

Structures algébriques

Plan du chapitre

1 Lois de composition interne	page 2
1.1 Définition	page 2
1.2 Exemples	page 2
1.3 Propriétés éventuelles des lois de composition interne	page 2
1.3.1 Commutativité	page 2
1.3.2 Associativité	page 2
1.3.2 Distributivité	page 2
1.4 Eléments particuliers	page 3
1.4.1 Elément neutre	page 3
1.4.2 Elément absorbant	page 3
1.4.3 Elément symétrisable	page 3
1.4.4 Elément simplifiable	page 4
1.5 Parties stables	page 4
2 Groupes	page 5
2.1 Définition	page 5
2.2 Groupes de référence	page 5
2.3 Sous-groupes	page 6
2.4 La notation nx ou x^n , $n \in \mathbb{Z}$	page 8
3 Anneaux	page 9
3.1 Définition	page 9
3.2 Calculs dans un anneau	page 10
3.3 Groupe des inversibles d'un anneau	page 10
3.4 Corps	page 11

1 Lois de composition interne

1.1 Définition

DÉFINITION 1. Soit E un ensemble non vide. Une **loi de composition interne** sur E (ou encore une opération dans E) est une application de $E \times E$ dans E .

Il s'agit de comprendre que le schéma : pour x et y réels, la somme de x et y est $x + y$, le schéma : pour A et B parties de E , l'intersection de A et B est $A \cap B$, et le schéma : pour f et g applications de \mathbb{C} dans \mathbb{C} , la composée de f suivie de g est $g \circ f$, sont un seul et même schéma. Dans les trois cas, on prend deux objets de même nature (deux réels dans le premier cas, deux parties d'un ensemble dans le deuxième et deux applications de \mathbb{R} dans \mathbb{R} dans le troisième), et on construit un nouvel objet de même nature que les deux objets de départ (la somme de deux réels est un réel, l'intersection de deux parties de E est une partie de E et la composée de deux applications de \mathbb{R} dans \mathbb{R} est une application de \mathbb{R} dans \mathbb{R}).

1.2 Exemples

- Dans \mathbb{N} , \mathbb{Z} , \mathbb{R} ou \mathbb{C} , l'addition et la multiplication sont des lois de composition interne.
- Dans \mathbb{N} , la soustraction n'est pas une loi interne, mais elle l'est dans \mathbb{Z} .
- La division dans \mathbb{R} n'est pas une loi interne mais la division dans \mathbb{R}^* l'est.
- Dans \mathbb{N}^* , l'exponentiation, c'est-à-dire l'application $(\mathbb{N}^*)^2 \rightarrow \mathbb{N}^*$, le PGCD ou le PPCM sont des lois internes.
 $(a, b) \mapsto a^b$
- E étant un ensemble donné, l'intersection et la réunion sont des lois de composition interne dans $\mathcal{P}(E)$.
- Si E est un ensemble non vide, la composition des applications de E dans E est une loi interne dans E^E .

La liste précédente est très loin d'être exhaustive.

1.3 Propriétés éventuelles des lois de composition interne

Soient E un ensemble non vide et $*$ une loi de composition interne sur E . $*$ peut avoir ou non une ou plusieurs des propriétés suivantes :

1.3.1 Commutativité

DÉFINITION 2. $*$ est **commutative** $\Leftrightarrow \forall (x, y) \in E^2, x * y = y * x$.

L'addition et la multiplication dans \mathbb{C} sont commutatives. La loi \circ dans E^E fournit l'exemple le plus important de loi non commutative (en général $f \circ g \neq g \circ f$).

1.3.2 Associativité

DÉFINITION 3. $*$ est **associative** $\Leftrightarrow \forall (x, y, z) \in E^3, (x * y) * z = x * (y * z)$.

Si $*$ est associative, les expressions $(x * y) * z$ et $x * (y * z)$ peuvent se noter tout simplement $x * y * z$.

L'addition et la multiplication dans \mathbb{C} ou la composition dans E^E sont des lois associatives ($(f \circ g) \circ h = f \circ (g \circ h)$ et on peut écrire plus simplement $f \circ g \circ h$). La division dans \mathbb{C}^* est interne mais n'est pas associative. Cela a pour conséquence

que la notation $\frac{\frac{A}{B}}{C}$ n'a pas de signification et qu'il faut affiner en $\frac{A}{\frac{B}{C}} = \frac{AC}{B}$ ou $\frac{\frac{A}{C}}{B} = \frac{A}{BC}$.

De même, l'exponentiation dans \mathbb{N}^* n'est pas associative, de sorte que l'écriture a^{b^c} n'a pas de sens. Il faut affiner en $a^{(b^c)}$ ou $(a^b)^c = a^{bc}$. Par exemple, $2^{(2^3)} = 2^8 = 256$ alors que $(2^2)^3 = 4^3 = 64$.

1.3.3 Distributivité d'une loi sur une autre

DÉFINITION 4. Soient E un ensemble non vide et $*$ et \top deux lois de composition internes sur E .
 \top est distributive sur $*$ $\Leftrightarrow \forall (x, y, z) \in E^3, x \top (y * z) = (x \top y) * (x \top z)$ et $(y * z) \top x = (y \top x) * (z \top x)$.

Si on sait que \top est commutative, une et une seule des deux égalités ci-dessus suffit.

Dans \mathbb{C} , la multiplication est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication.

Dans $\mathcal{P}(E)$, l'intersection est distributive sur la réunion et la réunion est distributive sur l'intersection.

