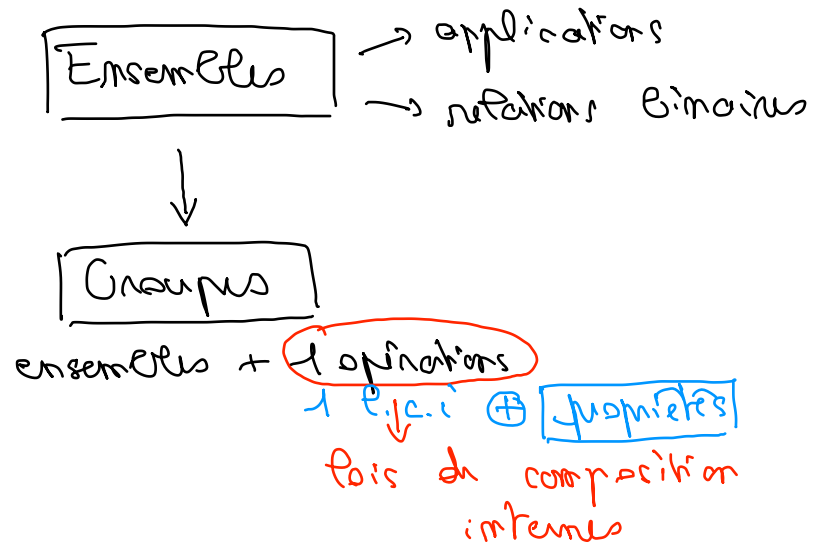


Chapitre 3 - Lois de composition internes, groupes



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

E : ensemble

* def: une loi de composition interne sur E

est une application
 $E \times E \rightarrow E$

→ un calcul entre éléments
 ↓
 produit et est du même type

Note de maniere générique $*$
 $(a * b)$

ex: sur \mathbb{Z}

+ x / - x mod y
 ↓
 division euclidienne

$x \equiv y [m]$

$\mathbb{Z} \times \mathbb{Z} \rightarrow \text{bool}$
 relation binaire

sur $\mathcal{P}(E)$	U	\neq r.e. binaires \subseteq
$A, B \in \mathcal{P}(E)$	∩	
$A \subseteq E$	Δ	
$B \subseteq A$	C _A ^B	
	=	

sur mots
 $m_1 \bullet m_2$
 \downarrow
 concaténation

rel. binaires
 m_1 sous-mot m_2
 fixe

sur $\mathbb{R}^m \sim (\alpha_1, \alpha_2, \dots, \alpha_m) \in \mathbb{R}^m$
 $\xrightarrow{\parallel}$

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

sur (\mathbb{R}^3) $\vec{x} \wedge \vec{y}$ \leftarrow produit interne pas défini sur \mathbb{R} valeurs

$\underbrace{\vec{x} \cdot \vec{y}}_{\mathbb{R}} : \mathbb{R}^m \times \mathbb{R}^m \rightarrow \mathbb{R}$ pas lci

sur | fonctions de $E \rightarrow E$
 groupe symétrique
 fonctions bijectives
 composition

Quelle sont les propriétés caractéristiques des lci?

Dans la suite $*$ est une lci sur E

\rightarrow associativité \rightarrow le parenthésage n'est pas important

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

ex: sur \mathbb{Z}

	+	x	-	/
assoc	↓			
assoc	↓			
$i + (j + k)$	$= (i + j) + k$			
			$i - (j - k)$	$\neq (i - j) - k$

sur $\mathcal{P}(E)$	\cup	\cap	Δ
	assoc	assoc	assoc
	$A \cup (B \cap C)$		$A \Delta (B \Delta C)$
	"		"
	$(A \cup B) \cap C$		$(A \Delta B) \Delta C$

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 $m_1 \circ (m_2 \circ m_3) = (m_1 \circ m_2) \circ m_3$

→ existence d'un élément neutre

$$\left\{ \begin{array}{l} e \in E \text{ est neutre pour } * \text{ si} \\ \forall x \in E \quad x * e = e * x = x \end{array} \right.$$

Prop. $\left[\begin{array}{l} \text{Si } * \text{ existe, } e \text{ neutre est unique} \end{array} \right.$

dém. par l'absurde, si $\boxed{e, e' \text{ sont neutres}}$ $\textcircled{e=e'}$?

