Université Moulay Ismail
Faculté des sciences et techniques d'Er-Rachidia

Cours de

Algèbre 1

Licence MIP S1
Module : M112

Pr. SALHI Jawad

Scanné avec CamScanner

Algèbre1
Chapitre 2: Structures algébriques

Jawad SALHI

Faculté des Sciences et Techniques - Errachidia

A.U. 2020/2021

Plan

1. Lois de composition interne
2. Structure de groupe
3. Structure d'anneau
4. Corps

Scanné avec CamScanner

Lois de composition interne

Définition (Loi de composition interne et magma)

Soit E un ensemble non vide.

- On appelle loi (de composition) interne sur E, ou simplement loi sur E toute application de $E \times E$ dans E.
- On appelle magma tout couple $(E, \star)$ constitué d'un ensemble E et d'une loi interne $\star$ sur E.

Explication : Une loi interne, c'est ce que vous avez souvent appelé une "opération" jusqu'ici, une manière de transformer deux objets d'un certain ensemble en un troisième objet du même ensemble.

Méthode

Pour montrer qu'une loi $\star$ est une loi de composition interne sur un ensemble E, il faut montrer que : $\forall (x, y) \in E \times E,\ x \star y \in E$.

Lois de composition interne

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 $\mathbb{Z}$.*
- *Dans $\mathbb{N}^*$, l'exponentiation, c'est-à-dire l'application $(\mathbb{N}^*)^2 \to \mathbb{N}^*$ $(a, b) \mapsto a^b$, le PGCD ou le PPCM sont des lois internes.*
- *Etant donné un ensemble E, 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.*

Scanné avec CamScanner

Lois de composition interne : Propriétés éventuelles

Définition (Commutativité et associativité)

Soit $(E, \star)$ un magma.

- On dit que $(E, \star)$ est commutatif ou que $\star$ est commutative si : $\forall (x, y) \in E^2, x \star y = y \star x$
- On dit que $(E, \star)$ est associatif ou que $\star$ est associative si : $\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$.

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

▷ L'associativité permet en particulier le définition des puissances.

- Notation multiplicative : Pour tous $x \in E$ et $n \in \mathbb{N}^*$, on pose :
$$x^n = \overbrace{x \star \cdots \star x}^{n \text{ fois}}.$$
- Notation additive : Pour tous $x \in E$ et $n \in \mathbb{N}^*$, on pose :
$$nx = \overbrace{x \star \cdots \star x}^{n \text{ fois}}.$$

Lois de composition interne : Propriétés éventuelles

Exemples

- *Les magmas* $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, +)$, $(\mathbb{R}, \times)$, $(\mathbb{C}, +)$, $(\mathbb{C}, \times)$ *sont commutatifs et associatifs.*
- *Les magmas* $(\mathcal{P}(E), \cup)$ *et* $(\mathcal{P}(E), \cap)$ *sont commutatifs et associatifs.*
- *Le magma* $(E^E, \circ)$ *est associatif* $(f \circ g) \circ h = f(g \circ h)$ *et on peut écrire plus simplement* $f \circ g \circ h$. *Mais non commutatif si* E *possède au moins deux éléments. En effet, par exemple,* x *et* y *sont deux éléments distincts de* E *et si* $f : E \to E$ *est l'application constante égale à* x *et* $g : E \to E$ *est l'application constante égale à* y, *alors* $f \circ g$ *est constante égale à* x *et* $g \circ f$ *est constante égale à* y, *donc* $f \circ g \neq g \circ f$.
- *Dans* $\mathbb{N}^*$, *l'exponentiation, c'est-à-dire l'application* $(\mathbb{N}^*)^2 \to \mathbb{N}^*, (a, b) \mapsto a^b$, *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* $(a^b)^c = a^{bc}$.
- *Le magma* $(\mathbb{Z}, -)$ *n'est ni commutatif ni associatif.*

Scanné avec CamScanner

Lois de composition interne : Propriétés éventuelles

Définition (Distributivité d'une loi sur une autre)

Soient E un ensemble non vide et $\star$ et $\top$ deux lois de composition internes sur E.

$$\top \text{ est distributive sur} \star \Leftrightarrow \forall (x,y,z) \in \mathrm{E}^3, x\top(y\star z) = (x\top y)\star(x\top z) \text{ et } (y\star z)\top x = (y\top x)\star(z\top x).$$

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

- Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, 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, $f\circ(g+h) \neq f\circ g + f\circ h$.)

Lois de composition interne : Eléments particuliers

Définition (Elément neutre)

Soient $(E,\star)$ un magma et $e \in E$. On dit que e est un élément neutre de $(E,\star)$ (ou pour $\star$) si : $\forall x \in E, e\star x = x\star e = x$.
$\star$ admet un élément neutre dans $E \Leftrightarrow \exists e \in E / \forall x \in E, e\star x = x\star e = x$.

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

Théorème (Unicité de l'élément neutre)

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

Démonstration.

Si $e, e' \in E$ sont deux éléments neutres pour $\star$, alors : $e = e\star e' = e'$, i.e. $e = e'$. □

Scanné avec CamScanner

Lois de composition interne : Eléments particuliers

▷ On peut donc parler, quand il existe, de l'élément neutre de E plutôt que d'"un" élément neutre de E. On le note généralement 1_E ou 1 en notation multiplicative et 0_E ou 0 en notation additive.

Exemples

- *Les magmas* $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *admettent* 0 *pour élément neutre et les magmas* $(\mathbb{N}, \times)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$, $(\mathbb{C}, \times)$ *admettent* 1 *pour élément neutre. Le magma* $(\mathbb{N}^*, +)$, *en revanche, ne possède pas d'élément neutre.*
- *Le magma* $(E^E, \circ)$ *admet* Id_E *pour élément neutre.*
- *Dans* $\mathcal{P}(E)$, E *est élément neutre pour l'intersection et* $\emptyset$ *est élémet neutre pour la réunion.*

Lois de composition interne : Eléments particuliers

Définition (Elément absorbant)

Soient $(E, \star)$ un magma et $a \in E$.
a est élément absorbant pour $\star \Leftrightarrow \forall x \in E, a \star x = x \star a = a$.

Exemples

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

Scanné avec CamScanner

Lois de composition interne : Eléments particuliers

Définition (Elément symétrisable)

Soient $(E, \star)$ un magma possédant un élément neutre e. Soit $x \in E$.

- x admet un symétrique à gauche pour $\star \Leftrightarrow \exists x' \in E / x' \star x = e$.
- x admet un symétrique à droite pour $\star \Leftrightarrow \exists x' \in E / x \star x' = e$.
- x admet un symétrique pour $\star \Leftrightarrow \exists x' \in E / x \star x' = x' \star x = e$.
- x est symétrisable à gauche pour $\star$ si et seulement si x admet un symétrique à gauche pour $\star$.
- x est symétrisable à droite pour $\star$ si et seulement si x admet un symétrique à droite pour $\star$.
- x est symétrisable pour $\star$ si et seulement si x admet un symétrique pour $\star$.

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

Lois de composition interne : Eléments particuliers

Théorème

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

Démonstration.

Soit $x \in E$. Soient x' et x'' deux éléments symétriques de x. Alors, $x'' = e \star x'' = (x' \star x) \star x'' = x' \star (x \star x'') = x' \star e = x'$. □

▷ On peut donc parler du symétrique de x plutôt que d'"un" symétrique. On le note x^{-1} en notation multiplicative (et s'appelle l'inverse de x) et $-x$ en notation additive (et s'appelle l'opposé de x).

▷ Dans $(\mathbb{N}, +)$, seul 0 possède un inverse (ou plutôt un opposé). On pourrait se dire que 1 possède aussi un opposé, à savoir -1, mais : $-1 \notin \mathbb{N}$. Dans le monde $(\mathbb{N}, +)$, 1 n'a pas d'opposé.

Attention, donc : Un élément peut posséder un symétrique dans un contexte, mais pas dans un contexte plus restrictif.

Scanné avec CamScanner

Lois de composition interne : Eléments particuliers

Exemples

- *Dans* $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ *et* $(\mathbb{C}, +)$ *tout élément possède un opposé.*
- *Dans* $(\mathbb{N}, \times)$, *seul* 1 *possède un inverse. Dans* $(\mathbb{Z}, \times)$, *seuls* -1 *et* 1. *Dans* $(\mathbb{C}, \times)$, *tout le monde sauf* 0. *Dans* $(\mathbb{C}^*, \times)$, *en revanche, qui est bien un magma, tout élément possède un inverse.*
- *Les éléments symétrisables du magma* $(E^E, \circ)$ *sont exactement les bijections de* E *sur* E. *Le symétrique d'une bijection* f *pour la loi* $\circ$ *n'est autre que sa réciproque* f^{-1}.

