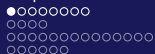


Licence 1 Maths-Info-Ing/ 2024-2025 / Cours  
d'Algèbre:  
**STRUCTURES ALGÉBRIQUES**  
Chapitre 2: Structures de Groupes

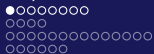
Enseignant: AKEKE E. D.

October 13, 2024



## 1 Chapitre 2: STRUCTURES DE GROUPES

- Définition et exemples
- Produit cartésien de groupes
- Sous-groupes d'un groupe
- Homomorphismes de groupes



## Chapitre 2: STRUCTURES DE GROUPES

### Définition

On appelle **groupe** un ensemble non vide  $G$ , muni d'une loi de composition interne  $*$ , vérifiant les propriétés suivantes:

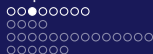
- i) la loi  $*$  est associative,
- ii) la loi  $*$  admet un élément neutre dans  $G$ ,
- iii) tout élément de  $G$  admet un symétrique dans  $G$ .

Si de plus la loi  $*$  est commutative, le groupe  $(G, *)$  est appelé **groupe commutatif** ou plus souvent **groupe abélien**.



## Exemple 1

- 1  $(\mathbb{Z}, +)$  est un groupe abélien. Mais  $(\mathbb{Z}, \times)$  n'est pas un groupe
- 2  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$  sont des groupes abéliens.
- 3  $(\mathbb{Q}, \times)$ ,  $(\mathbb{R}, \times)$ ,  $(\mathbb{C}, \times)$  ne sont pas des groupes.  
En revanche,  $(\mathbb{Q}^*, \times)$ ,  $(\mathbb{R}^*, \times)$ ,  $(\mathbb{C}^*, \times)$  sont des groupes abéliens.



## Exemple 2

- 1 Soient  $F$  un ensemble non vide et  $\mathcal{A}(F)$  l'ensemble des applications de  $F$  vers  $F$ . On pose

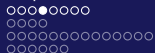
$$S(F) = \{ f \in \mathcal{A}(F) / f \text{ bijective} \}$$

Alors l'ensemble  $(S(F), \circ)$  est un groupe  
(où  $\circ$  est la loi de composition des applications).

Si  $n \in \mathbb{N}^*$  et  $F = \{1, 2, \dots, n\}$ , le groupe  $(S(F), \circ)$  se note  $S_n$ , appelé le **groupe des permutations** de  $F$  ou plus souvent le **groupe symétrique** de rang  $n$ .

Notons que

$$\text{Card}(S_n) = n!$$



Pour  $n = 2$ , on a

$$\text{Card}(S_2) = 2! = 2.$$

Les éléments du groupe symétrique  $S_2$  sont

$$id_F = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{et} \quad \theta = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Ainsi  $S_2 = \{id_F, \theta\}$ . **La table** du groupe symétrique  $S_2$  est

$\circ$	$id_F$	$\theta$
$id_F$	$id_F$	$\theta$
$\theta$	$\theta$	$id_F$



Pour  $n = 3$ , on a

$$\text{Card}(S_3) = 3! = 3 \times 2 \times 1 = 6.$$

Les 6 éléments du groupe symétrique  $S_3$  sont

$$id_F = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\theta_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \theta_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \theta_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Ainsi  $S_3 = \{id_F, \theta_1, \theta_2, \theta_3, \theta_4, \theta_5\}$ .

La table du groupe symétrique  $S_3$  est

$\vec{\gamma} \circ$	$id_F$	$\theta_1$	$\theta_2$	$\theta_3$	$\theta_4$	$\theta_5$
$id_F$	$id_F$	$\theta_1$	$\theta_2$	$\theta_3$	$\theta_4$	$\theta_5$
$\theta_1$	$\theta_1$	$id_F$	$\theta_5$	$\theta_4$	$\theta_3$	$\theta_2$
$\theta_2$	$\theta_2$	$\theta_4$		$\theta_5$		
$\theta_3$	$\theta_3$	?	?	?	?	?
$\theta_4$	$\theta_4$	?	?			
$\theta_5$	$\theta_5$					

Compléter cette table!



## Remarque

- 1) le groupe symétrique  $(S_2, \circ)$  est commutatif.
- 2) le groupe symétrique  $(S_3, \circ)$  n'est pas commutatif.

