1. Lois de composition ; associativité et commutativité

Étant donné un ensemble X, on appelle **loi de composition sur X** toute application de l'ensemble produit X × X dans l'ensemble X lui-même. Une loi de composition sur X consiste donc, intuitivement, à faire correspondre, à tout couple (x, y) d'éléments de X, un troisième élément de X qui dépend de x et de y suivant une loi donnée d'avance.

Dans la pratique on emploie pour désigner les lois de composition des notations telles que $(x, y) \mapsto x + y$, ou $(x, y) \mapsto xy$, ou $(x, y) \mapsto x \wedge y$, etc... Dans ce § nous utiliserons souvent le signe $\perp$, qui n'est utilisé nulle part ailleurs en Mathématiques actuellement (et qui par conséquent est susceptible de désigner n'importe quelle loi de composition).

Soit $(x, y) \mapsto x \perp y$ une loi de composition sur un ensemble X. On dit que cette loi de composition est **associative** si l'on a

$$x \perp (y \perp z) = (x \perp y) \perp z \quad \text{quels que soient } x, y, z \in \mathrm{X}.$$

Dans ce cas, étant donnés des éléments $x_1, x_2, \ldots, x_n$ de X, en nombre quelconque, on pose, par définition,

$$x_1 \perp x_2 \perp \ldots \perp x_n = (x_1 \perp \ldots \perp x_{n-1}) \perp x_n$$

(récurrence sur n), et on a alors la relation

$$x_1 \perp \ldots \perp x_n = (x_1 \perp \ldots \perp x_p) \perp (x_{p+1} \perp \ldots \perp x_n)$$

pour tout entier p tel que $1 \leqslant p \leqslant n$.

Supposons la loi de composition considérée notée $(x, y) \mapsto xy$, comme une multiplication — on dit alors qu'on utilise la **notation multiplicative.** Pour tout $x \in \mathrm{X}$ et tout entier $n \geqslant 1$, on définit alors la **puissance** n^e de x par la formule

$$x^n = x \ldots x \quad (n \text{ facteurs}),$$

et on a alors

$$x^p x^q = x^{p+q}$$

quels que soient les entiers $p, q \geqslant 1$.

Si au contraire on note $(x, y) \mapsto x + y$ la loi de composition considérée, auquel cas on dit qu'on utilise la **notation additive,** on définit

$$nx = x + \cdots + x \quad (n \text{ termes})$$

pour tout $x \in \mathrm{X}$ et tout entier $n \geqslant 1$; bien entendu, il n'y a entre cette notion et celle de puissance n^e qu'une différence dans les *notations* utilisées ; cela dit, la formule de multiplication des puissances écrite plus haut en notation multiplicative se traduit, en notation additive, par la relation

$$px + qx = (p + q)x.$$

Revenons à une loi de composition $(x, y) \mapsto x \perp y$ sur un ensemble X ; on dit qu'une telle loi est **commutative** si l'on a

$$x \perp y = y \perp x \quad \text{quels que soient } x, y \in \mathrm{X}.$$

On emploie la notation multiplicative aussi bien pour des lois de composition non commutatives que pour des lois de composition commutatives ; mais, dans la pratique, *la notation additive s'emploie uniquement pour des lois de composition commutatives.*

Soit $(x, y) \mapsto x \perp y$ une loi de composition *associative et commutative* sur un ensemble X, et soit $(x_i)_{i \in \mathrm{I}}$ une famille *finie* d'éléments de X. Soit n le nombre d'éléments de I et écrivons ceux-ci sous forme d'une suite $i_1, \ldots, i_n$; l'élément

$$x_{i_1} \perp x_{i_2} \perp \cdots \perp x_{i_n}$$

de X ne dépend évidemment pas (vu l'associativité et la commutativité de la loi de composition considérée) de la façon dont on a écrit les éléments de I sous la forme d'une suite de n termes. On pose alors, par définition,

$$\mathop{\perp}_{i \in \mathrm{I}} x_i = x_{i_1} \perp \cdots \perp x_{i_n}.$$

Si la loi de composition considérée est écrite *multiplicativement,* on écrit

$$\prod_{i \in \mathrm{I}} x_i = x_{i_1} \cdots x_{i_n} ;$$

si elle est écrite *additivement,* on utilise la notation

$$\sum_{i \in \mathrm{I}} x_i = x_{i_1} + \cdots + x_{i_n}.$$

Remarque 1. Les notations condensées qu'on vient d'introduire subissent dans la pratique de nombreuses modifications que l'usage enseignera. Par exemple, si I est l'ensemble formé des entiers $1, \cdots, n$, on écrit souvent

$$x_1 + \cdots + x_n = \sum_{i=1}^{i=n} x_i \qquad \text{ou} \qquad \sum_{1 \leqslant i \leqslant n} x_i;$$

