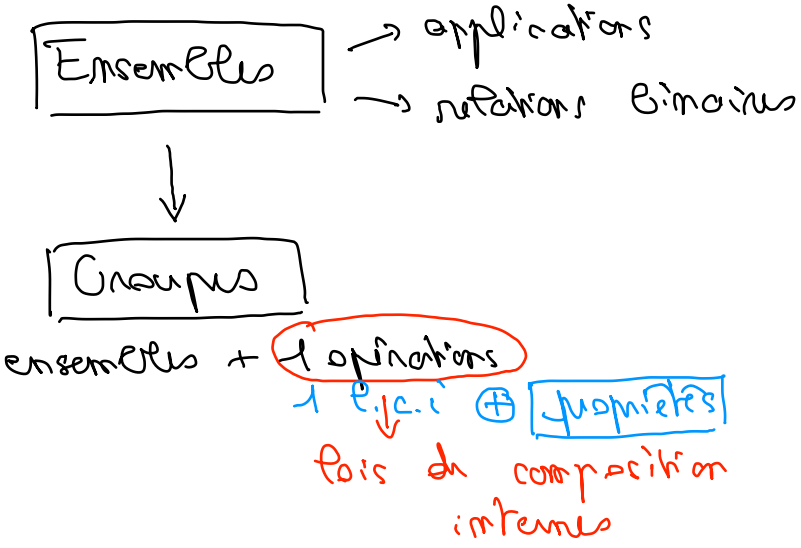
Chapitre 3 - Lois de composition internes, groupes



I. Lois de composition internes (l.c.i)

E : ensemble

* **déf:** une loi de composition interne sur E est une application

$$E \times E \longrightarrow E$$

→ un calcul entre éléments → produit 1 élt du même type

Notée de manière générique $*$ $(a * b)$

ex: sur $\mathbb{Z}$

$+ \quad \times \quad / \quad - \qquad x \bmod y$

↓ division euclidienne

$x \equiv y \ [n]$ bool $\qquad \mathbb{Z} \times \mathbb{Z} \longrightarrow$ bool

$x, y \in \mathbb{Z}$; relation binaire

---

sur $\mathcal{P}(E)$

$A, B \in \mathcal{P}(E)$

$A \subseteq E$

$B \subseteq A$

$\cup$

$\cap$

Δ

C_A^B

$\neq$ rel. binaires $\subset$

Sur mots

$m_1 \cdot m_2$

↓ concaténation

≠ rel. binaires

m_1 sous-mot m_2 préfixe

Sur $\mathbb{R}^n \sim (x_1, x_2, \dots x_n) \in \mathbb{R}^n$

$\vec{x}$

$\vec{x} + \vec{y}$

$\vec{x} * \vec{y}$?

Sur $\mathbb{R}^3$ $\vec{x} \wedge \vec{y}$ ← produit interne pas défini sur les vecteurs

$\vec{x} \cdot \vec{y}$ $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ pas lci

$\mathbb{R}$

Sur | fonctions de $E \to E$
groupe symétrique
fonctions bijectives
composition $\circ$

Quelles sont les propriétés caractéristiques des lci

Dans la suite $*$ est une lci sur E

→ associativité → le parenthésage n'est pas important

$\forall x,y,z \in E \quad x * (y * z) = (x * y) * z$

ex: Sur $\mathbb{Z}$ $+$ $\times$ $-$ $/$

$+$: assoc $i + (j + k) = (i + j) + k$

$\times$: assoc

$-$: $i - (j - k) \neq (i - j) - k$

Sur $\mathcal{P}(E)$: $\cup$ (assoc), $\cap$ (assoc), Δ (assoc)

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

$A \Delta (B \Delta C) = (A \Delta B) \Delta C$

Sur $\mathbb{R}^3$: $+$

$\vec{x} + (\vec{y} + \vec{z}) = (\vec{x} + \vec{y}) + \vec{z}$

~~Δ~~

$\vec{x} \wedge (\vec{y} \wedge \vec{z}) \neq (\vec{x} \wedge \vec{y}) \wedge \vec{z}$

