Espaces Vectoriels connus : · $V_2$, $V_3$
· $\mathbb{R}[X]$
· fonctions réelles

# I. Les groupes

Dans ce module d'algèbre linéaire, nous étudierons donc des phénomènes linéaires : espaces et sous-espaces vectoriels, applications linéaires, systèmes d'équations linéaires, etc. L'année passée, vous avez développé des techniques d'algèbre linéaire pour résoudre des questions géométriques dans le plan ou l'espace euclidien réel, $\mathbb{R}^2$ et $\mathbb{R}^3$. Vous avez aussi vu d'autres espaces vectoriels où ces méthodes s'appliquent : les polynômes à coefficients réels, les fonctions réelles d'une variable réelle. Au début de ce module, nous commencerons par parler de cette structure de corps dont les nombres réels sont munis. Il y a d'autres corps dans la nature, certains que nous connaissons depuis longtemps comme les nombres rationnels ou les nombres complexes, et d'autres que vous n'avez peut-être encore jamais vus !

Corps connus : $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ pas d'inverse pour ·

$\mathbb{N}$ et $\mathbb{Z}$ ne sont pas des corps
↳ pas d'opposé pour +

## 1 Lois de composition

Lorsque l'on a deux nombres réels en main, on peut les additionner ou les multiplier. Ces deux opérations, l'addition et la multiplication, sont des lois de composition.

**Définition 1.1.** Une *loi de composition* sur un ensemble $E$ est une application $E \times E \to E$.
Il s'agit donc une opération *interne* à $E$ ou *stable* *dans* $E$ qui fait correspondre à un couple $(x, y)$ d'éléments de $E$ un troisième élément que l'on notera souvent $x * y$.

Dans des situations particulières, on remplace la notation $x * y$ par une notation plus classique, ce que nous ferons déjà dans les exemples suivants.

**Exemple 1.2.**

a) L'addition $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ est une loi de composition notée $n + m$. La multiplication complexe $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ est une loi de composition notée $z \cdot z'$.

b) Il y a aussi des lois de composition d'une tout autre nature.
Soit $X$ un ensemble et posons $E = \mathcal{P}(X)$. Alors la réunion et l'intersection définissent des lois de composition sur $E$. La première fait correspondre à deux sous-ensembles $A, B \subset X$ leur réunion $A \cup B$ et la seconde leur fait correspondre leur intersection $A \cap B$.

c) Dans $\mathbb{N}$, la différence n'est pas une loi de composition interne car par exemple $1-2 \notin \mathbb{N}$. Par contre, c'en est une sur $\mathbb{Z}$.

Nous nous intéressons uniquement à certaines lois de composition, celles qui satisfont des propriétés de "symétrie". L'associativité permet de se passer des parenthèses :

**Définition 1.3.** Une loi de composition $*$ sur un ensemble $E$ est *associative* si

$$a * (b * c) = (a * b) * c \quad , \quad \forall\, a, b, c \in E$$

On note alors $a * b * c$ pour ce résultat.

**Exemple 1.4.**

a) L'addition $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ est une loi de composition associative puisque $a + (b + c) = (a + b) + c$ pour tous nombres réels $a, b$ et $c$.

b) La soustraction ne l'est pas : par exemple

$$1 - (2 - 3) = 1 - (-1) = 2 \neq (1 - 2) - 3 = -1 - 3 = -4$$

c) L'intersection est associative sur $\mathcal{P}(X)$. En effet, un élément appartient à $A \cap (B \cap C)$ si et seulement si il appartient à la fois à $A$ et à $B \cap C$, c'est-à-dire à $A$, $B$ et $C$, ou encore à $A \cap B$ et à $C$. Ainsi $A \cap (B \cap C) = (A \cap B) \cap C$.

