Structures algébriques
Faisons un peu de rangement

On va essayer de ranger les ensembles en fonctions de leur structure donnée par les lois qui la régisse.

1 Généralités

1.1 Premières définitions

Les structures des ensembles dépendent par les **lois de compositions internes**.

Définition 1 : Lois de composition interne

Soit E un ensemble. On appelle **loi de composition interne sur E**, ou simplement loi sur E, toute application

$$\begin{array}{rccc} \star : & E \times E & \longrightarrow & E \\ & (x,y) & \longmapsto & x \star y \ . \end{array}$$

On note souvent $(E, \star)$ cet ensemble (appelé magma). On dit que :

- la loi $\star$ est **associative** si $\quad \forall x,y,z \in E, \quad (x \star y) \star z = x \star (y \star z)$,
- les éléments $x, y \in E$ commutent (pour $\star$) si $\quad x \star y = y \star x$,
- la loi $\star$ est **commutative** si $\quad \forall x,y \in E, \quad x \star y = y \star x$,
- l'élément $e \in E$ est **neutre** pour la loi $\star$ si $\quad \forall x \in E, \quad e \star x = x \star e = x$,
- le sous ensemble F de E est **stable** pour $\star$ si $\quad \forall x,y \in F, \quad x \star y \in F$.
- l'élément $x \in E$ est **inversible** dans $(E, \star)$ s'il existe $x' \in E$, appelé un inverse de x, tel que $\quad x \star x' = x' \star x = e$.

Soit ∇ une autre loi de composition interne sur E. On dit que $\star$ **est distributive sur** ∇ si

$$\forall x,y,z \in E, \quad x \star (y \nabla z) = (x \star y) \nabla (x \star z) \quad \text{et} \quad (y \nabla z) \star x = (y \star x) \nabla (z \star x) \ .$$

Remarques

- Quand la loi est associative, peu importe la place des place des parenthèses importe peu, du moment que l'on respecte l'ordre des termes.
- Pour tout $x \in E$, on peut définir l'application $\quad \begin{array}{rccc} x \star \cdot : & E & \longrightarrow & E \\ & y & \longmapsto & x \star y \ . \end{array}$
- Pour tous $x, y \in G$, Si x et y sont inversibles, alors x^{-1} et $(x \star y)$ est inversible, et

$$\left(x^{-1}\right)^{-1} = x, \quad (x \star y)^{-1} = y^{-1} \star x^{-1}.$$

Exemple 1

Ensemble E	$\mathbb{Z}$	$\mathbb{N}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{Z}$	$\mathbb{C}$	$\mathbb{R}^{\mathbb{R}}$
Loi	$+$	$+$	$\times$	$\times$	$\times$	$\div$	$\circ$
Neutre	0	0	1	1	1	$\emptyset$	$\mathrm{Id}_{\mathbb{R}}$
Associative	Oui	Oui	Oui	Oui	Oui	Non	Oui
Commutative	Oui	Oui	Oui	Oui	Oui	Non	Non
E stable par la loi	Oui	Oui	Oui	Oui	Oui	Oui	Oui
E stable par inverse	Oui	Non	Oui	Oui	Non	$\emptyset$	Oui, mais n'existe pas toujours

Exemple 2

L'addition et la multiplication sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des lois de composition internes associatives et commutatives.
La soustraction sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ est une loi de composition interne qui **n'est pas** associative.
La division sur $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{R}_+^*$ et $\mathbb{C}^*$ est une loi de composition interne qui **n'est pas** associative.
La division sur $\mathbb{N}^*$ **n'est pas** une loi de composition interne.

Exemple 3

On se rappelle que

- $\times$ est distributive sur $+$ sur $\mathbb{C}$.
- Sur les ensembles que $\cup$ est distributive $\cap$, et inversement.

⚠ Attention Le fait que $a \star b = e$ ne suffit pas à affirmer que $b = a^{-1}$! On se rappelle du contre-exemple pour la composition de 2 fonctions ! A vous !

Définition 2 : Loi de composition externe

Soient E et F deux ensembles. On appelle **loi de composition externe sur E**, toute application

$$\begin{array}{rccc} \bullet : & F \times E & \longrightarrow & E \\ & (x, y) & \longmapsto & x \bullet y \ . \end{array}$$

Exemple 4

Sur $\mathbb{R}^{\mathbb{R}}$, la multiplication par un élément de $\mathbb{R}$

$$\begin{array}{ccc} \mathbb{R} \times \mathbb{R}^{\mathbb{R}} & \to & \mathbb{R}^{\mathbb{R}} \\ (x, f) & \mapsto & x \times f \end{array}$$

est une loi de composition externe sur $\mathbb{R}^{\mathbb{R}}$.

Définition 3 : Structures algébriques

Soit E un ensemble. On dit que E est

- un **groupe** s'il existe une loi de composition interne $\star$ associative tel que
  - ▷ la loi $\star$ admet un élément neutre $e \in E$,
  - ▷ tout élément de E admet un inverse dans E $\quad \forall x \in E,\ \exists y \in E,\ x \star y = y \star x = e$

  Dans ces cas, on le note en général $(E, \star)$. Si la loi $\star$ est commutative, on dit que E est un **groupe commutatif (ou abélien)**.
- un **anneau** s'il existe deux lois de composition interne, $+$ et $\times$, telles que
  - ▷ $(E, +)$ est un groupe commutatif dont l'élément neutre est traditionnellement noté 0_E ou 0,
  - ▷ la loi $\times$ est associative,
  - ▷ la loi $\times$ admet un élément neutre 1_A ou 1,
  - ▷ la loi $\times$ est distributive par rapport à l'addition $+$.

  Dans ces cas, on le note en général $(E, +, \times)$.
  Si $(A, \times)$ est commutatif, on dit que $(E, +, \times)$ est un **anneau commutatif**.
- un **corps** si $(E, +, \times)$ est un anneau et $(E, \times)$ est un groupe.
- un **espace vectoriel sur un corps commutatif $\mathbb{K}$** s'il existe une loi de composition interne, $+$, et une loi de composition externe , $\quad \cdot : \mathbb{K} \times E \to E$, telles que
  - ▷ $(E, +)$ est un groupe commutatif dont l'élément neutre est traditionnellement noté 0_E ou 0,
  - ▷ la loi $\cdot$ est distributive par rapport à la loi $+$,
  - ▷ $\forall x \in E,\ 1_{\mathbb{K}} \cdot x = x \cdot 1_{\mathbb{K}} = x$,
  - ▷ $\forall x \in E, \forall \lambda, \mu \in \mathbb{K},\ \lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$

  Si $\mathbb{K} = \mathbb{R}$, on dit que E est un **$\mathbb{R}$-espace vectoriel**.
  Si $\mathbb{K} = \mathbb{C}$, on dit que E est un **$\mathbb{C}$-espace vectoriel**.
  On appelle alors **vecteurs** les éléments de E et **scalaires** les éléments de $\mathbb{K}$.

