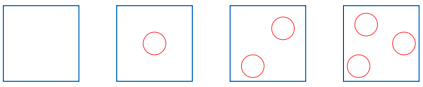
Structures algébriques

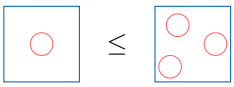
L'enfant, après avoir appris

— à **compter** le nombre d'objets en ajoutant des unités à partir de 0 c'est à dire en construisant l'ensemble $\mathbb{N}$ avec l'opération "suivant"



Désignation à l'aide d'un nombre de la quantité de cercles

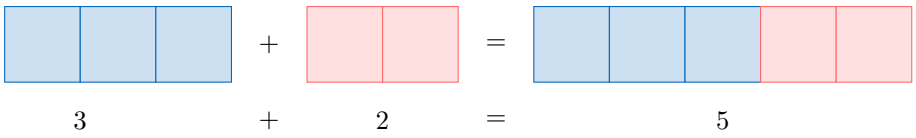
— à **ordonner** en comparant des quantités c'est à munir d'une structure d'ordre à l'ensemble $\mathbb{N}$



Comparaison de deux quantités de cercles

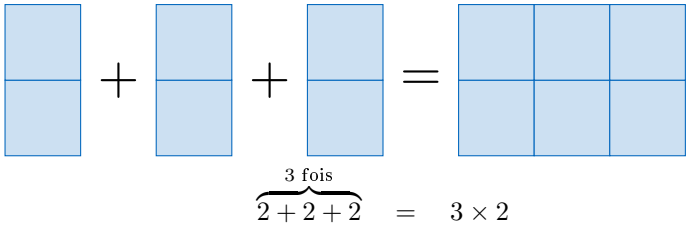
commence

— à **additionner** les nombres en opérant des regroupements.



Regroupement de cubes pour additionner

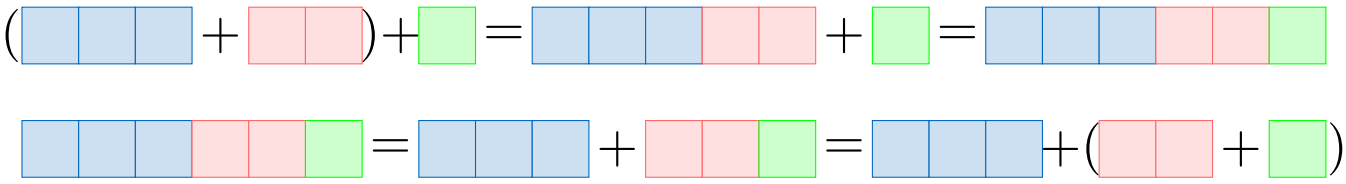
— à **multiplier** les nombres en opérant une addition itérée.



Regroupement itéré de cubes pour multiplier

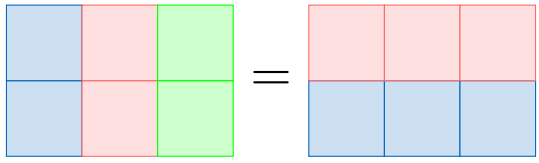
puis s'intéresse aux propriétés des opérations :

— **associativité** de l'addition $(a+b)+c = a+(b+c)$ et de la multiplication $(a \times b) \times c = a \times (b \times c)$