Dans $\mathbb{R}^{\mathbb{R}}$, \circ est distributive à droite sur $+$, mais pas à gauche ($(g+h) \circ f = g \circ f + h \circ f$, mais en général, $f \circ (g+h) \neq f \circ g + f \circ h$).

1.4 Eléments particuliers

1.4.1 Élément neutre

DÉFINITION 5. Soient E un ensemble non vide et $*$ une loi interne sur E .

Soit $e \in E$. e est **élément neutre** pour $*$ $\Leftrightarrow \forall x \in E, e * x = x * e = x$.

$*$ admet un élément neutre dans $E \Leftrightarrow \exists e \in E / \forall x \in E, x * e = e * x = x$.

\Rightarrow **Commentaire**.

\diamond Notez bien l'ordre des quantificateurs $\exists e \in E / \forall x \in E, \dots$ qui dit que e est précis et ne dépend pas de x , et non pas $\forall x \in E, \exists e \in E / \dots$ qui permettrait à e de changer quand x change.

\diamond Si on sait que la loi $*$ est commutative, une et une seule des deux égalités ($\forall x \in E, x * e = x$ ou $\forall x \in E, e * x = x$) ci-dessus suffit.

Théorème 1. Si $*$ admet un élément neutre, celui-ci est unique.

DÉMONSTRATION. Soient e et e' deux éléments neutres (pas nécessairement distincts). Alors $e = e * e' = e'$. \square

Exemples

- Dans \mathbb{C} , 0 est élément neutre pour l'addition et 1 est élément neutre pour la multiplication.
- Dans E^E , Id_E est élément neutre pour la loi \circ .
- Dans $\mathcal{P}(E)$, E est élément neutre pour l'intersection et \emptyset est élément neutre pour la réunion. \square

1.4.2 Élément absorbant

DÉFINITION 6. Soient E un ensemble non vide et $*$ une loi interne sur E .

Soit $a \in E$. a est élément **absorbant** pour $*$ $\Leftrightarrow \forall x \in E, a * x = x * a = a$.

- Dans \mathbb{C} , 0 est absorbant pour la multiplication.
- Dans $\mathcal{P}(E)$, E est absorbant pour la réunion et \emptyset est absorbant pour l'intersection.
- Pour l'exponentiation dans \mathbb{N}^* , 1 est absorbant à gauche ($\forall a \in \mathbb{N}^*, 1^a = 1$) et est élément neutre à droite ($\forall a \in \mathbb{N}^*, a^1 = a$).

1.4.3 Élément symétrisable

DÉFINITION 7. Soient E un ensemble non vide et $*$ une loi interne sur E possédant un élément neutre e .

Soit $x \in E$.

x admet un **symétrique à gauche** pour $*$ $\Leftrightarrow \exists x' \in E / x' * x = e$.

x admet un **symétrique à droite** pour $*$ $\Leftrightarrow \exists x' \in E / x * x' = e$.

x admet un **symétrique** pour $*$ $\Leftrightarrow \exists x' \in E / x * x' = x' * x = e$.

x est **symétrisable à gauche** pour $*$ si et seulement si x admet un symétrique à gauche pour $*$.

x est **symétrisable à droite** pour $*$ si et seulement si x admet un symétrique à droite pour $*$.

x est **symétrisable** pour $*$ si et seulement si x admet un symétrique pour $*$.

\Rightarrow **Commentaire**.

\diamond Notez que ici, on fournit x' après avoir fourni x (soit $x \in E \dots \exists x' \in E \dots$) et donc bien sûr, x' varie quand x varie.

\diamond Si on sait que la loi $*$ est commutative, une et une seule des deux égalités ci-dessus suffit.

Théorème 2. Soit x un élément de E . Si $*$ est associative, possède un élément neutre e et si x admet un symétrique pour $*$, celui-ci est unique.

DÉMONSTRATION. Soit x un élément de E . Soient x' et x'' deux éléments symétriques de x (pas nécessairement distincts).

Alors, $x'' = e * x'' = (x' * x) * x'' = x' * (x * x'') = x' * e = x'$. \square

Si $*$ est l'addition dans \mathbb{C} , le symétrique (défini ci-dessus de manière très générale) d'un complexe z n'est autre que $-z$ et s'appelle l'**opposé** de z .

Si $*$ est la multiplication dans $\mathbb{C} \setminus \{0\}$, le symétrique d'un complexe non nul z n'est autre que $\frac{1}{z}$ et s'appelle l'**inverse** de z . (Ainsi, l'égalité $i^2 = -1$ qui s'écrit encore $i \times (-i) = 1$ doit immédiatement signifier dans notre tête que i et $-i$ sont inverses l'un de l'autre et donc $\frac{1}{i} = -i$ et $\frac{1}{-i} = i$).

Si $*$ est la composition des applications, les éléments de E^E qui admettent un symétrique pour la loi \circ sont les **bijections** de E sur E . Le symétrique d'une bijection f pour la loi \circ n'est autre que sa **réciproque** f^{-1} .

Théorème 3. Soient E un ensemble non vide puis $*$ une loi de composition interne sur E , associative et possédant un élément neutre e .

Soient x et y deux éléments de E . Si x et y sont symétrisables, alors $x * y$ est symétrisable et $(x * y)' = y' * x'$.