Exemple 5

Vous connaissez déjà beaucoup de groupes :

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ et $(\mathbb{C}, +)$ sont des groupes commutatifs
- $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times), \left(\mathbb{Q}_+^*, \times\right)$ et $\left(\mathbb{R}_+^*, \times\right)$ sont des groupes commutatifs.
- $(\mathbb{R}^{\mathbb{R}}, +)$ est un groupe commutatif
- L'ensemble des fonctions continues strictement croissante de $\mathbb{R}$ dans $\mathbb{R}$ muni de la loi '$\circ$' est un groupe non commutatif.
- Cependant, $(\mathbb{Z}^*, \times)$ n'est pas un groupe car 2, par exemple, n'a pas d'inverse dans $\mathbb{Z}$.

Exemple 6

Vous connaissez déjà beaucoup d'anneaux :

- $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs.
- $(\mathcal{C}^0(\mathbb{R}, \mathbb{R}), +, \times)$ est un anneau commutatif
- L'ensemble $\mathbb{R}[X]$ des polynômes, muni des lois '$+$' et '$\times$', est un anneau non commutatif.

Parmi ces anneaux, lesquels sont des corps ?

Exemple 7
Vous connaissez déjà beaucoup d'espace vectoriels :

- $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des $\mathbb{R}$-espaces vectoriels.
- $(\mathbb{R}^n, +, \times)$ est un $\mathbb{R}$-espace vectoriel.
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$ est un $\mathbb{R}$-espace vectoriel.
- $(\mathbb{C}^n, +, \times)$ est un $\mathbb{C}$-espace vectoriel.

Les espaces vectoriels ont une structure que l'on trouve partout en mathématiques. On y consacrera plusieurs chapitres.
Une des raisons, est que localement, tout est linéaire. Par exemple, on a l'impression que la terre est plate, à l'échelle humaine.

Définition 4 : Sous-groupe/anneau/corps/espace vectoriel
Soient E un | groupe / anneau / corps / espace vectoriel | et F une partie de E. On dit que F est un sous- | groupe / anneau / corps / espace vectoriel | de E si F est un stable pour les lois de structures de E et si F est un | groupe / anneau / corps / espace vectoriel | pour les mêmes lois de structure de E.

On redonnera les définitions au cas par cas dans chaque partie.

Exemple 8

- L'ensemble $E = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$.
  En effet, $(-1, 1) \in E$, mais $-(-1, 1) = (1, -1) \notin E$.
- L'ensemble $F = \{(x, y) \in \mathbb{R}^2 \mid x + y = 1\}$ n'est pas un sous-espace vectoriel de $\mathbb{R}^2$.
  En effet, $(0, 0) \notin E$.
- L'ensemble $G = \{(x, y) \in \mathbb{R}^2 \mid x + y = 0\}$ est un sous-espace vectoriel de $\mathbb{R}^2$.
  En effet, $(0, 0) \in E$, et G vérifie tous les axiomes de la définition d'un espace vectoriel.

1.2 Morphismes

Définition 5 : Morphisme
On appelle morphisme entre deux ensembles E et F avec la même structure, toute application de E dans F qui envoie la structure de E sur celle de F.

Vocabulaire On parle de morphisme de **groupes**, d'**anneaux**, de **corps**. Pour les espaces vectoriels, on parle d'**application linéaire**.

Au cas par cas

Un **morphisme de groupes** de $(G, \times)$ vers $(H, \star)$ est une application $f : G \to H$, telle que $\forall x, y \in G$, $f(x \times y) = f(x) \star f(y)$.
Un **morphisme d'anneaux** de $(A, +, \times)$ vers $(B, \oplus, \otimes)$ est une application $f : A \to B$, telle que $\forall x, y \in A$,

- $f(x + y) = f(x) \oplus f(y)$,
- $f(x \times y) = f(x) \otimes f(y)$,
- $f(1_A) = 1_B$.

Une **application linéaire** entre deux $\mathbb{K}$-espaces vectoriels $(V,+,\times)$ et $(W,+,\times)$ est une application $f : V \to W$, telle que $\forall x, y \in V$, $\forall \lambda \in \mathbb{K}$,

- $f(x+y) = f(x) + f(y)$,
- $f(\lambda x) = \lambda f(x)$.

Exemple 9
Vous connaissez déjà des morphismes de groupes

1. $\ln : (\mathbb{R}_+^*, \times) \longrightarrow (\mathbb{R}, +)$,
2. $\exp : (\mathbb{C}, +) \longrightarrow (\mathbb{C}^*, \times)$,
3. $\begin{array}{ccc} (\mathbb{R},+) & \longrightarrow & (\mathbb{U},\times) \\ \theta & \longmapsto & e^{i\theta} \end{array}$,
4. $\begin{array}{ccc} (\mathbb{U},\times) & \longrightarrow & (\mathbb{U},\times) \\ z & \longmapsto & z^n \end{array}$, $\forall n \in \mathbb{N}$.

Exemple 10
Vous connaissez déjà des morphismes d'anneaux

1. La conjugaison complexe de $\mathbb{C}$ dans $\mathbb{C}$.
2. La conjugaison complexe de $\mathbb{U}$ dans $\mathbb{U}$.
3. $\begin{array}{ccc} \mathsf{Conv}(\mathbb{R}^{\mathbb{N}}) & \longrightarrow & \mathbb{R} \\ u & \longmapsto & \lim u \end{array}$, où $\mathsf{Conv}(\mathbb{R}^{\mathbb{N}})$ est l'ensemble des suites réelles convergentes.

Exemple 11
L'application $f : \begin{array}{ccc} \mathbb{R}^3 & \longrightarrow & \mathbb{R}^2 \\ (x,y,z) & \longmapsto & (x-y, x-z) \end{array}$ est linéaire.

Proposition 1 : Propriétés des morphismes
Soit $f : E \to F$ un morphisme. Soit $\star$ et $*$ des lois structurelles de E et F respectivement et 0_E et 0_F leur élément neutre respectif.

1. *S'il existe un inverse pour $\star$ dans E, alors $f(0_E) = 0_H$.*
2. $\forall x \in E, f\left(x^{-1}\right) = f(x)^{-1}$.
3. *La composée de deux morphismes est encore un morphisme.*

Preuve.

1. $f(0_E) = f(0_E \star 0_E) = f(0_E) * f(0_E)$ et d'autre part $f(0_E) = f(0_E) \star 0_F$ d'où $f(0_E) = 0_F$.
2. $0_F = f(0_E) = f\left(x \star x^{-1}\right) = f(x) * f\left(x^{-1}\right)$.
3. Soient $x, y \in E$ et $f : (F, \star) \to (G, \dot{)}$, $g : (E, *) \to (F, \star)$ deux morphismes.
   On a $f \circ g(x*y) = f(g(x*y)) \underset{g \text{ morphisme}}{=} f(g(x) \star g(y)) \underset{f \text{ morphisme}}{=} f\big(g(x)\big) \cdot f\big(g(y)\big) = f \circ g(x) \cdot f \circ g(y)$.