Lois de composition interne : Eléments particuliers

Théorème

Soient $(E, \star)$ *un magma associatif et possédant un élément neutre* e. *Soient* x *et* y *deux éléments de* E. *Si* x *et* y *sont symétrisables, alors* $x \star y$ *l'est aussi et* $(x \star y)' = y' \star x'$.

Démonstration.

Soient x et y deux éléments symétrisables de E. Soient x' et y' leurs symétriques respectifs. Par associativité de la loi $\star$, on a :

$$(x \star y) \star (y' \star x') = x \star (y \star y') \star x' = x \star e \star x' = x \star x' = e$$

et

$$(y' \star x') \star (x \star y) = y' \star (x' \star x) \star y = y' \star e \star y = y' \star y = e.$$

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

Scanné avec CamScanner

Lois de composition interne : Eléments particuliers

Exemples

- *Dans* $\mathbb{C}$, *l'opposé* $-(z_1 + z_2)$ *de* $z_1 + z_2$ *est* $-z_1 - z_2$.
- *Dans* $\mathbb{C}^*$, *l'inverse* $\dfrac{1}{z_1 \times z_2}$ *de* $z_1 \times z_2$ *est* $\dfrac{1}{z_1} \times \dfrac{1}{z_2}$.
- *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* $g^{-1} \circ f^{-1}$*).*

Lois de composition interne : Eléments particuliers

Définition (Elément simplifiable ou régulier)

Soient $(E, \star)$ un magma et $x \in E$.

- x est simplifiable à gauche pour $\star$
  $\Leftrightarrow \forall (y, z) \in E^2, x \star y = x \star z \Rightarrow y = z$.
- x est simplifiable à droite pour $\star$
  $\Leftrightarrow \forall (y, z) \in E^2, y \star x = z \star x \Rightarrow y = z$.
- x est simplifiable (ou régulier) si et seulement si x est simplifiable à gauche et à droite.

Exemples

1. *Dans* $\mathbb{N}$ *:*
   - *tous les éléments sont réguliers pour l'addition,*
   - *tous les éléments non nuls sont réguliers pour la multiplication.*
2. *Dans* $\mathcal{P}(E)$*, seul* E *est régulier pour l'intersection.*

Scanné avec CamScanner

Lois de composition interne : Eléments particuliers

Théorème

Soient $(E, \star)$ un magma associatif et possédant un élément neutre e. Tout élément symétrisable est simplifiable.

Démonstration.

Soit $x \in E$ symétrisable. Soit x' son symétrique pour $\star$. Pour $(y, z) \in E^2$,

- si $x \star y = x \star z$ avec x symétrisable, alors :

$$y = e \star y = (x' \star x) \star y = x' \star (x \star y) = x' \star (x \star z) = (x' \star x) \star z = e \star z = z.$$

- si $y \star x = z \star x$ avec x symétrisable, alors :

$$y = y \star e = y \star (x \star x') = (y \star x) \star x' = (z \star x) \star x' = z \star (x \star x') = z \star e = z.$$

D'où le résultat. □

Lois de composition interne : Partie stable-loi induite

Définition (Partie stable par une loi)

Soient $(E, \star)$ un magma et A une partie de E. On dit que A est stable par $\star$ si :

$$\forall a, b \in A, a \star b \in A.$$

Dans ces conditions, $(A, \star)$ est lui-même un magma, si l'on note encore $\star$ la restriction de $\star$ à $A \times A$.
L'application

$$\begin{aligned} A \times A &\to A \\ (a, b) &\mapsto a \star b \end{aligned}$$

est appelée loi induite par $\star$ sur A.

Explication : Dire que A est stable par $\star$, c'est-à-dire que les calculs qu'on effectue via $\star$ sur les éléments de A ne sortent jamais de A. A est comme un sous-monde autonome à l'intérieur de E.

Scanné avec CamScanner

Lois de composition interne : Eléments particuliers

Exemples

- *Dans $\mathbb{C}$, les parties $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont à la fois stables par addition et stables par produit.*
- *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 $\mathbb{R}^{\mathbb{R}}$, l'ensemble des fonctions croissantes est stable par composition.*

Lois de composition interne : Eléments particuliers

Attention ! Soient $(E, \star)$ un magma et A une partie de E stable par $\star$. L'intérêt de la stabilité, c'est qu'alors $(A, \star)$ est un magma. Cela dit, les propriétés de $(E, \star)$ sont-elles transmises intactes à $(A, \star)$? Réponse : ça dépend.

- Si $(E, \star)$ est commutatif, alors oui, $(A, \star)$ l'est aussi car qui peut le plus peut le moins (s'il est vrai que : $x \star y = y \star x$ pour tous $x, y \in E$, c'est bien sûr vrai pour tous $x, y \in A$).
- Le même raisonnement vaut pour l'associativité (si $(E, \star)$ est associatif, $(A, \star)$ l'est aussi).
- Attention, en revanche, $(E, \star)$ peut posséder un élément neutre sans que $(A, \star)$ en possède un (pensez à $(\mathbb{N}, +)$ et $(\mathbb{N}^*, +)$).
- Egalement, un élément de A peut être symétrisable dans $(E, \star)$ sans l'être dans $(A, \star)$ (pensez à 2 dans $(\mathbb{Q}, \times)$ et $(\mathbb{Z}, \times)$).

Scanné avec CamScanner

Groupe

Définition (Groupe)

Soit G un ensemble non vide muni d'une loi de composition interne $\star$. $(G, \star)$ est un groupe si et seulement si

- $\star$ est associative.
- $\star$ possède un élément neutre dans G.
- tout élément de G possède un symétrique pour $\star$ dans G.

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

▷ En d'autres termes, on appelle groupe tout magma associatif possédant un élément neutre et dans lequel tout élément est symétrisable.

Groupe

On peut tirer plusieurs conséquences de cette définition :

- l'élément neutre est unique et chaque élément $x \in G$ admet un unique symétrique noté x'.
- Dans un groupe, tout élément étant symétrisable, on peut toujours simplifier facilement. Par exemple, pour tous éléments x, y et z de G :

$$(x \star y = x \star z) \Rightarrow (y = z) \quad \text{et} \quad (y \star x = z \star x) \Rightarrow (y = z)$$

Remarque

Généralement, quand on introduit un groupe $(G, \star)$ abstrait, on omet volontairement de mentionner la loi $\star$ pour alléger les notations. On dit alors : "Soit G un groupe". Par convention, on note alors généralement multiplicativement la loi de G, et même on se contente de noter xy le produit de x et y.

Scanné avec CamScanner

Groupe

Exemples

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ *et* $(\mathbb{C}, +)$ *sont des groupes commutatifs.*
- $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ *et* $(\mathbb{C}^*, \times)$ *sont des groupes commutatifs.*
- *En revanche,* $(\mathbb{Z}^*, \times)$ *n'est pas un groupe car* 2 *par exemple n'a pas d'inverse entier.*
- $(\mathcal{M}_n(\mathbb{K}), +)$ *est un groupe commutatif, mais pas* $(\mathcal{M}_n(\mathbb{K}), \times)$ *car toute matrice n'y est pas inversible. Le magma* $(GL_n(\mathbb{K}), \times)$*, en revanche, est quant à lui un groupe, mais non commutatif si* $n \geq 2$*. Voilà pourquoi on appelle* $GL_n(\mathbb{K})$ *un groupe linéaire !*

Groupe

Attention : Tout ce qui "brille" n'est pas forcément un groupe !
L'hypothèse sur l'existence d'un symétrique est souvent celle qui fait défaut.

▷ Des exemples pour vous en convaincre : $(\mathbb{Q}, \times)$, $(\mathbb{R}, \times)$ et $(\mathbb{C}, \times)$ ne sont pas des groupes car 0 n'est pas inversible pour la multiplication.

Remarque

Désormais, quand on parlera du groupe $\mathbb{C}$*, il s'agira toujours du groupe* $(\mathbb{C}, +)$*, et quand on parlera du groupe* $\mathbb{C}^*$*, il s'agira du groupe* $(\mathbb{C}^*, \times)$*. Même chose avec* $\mathbb{R}$ *et* $\mathbb{Q}$*. De la même manière, quand on parlera du groupe* $\mathcal{M}_n(\mathbb{K})$*, il s'agira du groupe* $(\mathcal{M}_n(\mathbb{K}), +)$*, et quand on parlera du groupe* $GL_n(\mathbb{K})$*, il s'agira du groupe* $(GL_n(\mathbb{K}), \times)$*.*

Scanné avec CamScanner

Groupe

Exercice

Soit G un groupe d'élément neutre e tel que $\forall x \in G, x^2 = e$. Montrer que G est abélien.