DÉMONSTRATION . Soient x et y deux éléments symétrisables de E . Soient x' et y' leurs symétriques respectifs.

$$(x * y) * (y' * x') = x * (y * y') * x' = x * e * x' = x * x' = e$$

et

$$(y' * x') * (x * y) = y' * (x' * x) * y = y' * e * y = y' * y = e.$$

Donc, $x * y$ est symétrisable et son symétrique est $y' * x'$. □

Ainsi,

- dans \mathbb{C} , l'opposé $-(z_1 + z_2)$ de $z_1 + z_2$ est $-z_1 - z_2$,
- dans \mathbb{C}^* , l'inverse $\frac{1}{z_1 \times z_2}$ de $z_1 \times z_2$ est $\frac{1}{z_1} \times \frac{1}{z_2}$,
- et dans l'ensemble des bijections d'un ensemble E sur lui-même, la réciproque $(g \circ f)^{-1}$ de $g \circ f$ est $f^{-1} \circ g^{-1}$ (et pas $g^{-1} \circ f^{-1}$).

1.4.4 Élément simplifiable

DÉFINITION 8. Soient E un ensemble non vide et $*$ une loi interne sur E .

Soit $x \in E$.

x est **simplifiable à gauche** pour $*$ $\Leftrightarrow \forall (y, z) \in E^2, x * y = x * z \Rightarrow y = z$.

x est **simplifiable à droite** pour $*$ $\Leftrightarrow \forall (y, z) \in E^2, y * x = z * x \Rightarrow y = z$.

x est **simplifiable** si et seulement si x est simplifiable à gauche et à droite.

Théorème 4. Si $*$ est associative et possède un élément neutre e , tout élément symétrisable est simplifiable.

DÉMONSTRATION . Soit x un élément de E , symétrisable pour $*$. Soit x' son symétrique pour $*$. Pour $(y, z) \in E^2$,

$$x * y = x * z \Rightarrow x' * (x * y) = x' * (x * z) \Rightarrow (x' * x) * y = (x' * x) * z \Rightarrow e * y = e * z \Rightarrow y = z.$$

□

- Dans \mathbb{C} , tout élément est simplifiable pour l'addition : $\forall (z, z', z'') \in \mathbb{C}^3, (z + z' = z + z'' \Rightarrow z' = z'')$.
- Dans \mathbb{C} , les éléments simplifiables pour la multiplication sont les complexes non nuls : $\forall (z, z', z'') \in \mathbb{C}^* \times \mathbb{C} \times \mathbb{C}, (z \times z' = z \times z'' \Rightarrow z' = z'')$. Mais attention, on ne simplifie pas par 0 ($0 \times 1 = 0 \times 2$ mais $1 \neq 2$). Donc, $az = az' \not\Rightarrow z = z'$ mais ($az = az'$ et $a \neq 0$) $\Rightarrow z = z'$.
- Dans E^E , on peut montrer que les éléments simplifiables à gauche sont les injections, les éléments simplifiables à droite sont les surjections et les éléments simplifiables sont les bijections.

1.5 Parties stables

DÉFINITION 9. Soient E un ensemble non vide puis $*$ une loi de composition interne sur E . Soit F une partie non vide de E .

F est **stable** pour $*$ $\Leftrightarrow \forall (x, y) \in F^2, x * y \in F$.

- Dans \mathbb{Z} , l'ensemble des nombres pairs est stable pour l'addition (la somme de deux nombres pairs est un nombre pair) ou pour la multiplication (le produit de deux nombres pairs est un nombre pair) alors l'ensemble des nombres impairs est stable pour la multiplication (le produit de deux nombres impairs est un nombre impair) mais n'est pas stable pour l'addition (la somme de deux nombres impairs n'est pas toujours un nombre impair).

- Dans E^E , l'ensemble des injections, l'ensemble des surjections et l'ensemble des bijections sont stables pour \circ (la composée de deux injections (resp. deux surjections, deux bijections) est une injection (resp. une surjection, une bijection)).
- Dans \mathbb{C} , l'ensemble U des nombres complexes de module 1 est stable pour la multiplication (un produit de deux nombres complexes de module 1 est un nombre complexe de module 1).

DÉFINITION 10. Soient E un ensemble non vide puis $*$ une loi de composition interne sur E . Soit F une partie non vide de E , stable pour $*$.

L'application $F \times F \rightarrow F$ est appelée **loi induite** par $*$ sur F .

$$(x, y) \mapsto x * y$$

2 Groupes

2.1 Définition

DÉFINITION 11. Soit G un ensemble non vide muni d'une loi de composition interne (notée $*$).

$(G, *)$ est un **groupe** si et seulement si

- 1) $*$ est **associative**,
- 2) $*$ possède un **élément neutre** dans G
- 3) tout élément de G possède un **symétrique** pour $*$ dans G .

Si de plus, $*$ est commutative, le groupe $(G, *)$ est dit **commutatif** ou **abélien**.

Par exemple, $(\mathbb{C}, +)$ est un groupe abélien mais (\mathbb{C}, \times) n'est pas un groupe car 0 n'a pas d'inverse dans \mathbb{C} (pour \times). On peut noter que dans un groupe, tout élément est symétrisable et donc simplifiable.

2.2 Groupes de référence

Le théorème suivant « est immédiat » :

Théorème 5.

$(\mathbb{C}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{D}, +)$, $(\mathbb{Z}, +)$ sont des groupes commutatifs.

(\mathbb{C}^*, \times) , (\mathbb{R}^*, \times) , (\mathbb{Q}^*, \times) , (\mathbb{D}^*, \times) sont des groupes commutatifs.