En effet, on a

$$\theta_1 \circ \theta_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \theta_5$$

et

$$\theta_2 \circ \theta_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \theta_4$$

Donc  $\theta_1 \circ \theta_2 \neq \theta_2 \circ \theta_1$ .



3) Si  $n \geq 3$  alors le groupe  $(S_n, \circ)$  n'est pas commutatif.

En effet, soit

$$F = \{1, 2, 3, \dots, n\}.$$

Considérons les bijections  $f : F \rightarrow F$  et  $g : F \rightarrow F$  définies par

$$f(1) = 1, f(2) = 3, f(3) = 2 \quad \text{et} \quad k \in F \setminus \{1, 2, 3\}, f(k) = k$$

$$g(1) = 3, g(2) = 2, g(3) = 1 \quad \text{et} \quad k \in F \setminus \{1, 2, 3\}, g(k) = k.$$

Alors on a

$$(f \circ g)(1) = 2 \quad \text{et} \quad (g \circ f)(1) = 3,$$

donc  $f \circ g \neq g \circ f$ .



Soient  $(G, *)$  et  $(F, \cdot)$  deux groupes. Le produit cartésien  $G \times F$  est muni de la loi de composition interne naturel  $\top$  définie par

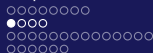
$$\forall (x, y) \in G \times F, \forall (x', y') \in G \times F, \quad (x, y) \top (x', y') = (x * x', y \cdot y').$$

### Proposition

*$(G \times F, \top)$  est un groupe, appelé le groupe produit cartésien du groupe  $(G, *)$  par le groupe  $(F, \cdot)$ .*

### Preuve

Il est clair que la loi  $\top$  est une loi de composition interne dans  $G \times F$ .



## Associativité de la loi $\top$

Soient  $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in G \times F$ . on a

$$\begin{aligned} [(x_1, y_1) \top (x_2, y_2)] \top (x_3, y_3) &= (x_1 * x_2, y_1 \cdot y_2) \top (x_3, y_3) \\ &= ((x_1 * x_2) * x_3, (y_1 \cdot y_2) \cdot y_3) \end{aligned}$$

$$\begin{aligned} (x_1, y_1) \top [(x_2, y_2) \top (x_3, y_3)] &= (x_1, y_1) \top (x_2 * x_3, y_2 \cdot y_3) \\ &= (x_1 * (x_2 * x_3), y_1 \cdot (y_2 \cdot y_3)) \end{aligned}$$

Les lois  $*$  et  $\top$  étant associatives, on a

$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$  et  $(y_1 \cdot y_2) \cdot y_3 = y_1 \cdot (y_2 \cdot y_3)$  d'où

$$[(x_1, y_1) \top (x_2, y_2)] \top (x_3, y_3) = (x_1, y_1) \top [(x_2, y_2) \top (x_3, y_3)].$$

La loi  $\top$  est donc associative.



### Élément neutre de la loi $\top$

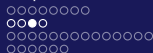
Soient  $e$  l'élément neutre de  $(G, *)$  et  $e'$  l'élément neutre de  $(F, \cdot)$ .

Pour tout  $(x, y) \in G \times F$  on a

$$(x, y) \top (e, e') = (x * e, y \cdot e') = (x, y)$$

$$(e, e') \top (x, y) = (e * x, e' \cdot y) = (x, y)$$

Par conséquent  $(e, e')$  est l'élément neutre de  $G \times F$ .



## Éléments symétriques

Soit  $(x, y) \in G \times F$ .

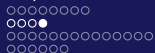
Soient  $x^{-1}$  le symétrique de  $x$  dans le groupe  $(G, *)$  et  $y^{-1}$  le symétrique de  $y$  dans le groupe  $(F, \cdot)$ . On a

$$(x, y) \top (x^{-1}, y^{-1}) = (x * x^{-1}, y \cdot y^{-1}) = (e, e')$$

$$(x^{-1}, y^{-1}) \top (x, y) = (x^{-1} * x, y^{-1} \cdot y) = (e, e')$$

Par conséquent  $(x, y)$  admet un symétrique dans  $G \times F$  et son symétrique est  $(x^{-1}, y^{-1})$ .

En somme,  $(G \times F, \top)$  est un groupe.



