Chapitre 19. Structures algébriques

Plan du chapitre

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 $\begin{array}{ccc}(\mathbb{N}^*)^2 & \to & \mathbb{N}^* \\ (a,b) & \mapsto & a^b\end{array}$, le PGCD ou le PPCM sont des lois internes.
- 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 $\dfrac{\frac{A}{B}}{C}$ n'a pas de signification et qu'il faut affiner en $\dfrac{\frac{A}{B}}{C} = \dfrac{AC}{B}$ ou $\dfrac{\frac{A}{B}}{C} = \dfrac{A}{BC}$.

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 T deux lois de composition internes sur E.
T est distributive sur $* \Leftrightarrow \forall (x,y,z) \in E^3,\ x\,T\,(y*z) = (x\,T\,y)*(x\,T\,z)$ et $(y*z)\,T\,x = (y\,T\,x)*(z\,T\,x)$.

Si on sait que T 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 Elément 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 $E \Leftrightarrow \exists e \in E/\ \forall x \in E,\ x*e = e*x = x$.

⇨ **Commentaire** .

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

◇ *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 $e = e*e' = e'$. ❑

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 $\varnothing$ est élémet neutre pour la réunion. ❑

1.4.2 Elément 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 $\varnothing$ 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 Elément 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 $*$.

⇨ **Commentaire** .

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

◇ *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, $x'' = e*x'' = (x'*x)*x'' = x'*(x*x'') = x'*e = x'$. ❑

Si $*$ est l'addition notée $+$ dans E (addition des nombres, des fonctions, des suites ou plus tard des matrices ...), le symétrique d'un élément x de E est noté $-x$ et s'appelle l'**opposé** de x.

Si $*$ est la multiplication notée $\times$ dans E, le symétrique d'un élément x de E est noté x^{-1} (ou aussi $\frac{1}{x}$ dans un ensemble de nombres par exemple mais pas dans l'ensemble des matrices) et s'appelle l'**inverse** de x. (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 $i^{-1} = \frac{1}{i} = -i$ 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 $g^{-1} \circ f^{-1}$).

Théorème 4. Soient E un ensemble non vide puis $*$ une loi de composition interne sur E, associative et possédant un élément neutre e.

Soit x un élément de E. Si x est symétrisable, alors son symétrique x' est symétrisable et $(x')' = x$.

Démonstration. Soit x un élément symétrisable de E. Soit x' son symétrique. Les égalités $x * x' = x' = x = e$ montre que x' est symétrisable et que le symétrique de x' est x.

❑

Donc, $\forall z \in \mathbb{C}$, $-(-z) = z$, $\forall z \in \mathbb{C}^*$, $1/(1/z) = z$ et $\forall f \in \mathcal{S}(E)$, $\left(f^{-1}\right)^{-1} = f$.

1.4.4 Elément 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 5. 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 que 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 (et même jamais) 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 $\begin{array}{ccc} F \times F & \to & F \\ (x,y) & \mapsto & x * y \end{array}$ est appelée **loi induite** par $*$ sur F.

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 6.

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

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

Théorème 7. Soit D une partie de non vide de $\mathbb{R}$.

$\left(\mathbb{R}^D,+\right)$ 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 $(f,g) \in \left(\mathbb{K}^D\right)^2$. Pour tout x de D,

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

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

• Soit $(f,g,h) \in \left(\mathbb{K}^D\right)^2$. 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 $(f,g,h) \in \left(\mathbb{K}^D\right)^3$, $(f+g)+h = f+(g+h)$. 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 $\left(\mathbb{K}^D,+\right)$ 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 $\mathcal{S}(E)$ ou S_E.

Théorème 8. $(\mathcal{S}(E),\circ)$ 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 $f \in \mathcal{S}(E)$, $f \circ Id_E = Id_E \circ f = f$ 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 $f \circ f^{-1} = f^{-1} \circ f = Id_E$. 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. ❑