Théorème 6. Soit D une partie non vide de \mathbb{R} .

$(\mathbb{R}^D, +)$ et $(\mathbb{C}^D, +)$ sont des groupes commutatifs.

DÉMONSTRATION. Dans ce qui suit, \mathbb{K} désigne \mathbb{R} ou \mathbb{C} . On rappelle que la somme de deux applications f et g de D dans \mathbb{K} est définie par :

$$\forall x \in D, (f + g)(x) = f(x) + g(x).$$

- La somme de deux applications de D dans \mathbb{K} est une application de D dans \mathbb{K} . Donc, $+$ est une loi de composition interne sur \mathbb{K}^D .
- Soit $(f, g) \in (\mathbb{K}^D)^2$. Pour tout x de D ,

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

Donc, pour tout $(f, g) \in (\mathbb{K}^D)^2$, $f + g = g + f$. La loi $+$ est commutative dans \mathbb{K}^D .

- Soit $(f, g, h) \in (\mathbb{K}^D)^2$. Pour tout x de D ,

$$((f + g) + h)(x) = (f + g)(x) + h(x) = f(x) + g(x) + h(x) = f(x) + (g + h)(x) = (f + (g + h))(x).$$

Donc, pour tout $(f, g, h) \in (\mathbb{K}^D)^3$, $(f + g) + h = f + (g + h)$. La loi $+$ est associative dans \mathbb{K}^D .

- En notant 0 , la fonction nulle sur D , pour tout f de D , on a $f + 0 = f$. Donc, $+$ possède un élément neutre dans \mathbb{K}^D à savoir 0 , la fonction nulle sur D .

- Soit $f \in \mathbb{K}^D$. En notant $-f$, la fonction $x \mapsto -f(x)$, on a $f + (-f) = 0$. Donc, tout élément f de \mathbb{K}^D possède un opposé dans \mathbb{K}^D à savoir $-f$.

On a montré que $(\mathbb{K}^D, +)$ est un groupe commutatif. □

DÉFINITION 12. Soit E un ensemble non vide. Une **permutation** de E est une bijection de E sur E . L'ensemble des permutations de E se note $\mathcal{S}(E)$.

Théorème 7. $(\mathcal{S}(E), \circ)$ est un groupe, non commutatif dès que E contient au moins trois éléments deux à deux distincts.

DÉMONSTRATION .

- La composée de deux permutations de E est une permutation de E . Donc, \circ est une loi de composition interne sur $\mathcal{S}(E)$.
- La composition des permutations est associative.
- Pour tout $f \in \mathcal{S}(E)$, $f \circ \text{Id}_E = \text{Id}_E \circ f = f$ et de plus Id_E est une permutation de E . Donc, \circ possède un élément neutre dans $\mathcal{S}(E)$ à savoir Id_E .
- Soit $f \in \mathcal{S}(E)$. On sait que f^{-1} est une permutation de E et $f \circ f^{-1} = f^{-1} \circ f = \text{Id}_E$. Donc, tout élément f de $\mathcal{S}(E)$ possède un symétrique pour \circ dans $\mathcal{S}(E)$, à savoir f^{-1} .

On a montré que $(\mathcal{S}(E), \circ)$ est un groupe.

Supposons de plus que E possède au moins trois éléments deux à deux distincts a, b et c . Pour $x \in E$, on pose $f(x) = \begin{cases} b & \text{si } x = a \\ a & \text{si } x = b \\ x & \text{si } x \notin \{a, b\} \end{cases}$

et $g(x) = \begin{cases} c & \text{si } x = b \\ b & \text{si } x = c \\ x & \text{si } x \notin \{b, c\} \end{cases}$. Puisque f et g sont des involutions de E , f et g sont en particulier des permutations de E . De plus, $g \circ f(a) = g(b) = c$ et $f \circ g(a) = f(a) = b$. Donc, $f \circ g(a) \neq g \circ f(a)$ puis $f \circ g \neq g \circ f$. Ceci montre que la loi \circ n'est pas commutative ou encore que le groupe $(\mathcal{S}(E), \circ)$ n'est pas un groupe commutatif. \square

2.3 Sous-groupes

DÉFINITION 13. Soient $(G, *)$ un groupe puis H une partie de G .

H est un sous-groupe de $(G, *)$ si et seulement si H est **non vide**, **stable** pour $*$ et, muni de la loi induite, est un groupe.

$\{e\}$ et G sont des sous-groupes de $(G, *)$ appelés sous-groupes triviaux du groupe $(G, *)$. Les autres sous-groupes, s'il en existe, sont appelés sous-groupes propres de $(G, *)$.

Si $(G, *)$ est un groupe et H une partie non vide et stable pour $*$ de G , il est par exemple automatique que la loi induite soit associative dans H car elle l'est dans G . Le théorème ci-dessous donne la liste des vérifications suffisantes pour affirmer qu'un certain sous-ensemble H de G est un sous-groupe de $(G, *)$ (en notant e l'élément neutre de $(G, *)$ et x' le symétrique dans G d'un élément x de G) :

Théorème 8 (caractérisations d'un sous-groupe). Soient $(G, *)$ un groupe puis H une partie de G .

H est un sous-groupe de $(G, *) \Leftrightarrow \begin{cases} (1) e \in H \\ (2) \forall (x, y) \in H^2, x * y \in H \\ (3) \forall x \in H, x' \in H \end{cases} \quad \text{(I)}$

H est un sous-groupe de $(G, *) \Leftrightarrow \begin{cases} (1) e \in H \\ (2) \forall (x, y) \in H^2, x * y' \in H \end{cases} \quad \text{(II)}.$

DÉMONSTRATION .