## Exemple

$$G = (\mathbb{R}, +), F = (\mathbb{R}, +).$$

$(\mathbb{R} \times \mathbb{R}, +)$  est un groupe: la loi  $+$  étant définie sur  $\mathbb{R} \times \mathbb{R}$  par

$$\forall (a, b) \in \mathbb{R}^2 \text{ et } \forall (c, d) \in \mathbb{R}^2, \quad (a, b) + (c, d) = (a + c, b + d)$$



## Sous-groupes d'un groupe

### Définition

Soient  $(G, *)$  un groupe d'élément neutre  $e$  et  $H$  un sous-ensemble de  $G$ . On dit que  $H$  est un **sous-groupe** du groupe  $(G, *)$  si les conditions suivantes sont satisfaites:

- i)  $e \in H$ ,
- ii) Pour tout  $x, y \in H$ , on a  $x * y \in H$ ,
- iii)  $\forall x \in H, x^{-1} \in H$ .  
où  $x^{-1}$  est le symétrique de  $x$  dans le groupe  $(G, *)$ .



## Proposition

*Soient  $(G, *)$  un groupe d'élément neutre  $e$  et  $H$  une partie de  $G$ .  $H$  est un sous-groupe du groupe  $(G, *)$  si et seulement si les conditions suivantes sont satisfaites:*

- 1)  $e \in H$ ,
- 2)  $\forall x, y \in H, \quad x * y^{-1} \in H$ .

Preuve (voir support de cours)



# Exemple 1

- 1  $\mathbb{Q}$  est un sous-groupe du groupe  $(\mathbb{R}, +)$
- 2  $\mathbb{Z}$  est un sous-groupe du groupe  $(\mathbb{Q}, +)$ , donc du groupe  $(\mathbb{R}, +)$ .



## Exemple 2

Soit  $n \in \mathbb{Z}$ . On pose  $n\mathbb{Z} = \{x \in \mathbb{Z} / \exists k \in \mathbb{Z}, x = nk\}$ .

### Proposition

*Pour tout  $n \in \mathbb{Z}$ , l'ensemble  $n\mathbb{Z}$  est un sous-groupe de  $(\mathbb{Z}, +)$ .*

Preuve

(i) On sait que  $0 = n \times 0$  donc  $0 \in n\mathbb{Z}$ .

(ii) Soient  $x \in n\mathbb{Z}$  et  $y \in n\mathbb{Z}$ . Alors il existe  $u, v \in \mathbb{Z}$  tels que  $x = nu$  et  $y = nv$ .

Donc

$$x + y = n(u + v)$$

avec  $u + v \in \mathbb{Z}$ . Donc  $x + y \in n\mathbb{Z}$ .



(iii) Pour tout  $x \in n\mathbb{Z}$  il existe  $u \in \mathbb{Z}$  tel que  $x = nu$ . Ainsi

$$-x = -(nu) = n(-u)$$

avec  $-u \in \mathbb{Z}$ , donc  $-x \in n\mathbb{Z}$ .

En somme,  $n\mathbb{Z}$  est un sous-groupe du groupe  $(\mathbb{Z}, +)$ .

(remarquons que  $n\mathbb{Z}$  est exactement l'ensemble des éléments de  $\mathbb{Z}$  qui sont multiples de  $n$  dans  $\mathbb{Z}$ .)



## Caractérisation des sous-groupes du groupe $(\mathbb{Z}, +)$

On dispose du résultat important suivant.

### Proposition

*Soit  $H$  une partie de  $\mathbb{Z}$ .*

*$H$  est un sous-groupe de  $(\mathbb{Z}, +) \Leftrightarrow \exists n \in \mathbb{N}$  tel que  $H = n\mathbb{Z}$*

*Noter que si  $H \neq \{0\}$  alors  $n = \min\{k \in \mathbb{N}^* / k \in H\}$ .*

Preuve (voir le support de cours)



## Remarques

*(important!)*

- 1 *Une partie stable d'un groupe n'est pas nécessairement un sous-groupe.  
Par exemple  $\mathbb{N}$  est une partie stable de  $\mathbb{Z}$  pour l'addition usuelle, mais ce n'est pas un sous-groupe de  $(\mathbb{Z}, +)$ .*
- 2 *Tout sous-groupe d'un groupe a une structure de groupe (relativement à la loi induite) et tout sous-groupe d'un groupe commutatif est un groupe commutatif.*
- 3 *Si  $G$  est un groupe d'élément neutre  $e$  alors  $\{e\}$  et  $G$  sont des sous-groupes de  $G$  appelés **sous-groupes triviaux** de  $G$ .*



Soient  $(G, *)$  un groupe.

