

chapitre 3: Structures algébriques

SI Généralités:

1) Lois de composition internes:

Soit E un ensemble.

Définition : On appelle loi de composition interne sur E , toute application de $E \times E$ dans E .

On note :

$$\begin{array}{l} \cdot : E \times E \rightarrow E \\ (x, y) \mapsto x \cdot y \end{array}$$
$$\begin{array}{l} * : E \times E \xrightarrow{\cong} E \\ (x, y) \mapsto x * y \end{array}$$
$$\begin{array}{l} \perp : E \times E \rightarrow E \\ (x, y) \mapsto x \perp y \end{array}$$

Remarque :

- 1- $x * y$ est le composé de x et y pour la loi $*$.
- 2- On désignera par LCI la loi de composition interne.

Exemple 1: le ppcm et le pgcd
sont des LCI sur \mathbb{N} .

En effet :

ppcm : $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$(x, y) \mapsto \text{ppcm}(x, y)$.

est une application.

et $\text{pgcd} : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$

$$(x, y) \mapsto \text{pgcd}(x, y)$$

est une application.

Exemple 2 :

L'addition et la multiplication sont des
L.C.I sur \mathbb{Z}

Car : $+ : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ est une
 $(x, y) \mapsto x + y$
application.

$$X : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$(x, y) \longmapsto x^y$$

est une application.

Exemple 3 : On définit dans \mathbb{R} la loi $*$ par :

$\forall (a, b) \in \mathbb{R}^2$, $a * b = \sqrt[3]{a^3 + b^3}$

Vérifions que $*$ est une loi sur \mathbb{R}

On a $a^3 \in \mathbb{R}, b^3 \in \mathbb{R}$ $a^3 + b^3 \in \mathbb{R}$

$\sqrt[3]{a^3 + b^3} \in \mathbb{R}$.

$a * b \in \mathbb{R}$

Montrons $*$: $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$

$$(x, y) \mapsto \sqrt[3]{x^3 + y^3}$$

est une application

S'orient (x, y) et (x', y') sont des éléments de $\mathbb{R} \times \mathbb{R}$ t.q. :

$$(x, y) = (x', y')$$

$$\begin{cases} x = x' \\ y = y' \end{cases} \Rightarrow \begin{cases} x^3 = x'^3 \\ y^3 = y'^3 \end{cases}$$

$$\sqrt[3]{x^3 + y^3} = \sqrt[3]{x'^3 + y'^3}$$

$$\sqrt[3]{x^3 + y^3} = \sqrt[3]{x'^3 + y'^3}$$

* st une application
Donc * st une L.C.I sur \mathbb{R} .



Exemple 4: Soit X un quelconque.

$\mathcal{F}(X, X)$: l'ensemble des applications de X dans X .

la composition des applications est une LCI

sur $\mathcal{F}(X, X)$

car:

$$\circ : \mathcal{F}(X, X) \times \mathcal{F}(X, X) \rightarrow \mathcal{F}(X, X)$$

$(f, g) \mapsto f \circ g$

et une application.

HomeWork

Soit $c \in \mathbb{R}^*$

On définit sur $]-c, c[$ la

loi suivante \perp par : $\perp(x, y) \in]-c, c[$

$$x \perp y = \frac{x+y}{1 + \frac{|xy|}{c^2}}$$

Verifier \perp est une loi sur $]c, c[$

2) Propriétés des lois de composition

internes

Soient $*$ et \perp 2 lois de composition internes sur un ensemble E .

2-1) Commutativité:

Définition : On dit que $*$ est commutative

si $\forall (x, y) \in E^2$, $x * y = y * x$

Exemple : 1- Dans \mathbb{R} , l'addition et la multiplication sont des opérations commutatives

En effet :

Soient $(x, y) \in \mathbb{R}^2$

Pour $+$: On a: $x+y = y+x$

Pour \times : On a $x \times y = y \times x$

Exemple: Dans $\mathcal{P}(\mathbb{E})$, l'intersection
et la réunion sont commutatives.

On effet: Soient A, B, C 3-éts de $\mathcal{P}(\mathbb{E})$

Pour \cap : On a $A \cap B = B \cap A$

Pour U : On a $A \cup B = B \cup A$.

2-2) Associativité:

Définition: On dit que $*$ est associative si $\forall (x, y, z) \in E^3$

$$(x * y) * z = x * (y * z)$$

Exemple: Dans \mathbb{R} , l'addition et la multiplication sont associatives.