- Supposons que H soit un sous-groupe de $(G, *)$, alors la propriété (2) de (I) est vérifiée.

Notons e_H l'élément neutre de H . On a $e_H * e = e_H$ car e est élément neutre de G et d'autre part, $e_H = e_H * e_H$ car e_H est élément neutre de H . Par suite, $e_H * e = e_H * e_H$. Maintenant, dans le groupe $(G, *)$, tout élément est symétrisable et en particulier, tout élément est simplifiable. Après simplification par e_H , on obtient $e = e_H$. Ceci montre en particulier que $e \in H$.

Soit x un élément de H . Notons x'_H son symétrique pour $*$ dans H . On a $x'_H * x * x' = e * x' = x'$ (puisque $e_H = e$) et d'autre part, $x_H * x * x' = x'_H * e = x'_H$. Donc, le symétrique x'_H de x dans H est son symétrique x' dans G . Ceci montre en particulier que x' est dans H .

On a montré que si H est un sous-groupe de $(G, *)$ alors (I) est vérifié.

- Montrons que : (I) \Rightarrow H sous-groupe de $(G, *)$. Supposons (I).

H est une partie non vide de G d'après (1). La restriction de $*$ à H^2 est une loi interne dans H d'après (2). $*$ est associative dans G et donc la loi induite est associative dans H .

L'élément neutre e de $(G, *)$ vérifie $\forall x \in H, x * e = e * x = x$ et donc e est élément neutre de H pour la loi induite.

Enfin, si x est un élément quelconque de H , le symétrique x' de x dans G est dans H et vérifie $x * x' = x' * x = e$ où e est maintenant élément neutre de H . x' est donc le symétrique de x dans H et on a montré que tout élément de H admet un symétrique dans H . De tout ceci, on en déduit bien que H est un sous-groupe de $(G, *)$ et donc que $(H \text{ sous-groupe}) \Leftrightarrow (I)$.

• Il est clair que $(I) \Rightarrow (II)$. Il reste à montrer que $(II) \Rightarrow (I)$. On suppose donc que H vérifie (II) .

Soit x un élément de H . Puisque e et x sont dans H , $e * x' = x'$ est dans H d'après (2). Ainsi, $\forall x \in H, x' \in H$.

Soient enfin, x et y deux éléments de H . D'après ce qui précède, y' est encore dans H et donc $x * (y')' = x * y$ est dans H . On a montré que $(II) \Rightarrow (I)$ et finalement que $(I) \Leftrightarrow (II)$. □

⇒ Commentaire .

◇ On a montré au passage que l'élément neutre e de G est dans tout sous-groupe de G . Ceci peut être faux dans une situation plus générale. Par exemple, Si E est un ensemble, l'intersection dans $\mathcal{P}(E)$ est interne, commutative, associative et possède un élément neutre, à savoir E .

Soit alors F une partie stricte de E . $\mathcal{P}(F)$ est une partie non vide de $\mathcal{P}(E)$, stable pour l'intersection (l'intersection de deux parties de F reste une partie de F). L'intersection possède un élément neutre dans $\mathcal{P}(F)$, à savoir F . Cet élément neutre est distinct de l'élément neutre de $(\mathcal{P}(E), \cap)$. Une conséquence est que $(\mathcal{P}(E), \cap)$ n'est pas un groupe.

◇ On a aussi montré que pour tout sous-groupe H d'un groupe $(G, *)$, le symétrique d'un élément de H dans H est son symétrique dans G . De la même manière que précédemment, on peut construire des exemples où ces symétriques sont distincts (pas dans un groupe).

On peut redonner explicitement les caractérisations précédentes quand $*$ est la loi $+$ ou la loi \times pour une partie H de G :

$$H \text{ est un sous-groupe de } (G, +) \Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2, x + y \in H \\ (3) \forall x \in H, -x \in H \end{cases} \quad (I) \Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2, x - y \in H \end{cases} \quad (II).$$

$$H \text{ est un sous-groupe de } (G, \times) \Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2, x \times y \in H \\ (3) \forall x \in H, x^{-1} \in H \end{cases} \quad (I) \Leftrightarrow \begin{cases} (1) H \neq \emptyset \\ (2) \forall (x, y) \in H^2, x \times y^{-1} \in H \end{cases} \quad (II).$$

Théorème 9. Si H et K sont des sous-groupes de $(G, *)$, $H \cap K$ est un sous-groupe de $(G, *)$. Ainsi, une intersection de sous-groupes est un sous-groupe.

DÉMONSTRATION . (On utilise la caractérisation (II) ci-dessus). Soient H et K deux sous-groupes. D'après ce qui précède, H et K contiennent l'élément neutre e de G et donc $H \cap K \neq \emptyset$. D'autre part, bien sûr $H \cap K \subset G$.

Soient alors x et y deux éléments de $H \cap K$.

$$(x, y) \in (H \cap K)^2 \Rightarrow ((x, y) \in H^2 \text{ et } (x, y) \in K^2) \Rightarrow (x * y' \in H \text{ et } x * y' \in K) \Rightarrow x * y' \in H \cap K.$$

Ceci montre que $H \cap K$ est un sous-groupe de $(G, *)$. □

On complète maintenant (un peu) la liste des groupes de référence.