Démonstration géométrique élémentaire de l'associativité de l'addition

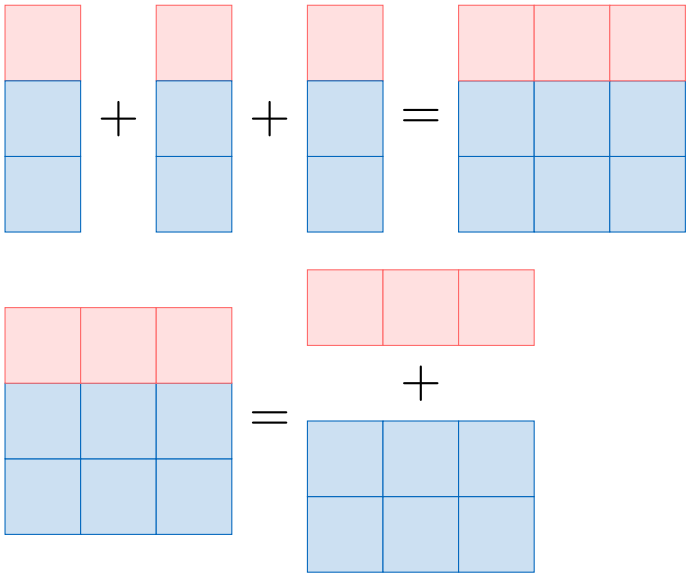
— **commutativité** de l'addition $a+b = b+a$ et de la multiplication $a \times b = b \times a$



$\overbrace{a}^{\text{Nombre de colonnes}} \times \overbrace{b}^{\text{Nombre de cubes par colonne}} = \overbrace{b}^{\text{Nombre de lignes}} \times \overbrace{a}^{\text{Nombre de cubes par ligne}}$

Démonstration géométrique élémentaire de la commutativité de la multiplication

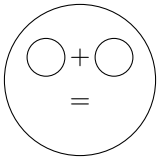
— **distributivité** de la multiplication sur l'addition $a \times (b+c) = (a \times b) + (a \times c)$



Démonstration géométrique élémentaire de la distributivité

$$\overbrace{(b+c)+\cdots+(b+c)}^{a \text{ fois}} = \overbrace{(b+\cdots+b)}^{a \text{ fois}} + \overbrace{(c+\cdots+c)}^{a \text{ fois}}$$

ensuite après avoir défini 0 comme l'**élément neutre** de l'addition (additionner 0 à un nombre donne ce même nombre)



Cas particulier bien connu 0+0=0

on construit l'ensemble des entiers relatifs à partir de l'**opposé** d'un entier naturel :

$$\begin{aligned} 2+(2-4) &= (2+2)-4 = 0 \\ 2+(1-3) &= (2+1)-3 = 0 \\ 2+(0-2) &= (2+0)-2 = 0 \end{aligned}$$

Ainsi "en supprimant le zéro",

$$2+(-2)=0.$$

le nombre négatif -2 "naît".
Dans le supérieur, nous rencontrons de nombreux ensembles : les entiers naturels, les entiers relatifs, les fractions, les réels, les complexes, les polynômes, les vecteurs, les matrices, les fonctions continues etc. L'objectif de ce cours est de suivre le cheminement de l'enfant en généralisant à un ensemble A quelconque et non plus l'ensemble des entiers.
Structurer un ensemble A avec une relation d'ordre $\leq$ pour définir un ensemble ordonné $(A \leq)$ sera faite dans un autre cours. Comme un enfant aimant additionner et multiplier, un Mathématicien souhaite structurer un ensemble avec des opérations appelées **lois de composition** qu'il appelle une **structure algébrique**. L'addition et la multiplication obéissent à plusieurs propriétés algébriques : l'associativité et la commutativité. De nombreuses structures algébriques étudiées obéissent à certaines, mais pas nécessairement à toutes, de ces lois.
0 est un élément particulier de l'addition appelé l'**élément neutre** c'est à dire il laissent tous les autres éléments inchangés lorsqu'il est composé avec eux. On se posera la question d'existence et d'unicité de l'élément neutre. La notion d'**élément symétrique** généralise le concept d'opposé en rapport avec l'addition.
Enfin, on étudiera une première structure algébrique appelé **groupe**.