S. a. d.:

sont $(x, y, z) \in \mathbb{R}^3$

Pour + : $(x+y)+z = x+(y+z)$

Pour \times : $(x \times y) \times z = x \times (y \times z)$

Exemple : Dans $\mathcal{P}(E)$, l'intersection
et la réunion sont des opérations associatives

c.a.d : Soient $(A, B, C) \in \mathcal{G}^3(\mathbb{E})$

Pour \cap : $(A \cap B) \cap C = A \cap (B \cap C)$

Pour \cup : $(A \cup B) \cup C = A \cup (B \cup C)$.

2-3) Élément neutre :

Définition: - On dit qu'un élément $e \in E$ est élément neutre à gauche pour la loi $*$ si

$$\forall x \in E, e * x = x$$

- On dit qu'un élément $e \in E$ est élément neutre à droite pour la loi $*$ si $\forall x \in E, x * e = x$

- On dit qu'un élément $e \in E$ est neutre pour l'algébre si $\forall x \in E, x * e = e * x = x$

Exemple: Dans \mathbb{R}

i) 0 est l'élément neutre de \mathbb{R} pour l'addition

car: $\forall x \in \mathbb{R}, x + 0 = 0 + x = x$

ii) 1 est l'élément neutre de \mathbb{R} pour la multiplication.

car : $\forall x \in \mathbb{R}, 1 \times x = x \times 1 = x$.

Exemple : Dans $\mathcal{G}(E)$

i) E est l'elt neutre de $\mathcal{G}(E)$ pour l'intersection

Car $\forall A \in S(\epsilon)$, $A \cap E = E \cap A = A$.

ii) ϕ est l'elt neutre de $S(\epsilon)$ pour la
réunion

Car $\forall A \in S(\epsilon)$, $A \cup \phi = \phi \cup A = A$.

Exemple : Dans \mathbb{R} , on dit definit la loi \perp

par $x \perp y = x - y$.

i) Cherchons $e \in \mathbb{R}$ tq $\forall x \in \mathbb{R}, e \perp x = x$

$$e \perp x = x \Rightarrow e - x = x$$

$$e = 2x$$

Donc l'élément à gauche de e n'existe pas.

ii) Cherchons $e \in \mathbb{R}$ tq $\forall x \in \mathbb{R}, x \perp e = x$

$$x \perp e = x \Rightarrow x - e = x$$

$$-e = 0 \Rightarrow e = 0$$

Donc l'élément à droite e existe



2-4) élément symétrique:

Soyent e l'elt neutre de E pour la loi $*$ et x un élément de E .

Définition: — On dit que x admet un symétrique à gauche pour la loi $*$ s'il existe un élément $x' \in E$ tel que $x'*x = e$.

- On dit que x admet un symétrique à droite pour la loi $*$ si existe un élément $x' \in E$ tel que $x * x' = e$.
- On dit que x admet un symétrique pour la loi $*$ si il existe un élément $x' \in E$ tel que $x * x = x * x' = e$.

~~Exemple~~ : Dans \mathbb{R}

i) Soit $x \in \mathbb{R}$, le symétrique de x pour l'addition s'appelle l'opposé de x et

est noté $(-x)$

c.a.d : $x + (-x) = (-x) + x = 0$

ii) Soit $x \in \mathbb{R}^*$, le symétrique de x pour
la multiplication s'appelle l'inverse de x
et est note

$$\frac{1}{x}$$

c.a.d:

$$\frac{1}{x} \times x = x \times \frac{1}{x} = 1.$$

2-5) Distributivité

Soient $*$ et \perp deux lois de composition internes sur E .

Définition: On dit que $*$ est distributive par rapport à la loi \perp si $\forall (x, y, z) \in E^3$

$$x * (y \perp z) = (x * y) \perp (x * z)$$

$$(y_1 z) * x = (y * x) \perp (z * x)$$

Exemple : Dans \mathbb{R}^3 la multiplication
est distributive par rapport à l'addition.

C'est à dire $\forall (x, y, z) \in \mathbb{R}^3$, $x \times (y + z) = xy + xz$
 $(y + z) \times x = y \times x + z \times x$.

Exemple : Dans $\mathcal{P}(E)$.

i) La réunion est distributive par rapport
à l'intersection

c.q.d : $\forall (A, B, C) \in \mathcal{P}(E)$.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

$$(B \cap C) \cup A = (B \cup A) \cap (C \cup A).$$

ii) L'intersection est distributive par rapport
à la réunion.

C.-à-d : $\forall (A, B, C) \in \mathcal{P}(\mathbb{E})^3$,

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$(B \cup C) \cap A = (B \cap A) \cup (C \cap A).$$

- § II) Groupes :
- 1) Définitions et exemples
- Définition : On appelle groupe, tout ensemble G muni d'une loi de composition interne notée $*$ et possédant les propriétés suivantes :
- 1 - la loi $*$ est associative
 - a - G admet un élément neutre pour la loi notée e

3. Tout élément de G admet un symétrique pour la loi $*$.

Remarque :

1- Si de plus la loi $*$ est commutative alors G est dit groupe commutatif ou abélien.