$(\vec{x} \cdot \vec{y})\vec{z} - (\vec{x} \cdot \vec{z})\vec{y}$

Sur mots : $m_1 \cdot (m_2 \cdot m_2) = (m_1 \cdot m_1) \cdot m_3$

→ existence d'un élément neutre

$e \in E$ est neutre pour $*$ si

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

Prop. S'il existe, le neutre est unique

dém : par l'absurde, si e, e' sont neutres $\quad e = e'$? ✗

$e * e' \overset{e \text{ neutre}}{=} e'$

e' neutre $\parallel$

e Donc $e = e'$ ✓

◇

On parle donc du neutre (unique).

ex :

$\mathbb{Z}$	$+0$	$\times 1$
$\mathcal{P}(E)$	$\cap E$	$\cup \emptyset$ $\quad \Delta \emptyset$
$\mathbb{R}^n$	$+ \vec{0}$	
mots	concaténation	ε

neutres

→ **Eléments symétrisables**

$x \in E$ | admet un symétrique pour $*$ si et symétrisable

$\exists y \in E$ tq $x * y = y * x = e$

ex: dans $\mathbb{Z}$: $x + (-x) = 0$ → x symétrisable pour $+$

mot x cryptage $x + clé$ → $+(-clé)$

$x * clé * (.?.) = x$

sym de la clé

Prop. si x est symétrisable et $*$ associative

le symétrique y est unique

dém:

Par l'absurde, si y_1, y_2 sont deux symétriques de x ($y_1 = y_2$?)

y_1 est sym. de x : $x * y_1 = e$

$y_2 * (x * y_1) = y_2 * e$ (y_1 sym. de x)

$= y_2$ car e neutre

$*$ ‖ assoc

$(y_2 * x) * y_1$

y_2 ‖ symétrique de x

e

‖

$e * y_1$

‖

y_1

$= y_1$?

$y_1 = y_2$ ✓

◇

Si $*$ associative le symétrique de x, s'il existe est unique

$\rightsquigarrow \tilde{x}$

$\rightsquigarrow e$ est toujours symétrisable $\tilde{e} = e$

ex:

sur $\mathbb{Z}$	$+$	$\times$
e	0	1
symétrisables	tous	$-1, 1$ symétrisable
i	$\tilde{i} = -i$	$\tilde{1} = 1$

~~0~~ ~~2~~

$2 \times \tilde{2} = 1$ dans $\mathbb{Z}$ ....

sur $\mathbb{Q}$

$\mathbb{Q}^*$ symétrisables $\frac{p}{q} \times \left(\frac{q}{p}\right) = 1$ $\left(\widetilde{\frac{p}{q}}\right)$

sur $\mathcal{P}(E)$	$\cup$	$\cap$	Δ
e	$\emptyset$	E	$\emptyset$
symétrisables	seul $\emptyset$	seul E	tout $A \in \mathcal{P}(E)$ $\tilde{A} = A$
	$A \cup \emptyset = \emptyset$ (e)	$A \cap E = E$ (e)	$A \Delta \tilde{A} = \emptyset$ ($A = \tilde{A}$)

commutativité

$*$ commutative si $\forall x, y \in E \quad x * y = y * x$

commutative

ex:

$\mathbb{Z} \to + \quad \times$

$\mathcal{P}(E) \to \cap \quad \cup \quad \Delta$

non commutative

mots $\to$ concaténation

matrices $\to \times$

fonctions $E \to E$ $\to \circ$

$f \circ g \neq g \circ f$

ex :

(fonctions $E \to E$) ensemble

$\circ$

loi :

→ assoc ? $f \circ (g \circ h) = (f \circ g) \circ h$ ✓

→ neutre ? $id_E : E \to E$, $x \mapsto x$ $\quad f \circ id = id \circ f = f$ ✓

→ fonctions symétrisables ? ⇢ $\exists g$ tq $f \circ g = id$, $g \circ f = id$

→ fonctions bijectives ⇔ inversibles

$\Downarrow$

$g = f^{-1}$ existe seulement si f bijective.

