Lois de composition interne - Monoïdes

I/ Notion d'opération (Loi de composition interne)

1. Définition

Une **loi de composition interne** sur un ensemble E ou **opération** dans E
est une application de E × E dans E.
Si l'opération est notée $*$, on écrit plutôt $a*b$ que $*(a,b)$ pour l'image du couple (a,b)

$$* : \begin{array}{ccc} E\times E & \to & E \\ (a,b) & \to & a*b \end{array}$$

On utilise aussi les notations : + , o , • , × , ⊥ , ⋆...

Exemples :

- L'addition et la multiplication dans $\mathbb{N}$
- L'intersection, la réunion, la différence dans $\mathcal{P}(E)$.
- La concaténation (&) dans l'ensemble des mots (ex "ISEN-" & "CIR2" ="ISEN-CIR2")
- La fonction qui, à deux points du plan, associe leur milieu.
- La composition $\circ$ des applications d'un ensemble E vers lui-même.
- Le produit de 2 relations binaires (noté $\mathcal{R}.\mathcal{S}$ ou $\mathcal{R}$ suivi de $\mathcal{S}$)

Contre-exemples :

- La multiplication d'un vecteur par un réel
- La division dans $\mathbb{R}$
- L'addition dans $\{-3,-2,-1,0,1,2,3\}$
- Le produit scalaire $\mathbb{R}^2$

2. Table d'opération (table de Pythagore) pour un ensemble fini

Une opération "quelconque" dans $\{a,b,c,d\}$

$\nearrow$	a	b	c	d
a	b	a	b	b
b	c	c	b	a
c	b	b	d	c
d	d	a	d	b

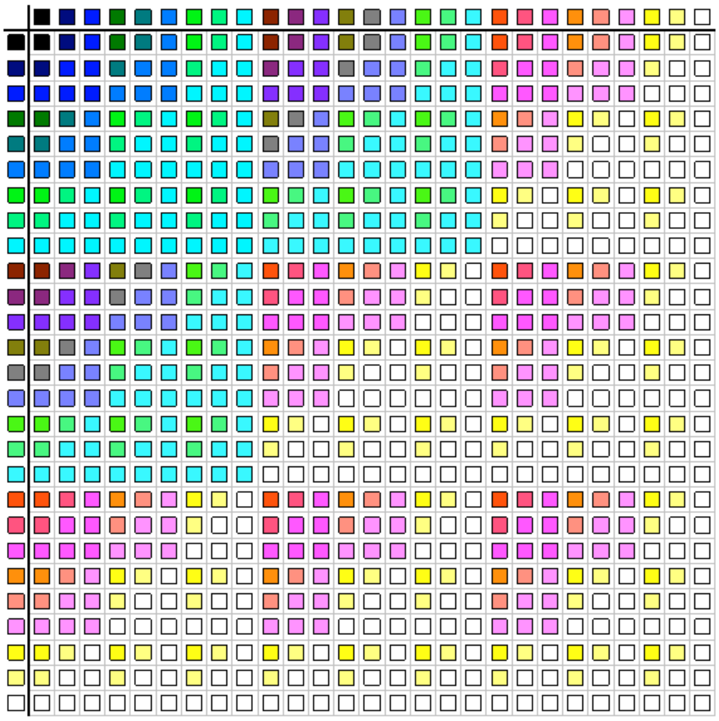
L'addition dans $\mathbb{Z}/6\mathbb{Z}$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