□

Définition 6 : Noyau

Soient $f : E \to F$ un morphisme entre deux $\left|\begin{array}{c}\text{groupes}\\ \text{anneaux}\\ \text{corps}\\ \text{espaces vectoriels}\end{array}\right|$ et

$e_F \left|\begin{array}{c}\text{l'élément neutre du groupe}\\ \text{l'élément neutre pour l'addition dans l'anneau}\\ \text{l'élément neutre pour l'addition dans le corps}\\ \text{l'élément neutre pour l'addition dans l'espace vectoriel}\end{array}\right|$. Le **noyau de f** est le sous-ensemble de E

$$\mathsf{Ker}(f) := \{x \in E \mid f(x) = 0_F\} \ .$$

Exemple 12

Regardons les noyaux des morphismes de l'exemple 9.

1. $\forall x \in \mathbb{R}_+^*$, $\ln(x) = 0 \iff x = \exp(0) = 1$. Donc $\mathsf{Ker}\ln = \{1\}$.
2. $\forall z \in \mathbb{C}$, $\exp(z) = 1 \iff z = 2ki\pi$, avec $k \in \mathbb{Z}$. Donc $\mathsf{Ker}\exp = \{2ki\pi \mid k \in \mathbb{Z}\}$.
3. $\forall \theta \in \mathbb{R}$, $\exp(i\theta) = 1 \iff i\theta = 2ki\pi$, avec $k \in \mathbb{Z}$. Donc le noyau est $\{2k\pi \mid k \in \mathbb{Z}\}$.
4. $\forall z \in \mathbb{C}$, $z^n = 1 \iff z \in \mathbb{U}_n$. Donc le noyau est $\mathbb{U}_n$.

Exemple 13

Soit G un groupe. Pour tout $g \in G$, l'application $\left\{\begin{array}{ccc} G & \to & G \\ x & \mapsto & x \star g \end{array}\right.$ est un morphisme de groupe bijectif.

Vocabulaire

- **Isomorphisme** = Morphisme bijectif
- **Endmorphisme** = Morphisme de E dans E
- **Automorphisme** = Endomorphisme de E bijectif
- **Épimorphisme** = Morphisme surjectif
- **Monomorphisme** = Morphisme injectif

Les deux derniers noms n'étant pas beaucoup utilisés.

Proposition 2 : Caractérisation de l'injectivité par le noyau

Dans les notations de la définition, si $\mathsf{Ker}f = \{0_E\}$, alors f est un morphisme injectif.

Preuve. Soit $+$ la loi pour laquelle 0_E est le neutre.
Si $\mathsf{Ker}f = \{0_E\}$, il suffit de remarquer que $f(x) = f(y) \iff f\left(x \star y^{-1}\right) = f(x) * f(y)^{-1} = 0_F$, c'est-à-dire $x \star y^{-1} \in \mathrm{Ker}\, f$. Donc $x \star y^{-1} = 0_E$ et donc $x = y$.
Si f est injective, pour tout $x \in \mathsf{Ker}f$, $\quad f(x) = 0 = f(0_E)$ donc $x = 0_E$. Cela montre que $\mathsf{Ker}f \subset \{0_E\}$, d'où l'égalité par double inclusion. □

Surjectivité

On rappelle que $f : E \to F$ est surjectif si, et seulement si,

$$\mathsf{Im}f := \{f(x) \mid x \in E\} = F \ .$$

Exemple 14
Soit $(G,\cdot)$ un groupe. Pour tout $a \in G$, on note $\tau_a : G \longrightarrow G$ l'application définie par

$$\tau_a(x) = axa^{-1}$$

On a alors $\forall (x,y) \in G^2$, $\tau_a(xy) = a(xy)a^{-1} = \left(axa^{-1}\right)\left(aya^{-1}\right) = \tau_a(x)\tau_a(y)$. Donc τ_a est un endomorphisme de G.
De plus, $\forall x \in G$, on a

$$\begin{cases} \left(\tau_a \circ \tau_{a^{-1}}\right)(x) = \tau_a\left(a^{-1}xa\right) = a\left(a^{-1}xa\right)a^{-1} = x \\ \left(\tau_{a^{-1}} \circ \tau_a\right)(x) = \tau_{a^{-1}}\left(axa^{-1}\right) = a^{-1}\left(axa^{-1}\right)a = x \end{cases}$$

donc $\tau_a \circ \tau_{a^{-1}} = \tau_{a^{-1}} \circ \tau_a = \mathrm{Id}_G$, ce qui montre que τ_a est bijective, de réciproque $\tau_{a^{-1}}$. Ainsi, τ_a est un automorphisme du groupe G.

La proposition suivante reste vraie pour les autres structures.

Proposition 3
Soit $f : G \to G'$ un morphisme de groupes.

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

⚠ Attention On rappelle que la notation $f^{-1}(H')$ peut être écrit même si f n'est pas une bijection. Elle représente l'image réciproque de H par f, définie par $f^{-1}(H) = \{x \in G \mid f(x) \in H'\}$.

Preuve. On fait la démonstration pour les groupes. On utilise la caractérisation des sous groupes (Proposition 4

- L'ensemble $f(H)$ est non vide puisqu'il contient $e_H = f(e_G)$. Pour tous $x, y \in f(H)$, il existe $s, t \in H$ tels que $x = f(s)$ et $y = f(t)$. Alors
$$x \star y^{-1} = f(s) \star f(t)^{-1} = f\left(s \star t^{-1}\right) \in f(H)$$
Ainsi, $f(H)$ est un sous-groupe de G d'après la caractérisation des sous-groupes.
- L'ensemble $f^{-1}(H')$ est non vide puisqu'il contient l'élément neutre de G. Pour tous $x, y \in f^{-1}(H'), f(x), f(y) \in H'$ donc
$$f\left(x \star y^{-1}\right) = f(x) \star f(y)^{-1} \in H'$$
Ainsi, $x \star y^{-1} \in f^{-1}(H')$ et $f^{-1}(H')$ est un sous-groupe de G d'après la caractérisation précédente.

□

2 Groupes

Exemple 15
Un groupe $(G,\cdot)$ a la «propriété du sudoku».

Pour tout $(a,b) \in G^2$, il existe un unique $g \in G$ tel que $a \cdot g = b$ et il existe un unique $h \in G$ tel que $h \cdot a = b$.

On peut alors s'amuser un peu avec les groupes de petit cardinal, en donnant leurs tables de loi.