(f bijective $\Leftrightarrow$ injective + surjective

$\exists$ application réciproque (unique) f^{-1} tq $f \circ f^{-1} = f^{-1} \circ f = id$)

$\widetilde{\mathcal{F}}(E,E)$ = (fonctions $E \to E$)

$\Downarrow$

seules les fct. bijectives sont symétrisables / $\circ$

→ associative ✓

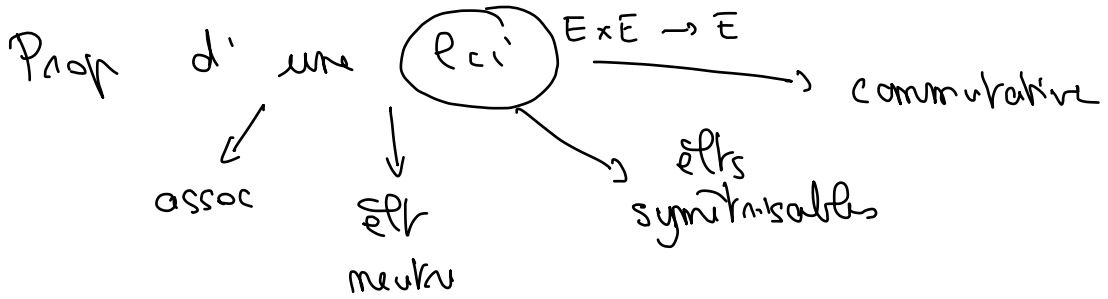
→ neutre : fonction nulle

→ $\widetilde{f} = (-f)$ — toutes les fct sont symétrisables.

$f + \widetilde{f} = 0$

→ $\widetilde{\mathcal{F}}(\mathbb{R},\mathbb{R})$, $+$

$f + g$



II. Groupes

(1) Généralités

* **déf:** Soit G un ensemble
  * une l.c.i sur G

  $(G, *)$ est un **groupe** si
  - i) $*$ associative
  - ii) $*$ admet un élément neutre
  - iii) tous les éléments de G sont symétrisables.

  Si en plus $*$ commutative
  G groupe **commutatif** ou **abélien**

ex: sur $\mathbb{Z}$ $(\mathbb{Z}, +)$ Groupe commutatif

$(\mathbb{Z}, \times)$ n'est pas symétrisable pour $\times$ ($\frac{1}{n} \notin \mathbb{Z}$)

$(\mathbb{Q}^*, \times)$

sur $\mathcal{P}(E)$ $(\mathcal{P}(E), \Delta)$ groupe commutatif

$\cup$ $\cap$ Δ $\tilde{A} = A$

Par mots $\quad$ (mots, ~~...~~)

② $\mathbb{Z}/n\mathbb{Z}$

Rappel : ensemble quotient de $\mathbb{Z}$ par la relation d'équivalence $\equiv [n]$ $\quad = \mathcal{R}_n$

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\mathcal{R}_n$$

$\downarrow$

ensemble des classes d'équivalence de $\mathbb{Z}$ pour $\mathcal{R}_n : \equiv [n]$

$\mathbb{Z}/5\mathbb{Z} \rightsquigarrow$ 5 elts $\quad \{ \dot{0}, \dot{1}, \dots, \dot{4} \}$

$\dot{0} = \dot{5} = \dot{10} = \dots$

$\dot{1} = \dot{6} = \dot{-4} = \dots$

$\dot{x} = \dot{y}$ ssi $x \mathcal{R} y$

$\mathbb{Z} \rightsquigarrow x \overset{\times}{+} y$ l.c.i tq $(\mathbb{Z}, +)$ groupe commutatif, $(\mathbb{Z}, \times)$ ~~×~~

$x \mapsto \dot{x}$ dans $\mathbb{Z}/n\mathbb{Z}$

$\dot{x} \oplus \dot{y} = \dot{x+y}$ opération quotient ? (bien définie ?)