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

$$e' \stackrel{e' \text{ neutre}}{=} e$$

Donc $e = e'$ ✓

◊

On parle donc du neutre (unique).

ex:

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

neutres

→ éléments symétrisables

$$\left[\begin{array}{l} x \in E \text{ (et symétrisable)} \\ \text{admet un symétrique pour } * \text{ si} \\ \exists y \in E \text{ tq } x * y = y * x = e \end{array} \right.$$

ex:
sur \mathbb{Z}

$$x + (-x) = 0$$

↓
symétrisable pour +

mat x
cryptage

$$x + ce^{-}$$

↑ $(-ce^{-})$

$$x * ce^{-} * (\dots) = x$$

sym de la ce^{-}

Prop. si x est symétrisable

et $*$ associative

↓ le symétrique y est unique

dém:

Par e^{-} absurde, si y_1, y_2 sont deux symétriques de x

$y_1 = y_2 ?$

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

$$y_2 * (x * y_1) = y_2 * e$$

y_1 sym. de x

$y_2 * e = y_2$ car e neutre

$*$ // assoc

$$(y_2 * x) * y_1$$

y_2 // symétrique de x

$$= y_1$$

$e * y_1 = y_1$

$y_1 = y_2 \checkmark$

□

Si $*$ associative & symétrique de α ,
 s'il existe est unique
 $\sim \tilde{\alpha}$

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

ex: sur \mathbb{Z}
 e
 symétrisables
 i
 \rightarrow sur \mathbb{Q}

$+$
 0
 tous
 $\tilde{i} = -i$

\times
 1
 $-1, 1$ symétrisables
 $\tilde{1} = 1$
 ~~\times~~ ~~\times~~
 $2 \times \tilde{2} = 1$
 ds \mathbb{Z}

\mathbb{Q}^*
 symétrisables
 $\frac{4}{9} \times \left(\frac{9}{4}\right) = 1$
 $\left(\frac{4}{9}\right)$

sur $\mathcal{P}(E)$
 e
 symétrisables

\cup
 \emptyset
 seul \emptyset
 \downarrow
 $A \cup \emptyset = \emptyset$
 e

\cap
 E
 seul E
 $A \cap E = E$
 e

Δ
 \emptyset
 tout $A \in \mathcal{P}(E)$
 $\tilde{A} = A$
 $A \Delta \tilde{A} = \emptyset$



commutativité

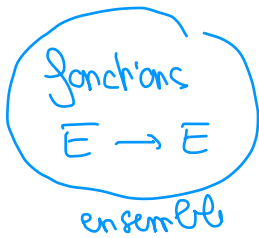
$*$ commutative p:
 $\forall x, y \in E \quad x * y = y * x$

ex: commutative
 $\mathbb{Z} \rightarrow + \quad \times$
 $\mathcal{P}(E) \rightarrow \cap \quad \cup \quad \Delta$

non commutative
 mots \rightarrow concaténation
 matrices $\rightarrow \times$
 fonctions $E \rightarrow E \rightarrow \circ$



ex:



o
lci

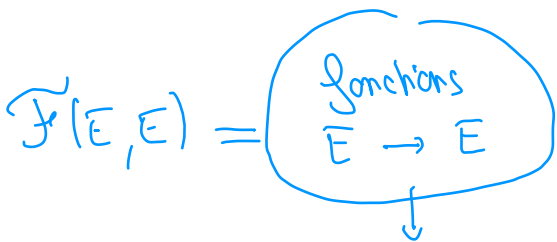
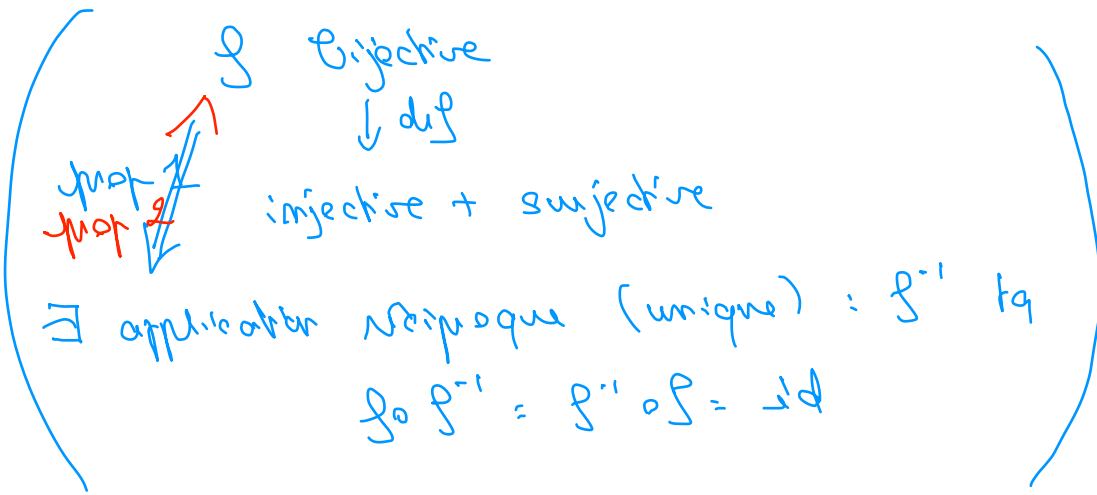
→ assoc ? $f \circ (g \circ h) = (f \circ g) \circ h \quad \checkmark$

