétiques de l'anneau $(Z[i], +, \times)$ où $Z[i] = \{a + ib \mid a \in \mathbb{Z}, b \in \mathbb{Z}\}$.
$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$

Théorème des deux carrés :

1. Soit p un nombre premier.
$$\exists (a, b) \in \mathbb{N}^2, p = a^2 + b^2 \iff p \equiv 1 \ [4]$$
2. Soit $n \in \mathbb{N}_*$, $n = \prod_{p \in \mathscr{P}} p^{\alpha(p)}$
$$\exists (a, b) \in \mathbb{N}^2, n = a^2 + b^2 \iff \forall p \in \mathscr{P} \text{ tel que } \alpha(p) \neq 0, p \equiv 1 \ [4]$$

Définition: Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un sous anneau de A si

1. B est un sous groupe de $(A, +)$
2. $\forall (a, b) \in B^2, a \times b \in B$
3. $1_A \in B$

Exemple:
$Z[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$

Proposition: Soit $(A, +, \times)$ un anneau et B un sous anneau de A. Alors, $(B, +, \times)$ est un anneau. $\square$

Exercice (Exercice à connaître):
Soit $(A, +, \times)$ un anneau. Le centre de A est
$$Z(A) = \{x \in A \mid \forall a \in A, a \times x = x \times a\}$$
$Z(A)$ est un sous anneau de A.

Proposition: Soit $(A, +, \times)$ un anneau.
Si $0_A = 1_A$ alors $A = \{0_A\}$. On dit alors que A est l'anneau nul.

Preuve:
Soit $a \in A$.
$$a = a \times 1_A = a \times 0_A = 0_A$$
$\square$

Définition: Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux (les lois notés de la même façon mais ne sont pas forcément les mêmes !).
Soit $f : A \to B$. On dit que f est un <u>(homo)morphisme d'anneaux</u> si

1. $\forall (a,b) \in A^2, f(a+b) = f(a) + f(b)$
2. $\forall (a,b) \in A^2, f(a \times b) = f(a) \times f(b)$
3. $f(1_A) = 1_B$

Proposition: Avec les notations précédentes, **si** $a \in A^\times$ alors $f(a) \in B^\times$ et dans ce cas,

$$f(a)^{-1} = f\left(a^{-1}\right)$$

Preuve:
On suppose $a \in A^\times$.

$$\begin{cases} f\left(a^{-1}\right) \times f(a) = f\left(a^{-1} \times a\right) = f(1_A) = 1_B \\ f(a) \times f\left(a^{-1}\right) = f\left(a \times a^{-1}\right) = f(1_A) = 1_B \end{cases}$$

Donc, $f(a) \in B^\times$ et $f(a)^{-1} = f\left(a^{-1}\right)$ $\square$

Définition: Soient $(A,+,\times)$ et $(B,+,\times)$ deux anneaux et $f : A \to B$ un morphisme d'anneaux.
On dit que f est un

- <u>isomorphisme d'anneaux</u> si f est bijective
- <u>endomorphisme d'anneaux</u> si $\begin{cases} A = B \\ + = + \\ \times = \times \end{cases}$
- <u>automorphisme d'anneaux</u> si f est à la fois un isomorphisme et un endomorphisme d'anneaux

Exemple:

1. Soit $a \in \mathbb{Z}$ et
$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ x &\longmapsto ax \end{aligned}$$
f endomorphisme d'anneaux $\iff a = 1$
2. $$\begin{aligned} f : \mathscr{M}_n(\mathbb{C}) &\longrightarrow \mathscr{M}_n(\mathbb{C}) \\ A &\longmapsto A^2 \end{aligned}$$
f n'est pas un morphisme d'anneaux car
$$(A+B)^2 \neq A^2 + B^2$$
3. $$\begin{aligned} f : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \overline{z} \end{aligned}$$
est un automorphisme d'anneaux

4.

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{R} \\ x &\longmapsto x \end{aligned}$$

f est un morphisme d'anneaux mais ce n'est pas un endomorphisme.

5.

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ k &\longmapsto \overline{k} \end{aligned}$$

f est un morphisme d'anneaux surjectif.

Proposition: La composée de deux morphismes d'anneaux est un morphisme d'anneaux. □

Proposition: La réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux. □

Proposition: L'ensemble des automorphismes d'anneaux de A est un sous groupe de $(S(A), \circ)$. □

Proposition: L'image directe ou réciproque d'un sous anneau par un morphisme d'anneaux est un sous anneaux.