- **Groupe à 0 élément** Il n'y a pas de groupe à 0 élément, puisqu'il faut un élément neutre.
- **Groupe à 1 élément** Si $G = \{e\}$ alors G est un groupe muni de l'opération $\star$ telle que $e \cdot e = e$.
- **Groupe à 2 éléments** Notons $G = \{e, a\}$. On définit la loi de G par le tableau suivant : On a nécessairement $a \cdot a = e$ car si $a \cdot a = a$, alors $a = e$ et le groupe aurait un seul élément.

- **Groupe à 3 éléments** $G = \{e, a, b\}$:

x \ y	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

En effet, $a \cdot a \neq a$ sinon on aurait $a = e$ en multipliant des deux côtés à gauche par a^{-1}. Et $a \cdot a \neq e$ sinon par propriété du Sudoku, $b \cdot b = b$ or on a déjà $e \cdot b = b$ dans cette colonne.

- **Groupe à 4 éléments** $G = \{e, a, b, c\}$. On donne deux lois différentes.

x \ y	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

x \ y	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Notations additive et multiplicatives

Vous aurez remarqué que la loi $\star$ n'est a priori comme aucune autre que vous avez déjà vu. Quand la loi est associative, on peut itérer plusieurs fois la loi sur un élément de E, $x \star x \star \cdots \star x$. Il y a alors les deux notations que vous connaissez déjà. Pour tous $x \in E$ et $n \in \mathbb{N}^*$, on pose

- **Notation multiplicative** $x^n := \underbrace{x \star \ldots \star x}_{n \text{ fois}}$.
- **Notation additive** $nx := \underbrace{x + \ldots + x}_{n \text{ fois}}$.

On préfère le mot **multiple** dans le cas additif, au mot **puissance** dans la cas multiplicatif, mais c'est au fond la même chose.
Souvent quand la notation est multiplicative, on abrège $x \star y$ en xy.

Définition 7 : Permutation, groupe symétrique

Soit E un ensemble non vide.

- On appelle **permutation de E** toute bijection de E sur E.
- On appelle **groupe symétrique de E** l'ensemble des permutations de E, noté S_E. Alors $(S_E, \circ)$ est un groupe d'élément neutre Id_E.

Il y a quelque chose à démontrer ici. À vous !

Notation des permutations

Soit

$$\begin{array}{rccc} \sigma : & [\![1,6]\!] & \longrightarrow & [\![1,6]\!] \\ & 1 & \longmapsto & 3 \\ & 2 & \longmapsto & 5 \\ & 3 & \longmapsto & 4 \\ & 4 & \longmapsto & 6 \\ & 5 & \longmapsto & 2 \\ & 6 & \longmapsto & 1 \end{array}$$

La permutation σ est alors notée

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 6 & 2 & 1 \end{pmatrix}$$

Groupe symétrique d'un ensemble E de cardinal fini

Si $\text{Card}(E) = n \in \mathbb{N}^*$, alors il y a $n!$ élément dans $S_n := S_E$. En effet, il y a n images possibles pour le premier élément, $n-1$ images possibles pour le deuxième élément, car on ne peut pas choisir la même image que le premier élément ! Ainsi de suite, on obtient $n \times (n-1) \times (n-2) \times \cdots \times 1 = n!$ possibilités !

Exemple 16

Dans S_3, il y a donc $3! = 6$ permutations. Essayons de toutes les donner.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Pour S_4, il y a déjà $4! = 24$ éléments... Il faut trouver un moyen de les classer, pour ne pas avoir à tout écrire à chaque fois !

Définition 8 : Sous-groupe

Soient G un groupe et H une partie de G stable par produit. On dit que H est un sous-groupe de G si H est un groupe pour la loi de G.

Exemple 17

Si G est un groupe de neutre e, alors $\{e\}$ et G sont toujours des sous-groupes de G.

Est ce que l'élément neutre de H est celui de G ? Est ce que les inverses de H par la loi de G sont tous dans H ? Oui !

Proposition 4 : Caractérisation des sous-groupe

Soient $(G, \star)$ un groupe, $1_G \in G$ son élément neutre et $H \subset G$. Alors H est un sous-groupe de G si et seulement si

$$1_G \in H \qquad et \qquad \forall (x,y) \in H^2,\ x \star y \in H \qquad et \qquad \forall x \in H,\ x^{-1} \in H\ .$$

*Autrement dit, H contient le neutre de G et est **stable par produit et passage à l'inverse***

Preuve.

($\Rightarrow$) Si H est un sous-groupe de G alors H muni de $\star$ est un groupe. Par définition d'un groupe, il est stable (car la loi est de composition interne). Montrons qu'il contient le neutre et il stable par inverse

- Notons 1_H l'élément neutre de H. Comme 1_H est neutre dans H : $1_H 1_H = 1_H$. Mais 1_G est neutre dans G, donc, $1_H 1_G = 1_H$.
  On obtient $1_H 1_H = 1_H 1_G$. Or $1_H \in G$, donc admet un inverse dans G. Enfin, $1_H = 1_G$, et donc $1_G \in H$.
- Soit $h \in H$. Notons i l'inverse de h dans H et gardons h^{-1} l'inverse de h dans G.
  Alors $i = 1_G i = \left(h^{-1}h\right) i = h^{-1}\left(hi\right) = h^{-1}1_H = h^{-1}1_G = h^{-1}$.
  Donc $h^{-1} = i \in H$.

($\Leftarrow$) Supposons que $H \subset G$ vérifie les trois hypothèses de la proposition. Alors

- La deuxième assure que H est stable par $\star$, donc c'est bien une loi de composition interne sur H. De plus $\star$ est associative sur G donc sur H.
- 1_G est neutre pour $\star$ dans G, donc dans H, car tout élément de H est dans G.
- La troisième assure que tout élément de H est inversible dans H.

Donc H est bien un sous-groupe de G

□

En pratique

Pour montrer en une fois la stabilité par produit et inverse, on montre que $\forall h, h' \in H, \quad h^{-1}h' \in H$.
On note bien l'importance du caractère non vide de H dans cette caractérisation. Pour le montrer, on remarque en général que l'élément neutre de G appartient à H.
On utilise **toujours** la caractérisation des sous-groupes pour montrer qu'un ensemble est un sous-groupe... ou un groupe d'ailleurs ! On économise l'associativité qui n'est plus à montrer !
Par exemple, pour montrer que $(\mathbb{Z}, +)$ est un groupe, on montre que c'est un sous-groupe de $(\mathbb{R}, +)$. Pour cela, il faut savoir que $(\mathbb{R}, +)$ est un groupe !

Exemple 18
Montrons que $(\mathbb{Z}, +)$ est un groupe. On sait que $(\mathbb{R}, +)$ est un groupe. On a

- $\mathbb{Z} \subset \mathbb{R}$,
- $0 \in \mathbb{Z}$,
- $\forall (m, n) \in \mathbb{Z}^2, \ m - n \in \mathbb{Z}$.