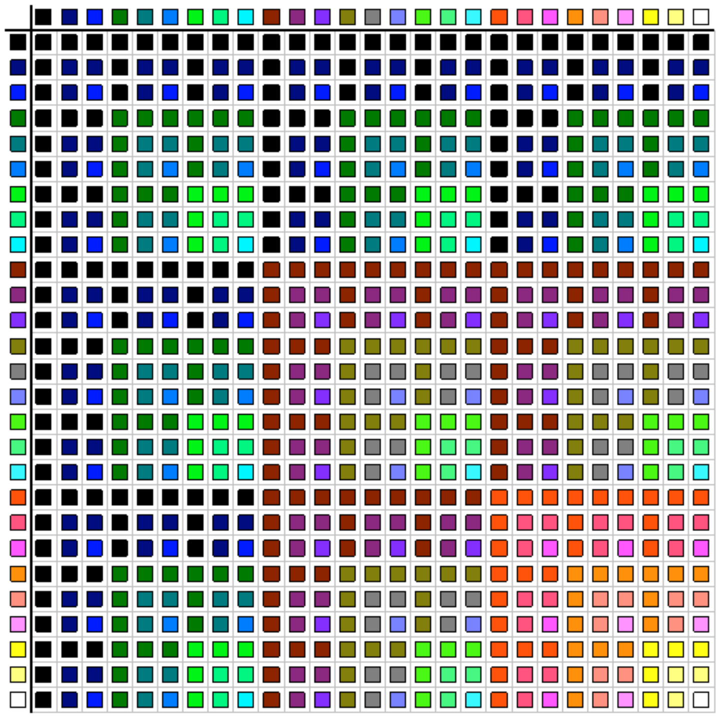
La multiplication dans $\mathbb{Z}/4\mathbb{Z}$

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Synthèse additive des couleurs



Synthèse soustractive des couleurs



II/ Propriétés des opérations

1. Commutativité - Associativité

Soit $(E,*)$ un ensemble muni d'une opération $*$, on dit que :

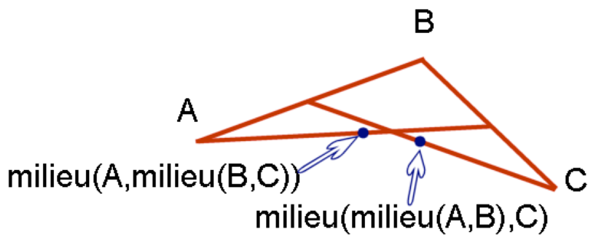
- la loi $*$ est associative ssi $\forall\ a,\ b,c \in E,\ a*(b*c)=(a*b)*c$
- la loi $*$ est commutative ssi $\forall\ a,\ b \in E,\ a*b\ =b*a$

Exemples :

- L'addition et la multiplication dans $\mathbb{N}$ sont commutatives et associatives.
- La soustraction dans $\mathbb{Z}$ n'est ni commutative ni associative.
- L'intersection, la réunion dans $\mathcal{P}(E)$ sont commutatives et associatives.
- La concaténation est associative mais pas commutative.
- Le produit vectoriel de 2 vecteurs de l'espace n'est ni commutatif ni associatif . Par exemple si $\left(\vec{i},\vec{j},\vec{k}\right)$

est la base orthonormée canonique, $\vec{i}\wedge\vec{j}=....$ et $\vec{j}\wedge\vec{i}=....$, $\left(\vec{i}\wedge\vec{j}\right)\wedge\vec{j}=....$ et $\vec{i}\wedge\left(\vec{j}\wedge\vec{j}\right)=....$

- L'opération 'milieu' dans le plan est commutative, mais pas associative.



2. Associativité généralisée

- Soient E un ensemble muni d'une opération $\star$, $x_1, x_2, ..., x_n$ des éléments de E.
- Un parenthésage admissible d'une expression est un parenthésage qui permet de regrouper 2 par 2 des éléments $x_1, x_2, ..., x_n$, ou des expressions calculées à partir de ceux-ci par un parenthésage plus fin.
  On peut définir cette notion récursivement :
  - (initialisation) Une expression constituée d'un unique élément $\boxed{x_i}$ est bien parenthésée.
  - Le parenthésage $\boxed{\left(expression_1 \star expression_2 \right)}$ est admissible si et seulement si les deux expressions sont bien parenthésées.
  - Remarque : Le parenthésage le plus externe n'est pas complètement utile, et ne sert qu'à continuer la construction si d'autres termes doivent s'ajouter à l'expression. Ainsi, dans une expression munie d'un parenthésage admissible, on omet souvent le jeu de parenthèses externes.
    Par exemple, l'expression $\left(x_1 \star x_2\right)$ est bien parenthésée mais on l'écrit plutôt $x_1 \star x_2$,
    l'expression $\left(x_1 \star \left(x_2 \star x_3\right)\right)$ est bien parenthésée mais on l'écrit plutôt $x_1 \star \left(x_2 \star x_3\right)$
- Si l'opération $\star$ est **associative**, tous les parenthésages admissibles de $x_1 \star x_2 \star ... \star x_n$ donnent le même résultat. On convient alors de ne pas écrire de parenthèses.
- Si l'opération $\star$ est **commutative et associative**, alors quelle que soit la permutation σ des indices $1,2,..,n$, l'expression $x_{\sigma(1)} \star x_{\sigma(2)} \star ... \star x_{\sigma(n)}$ donne toujours le même résultat.