Solution

Suppposons que tout carré soit égal à l'élément neutre. Alors

$$xy = y^2xyx^2 = y(yxyx)x = y(yx)^2x = yex = yx.$$

Autre méthode : Soit $x, y \in G$. En utilisant le fait que pour tout $z \in G$ on a $z^2 = 1$, i.e. $z = z^{-1}$, on en déduit que

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

et G est abélien.

Groupe : groupe symétrique

Définition (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 $\mathcal{S}_E$. Le magma $(\mathcal{S}_E, \circ)$ est un groupe d'élément neutre Id_E.

Exercice

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

Scanné avec CamScanner

Groupe : sous-groupe

Définition (Sous-groupe)

Soit $(G, \star)$ un groupe et H une partie de G.
On dit, que H est un sous-groupe de G si H est **non vide**, **stable** pour la loi $\star$ et qui est un groupe pour la loi induite sur H par $\star$.

Exemples

- *$\{e\}$ et G sont des sous-groupes de $(G, \star)$ appelés sous-groupes triviaux du groupe $(G, \star)$. Les autres sous-groupes, s'il en existe, sont appelés sous-groupes propres de $(G, \star)$.*
- *$\{-1, 1\}$ est un sous-groupe de $(\mathbb{Z}, \times)$.*

Groupe : sous-groupe

Théorème (Elémént neutre et inverses dans un sous-groupe)

Soient $(G, \star)$ un groupe et H un sous-groupe de G.

1. *$e_G \in H$.*
2. *H est stable par passage au symétrique : $\forall x \in H, x' \in H$.*

Démonstration.

1. Notons e_H l'élément neutre de H. On a $e_H \star e_G = e_H$ car e_G est le neutre de $(G, \star)$. De plus, comme e_H est élémént neutre de H, on a $e_H \star e_H = e_H$ et donc : $e_H \star e_H = e_H \star e_G$. Or on peut simplifier par e_H car G est un groupe, donc : $e_H = e_G$ et enfin : $e_G \in H$.
2. Soit $x \in H$. Notons x'_H le symétrique de x dans H pour le distinguer du symétrique x' de x dans G. Alors : $x'_H = x'$, car $x'_H = e_G \star x'_H = (x' \star x) \star x'_H = x' \star (x \star x'_H) = x' \star e_H = x' \star e_G = x'$, donc : $x' \in H$.

□

Scanné avec CamScanner

Groupe : sous-groupe

On retiendra les caractérisations suivantes des sous-groupes d'un groupe $(G, \star)$ donné.

Théorème (Caractérisation des sous-groupes)

Soient $(G, \star)$ un groupe et H une partie de G.

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

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

Groupe : sous-groupe

Démonstration.

Montrons que : $(I) \Leftrightarrow (II)$.

$\Rightarrow$ Si H est un sous-groupe de G, alors H est stable par $\star$ et nous avons vu que : $e_G \in H$ et que H est stable par passage au symétrique. Bref, pour tout $x, y \in H$, on a : $x \star y' \in H$.

$\Leftarrow$ Supposons (II).

- Comme $e_G \in H$, alors d'après (II) : $\forall y \in H$, $y' = e_G \star y' \in H$, i.e. H est stable par passage au symétrique. Ce qui entraine, toujours d'après (II) : $\forall x, y \in H$, $x \star y = x \star (y')' \in H$, i.e. H est stable par $\star$.
- Il nous reste à montrer que H est un groupe pour la loi $\star$. En fait, l'associativité de G est transmise intacte à H. Ensuite, puisque $e_G \in H$, alors e_G est un élément neutre de H. Enfin, tout élément de H admet un symétrique dans H puisque H est stable par passage au symétrique.

□

Scanné avec CamScanner

Groupe : sous-groupe

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

En notation additive :

$$H \text{ est un sous-groupe de } (G,+) \Leftrightarrow \begin{cases} 0_G \in H \\ \forall (x,y) \in H^2, x+y \in H \\ \forall x \in H, -x \in H. \end{cases}$$

$$\Leftrightarrow \begin{cases} 0_G \in H \\ \forall (x,y) \in H^2, x-y \in H. \end{cases}$$

Groupe : sous-groupe

En notation multiplicative :

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

$$\Leftrightarrow \begin{cases} 1_G \in H \\ \forall (x,y) \in H^2, x \times y^{-1} \in H. \end{cases}$$

Scanné avec CamScanner

Groupe : sous-groupe

En pratique :

- C'est toujours les caractérisations précédentes qu'il faut utiliser pour montrer qu'une partie d'un groupe en est un sous-groupe.
- Pour montrer qu'un certain ensemble H muni d'une certaine loi est un groupe, il suffit souvent de montrer que H est un **sous**-groupe d'un autre groupe connu.

On retiendra la méthode suivante de caractérisation des sous-groupes d'un groupe donné.

Méthode (Prouver que H est une sous-groupe de G)

Une partie H d'un groupe donné $(G, \star)$ est un sous-groupe de $(G, \star)$ si et seulement si

$$e_G \in H \quad \text{et} \quad \forall (x, y) \in H^2,\ x \star y' \in H.$$

Groupe : sous-groupe

Exemples

- $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$ *est un sous-groupe de* $(\mathbb{C}^*, \times)$. *En effet,* $\mathbb{U} \subset \mathbb{C}^*$, $1 \in \mathbb{U}$ *et pour tous* $z_1, z_2 \in \mathbb{U}$, *on a* $|z_1 z_2^{-1}| = \dfrac{|z_1|}{|z_2|} = \dfrac{1}{1} = 1$ *donc* $z_1 z_2^{-1} \in \mathbb{U}$.
- *Pour tout entier naturel n non nul, l'ensemble* $\mathbb{U}_n = \{z \in \mathbb{C} : z^n = 1\}$ *(appelé ensemble des racines n-ièmes de l'unité) est un sous-groupe de* $(\mathbb{U}, \times)$. *En effet,* $\mathbb{U}_n \subset \mathbb{U}$ *(toute racine n-ième de l'unité est de module* 1*),* $1 \in \mathbb{U}_n$ *et, pour tous* $z_1, z_2 \in \mathbb{U}_n$, *on a* $(z_1 z_2^{-1})^n = \dfrac{z_1^n}{z_2^n} = \dfrac{1}{1} = 1$ *donc* $z_1 z_2^{-1} \in \mathbb{U}_n$.
- *Plus subtil : l'ensemble* $\Gamma = \bigcup_{n \in \mathbb{N}^*} \mathbb{U}_n$ *de toutes les racines de l'unité est un sous-groupe de* $(\mathbb{U}, \times)$.

Scanné avec CamScanner

Groupe : sous-groupe

Théorème

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

Démonstration.

Soient H et K deux sous-groupes. On a bien sûr $H \cap K \subset G$. De plus, d'après ce qui précède, H et K contiennent l'élément neutre e_G de G et donc $e_G \in H \cap K$. Soient x et y deux éléments de $H \cap K$. Alors :

$$\begin{cases} x, y \in H \\ x, y \in K \end{cases}, \text{ donc } \begin{cases} x \star y' \in H \\ x \star y' \in K \end{cases} \text{ et donc } x \star y' \in H \cap K. \text{ Ceci montre}$$

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

Remarque

Le résultat est faux dans le cas d'une réunion.

Groupe : sous-groupe

Exercice

Soient $(G, \star)$ un groupe et H_1, H_2 deux sous-groupes de G. On suppose que $H_1 \cup H_2$ est un sous-groupe de G. Montrer que $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Solution

Raisonnons par l'absurde et supposons que $H_1 \not\subset H_2$ et $H_2 \not\subset H_1$. Alors, il existe $x_1 \in H_1$, $x_1 \notin H_2$ et il existe $x_2 \in H_2$, $x_2 \notin H_1$. Comme $H_1 \cup H_2$ est un sous-groupe, $x_1 \star x_2 \in H_1 \cup H_2$. Si $x_1 \star x_2 \in H_1$, alors $x_2 = x_1' \star (x_1 \star x_2) \in H_1$, ce qui est absurde. De même, on parvient à une absurdité en supposant $x_1 \star x_2 \in H_2$. D'où le résultat.

▷ Remarquons que le dernier sous-groupe de l'exemple précédent, Γ, est la réunion de sous-groupes $\mathbb{U}_n$ pour n dans $\mathbb{N}^*$. Γ est tout de même un sous-groupe de $(\mathbb{C}^*, \times)$ car cette réunion est filtrante, c'est-à-dire que, $\forall (n, m) \in (\mathbb{N}^*)^2$, il existe $p \in \mathbb{N}^*$ tel que $\mathbb{U}_n \cup \mathbb{U}_m \subset \mathbb{U}_p$.