## Remarques

- 1 *Si  $H$  et  $K$  sont des sous-groupes du groupe  $(G, *)$  alors l'intersection  $H \cap K$  est un sous-groupe du groupe  $(G, *)$ .*
- 2 **ATTENTION!** *La réunion de 2 sous-groupes d'un groupe  $(G, *)$  n'est pas en général un sous-groupe de  $(G, *)$ .*

Par exemple,  $3\mathbb{Z}$  et  $5\mathbb{Z}$  sont des sous groupes de  $(\mathbb{Z}, +)$ ,  
 mais  $3\mathbb{Z} \cup 5\mathbb{Z}$  n'est pas un sous-groupe de  $\mathbb{Z}$ .

En effet,  $3 \in 3\mathbb{Z}$  et  $5 \in 5\mathbb{Z}$  mais  $3 + 5 = 8 \notin 3\mathbb{Z} \cup 5\mathbb{Z}$



# A SAVOIR

Soient  $(G, *)$  un groupe,  $H$  et  $K$  deux sous-groupes de  $(G, *)$ .  
Alors

$$H \cup K \text{ un sous-groupe de } (G, *) \Leftrightarrow H \subseteq K \text{ ou } K \subseteq H$$



## Corollaires de la proposition 1.4

### Corollaire

Soient  $m, n \in \mathbb{Z}$ . On a

$$m\mathbb{Z} \cap n\mathbb{Z} = p\mathbb{Z}$$

où  $p = \text{PPCM}(m, n)$

Preuve (cf Travaux Dirigés)



Soient  $m, n \in \mathbb{Z}$ . On pose

$$m\mathbb{Z} + n\mathbb{Z} = \{x \in \mathbb{Z} / \exists a, b \in \mathbb{Z}, x = ma + nb\}.$$

L'ensemble  $m\mathbb{Z} + n\mathbb{Z}$  est un sous-groupe du groupe  $(\mathbb{Z}, +)$ .

En effet,

(i) On a  $0 = m \times 0 + n \times 0$  donc  $0 \in m\mathbb{Z} + n\mathbb{Z}$

(ii) Soit  $x \in m\mathbb{Z} + n\mathbb{Z}$  et  $y \in m\mathbb{Z} + n\mathbb{Z}$ . Alors il existe des entiers  $a, b, c, d \in \mathbb{Z}$  tels que

$$x = ma + nb \quad \text{et} \quad y = mc + nd$$

Ainsi

$$x - y = m(a - c) + n(b - d) \in m\mathbb{Z} + n\mathbb{Z}$$

En somme,  $m\mathbb{Z} + n\mathbb{Z}$  est un sous-groupe du groupe  $(\mathbb{Z}, +)$ .



## Corollaire

Soient  $m, n \in \mathbb{Z}$ . On a

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$$

où  $d = \text{PGCD}(m, n)$ .

Preuve (cf. Travaux Dirigés)

### Égalité de Bézout

Soient  $m, n \in \mathbb{Z}$  et  $d \in \mathbb{N}$ . D'après le corollaire précédent, on a

$$d = \text{pgcd}(m, n) \Rightarrow \exists u, v \in \mathbb{Z} \text{ tel que } mu + nv = d.$$

En particulier,

$$m \text{ et } n \text{ sont premiers entre eux} \Leftrightarrow \exists u, v \in \mathbb{Z}, \quad mu + nv = 1$$

(Faire des recherches sur l'Algorithme d'Euclide)





## Exercice

- 1) Déterminer l'entier naturel  $n$  tel que  $6\mathbb{Z} + 4\mathbb{Z} = n\mathbb{Z}$ .
- 2) Déterminer l'entier naturel  $m$  tel que  $6\mathbb{Z} \cap 14\mathbb{Z} = m\mathbb{Z}$ .
- 3) Expliciter les groupes suivants:
  - a)  $6\mathbb{Z} + 4\mathbb{Z} + 15\mathbb{Z}$
  - b)  $6\mathbb{Z} \cap 4\mathbb{Z} \cap 15\mathbb{Z}$ .