  On convient alors de le noter $\mathop{\bigstar}\limits_{i=1}^{n} x_i$, l'ordre n'ayant pas d'importance.

  En notation additive, on aura $\sum\limits_{i=1}^{n} x_i$ et en notation multiplicative $\prod\limits_{i=1}^{n} x_i$

Notations :

- Si l'opération est commutative, on la note *souvent* '+' comme une addition
  Exemple : Synthèse additive : bleu+vert = RGB(0,0,1)+RGB(0,1,0) = RGB(0,1,1) = cyan
- Si l'opération n'est pas commutative (ou si on ne le sait pas), on la note *souvent* '.' comme une multiplication.
  Exemples : la composée de 2 applications f et g peut se noter $f \circ g$ ou $f.g$ ou fg
  la chaîne concaténée de s_1 et s_2 sera notée $s_1.s_2$

3. Elément neutre, symétrique

Soit $(E,*)$ un ensemble muni d'une opération $*$, on dit que :

- un élément e de E est élément neutre de la loi $*$ ssi $\forall\ a \in E,\ a * e = a$ et $e * a = a$
- Dans ce cas, on dit qu'un élément a de E est symétrisable pour la loi $*$
  ssi $\exists\ b \in E,\ a * b = e$ et $b * a = e$. On dit alors que b est **un** symétrique de a.

Exemples :

- Addition dans $\mathbb{N}$: 0 est élément neutre mais seul 0 possède un symétrique (opposé).
- Multiplication dans $\mathbb{Z}$: 1 est élément neutre mais seuls 1 et -1 possèdent un symétrique (inverse).
- $\mathbb{R}$ n'a pas d'élément neutre pour la soustraction.
- $\varnothing$ est élément neutre de la réunion dans $\mathcal{P}(E)$ et lui seul possède un symétrique.
  E est élément neutre de l'intersection dans $\mathcal{P}(E)$ et lui seul possède un symétrique.
- La chaîne vide est élément neutre de la concaténation.
- $\mathbb{R}^3$ n'a pas d'élément neutre pour le produit vectoriel
- Le plan n'a pas d'élément neutre pour l'opération 'milieu'
- I est élément neutre de la multiplication des matrices $n \times n$.
  Une matrice réelle a un symétrique (inverse) si et seulement si son déterminant est non nul.
- La relation " = " est l'élément neutre du produit des relations binaires.

Notations :

- Si l'opération est notée '+', l'élément neutre est noté '0' et le symétrique d'un élément x est appelé son opposé et noté '$-x$' *(sous réserve d'unicité ! voir plus loin)*
- Si l'opération est notée multiplicativement, l'élément neutre est appelé unité et noté '1' et le symétrique d'un élément x est appelé son inverse et noté 'x^{-1}' *(sous réserve d'unicité ! voir plus loin)*

  Attention on évitera les notations $\dfrac{1}{x}$ et $\dfrac{y}{x}$

  car si l'opération $\star$ n'est pas commutative, on peut avoir $y\star\dfrac{1}{x}\neq\dfrac{1}{x}\star y$

  Exemple : pour des matrices A et B, distinguer $A\,B^{-1}$ et $B^{-1}A$

4. Elément absorbant

Soit $(E,*)$ un ensemble muni d'une opération $*$, on dit que :

- un élément a de E est élément absorbant la loi $*$ ssi $\forall\, x\in E,\ a*x=\ a$ et $x*a=a$

Exemples :

- Multiplication dans $\mathbb{N}$, $\mathbb{Z}$ ou $\mathbb{R}$: 0 est élément absorbant
- Dans $\mathcal{P}(E)$, E est absorbant pour la réunion et $\varnothing$ absorbant pour l'intersection.
- Synthèse additive des couleurs : RGB(0,0,0) est neutre et RGB(1,1,1) absorbant
- Synthèse soustractive des couleurs : RGB(1,1,1) est neutre et RGB(0,0,0) absorbant

5. Itérations d'une opération:

- Soit $\star$ une loi **associative** sur E pour laquelle il existe un élément neutre e.