2- Si $(G, *)$ est un groupe alors le symétrique d'un élément x de G est noté par x^{-1} .

Exemple : - $(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$; $(\mathbb{C}, +)$

Sont des groupes abéliens.

- $(\{-1, 1\}, \times)$; (\mathbb{Q}^*, \times) ; (\mathbb{R}^*, \times) ; (\mathbb{C}^*, \times)

Sont des groupes abéliens.

Exemple :

Soit E un ensemble non vide et fini ; $\mathcal{S}(E)$: l'ensemble des bijections de E



est un groupe non nécessairement commutatif.

Cas particulier :

Si $E = \{1, 2, 3, \dots, n\}$

Définition : On appelle permutation de E ,
toute bijection σ de E dans E .

on note : S_n : l'ensemble des permutations de E
 (S_n, \circ) : est un groupe, appelé le groupe
des permutations.

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

Pour $n=2$:

$$I_d = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$J_2 = \{ I_d, \sigma_1 \}$$

avec

Pour $n=3$:

$$\text{card}(J_3) = 3! = 6$$

$$J_3 = \{ I_d, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \}$$

$$t u$$

$$I_d = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\sigma_1^2 = \sigma_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I_d ; \quad \sigma_2^2 = I_d \quad \text{et} \quad \sigma_3^2 = I_d$$

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_4 ; \quad \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_3$$

$$\sigma_4^2 = \sigma_4 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5 \quad = g$$

σ	I_d	σ_1	σ_2	σ_3	σ_4	σ_5
I_d	I_d	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	I_d	σ_4			
σ_2	σ_2	σ_5	I_d			
σ_3	σ_3	σ_4		I_d		
σ_4	σ_4	σ_3			I_d	
σ_5	σ_5	σ_4				I_d

table
de Cayley

Homework: Compléter la table de Cayley.

2) Sous-groupes:

Soit $(G, *)$ un groupe d'élément neutre e

2-1) Définitions et exemples.

Soit H une partie de G .

Définition

: On dit que H est un sous-groupe

si les conditions suivantes sont vérifiées :

- 1 - $H \neq \emptyset$
- 2 - $\forall (x, y) \in H^2, x * y \in H$
- 3 - $\forall x \in H, \exists x^{-1} \in H$

Définition: On dit que H est un sous-groupe

si : 1 - $H \neq \emptyset$
2 - $\forall (x, y) \in H, x * y^{-1} \in H$.

Remarque: H est un sous-groupe si et

seulement si $e \in H$ et $\forall (x, y) \in H$
 $x * y^{-1} \in H$.

Exemple: soit $(G, *)$ un groupe
d'élément neutre e .

Alors $\{e\}$ et G sont des
sous-groupes de G .

~~Exemple~~ : Considérons le groupe

abélien

$(\mathbb{R}, +)$

- \mathbb{Z} et \mathbb{Q} sont des sous-groupes de \mathbb{R}

- \mathbb{N} n'est pas un sous-groupe de $(\mathbb{R}, +)$

- \mathbb{Z} n'est pas un sous-groupe de (\mathbb{R}^*, \times)

Exemple : Considérons le groupe (\mathbb{C}^*, \times)

$$H = \{ z \in \mathbb{C}^* \mid |z| = 1 \}$$

est un sous-groupe de \mathbb{C}^* .

En effet :

i) On a $|1| = 1$. Donc $1 \in H$

ii) Soient z et z' deux éléments de H .
Vérifions $\bar{z} \times z' \in H$?

$$\beta \in H \Rightarrow |\beta| = 1$$

$$\beta' \in H \Rightarrow |\beta'| = 1$$

$$|\beta^{-1} \times \beta'| = |\beta^{-1}| \cdot |\beta'| = \frac{1}{|\beta|} \times |\beta'|$$

$$= \frac{1}{1} \times 1 = 1$$

$$\beta^{-1} \times \beta' \in H$$

D'où H est un sous-groupe de \mathbb{C}^* .

Exemple: Considérons le groupe $(\mathbb{Z}, +)$

Les sous-groupes de \mathbb{Z} sont de la forme $p\mathbb{Z}$ où $p \in \mathbb{N}^*$.

$\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, \dots$

2-2) Opérations sur les sous-groupes:

Soyons $(G, *)$ un groupe d'élément neutre

e, H, K & sous-groupes et

$(H_i)_{i \in I}$ une famille de sous-groupes de

a) Intersection:

Proposition: Les assertions suivantes sont vérifiées

- 1- $H \cap K$ est un sous-groupe de G
- 2- $\bigcap_{i \in I} H_i$ est un sous-groupe de G .

