Lois

1 Généralités

Définition : une *loi de composition* sur un ensemble E est une fonction φ de $E \times E$ dans E. Le *composé* de deux éléments a et b de E est $\varphi(a, b)$, que l'on note plutôt $a \, \varphi \, b$. L'expression *loi de composition* désigne en fait ce que l'on appelle usuellement *opération*.

Exemples : :

- l'addition, dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;
- la multiplication, dans chacun de ces ensembles, mais aussi dans l'ensemble $\mathcal{M}_2(\mathbb{K})$ des matrices carrées d'ordre 2 à coefficients dans $\mathbb{K}$;
- la composition des fonctions d'un ensemble E dans lui-même ;
- le produit vectoriel ;
- les fonctions min et max, dans $\mathbb{R}$;
- les fonctions pgcd et ppcm, dans $\mathbb{N}$;
- les lois $\cup$ (union) et $\cap$ (intersection) sur l'ensemble des parties de E.

Définition : une loi sur un ensemble E muni d'une loi $\star$ est *associative* si elle vérifie $a \star (b \star c) = (a \star b) \star c$ quels que soient $a, b, c \in E$.

Exemples :

- l'addition, la multiplication, la composition des fonctions sont associatives ;
- la soustraction, la division (dans $\mathbb{R}^*$), le produit vectoriel ne le sont pas ; par exemple $(9-7)-4 = -2$ tandis que $9-(7-4) = 6$.

Remarque : l'associativité est une propriété essentielle ; lorsqu'une loi $\star$ est asociative, on peut écrire $a \star b \star c$ sans risque d'ambiguïté. Sinon, il faut faire la différence entre $(a \star b) \star c$ et $a \star (b \star c)$.

Définition : une loi sur un ensemble E muni d'une loi $\star$ est *commutative* si elle vérifie $a \star b = b \star a$ quels que soient $a, b \in E$.

Exemples : l'addition, la multiplication (dans $\mathbb{C}$) sont commutatives ; la composition des fonctions, le produit matriciel, la soustraction ne le sont pas.

Définition : soit E un ensemble muni d'une loi $\star$; un élément e est le *neutre* de $\star$ si $a \star e = e \star a = a$ quel que soit $a \in G$.

Exemples :

- dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ le neutre de l'addition est 0 ;
- celui de la multiplication est 1 ;
- pour la loi $\cup$ (union), le neutre est l'ensemble vide.

Proposition : le neutre, s'il existe, est unique

Preuve : par l'absurde : supposons qu'il existe un deuxième neutre e'. Alors $e' = e \star e' = e$.

Définition : un élément a de E est dit *régulier* (ou *simplifiable*) pour la loi $\star$ si $a \star x = a \star y$ implique $x = y$, et $x \star a = y \star a$ implique $x = y$.

Exemples :

- dans $\mathbb{Z}$, tout élément est régulier pour $+$;
- pour $\times$, seul 0 n'est pas régulier.

Proposition : si une loi $\star$ est associative, alors le produit de deux éléments réguliers est régulier.

Preuve : soient a, b deux éléments réguliers, et x, y deux éléments quelconques de E. Alors :

$$(a \star b) \star x = (a \star b) \star y \Rightarrow a \star (b \star x) = a \star (b \star y) \Rightarrow b \star x = b \star y \Rightarrow x = y$$

Définition : un élément a de E est dit *symétrisable* pour la loi $\star$ s'il existe un élément a' de E tel que $a \star a' = a' \star a = e$. Nous dirons alors que a' est le *symétrique* de a. Lorsque la loi est multiplicative, on utilise les termes *inversible* et *inverse*, et on note a^{-1} l'inverse de a ; lorsque la loi est additive, on utilise le terme *opposé*, et on note $-a$ l'opposé de a

Proposition : si la loi est associative, alors l'inverse de a est unique.

Preuve : supposons qu'il existe deux inverses a' et a'' ; alors : $a'' = a'' \star e = a'' \star (a \star a') = (a'' \star a) \star a' = e \star a' = a'$.

Proposition : si la loi est associative, le produit de deux éléments inversibles est inversible ; de plus, l'inverse du produit est égal au produit des inverses *dans l'ordre inverse* : $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Preuve : c'est une simple vérification : $(b^{-1} \star a^{-1}) \star (a \star b) = b^{-1} \star (a^{-1}) \star a) \star b = b^{-1} \star e \star b = b^{-1} \star b = e$
On vérifierait de même que $(a \star b) \star (b^{-1} \star a^{-1}) = e$.

Proposition : tout élément inversible est régulier.

Preuve : soit a inversible ; alors : $a \star x = a \star y \Rightarrow a^{-1} \star (a \star x) = a^{-1} \star (a \star y) \Rightarrow (a^{-1} \star a) \star x = (a^{-1} \star a) \star y \Rightarrow e \star x = e \star y \Rightarrow x = y$.
Remarque : la réciproque est fausse : dans $\mathbb{N}$, un naturel $n \geqslant 2$ est régulier, mais n'est pas inversible.
Définition : soient E un ensemble muni d'une loi $\star$ et A une partie de E. Nous dirons que A est *stable* pour $\star$ si $a \star b \in A$ quels que soient $a, b \in A$.

Exemples :

- E est stable pour sa loi ;
- si la loi possède un neutre e, alors $\{e\}$ est stable pour la loi ;
- l'ensemble des éléments réguliers est stable pour la loi.

Définition : soient E un ensemble muni d'une loi $\star$ et A une partie de E stable pour la loi $\star$; alors la *loi induite* par $\star$ sur A est définie comme suit : $a \,\overline{\star}\, b = a \star b$. C'est donc une fonction de $A \times A$ dans A.

FIN