Prop $\oplus$ et $\otimes$ sont bien définies sur $\mathbb{Z}/n\mathbb{Z}$

$$\dot{x} \otimes \dot{y} = \dot{\overline{x \times y}}$$
$$\dot{x} \oplus \dot{y} = \dot{\overline{x + y}}$$

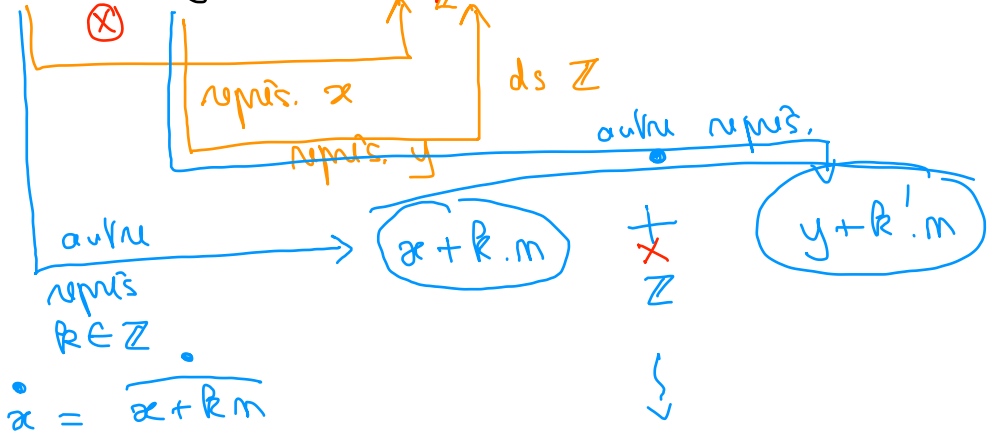
opérations de $\mathbb{Z}$ usuelles

"dém"

Bien définie ? Vérifier !

$$\dot{x} \oplus \dot{y} = \dot{\overline{x+y}}$$

$\otimes$



même résultat ?

$$\dot{\overline{(x+kn)+(y+k'n)}} = \dot{\overline{x+y+(k+k')n}} = \dot{\overline{x+y}} \quad \checkmark$$

$\oplus$ bien définie

$\otimes$ $\dot{\overline{(x+kn) \times (y+k'n)}} \overset{?}{=} \dot{\overline{x \times y}}$

$$\dot{\overline{xxy + x.k'n + kny + kk'n^2}}$$

$$n(xk' + ky + kk'n)$$

Donc $\otimes$ bien définie

Proposition $\left(\mathbb{Z}/n\mathbb{Z}, \oplus\right)$ $\left(\{\dot{0}, \dot{1} \dots \dot{n-1}\}\right)$ est un groupe commutatif fini

- $e = \dot{0}$
- $\widetilde{\dot{m}} = \dot{-m}$

$\dot{x} \oplus \dot{0} = \dot{\overline{x+0}} = \dot{x}$

groupe quotient

Proposition $\left(\mathbb{Z}/n\mathbb{Z}, \otimes\right)$ n'est pas un groupe

i) neutre : $\dot{1}$ $\quad \dot{1} \otimes \dot{x} = \dot{\overline{1 \times x}} = \dot{x}$

ii) Les symétrisables sont tous les $\dot{m}$ tq $\text{pgcd}(n, m) = 1$

ex: $\mathbb{Z}/8\mathbb{Z}$ ⟶ les symétrisables pour $\otimes$: $\{\dot{1}, \dot{3}, \dot{5}, \dot{7}\}$ $\dot{m}$ avec $\text{pgcd}(m, 8) = 1$

ds $\mathbb{Z}$, ~~$\widetilde{\dot{2}}$~~

$\widetilde{\dot{3}} \cdot \dot{3} = \dot{1}$

$\widetilde{\dot{5}} \cdot \dot{5} = \dot{1}$

$\widetilde{\dot{7}} \cdot \dot{7} = \dot{1}$

$\widetilde{\dot{1}} \cdot \dot{1} = \dot{1}$ ← neutre

$\widetilde{\dot{m}}$ pour $\otimes$

③ Sous-groupes

Ensembles ⟶ sous-ensembles

?