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

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

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

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 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 $x'_H * x * x' = e_H * x' = e * x' = x'$ 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 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 $+$ (notation additive) ou la loi $\times$ (notation multiplicative) pour une partie H de G ou la loi $\circ$ dans $\mathcal{S}(E)$. Il s'agit simplement d'adapter les notations :

$$\text{H est un sous-groupe de } (G,+) \Leftrightarrow \left\{\begin{array}{l}(1)\ 0_G \in H\\(2)\ \forall (x,y)\in H^2,\ x+y\in H\\(3)\ \forall x\in H,\ -x\in H\end{array}\right. \quad (I) \Leftrightarrow \left\{\begin{array}{l}(1)\ 0_G \in H\\(2)\ \forall (x,y)\in H^2,\ x-y\in H\end{array}\right. \quad (II).$$

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

$$\text{H est un sous-groupe de } (\mathcal{S}(E),\circ) \Leftrightarrow \left\{\begin{array}{l}(1)\ Id_E \in H\\(2)\ \forall (f,g)\in H^2,\ f\circ g\in H\\(3)\ \forall f\in H,\ f^{-1}\in H\end{array}\right. \quad (I) \Leftrightarrow \left\{\begin{array}{l}(1)\ Id_E \in H\\(2)\ \forall (f,g)\in H^2,\ f\circ g^{-1}\in H\end{array}\right. \quad (II).$$

Théorème 10. 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)). Soient H et K deux sous-groupes. D'après ce qui précède, H et K contiennent l'élément neutre e de G et donc $e \in H\cap K$. 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 11.

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 en particulier 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 $\frac{z_1}{z_2} \in U_n$. On a montré que U_n est un sous-groupe de $(U, \times)$.

❑

Ainsi, $(U, \times)$ et $(U_n, \times)$ sont deux nouveaux groupes de référence.

2.4 La notation nx 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

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

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

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

Théorème 12.

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, on découvrira 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 .

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

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

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

Si $n<0$, alors $-n>0$ puis $\left(x^{-n}\right)^{-1} = x^{-(-n)} = x^n$ puis, en prenant l'inverse des deux membres, $x^{-n} = (x^n)^{-1}$.

2) Soit $x\in G$. Il est clair que $\forall m\in\mathbb{N}$, $x^{m+1} = x^m\times x$. Si $m<0$, alors $-m\geqslant 0$, $-(m+1)\geqslant 0$ puis $x^{-(m+1)}\times x = x^{-m-1+1} = x^{-m}$ puis $x^m\times x = x^{m+1}$. Ainsi, $\forall m\in\mathbb{Z}$, $x^{m+1} = x^m\times x$.

Soit $n\in\mathbb{N}$. Montrons par récurrence que $\forall m\geqslant -n$, $x^n\times x^m = x^{n+m}$.

- $x^n\times x^{-n} = 1_G = x^0 = x^{n+(-n)}$. L'égalité est donc vraie pour $m=-n$.
- Soit $m\geqslant -n$. 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, $\forall(m,n)\in\mathbb{Z}\times\mathbb{N}$, $(m+n\geqslant 0\Rightarrow x^{n+m} = x^n\times x^m)$.
Par symétrie des rôles, $\forall(m,n)\in\mathbb{N}\times\mathbb{Z}$, $(m+n\geqslant 0\Rightarrow x^{n+m} = x^n\times x^m)$ et donc $\forall(m,n)\in\mathbb{Z}^2$, $(m+n\geqslant 0\Rightarrow x^{n+m} = x^n\times x^m)$.

Si $m+n<0$, $x^{m+n} = \left(x^{-m-n}\right)^{-1} = \left(x^{-n}\right)^{-1}\times\left(x^{-m}\right)^{-1} = x^m\times x^n$. Finalement, $\forall(m,n)\in\mathbb{Z}^2$, $x^{n+m} = x^n\times x^m$.

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

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

  Si $n<0$, $(x^n)^m\times x^{-nm} = (x^n)^m\times\left(x^{-n}\right)^m = x^n\times\ldots\times x^n\times x^{-n}\times\ldots\times x^{-n} = x^n\times x^{-n}\times\ldots\times x^n\times x^{-n} = 1_G\times\ldots\times 1_G = 1_G$ 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 $n>0$, $(x\times y)^n = x\times y\times\ldots\times x\times y = x\times\ldots\times x\times y\times y = x^n\times y^n$.
- Si $n<0$, $((x\times y)^n)^{-1} = (x\times y)^{-n} = x^{-n}\times y^{-n} = y^{-n}\times x^{-n}$ (clair) puis $(x\times y)^n = \left(y^{-n}\times x^{-n}\right)^{-1} = \left(x^{-n}\right)^{-1}\left(y^{-n}\right)^{-1} = x^n y^n$.