  Soit x un élément de E et $n\in\mathbb{N}^*$.

  $x\star x\star\ldots\star x$ (n fois le terme x) est noté $x^{\star n}$ ou x^n (s'il n'y a pas ambiguïté ou en notation multiplicative).

  Par définition, on pose $x^{\star 0}=e$ ($x^0=1$ en notation multiplicative)

  Exemple : Pour la concaténation $"Bla\ "^{10}="Bla\ Bla\ Bla\ Bla\ Bla\ Bla\ Bla\ Bla\ Bla\ Bla\ "$

  Remarque : Si la loi n'est pas associative, le parenthèsage peut avoir de l'importance.

  exemple dans $\mathbb{R}$ avec la loi $x\star y=3x+2y$: $\begin{array}{l}(x\star x)\star x=(5x)\star x=17x\\ x\star(x\star x)=x\star(5x)=13x\end{array}$
- Pour tous n,p dans $\mathbb{N}$ on a $x^{\star n}\star x^{\star p}=x^{\star(n+p)}$ ou, plus simplement, $x^n\,x^p=x^{(n+p)}$

  et $\left(x^{\star n}\right)^{\star p}=x^{\star(np)}$ ou, plus simplement, $\left(x^n\right)^p=x^{np}$
- Si x est inversible, pour $n\in\mathbb{N}$ on pose $x^{\star(-n)}=\left(x^{\star n}\right)^{-1}$ ou, plus simplement, $x^{-n}=\left(x^n\right)^{-1}$

  On a alors pour tous n,p dans $\mathbb{Z}$ $x^n\,x^p=x^{(n+p)}$ et $\left(x^n\right)^p=x^{np}$
- Attention ! Si $\star$ n'est pas **commutative, on n'a pas forcément** $(x\star y)^n=x^{\star n}\star y^{\star n}$

  Exemple : pour des matrices $n\times n$ $(AB)^2=AB\,AB$ et pas forcément A^2B^2
- En notation additive on écrit $x+x+\ldots+x=n\,x$ et $0\,x=0$ (plus précisément $0_{\mathbb{Z}}\,x=0_E$)

  Les propriétés s'écrivent alors $\forall n,p\in\mathbb{N}$ $(\forall n,p\in\mathbb{Z}$ si x a un opposé $)$:

  $n\,x+p\,x=(n+p)\,x$, $n(p\,x)=(n\,p)\,x$

III/ Monoïde

1. Définition

Un ensemble E muni d'une opération $*$ est un **monoïde** si

- la loi $*$ est associative
- et E admet un élément neutre pour la loi $*$.

Exemples :

- Addition dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$: 0 est élément neutre
- Multiplication dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$: 1 est élément neutre
- L'ensemble A^A des applications de A dans lui-même est un monoïde pour la loi $\circ$. Id est l'élément neutre.
- L'ensemble $\mathcal{L}(E)$ est endomorphismes d'un espace vectoriel E est un monoïde pour la loi $\circ$.
- L'ensemble des chaînes de caractères est un monoïde pour la concaténation.

2. Propriétés

Dans un monoïde $(E,*)$:

- L'élément neutre est unique
- Si un élément a admet un symétrique, alors ce symétrique est unique.
  On note alors $a^{*(-1)}$ (ou, plus simplement a^{-1}) **le** symétrique de a.
- Si deux éléments a et b sont symétrisables, alors $a*b$ est symétrisable et $(a*b)^{-1} = b^{-1}*a^{-1}$.