Preuve

1) On a $e \in H$ et $e \in K$
Donc $e \in H \cap K$

Donc $H \cap K \neq \emptyset$

ii) Soient x et y 2 éléments de $H \cap K$.

$$x \in H \cap K \Rightarrow x \in H \text{ et } x \in K$$

$$y \in H \cap K \Rightarrow y \in H \text{ et } y \in K$$

On a $\bar{x} * y \in H$ car H est un sous-groupe de G

$\bar{x} * y \in K$ car K est un sous-groupe de G

Donc $\bar{x} * y \in H \cap K$.

D'où $H\backslash K$ est un sous-groupe de G .

2 - Homework

b) Réunion :

Proposition : Les assertions suivantes sont

Vérifiées :

1- En général $H\backslash K$ n'est pas un sous-groupe.

2 - $H \cup K$ est un sous-groupe de $G \iff H \subset K$ ou $K \subset H$.

3 - Si $\forall i \in I$, $H_i \subset G$, $\exists k \in I$ tel que
 $H_i \subset H_k$ et $H_j \subset H_k$. Alors $\bigcup_{i \in I} H_i$
est un sous-groupe de G .

Preuve : 1) Considerons le groupe $(\mathbb{Z}_1^+, +)$
et $H = 2\mathbb{Z}$, $K = 3\mathbb{Z}$ deux sous-groupes

de \mathbb{Z} .

Vérifions que $H \cup K$ n'est pas un sous-groupe de \mathbb{Z} .

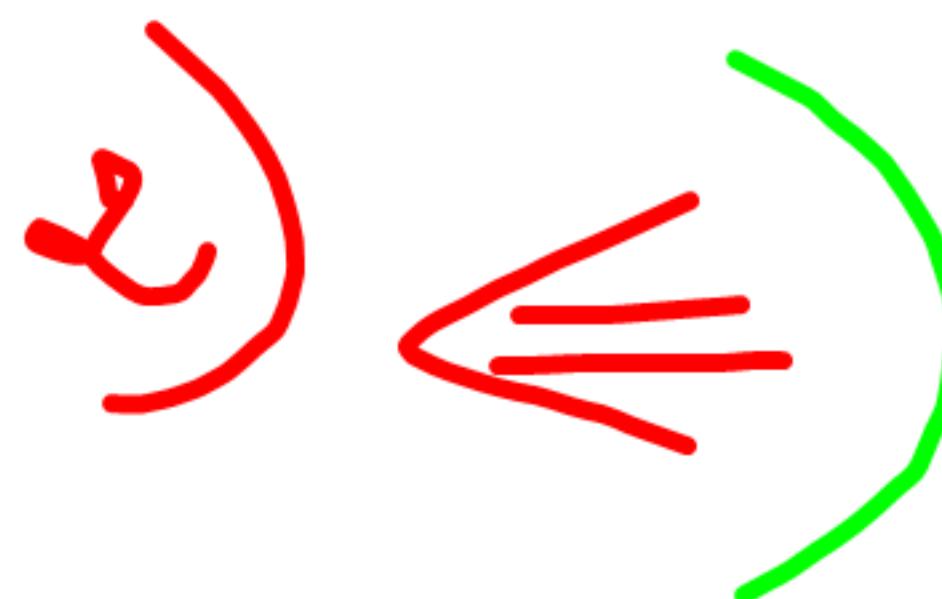
$$\text{On a } \alpha = 2x_1 \in H \subset H \cup K \implies \alpha \in H \cup K$$

$$\beta = 3x_1 \in K \subset H \cup K \implies \beta \in H \cup K$$

On a $2+3=5 \notin HUK$ car $5 \notin H$ et $5 \notin K$

D'mc HUK n'est pas stable pour l'addition

D'où HUK n'est pas un sous-groupe de \mathbb{Z} .



Supposons que $H \subset G$

Montrons que HUK est un sous-groupe de G ?

si HCK alors $HUK = K$

si KCH alors $HUK = H$

Donc HUK est un sous-groupe de G

Supposons que HUK est un sous-groupe
Montrons que HCK ou KCH ?

Montrer que $H \subset K$ ou $K \subset H$ \iff
(si $H \not\subset K$ alors $K \subset H$) et (si $K \not\subset H$ alors $H \subset K$)

Supposons que $H \not\subset K$ et montrons que $K \subset H$
Il existe $x \in K$. Vérifions que $x \in H$?

Comme $K \subset H \cup K$, donc $x \in H \cup K$

$H \not\subset K \Rightarrow \exists y \in H$ et $y \notin K$.