I Loi de composition

A Définition

Définition Loi de composition interne

Soit A un ensemble.
Une **loi de composition interne**, $\triangle$, est une application qui, à deux éléments de A, associe un élément de A :

$$\triangle \left| \begin{array}{ccc} A \times A & \longrightarrow & A \\ (x,y) & \longmapsto & x \triangle y \end{array} \right. .$$

Exemple

- Sur $\mathbb{R}$, l'addition définie par $+ \left| \begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x+y \end{array} \right.$, la soustraction $- \left| \begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x-y \end{array} \right.$ et la multiplication $- \left| \begin{array}{ccc} \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,y) & \longmapsto & x \times y \end{array} \right.$ sont des lois de composition internes.
- Sur $\mathbb{N}$, la soustraction n'est pas une loi interne, mais elle l'est dans $\mathbb{Z}$.
- Sur $\mathbb{N}^*$, l'exponentiation définie par $\left| \begin{array}{ccc} \mathbb{N}^* \times \mathbb{N}^* & \longrightarrow & \mathbb{N}^* \\ (a,b) & \longmapsto & a^b \end{array} \right.$, le PGCD ou le PPCM sont des lois internes.
- Soit X un ensemble. Sur l'ensemble des parties de X, $\mathcal{P}(X)$, l'union définie par $\cup \left| \begin{array}{ccc} \mathcal{P}(X) \times \mathcal{P}(X) & \longrightarrow & \mathcal{P}(X) \\ (A,B) & \longmapsto & A \cup B \end{array} \right.$ et l'intersection $\cap \left| \begin{array}{ccc} \mathcal{P}(X) \times \mathcal{P}(X) & \longrightarrow & \mathcal{P}(X) \\ (A,B) & \longmapsto & A \cap B \end{array} \right.$ sont des lois de composition internes.

Définition Loi de composition externe

Soit X et A deux ensembles.
Une **loi de composition externe**, ., est une application qui, à un élément de X et un élément de A, associe un élément de A :

$$. \left| \begin{array}{ccc} X \times A & \longrightarrow & A \\ (\lambda, x) & \longmapsto & \lambda.x \end{array} \right.$$

Exemple : $(\mathbb{R}^2, .)$

La multiplication par un scalaire sur l'ensemble des vecteurs du plan $\mathbb{R}^2$ définie par

$$. \left| \begin{array}{ccc} \mathbb{R} \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (\lambda, (x_1, x_2)) & \longmapsto & (\lambda.x_1, \lambda.x_2) \end{array} \right. .$$

est une loi de composition externe.

B Propriétés éventuelles des lois de composition interne

Définition Commutativité et associativité

$\triangle$ est

1. **associative** : si $\in (x,y,z) \in A^3$, $x \triangle (y \triangle z) = (x \triangle y) \triangle z$. On ne considèrera que des loi associatives.
2. **commutative** : si $\forall (x,y) \in A^2$, $x \triangle y = y \triangle x$.

Exemple

— Sur $\mathbb{R}$, l'addition et la multiplication sont commutatives et associatives. Ce n'est pas le cas de la soustraction car $1-0 \neq 0-1$ et $1-(2-3)=2 \neq -4=(1-2)-3$.

— Sur $\mathbb{N}^*$, l'exponentiation n'est pas commutative $1^2=1 \neq 2=2^1$ et non plus associative $\left(2^2\right)^3=64 \neq$

$256 = 2^{(2^3)}$.

— Sur $\mathcal{P}(X)$, l'union et l'intersection sont commutatives et associatives.

Remarque

Quand la loi est associative, la **notation itérée** est

— en cas d'une loi de multiplication : $\forall a \in A, \forall n \in \mathbb{N}^* : x^n = \overbrace{x \times \cdots \times x}^{\text{n fois}}$

— en cas d'une loi d'addition : $\forall a \in A, \forall n \in \mathbb{N}^* : nx = \overbrace{x + \cdots + x}^{\text{n fois}}$.

Définition **Distributivité d'une loi sur une autre**

Soit A un ensemble et $\triangle$ et $\square$ deux lois de composition internes sur A.
On dit que $\triangle$ est **distributive** sur $\square$ si :

$$\forall x, y, z \in A : \quad x \triangle (y \square z) = (x \triangle y) \square (x \triangle z) \text{ et } (y \square z) \triangle x = (y \triangle x) \square (z \triangle x).$$

Exemple

— Sur $\mathbb{R}$, la multiplication est distributive sur l'addition mais l'addition n'est pas distributive sur la multiplication car $1 + (2 \times 3) = 7 \neq 5 = 1 \times 2 + 1 \times 3$.