Scanné avec CamScanner

Groupe : sous-groupe

Exercice

Soit G un groupe. Montrer que les parties suivantes sont des sous-groupes de G :

1. $\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ ($\mathcal{Z}(G)$ s'appelle le centre de G).
2. $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ où $a \in G$ et H est un sous-groupe de G.

Groupe : sous-groupe

Solution

1. 1_G est élément de $\mathcal{Z}(G)$ car $1_G y = y 1_G = y$ pour tout $y \in G$. Soient $x_1, x_2 \in \mathcal{Z}(G)$. Alors, pour tout $y \in G$, on a $x_1 x_2 y = x_1 (x_2 y) = (x_1 y) x_2 = y x_1 x_2$ et donc $x_1 x_2 \in \mathcal{Z}(G)$. Enfin, si $x \in \mathcal{Z}(G)$, alors pour tout $y \in G$,

$$xy = yx \Longrightarrow xyx^{-1} = y \Longrightarrow yx^{-1} = x^{-1}y.$$

   On en déduit que $x^{-1} \in \mathcal{Z}(G)$ qui est donc un sous-groupe de G.
2. Puisque H est un sous-groupe de $G, 1_G \in H$ et donc $a1_G a^{-1} \in aHa^{-1}$. Mais $a1_G a^{-1} = 1_G$ et donc $1_G \in aHa^{-1}$. soient $x = aha^{-1}$ et $y = ah'a^{-1}$ deux éléments de aHa^{-1} avec donc $h, h' \in H$. On a $xy^{-1} = aha^{-1}(ah'a^{-1})^{-1} = aha^{-1}(ah'^{-1}a^{-1}) = ahh'^{-1}a^{-1} \in aHa^{-1}$ puisque $hh'^{-1} \in H$. aHa^{-1} est donc bien un sous-groupe de G.

Scanné avec CamScanner

Groupe : sous-groupe

Exercice

Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB = \{ab; a \in A, b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Groupe : sous-groupe

Solution

$\Rightarrow$ Supposons que AB est un sous-groupe de G et montrons que $AB = BA$. Soit $x = ab \in AB$. Alors $x^{-1} = (ab)^{-1} = b^{-1}a^{-1} \in AB$ et donc $b^{-1}a^{-1} = a'b'$ avec $a' \in A$ et $b' \in B$. Par passage à l'inverse, on obtient : $x = ab = b'^{-1}a'^{-1} \in BA$.
De même, si $y = ba \in BA$, alors $y^{-1} = a^{-1}b^{-1} \in AB$ et donc $y = (y^{-1})^{-1} \in AB$.
$\Leftarrow$ Supposons que $AB = BA$ et montrons que AB est un sous-groupe de G.

- Puisque A et B sont deux sous-groupes de G, alors $1_G \in A$ et $1_G \in B$ et donc $1_G = 1_G 1_G \in AB$.
- Soit $x = ab \in AB$ et $y = a'b' \in AB$. Alors, $xy = aba'b'$. Or, $ba' \in BA = AB$ et donc $ba' = a''b''$ avec $a'' \in A$ et $b'' \in B$. On en déduit que : $xy = aa''b''b' \in AB$.
- Soit $x = ab \in AB$. Alors, $x^{-1} = b^{-1}a^{-1} \in BA = AB$.

Scanné avec CamScanner

Groupe : sous-groupes de $\mathbb{Z}$

Proposition

Les sous-groupes de $(\mathbb{Z}, +)$ sont de la forme $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

L'ensemble $n\mathbb{Z}$ désigne l'ensemble des multiples de n :

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}.$$

Groupe : sous-groupes de $\mathbb{Z}$

Démonstration.

Fixons $n \in \mathbb{N}$. L'ensemble $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. En effet :

- $n\mathbb{Z} \subset \mathbb{Z}$, l'élément neutre 0 appartient à $n\mathbb{Z}$ et
- pour $x = nk$ et $y = nk'$ des éléments de $n\mathbb{Z}$, on a $x - y = n(k - k') \in n\mathbb{Z}$.

Réciproquement soit H un sous-groupe de $(\mathbb{Z}, +)$. Si $H = \{0\}$ alors $H = 0\mathbb{Z}$ et c'est fini. Sinon H contient au moins un élément non-nul et positif et notons $n = \min\{h > 0 \mid h \in H\}$. Alors $n > 0$. Comme $n \in H$ et H est un groupe alors pour tout $k \in \mathbb{Z}$ on a $kn \in H$. Ainsi $n\mathbb{Z} \subset H$.
D'autre part, soit $h \in H$. Écrivons la division euclidienne de h par n :

$$h = kn + r, \quad \text{avec } k, r \in \mathbb{Z} \text{ et } 0 \leq r < n.$$

Or $h \in H$ et $kn \in H$ donc $r = h - kn \in H$. Par la définition de n, nécessairement $r = 0$, i.e. $h = kn$ et donc $h \in n\mathbb{Z}$. Conclusion $H = n\mathbb{Z}$. □

Scanné avec CamScanner

Groupe : Morphismes de groupes

Définition (Morphisme de groupes)

Soient $(G, \star)$ et $(G', \top)$ deux groupes. Une application $f : G \to G'$ est un morphisme de groupes si pour tous $x, y \in G$, :

$$f(x \star y) = f(x) \top f(y).$$

Si f est bijective, on dit que f est un isomorphisme de groupes ; si de plus $G' = G$, on dit que f est un automorphisme du groupe G.

- Toute proposition mathématiques du genre "Le machin des trucs et le truc des machins" cache un morphisme de groupes. Par exemple, l'exponentielle d'une somme et le produit des exponentielles, ou le carré d'un produit est le produit des carrés.

Groupe : Morphismes de groupes

Exemples

- *La fonction $x \mapsto x^2$ est un morphisme de groupes de $\mathbb{R}_+^*$ dans lui même, et c'est un automorphisme de réciproque $x \mapsto \sqrt{x}$.*
- *L'exponentielle complexe est un morphisme de groupes de $\mathbb{C}$ dans $\mathbb{C}^*$.*
- *La fonction logarithme est un morphisme de groupes de $\mathbb{R}_+^*$ dans $\mathbb{R}$, et c'est même un isomorphisme de réciproque la fonction exponentielle sur $\mathbb{R}$.*
- *Pour tout corps $\mathbb{K}$, le déterminant est un morphisme de groupes de $GL_n(\mathbb{K})$ dans $\mathbb{K} \setminus \{0\}$.*

Scanné avec CamScanner

Groupe : Morphismes de groupes

Ici, pour $x \in G$, x^{-1} désigne le symétrique de x dans le groupe. De même, dans le groupe G', nous noterons le symétrique de $f(x)$ par $(f(x))^{-1}$.

Proposition

Soit $f : (G, \star) \to (G', \top)$ un morphisme de groupes alors :

1. $f(e_G) = e_{G'}$,
2. *pour tout $x \in G$, $f(x^{-1}) = (f(x))^{-1}$.*

Démonstration.

1. On a $f(e_G) = f(e_G \star e_G) = f(e_G) \top f(e_G)$. En composant (à droite par exemple) par $(f(e_G))^{-1}$, on obtient : $e_{G'} = f(e_G)$.
2. Soit $x \in G$. On a $x \star x^{-1} = e_G$ et donc $f(x \star x^{-1}) = f(e_G)$. Cela entraine que $f(x) \top f(x^{-1}) = e_{G'}$ et en composant à gauche par $(f(x))^{-1}$, on obtient : $f(x^{-1}) = (f(x))^{-1}$.

□

Groupe : Morphismes de groupes

Proposition

- *Soient deux morphismes de groupes $f : (G, \star) \to (G', \top)$ et $g : (G', \top) \to (G'', \Delta)$. Alors $g \circ f : G \to G''$ est un morphisme de groupes.*
- *Si $f : (G, \star) \to (G', \top)$ est un morphisme bijectif (isomorphisme) alors $f^{-1} : (G', \top) \to (G, \star)$ est aussi un morphisme de groupes.*

Démonstration.

La première partie est facile. Montrons la deuxième : Soit $y, y' \in G'$.
Comme f est bijective, alors $\exists x, x' \in G$ tel que $f(x) = y$ et $f(x') = y'$.
Alors,
$f^{-1}(y \top y') = f^{-1}(f(x) \top f(x')) = f^{-1}(f(x \star x')) = x \star x' = f^{-1}(y) \star f^{-1}(y')$.
D'où, f^{-1} est un morphisme de G' vers G. □

Scanné avec CamScanner

Groupe : Morphismes de groupes

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

Définition (Noyau)

Le noyau de f est

$$Ker(f) = \{x \in G \mid f(x) = e_{G'}\}.$$

C'est donc un sous-ensemble de G. En terme d'image réciproque nous avons par définition $Ker(f) = f^{-1}(\{e_{G'}\})$.

