Chapitre 5

Lois de composition internes - Relations

1. Lois de composition internes

1.1. Définition et exemples

Définition 5.1 – *Soit E un ensemble. Une loi de composition interne sur E est une application de $E \times E$ dans E. Si on la note* $\begin{array}{ccc} E \times E & \longrightarrow & E \\ (a,b) & \longmapsto & a * b \end{array}$, *on parle de la loi $*$ et on dit que $a * b$ est le composé de a et b pour la loi $*$.*

Exemples - • Sur $E = \mathbb{Z}$, l'addition définie par $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (a,b) & \longmapsto & a + b \end{array}$, la multiplication $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (a,b) & \longmapsto & a \times b \end{array}$ et la soustraction $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ (a,b) & \longmapsto & a - b \end{array}$ sont des lois de composition internes. Ce n'est pas le cas de la division car a/b n'est pas défini pour tous les couples (a,b) d'entiers.

• Soit X un ensemble. Sur $\mathcal{P}(X)$, la réunion $\begin{array}{ccc} \mathcal{P}(X)^2 & \to & \mathcal{P}(X) \\ (A,B) & \mapsto & A \cup B \end{array}$ est une loi de composition interne. De même, pour l'intersection $\cap$ et la différence symétrique Δ.

• Soit X un ensemble. On note $E = \mathcal{F}(X)$ l'ensemble des applications de X dans X. La composition des applications $\begin{array}{ccc} E \times E & \longrightarrow & E \\ (f,g) & \longmapsto & f \circ g \end{array}$ est une loi interne sur E.

• Sur $E = \mathbb{R}^2$, l'addition $\begin{array}{ccc} E \times E & \to & E \\ ((x,y),(x',y')) & \mapsto & (x+x', y+y') \end{array}$ est une loi interne. La multiplication par un scalaire $\begin{array}{ccc} \mathbb{R} \times E & \to & E \\ (\lambda, (x,y)) & \mapsto & (\lambda x, \lambda y) \end{array}$ n'est pas une loi interne, car son ensemble de départ n'est pas $E \times E$.

1.2. Propriétés usuelles des lois internes

Définition 5.2 – *Soit $*$ une loi interne sur un ensemble E. On dit que*
1 – la loi $*$ est commutative si pour tous les éléments x, y de E, on a $(x * y = y * x)$.
2 – la loi $*$ est associative si pour tous les éléments x, y, z de E, on a $((x*y)*z = x*(y*z))$.

Exemples - • L'addition et la multiplication dans $\mathbb{Z}$ sont commutatives et associatives. Ce n'est pas le cas de la soustraction (montrez le).
• La composition des applications dans $\mathcal{F}(X,X)$ est associative, mais n'est en général pas commutative (trouvez un contre-exemple).
• Que pensez-vous des autres exemples du paragraphe précédent ?

Définition 5.3 – *Soit $*$ une loi interne sur un ensemble E. Un élément e de E est un élément neutre pour la loi $*$ si pour tout élément a de E on a $(a * e = e * a = a)$.*

Exemples - • Dans $\mathbb{Z}$, 0 est un élément neutre pour l'addition et 1 est un élément neutre pour la multiplication.
• La composition des applications dans $\mathcal{F}(X, X)$ admet Id_X pour élément neutre.
• Etudiez les autres exemples.

Proposition 5.4 – *Soit $*$ une loi interne sur un ensemble E, si $*$ possède un élément neutre, il est unique.*
Démonstration : supposons que $*$ ait deux éléments neutres e et e', alors on a $e * e' = e$ car e' est élément neutre et $e * e' = e'$ car e est élément neutre. On en déduit que $e = e'$. □

Définition 5.5 – *Soit $*$ une loi interne sur un ensemble E, possédant un élément neutre e et soit a un élément de E. On dit que a admet un symétrique b pour la loi $*$, si l'on a $(a * b = b * a = e)$.*

Exemples - • Dans $\mathbb{R}$, chaque élément a possède un symétrique pour l'addition qui est son opposé $-a$. Mais a n'a un symétrique pour la multiplication que s'il est non nul ; son symétrique est alors l'inverse $1/a$ de a.
• Dans $\mathcal{F}(X, X)$, un élément f a un symétrique (pour la composition $\circ$) si et seulement si f est bijective et alors son symétrique est l'application réciproque f^{-1}.