## Correction de l'exercice

1) On trouve

$$6\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z} \quad \text{car} \quad n = \text{PGCD}(6, 4) = 2.$$

2) On trouve

$$6\mathbb{Z} \cap 14\mathbb{Z} = 42\mathbb{Z} \quad \text{car} \quad m = \text{PPCM}(6, 14) = 42.$$

3) Explicitons ces groupes:

$$\text{a) } 6\mathbb{Z} + 4\mathbb{Z} + 15\mathbb{Z} = (6\mathbb{Z} + 4\mathbb{Z}) + 15\mathbb{Z} = 2\mathbb{Z} + 15\mathbb{Z} = \mathbb{Z}$$

$$\text{b) } 6\mathbb{Z} \cap 4\mathbb{Z} \cap 15\mathbb{Z} = (6\mathbb{Z} \cap 4\mathbb{Z}) \cap 15\mathbb{Z} = 12\mathbb{Z} \cap 15\mathbb{Z} = 60\mathbb{Z}.$$



# Théorème de Lagrange

## Théorème

*Soient  $G$  un groupe **fini** et  $H$  est un sous-groupe de  $G$ .  
Alors  $\text{card}(H)$  divise  $\text{card}(G)$ .*

Preuve (cf. support de cours)



## Définition

Soient  $(G, *)$ ,  $(H, \top)$  deux groupes et  $f : G \rightarrow H$  une application. On dit que  $f$  est un **homomorphisme** du groupe  $(G, *)$  vers le groupe  $(H, \top)$  si pour tout  $x, y \in G$ , on a

$$f(x * y) = f(x) \top f(y)$$



## Exemples

- L'application  $g : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$  définie par  $x \longmapsto \ln(x)$  est un homomorphisme de groupes.
- Soit  $n \in \mathbb{N}^*$ . L'application  $f : (\mathbb{C}^*, \times) \longrightarrow (\mathbb{C}^*, \times)$  définie par  $z \longmapsto z^n$  est un homomorphisme de groupes.



## Définition

(1) On appelle **noyau** de  $f$  et on note  $\ker(f)$ , le sous-ensemble de  $G$  contenant exactement tous les éléments de  $G$  ayant pour image par  $f$ , l'élément neutre du groupe  $(H, \top)$ . Ainsi

$$\ker(f) = \{x \in G / f(x) = e_H\}$$

où  $e_H$  est l'élément neutre du groupe  $H$ .

(2) **L'image** de  $f$ , notée  $\text{Im}(f)$  ou  $f(G)$ , est le sous-ensemble de  $H$  contenant exactement de tous les éléments de  $H$  ayant au moins un antécédant par  $f$ . Ainsi

$$\text{Im}(f) = \{h \in H / \exists x \in G, y = f(x)\}.$$



## Remarques

Soient  $(G, *)$ ,  $(H, \top)$  deux groupes et  $f : (G, *) \longrightarrow (H, \top)$  un homomorphisme de groupes. On a les propriétés suivantes:

- 1)  $f(e_G) = e_H$
- 2) Pour tout élément  $x \in G$ , on a

$$f(x^{-1}) = (f(x))^{-1}.$$



Preuve

1) On sait que

$$e_G * e_G = e_G$$

donc  $f(e_G * e_G) = f(e_G)$ . Comme  $f$  est un homomorphisme de groupes, on a

$$f(e_G * e_G) = f(e_G) \top f(e_G)$$

donc  $f(e_G) \top f(e_G) = f(e_G)$ . On en déduit que

$$(f(e_G))^{-1} \top f(e_G) \top f(e_G) = (f(e_G))^{-1} \top f(e_G)$$

donc  $e_H \top f(e_G) = e_H$  par conséquent,  $f(e_G) = e_H$



On sait que

$$x * x^{-1} = e_G \quad \text{et} \quad x^{-1} * x = e_G$$

donc  $f(x * x^{-1}) = f(e_G)$  et  $f(x^{-1} * x) = f(e_G)$ . Comme  $f$  est un homomorphisme alors

$$f(x) * f(x^{-1}) = f(e_G) \quad \text{et} \quad f(x^{-1}) * f(x) = f(e_G).$$

Ainsi, le symétrique  $(f(x))^{-1}$  de  $f(x)$  dans le groupe  $(H, \top)$  est  $f(x^{-1})$ .



## Proposition

*Soient  $(G, *)$ ,  $(H, \top)$  deux groupes et  $f : (G, *) \longrightarrow (H, \top)$  un morphisme de groupes. Alors*

- (1) Le noyau  $\ker(f)$  de  $f$  est un sous-groupe du groupe  $(G, *)$ .*
- (2) L'image  $\text{Im}(f)$  est un sous-groupe du groupe  $(H, \top)$ .*

Preuve (voir support de cours)