Définition: Soi $f : A \to B$ un morphisme d'anneaux. Le noyau de f est

$$\operatorname{Ker}(f) = \{a \in A \mid f(a) = 0_B\}$$

Proposition: Avec les notations précédents,

$$f \text{ injective} \iff \operatorname{Ker}(f) = \{0_A\}$$

□

Remarque:
$\operatorname{Ker}(f)$ n'est pas un sous anneau en général (car $1_A \notin \operatorname{Ker}(f)$ sauf si $A = \{0_A\}$)

Définition: Soit $(A, +, \times)$ un anneau et $a \in A \setminus \{0_A\}$.
On dit que a est un diviseur de zéro s'il existe $b \in A \setminus \{0_A\}$ tel que $a \times b = b \times a = 0_A$

Proposition: Les diviseurs de zéro ne sont pas inversibles. □

Exemple:
$A = \mathscr{M}_2(\mathbb{C})$

$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro
car $M \times M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Troisième partie

Corps

Exemple (Problème): — avec $A = \mathbb{Z}/9\mathbb{Z}$, résoudre $\overline{x}^2 = \overline{0}$

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{x}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{0}$	$\overline{7}$	$\overline{7}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{0}$

On a trouvé 3 solutions : $\overline{0}, \overline{3}, \overline{6}$.

— $\mathbb{Z}/8\mathbb{Z}$

$\overline{x}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{x}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{1}$

$\overline{x}^2 = \overline{1}$ a 4 solutions : $\overline{1}, \overline{7}, \overline{3}$, et $\overline{5}$

— $A = \mathbb{H} = \{a + bi + cj + dk \mid (a, b, c, d) \in \mathbb{R}^4\}$
$i^2 = j^2 = k^2 = -1$

$$\begin{matrix} ij = k & jk = i & ji = j \\ ji = -k & kj = -i & ik = -j \end{matrix}$$

Dans cet anneau, -1 a 6 racines !

Définition: Soit $(\mathbb{K}, +, \times)$ un ensemble muni de deux lois de composition internes. On dit que c'est un corps si

1. $(\mathbb{K}, \times)$ est un groupe abélien
2. $(\mathbb{K}, \times)$ est un monoïde commutatif
3. $\forall x \in \mathbb{K} \setminus \{0_\mathbb{K}\}, \exists y \in \mathbb{K}, xy = 1_\mathbb{K}$
4. $0_\mathbb{K} \neq 1_\mathbb{K}$

Exemple: — $(\mathbb{C}, +, \times)$ est un corps
— $(\mathbb{R}, +, \times)$ est un corps
— $(\mathbb{Q}, +, \times)$ est un corps
— $(\mathbb{Z}, +, \times)$ n'est pas un corps

Proposition: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Preuve:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{\overline{k} \mid k \wedge n = 1\right\}$$

□

Proposition: Tout corps est un anneau intègre.

Preuve:
Soit $(\mathbb{K}, +, \times)$ un corps. Soient $(a, b) \in \mathbb{K}^2$ tel que $a \times b = 0_\mathbb{K}$.
On suppose $a \neq 0_\mathbb{K}$. Alors, a est inversible et donc

$$b = a^{-1} \times a \times b = a^{-1} \times 0_\mathbb{K} = 0_\mathbb{K}$$

□

Exemple:
Soit $(\mathbb{K}, +, \times)$ un corps.
Résoudre

$$\begin{cases} x^2 = 1_\mathbb{K} \\ x \in \mathbb{K} \end{cases}$$

$$\begin{aligned} x^2 = 1_{\mathbb{K}} &\iff x^2 - 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ &\iff (x - 1_{\mathbb{K}})(x + 1_{\mathbb{K}}) = 0_{\mathbb{K}} \\ &\iff x - 1_{\mathbb{K}} = 0_{\mathbb{K}} \text{ ou } x + 1_{\mathbb{K}} = 0_{\mathbb{K}} \\ &\iff x = 1_{\mathbb{K}} \text{ ou } x = -1_{\mathbb{K}} \end{aligned}$$

Il y a au plus 2 solutions.

Proposition: Soit $(\mathbb{K}, +, \times)$ un corps et P un polynôme à coefficients dans $\mathbb{K}$ de degré n. Alors, l'équation $P(x) = 0_{\mathbb{K}}$ a au plus n solutions dans $\mathbb{K}$ □

Corollaire ((Théorème de Wilson))**:** voir exercice 16 du TD 12

Définition: Soit $(\mathbb{K}, +, \times)$ un corps et $L \subset \mathbb{K}$.
On dit que L est un <u>sous corps</u> de $\mathbb{K}$ si

1. L est un anneau de $(\mathbb{K}, +, \times)$ non nul
2. $\forall x \in L \setminus \{0_{\mathbb{K}}\}, x^{-1} \in L$

en d'autres termes si

1. $\forall (x, y) \in L^2, x - y \in L$
2. $\forall (x, y) \in L^2, x \times y^{-1} \in L$

On dit aussi que $\mathbb{K}$ est une <u>extension</u> de L.