Théorème 10.

- 1) U est un sous-groupe de (\mathbb{C}^*, \times) .
- 2) Pour tout $n \in \mathbb{N}^*$, U_n est un sous-groupe de (U, \times) .

DÉMONSTRATION .

1) Un nombre complexe de module 1 est non nul et donc $U \subset \mathbb{C}^*$. 1 a pour module 1 et donc $1 \in U$. Soit alors $(z_1, z_2) \in U^2$.

$$\left| \frac{z_1}{z_2} \right| = \frac{|z_1|}{|z_2|} = \frac{1}{1} = 1,$$

et donc $\frac{z_1}{z_2} \in U$. On a montré que U est un sous-groupe de (\mathbb{C}^*, \times) .

2) Soit $n \in \mathbb{N}^*$. Une racine n -ème de 1 dans \mathbb{C} est un nombre complexe de module 1 donc $U_n \subset U$. 1 est une racine n -ème de 1 et donc $1 \in U_n$. Soit alors $(z_1, z_2) \in U_n^2$.

$$\left(\frac{z_1}{z_2}\right)^n = \frac{z_1^n}{z_2^n} = \frac{1}{1} = 1,$$

et donc $\frac{z_1}{z_2} \in \mathbb{U}_n$. On a montré que \mathbb{U}_n est un sous-groupe de (\mathbb{U}, \times) . □

2.4 La notation x^n ou x^n , $n \in \mathbb{Z}$

Soit $(G, *)$ un groupe.

• On se place dans la situation où la loi du groupe $*$ est \times (ou \circ) ou encore on travaille notation multiplicative. L'élément neutre de G est alors noté 1_G et le symétrique d'un élément x de G est noté x^{-1} . Plus généralement, pour $x \in G$ et $n \in \mathbb{Z}$, on pose

$$x^n = \begin{cases} \underbrace{x \times x \dots \times x}_{n \text{ facteurs}} & \text{si } n > 0 \\ 1_G & \text{si } n = 0 \\ \underbrace{x^{-1} \times x^{-1} \dots \times x^{-1}}_{-n \text{ facteurs}} & \text{si } n < 0 \end{cases}.$$

$$\text{Si } * \text{ est la loi } \circ \text{ dans } S(E) \text{ (} E \text{ ensemble non vide donné) et } f \text{ est un élément de } S(E), f^n = \begin{cases} \underbrace{f \circ f \dots \circ f}_{n \text{ facteurs}} & \text{si } n > 0 \\ \text{Id}_E & \text{si } n = 0 \\ \underbrace{f^{-1} \circ f^{-1} \dots \circ f^{-1}}_{-n \text{ facteurs}} & \text{si } n < 0 \end{cases}.$$

Avec ces notations, on a les règles usuelles de calcul sur les exposants :

Théorème 11.

- 1) $\forall x \in G, \forall n \in \mathbb{Z}, x^{-n} = (x^n)^{-1}$.
- 2) $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, x^n \times x^m = x^{n+m}$.
- 3) $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, (x^n)^m = x^{nm}$.
- 4) $\forall (x, y) \in G^2, \forall n \in \mathbb{Z}, (x \times y = y \times x \Rightarrow (x \times y)^n = x^n \times y^n)$.

⇒ **Commentaire.** La dernière affirmation mérite d'être explicitée. Dire que $x \times y = y \times x$, c'est dire que x et y **commutent**. Le problème ne se pose pas dans les groupes (\mathbb{R}^*, \times) ou (\mathbb{C}^*, \times) qui sont des groupes commutatifs. Dans ce cas, deux éléments quelconques x et y commutent et on peut toujours affirmer que pour $n \in \mathbb{Z}$, $(x \times y)^n = x^n \times y^n$.

A ce jour, la seule loi non commutative que nous connaissions est la loi \circ . Si f et g sont deux permutations d'un certain ensemble E , on pourra écrire $(f \circ g)^n = f^n \circ g^n$ **si f et g commutent**. Si f et g ne commutent pas, tout ce qu'on peut faire est par exemple $(f \circ g)^2 = f \circ g \circ f \circ g$ et cette dernière expression n'a aucune raison d'être égale à $f \circ f \circ g \circ g$ qui est $f^2 \circ g^2$. On rappelle aussi que $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ (et pas $f^{-1} \circ g^{-1}$).

Dans l'année, les élèves qui n'ont pas pris la spécialité maths en terminale S découvriront une multiplication non commutative, la multiplication des matrices. Quand on aura deux matrices carrées A et B qui ne commutent pas, on pourra écrire $(A \times B)^2 = A \times B \times A \times B$ mais on ne pourra pas écrire $(AB)^2 = A^2B^2$.

DÉMONSTRATION. Il est clair que $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, x^n \times x^m = x^m \times x^n$ (deux puissances de x commutent).

1) Soient $x \in G$ et $n \in \mathbb{Z}$. Si $n = 0$, $(x^n)^{-1} = (1_G)^{-1} = 1_G = 1_G^{-n}$.
Si $n > 0$,

$$\begin{aligned} x^n \times x^{-n} &= x \times \dots \times x \times x^{-1} \times \dots \times x^{-1} \\ &= x \times x^{-1} \times x \times x^{-1} \times \dots \times x \times x^{-1} \text{ (car } x \text{ et } x^{-1} \text{ commutent)} \\ &= 1_G \times \dots \times 1_G = 1_G \end{aligned}$$

et de même, $x^{-n} \times x^n = 1_G$. Donc, $x^{-n} = (x^n)^{-1}$.