Comme $y \in H$ et $H \subset HUK$, donc $y \in HUK$.

$$\begin{array}{c} x \in HUK \\ y \in HUK \end{array} \quad \left\{ \Rightarrow \bar{x}^{-1} * y \in HUK \right.$$

Car HUK est un sous-groupe

Supposons par l'absurde que $\bar{x}^{-1} * y \notin K$.

On a $\bar{x}^{-1} * y \in K$ et $x \in K$

Comme K est un sous-groupe, donc $x * (\bar{x}^{-1} * y) \in K$
 $(x * \bar{x}^{-1}) * y = e * y = y \in K$

Ce qui est une contradiction. Donc $\bar{x}^{-1} * y \notin K$.

Comme $\left\{ \begin{array}{l} \bar{x}^{-1} * y \in H \cup K \\ \bar{x}^{-1} * y \in K \end{array} \right.$. Donc $\bar{x}^{-1} * y \in H$.

Or $\left\{ \begin{array}{l} \bar{x}^{-1} * y \in H \\ y \in H \end{array} \right.$ $\Rightarrow (\bar{x}^{-1} * y) * \bar{y}^{-1} \in H$

car H est un sous-groupe de G .

$$\bar{x} * (y * \bar{y}^{-1}) = \bar{x}^{-1} * e = \bar{x} \in H^{-1}$$

Comme H est 1 sous-groupe, donc $(x^{-1}) \in H$

$x \in H$.

Donc KCH .

Donc si $H \neq K$ alors KCH

De manière analogue. On montre que si

KCH alors HCK

Donc le résultat

3 - Homework :

① Produit de sous-groupes :

Sont H et K des sous-groupes de G

$$H * K = \{x * y \mid x \in H, y \in K\}$$

Proposition: Les assertions suivantes sont

1. vérifiées :

1- En général $H * K$ n'est pas un sous-groupe de G .

2- $H * K$ est un sous-groupe de $G \iff H * K = K * H$.

Preuve : 1) - Considérons le groupe symétrique

avec $\mathcal{G}_3 = \{I_d, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$

$I_d = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
 $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$H = \{I_d, \sigma_1\}$ et $K = \{I_d, \sigma_2\}$

H et K sont des sous-groupes de \mathcal{G} .

$$H \circ K = \{x \circ y \mid x \in H, y \in K\} = \{I_d, \sigma_1, \sigma_2, \sigma_4\}$$

or $\sigma_4^{-1} = \sigma_5 \notin H \circ K$.

Donc $H \circ K$ n'est pas un sous-groupe de \mathcal{G} .

& - Homework:

d) Sous-groupes engendrés :

Soient $(G, *)$ un groupe d'élément neutre e
et A une partie de G .

Définition : On appelle sous-groupe de G
engendré par A , l'intersection de tous les
sous-groupes de G contenant A .
On note $\langle A \rangle$.

Remarque :

- 1 - $\langle A \rangle$ est le plus petit des sous-groupes de G contenant A .
- 2 - Si $H = \langle A \rangle$ alors A s'appelle la partie génératrice de H .
- 3 - Si $A = \emptyset$ alors $\langle A \rangle = \{e\}$

4- Si $A \neq \emptyset$ alors $\langle A \rangle$ est l'ensemble

$$H = \left\{ x = a_1^{d_1} * a_2^{d_2} * \cdots * a_n^{d_n} \mid \begin{array}{l} n \in \mathbb{N}^+ \\ a_i \in A \\ d_i = \pm 1 \end{array} \right.$$
$$= \left\{ a_1^{d_1} * a_2^{d_2} * \cdots * a_n^{d_n} \mid a_i \in A \cup A^{-1}, n \in \mathbb{N}^+ \right\}$$

Définition: On dit que G est un groupe de type fini s'il admet un système génératrice fini.

Définition: Un groupe G est dit monogène si il existe $a \in G$ tel que $G = \langle a \rangle = \langle \{a\} \rangle$, avec $\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$.

Definition: On appelle groupe cyclique tout groupe monogène fini.