Donc $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$, et donc c'est un groupe.

Exemple 19
Montrons que $(\mathbb{U}, \times)$ est un sous-groupe de $(\mathbb{C}^*, \times)$. On a

- si $z \in \mathbb{U}$, alors $|z| = 1$, donc $z \neq 0$, d'où $\mathbb{U} \subset \mathbb{C}^*$.
- $1 = e^{i0} \in \mathbb{U}$
- $\forall (z, z') \in \mathbb{U}^2, \left|z^{-1}z'\right| = |z^{-1}|\,|z'| = 1 \times 1 = 1$ donc $z^{-1}z' \in \mathbb{U}$.

Exemple 20
On a déjà montré que les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$, dans le chapitre Arithmétique.

Exemple 21
Soient E un ensemble non vide et $x \in E$. Montrons que l'ensemble $\mathsf{Stab}(x) := \{\sigma \in S_E \mid \sigma(x) = x\}$ est un sous-groupe de S_E. On a

- $\mathsf{Stab}(x) \subset S_E$,
- $\mathrm{Id}_E(x) = x$, pour tout $x \in E$, donc $\mathrm{Id}_E \in \mathrm{Stab}(x)$,
- $\sigma, \tau \in \mathrm{Stab}(x)$. On a ainsi $\tau(x) = x$ et $\sigma(x) = x$, et en composant par σ^{-1}, on a $\sigma^{-1}(x) = x$. Donc $\sigma^{-1} \circ \tau(x) = \sigma^{-1}(x) = x$, d'où $\sigma^{-1} \circ \tau \in \mathsf{Stab}(x)$.

Ce groupe est appelé le stabilisateur de x.

Exemple 22
On définit $\mathcal{C}_0^n(\mathbb{R}, \mathbb{R}) := \{f \in \mathcal{C}^n(\mathbb{R}, \mathbb{R}) \mid \forall x \in \mathbb{R}, \ f'(x) \neq 0\}$.
Montrer que $(\mathcal{C}_0^n(\mathbb{R}, \mathbb{R}), \circ)$ est un groupe, on montre que c'est un sous-groupe de $(\mathbb{R}^{\mathbb{R}}, \circ)$.

Exemple 23
Le centre du groupe $(G, \star)$ est le sous-groupe $Z(G)$ des éléments de G qui commutent avec tous les autres éléments, c'est-à-dire

$$Z(G) = \{x \in G, \quad \forall y \in G, \quad x \star y = y \star x\}.$$

En particulier, $Z(G) = G$, si G est abélien.
Montrons que $Z(G)$ est bien un sous-groupe de G. Tout d'abord, $Z(G)$ est non vide car $e \in Z(G)$. Ensuite, pour tous $x, y \in Z(G)$ et tout $z \in G$,

$$\begin{aligned}\left(x \star y^{-1}\right) \star z &= x \star \left(y^{-1} \star z\right) = x \star \left(z \star y^{-1}\right) \\ &= (x \star z) \star y^{-1} = (z \star x) \star y^{-1} = z \star \left(x \star y^{-1}\right).\end{aligned}$$

On a utilisé respectivement l'associativité, le fait que $y^{-1} \in Z(G)$, l'associativité à nouveau, le fait que $x \in Z(G)$ et encore l'associativité. Ainsi, $x \star y^{-1} \in Z(G)$ ce qui termine la caractérisation de sous-groupe de G.

Proposition 5
Une intersection de sous-groupes de $(G, \star)$ est encore un sous-groupe de G.

Preuve. A vous ! □

Attention La réunion de deux sous-groupes est rarement un sous-groupe. En effet, on peut montrer que si H et K sont deux sous-groupes de G, alors $H \cup K$ est un sous-groupe de G si, et seulement si, $H \subset K$ ou $K \subset H$.

Proposition 6 : Groupe produit
*Soient $(G_1, \star)$ et $(G_2, *)$ deux groupes. On définit une **loi de composition interne** sur l'ensemble $G_1 \times G_2$ en posant*

$$\forall (x_1, x_2), (y_1, y_2) \in G_1 \times G_2, \ (x_1, x_2) \cdot (y_1, y_2) = (x_1 \star y_1, x_2 * y_2) \ .$$

*Muni cette loi, $G_1 \times G_2$ est un groupe d'élément neutre $(1_{G_1}, 1_{G_2})$ appelé le **groupe produit de G_1 et G_2**.*
On peut généraliser cette construction au produit d'une famille quelconque de groupes.

Preuve. La preuve est directe sans accroc.

- **Associativité** Pour tous $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in G_1 \times G_2$, on a

$$(x_1, x_2)\left((y_1, y_2)(z_1, z_2)\right) = (x_1, x_2)(y_1 z_1, y_2 z_2) = (x_1 y_1 z_1, x_2 y_2 z_2) = (x_1 y_1, x_2 y_2)(z_2, z_2) = \left((x_1, x_2)(y_1, y_2)\right)(z_1, z_2) \ .$$

- **Élément neutre** Pour tout $(x_1, x_2) \in G_1 \times G_2$,

$$(1_{G_1}, 1_{G_2})(x_1, x_2) = (1_{G_1} x_1, 1_{G_2} x_2) = (x_1, x_2) \quad \text{et} \quad (x_1, x_2)(1_{G_1}, 1_{G_2}) = (x_1 1_{G_1}, x_2 1_{G_2}) = (x_1, x_2) \ .$$

- **Inversibles** Soit $(x_1, x_2) \in G_1 \times G_2$. Montrons que (x_1, x_2) est inversible d'inverse $\left(x_1^{-1}, x_2^{-1}\right)$.

$$(x_1, x_2)\left(x_1^{-1}, x_2^{-1}\right) = \left(x_1 x_1^{-1}, x_2 x_2^{-1}\right) = (1_{G_1}, 1_{G_2}) \quad \text{et} \quad \left(x_1^{-1}, x_2^{-1}\right)(x_1, x_2) = \left(x_1^{-1} x_1, x_2^{-1} x_2\right) = (1_{G_1}, 1_{G_2}) \ .$$

□

3 Anneaux

3.1 Cas particulier de la structure

Définition 9 : Intégrité
On dit qu'un anneau $(A, +, \times)$ est **intègre** lorsque

$$\forall a, b \in A, \quad a \times b = 0_A \quad \Rightarrow \quad a = 0_A \text{ ou } b = 0_A$$

Exemple 24
Vous aviez cette règle en tête depuis le début de votre scolarité. Tous les nombres que vous avez utilisés jusque maintenant vérifiaient cette propriété. Donc les anneaux $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{C}$, sont intègre. Mais on a aussi vu que cela ne fonctionne pas avec les fonctions. Donc $\mathbb{R}^{\mathbb{R}}$ n'est pas intègre.