→ neutre ? $id_E : E \rightarrow E$
 $x \mapsto x$ $f \circ id = id \circ f = f \quad \checkmark$

→ fonctions symétrisables ? $\dots \rightarrow \exists g \text{ tq } f \circ g = id$
 $g \circ f = id$

fonctions bijectives
 |
 inversibles

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



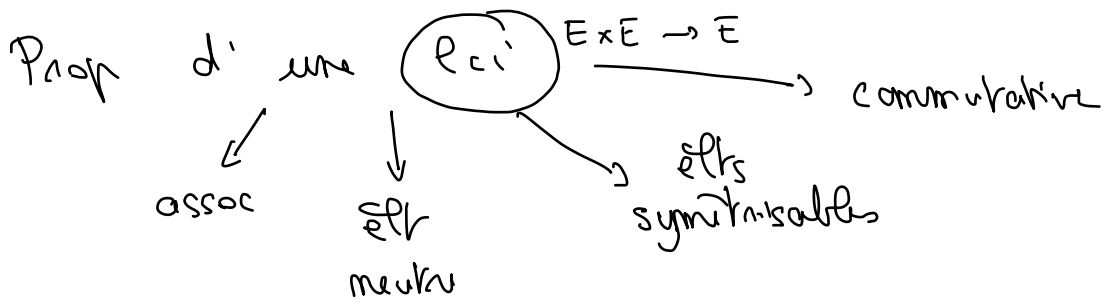
seules les
 fct. bijectives
 sont symétrisables / o

→ associative \checkmark

→ neutre : fonction nulle

→ $\tilde{f} = (-f)$ — toutes les fct sont symétrisables.
 $f + \tilde{f} = 0$

→ $\tilde{f}(\mathbb{R}, \mathbb{R})$, +
 $f + g$



II. Groupes

① Généralités

* def: 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 pas symétrisable
pour x

$(\frac{1}{n} \notin \mathbb{Z})$

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

sur $\mathcal{P}(E)$

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

$\cup \cap \Delta \sim \tilde{A} = A$

pas mots

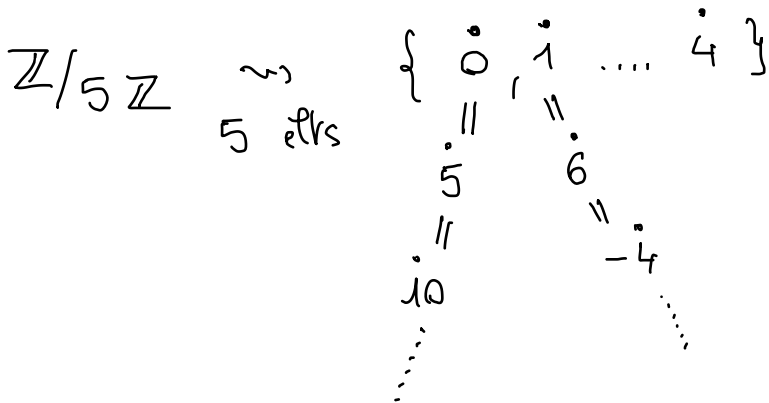
(mots, ~~...~~)

② $\mathbb{Z}/m\mathbb{Z}$

Rappel: ensemble quotient de \mathbb{Z} par la relation d'équivalence $\equiv [m]$

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\mathcal{R}_m$$

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



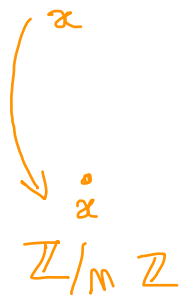
$$\overset{\cdot}{x} = \overset{\cdot}{y}$$

$$\backslash \ /$$

$$x \mathcal{R}_y$$

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

(\mathbb{Z}, \times) ~~X~~



opération quotient ? (bien définie ?)