Attention ! la notation f^{-1} ici désigne l'image réciproque, et ne signifie pas que f est bijective.

Définition (Image)

L'image de f est

$$Im(f) = \{f(x) \mid x \in G\}.$$

C'est donc un sous-ensemble de G' et en terme d'image directe nous avons $Im(f) = f(G)$.

Groupe : Morphismes de groupes

Proposition

Soit $f : (G, \star) \to (G', \Delta)$ un morphisme de groupes.

1. *$Ker(f)$ est un sous-groupe de G.*
2. *$Im(f)$ est un sous-groupe de G'.*

Scanné avec CamScanner

Démonstration.

1. Montrons que le noyau est un sous-groupe de G.
   - $f(e_G) = e_{G'}$ donc $e_G \in \operatorname{Ker} f$.
   - Soient $x, y \in \operatorname{Ker} f$. Alors $f\left(x \star y^{-1}\right) = f(x) \Delta f\left(y^{-1}\right) = f(x) \Delta \left(f(y)\right)^{-1} = e_{G'} \Delta e_{G'}^{-1} = e_{G'}$ et donc $x \star y^{-1} \in \operatorname{Ker} f$.
2. Montrons que l'image est un sous-groupe de G'.
   - $f(e_G) = e_{G'}$ donc $e_{G'} \in \operatorname{Im} f$.
   - Soient $z_1, z_2 \in \operatorname{Im} f$. Il existe alors $x_1, x_2 \in G$ tels que $f(x_1) = z_1, f(x_2) = z_2$. Alors $z_1 \Delta z_2^{-1} = f(x_1) \Delta \left(f(x_2)\right)^{-1} = f(x_1) \Delta f\left(x_2^{-1}\right) = f\left(x_1 \star x_2^{-1}\right) \in \operatorname{Im} f$.

□

Proposition

Soit $f : (G, \star) \to (G', \Delta)$ un morphisme de groupes.

1. *f est injectif si et seulement si $Ker(f) = \{e_G\}$.*
2. *f est surjectif si et seulement si $Im(f) = G'$.*

On en déduit la méthode suivante.

Méthode (Prouver l'injectivité d'un morphisme de groupes)

Dans la pratique, pour établir qu'un morphisme $f : (G, \star) \to (G', \Delta)$ est injectif, on montre que son noyau est réduit à l'élément neutre du groupe de départ, ce qui revient à prouver que l'équation $f(x) = e_{G'}$ admet dans G l'unique solution $x = e_G$.

Scanné avec CamScanner

Démonstration.

1. Supposons f injective. Soit $x \in \operatorname{Ker} f$, alors $f(x) = e_{G'}$ donc $f(x) = f(e_G)$ et comme f est injective alors $x = e_G$. Donc $\operatorname{Ker} f = \{e_G\}$.
   Réciproquement supposons $\operatorname{Ker} f = \{e_G\}$. Soient $x, y \in G$ tels que $f(x) = f(y)$ donc $f(x)\Delta\left(f(y)\right)^{-1} = e_{G'}$, d'où $f(x)\Delta f\left(y^{-1}\right) = e_{G'}$ et donc $f\left(x \star y^{-1}\right) = e_{G'}$. Ceci implique que $x \star y^{-1} \in \operatorname{Ker} f$.
   Comme $\operatorname{Ker} f = \{e_G\}$ alors $x \star y^{-1} = e_G$ et donc $x = y$. L'application f est par conséquent injective.
2. La proposition est claire et valable pour toute application f de G dans G' qu'il s'agisse d'un morphisme ou non.

□

Théorème (Image d'un sous-groupe par un morphisme de groupes)

Soient $(G, \star)$ et (G', Δ) deux groupes, H un sous-groupe de G et $\varphi : G \to G'$ un morphisme de groupes. L'image $\varphi(H)$ de H par φ est un sous-groupe de G'.

- Dans le cas particulier où φ est injectif, la restriction $\varphi_{|H}$ est un isomorphisme de H sur $\varphi(H)$. On peut de cette manière identifier H à un sous-groupe de G', en l'occurence $\varphi(H)$.

Démonstration.

D'abord : $e_{G'} = \varphi(e_G) \in \varphi(H)$ car $e_G \in H$. Ensuite, pour tous $x', y' \in \varphi(H)$, disons : $x' = \varphi(x)$ et $y' = \varphi(y)$ avec $x, y \in G$, on a : $x'\Delta y'^{-1} = \varphi(x)\Delta\varphi(y)^{-1} = \varphi(x)\Delta\varphi(y^{-1}) = \varphi(x \star y^{-1}) \in \varphi(H)$ car $x \star y^{-1} \in H$.

□

Scanné avec CamScanner

Groupe : Morphismes de groupes

Exercice

Soit G un groupe multiplicatif et $f : \begin{array}{c} G \to G \\ x \mapsto x^{-1} \end{array}$ une application.

Montrer que f est un morphisme de groupes si et seulement si G est abélien.

Solution

- Supposons que f est un morphisme de groupes. Pour tous $g_1, g_2 \in G$, on a

$$g_1 g_2 = f(g_1^{-1}) f(g_2^{-1}) = f(g_1^{-1} g_2^{-1}) = (g_1^{-1} g_2^{-1})^{-1} = g_2 g_1$$

  et G est abélien.
- Réciproquement, supposons que G est abélien. Soit $g_1, g_2 \in G$. On a $f(g_1 g_2) = (g_1 g_2)^{-1} = g_2^{-1} g_1^{-1} = g_1^{-1} g_2^{-1} = f(g_1) f(g_2)$ et donc f est un morphisme de groupes.

Groupe : Morphismes de groupes

Exercice

Soit G un groupe multiplicatif et $f : \begin{array}{c} G \to G \\ x \mapsto x^2 \end{array}$ une application. Montrer que f est un morphisme de groupes si et seulement si G est abélien.

Exercice

Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Solution

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$. $Im(f)$ est un sous-groupe de $\mathbb{Z}$ et donc $Im(f) = n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$. Supposons que $n \geq 1$. Soit x un antécédant de n. On obtient alors :
$2f(\frac{x}{2}) = f(x) = n$ et donc $\frac{n}{2} = f(\frac{x}{2}) \in n\mathbb{Z}$, ce qui est absurde. On a donc $n = 0$ et f est nul.

Scanné avec CamScanner

Groupe : Théorème de Lagrange

Définition (Ordre d'un groupe)

Si G est un groupe fini, $\text{Card}(G)$ s'appelle l'ordre de G.

Le résultat suivant est un théorème fondamental en théorie des groupes : le cardinal d'un sous-groupe H d'un groupe **fini** $(G, \star)$ divise le cardinal de G.

Théorème (Lagrange)

Soient G un groupe fini et H un sous-groupe de G. Alors, l'ordre de H divise l'ordre de G.

Groupe : Théorème de Lagrange

Démonstration.

La relation $x\mathcal{R}y \iff x^{-1}y \in H$ est une relation d'équivalence. Si on note $\bar{x}$ la classe de $x \in G$, on a $\bar{x} = xH = \{xz, z \in H\}$. En effet :

$$y \in \bar{x} \iff x\mathcal{R}y \iff x^{-1}y \in H \iff y \in xH.$$

Pour tout $x \in G$, l'application $H \to xH, \quad y \mapsto xy$ est une bijection comme on le vérifie facilement, donc $\text{Card}(xH) = \text{Card}(H)$. Ainsi, les classes ont toutes $\text{Card}(H)$ éléments. Les classes d'équivalences formant une partition de G, on a donc $\text{Card}(G) = n\,\text{Card}(H)$ où $n = \text{Card}(G/\mathcal{R})$ désigne le nombre de classes d'équivalence. □

Scanné avec CamScanner

Groupe : Théorème de Lagrange

Remarque

- *Les classes utilisées dans la preuve du théorème (de la forme xH) sont appelées classes à gauche suivant le sous-groupe H. On aurait aussi pu considérer la relation d'équivalence définie par $x\mathcal{R}y \iff xy^{-1} \in H$, dont les classes sont de la forme Hx et sont appelées classes à droite suivant H.*
- *L'entier* $\mathrm{Card}(G/\mathcal{R})$ *est appelé indice de H dans G et noté* $[G : H]$. *On a*

$$\mathrm{Card}(G) = [G : H] \times \mathrm{Card}(H).$$

Anneau

Définition (Anneau)

Soit A un ensemble non vide muni de deux lois de composition internes, une loi $+$ appelée addition et une loi $\times$ appelée multiplication.