Définition 5.6 – *Soit E un ensemble muni de deux lois de composition internes, notées $+$ et $*$. On dit que $*$ est distributive par rapport à $+$ si pour tous les éléments x, y, z de E, on a $x * (y + z) = (x * y) + (x * z)$ et $(x + y) * z = (x * z) + (y * z)$).*

Exemples - • Dans $\mathbb{R}$, la multiplication est distributive par rapport à l'addition. L'addition est-elle distributive par rapport à la multiplication ?
• Dans l'ensemble $\mathcal{P}(X)$ des parties d'un ensemble X, la réunion est distributive par rapport à l'intersection et l'intersection est distributive par rapport à la réunion.

1.3. Exemples de structures algébriques (pour votre culture générale)

Définition 5.7 – *Soit E un ensemble muni d'une loi de composition interne $*$. On dit que $(E, *)$ est un groupe si la loi $*$ satisfait aux trois conditions suivantes :*
1 – Elle est associative.
2 – Elle admet un élément neutre.
3 – Chaque élément de E admet un symétrique pour $*$.
Si de plus, la loi est commutative, on dit que le groupe est commutatif ou abélien (du nom du mathématicien Abel).

Exemples - • L'ensemble des entiers relatifs muni de l'addition $(\mathbb{Z}, +)$ est un groupe commutatif.
• De même $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$ sont des groupes commutatifs.
• Dans l'ensemble des applications $\mathcal{F}(X, X)$ d'un ensemble X dans lui-même, considérons le sous-ensemble $\mathcal{BIJ}$ des bijections. Vérifier que la composition des applications définit une loi interne sur $\mathcal{BIJ}$ et que $(\mathcal{BIJ}, \circ)$ est un groupe, en général non commutatif.
• Soient n un entier non nul et $U_n = \{z \in \mathbb{C}\} \mid z^n = 1\}$ l'ensemble des racines $n^{\text{ièmes}}$ de l'unité. Alors $(U_n, \times)$ est un groupe commutatif.

Définition 5.8 – *Soit E un ensemble muni de deux lois de composition internes que nous noterons $+$ et $*$. On dit que $(E, +, *)$ est un anneau si les conditions suivantes sont remplies :*
1 – $(E, +)$ est un groupe commutatif.

2 – La loi $*$ est associative.
3 – La loi $*$ est distributive par rapport à la loi $+$.
Si de plus la loi $*$ est commutative, on dit que l'anneau est commutatif ; si elle admet un élément neutre, on dit que l'anneau est unitaire. On note en général 0 l'élément neutre de la loi $+$ et 1 celui de la loi $*$ lorsqu'il existe.

Exemples - • L'ensemble des entiers muni de l'addition et de la multiplication $(\mathbb{Z}, +, \times)$ est un anneau commutatif et unitaire.
• De même pour $(\mathbb{R}, +, \times)$ et pour $(\mathbb{R}[X], +, \times)$ où $\mathbb{R}[X]$ désigne l'ensemble des polynômes à coefficients réels.
• De même pour $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, où $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des entiers modulo n.

Dans un anneau commutatif et unitaire $(E, +, *)$ les règles de calcul qui ne font intervenir que l'addition, la soustraction et la multiplication sont les mêmes que dans $(\mathbb{Z}, +, \times)$. Par contre, il faut être prudent avec les divisions : l' équation $(x * y = x * z)$ n'est pas toujours équivalente à ($y = z$ ou $x = 0$), $n.x = 0$ n'implique pas toujours ($x = 0$ ou $n = 0$) (pour des exemples, voir le cours d'arithmétique sur les congruences).

Définition 5.9 – *Soit E un ensemble muni de deux lois de composition internes toujours notées $+$ et $*$. On dit que $(E, +, *)$ est un corps commutatif si les conditions suivantes sont remplies :*
1 – $(E, +, *)$ est un anneau commutatif et unitaire.
2 – Chaque élément de $E \setminus \{0\}$ a un symétrique pour la loi $*$.
Si $(E, +, *)$ est un corps commutatif, et si on note $E^* = E \setminus \{0\}$, alors $(E^*, *)$ a une structure de groupe commutatif, dont l'élément neutre est 1.

Exemples - • $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps commutatifs.
• On note $\mathbb{R}(X)$ l'ensemble des fractions rationnelles à coefficients réels. Alors, $(\mathbb{R}(X), +, \times)$ est un corps commutatif.
• L'anneau $(\mathbb{Z}, +, \times)$ n'est pas un corps. (Quels sont les éléments inversibles ?)