Exemple: $(\mathbb{Z}, +)$ est un groupe monogène

$$\mathbb{Z} = \langle 1 \rangle$$

En effet: Soit $x \in \mathbb{Z}$

$$x = \begin{cases} 1 - 1 & \text{si } x = 0 \\ 1 + 1 + 1 + \dots + 1 & x \text{ fois si } x > 0 \\ -1 - 1 - 1 - 1 - \dots - 1 & |x| \text{ fois si } x < 0 \end{cases}$$

Exemple

$$G = \mathcal{G}_3 = \{ \text{Id}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \}$$

$A = \{\sigma_1, \sigma_4\} \cdot \text{On a } \mathcal{G}_3 = \langle A \rangle$

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\text{Id} = \sigma_4^3; \quad \sigma_3 = \sigma_4 \circ \sigma_1; \quad \sigma_5 = \sigma_4^2$

$= \sigma_1 \circ \sigma_1;$ $\sigma_2 = \sigma_1 \circ \sigma_4.$

Exemple : Considérons le groupe (\mathbb{C}^*, \times)

$$H = \left\{ z \in \mathbb{C}^* \mid z^n = 1 \right\}$$

Pour $w = e^{\frac{2\pi i}{n}}$

On a $H = \langle w \rangle$

III) Homomorphisme - Groupe-quotient

1) Homomorphisme de groupes:
Soient $(G, *)$ et (G', \cdot) deux groupes
d'éléments neutres respectifs e et e' .

Definition: On appelle homomorphisme ou morphisme toute application $f: (G^*) \rightarrow (G'^*)$ vérifiant $\forall (x, y) \in G$, $f(x * y) = f(x) + f(y)$

Exemple: $f: (\mathbb{R}^*, +, \times) \rightarrow (\mathbb{R}, +)$ tel que $f(x) = \ln(x)$

En effet Soient $(x, y) \in \mathbb{R}_+^*$

$$\begin{aligned} f(x \times y) &= \ln(x \times y) \\ &= \ln(x) + \ln(y) \\ &= f(x) + f(y) \end{aligned}$$

Donc f est un homomorphisme de groupes.

~~Example~~: $g: (\mathbb{R}_+, +) \rightarrow (\mathbb{R}^*, +, \times)$

g est un morphisme de groupes.

~~En effet:~~

Soient $(x, y) \in \mathbb{R}^2$

$$g(x+y) = e^{x+y} = e^x \times e^y = g(x) \times g(y)$$

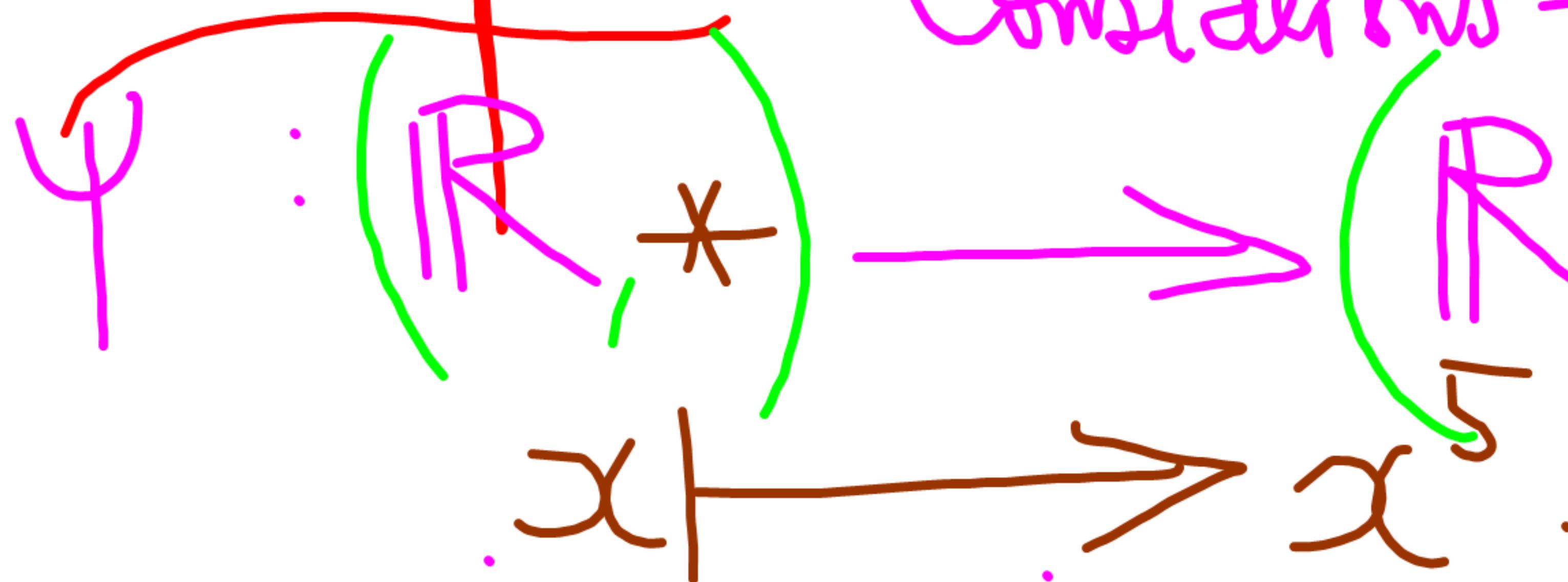
g est un morphisme de groupes.