↓

connaître la notion se comporte avec un groupe ?

$(G, *)$ groupe

soit $A \subseteq G$ (sous-ensemble de G)

$(A, *)$ groupe ?

ex: $(\mathbb{Z}, +)$

$A = \{2\} \subseteq \mathbb{Z}$ sous-ensemble

$(A, +)$ groupe ? — pas de neutre

l.c.i ?

$A_1 = \{0, 2\}$

$(A_1, +)$ groupe ? — neutre 0 ✓

l.c.i — 2 pas symétrisable.

l.c.i :
2 elts : x, y
$x + y \in$ ensemble ...

$A_2 = \{-2, 0, 2\}$

$(A_2, +)$ groupe ? — $2+2 \notin A_2$

l.c.i

$A_3 = \{0\}$ $(A_3, +)$ groupe

$A_4 = \{ 2k ; k \in \mathbb{Z} \} \subseteq \mathbb{Z}$ (contient 0, 2)

+ l.c.i sur A_4

neutre : $0 \in A_4$ ✓

tous les elts sont symétrisables

$(A_4, +)$ groupe

$A_4 \subsetneq \mathbb{Z}$

$\rightarrow A_4$ sous-groupe de $\mathbb{Z}$ $(A_4 \lhd \mathbb{Z})$

* déf: soit $H \subseteq G$ $(G, *)$ groupe

On dit que $(H, *)$ est un sous-groupe de $(G, *)$ si

$(H, *)$ groupe

Prop (caractérisation d'un sous-groupe)

$H \subseteq G$ est un sous-groupe de G ssi :

i) $H \neq \emptyset$

et

ii) • H stable par $*$ ($*$ lci sur H) : $\forall x,y \in H \quad x * y \in H$

• H stable par les symétriques : $\forall x \in H \quad \tilde{x} \in H$

$\forall x,y \in H \quad x * \tilde{y} \in H$

Version longue $\Longleftrightarrow$ Version courte

↓

dém:

$e \in H$?

$H \neq \emptyset \rightsquigarrow \exists x \in H$ $\xrightarrow{H \text{ stable par Cosym}}$ $\tilde{x} \in H$ $\xrightarrow{H \text{ stable par } *}$ $x * \tilde{x} \in H$, $x * \tilde{x} = e$

④ Construire des sous-groupes $\rightsquigarrow$ sous-groupe engendré

$(G, *)$ groupe

$A \subseteq G$ sous-ensemble quelconque $(\neq \emptyset)$

1) ajouter tous les sym. des éls de A

2) ajouter toutes les combinaisons entre ces éléments

stabilité par $*$

stabilité par les sym ✓

H sous-groupe engendré par A

sous-groupe de G

$G_n(A)$

$(A, *)$ groupe — souvent non ....

* **def:** soit $A \subseteq G$ avec $(G, *)$ groupe

Le sous-groupe engendré par A ($G_n(A)$) est le plus petit sous-groupe de G contenant A.