2. Relations

2.1. Définitions et exemples

Définition 5.10 – *Soit E un ensemble. Une relation dans E est une propriété concernant les couples (x, y) d'éléments de E.*
Notons $\mathcal{R}$ une telle relation ; on écrit en général $x\mathcal{R}y$ pour signifier que le couple (x, y) vérifie la relation $\mathcal{R}$.

Exemples - • Dans $E = \mathbb{C}$, la relation d'égalité : $x = y$.
• Dans $E = \mathbb{R}$, la relation : $x = y^2$.
• Dans $E = \mathbb{R}$, la relation d'inégalité : $x \leq y$.
• Dans l'ensemble des droites du plan (affine) la relation de parallèlisme : D *est parallèle à* D'.
• Soit X un ensemble et $E = \mathcal{P}(X)$; dans E, on a la relation d'inclusion : $A \subset B$.
• Sur $E = \mathbb{Z}$, la relation : x et y *sont de même parité*, appelée *relation de congruence modulo 2* et notée : $x \equiv y (\mathrm{mod}\, 2)$.
• Si f est une application de E dans un ensemble F, on peut lui associer la relation $\mathcal{R}$ définie par $(x\mathcal{R}y \Leftrightarrow f(x) = f(y))$.

2.2. Propriétés usuelles des relations

Définition 5.11 – *Soit $\mathcal{R}$ une relation sur un ensemble E. On dit que :*
1 – La relation $\mathcal{R}$ est réflexive si pour tout élément x de E, on a $x\mathcal{R}x$.
2 – La relation $\mathcal{R}$ est symétrique si pour tous les éléments x, y de E, on a $(x\mathcal{R}y \Rightarrow y\mathcal{R}x)$.
3 – La relation $\mathcal{R}$ est antisymétrique si pour tous les éléments x, y de E on a

$$((x\mathcal{R}y \text{ et } y\mathcal{R}x) \Rightarrow x = y).$$

4 – La relation $\mathcal{R}$ est transitive si pour tous les éléments x, y, z de E, on a

$$((x\mathcal{R}y \quad \text{et} \quad y\mathcal{R}z) \Rightarrow x\mathcal{R}z).$$

Définition 5.12 – *Soit $\mathcal{R}$ une relation. Si $\mathcal{R}$ est réflexive, symétrique et transitive, on dit que $\mathcal{R}$ est une relation d'équivalence. Si $\mathcal{R}$ est réflexive, antisymétrique et transitive, on dit que $\mathcal{R}$ est une relation d'ordre.*

Exemple - Reprenons les exemples ci-dessus. On voit facilement que les relations d'égalité (ex.1), de parallélisme (ex.4) ou de congruence modulo 2 (ex.6) sont des relations d'équivalence et que les relations d'inégalité (ex.3) ou d'inclusion (ex.5) sont des relations d'ordre. Que pensez-vous de l'exemple 2 ?

Définition 5.13 – *Soit $\mathcal{R}$ une relation d'ordre dans un ensemble E. On dit que $\mathcal{R}$ est une relation d'ordre total si pour chaque (x, y) de $E \times E$, on a $(x\mathcal{R}y$ ou $y\mathcal{R}x)$. C'est une relation d'ordre partiel sinon.*

Exemples -
- La relation $\leq$ dans $\mathbb{R}$ est une relation d'ordre total.
- Soit $X = \{0, 1, 2\}$, la relation $\subset$ dans l'ensemble $E = \mathcal{P}(X)$ est une relation d'ordre partiel. En effet, si on considère les éléments $A = \{0\}$ et $B = \{1\}$ de $\mathcal{P}(X)$, on n'a ni $A \subset B$ ni $B \subset A$.

2.3. Etude des relations d'équivalence

Fixons une relation d'équivalence $\mathcal{R}$ dans un ensemble E. La notation $x\mathcal{R}y$ se lit souvent "x et y *sont équivalents pour* $\mathcal{R}$".

Définition 5.14 – *Soit x un élément de E. On appelle classe d'équivalence de x l'ensemble qu'on notera ici $\overline{x}$:*

$$\overline{x} = \{y \in E \mid x\mathcal{R}y\}.$$

L'ensemble des classes d'équivalence est appelé l'ensemble quotient de E par la relation $\mathcal{R}$. On le note $E/\mathcal{R}$.