❑

• 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

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

Avec ces notations, on a

Théorème 13.

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

Démonstration. Démonstration identique à la démonstration du théorème 12 en remplaçant $\times$ par $+$ (et donc 1_G par 0_G, x^{-1} par $-x$ et x^n par nx).

❑

2.5 Groupe produit

Théorème 14 (et définition).

Soient $n \geqslant 2$ puis $(G_1, *_1)$, ..., $(G_n, *_n)$ n groupes. Soit $G = \prod_{i=1}^{n} G_i$.

Pour tous $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ éléments de G, on pose $x * y = (x_1 *_1 y_1, \ldots, x_n *_n y_n)$.

$(G, *)$ est un groupe appelé **groupe produit** des groupes $(G_1, *_1)$, ..., $(G_n, *_n)$.

Démonstration. • Aucun des G_i, $1 \leqslant i \leqslant n$, n'est vide et donc G n'est pas vide.

• Pour chaque $i \in [\![1, n]\!]$, $*_i$ est une loi de composition interne dans G_i. Donc, $*$ est une loi de composition interne dans G.

• Soient $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ et $z = (z_1, \ldots, z_n)$ trois éléments de G.

$$\begin{aligned}(x * y) * z &= (x_1 *_1 y_1, \ldots, x_n *_n y_n) * (z_1, \ldots, z_n)\\ &= ((x_1 *_1 y_1) *_1 z_1, \ldots, (x_n *_n y_n) *_n z_n) = (x_1 *_1 (y_1 *_1 z_1), \ldots, x_n *_n (y_n *_n z_n))\\ &= (x_1, \ldots, x_n) * (y_1 *_1 z_1, \ldots, y_n *_n z_n)\\ &= x * (y * z).\end{aligned}$$

$*$ est associative dans G.

• Pour chaque $i \in [\![1, n]\!]$, on note e_i l'élément neutre de G_i pour $*_i$. On pose $e = (e_1, \ldots, e_n)$. Pour $x = (x_1, \ldots, x_n) \in G$,

$$x * e = (x_1, \ldots, x_n) * (e_1, \ldots, e_n) = (x_1 *_1 e_1, \ldots, x_n *_n e_n) = (x_1, \ldots, x_n) = x$$

et de même, $e * x = x$. Donc, $*$ admet un élément neutre dans G à savoir e.

• Soit $x = (x_1, \ldots, x_n) \in G$. Soit $x' = (x'_1, \ldots, x'_n)$ où, pour chaque $i \in [\![1, n]\!]$, x'_i désigne le symétrique de x_i pour $*_i$ dans G_i. x' est un élément de G tel que

$$x * x' = \left(x_1 *_1 x'_1, \ldots, x_n *_n x'_n\right) = (e_1, \ldots, e_n) = e$$

et de même, $x' * x = e$. Donc, tout élément $x = (x_1, \ldots, x_n)$ de G admet un symétrique pour $*$ dans G à savoir $x' = (x'_1, \ldots, x'_n)$.

On a montré que $(G, *)$ est un groupe.

❑

Par exemple, dans $\mathbb{R}^3$, si on pose

$$\forall ((x_1, y_1, z_1), (x_2, y_2, z_2)) \in \left(\mathbb{R}^3\right)^2,\ (x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + y_1, x_2 + y_2, x_3 + y_3),$$

alors, $\left(\mathbb{R}^3, +\right)$ est un groupe (commutatif). L'élément neutre pour $+$ est le triplet $(0, 0, 0)$ et l'opposé d'un triplet (x, y, z) de $\mathbb{R}^3$ est le triplet $(-x, -y, -z)$.

2.6 Morphismes de groupes

2.6.1 Définition

Définition 14. Soient $(G, *)$ et $(G', *')$ deux groupes. Soient f une application de G vers G'

f est un **morphisme de groupes** si et seulement si $\forall (x, y) \in G^2,\ f(x * y) = f(x) *' f(y)$.

Un **isomorphisme** du groupe $(G, *)$ sur le groupe $(G', *')$ est un morphisme du groupe $(G, *)$ sur le groupe $(G', *')$ qui de plus est bijectif.
On dit que les groupes $(G, *)$ et $(G', *')$ sont **isomorphes** si et seulement si il existe un isomorphisme du groupe $(G, *)$ sur le groupe $(G', *')$.