si I est l'ensemble des couples (i, j) d'entiers tels que $1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$, et si l'on note x_{ij} le terme « général » de la famille considérée, on utilise fréquemment la notation

$$\sum_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant q}} x_{ij} \qquad \text{au lieu de} \qquad \sum_{(i,\, j) \in \mathrm{I}} x_{ij};$$

on notera que, dans ce cas, l'associativité de la loi de composition se traduit par la relation

$$\sum_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant q}} x_{ij} = \sum_{1 \leqslant i \leqslant p} \Big(\sum_{1 \leqslant j \leqslant q} x_{ij} \Big),$$

où le second membre désigne la somme

$$(x_{11} + x_{12} + \cdots + x_{1q}) + \cdots + (x_{p1} + x_{p2} + \cdots + x_{pq});$$

l'emploi de ces notations condensées est souvent indispensable pour éviter des formules inextricables.

Notons enfin que dans la notation

$$\sum_{i \in \mathrm{I}} x_i,$$

la lettre i ne joue aucun rôle et n'intervient pas réellement dans le résultat — elle indique simplement une opération à effectuer (à savoir prendre la somme de tous les x_i obtenus en faisant varier i dans I), et on peut la remplacer par toute autre lettre *non encore utilisée par ailleurs* (cette dernière précaution est essentielle pour éviter des erreurs grossières).

Reprenons une loi de composition quelconque $(x, y) \mapsto x \perp y$ sur un ensemble X. On appelle **élément neutre** pour cette loi de composition tout élément $e \in \mathrm{X}$ tel que l'on ait

$$x \perp e = e \perp x = x \qquad \text{pour tout } x \in \mathrm{X}.$$

THÉORÈME 1. *Si une loi de composition admet un élément neutre, elle en admet un seul.*

Supposons en effet que e' et e'' soient des éléments neutres; la formule $e' \perp x = x$ donne en particulier $e' \perp e'' = e''$; la formule $x \perp e'' = x$ donne en particulier $e' \perp e'' = e'$; on a donc $e' = e''$, d'où le Théorème.

Donnons maintenant quelques exemples importants de lois de composition.

Exemple 1. Sur l'ensemble $\mathbf{Z}$ des entiers rationnels (entiers de signe quelconque), on a trois lois de composition que tout le monde connaît : l'*addition* $(x, y) \mapsto x + y$, qui est commutative, associative, et admet un élément neutre (à savoir le nombre 0); la *multiplication* $(x, y) \mapsto xy$, qui est commutative, associative, et admet un élément neutre (à savoir le nombre 1); enfin la *soustraction* $(x, y) \mapsto x - y$, qui n'est pas commutative, ni associative, et n'admet pas d'élément neutre.

On pourrait dans cet Exemple remplacer $\mathbf{Z}$ par l'ensemble $\mathbf{Q}$ des nombres rationnels, ou par l'ensemble $\mathbf{R}$ des nombres réels.

Exemple 2. Soit $\mathbf{Q}^*$ l'ensemble des nombres rationnels *non nuls*; la multiplication $(x, y) \mapsto xy$ est une loi de composition (associative, commutative et avec élément neutre) sur $\mathbf{Q}^*$; il en est de même de la division $(x, y) \mapsto x/y$ (qui n'est pas associative, ni commutative, et n'admet pas d'élément neutre). On aura soin de remarquer que la division *n'est pas* une loi de composition sur l'ensemble $\mathbf{Q}$ de tous les nombres rationnels, car, le quotient x/y n'étant pas défini pour $y = 0$, l'application $(x, y) \to x/y$ n'est pas définie sur $\mathbf{Q} \times \mathbf{Q}$ tout entier.

Exemple 3. On prend $\mathrm{X} = \mathbf{N}$, ensemble des entiers naturels, et les applications $(x, y) \mapsto \mathrm{ppcm}\,(x, y)$ et $(x, y) \to \mathrm{pgcd}\,(x, y)$; ce sont des lois de composition commutatives et associatives; la première admet un élément neutre, la seconde n'en admet pas (le lecteur devra bien entendu démontrer lui-même ces assertions à titre d'exercice).

Exemple 4. Soient E un ensemble quelconque et X l'ensemble de toutes les applications de E dans E; l'application $(f, g) \mapsto f \circ g$ de $\mathrm{X} \times \mathrm{X}$ dans X est une loi de composition sur X, laquelle est associative (§ 2, Théorème 2), admet un élément neutre (l'application identique j_{E}), mais n'est pas commutative.