Définition: On appelle endomorphisme de G tout morphisme f de G dans G .

Définition: On appelle isomorphisme entre G et G' tout homomorphisme bijectif $f: G \rightarrow G'$

Définition: On appelle automorphisme de G tout endomorphisme de G qui est bijectif.

Exemple:



Considérons l'application

$$\text{avec } x * y = \sqrt[5]{x^5 + y^5}.$$

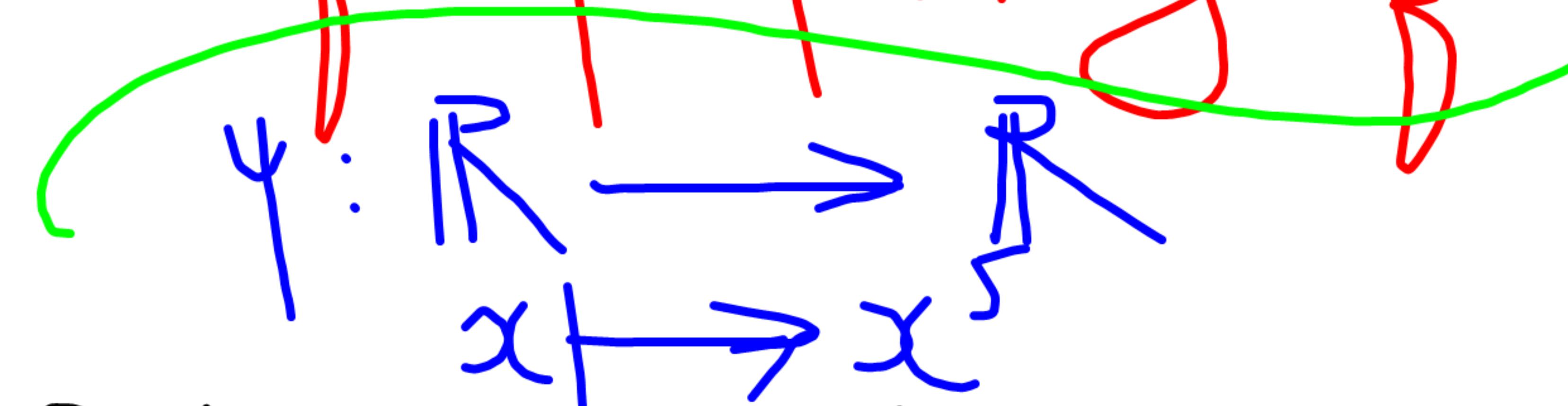
Ψ est un isomorphisme de groupes.

En effet :

i) Montreons que Ψ est un morphisme.

$$\begin{aligned} \text{Soient } (x, y) \in \mathbb{R}^2, \quad & \Psi(x * y) = (x * y)^5 \\ & = (\sqrt[5]{x^5 + y^5})^5 = x^5 + y^5 = \Psi(x) + \Psi(y). \end{aligned}$$

ii) Vérifions que ψ est bijective.



Soit $y \in \mathbb{R}$, cherchons $x \in \mathbb{R}$ tel que

$$y = \psi(x)$$

$$x = \sqrt{y} \Rightarrow x = \sqrt{y}$$

Donc ψ est bijective.

D'où ψ est un isomorphisme de groupes.

~~Remarque : Soit $f: (G, *) \rightarrow (G', \cdot)$~~

~~un morphisme de groupes. Alors les~~

~~assertions suivantes sont vérifiées.~~

1 - $f(e) = e'$

2 - $\forall x \in G, f(x^{-1}) = [f(x)]^{-1}$.

En effet i) Montre que $f(e) = e'$
 On a $e * e = e$
 $f(e * e) = f(e)$ $\Rightarrow f(e) \perp f(e) = f(e)$
 $f(e) \perp (f(e) \perp f(e)) = f(e) \perp (f(e))$
 $f(e) \perp e = e'$

ii) Montrons $\forall x \in G$, $f(\bar{x}^{-1}) = (f(x))^{-1}$

On a $x * \bar{x}^{-1} = \bar{x}^{-1} * x = e$

$$f(x * \bar{x}^{-1}) = f(\bar{x}^{-1} * x) = f(e) = e'$$

$$f(x) \perp f(\bar{x}^{-1}) = f(\bar{x}^{-1}) \perp f(x) = e'$$

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

Proposition: Soit $f : (G, *) \rightarrow (G', \cdot)$

un morphisme de groupes. Alors les assertions suivantes sont vérifiées

- 1 - Si H est un sous-groupe de G alors $f(H)$ est un sous-groupe de G' .
- 2 - Si H' est un sous-groupe de G' alors $f^{-1}(H')$ est un sous-groupe de G .