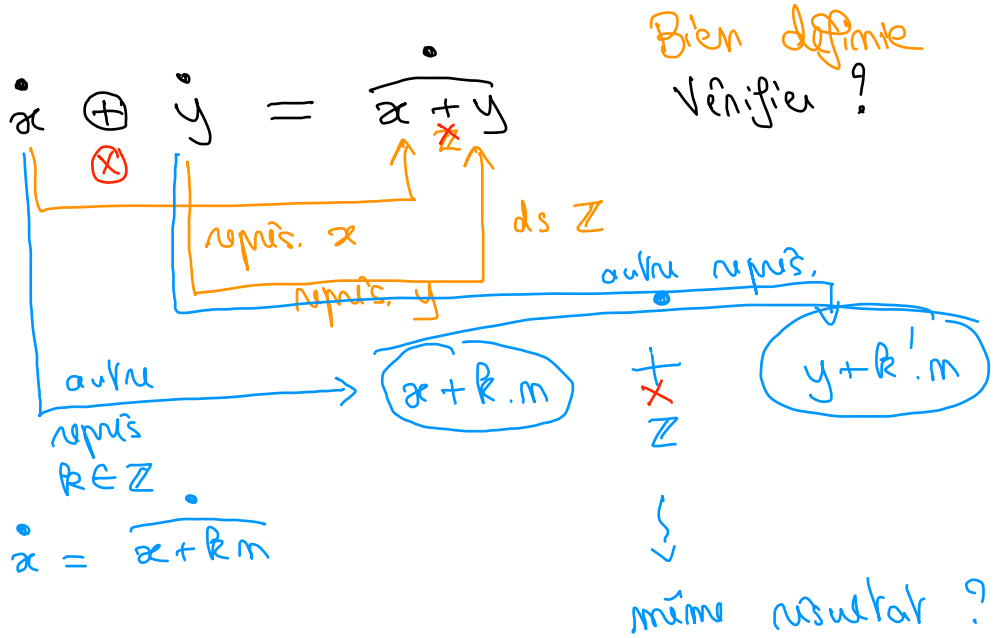
Prop \oplus et \otimes sont bien définies sur

$$\mathbb{Z}/m\mathbb{Z}$$

$$\begin{aligned} \dot{x} \otimes \dot{y} &= \overline{\dot{x} \times y} \\ \dot{x} \oplus \dot{y} &= \overline{\dot{x} + y} \end{aligned}$$

opérations de \mathbb{Z}
usuelles

"dém"



$$\overline{\dot{x} + km} + \overline{\dot{y} + k'm} = \overline{\dot{x} + \dot{y} + (k+k')m}$$

$\dot{x} + \dot{y}$ ✓

\oplus bien définie

\otimes

$$\overline{\dot{x} + km} \times \overline{\dot{y} + k'm} \stackrel{?}{=} \overline{\dot{x} \times y}$$

$$\overline{\dot{x} \times y + \dot{x} \cdot k'm + km \cdot \dot{y} + k k' m^2}$$

$$m(\dot{x} k' + km \dot{y} + k k' m)$$

Donc \otimes bien définie

Proposition

$(\mathbb{Z}/m\mathbb{Z}, \oplus)$ est un groupe commutatif fini

$e = \overset{\circ}{0}$

$\overset{\circ}{x} \oplus \overset{\circ}{0} = \overset{\circ}{x+0} = \overset{\circ}{x}$

$\overset{\circ}{m} = \overset{\circ}{-m}$

groupe quotient

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

i) neutre : 1

$1 \otimes \overset{\circ}{x} = \overset{\circ}{1 \times x} = \overset{\circ}{x}$

ii) les symétrisables sont tous les

$\overset{\circ}{m}$ tq $\text{pgcd}(m, m) = 1$

ex: $\mathbb{Z}/8\mathbb{Z} \rightarrow$ les symétrisables pour \otimes

$\{ \overset{\circ}{1}, \overset{\circ}{3}, \overset{\circ}{5}, \overset{\circ}{7} \}$

$\overset{\circ}{m}$ avec $\text{pgcd}(m, 8) = 1$

ds \mathbb{Z}, \times

~~\mathbb{Z}~~

$\overset{\circ}{1} = \overset{\circ}{1}$
 $\overset{\circ}{2} = \overset{\circ}{2}$
 $\overset{\circ}{3} = \overset{\circ}{3}$
 $\overset{\circ}{4} = \overset{\circ}{4}$
 $\overset{\circ}{5} = \overset{\circ}{5}$
 $\overset{\circ}{6} = \overset{\circ}{6}$
 $\overset{\circ}{7} = \overset{\circ}{7}$
neutre $\leftarrow \overset{\circ}{1}$

$\overset{\circ}{m}$ pour \otimes

③ Sous-groupes

Ensembles

\rightsquigarrow

sous-ensembles

?

comment 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 ?
~~l.c.i. !~~

- pas de neutre

$A_1 = \{0, 2\}$

$(A_1, +)$ groupe ?
~~l.c.i.~~

- neutre 0 ✓

- pas symétrisable.

l.c.i.

2 éls : x, y

$x + y \in$ ensemble ...

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

$(A_2, +)$ groupe ?

$2 + 2 \notin A_2$
↓

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

contient 0, 2

$A_4 = \{2k ; k \in \mathbb{Z}\} \subseteq \mathbb{Z}$

+ l.c.i sur A_4

neutre : $0 \in A_4$ ✓

Tous les éls
sont symétrisables

$(A_4, +)$ groupe

$A_4 \subsetneq \mathbb{Z}$

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

$(A_4 \triangleleft \mathbb{Z})$

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

|

On dit que H est un sous-groupe de G si

$(H, *)$ groupe