Si $n < 0$, alors $-n > 0$ puis $(x^{-n})^{-1} = x^{-(-n)} = x^n$ puis $x^{-n} = (x^n)^{-1}$.

2) Soit $x \in G$. Il est clair que $\forall m \in \mathbb{N}, x^{m+1} = x^m \times x$. Soit $n \in \mathbb{Z}$. Montrons par récurrence que $\forall m \geq 0, x^n \times x^m = x^{n+m}$.

- $x^n \times x^0 = x^n \times 1_G = x^n = x^{n+0}$. L'égalité est donc vraie pour $m = 0$.
- Soit $m \geq 0$. Supposons que $x^n \times x^m = x^{n+m}$. Alors, $x^n \times x^{m+1} = x^n \times x^m \times x = x^{n+m} \times x = x^{n+m+1}$.

Le résultat est démontré par récurrence. Ainsi, $\forall (n, m) \in \mathbb{N}^2, x^{n+m} = x^n x^m$.

Si $-n \leq m < 0$, alors $n + m \geq 0$ et $-m \geq 0$ puis $x^{n+m} \times x^{-m} = x^{n+m+(-m)} \times x^m$. Si $m < -n$, alors $m + n < 0$ alors $-n - m > 0$ puis $x^{n+m} = (x^{-n-m})^{-1} = (x^{-n} x^{-m})^{-1} = x^n x^m$. Ainsi, $\forall (n, m) \in \mathbb{N} \times \mathbb{Z}, x^{n+m} = x^n x^m$ et finalement, en échangeant les rôles de n et m , $\forall (n, m) \in \mathbb{Z}^2, x^{n+m} = x^n x^m$.

3) Soient $x \in G$ et $n \in \mathbb{Z}$. Pour $m \in \mathbb{Z}$,

- si $m = 0$, $(x^n)^m = 1_G = x^0 = x^{nm}$,
- si $m > 0$, $(x^n)^m = \underbrace{x^n \times \dots \times x^n}_{m \text{ facteurs}} = \begin{cases} 1_G = x^{mn} & \text{si } n = 0 \\ = \underbrace{x \times \dots \times x}_{mn \text{ facteurs}} = x^{mn} & \text{si } n > 0 \end{cases}$.

Si $n < 0$, $(x^n)^m \times x^{-nm} = (x^n)^m \times (x^{-n})^m = x^n \times \dots \times x^n \times x^{-n} \times \dots \times x^{-n} = x^n \times x^{-n} \times \dots \times x^n \times x^{-n} = 1_G \times \dots \times 1_G = 1_G$ et de même, $x^{-nm} \times (x^n)^m = 1_G$ puis $(x^n)^m = x^{nm}$.

Donc, $\forall x \in G, \forall (n, m) \in \mathbb{Z} \times \mathbb{N}, (x^n)^m = x^{nm}$.

- si $m < 0$, $(x^n)^m \times x^{-nm} = (x^n)^m \times (x^n)^{-m} = 1_G$ et donc $(x^n)^m = x^{nm}$.

On a montré que $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, (x^n)^m = x^{nm}$.

4) Soit $(x, y) \in G^2$ tel que $x \times y = y \times x$. Soit $n \in \mathbb{Z}$.

- Si $n = 0$, $(x \times y)^n = 1_G = 1_G \times 1_G = x^n \times y^n$.
- Si $n > 0$, $(x \times y)^n = x \times y \times \dots \times x \times y = x \times \dots \times x \times y \times y = x^n \times y^n$.
- Si $n < 0$, $((x \times y)^n)^{-1} = (x \times y)^{-n} = x^{-n} \times y^{-n} = y^{-n} \times x^{-n}$ (clair) puis $(x \times y)^n = (y^{-n} \times x^{-n})^{-1} = (x^{-n})^{-1} (y^{-n})^{-1} = x^n y^n$. □

• On se place maintenant dans la situation où la loi du groupe $*$ est $+$ ou encore on travaille notation additive. L'élément neutre de G est alors noté 0_G et le symétrique d'un élément x de G est noté $-x$. Plus généralement, pour $x \in G$ et $n \in \mathbb{Z}$, on pose

$$nx = \begin{cases} \underbrace{x + x \dots + x}_{n \text{ termes}} & \text{si } n > 0 \\ 0_G & \text{si } n = 0 \\ \underbrace{(-x) + (-x) \dots + (-x)}_{-n \text{ termes}} & \text{si } n < 0 \end{cases} .$$

Avec ces notations, on a

Théorème 12.

- $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, nx + mx = (n + m)x$.
- $\forall x \in G, \forall n \in \mathbb{Z}, (-n)x = -nx$.
- $\forall x \in G, \forall (n, m) \in \mathbb{Z}^2, n(mx) = nm$.
- $\forall (x, y) \in G^2, \forall n \in \mathbb{Z}, (x + y = y + x \Rightarrow n(x + y) = nx + ny)$.

DÉMONSTRATION. Démonstration identique à la démonstration du théorème 11 en remplaçant \times par $+$ (et donc 1_G par 0_G , x^{-1} par $-x$ et x^n par nx). □

3 Anneaux et corps

3.1 Définition

DÉFINITION 14. Soit A un ensemble non vide ayant au moins deux éléments muni de deux lois de composition interne (notées $+$ et $*$).

$$(A, +, *) \text{ est un } \mathbf{anneau} \Leftrightarrow \begin{cases} \mathbf{1)} & (A, +) \text{ est un groupe commutatif} \\ \mathbf{2)} & \mathbf{a)} \quad * \text{ est associative} \\ & \mathbf{b)} \quad * \text{ possède un élément neutre dans } A \\ \mathbf{3)} & * \text{ est distributive sur } + \end{cases} .$$

L'anneau est **commutatif** si et seulement si $*$ est commutative.