Exemple 5. Soient E un ensemble quelconque et $\mathrm{X} = \mathfrak{P}(\mathrm{E})$ l'ensemble des parties de E; alors les applications $(x, y) \mapsto x \cap y$ et $(x, y) \mapsto x \cup y$ sont des lois de composition associatives et commutatives sur X, en vertu des formules du § 3, nº 1. La première de ces lois admet pour élément neutre l'ensemble E, la seconde, l'ensemble vide.

Exemple 6. Soit X l'ensemble des vecteurs d'origine donnée 0 dans l'espace (ce mot étant pris au sens usuel); à tout couple de vecteurs x, y d'origine 0, associons leur produit « vectoriel » (noté, suivant les auteurs, $x \times y$ ou $x \wedge y$; nous emploierons ici la notation $x \wedge y$); on obtient ainsi une loi de composition qui n'est ni associative, ni commutative.

2. *Éléments symétrisables*

Soit $(x, y) \mapsto x \perp y$ une loi de composition sur un ensemble X, admettant un élément neutre e. Étant donné un élément $x \in \mathrm{X}$, on appelle **symétrique à gauche** (resp. **symétrique à droite**) de x tout élément $x' \in \mathrm{X}$ tel que l'on ait

$$x' \perp x = e \qquad (\text{resp. } x \perp x' = e);$$

et on appelle **symétrique** de x tout élément x' vérifiant

$$x' \perp x = x \perp x' = e.$$

Enfin, on dit que x est **symétrisable** s'il existe un élément symétrique de x.

Lorsqu'on a affaire à une loi de composition écrite en notation *multiplicative*, on emploie le mot **inverse** au lieu du mot symétrique, et le mot **inversible** au lieu du mot symétrisable [par exemple, si l'on considère sur **Q** la loi de composition $(x, y) \mapsto xy$, les éléments inversibles sont les nombres rationnels *non nuls*, et l'inverse d'un tel nombre x est le nombre $1/x$]; l'inverse d'un élément inversible x de X se note alors généralement

$$x^{-1}.$$

Lorsqu'on a affaire à une loi de composition écrite en notation *additive*, on dit **opposé** au lieu de symétrique, et on note

$$-x$$

l'opposé d'un $x \in X$ (tout au moins si l'on note 0 l'élément neutre de X, ce qui est presque toujours le cas en notation additive).

Notons enfin que la distinction entre symétrique à gauche et symétrique à droite n'a intérêt que pour une loi de composition non commutative.

Donnons un exemple qui montre que, dans le cas non commutatif, les trois notions sont distinctes.

Exemple 7. Prenons la loi de composition de l'*Exemple* 4 ci-dessus. Dire qu'un $f \in X$ admet un *inverse à gauche* signifie qu'il existe une application $g \in X$ telle que $g \circ f = j_E$; pour cela, il faut et il suffit que f soit *injective* (§ 2, Théorème 3). Dire f admet un *inverse à droite* signifie qu'il existe une application g telle que $f \circ g = j_E$; pour cela il faut et il suffit que f soit *surjective* (§ 2, Théorème 4). Enfin dire que que f est inversible signifie évidemment que f est *bijective*, et alors l'inverse de f pour la loi de composition considérée n'est autre que l'application réciproque au sens du § 2.

Théorème 2. *Soit $(x, y) \mapsto x \perp y$ une loi de composition associative et admettant un élément neutre sur un ensemble* E. *Pour qu'un élément x de* E *soit symétrisable, il faut et il suffit qu'il admette un symétrique à gauche et un symétrique à droite; x admet alors un seul symétrique, qui est aussi l'unique symétrique à gauche et l'unique symétrique à droite de x.*

Soient x' un symétrique à gauche et x'' un symétrique à droite de x; on a donc $x' \perp x = x \perp x'' = e$, élément neutre de E; tenant compte de l'associativité, on déduit de là que $x'' = e \perp x'' = (x' \perp x) \perp x'' = x' \perp (x \perp x'') = x' \perp e = x'$; tout symétrique à droite de x est donc égal à tout symétrique à gauche, ce qui montre que x admet *un seul* symétrique à gauche, *un seul* symétrique à droite, et qu'ils sont égaux; notant x' leur valeur commune, on a $x' \perp x = x \perp x' = e$, de sorte que x est symétrisable et admet x' pour symétrique (nécessairement unique, car un symétrique de x est *a fortiori* symétrique à gauche et symétrique à droite, donc égal à x'). Ceci achève la démonstration.

Nous supposerons jusqu'à la fin de ce § que la loi de composition considérée sur l'ensemble E *est associative et admet un élément neutre e.* Pour un élément symétrisable x de E, on peut donc parler *du* symétrique x' de x (ou de l'inverse x^{-1} en notation multiplicative, de l'opposé $-x$ en notation additive).