Exemple 25
L'ensemble des entiers de Gauss $\mathbb{Z}[i] = \{a + ib, \text{ avec } a, b \in \mathbb{Z}\}$ est un anneau commutatif pour l'addition et la multiplication, qui est intègre.

Attention Tout anneau n'est pas intègre. Dans ce cas certaines règles de calcul ne sont plus valables ! Pour tout $a, b, x, y \in A$,

$$ax = ay \not\Longrightarrow a = 0_A \text{ ou } x = y \qquad \text{et} \qquad a^2 = b^2 \not\Longrightarrow a = b \text{ ou } a = -b$$

L'élément neutre de l'addition

Dans un anneau, la "première" loi est notée additivement '+' et la "seconde" multiplicativement '×'.

- L'élément 0_A est «absorbant» pour $\times$. En effet,

$$\forall x \in A, \quad x = (0_A + 1_A) \times x = 0_A \times x + x.$$

  D'où, en ajoutant l'opposé $-x$ des deux côtés de l'égalité, $0_A \times x = 0_A$.

- Pour tout $x \in A, (-1_A) \times x$ est le symétrique de x pour $+$, c'est-à-dire $-x$, car

$$\begin{aligned} 0_A &= 0_A \times x \\ &= (1_A - 1_A) \times x \\ &= 1_A \times x + (-1_A) \times x \\ &= x + (-1_A) \times x. \end{aligned}$$

Règles de calculs

Dans un anneau A, on dispose des règles de calcul suivantes qui généralisent les identités remarquables

$$\forall a \in A, \forall n \in \mathbb{N}, \quad (1_A - a) \times \left(\sum_{k=0}^{n} a^k \right) = 1_A - a^{n+1}.$$

De même, on obtient la formule du binôme et celle de Bernoulli, par récurrence pour deux éléments d'un anneau A **qui commutent**. $\forall a, b \in A, \forall n \in \mathbb{N}, \quad a \times b = b \times a$,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k} \qquad \text{et} \qquad (b-a) \times \left(\sum_{k=0}^{n} a^k \times b^{n-k} \right) = b^{n+1} - a^{n+1}$$

En particulier, la formule du binôme de Newton est toujours vraie dans un anneau **commutatif**.

Notation On note A^* l'ensemble des éléments inversibles d'un anneau $(A, +, \times)$.

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

En effet, par définition d'anneau, $\times$ est associative et son élément neutre 1_A appartient à A^*. Soit $x, y \in A^*$. Alors, $x \times y$ est inversible d'inverse $y^{-1} \times x^{-1}$ donc $x \times y \in A^*$ et $\times$ est une loi de composition interne pour A^*. De plus, pour tout $x \in A^*, x^{-1}$ est inversible, d'inverse x, donc appartient à A^*.

Exemple 26

- Dans $\mathbb{Z}$, seuls 1 et -1 sont inversibles. Donc $\mathbb{Z}^* = \{-1, 1\}$.

- Le groupe des inversibles de l'ensemble $\mathbb{D}$ des décimaux est

$$\mathbb{D}^* = \left\{2^\alpha 5^\beta, (\alpha,\beta) \in \mathbb{Z}^2\right\}$$

En effet, soit $n \in \mathbb{Z}$ et $a \in \mathbb{N}$ tel que $\frac{n}{10^a} \in \mathbb{D}^*$; il existe $m \in \mathbb{Z}$ et $b \in \mathbb{N}$ tels que

$$\frac{n}{10^a} \cdot \frac{m}{10^b} = 1$$

Par conséquent, n est un diviseur de 10^{a+b} et $\frac{n}{10^a} \in \left\{2^\alpha 5^\beta, (\alpha,\beta) \in \mathbb{Z}^2\right\}$. Réciproquement, on vérifie que tous les éléments de la forme $2^\alpha 5^\beta$ sont des décimaux inversibles.

- Le groupe des inversibles de l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est $\mathbb{U}_4$.
Supposons $z \in \mathbb{Z}[i]$ est inversible. On a $|z|^2 \in \mathbb{N}$ et $|z^{-1}|^2 \in \mathbb{N}$. Or $|z|^2|z^{-1}|^2 = |1|^2 = 1$. Donc $|z| = 1$. De plus, si $|z| = 1$ alors $z^{-1} = \bar{z} \in \mathbb{Z}[i]$. Donc l'ensemble des inversibles de $\mathbb{Z}[i]$ est exactement l'ensemble des $z \in \mathbb{U} \cap \mathbb{Z}[i]$. Ainsi, $a + ib \in \mathbb{Z}[i]^*$ si, et seulement si, $a^2 + b^2 = 1$. Comme a et b sont entiers, on obtient quatre possibilités qui correspondent à $1, i, -1, -i$.

Définition 10 : Corps

Soit $(K, +, \times)$ un anneau commutatif et non réduit à 0_K. On dit que K est un **corps**, lorsque tout élément non-nul de K est inversible pour la loi $\times$.

Exemple 27

Les anneaux $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{C}$ sont des corps, mais $\mathbb{Z}$ ou $\mathbb{R}^\mathbb{R}$ ne le sont pas.

Définition 11 : Sous-anneau

Soit $(A, +, \times)$ un anneau et $B \subset A$. On dit que B est un sous-anneau de A lorsque $(B, +, \times)$ est un anneau.

Proposition 7 : Caractérisation des sous-anneaux

Soit $(A, +, \times)$ un anneau, soit $B \subset A$. Alors B est un sous-anneau de A si et seulement si

- $1_A \in B$,
- ***Stabilité par soustraction*** $\forall (x, y) \in B^2, x - y \in B$,
- ***Stabilité par produit*** $\forall (x, y) \in B^2, xy \in B$.

Exemple 28

$\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, qui est un sous-anneau de $\mathbb{R}$, qui est un sous-anneau de $\mathbb{C}$.

3.2 Morphismes

Proposition 8 : Cas particulier d'un morphisme d'anneaux

Si $f : A \to B$ est un morphisme d'anneaux alors

- $f(0_A) = 0_B$,
- *Pour tout $a \in A$, $f(-a) = -f(a)$.*
- *Si $a \in A$ est inversible alors $f(a)$ l'est aussi et $f(a)^{-1} = f\left(a^{-1}\right)$.*

Preuve.

- $f(0_A) = f(0_A + 0_A) = f(0_A) \oplus f(0_A)$ et en ajoutant l'opposé (pour $\oplus$) de $f(0_A)$ des deux côtés il vient $0_B = f(0_A)$.
- Soit $a \in A$. $f(-a) = f(0_A - a) = 0_B - f(a) = -f(a)$ par la proposition précédente.

- Soit $a \in A$ inversible. Alors $f(a)f\left(a^{-1}\right) = f\left(aa^{-1}\right) = f\left(1_A\right) = 1_B$ ce qui prouve que $f(a)$ est inversible, d'inverse $f\left(a^{-1}\right)$.