Par exemple, $(\mathbb{R}, +)$ et $(]0, +\infty[, \times)$ sont deux groupes (commutatifs). On sait que pour tout $(x, y) \in \mathbb{R}^2$, $e^{x+y} = e^x \times e^y$ et que l'application $\begin{array}{ccc}\mathbb{R} & \to &]0, +\infty[\\ x & \mapsto & e^x\end{array}$ est bijective. Donc, $\begin{array}{ccc}(\mathbb{R}, +) & \to & (]0, +\infty[, \times)\\ x & \mapsto & e^x\end{array}$ est un isomorphisme de groupes.

2.6.2 Quelques propriétés des morphismes de groupes

Théorème 15. Soient $(G,*)$ et $(G',*')$ deux groupes dont les éléments neutres sont notés respectivement e et e'. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$. Alors,

1) $f(e)=e'$.
2) $\forall x\in G,\ f\left(x^{-1}\right)=(f(x))^{-1}$ (en notant x^{-1} plutôt que x' le symétrique de x pour $*$ dans G).

Démonstration .

1) $f(e)*'f(e)=f(e*e)=f(e)=f(e)*'e'$. Dans le groupe $(G',*')$, tout élément est simplifiable. Après simplification par $f(e)$, on obtient $f(e)=e'$.

2) Soit $x\in G$. $f(x)*'f\left(x^{-1}\right)=f\left(x*x^{-1}\right)=f(e)=e$ et de même $f\left(x^{-1}\right)*'f(x)=e'$. Donc, $(f(x))^{-1}=f\left(x^{-1}\right)$.

❑

Par exemple, puisque l'exponentielle est un morphisme du groupe $(\mathbb{R},+)$ vers le groupe $(]0,+\infty[,\times)$, les règles de calcul du théorème précédent se traduisent explicitement par les égalités $e^0=1$ (l'image de l'élément neutre 0 de $(\mathbb{R},+)$ est l'élément neutre 1 de $(]0,+\infty[,\times)$) et pour tout réel x, $e^{-x}=\dfrac{1}{e^x}$ (l'image de l'opposé est l'inverse de l'image).
De même, la fonction logarithme népérien est un morphisme du groupe $(]0,+\infty[,\times)$ vers le groupe $(\mathbb{R},+)$, et donc $\ln(1)=0$ et pour tout réel $x>0$, $\ln\left(\dfrac{1}{x}\right)=-\ln(x)$ (l'image de l'inverse est l'opposé de l'image).

Théorème 16. Soient $(G,*)$ et $(G',*')$ deux groupes. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$. Alors,

1) si H est un sous-groupe de $(G,*)$, $f(H)$ est un sous-groupe de $(G',*')$.
2) Si H' est un sous-groupe de $(G',*')$, $f^{-1}(H)$ est un sous-groupe de $(G,*)$.

Démonstration .

1) Soit H un sous-groupe de $(G,*)$. Montrons que $f(H)$ est un sous-groupe de $(G',*')$.

- $f(H)\subset G'$.
- $e\in H$ et donc $e'=f(e)\in f(H)$.
- Soit $(y_1,y_2)\in(f(H))^2$. Il existe $(x_1,x_2)\in H^2$ tel que $y_1=f(x_1)$ et $y_2=f(x_2)$. Mais alors,

$$y_1*'y_2^{-1}=f(x_1)*'(f(x_2))^{-1}=f(x_1)*'f\left(x_2^{-1}\right)=f\left(x_1*x_2^{-1}\right).$$

Puisque H est un sous-groupe de $(G,*)$, $x_1*x_2^{-1}\in H$ et donc $y_1*'y_2^{-1}\in f(H)$. On a montré que $f(H)$ est un sous-groupe de $(G',*')$.

2) Soit H' un sous-groupe de $(G',*')$. Montrons que $f^{-1}(H')$ est un sous-groupe de $(G,*)$.