Proposition: Tout sous corps est un corps. □

Définition: Soient $(\mathbb{K}_1, +, \times)$ et $(\mathbb{K}_2, +, \times)$ deux corps et $f : \mathbb{K}_1 \to \mathbb{K}_2$.
On dit que f est un <u>morphisme de corps</u> si f est un morphisme d'anneaux.
i.e. si

$$\begin{cases} \forall (x, y) \in {\mathbb{K}_1}^2, & f(x + y) = f(x) + f(y) \\ \forall (x, y) \in {\mathbb{K}_1}^2, & f(x \times y) = f(x) \times f(y) \end{cases}$$

Proposition: Tout morphisme de corps est injectif.

Preuve:
Soit $f : \mathbb{K}_1 \to \mathbb{K}_2$ un morphisme de corps.

— $\mathrm{Ker}(f)$ est un sous groupe de $(\mathbb{K}_1, +)$
— Soit $x \in \mathrm{Ker}(f)$ et $y \in \mathbb{K}_1$

$$f(x \times y) = f(x) \times f(y) = 0_{\mathbb{K}_2} \times f(y) = 0_{\mathbb{K}_2}$$

— Soit $x \in \mathrm{Ker}(f) \setminus \{0_{\mathbb{K}_1}\}$.
Alors, x est inversible.

$$\left.\begin{array}{l} x \in \mathrm{Ker}(f) \\ x^{-1} \in \mathbb{K}_1 \end{array}\right\} \text{donc } x \times x^{-1} \in \mathrm{Ker}(f)$$

$$\text{donc } 1_{\mathbb{K}_1} \in \mathrm{Ker}(f)$$

$$\text{donc } f(1_{\mathbb{K}_1}) = 0_{\mathbb{K}_2}$$

Or, $f(1_{\mathbb{K}_1}) = 1_{\mathbb{K}_2} \neq 0_{\mathbb{K}_2}$

Donc, $\mathrm{Ker}(f) = \{0_{\mathbb{K}_1}\}$ donc f est injective. □

Exemple:

$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$ est un morphisme de corps

Quatrième partie

Actions de groupes

Définition: Soit $(G, \cdot)$ un groupe et X un ensemble non vide. Une action de G sur X est une application

$$\begin{aligned} \varphi : G \times X &\longrightarrow X \\ (g, x) &\longmapsto \underbrace{g \cdot x}_{\text{ce n'est pas la loi de } G} \end{aligned}$$

qui vérifie

1. $\forall x \in X, \varphi(e, x) = e \cdot x = x$
2. $\forall x \in X, \forall g, h \in G, g \cdot (h \cdot x) = (g \cdot h) \cdot x$

Dans ce cas, $\begin{array}{ccc} G & \longrightarrow & S(X) \\ g & \longmapsto & \varphi(g, \cdot) \end{array} : \begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & g \cdot x \end{array}$ est un morphisme de groupes.

Preuve:
$\forall g \in G\, (x \mapsto g \cdot x)^{-1} =$ $\square$

Cinquième partie

Bilan

Groupe

On dit que $(G, \diamond)$ est un groupe si
- $\diamond$ est associative ;
- $\diamond$ a un neutre $e \in G$;
- tout élément $x \in E$ a un inverse $y \in E$:
$$x \diamond y = y \diamond x = e.$$

Sous-groupe

On dit que $H \subset G$ est un sous-groupe de G si
- $e \in H$;
- $\forall x, y \in H,\ x \diamond y \in H$;
- $\forall x \in H,\ x^{-1} \in H$.

Si $\diamond$ est commutative, on dit que $(G, \diamond)$ est un groupe commutatif ou abélien.

Pour monter que H est un sous-groupe de G, on montre
- $H \neq \varnothing$;
- $\forall x, y \in H,\ x \diamond y^{-1} \in H$.

L'intersection de sous-groupes est un sous-groupe. Attention, l'union de sous-groupes n'est pas forcément un sous-groupe.

Sous-groupe engendré

Le sous-groupe engendré par A, $\langle A \rangle$, est le plus petit sous groupe de G contenant A.

S'il existe $a \in G$ tel que $G = \langle a \rangle$, on dit que G est monogène et a est un générateur de G.

Soit $a \in G$. L'ordre de a est $\# \langle a \rangle$ i.e. $a^n = e$.

Morphisme de groupes

Soit $f : G_1 \to G_2$ où $(G_1, \cdot)$ et $(G_2, \times)$ sont des groupes. f est un morphisme de groupes si
$$\forall x, y \in G_1,\ f(x \cdot y) = f(x) \times f(y).$$
L'image directe d'un sous-groupe de G_1 est un sous-groupe de G_2. L'image réciproque d'un sous-groupe de G_2 est un sous-groupe de G_1.
$$\forall u \in G_1;\ f\left(u^{-1}\right) = f(u)^{-1}.$$

$$f \text{ injective} \iff \operatorname{Ker} f = \{e_1\}.$$