**Proposition 1.5.** *Si $*$ est une loi de composition associative sur $E$, alors*

$$\big((x * y) * (z * t)\big) = x * \big((y * z) * t\big) \qquad (a)$$

*pour tous $x, y, z, t \in E$.*

*Démonstration.* On utilise l'associativité avec $x$, $y$, $w = z * t$ (d)

Ainsi, $(x * y) * (z * t) \overset{(d)}{=} (x * y) * w \overset{(a)}{=} x * (y * w)$
$\overset{(d)}{=} x * (y * (z * t))$
$\overset{(a)}{=} x * ((y * z) * t)$

⚠ l'ordre des éléments $x, y, z, t$ est toujours le même !

□

De manière générale, on peut se passer du parenthésage lors de la composition de $n$ éléments pour tout $n \geq 3$. Une autre propriété essentielle qui nous permet de travailler simplement avec l'addition est l'existence du zéro, ou celle de 1 pour la multiplication.

**Définition 1.6.** Une loi de composition $*$ sur un ensemble $E$ admet un *élément neutre* s'il existe $e \in E$ tel que $e * x = x = x * e$ pour tout $x \in E$.

**Exemple 1.7.**

Pour la multiplication complexe, l'élément neutre est $1 (= 1 + 0i)$

car $1 \cdot z = z = z \cdot 1 \quad \forall z \in \mathbb{C}$.

Pour la réunion dans $\mathcal{P}(X)$, l'élément neutre est $\emptyset$ car

$A \cup \emptyset = A = \emptyset \cup A, \quad \forall A \subset X$.

Pour l'intersection dans $\mathcal{P}(X)$, l'élément neutre est $X$ car

$A \cap X = A = X \cap A, \quad \forall A \subset X$.

Pour la soustraction dans $\mathbb{Z}$, il n'y a pas d'élément neutre !

Candidat : $e = 0$ qui ne fonctionne qu'à droite :

$X - 0 = X$ mais $0 - x = -x \neq x$ si $x \neq 0$ ...

Toute loi de composition admet au plus un élément neutre. La preuve utilise un principe de comparaison bien utile.

**Proposition 1.8.** *Si $e$ et $e'$ sont des éléments neutres pour une loi de composition $*$ sur $E$, alors*

$$e = e'.$$

*Démonstration.*

$e$ élément neutre $\Rightarrow e * e' = e'$

$e'$ élément neutre $\Rightarrow e * e' = e$

$\Rightarrow e * e' = e' = e$

□

Le rôle de l'unité dans la multiplication est plus important dans $\mathbb{Q}$ que dans $\mathbb{Z}$ :

dans $\mathbb{Q}$, on peut "inverser" tous les éléments non nuls : si $r = \frac{a}{b}$ et $a \neq 0$, alors $s = \frac{b}{a}$ est l'inverse de $r$ dans le sens où $r \cdot s = 1$.

**Définition 1.9.** Soit $*$ une loi de composition sur un ensemble $E$ qui admet un élément neutre $e$. Un élément $x \in E$ est *inversible à gauche* (respectivement à droite) s'il existe un élément $y \in E$ tel que $y * x = e$ (respectivement $x * y = e$).

**Exemple 1.10.** Quel est l'inverse (à gauche et à droite) de $A \subset X$ pour la réunion dans $\mathcal{P}(X)$ ?

On cherche $B$ t.q. $A \cup B = \emptyset = e_\cup$ ou $C$ t.q $C \cup A = \emptyset$

⚠ $B$ et $C$ n'existent pas si $A \neq \emptyset$.

**Théorème 1.11.** *Soit $*$ une loi de composition associative sur un ensemble $E$ admettant un élément neutre. Si un élément $x$ admet un inverse à gauche $y$ et un inverse à droite $z$, alors $y = z$. On appelle cet élément l'inverse de $x$ et on le note $x^{-1}$. L'inverse de $x$, s'il existe, est unique.*

*Démonstration.* Si $y * x = e = x * z$, on utilise l'astuce suivante :

$z = e * z = (y * x) * z \overset{\text{assoc.}}{=} y * (x * z) = y * e = y$

Et si $x$ admet deux inverses, par le même procédé, on démontre qu'ils sont égaux !

□

Pour terminer cette première partie concernant les lois de composition, nous nous intéressons à une dernière propriété, celle de l'importance de l'ordre.