— Sur $\mathcal{P}(X)$, l'union et l'intersection sont distributives l'une par rapport à l'autre.

C Élément neutre et symétrique

Définition **Elément neutre**

$\triangle$ admet **un élément neutre** si il existe $e \in A$ tel que $\forall x \in A$, $x \triangle e = e \triangle x = x$.

Proposition **Unicité de l'élément neutre**

Si $\triangle$ admet un élément neutre, alors celui-ci est unique.

Démonstration

Supposons qu'il existe deux éléments neutres e et e'.
On a $e \triangle e' \overset{e \text{ elt neutre}}{=} e'$ et $e \triangle e' \overset{e' \text{ elt neutre}}{=} e$. Ainsi $e = e'$.

Exemple

— Sur $\mathbb{R}$, 1 est l'élément neutre de la multiplication et 0 de l'addition.

— Sur $\mathcal{P}(X)$, l'ensemble vide $\emptyset$ est l'élément neutre de l'union et X de l'intersection.

Définition **Élément symétrique et loi symétrique**

Soit $x \in A$ et la loi $\triangle$ admettant un élément neutre e .
x admet un **symétrique** pour $\triangle$ si il existe $x' \in A$ tel que $x \triangle x' = x' \triangle x = e$. Dans ce cas, x' est appelé le **symétrique** de x.

Proposition **Unicité de l'élément symétrique**

Soit $\triangle$ une loi associative et admettant un élément neutre e.
Si x admet un symétrique x', alors celui-ci est unique.

Démonstration

Supposons qu'il existe deux éléments symétriques x' et x''.

On a $(x' \triangle x) \triangle x'' = e \triangle x'' = x''$ et $(x' \triangle x) \triangle x'' \overset{\triangle \text{ associative}}{=} x' \triangle (x \triangle x'') = x' \triangle e = x'$. Ainsi $x' = x''$.

Vocabulaire

Le symétrique est appelé :

— **opposé** en cas d'une loi additive $+$

— **inverse** en cas d'une loi multiplicative $\times$

Exemple

Sur $\mathbb{R}$, l'inverse de la multiplication d'un réel non nul x est $\frac{1}{x}$ et l'opposé de l'addition d'un réel x est $-x$.

Définition **Loi symétrique**

La loi $\triangle$ est **symétrique** si la loi est associative et si tout élément de A admet un symétrique.

Exemple

Sur $\mathbb{R}$, la multiplication n'est pas inversible car 0 n'a pas d'inverse. En revanche sur $\mathbb{R}^*$, la multiplication est inversible.

D Parties stables

Définition **Partie stable**

Soit B une partie non vide de A.

B est **stable** pour $\triangle$ si

$$\forall x, y \in B : \quad x \triangle y \in B.$$

Exemple

— Sur $\mathbb{R}$, les ensembles $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ et les nombres pairs sont stables pour l'addition.

— Sur $\mathbb{C}$, l'ensemble $\mathcal{U}$ des nombres complexes de module 1 est stable pour la multiplication car le produit de deux nombres complexes de module 1 est un nombre complexe de module 1.

Définition **Loi induite**

Soit $\triangle$ une loi sur A et B une partie de A stable pour $\triangle$.

La **loi induite** $\tilde{\triangle}$ est définie par :

$$\tilde{\triangle} \left| \begin{array}{ccc} B \times B & \longrightarrow & B \\ (x, y) & \longmapsto & x \triangle y \end{array} \right. .$$

Pour alléger les notations, on identifie $\tilde{\triangle}$ à $\triangle$.

Exemple

On munit l'ensemble $\mathcal{U}$ des nombres complexes de module 1 avec la loi induite $*$ sur $\mathbb{C}$.