- $f^{-1}(H')\subset G$.
- $f(e)=e'\in H'$ et donc $e\in f^{-1}(H')$.
- Soit $(x_1,x_2)\in\left(f^{-1}(H')\right)^2$. Alors, $f(x_1)$ et $f(x_2)$ sont dans H' puis

$$f\left(x_1*x_2^{-1}\right)=f(x_1)*'f\left(x_2^{-1}\right)=f(x_1)*'(f(x_2))^{-1}\in H',$$

et donc $x_1*x_2^{-1}\in f^{-1}(H')$. On a montré que $f^{-1}(H')$ est un sous-groupe de $(G,*)$.

❑

Théorème 17.

1) Soient $(G,*)$, $(G',*')$ et $(G'',*'')$ trois groupes. Soient f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$ et g un morphisme du groupe $(G',*')$ vers le groupe $(G'',*'')$. Alors $g\circ f$ est un morphisme du groupe $(G,*)$ vers le groupe $(G'',*'')$ (une composée de morphismes de groupes est un morphisme de groupes).

2) Soient $(G,*)$, $(G',*')$ deux groupes. Soit f un isomorphisme du groupe $(G,*)$ sur le groupe $(G',*')$. Alors f^{-1} est un isomorphisme du groupe $(G',*')$ sur le groupe $(G,*)$ (la réciproque d'un isomorphisme de groupes est un isomorphisme de groupes).

Démonstration .

1) Pour tout $(x,y)\in G^2$, $g\circ f(x*y)=g(f(x*y))=g(f(x)*'f(y))=g(f(x))*''g(f(y))=g\circ f(x)*''g\circ f(y)$. Donc, $g\circ f$ est un morphisme du groupe $(G,*)$ vers le groupe $(G'',*'')$.

2) Soit $(x,y)\in G'^2$. $f\left(f^{-1}(x)*f^{-1}(y)\right)=f\left(f^{-1}(x)\right)*'f\left(f^{-1}(y)\right)=x*'y=f\left(f^{-1}(x*'y)\right)$. Puisque f est injective, on en déduit que $f^{-1}(x)*f^{-1}(y)=f^{-1}(x*'y)$. Donc, f^{-1} est un morphisme du groupe $(G',*')$ sur le groupe $(G,*)$.

❑

2.6.3 Noyau et image d'un morphisme de groupes

DÉFINITION 15. Soient $(G,*)$ et $(G',*')$ deux groupes dont les éléments neutres sont notés respectivement e et e'. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$.

Le **noyau** de f, noté $\mathrm{Ker}(f)$, est l'ensemble des éléments de G dont l'image par f est e' :

$$\forall x \in G,\ (x \in \mathrm{Ker}(f) \Leftrightarrow f(x) = e') \qquad \mathrm{Ker}(f) = \{x \in G/\ f(x) = e'\}.$$

L'**image** de f, noté $\mathrm{Im}(f)$, est l'ensemble des images des éléments de G par f :

$$\forall y \in G',\ (y \in \mathrm{Im}(f) \Leftrightarrow \exists x \in G/\ y = f(x)) \qquad \mathrm{Im}(f) = \{f(x),\ x \in G\}.$$

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

⇨ **Commentaire** . *En anglais, le mot noyau se traduit par kernel et allemand, le mot noyau de traduit par kern.*

Théorème 18. Soient $(G,*)$, $(G',*')$ deux groupes. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$. Alors,

1) $\mathrm{Ker}(f)$ est un sous-groupe du groupe $(G,*)$.

2) $\mathrm{Im}(f)$ est un sous-groupe du groupe $(G',*')$.

DÉMONSTRATION .

1) $\{e'\}$ est un sous-groupe du groupe $(G',*')$. D'après le théorème 16, $\mathrm{Ker}(f) = f^{-1}(\{e'\})$ est un sous-groupe du groupe $(G,*)$.

1) G est un sous-groupe du groupe $(G,*)$. D'après le théorème 16, $\mathrm{Im}(f) = f(G)$ est un sous-groupe du groupe $(G',*')$.

❑

Théorème 19. Soient $(G,*)$, $(G',*')$ deux groupes. Soit f un morphisme du groupe $(G,*)$ vers le groupe $(G',*')$. Alors,

1) f est injectif $\Leftrightarrow \mathrm{Ker}(f) = \{e\}$.

2) f est surjectif $\Leftrightarrow \mathrm{Im}(f) = G'$.

3) f est un isomorphisme $\Leftrightarrow \mathrm{Ker}(f) = \{e\}$ et $\mathrm{Im}(f) = G'$.