**Définition 1.12.** Une loi de composition $*$ sur un ensemble $E$ est *commutative* si $x * y = y * x$ pour tous $x, y \in E$. Dans ce cas, on dit que les éléments $x$ et $y$ commutent entre eux.

La vie n'est en général pas commutative. S'habiller le matin puis se rendre à l'école ne fait pas le même effet que se rendre à l'école puis s'habiller ...
Par contre, dans un ensemble $E$ muni d'une loi de composition associative et commutative, ni l'ordre, ni le parenthésage n'importent.

**Exemple 1.13.**
L'addition est commutative dans $\mathbb{R}$, donc $a + b = b + a$ pour tous nombres réels $a$ et $b$.

## 2 Les groupes

Nous continuons en établissant une hiérarchie parmi les ensembles munis d'une, puis, la semaine suivante, de deux lois de composition.

notation → $G = (E ; *)$

**Définition 2.1.** Un *groupe* est un ensemble $E$ muni d'une loi de composition associative, qui admet un élément neutre et pour laquelle tout élément est inversible. Un groupe est dit *commutatif* ou *abélien* si la loi de composition est commutative.

**Remarque 2.2. Un peu d'histoire.** Le terme de groupe abélien honore le mathématicien norvégien Niels Henrik Abel (1802 - 1829), célèbre pour ses travaux sur l'impossibilité de résoudre les équations du cinquième degré par radicaux, mais aussi pour être mort à l'âge de 26 ans de la tuberculose.

**Exemple 2.3.** $G = (\mathbb{R} ; +)$

a) Les nombres réels munis de l'addition forment un groupe abélien. Nous avons déjà vu un peu plus tôt que l'addition est associative et commutative et que zéro est l'élément neutre.
Pour l'addition, l'inverse de $x \in \mathbb{R}$ est en fait *l'opposé* $-x$ puisque $x + (-x) = 0$.

b) Les nombres rationnels non-nuls $\mathbb{Q}^*$ munis de la multiplication usuelle $(\mathbb{Q}^* ; \cdot)$ est un groupe abélien.

Par contre, $(\mathbb{Q} ; \cdot)$ n'est pas un groupe car 0 n'est pas inversible.

**Exemple 2.4.** Considérons l'ensemble $E = \{0, 1, 2\}$ et définissons une loi de composition, appelée addition et notée $+$, en précisant sa table (on lit $a + b$ dans la ligne de $a$ et la colonne de $b$) :

| $+$ | $b$ 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| $a$ 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

On voit que cette loi de composition est commutative car la table admet la diagonale descendante comme axe de symétrie.

L'élément neutre est 0 car la ligne des entrées = la ligne "0" et la colonne des entrées = la colonne "0"

Tous les éléments sont inversibles car "0" apparait exactement une fois dans chaque ligne et dans chaque colonne.

Associativité : On doit montrer que $(x+y)+z = x+(y+z)$ pour chacun des 27 triplets $(x, y, z)$ possibles !

- Si $x = 0$, il vient $(0+y)+z = y+z = 0+(y+z)$
- Idem $y = 0$ ou si $z = 0$
- Si $x = y = z \neq 0$ : $(1+1)+1 = 2+1 \overset{\text{commut.}}{=} 1+2 = 1+(1+1)$
  Idem avec $x = y = z = 2$.
- $1+(1+2) = 1+0 = 1 = 2+2 = (1+1)+2$
- $2+(2+1) = 2+0 = 2 = 1+1 = (2+2)+1$
- Les autres cas s'obtiennent par commutativité.

On appelle ce groupe abélien $\mathbb{Z}/3\mathbb{Z}$. L'addition dans $\mathbb{Z}/3\mathbb{Z}$ est une addition modulo 3 dans $\mathbb{Z}$.

**Définition 2.5.** Soit $(G, *)$ un groupe. Un sous-ensemble $H \subset G$ est un *sous-groupe* si la loi de composition de $G$ définit une loi de composition sur $H$ qui en fait un groupe.