Définition: Soit $f: (G, *) \rightarrow (G', \cdot)$
un morphisme de groupes.
On appelle noyau de f , le sous-groupe

$$\bar{f}^{-1}(\{e'\})$$

On note

$$\text{Ker}(f) = \{x \in G \mid f(x) = e'\}$$

Définition : Soit $f: (G, *) \rightarrow (G', \cdot)$ un morphisme de groupes.

On appelle image de f , le sous-groupe $f(G)$.

On note : $\overline{\text{Im}}(f) = \{y \in G' \mid \exists x \in G : y = f(x)\}$

~~Proposition :~~ Soit $f: (G_1^*, \cdot) \rightarrow (G_1' \sqcup)$

un morphisme de groupes. Alors

f est injectif si et seulement si $\text{Ker}(f) = \{e\}$

Preuve :

Supposons que f est injective et montrons que $\text{Ker}(f) = \{e\}$

Soit $x \in \text{Ker}(f)$.

Donc $f(x) = e$ or $f(e) = e'$

$$\begin{cases} f(x) = e' \\ f(e) = e' \end{cases} \Rightarrow f(x) = f(e)$$

Comme f est injective, donc $x = e$

Donc $\text{Ker}(f) = \{e\}$.

\Leftarrow Supposons que $\text{Ker}(f) = \{e\}$.
Montrons que f est injective.

- Soient $(x, x') \in G^2$ tels que $f(x) = f(x')$

$$f(x) \perp f(x') \Rightarrow f(x) = e$$
$$f(x) \perp f(x') \Rightarrow f(x') = e$$
$$f(x) \perp f(x'^{-1}) = e$$
$$f(x * x'^{-1}) = e$$

Donc $x * \bar{x}'^1 \in \text{Ker}(f)$

or $\text{Ker}(f) = \{e\}$.

Donc $x * x' = e$.

$$x * (\bar{x}'^1 * x') = e * x'$$

$$x * e = x' \Rightarrow x = x'$$

Donc f est injective.

2) Groupe-quotient :

2-1 Ordre d'un groupe :

Soit $(G, *)$ un groupe d'élément neutre

Definition : On appelle ordre de G, k .

Cardinal de G .

On note : $\text{ordre}(G) = {}^o(G) = \text{Card}(G) = |G|$

Remarque :

l'ordre du groupe G est le plus petit λ tel que $\forall x \in G, x^\lambda = e$.

avec $x^\lambda = x * x * \dots * x$
 λ fois.

Definition:

Soit $a \in G$.

On appelle ordre de a , le cardinal du sous-groupe engendré par a .

On note :

$${}^o(a) = {}^o(\langle a \rangle) = \text{card}(\langle a \rangle)$$

Exemple :

$$G = \{-1, 1\} \quad (G, \times) \text{ est un groupe}$$

$${}^o(G) = 2.$$

Exemple :

• (S_n, \circ) est un groupe

$$\bullet (S_n) = n!$$

$$\bullet (S_3) = 3! = 6$$

Exemple :

e	a	b	c
a	e	b	c
b	c	e	a
c	b	a	e

$$K = \{e, a, b, c\}$$

(K, \circ) est un groupe, appelé

Le groupe de Klein

$$\circ(K) = \text{card}(K) = 4$$

Homework: Chercher les autres groupes d'ordre 4.

Théorème: (théorème de Lagrange)

Soit H un sous-groupe de G .

Alors l'ordre de H est un diviseur de l'ordre de G .

Exemple :

- \mathbb{Z}_n est un groupe d'ordre fini
- \mathbb{Z} est un groupe d'ordre infini

2-2) Structure de groupe-quotient:

Soyons $(G, *)$ un groupe d'élément neutre e
et H un sous-groupe de G .

Proposition:
—sont vérifiées :

Les assertions suivantes

1 - La relation binaire R' définie sur G par
 $\forall (x, y) \in G^2 (x R' y \Leftrightarrow \exists g \in G. x * y * g^{-1} \in H)$

est une relation d'équivalence sur G .

2 - La relation binaire R'' définie sur G par
 $\forall (x, y) \in G^2 (x R'' y \Leftrightarrow y * x^{-1} \in H)$

est une relation d'équivalence sur G .

3 - La classe d'équivalence modulo R d'un élément x de G est $\dot{x} = x * H$.

4 - La classe d'équivalence modulo R d'un élément x de G est $\dot{x} = H * x$.

Preuve : 1) Montrons que R est une relation d'équivalence sur G ?