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

L'anneau est commutatif si et seulement si $\times$ est commutative.

Scanné avec CamScanner

Anneau

Exemples

- $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ *sont des anneaux commutatifs.*
- $\mathcal{M}_n(\mathbb{K}, +, \times)$ *est un anneau non commutatifs si* $n \geq 2$.

Remarque

Comme avec les groupes, on allège souvent les notations. Quand on écrit "Soit A un anneau", il est sous-entendu que l'addition est notée $+$ *et la multiplication* $\times$ *(mais souvent on omet le* $\times$*). Pour tout* $a \in A$*, rappelons que :* $na = \underbrace{a + \cdots + a}_{n \text{ fois}}$ *et* $a^n = \underbrace{a \times \cdots \times a}_{n \text{ fois}}$ *si* $n \in \mathbb{N}$ *et*

$na = \underbrace{(-a) + \cdots + (-a)}_{-n \text{ fois}}$, *si* $n \in \mathbb{Z} \setminus \mathbb{N}$.

Anneau

Théorème (Régles de calcul dans un anneau)

Soit $(A, +, \times)$ *un anneau et* $a, b \in A$*. On note* 0_A *l'élément neutre de A pour* $+$ *et* 1_A *l'élément neutre de A pour* $\times$*.*

1. $a \times 0_A = 0_A \times a = 0_A$.
2. *Pour tout* $n \in \mathbb{Z}$ *:* $n \times (a \times b) = (n \times a) \times b = a \times (n \times b)$*. En particulier :* $-(a \times b) = (-a) \times b = a \times (-b)$.
3. $(-a) \times (-b) = a \times b$*. En particulier :* $(-1_A)^2 = 1_A$.
4. *Pour tout* $n \in \mathbb{N}$*, si a et b commutent :*

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k} \quad \textit{(formule du binôme)} \quad \textit{et}$$

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

Scanné avec CamScanner

Démonstration.

1. Soit $a \in A$. On a
   $a \times 0_A + a \times 0_A = a \times (0_A + 0_A) = a \times 0_A = a \times 0_A + 0_A$, car $\times$ est distributive sur $+$. Comme, $(A, +)$ est un groupe, alors tout élément est simplifiable. Ainsi, on simplifie par $a \times 0_A$ dans le groupe $(A, +)$ pour obtenir : $a \times 0_A = 0_A$. De même : $0_A \times a = 0_A$.
2. En utilisant la distributivité, on a pour tout $n \in \mathbb{N}$:
   $n \times (a \times b) = \overbrace{(a \times b) + \cdots + (a \times b)}^{n \text{ fois}} = a \times (\overbrace{b + \cdots + b}^{n \text{ fois}}) = a \times (n \times b)$.
   Pour $n = -1$: $a \times b + a \times (-b) = a \times (b - b) = a \times 0_A = 0_A$, donc : $-(a \times b) = a \times (-b)$. De même, on a $-(a \times b) = (-a) \times b$.
   Finalement, pour $n \in \mathbb{Z}$ négatif, il suffit de travailler avec $-n \in \mathbb{N}$.
3. $(-a) \times (-b) - (a \times b) = (-a) \times (-b) + (-a) \times b =$
   $(-a) \times (-b + b) = (-a) \times 0_A = 0_A$. D'où le résultat.

□

Dans un anneau A, est-il possible d'avoir : $0_A = 1_A$?

▷ Si c'est le cas, pour tout $a \in A$: $a = a \times 1_A = a \times 0_A = 0_A$, donc :

$$A = \{0_A\}.$$

Un tel anneau est qualifié d'anneau nul.

Scanné avec CamScanner

Anneau : Anneau intègre

Définition (Anneau intègre)

Soit A un anneau. On dit que A est intègre si A est **non nul** et si :

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

ou encore, par contraposition, si

$$\forall a, b \in A, \quad (a \neq 0_A \quad \text{et} \quad b \neq 0_A \Rightarrow ab \neq 0_A).$$

Attention : Tout anneau n'est pas intègre. Et que se passe-t-il quand un anneau n'est pas intègre ?

▷ Il n'est alors pas forcément vrai que pour tous $a, b, x, y \in A$:

$$ax = ay \Rightarrow a = 0_A \quad \text{ou} \quad x = y$$

ni que

$$a^2 = b^2 \Rightarrow a = b \quad \text{ou} \quad a = -b.$$

Anneau : Anneau intègre

Exemples

- *Les anneaux $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont intègres.*
- *L'anneau $\mathcal{M}_n(\mathbb{K})$ en revanche ne l'est pas pour $n \geq 2$. En effet, nous savons que le produit de matrices non nulles peut être nul. Par exemple :*

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Exercice (Anneau de Boole)

Soit A un anneau tel que tout élément de A soit idempotent (i.e. $\forall x \in A, x^2 = x$).

1. Si $x \in A$ montrer que $2x = 0$. Montrer que A est commutatif.
2. Montrer que si $x, y \in A$ alors $xy(x + y) = 0$. Que dire si A est intègre ?

Scanné avec CamScanner

Anneau : Anneau intègre

Solution

1. Soit $x \in A$. Alors $(2x)^2 = 2x$ donc $4x^2 = 2x$, ce qui entraine $4x = 2x$ et donc $2x = 0$. Ce qui s'écrit encore $x = -x$.
   Montrons que A est commutatif. Soit $x, y \in A$, alors $x + y \in A$. Ainsi, par définition de A, on obtient $(x + y)^2 = x + y$ et donc $x^2 + xy + yx + y^2 = x + y = x^2 + y^2$. D'où, $xy + yx = 0$ et donc $xy = -yx = yx$. Ce qui montre que A est commutatif.
2. Soit $x, y \in A$, alors $xy(x + y) = xyx + xy^2 = x^2y + xy^2 = 2xy = 0$. Sopposons que A est intègre. Alors A au plus deux éléments. En effet, sinon il existe $x, y \in A$ distincts et différents de 0. Donc $(x + y) \neq 0$ (car sinon $x = -y = y$) et A étant intègre $xy(x + y) \neq 0$, absurde.

Anneau : Groupe des inversibles d'un anneau

Remarque

Par définition, tout anneau est en particulier un groupe pour son addition, donc quand on parle des éléments inversibles d'un anneau, c'est toujours aux ***éléments inversibles pour la multiplication*** *qu'on fait référence.*

Définition (Inversible de A)

Soit A un anneau. Un élément $a \in A$ est dit inversible dans A (on dit parfois une unité de A) s'il existe $a' \in A$ (nécessairement unique) tel que l'on ait $a'a = aa' = 1_A$. Si a est inversible, l'élément a' tel que $a'a = aa' = 1_A$ s'appelle l'inverse de A et se note a^{-1}.
On note $\mathcal{U}(A)$ ou $A^\times$ l'ensemble des éléments inversibles de A.

▷ On ne confondra pas les ensembles A^* et $A^\times$ respectivement ensemble des éléments non nuls de A et ensemble des unités de A.

Scanné avec CamScanner

Anneau : Groupe des inversibles d'un anneau

Théorème (Groupe des inversibles d'un anneau)

Soit A un anneau. L'ensemble des éléments inversibles de A est un groupe pour la multiplication.

Démonstration.

- Il est facile de vérifier que $\mathcal{U}(A)$ est stable par produit. En effet, si $u, v \in \mathcal{U}(A)$, alors uv est inversible, d'inverse $v^{-1}u^{-1}$. Ainsi, $(\mathcal{U}(A), \times)$ est un magma.
- La multiplication est associative sur A, donc a fortiori sur $\mathcal{U}(A)$.
- Ensuite : $1_A 1_A = 1_A$, donc 1_A est inversible dans A, donc $1_A \in \mathcal{U}(A)$.
- Si $u \in \mathcal{U}(A)$, alors $u^{-1} \in \mathcal{U}(A)$ car u^{-1} est inversible d'inverse u. Ainsi, tout élément de $\mathcal{U}(A)$ est inversible dans $\mathcal{U}(A)$.

□

Anneau : Groupe des inversibles d'un anneau

Exemples

- $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$. *En effet,* $n \in \mathcal{U}(\mathbb{Z})$ *si et seulement si il existe* $m \in \mathbb{Z}$ *tel que* $nm = 1$, *ce qui impose* $|n| = 1$ *et donc* $n = -1, 1$. *Il est clair que seuls* 1 *et* -1 *sont des unités de* $(\mathbb{Z}, +, \times)$.
- $\mathcal{U}(\mathbb{Q}) = \mathbb{Q}^*$, $\mathcal{U}(\mathbb{R}) = \mathbb{R}^*$, $\mathcal{U}(\mathbb{C}) = \mathbb{C}^*$ *et* $\mathcal{U}(\mathcal{M}_n(\mathbb{K})) = GL_n(\mathbb{K})$.