DÉMONSTRATION .

• Puisque f est un morphisme de groupes, on sait que $f(e) = e'$. Supposons f injectif. Soit $x \in G$.

$$x \in \mathrm{Ker}(f) \Leftrightarrow f(x) = e' \Leftrightarrow f(x) = f(e) \Leftrightarrow x = e \text{ (car } f \text{ est injectif).}$$

• Supposons $\mathrm{Ker}(f) = \{e\}$. Soit $(x_1, x_2) \in G^2$.

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow f(x_1) * (f(x_2))^{-1} = e' \\ &\Rightarrow f\left(x_1 * x_2^{-1}\right) = e' \text{ (d'après le théorème 15)} \\ &\Rightarrow x_1 * x_2^{-1} \in \mathrm{Ker}(f) \Rightarrow x_1 * x_2^{-1} = e \\ &\Rightarrow x_1 = x_2. \end{aligned}$$

Donc, f est injectif.

2) est immédiat et 3) est une conséquence de 1) et 2).

❑

3 Anneaux et corps

3.1 Définition

DÉFINITION 16. Soit A un ensemble non vide ayant au moins deux éléments muni de deux lois de composition interne (notées $+$ et $*$).

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

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

Exemples fondamentaux d'anneaux commutatifs : $(\mathbb{Z},+,\times)$, $(\mathbb{D},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ (les démonstrations de ces résultats sont longues, fastidieuses et simples et nous les reproduirons pas ici).

On rencontrera d'autres exemples d'anneaux par la suite et en particulier, dès le chapitre suivant (« Matrices »), on rencontrera un exemple d'anneau non commutatif.

Un exemple très particulier d'anneau est l'anneau nul. Il ne contient qu'un élément : $A=\{0_A\}$ et les deux opérations $+$ et $*$ sont très simples. Leurs définitions respectives tient en 2 égalités à savoir $0_A+0_A=0_A$ et $0_A*0_A=0_A$. Dans ce cas, l'élément neutre pour l'addition et l'élément neutre pour la multiplication sont un seul et même élément ($1_A=0_A$). On verra plus loin que si l'anneau contient au moins deux éléments, ces éléments neutres sont nécessairement distincts.

3.2 Calculs dans un anneau

Théorème 20. 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, $x*0_A=0_A$. ❑

Supposons maintenant que l'élément neutre 0_A pour l'addition et l'élément neutre 1_A pour la multiplication soit un seul et même élément. Alors, pour tout élément x de l'anneau :

$$x=x*1_A=x*0_A=0_A.$$

Dans ce cas, $A=\{0_A\}$ ne contient qu'un élément. Par contraposition, si A contient au moins deux éléments, alors $1_A\neq 0_A$.

Théorème 21. 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 $a*(-b)=-a*b$. ❑

⇨ **Commentaire.** *Le théorème 21 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 22. Soit $(A,+,*)$ un anneau. Soient a et b deux éléments de A. **Si a et b commutent**,

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

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

(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 $a \times b \times b \times \ldots \times a \times b$ sous la forme $a^p b^q$.

❑

3.3 Groupe des inversibles d'un anneau

Dans ce paragraphe, la deuxième loi de l'anneau est notée $\times$ au lieu de $*$, l'élément neutre pour la deuxième loi est notée 1_A et le symétrique éventuel d'un élément x pour la deuxième loi est noté x^{-1}, tout ceci pour faciliter la lecture. De plus, les anneaux considérés contiennent au moins deux éléments de sorte que $1_A \neq 0_A$.

Théorème 22. Soit $(A, +, \times)$ un anneau non nul. 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, $A^* \neq \varnothing$.
• 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 $\left(x^{-1}\right)^{-1} = x$. Donc, tout élément de A^* admet un symétrique pour $\times$ **dans** A^*.

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

❑

⇨ **Commentaire** .

◇ *Le résultat du théorème 22 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 $\circ$.*

◇ *Les inversibles de l'anneau $(\mathbb{Z}, +, \times)$ sont 1 et -1 et de fait $(\{-1, 1\}, \times)$ est un groupe : c'est le sous-groupe U_2 de $(\mathbb{C}^*, \times)$.*

◇ *Pour $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, la notation A^* coïncide avec la notation du lycée : $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ et $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Mais pas pour $\mathbb{Z}$: $\mathbb{Z}^* = \{-1, 1\}$.*

3.4 Anneaux intègres

Définition 17. Soit $(A, +, \times)$ un anneau commutatif.