Un exemple fondamental d'anneau commutatif est $(\mathbb{Z}, +, \times)$. On rencontrera d'autres exemples d'anneaux par la suite. A cet instant, on ne peut pas encore fournir d'exemples d'anneau non commutatif. Ces exemples viendront au deuxième semestre.

3.2 Calculs dans un anneau

Théorème 13. Soit $(A, +, *)$ un anneau. On note 0_A l'élément neutre de A pour $+$.

$\forall x \in A, x * 0_A = 0_A * x = 0_A$ (l'élément neutre pour l'addition est toujours absorbant pour la multiplication).

DÉMONSTRATION. Soit $x \in A$. $0_A * x = (0_A + 0_A) * x = 0_A * x + 0_A * x$ car $*$ est distributive sur $+$. Maintenant, $(A, +)$ est un groupe et dans un groupe, tout élément est simplifiable. Donc, $0_A * x + 0_A * x = 0_A * x = 0_A * x + 0_A$ entraîne $0_A * x = 0_A$. De même, $x * 0_A = 0_A$. \square

Théorème 14. Soit $(A, +, *)$ un anneau.

$\forall (a, b) \in A^2, (-a) * b = a * (-b) = -(a * b)$

DÉMONSTRATION. Soit $(a, b) \in A^2$.

$$a * b + (-a) * b = (a + (-a)) * b = 0_A * b = 0_A$$

et donc $(-a) * b = -a * b$. De même, $a * b + a * (-b) = a * (b + (-b)) = a * 0_A = 0_A$ et donc $a * (-b) = -a * b$. \square

\Rightarrow **Commentaire.** Le théorème 14 n'énonce pas une évidence. Il dit que le produit de l'opposé de a par b est l'opposé du produit de a par b et il doit être démontré.

Théorème 15. Soit $(A, +, *)$ un anneau. Soient a et b deux éléments de A . Si a et b commutent,

$$\forall n \in \mathbb{N}, (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k} \text{ (formule du binôme de NEWTON),}$$

$$\forall n \in \mathbb{N}^*, a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k},$$

(avec la convention $\forall x \in A, x^0 = 1_A$).

DÉMONSTRATION. Les démonstrations sont identiques à celles déjà faites dans le chapitre « Les symboles Σ et Π . Le binôme de NEWTON », l'hypothèse « a et b commutent » permettant de réécrire des produits du type $a \times b \times b \times \dots \times a \times b$ sous la forme $a^p b^q$. \square

3.3 Groupe des inversibles d'un anneau

Théorème 15. Soit $(A, +, \times)$ un anneau. On note A^* l'ensemble des éléments de A qui sont inversibles c'est-à-dire l'ensemble des éléments de A symétrisables pour \times .

(A^*, \times) est un groupe.

DÉMONSTRATION.

- 1_A est un élément de A^* car 1_A est inversible pour \times , d'inverse lui-même. En particulier, $A^* \neq \emptyset$.
- Si x et y sont deux éléments de A^* , on sait que $x \times y$ est dans A^* et que $(x \times y)^{-1} = y^{-1} \times x^{-1}$. Donc, \times induit une loi de composition interne sur A^* que l'on note encore \times .
- \times est associative dans A et donc \times est associative dans A^* .
- $1_A \in A^*$ et pour tout x de A^* , $1_A \times x = x \times 1_A = x$. Donc, \times possède un élément neutre dans A^* .
- Soit $x \in A^*$. On sait que $x^{-1} \in A^*$ et que $(x^{-1})^{-1} = x$. Donc, tout élément de A^* admet un symétrique pour \times dans A^* .

On a montré que (A^*, \times) est un groupe. \square

\Rightarrow **Commentaire.**

◇ Le résultat du théorème 15 a été énoncé et démontré en notant \times la deuxième loi de A . Les notations devront être adaptées si par exemple, la deuxième loi de A est \circ .

3.4 Corps

DÉFINITION 14. Soit $(K, +, \times)$ un anneau.

$(K, +, \times)$ est un **corps** si et seulement si tout élément non nul de K admet un inverse (pour \times) dans K .

Le corps est **commutatif** si et seulement si $*$ est commutative.

$(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps commutatifs. En maths sup et en maths spé, tous les corps que l'on rencontre sont commutatifs. $(\mathbb{Z}, +, \times)$ est un anneau commutatif qui n'est pas un corps car par exemple, le nombre 2 n'est pas inversible dans \mathbb{Z} .

Théorème 16. Dans un corps, un produit de facteurs est nul si et seulement si l'un de ces facteurs est nul.

DÉMONSTRATION . Soit $(K, +, \times)$ un corps. On note 0 (resp. 1) l'élément neutre pour + (resp. \times). Soit $(a, b) \in K^2$ tel que $a \times b = 0$.

Si $a \neq 0$, a admet un inverse pour \times noté a^{-1} . On peut écrire

$$a \times b = 0 \Rightarrow a^{-1} \times a \times b = a^{-1} \times 0 \Rightarrow 1 \times b = 0 \Rightarrow b = 0.$$

□