□

Exemple 29
Cherchons tous les morphismes d'anneaux $f : \mathbb{Q} \to \mathbb{Q}$. Puisque f est un morphisme d'anneaux, on a $f(1) = 1$, puis $f(2) = f(1+1) = f(1) + f(1) = 2$. Par une récurrence immédiate, basée sur la formule $f(n+1) = f(n) + f(1)$, on trouve que pour tout $n \in \mathbb{N}$, on a $f(n) = n$.
D'autre part, si $n \in \mathbb{Z}$ est strictement négatif, alors $-n \geq 0$ et $-f(n) = f(-n) = -n$.
Ainsi, pour tout $n \in \mathbb{Z}$, on a $f(n) = n$.
Soit maintenant $n \in \mathbb{N}^*$. Alors on a

$$1 = f(1) = f\left(n \times \frac{1}{n}\right) = f(n)f(1/n) = nf(1/n)$$

d'où $f(1/n) = 1/n$. Finalement, si $x \in \mathbb{Q}, x$ s'écrit $x = p/q$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Par les propriétés de morphisme de f, on a

$$f(p/q) = f(p)f(1/q) = p/q$$

En fait, il n'existe qu'un morphisme d'anneaux de $\mathbb{Q}$ dans $\mathbb{Q}$ qui est $f = \mathrm{Id}_{\mathbb{Q}}$.

4 Espaces vectoriels

Les éléments d'un espace vectoriel sont appelés **vecteurs** et les éléments du corps de base sont appelés **scalaires**. On note toujours les produits dans l'ordre scalaire puis vecteur : $\forall \lambda \in \mathbb{R}$, $\forall u \in \mathbb{R}^3$, on note λu et pas $u\lambda$.

Les *espaces vectoriels* sont présent partout en mathématiques. C'est une structure très importante parce que tout peut être ramené à un espace vectoriel, en prenant une loupe assez grossissante. C'est d'ailleurs pour cela que les humains ont cru que la terre était plate. Si on zoom sur un arc de cercle suffisamment, il devient plat comme une droite.

Proposition 9 : Règles de calcul
Soient $\lambda \in \mathbb{K}$ et x dans un $\mathbb{K}$-espace vectoriel E. Alors,

- $\lambda \cdot 0_E = 0_E$
- $(-1) \cdot x = -x$
- $0 \cdot x = 0_E$
- $\lambda \cdot x = 0_E \implies \lambda = 0$ *ou* $x = 0_E$.

Preuve.

- Comme $0_E + 0_E = 0_E$, on obtient
$$\lambda.0_E = \lambda.\left(0_E + 0_E\right) = \lambda.0_E + \lambda.0_E.$$
En ajoutant l'opposé de $\lambda.0_E$ (qui existe d'après la propriété de groupe additif), on obtient $0_E = \lambda.0_E$.
- On procède de même en partant de $0 + 0 = 0$ (dans le corps $\mathbb{K}$) et on obtient
$$0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$$
donc $0.x = 0_E$.
- On part cette fois-ci de $0 = 1 + (-1)$ et on obtient
$$0_E = 0 \cdot x = (1 + (-1)) \cdot x = 1 \cdot x + (-1) \cdot x = x + (-1) \cdot x$$
En ajoutant l'opposé $-x$ de x, on obtient bien $-x = (-1).x$.
- Supposons $\lambda.x = 0_E$. Si $\lambda \neq 0$, alors λ est inversible et
$$0_E = \lambda^{-1} \cdot 0_E = \lambda^{-1} \cdot (\lambda \cdot x) = \left(\lambda^{-1}\lambda\right) \cdot x = 1 \cdot x = x$$

□

Définition 12 : Sous espace vectoriel

Une partie F d'un $\mathbb{K}$-espace vectoriel E est un sous-espace vectoriel de E si

- F est stable par $+$ et $\cdot$,
- muni de ces lois, F est un $\mathbb{K}$-espace vectoriel.

Exemple 30

Si E est un $\mathbb{K}$-espace vectoriel, E et $\{0_E\}$ sont deux sous-espaces vectoriels de E.

⚠ Attention L'ensemble vide n'est pas un sous-espace vectoriel de E, car il ne contient pas l'élément neutre de l'addition 0_E, donc n'est pas un groupe additif.

En pratique

En pratique, pour montrer que W est un sous-espace vectoriel d'un $\mathbb{K}$-espace vectoriel V, il suffit de montrer que,

- $F \subset E$,
- $0_E \in F$,
- $\forall x, y \in F, \forall \lambda \in \mathbb{K}, \quad \lambda x + y \in F$.

Exemple 31

Soient $F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y - z = 0\}$ et $G = \{(a - b, a + b, a - 3b) \mid a, b \in \mathbb{R}\}$. F et G sont des sous-espaces vectoriels de $\mathbb{R}^3$.
En effet, $F \subset \mathbb{R}^3, 0^3_{\mathbb{R}} = (0, 0, 0) \in F$ car $0 + 0 - 0 = 0$.
De plus, pour tous $\lambda \in \mathbb{R}$, $\vec{u}, \vec{v} \in F$, on peut écrire $\vec{u} = (x, y, z)$ et $\vec{v} = (x', y', z')$ avec $x + y - z = 0$ et $x' + y' - z' = 0$.
On a alors $\lambda\vec{u} + \vec{v} = (\lambda x + x', \lambda y + y', \lambda z + z')$ avec

$$(\lambda x + x') + (\lambda y + y') - (\lambda z + z') = \lambda(x + y - z) + (x' + y' - z') = 0$$

donc $\lambda\vec{u} + \vec{v} \in F$.

De même, $G \subset \mathbb{R}^3$, et $\vec{o} = (0, 0, 0) \in G$ car $(0, 0, 0) = (a - b, a + b, a - 3b)$ pour $a = b = 0$.
Pour tout $\lambda \in \mathbb{R}, \vec{u}, \vec{v} \in G$, on peut écrire $\vec{u} = (a - b, a + b, a - 3b)$ et $\vec{v} = (a' - b', a' + b', a' - 3b')$ avec $a, b, a', b' \in \mathbb{R}$.
On a alors

$$\lambda\vec{u} + \vec{v} = \ldots = (a'' - b'', a'' + b'', a'' - 3b'')$$

avec $a'' = \lambda a + a'$ et $b'' = \lambda b + b'$ donc $\lambda\vec{u} + \vec{v} \in G$.