Remarques :

- L'application $f : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \to & 10x \end{array}$ a plusieurs inverses à gauche, dont $g_0 : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \to & E\left(\frac{x}{10}\right) \end{array}$ et $g_1 : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \to & E\left(\frac{x+1}{10}\right) \end{array}$
  car $g_0 \circ f = g_1 \circ f = id$ mais $g_0(9) = 0$ et $g_1(9) = 1$. Mais f n'a pas d'inverse à droite.
- Soit $A \in M_n(\mathbb{R})$. A est inversible $\Leftrightarrow$ A est inversible à gauche $\Leftrightarrow$ A est inversible à droite $\Leftrightarrow$ $\det A \neq 0$

3. Elément régulier

Définition : Soit $(E,*)$ un ensemble muni d'une opération $*$, et $a \in E$

- a est **régulier à droite** si $\forall (x,y) \in E,\ x*a = y*a \Rightarrow x = y$
- a est **régulier à gauche** si $\forall (x,y) \in E,\ a*x = a*y \Rightarrow x = y$
- a est **régulier** s'il est régulier à droite et à gauche

Exemples :

- Dans $(\mathbb{R},\times)$ 0 n'est pas un élément régulier. Tous les autres sont réguliers
- Dans $(\mathbb{N}^*,\times)$, tout élément est régulier
- Dans $(\mathcal{P}(E),\cup)$, $\{a,b\}\cup\{b,c\} = \{a,c\}\cup\{b,c\}$ donc $\{b,c\}$ n'est pas régulier
- Toute chaîne est régulière pour la concaténation

Propriété

Dans un monoïde, tout élément inversible est régulier (mais réciproque fausse)

Remarque

- Dans $(\mathbb{N}^*,\times)$, tout élément est régulier, mais seul 1 est inversible.
- Dans $(M_n(\mathbb{R}),\times)$ une matrice est régulière si et seulement elle est inversible

4. Préordre associé à un monoïde

Soit $(E,*)$ un monoïde. On définit la relation $\mathcal{R}$ dans E par :

$\forall x, y \in E \ / \ x \mathcal{R} y \Leftrightarrow \exists z \in E \ / \ y = z\,x$

La relation $\mathcal{R}$ est une relation de pré-ordre sur E

La relation d'équivalence associée est la relation $\approx$ définie par

$\forall x, y \in E \ / \ x \approx y \Leftrightarrow \exists z \in E \ / \ z$ inversible et $y = z\,x$

La relation de pré-ordre $\mathcal{R}$ induit une relation d'ordre sur les classes d'équivalence.

Exemples

- Dans $(\mathbb{Z}, \times)$: $a \mid b \Leftrightarrow \exists k \in \mathbb{Z} / b = k\,a$ l'équivalence associée est $a \approx b \Leftrightarrow a \mid b$ et $b \mid a \Leftrightarrow |a| = |b|$.
  La divisibilité dans $\mathbb{Z}$ induit la relation d'ordre de divisibilité dans $\mathbb{N}$
- Dans $\left(\mathcal{P}(E), \cup\right)$, le pré-ordre associé est la relation d'inclusion. C'est ici une relation d'ordre.
- Dans l'ensemble des chaînes de caractères, la relation de pré-ordre est :
  $s_1 \mathcal{S} s_2 \Leftrightarrow \exists s_3 / s_2 = s_3 . s_1 \Leftrightarrow s_1$ est un *suffixe* (ou *section finissante*) de s_2
  exemple « LABLA » est un suffixe de « BLABLABLA »
  C'est une relation d'ordre.
  On peut aussi définir $s_1 \mathcal{P} s_2 \Leftrightarrow \exists s_3 / s_2 = s_1 . s_3 \Leftrightarrow s_1$ est un *préfixe* (ou *section commençante*) de s_2
- Dans le monoïde $\left(\mathscr{L}(E), \circ\right)$ des endomorphismes d'un espace vectoriel E, le pré-odre associé est :
  $\forall f, g \in \mathscr{L}(E) \ / \ f \mathcal{R} g \Leftrightarrow \exists h \in \mathscr{L}(E) \ / \ g = h\,f \Leftrightarrow Ker(f) \subset Ker(g)$