$H \subseteq G$

ex : ds $(\mathbb{Z},+)$ $A=\{2\}$ ⟶ pas un sous-groupe de $\mathbb{Z}$ …

$Gr(A) = \{ 2k \ ; \ k \in \mathbb{Z} \}$

$A=\{2\}$

ajouter des éléments pour obtenir 1 groupe

-2 $\quad 2+(-2)=0$

+ ici $\quad 2+2+\cdots+2$

$-2-2\ldots-2$

$Gr(A)$

$-4+9$

$4-4-4+6-6+9$

$4+6+-4+-4+-6+9$

k $\quad k'$

$4+\cdots+4 + 6+\cdots+6$

$k.4 + k'.6 + k''.9$

$3.4+1.6+1.9$

+ commut ↑

$4+6+4+4+9$

$(\mathbb{Z},+)$

$Gr\{4,6,9\} = \{ x_1+\cdots+x_k \ ; \ x_i = 4,6,9 \text{ ou } -4,-6,-9 \}$

A

Prop Caractérisation combinatoire

i) Cas général

$Gr(A) = \{ x_1 * \cdots * x_k \ ; \ k \in \mathbb{Z}, \ x_i \in A \cup \tilde{A} \}$ (*)

$\tilde{A}$: ensemble des symétriques des éls de A

ii) Si $*$ commutative

On peut simplifier (*) en :

$Gr(A) = \{ x_1^{(k_1)} * \cdots * x_m^{(k_m)} \ ; \ x_i \in A, \ k_i \in \mathbb{Z} \}$

avec $x^{(k)} = \underbrace{x * \cdots * x}_{k \text{ fois}}$ si $k \geq 0$

notation $= \underbrace{\tilde{x} * \cdots * \tilde{x}}_{-k \text{ fois}}$ si $k<0$

ex :

pour $+$ $\quad x^{(3)} = \overbrace{x+x+x}^{3} = 3.k$

pour $\times$ $\quad x^{(3)} = \overbrace{x \times x \times x}^{3} = x^3$

$k=-3$

$x^{(-3)} \overset{\text{def}}{=} \underbrace{\tilde{x} * \tilde{x} * \tilde{x}}_{-k \text{ fois}}$ ($-k = 3$)

Prop.

Les sous-groupes de $(\mathbb{Z}, +)$ sont les $n\mathbb{Z}$. (→ sous-groupe de $(\mathbb{Z},+)$)

$n\mathbb{Z} = \{k.n ; k \in \mathbb{Z}\}$

(5) Morphismes de groupes

$(\mathbb{Z}/12\mathbb{Z}, \otimes)$

↓

$(\{\dot{1}, \dot{5}, \dot{7}, \dot{11}\}, \otimes)$ — groupe à 4 éléments

$g \circ$ le même à renommage près

$(\mathbb{Z}/4\mathbb{Z}, \oplus)$ — groupe à 4 éléments

morphisme de groupes

$(\mathbb{R}, +)$ groupe

$(\mathbb{R}_+^*, \times)$ groupe

$x + y \xrightarrow{f(x+y) = f(x) \times f(y)}$

$f = $ exponentielle

$f : (\mathbb{R}, +) \xrightarrow{\text{bij}} (\mathbb{R}_+^*, \times)$ isomorphisme de groupes

$x \longmapsto e^x$

$x+y \longrightarrow e^{x+y} = f(x+y)$

$f(x) \times f(y) = e^x \times e^y$

* **déf :** $f : G \longrightarrow G'$ avec $(G, *)$ et $(G', *')$ deux groupes
($*$ sur G, $*'$ sur G')

est un **morphisme de groupes** si (iso : si f bijective)

$\forall x, y \in G \quad f(x * y) = f(x) *' f(y)$

$f : G \longrightarrow (G', *')$

Prop. $\mathrm{Im} f = f(G) = \{ f(x) ; x \in G \}$ est un sous-groupe de $(G', *')$ ($\subset G'$)

(Im f : l'image directe de G par f (§1))

* **déf :** $f : G \longrightarrow G'$ morphisme
(e' neutre de G')

(antécédents : . . . .)

on appelle **noyau de f** (Ker f) :

$\mathrm{Ker} f = \{ x \in G ; f(x) = e' \}$ — sous-groupe de $(G, *)$

(Ker f : antécédents de e')

Prop. f morphisme est injective ssi

$\mathrm{Ker}(f) = \{e\}$ — réduit à 1 élt. $\equiv$ si e' n'a qu'un antécédent (e)