Exemples -
- Dans l'exemple 1 ci-dessus, on a $\overline{x} = \{x\}$
- Dans l'exemple 6, si x est pair, on a $\overline{x} = 2\mathbb{Z}$ et si x est impair, on a $\overline{x} = 2\mathbb{Z}+1$. On a $\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1}\}$. On voit que $x \equiv y$ est équivalent à $\overline{x} = \overline{y}$ et que les deux classes distinctes forment une partition de $\mathbb{Z}$.

Ceci se généralise par le théorème suivant :

Théorème 5.15 –

1) Soit x un élément de E, on a : $x \in \overline{x}$.
2) Soient x et y des éléments de E. On a l'équivalence :

$$x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}.$$

3) Les classes d'équivalence distinctes forment une partition de E.

Démonstration :

1) Puisque $\mathcal{R}$ est réflexive, on a $x\mathcal{R}x$ pour tout élément x de E, donc $x \in \overline{x}$.
2) Supposons $x\mathcal{R}y$. Montrons que l'on a $\overline{y} \subset \overline{x}$. Soit z un élément de $\overline{y}$; on a donc $y\mathcal{R}z$; comme $\mathcal{R}$ est transitive et que l'on a ($x\mathcal{R}y$ et $y\mathcal{R}z$), on obtient $x\mathcal{R}z$; donc $z \in \overline{x}$. On a montré que $\overline{y} \subset \overline{x}$. Comme $\mathcal{R}$ est symétrique et $x\mathcal{R}y$, on a aussi $y\mathcal{R}x$. En échangeant les rôles de x et y, on obtient de même $\overline{x} \subset \overline{y}$. On a montré que l'on a $\overline{x} \subset \overline{y}$ et $\overline{y} \subset \overline{x}$; on a donc $\overline{x} = \overline{y}$.
   Supposons $\overline{x} = \overline{y}$; on a $x \in \overline{x}$ donc $x \in \overline{y}$, c'est à dire $y\mathcal{R}x$; comme $\mathcal{R}$ est symétrique, on a aussi $x\mathcal{R}y$.
   On a montré l'équivalence ($x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}$).
3) La classe $\overline{x}$ d'un élément x de E contient x d'après 1 ; elle est donc non vide.
   Montrons que deux classes distinctes sont disjointes, et pour cela supposons $\overline{x} \cap \overline{y} \neq \emptyset$ et montrons $\overline{x} = \overline{y}$. Soit z un élément de l'ensemble $\overline{x} \cap \overline{y}$; on a ($x\mathcal{R}z$ et $y\mathcal{R}z$) donc $\overline{x} = \overline{z} = \overline{y}$; d'où le résultat.
   Notons E' la réunion des classes : $E' = \bigcup_{x \in E} \overline{x}$ et montrons que $E = E'$. Soit x un élément de E. On a $x \in \overline{x}$, donc $x \in E'$; on obtient $E \subset E'$. Comme on a évidemment $E' \subset E$, on obtient $E = E'$.
   De tout ceci, on déduit le résultat 3. □

D'après la deuxième partie de la proposition, l'équivalence se ramène à l'égalité des classes. Pour illustrer ceci, considérons l'exemple 4 : si on appelle *direction* d'une droite D la classe d'équivalence de D, dire que deux droites sont parallèles revient à dire qu'elles ont même direction et l'ensemble quotient est l'ensemble des directions du plan.
Plus généralement si $\mathcal{R}$ est une relation d'équivalence sur un ensemble E, on peut construire l'application $f : \begin{array}{ccc} E & \longrightarrow & E/\mathcal{R} \\ x & \longmapsto & \overline{x} \end{array}$. Dire que $x\mathcal{R}y$ équivaut à dire que $f(x) = f(y)$. Les classes d'équivalence sont exactement les ensembles $f^{-1}(\{y\})$ où y décrit $E/\mathcal{R}$.
Inversement, si f est une application d'un ensemble E dans un ensemble F, on peut considérer la relation d'équivalence ($x\mathcal{R}y \Leftrightarrow f(x) = f(y)$) sur E. Ses classes d'équivalence sont les ensembles $f^{-1}(\{y\})$ où y décrit l'image de f. D'après ce qui précède, toutes les relations d'équivalence sont obtenues ainsi.