**Théorème 2.6.** *Soit $(G, *)$ un groupe. Alors un sous-ensemble non-vide $H \subset G$ est un sous-groupe si et seulement si $x * y$ et $y^{-1}$ appartiennent à $H$ pour tous $x, y \in H$.*

*Démonstration.* Si $H$ est un sous-groupe de $G$, la condition est vraie car $*$ est une loi de composition sur $H$ pour laquelle tout élément de $H$ admet un inverse (dans $H$).
Supposons maintenant que les deux conditions sont vérifiées. Alors $*$ est une loi de composition sur $H$ puisque $\forall\, x, y \in H$ , $x * y \in H$ par hypothèse

Elle est associative car elle l'est dans $G$

Comme $H$ est non-vide, on peut choisir un élément $x \in H$. Alors, par hypothèse $x^{-1} \in H$
et par suite $x * x^{-1} = e$
et tous les éléments sont inversibles dans $H$ par hypothèse.

Ainsi, $H$ est bien un groupe. Il est abélien si $G$ l'est.

□

La possibilité de parler de sous-groupe simplifie parfois considérablement la vérification des axiomes de groupe.

**Exemple 2.7.**

a) L'ensemble des isométries du plan muni de la composition forme un groupe non abélien. En effet, la composition de deux isométries est une isométrie, l'identité est l'élément neutre, la composition est associative, et enfin chaque isométrie admet une isométrie inverse.

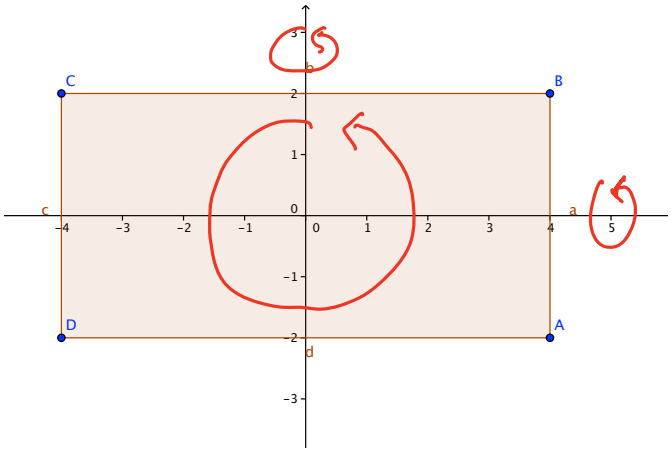
b) L'ensemble des isométries du plan qui fixent l'origine forment un groupe. En effet,
(on renonce aux translations)

$x * y \in H$. La composition de deux isométries qui fixent l'origine, fixe l'origine.

$x \in H \Rightarrow x^{-1} \in H$. L'inverse d'une isométrie qui fixe l'origine, fixe aussi l'origine.

c) L'ensemble des isométries qui fixent globalement un rectangle centré en l'origine forment un groupe, car il s'agit d'un sous-groupe du groupe des isométries qui fixent l'origine. On l'appelle le groupe des isométries du rectangle ou le *groupe du matelas*. Mais quels sont ses éléments ?

Id




Il y a quatre façons de replacer son matelas dans le lit :

- On le laisse tel quel → Id
- On le retourne dans le sens de la longueur ou de la largeur
  → Symétrie d'axe Ox, resp. d'axe Oy
- On le fait tourner, sans le retourner, de sorte à inverser les pieds et la tête → rotation d'angle $\pi$, de centre O.

⇒ Le groupe du matelas contient donc 4 éléments.

**Proposition 2.8.**
*Soit $n \in \mathbb{N}$. L'ensemble $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ muni de l'addition usuelle forme un groupe abélien.*

*Démonstration.* Il suffit de se rendre compte qu'il s'agit d'un sous-groupe de $(\mathbb{Z}, +)$. En effet la somme de $nk$ et $nk'$ est encore un multiple de $n$ et l'opposé de $nk$ est $-nk = n(-k) \in n\mathbb{Z}$. □

Il s'agit en fait des *seuls* sous-groupes de $\mathbb{Z}$.