$(A, +, \times)$ est **intègre** si et seulement si $\forall (a, b) \in A^2$, $(ab = 0_A \Leftrightarrow a = 0_A$ ou $b = 0_A)$.

(Un anneau intègre est un anneau dans lequel la phrase « un produit de facteurs est nul si et seulement si l'un de ses facteurs est nul » est vraie).

Par exemple, l'anneau $(\mathbb{Z}, +, \times)$ est un anneau intègre. En effet, si a et b sont deux entiers relatifs non nuls, alors $|ab| = |a||b| \geqslant 1 \times 1 = 1$ et en particulier, $ab \neq 0$. Par contraposition, si $ab = 0$, alors $a = 0$ ou $b = 0$.

Des éléments a et b tels que $a \neq 0_A$, $b \neq 0_A$ et $ab = 0_A$ sont appelés **diviseurs de zéros**. Nous rencontrerons dans le chapitre suivant le premier exemple d'anneau dans lequel il y a des diviseurs de zéro : l'anneau des matrices carrées.

3.5 Sous-anneaux

Définition 18. Soit $(A, +, *)$ un anneau et B une partie non vide de A.

B est un sous-anneau de l'anneau $(A, +, *)$ si et seulement si B contient 1_A (et en particulier est non vide), est stable pour les deux lois et, muni des lois induites, est un anneau.

En particulier, $(B, +)$ est un sous-groupe du groupe $(A, +)$ et on a immédiatement la caractérisation suivante des sous-anneaux :

Théorème 23. Soit $(A,+,\times)$ un anneau puis B une partie de A.

B est un sous-anneau de l'anneau $(A,+,*)$ si et seulement si $\begin{cases} 1)\ 1_A \in B \\ 2)\ \forall (x,y)\in B^2,\ x-y\in B \\ 3)\ \forall (x,y)\in B^2,\ x*y\in B \\ 4)\ *\text{ admet un élément neutre dans } B \end{cases}$.

Dans le cadre du programme de classe préparatoire, la notion de sous-anneau est très pauvre. Par exemple, un sous-anneau de l'anneau $(\mathbb{Z},+,\times)$ doit contenir 1 et 0, puis pour tout $n\in\mathbb{N}^*$, doit contenir $\underbrace{1+\ldots+1}_{n \text{ termes}}=n$ et donc tous les entiers naturels et enfin doit contenir tous les opposés de ces entiers. Finalement, un tel sous-anneau ne peut être que $\mathbb{Z}$ lui-même.

3.6 Morphismes d'anneaux

Définition 19. Soient $(A,+,*)$ et $(A',+',*')$ deux anneaux. Soit f une application de A vers A'.

f est un **morphisme d'anneaux** si et seulement si $\begin{cases} \forall (x,y)\in A^2,\ f(x+y)=f(x)+'f(y) \\ \forall (x,y)\in A^2,\ f(x*y)=f(x)*'f(y) \\ f(1_A)=1_{A'} \end{cases}$.

Un **isomorphisme d'anneaux** est un morphisme d'anneaux qui de plus, est bijectif.

Par exemple, soit $f : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array}$. On sait que pour tout $(z,z')\in\mathbb{C}^2$, $f(z+z')=\overline{z+z'}=\overline{z}+\overline{z'}=f(z)+f(z')$, $f(z\times z')=\overline{z\times z'}=\overline{z}\times\overline{z'}=f(z)\times f(z')$ et enfin $f(1)=\overline{1}=1$. Donc, f est un morphisme d'anneaux. C'est même un isomorphisme d'anneaux car f est involutive ($\forall z\in\mathbb{C}$, $f(f(z))=z$) et en particulier bijective.

3.7 Corps

Définition 20. 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 23. Un corps est en particulier un anneau intègre ou encore, dans un corps, un produit de facteurs est nul si et seulement si l'un de ces facteurs est nuls.

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

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

❑

La réciproque de l'implication du théorème 23 est fausse. L'anneau $(\mathbb{Z},+,\times)$ constitue un exemple d'anneau intègre qui n'est pas un corps.