Théorème 3. *Si un $x \in$ E est symétrisable, il en est de même de son symétrique x', et celui-ci admet x pour symétrique. Si x et y sont symétrisables, il en est de même de $x \perp y$, et on a la relation*

$$(x \perp y)' = y' \perp x'.$$

Les relations

$$x' \perp x = x \perp x' = e$$

rendent triviale la première assertion de l'énoncé. Pour établir la seconde, on calcule

$$(y' \perp x') \perp (x \perp y) = y' \perp (x' \perp x) \perp y = y' \perp e \perp y = y' \perp y = e,$$
$$(x \perp y) \perp (y' \perp x') = x \perp (y \perp y') \perp x' = x \perp e \perp x' = x \perp x' = e,$$

ce qui montre bien que $x \perp y$ est symétrisable et admet $y' \perp x'$ pour symétrique.

En notation multiplicative, le Théorème 3 se traduit comme suit : si x est inversible il en est de même de son inverse, et on a

$$(x^{-1})^{-1} = x;$$

si x et y sont inversibles, il en est de même de xy et on a

$$(xy)^{-1} = y^{-1}x^{-1}.$$

En notation additive, ce qui suppose la loi de composition considérée commutative, le Théorème 3 se traduit ainsi : si x admet un opposé, il en est de même de son opposé, et on a

$$-(-x) = x;$$

si x et y admettent des opposés, il en est de même de $x + y$, et on a

$$-(x + y) = (-x) + (-y),$$

ce qu'on écrit d'ailleurs en général sous la forme

$$-(x + y) = -x - y.$$

Théorème 4. *Soit a un élément symétrisable de* E; *alors, pour tout $b \in$ E, il existe un et un seul $x \in$ E tel que*

$$a \perp x = b,$$

à savoir

$$x = a' \perp b.$$

En effet, la relation $a \perp x = b$ implique $a' \perp (a \perp x) = a' \perp b$, i.e.

$$a' \perp b = (a' \perp a) \perp x = e \perp x = x;$$

inversement, de $x = a' \perp b$ résulte

$$a \perp x = a \perp (a' \perp b) = (a \perp a') \perp b = e \perp b = b,$$

ce qui achève la démonstration.

En notation multiplicative: si a est inversible, l'équation

$$ax = b$$

possède une et une seule solution, à savoir

$$x = a^{-1}b;$$

en notation additive: si a admet un opposé, alors l'équation

$$a + x = b$$

possède une et une seule solution, à savoir

$$x = b + (-a),$$

qu'on écrit d'ailleurs

$$x = b - a$$

(**différence** entre b et a).

Indiquons pour terminer ce § que, dans le reste de cet ouvrage, on n'utilisera *jamais plus* le signe $\perp$, ni les mots « symétrisable », « symétrique », etc... On aura *toujours* affaire à des lois de composition notées soit multiplicativement, soit additivement; utiliser pour de telles lois de composition les mots « symétrisable » et « symétrique » (par exemple, parler du « symétrique pour la multiplication » d'un nombre réel non nul, comme le font souvent les débutants), serait parfaitement ridicule.

EXERCICES

Il est parfaitement utopique d'espérer apprendre des Mathématiques, si élémentaires ou si supérieures soient-elles, sans résoudre des Exercices.

Les Exercices qu'on trouvera dans ce livre sont de trois sortes. Certains sont des illustrations pratiques ou même numériques des théories exposées dans le texte; le lecteur débutant ne pourra pas acquérir la technique du calcul sans résoudre une partie appréciable des Exercices de ce genre. D'autres apportent au texte des compléments théoriques élémentaires; en les étudiant, le lecteur s'habituera à manipuler le langage et les modes de raisonnements utilisés dans le texte; ceux de ces Exercices qui ne sont pas *très faciles* sont précédés d'un signe ¶. Enfin, la dernière catégorie est constituée par des Exercices qui apportent au texte des compléments importants et difficiles; ils sont destinés uniquement aux étudiants déjà avancés qui s'intéressent vraiment aux Mathématiques; ces Exercices sont précédés de deux ou même trois signes ¶.

Nous ne saurions trop insister enfin sur le fait que résoudre un Exercice ne consiste pas seulement à se convaincre, à l'aide d'un « brouillon » fait à la hâte, du fait qu'on en a à peu près compris la solution; si cette méthode est admissible pour les Exercices de calcul numérique, il faut par contre s'efforcer de *rédiger intégralement* les Exercices plus théoriques, où l'on doit construire de véritables démonstrations. De cette façon, et uniquement de cette façon, l'étudiant parviendra à acquérir un langage clair et correct, et à utiliser les termes techniques dans leur sens propre, ce qui, en Mathématiques, est le signe le plus certain de la compréhension d'un sujet.