Exemple 32

Pour tout $n \in \mathbb{N}$, on note $\mathbb{R}_n[X]$ l'ensemble des polynômes de degré inférieur ou égal à n.
L'ensemble $\mathbb{R}_n[X]$ sous-espace vectoriel de $\mathbb{R}[X]$. En effet, on a

- $\mathbb{R}_n[X] \subset \mathbb{R}[X]$.
- $0 \in \mathbb{R}_n[X]$ car $\deg(0) = -\infty \leqslant n$.
- Montrons enfin que $\mathbb{R}_n[X]$ est stable par combinaison linéaire. Soient $P, Q \in \mathbb{R}_n[X]$ et $\lambda \in \mathbb{R}$. Nous savons que $\deg(\lambda P + Q) \leqslant \max\{\deg(P), \deg(Q)\} \leqslant n, \quad$ donc $\quad \lambda P + Q \in \mathbb{R}_n[X]$.

⚠ Attention L'ensemble des polynômes de degré égal à n n'est pas un sous-espace vectoriel de $\mathbb{K}[X]$. Il ne contient même pas le polynôme nul !

Proposition 10 : Espace vectoriel produit

Soient $E_1, \dots, E_n$ des $\mathbb{K}$-espaces vectoriels. On munit $E_1 \times \dots \times E_n$ de deux lois $+$ et $\cdot$ en posant, pour tous $\lambda \in \mathbb{K}$ et $(x_1, \dots, x_n), (y_1, \dots, y_n) \in E_1 \times \dots \times E_n$

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n) \quad \text{et} \quad \lambda \cdot (x_1, \dots, x_n) = (\lambda \cdot x_1, \dots, \lambda \cdot x_n).$$

Alors $(E_1 \times \dots \times E_n, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel.
On a $0_{E_1 \times \dots \times E_n} = (0_{E_1}, \dots, 0_{E_n})$.

Preuve. Il suffit de montrer les axiomes dans la définition d'espace vectoriel un à un. A vous ! □

Définition 13 : Combinaison linéaire

Soit $(x_i)_{i \in I}$ une famille de vecteurs d'un $\mathbb{K}$-espace vectoriel E. Une combinaison linéaire de $(x_i)_{i \in I}$ est un vecteur de la forme $\sum_{i \in I} \lambda_i x_i$ où $(\lambda_i)_{i \in I}$ est une famille presque nulle de scalaires.

Exemple 33

Dans $\mathbb{R}^3$, par exemple, les combinaisons linéaires des vecteurs $(1, 2, 3)$ et $(1, 0, 1)$ sont les vecteurs $\lambda \cdot (1, 2, 3) + \mu \cdot (1, 0, 1) = (\lambda + \mu, 2\lambda, 3\lambda + \mu)$, avec $\lambda, \mu \in \mathbb{R}$.

Attention On ne peut pas identifier les scalaires en général !

$\sum_{k=1}^{n} \lambda_k x_k = \sum_{k=1}^{n} \mu_k x_k \not\Longrightarrow \lambda_k = \mu_k$, pour tout $k \in [\![1, n]\!]$.

Exemple 34

Dans $\mathbb{R}^2$, $(4, 3)$ est-il une combinaison linéaire des vecteurs $(1, -1)$ et $(2, 3)$?
Pour cela, il faut résoudre l'équation $(4, 3) = \lambda(1, -1) + \mu(2, 3)$, où $\lambda, \mu \in \mathbb{R}$. On a

$$\begin{aligned} (4,3) = \lambda(1,-1) + \mu(2,3) &\iff (4,3) = (\lambda + 2\mu, -\lambda + 3\mu) \\ &\iff \begin{cases} \lambda + 2\mu = 4 \\ -\lambda + 3\mu = 3 \end{cases} \iff \begin{cases} \lambda + 2\mu = 4 \\ 5\mu = 7 \end{cases} \\ &\iff \begin{cases} \lambda = \frac{6}{5} \\ \mu = \frac{7}{5} \end{cases} \end{aligned}$$

Donc $(4, 3) = \frac{6}{5}(1, -1) + \frac{7}{5}(2, 3)$.

Proposition 11 : Intersection de sous-espaces vectoriels

Soit E un $\mathbb{K}$-espace vectoriel. Toute intersection de sous-espaces vectoriels de E est encore un sous-espace vectoriel de E.

Preuve. Soit $(F_i)_{i \in I}$ une famille de sous-espaces vectoriels de E. Nous voulons montrer que $F = \bigcap_{i \in I} F_i$ est un sous-espace vectoriel de E.

- $F \subset E$.
- $0_E \in F_i$, pour tout $i \in I$ puisque F_i est un sous-espace vectoriel de E, donc $0_E \in F$.
- Enfin, soient $x, y \in F$ et $\lambda \in \mathbb{K}$. Pour tout $i \in I$, $\lambda x + y \in F_i$, car F_i est un sous-espace vectoriel de E et $x, y \in F_i$, donc $\lambda x + y \in F$. Donc F est stable par combinaison linéaire.

□

Attention Comme pour les groupes, la réunion de deux sous-espaces vectoriels **n'est pas** un sous-espace vectoriel en général !
C'est clair que la réunion de deux droites passant par 0 dans le plan n'est ni une droite, ni un plan !

Exemple 35
Reprenons les données de l'exemple 31. Cherchons à déterminer $F \cap G$. $\vec{u} = (x, y, z) \in F \cap G$ si, et seulement $\vec{u} = (x, y, z) \in F$ et $\vec{u} = (x, y, z) \in G$ si, et seulement s'il existe $a, b \in \mathbb{R}$ tels que

$$\begin{cases} x &= a - b \\ y &= a + b \\ z &= a - 3b \\ x + y - z &= 0 \end{cases} \iff \begin{cases} x &= a - b \\ y &= a + b \\ z &= a - 3b \\ a + 3b &= 0 \end{cases} \iff \begin{cases} x &= -4b \\ y &= -2b \\ z &= -6b \end{cases}$$

Ainsi $F \cap G = \{(-4b, -2b, -6b) \mid b \in \mathbb{R}\} = \{(2c, c, 3c) \mid c \in \mathbb{R}\} = (2, 1, 3)\mathbb{R}$.

Exemple 36
Soient E un $\mathbb{K}$-espace vectoriel, et F, G, H des sous-espaces vectoriels de E. On suppose que

$$F \cap G \subset F \cap H, \quad F + G \subset F + H, \quad H \subset G.$$

Montrons que $H = G$.

Soit $x \in G$. Puisque $x \in G \subset F + G \subset F + H$, il existe $f \in F, h \in H$ tels que $x = f + h$.
On a alors $x \in G, h \in H \subset G$, donc, puisque G est un sous-espace vectoriel de E, $f = x - h \in G$.
D'où $f \in F$ et $f \in G$, donc $f \in F \cap G \subset F \cap H$, donc $f \in H$. Ainsi, $f \in H$ et $h \in H$, donc, puisque H est un sous-espace vectoriel de E, $x = f + h \in H$. Ceci montre $G \subset H$. Comme, de plus, par hypothèse, $H \subset G$, on conclut $H = G$.