Scanné avec CamScanner

Anneau : Sous-anneau

Définition (Sous-anneau)

Soient A un anneau et B une partie de A **stable par addition et produit**. On dit que B est un sous-anneau de A si B **contient** 1_A et si B est un anneau pour les lois de A.

Théorème (Caractérisation des sous-anneaux)

Soient A un anneau et B une partie de A. Alors B est un sous-anneau de A si et seulement si

$$(*)\begin{cases} 1_A \in B \\ B \text{ est stable par différence.} \\ B \text{ est stable par produit.} \end{cases}$$

Anneau : Sous-anneau

Démonstration.

Les conditions dans $(*)$ sont clairement nécessaires. Réciproquement, supposons ces propriétés vérifiées. On a $1_A \in B$ et et la condition $\forall (b, b') \in B, b - b' \in B$ implique que $(B, +)$ est un sous-groupe additif de $(A, +)$. La propriété $\forall (b, b') \in B, b \times b' \in B$ prouve que B est stable par $\times$, ce qui achève la démonstration car la distributivité de $\times$ par rapport à $+$ et l'associativité de $\times$ sur B découlent de la structure d'anneau $(A, +, \times)$. □

On retiendra cette caractérisation des sous-anneaux d'un anneau $(A, +, \times)$ donné.

Méthode (Prouver que B est un sous-anneau de $(A, +, \times)$)

Une partie B de A est un sous-anneau de $(A, +, \times)$ si et seulement si

$$1_A \in B \quad \text{et} \quad \forall (b, b') \in B,\ b - b' \in B \text{ et } bb' \in B.$$

Scanné avec CamScanner

Anneau : Sous-anneau

Exemples

$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ *est un sous-anneau de* $(\mathbb{C}, +, \times)$.

- *On a* $1 = 1 + 0 \times i$ *donc* $1 \in \mathbb{Z}[i]$. *Soient* z_1 *et* z_2 *dans* $\mathbb{Z}[i]$. *Il existe* a_1, b_1, a_2 *et* b_2 *dans* $\mathbb{Z}$ *tels que* $z_1 = a_1 + ib_1$ *et* $z_2 = a_2 + ib_2$. *On a alors*

$$z_1 - z_2 = (a_1 - a_2) + i(b_1 - b_2) \quad et \quad z_1 z_2 = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)$$

et comme $a_1 - a_2, b_1 - b_2, a_1 a_2 - b_1 b_2$ *et* $a_1 b_2 + a_2 b_1$ *appartiennent à* $\mathbb{Z}$, $z_1 - z_2 \in \mathbb{Z}[i]$ *et* $z_1 z_2 \in \mathbb{Z}[i]$.

$\mathbb{Z}[i]$ est appelé le sous-anneau des entiers de Gauss. Il est utile en arithmétique.

Anneau : Sous-anneau

Exercice

Déterminer $\mathcal{U}(\mathbb{Z}[i])$.

Solution

Soit $z = a + ib \in \mathcal{U}(\mathbb{Z}[i])$, où $a, b \in \mathbb{Z}$. Alors, il existe $z' = a' + ib' \in \mathbb{Z}[i]$ tel que $zz' = 1$. Donc $|z|^2|z'|^2 = 1$. Or, comme $z, z' \in \mathbb{Z}[i]$, alors $|z|^2, |z'|^2 \in \mathbb{N}$. Ainsi : $|z|^2 = |z'|^2 = 1$. Donc $a^2 + b^2 = 1$ et puisque $a, b \in \mathbb{Z}$, alors

$$\begin{cases} a^2 = 1 \text{ et } b^2 = 0 \\ \text{ou} \\ a^2 = 0 \text{ et } b^2 = 1 \end{cases}$$

et donc $z \in \{-1, 1, i, -i\}$. D'où $\mathcal{U}(\mathbb{Z}[i]) \subset \{-1, 1, i, -i\}$.
Inversement, il est facile de vérifier que $\{-1, 1, i, -i\} \subset \mathcal{U}(\mathbb{Z}[i])$. D'où l'égalité.

Scanné avec CamScanner

Anneau : Elément nilpotent

Définition (Elément nilpotent)

Soit A un anneau. Un élément $a \in A$ est dit nilpotent si $\exists n \in \mathbb{N}^*$ tel que $a^n = 0_A$. Dans ce cas, le plus petit p (existe) vérifiant cette propriété est appelé l'indice de nilpotence de a.

Exercice

Montrer que si $a \in A$ est nilpotent, alors $1_A - a \in \mathcal{U}(A)$.

Solution

Soit p l'indice de nilpotence de a. On a

$1_A = 1_A - a^p = (1_A - a)\sum_{k=0}^{p-1} a^k = \sum_{k=0}^{p-1} a^k(1_A - a)$. Donc $1_A - a \in \mathcal{U}(A)$ et

$(1_A - a)^{-1} = \sum_{k=0}^{p-1} a^k$.

Anneau : Morphismes d'anneaux

Définition (Morphisme d'anneaux)

Soient $(A, +, \times)$ et $(B, \star, \Delta)$ deux anneaux et $f : A \to B$ une application. On dit que f est un morphisme d'anneaux si :

(i) $f : (A, +) \to (B, \star)$ est un morphisme de groupes.

(ii) $\forall a, b \in A : f(a \times b) = f(a)\Delta f(b)$.

(iii) $f(1_A) = 1_B$.

Si de plus f est bijective, on dit alors que f est un isomorphisme d'anneaux.

Cas particuliers :

- Un morphisme de A vers A est appelé un endomorphisme de l'anneau A.
- Un isomorphisme de A dans A est appelé un automorphisme de l'anneau A.

Scanné avec CamScanner

Anneau : Morphismes d'anneaux

Proposition

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

(i) *L'image directe d'un sous-anneau de A est un sous-anneau de B.*

(ii) *$Im(f) = f(A)$ est un sous-anneau de B.*

(iii) *L'image réciproque d'un sous-anneau de B est un sous-anneau de A.*

Proposition

Soient $f : A \to B$, $g : B \to C$ deux morphismes d'anneaux. Alors :

1. *$g \circ f : A \to C$ est un morphisme d'anneaux.*
2. *Si f est un isomorphisme d'anneaux, alors l'application réciproque $f^{-1} : B \to A$ est un isomorphisme d'anneaux.*

Corps

Définition (Corps)

On appelle corps tout anneau commutatif non nul dans lequel tout élément non nul est inversible.

▷ Autrement dit, un corps est un anneau K tel que $\mathcal{U}(K) = K \setminus \{0_K\}$.
Explication : L'énorme différence entre un anneau et un corps, c'est que dans un anneau on ne peut pas diviser comme on veut par un élément non nul. Dans un corps c'est possible. En particulier, **tout corps est un anneau intègre**, car si : $ab = 0_A$ avec $a \neq 0_A$, alors : $b = 0_A$. En effet, comme $a \neq 0_A$, a admet un inverse pour $\times$ noté a^{-1}. Ainsi :
$ab = 0_A \Rightarrow a^{-1}ab = a^{-1} \times 0_A \Rightarrow 1_A \times b = 0_A \Rightarrow b = 0_A$.

Exemples

Les anneaux $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps, mais pas $\mathbb{Z}$ car :
$\mathcal{U}(\mathbb{Z}) = \{-1, 1\} \neq \mathbb{Z}^*$.

Scanné avec CamScanner

Corps

Définition (Sous-corps)

Si K est un corps, une partie L de K est un sous-corps de K si L est un sous-anneau de K qui est un corps. Autrement dit, L est un sous-corps de K si et seulement si

- $1_K \in L$.
- pour tous $a, b \in L$, $a - b \in L$.
- pour tous $a, b \in L$, $ab \in L$.
- pour tout $a \in L$ non nul, on a $a^{-1} \in L$.

Corps

Exercice

Soient $(K, +, \cdot)$ et $(L, +, \cdot)$ deux corps et soit $f : K \to L$ un morphisme d'anneaux.

1. Montrer que si $x \in K \setminus \{0_K\}$, alors $f(x)$ est inversible et déterminer son inverse.
2. En déduire qu'un morphisme de corps est injectif.