2.4. Relations d'ordre

Dans la suite, on se contentera d'étudier les relations $\leq$ dans $E = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ou $\mathbb{R}$.

Définition 5.16 – *Soient A un sous-ensemble de E et M un élément de E.*
1 – On dit que M est un majorant de A si pour tout élément a de A, on a : $a \leq M$.
2 – On dit que M est un plus grand élément de A si M est un majorant de A et si M appartient à A.
3 – On définit de même la notion de minorant et celle de plus petit élément.

Remarque et exemples

1) S'il existe un plus grand élément de A, il est unique. En effet, si a et a' sont deux plus grands éléments de A, a est un élément de A et a' majore A, donc $a \leq a'$; de même en échangeant les rôles de a et a', on obtient $a' \leq a$. Comme la relation $\leq$ est antisymétrique, on obtient $a = a'$. On peut donc dire qu'un élément a est *le* plus grand (ou *le* plus petit) élément de A.
2) Considérons la relation $\leq$ dans $E = \mathbb{R}$ et soit $A = [0, 1[$. Alors, les majorants de A sont les réels M tels que $1 \leq M$, les minorants de A sont les réels m tels que $m \leq 0$, A a 0 pour plus petit élément, mais A n'a pas de plus grand élément.
3) Considérons la relation $\leq$ dans $E = \mathbb{N}$ et soit $A = \{x \in \mathbb{N} \mid x^2 \leq 2\}$. Alors, $A = \{0, 1\}$, 0 est le seul minorant de A et c'est le plus petit élément de A ; les majorants de A sont les entiers naturels non nuls et 1 est le plus grand élément de A.

Définition 5.17 – *Soient A un sous-ensemble de E et M un élément de E. On dit que M est une borne supérieure de A si M est un plus petit élément de l'ensemble des majorants de A, c'est à dire si les deux conditions suivantes sont vérifiées :*

1) M est un majorant de A
2) Si M' est un autre majorant de A, alors $M \leq M'$.

ou de façon équivalente si :

1) M est un majorant de A.
2) Si $M' < M$, il existe un élément a de A tel que $M' < a \leq M$.

On définit de même une borne inférieure.

Exercice - Ecrire avec des quantificateurs la définition d'une borne supérieure et d'une borne inférieure.

Exemples et remarques

1) Reprenons le premier exemple ci-dessus. L'ensemble $A = [0, 1[$ admet 0 comme borne inférieure et 1 comme borne supérieure.
2) S'il existe une borne supérieure de A , elle est unique. On peut donc dire qu'un élément M est **la** borne supérieure de A et noter $M = \sup A$. De même s'il existe une borne inférieure m, elle est unique, on parle de **la** borne inférieure de A et on note $m = \inf A$.
3) Si A a une borne supérieure et si elle appartient à A, c'est le plus grand élément de A et inversement, un plus grand élément est une borne supérieure. Le premier exemple montre cependant que $\sup \mathcal{A}$ n'est pas forcément un plus grand élément.
4) Pour que la borne supérieure existe, il est évidemment nécessaire que l'ensemble soit majoré. Mais ce n'est pas toujours suffisant. Par exemple, dans l'ensemble $\mathbb{Q}$ muni de la relation $\leq$, considérons le sous-ensemble $A = \{x \in \mathbb{Q} \mid x^2 \leq 2\}$. Il est majoré (par 3 par exemple). Mais A n'a pas de borne supérieure ; en effet, s'il existe une borne supérieure M, on peut montrer qu'elle vérifie $M^2 = 2$; mais il est facile de montrer qu'il n'existe pas de rationnel M tel que $M^2 = 2$ (essayez) ; on aboutit donc à une contradiction.
5) Par contre l'ensemble $\mathbb{R}$ muni de la relation $\leq$ possède la propriété fondamentale suivante :

   Tout sous-ensemble non vide et majoré de $\mathbb{R}$ admet une borne supérieure.

   et de même :

   Tout sous-ensemble non vide et minoré de $\mathbb{R}$ admet une borne inférieure.

Cette propriété est à la base de nombreux théorèmes d'analyse. Nous y reviendrons au cours du chapitre sur les suites réelles. Elle permet par exemple de démontrer l'existence de $\sqrt{2}$: en effet, le sous-ensemble de $\mathbb{R}$ égal à $\{x \in \mathbb{R} \mid x^2 \leq 2\}$ a une borne supérieure a, et on peut montrer que l'on a $a^2 = 2$.