II Groupes

A Définition

Définition Groupe

Un **groupe** est un couple $(G, *)$ où G est un ensemble et $*$ une loi de composition interne sur G associative, admettant un neutre et pour laquelle tout élément de G admet un symétrique pour la loi $*$. Un groupe est dit **abélien** ou **commutatif** si la loi $*$ est de plus commutative.

Proposition Groupes de référence

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

Démonstration

Les hypothèses à vérifier ont été énoncées dans la section précédente.

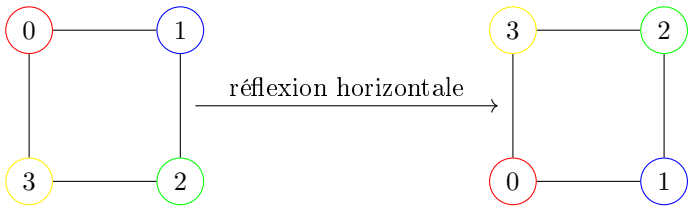
Exemple

Une symétrie transforme une figure du plan en elle-même. Pour le carré, l'ensemble des symétrie est congruente à elle-même. Cependant, certaines figures sont congruentes à elles-mêmes de plus d'une manière, et ces congruences supplémentaires sont appelées symétries. Un carré a huit symétries

— l'application identité, laissant tout inchangé,

— les rotations de 90° , 180° et 270° vers la droite de Le centre le point d'intersection des diagonales du carré,

— les réflexions ayant pour axes les médiatrices des côtés du carré ou ses diagonales .



Les sommets du carré sont identifiés par une couleur et une nombre.

Les éléments du groupe de symétrie du carré (D4). Groupe D8 id.svg id (en le gardant tel quel) Groupe D8 90.svg r1 (rotation de 90 ° dans le sens des aiguilles d'une montre) Groupe D8 180.svg r2 (rotation de 180 °) Groupe D8 270.svg r3 (rotation de 270 ° dans le sens des aiguilles d'une montre) Groupe D8 fv.svg fv (réflexion verticale) Groupe D8 fh.svg fh (réflexion horizontale) Groupe D8 f13.svg fd (réflexion diagonale) Groupe D8 f24.svg fc (réflexion contre-diagonale) l'opération d'identité laissant tout inchangé, notée id ; des rotations du carré autour de son centre de 90 °, 180 ° et 270 ° dans le sens des aiguilles d'une montre, désignées respectivement par r1, r2 et r3 ; réflexions sur la ligne médiane horizontale et verticale (fv et fh), ou à travers les deux diagonales (fd et fc). Ces symétries sont des fonctions. Chacun envoie un point dans le carré au point correspondant sous la symétrie. Par exemple, r1 envoie un point à sa rotation de 90 ° dans le sens des aiguilles d'une montre autour du centre du carré, et fh envoie un point à sa réflexion sur la ligne médiane verticale du carré. La composition de deux de ces symétries donne une autre symétrie. Ces symétries déterminent un groupe appelé groupe dièdre de degré 4, noté D4. L'ensemble sous-jacent du groupe est l'ensemble de symétries ci-dessus, et l'opération de groupe est la composition de fonctions. [9] Deux symétries sont combinées en les composant comme des fonctions, c'est-à-dire en appliquant la première au carré et la seconde au résultat de la première application. Le résultat de l'exécution de a, puis de b est écrit symboliquement de droite à gauche comme displaystyle b circ a displaystyle b circ a ("appliquer la symétrie b après avoir effectué la symétrie a"). (C'est la notation habituelle pour la composition des fonctions.)

Remarque

Lors de l'introduction d'un groupe $(G, *)$, on omet de mentionner la loi $*$ afin d'alléger les notations.
L'ensemble G ne peut pas être vide car il contient au moins l'élément neutre.

B Sous-groupes

Définition Sous-Groupe

Soit $(G, *)$ un groupe et H une partie de G.
$(H, *)$ est un **sous-groupe** de $(G, *)$ si H est stable pour $*$ et, muni de la loi induite, est un groupe.