Solution

1. Soit $x \in K \setminus \{0_K\}$. Alors on a $x \cdot x^{-1} = 1_K$. On applique f à cette identité, et en utilisant que f est un morphisme d'anneaux, on trouve $f(x) \cdot f\left(x^{-1}\right) = 1_L$. Ainsi, $f(x)$ est inversible, d'inverse $f\left(x^{-1}\right)$.
2. Il suffit de démontrer que le noyau de f est réduit à 0_K. Mais si $f(x) = 0$, alors $x \notin K \setminus \{0_K\}$ d'après la question précédente, et donc $x = 0$.

Scanné avec CamScanner

Corps

Exercice

Montrer que tout anneau intègre commutatif et fini est un corps.

Solution

Soit $a \in A$ non nul. L'application $\mu_a \mid \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array}$ est injective. En effet, puisque A est un anneau intègre et a est non nul, pour tous $x, y \in A$, on a

$$\mu_a(x) = \mu_a(y) \Longrightarrow ax = ay \Longrightarrow ax - ay = 0 \Longrightarrow a(x-y) = 0 \Longrightarrow x = y.$$

Et comme A est un ensemble fini, toute injection de A dans A est une bijection. Ainsi μ_a est bijective. Soit $b \in A$ l'antécédent de 1 par μ_a. Alors : $ab = \mu_a(b) = 1$. Et puisque A est un anneau commutatif, on a aussi $ba = 1$ et donc b est l'inverse de a. Ainsi A est un corps.

Corps

Exercice

Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note :

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a, b) \in \mathbb{Q}^2\}.$$

Montrer que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un corps.

Scanné avec CamScanner

Solution

On va montrer qu'il s'agit d'un sous-corps de $(\mathbb{R}, +, \times)$. Remarquons d'abord que $\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$ et que $1 \in \mathbb{Q}[\sqrt{d}]$. soient $x, y \in \mathbb{Q}[\sqrt{d}]$. On les écrit $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$. Alors :

$$x - y = (a - a') + (b - b')\sqrt{d}$$
$$xy = (aa' + dbb') + (ab' + a'b)\sqrt{d}$$

ce qui prouve que $x - y$ et $xy \in \mathbb{Q}[\sqrt{d}]$. D'autre part, si $x \neq 0$, alors

$$\frac{1}{x} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$

et donc $\frac{1}{x} \in \mathbb{Q}[\sqrt{d}]$. Remarquons qu'il était possible de multiplier par la quantité conjuguée qui est non nulle car $\sqrt{d} \notin \mathbb{Q}$. D'où le résultat.

Exercice (Endomorphisme du corps $\mathbb{R}$)

On veut montrer que le seul endomorphisme du corps $\mathbb{R}$ est l'identité. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps (ou d'anneaux).

1. Montrer que pour tout $x \in \mathbb{Q}$, on a $f(x) = x$.
2. Montrer que pour tout $x \in \mathbb{R}^+$, on a $f(x) \in \mathbb{R}^+$.
3. Montrer que f est croissante.
4. Conclure.

Scanné avec CamScanner

Corps

Solution

1. Puisque f est un morphisme d'anneaux, alors f(1)=1 et $\forall n \in \mathbb{Z}, f(n) = f(n.1) = nf(1) = n$.
   Soit $x = \frac{p}{q} \in \mathbb{Q}$, où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. D'après ce qui précède, on a :
   $p = f(p) = f(qx) = qf(x)$. Donc $f(x) = \frac{p}{q} = x$.
2. Soit $x \in \mathbb{R}^+$. On a $f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 \in \mathbb{R}^+$.
3. soit $x, y \in \mathbb{R}$ tel que $x \leq y$. Comme $y - x \geq 0$, alors d'après la question (2) on a : $f(y - x) = f(y) - f(x) \geq 0$. Donc $f(x) \leq f(y)$. Ce qui montre que f est croissante.
4. Soit $x \in \mathbb{R}$. Il existe deux suites $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ convergentes vers x telles que : $\forall n \in \mathbb{N}$, $r_n \leq x \leq s_n$. En utilisant le fait que f est croissante, alors : $\forall n \in \mathbb{N}$, $f(r_n) = r_n \leq f(x) \leq f(s_n) = s_n$. Les suites extrémités convergent vers x et donc $f(x) = x$. Ainsi le seul endomorphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$ est l'identité.

Corps : Exercices d'approfondissement

Exercice d'approfondissement

1. Quels sont les morphismes de corps de $\mathbb{Q}$ dans $\mathbb{Q}$?
2. Quels sont les morphismes de corps continus de $\mathbb{R}$ dans $\mathbb{R}$?
3. Le résultat persiste-t-il si l'on ne suppose plus la continuité ?
4. Quels sont les morphismes de corps de $\mathbb{C}$ dans $\mathbb{C}$ qui préservent $\mathbb{R}$?
5. Quels sont les morphismes de corps de $\mathbb{C}$ dans $\mathbb{R}$?

Scanné avec CamScanner

Corps : Exercices d'approfondissement

Exercice d'approfondissement

Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction telle que :

(i) $\forall x, y \in \mathbb{R}^2$, $f(x+y) = f(x) + f(y)$.

(ii) f est continue en 0.

Montrer que f est continue en tout point de $\mathbb{R}$ et on a : $f(x) = f(1)x$ pour tout x réel.

Exercice d'approfondissement

Trouver toutes les applications croissantes $f : \mathbb{R} \to \mathbb{R}$ telles que :

$$\forall x, y \in \mathbb{R}^2, f(x+y) = f(x) + f(y).$$

Bibliographie

Voici une liste d'ouvrages auxquels le texte fait référence et qui contiennent des précisions sur les notions abordées.

✓ **Jean-Marie Arnaudiès et Henri Fraysse,** *Cours de mathématiques 1, Algèbre*, Dunod 1987.

✓ **Claude Deschamps et André Warusfel,** *Mathématiques tout-en-un, 1re année Cours et exercices corrigés*, 2e édition, Dunod 2003.

✓ **Jean-Pierre Marco et Laurent Lazzarini,** *Mathématiques L1 Cours complet avec 1000 tests et exercices corrigés*, Pearson Education 2007.

✓ **Aviva Szpirglas,** *Exercices d'algèbre*, Cassini 2001.

Scanné avec CamScanner

Algèbre1
Chapitre 3: Polynômes et fractions rationnelles

Jawad SALHI

Faculté des Sciences et Techniques - Errachidia

A.U. 2020/2021

Plan

1. Polynômes à une indéterminée sur le corps $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$
2. Factorisation irréductible sur $\mathbb{R}$ ou $\mathbb{C}$
3. Fractions rationnelles

Scanné avec CamScanner

Polynômes : Construction des polynômes

Dans tout ce qui suit, $\mathbb{K}$ désigne le corps $\mathbb{R}$ ou $\mathbb{C}$.

Définition (Polynôme à une indéterminée a coefficients dans $\mathbb{K}$)

On appelle polynôme (à une indéterminée) à coefficients dans $\mathbb{K}$ toute suite presque nulle d'éléments de $\mathbb{K}$,i.e. toute suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de $\mathbb{K}$ dont tous les éléments sont nuls à partir d'un certain rang. Pour $k \in \mathbb{N}$, le coefficient a_k est appelé le coefficient de degré k du polynôme.
L'ensemble des polynômes à coefficients dans $\mathbb{K}$ est noté $\mathbb{K}[X]$ si on choisit de noter X l'indéterminée.

Un polynôme est donc une **suite** de la forme $(a_0, a_1, \cdots, a_n, \cdots)$ à coefficients dans $\mathbb{K}$.

- Avec cette présentation des polynômes, on peut immédiatement énoncer le résultat suivant :

Théorème

Deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Polynômes : Construction des polynômes

Définition (Polynôme constant, polynôme nul)

On appelle polynôme constant de $\mathbb{K}[X]$ tout polynôme $(\lambda, 0, 0, \cdots)$ avec $\lambda \in \mathbb{K}$. Un tel polynôme sera simplement noté λ.
Avec cette notation, le polynôme 0 est le polynôme nul.

Définition (Degré d'un polynôme, coefficient dominant, polynôme unitaire)

- Soit $P = (a_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$ un polynôme **non nul**. Le plus grand indice k pour lequel : $a_k \neq 0$ est appelé degré de P et noté $\deg(P)$, i.e. $\deg(P) = \max\{k \in \mathbb{N} | a_k \neq 0\}$.
  Le coefficient de degré $\deg(P)$ de P est appelé son coefficient dominant et est noté $\mathrm{dom}(P)$. S'il est égale à 1, on dit que P est **unitaire**.
- Par convention, le polynôme nul est de degré $-\infty$: $\deg(0) = -\infty$.

Scanné avec CamScanner

Polynômes : Construction des polynômes

Remarque

On définit aussi la valuation de P comme étant le degré minimum dans P : $\text{val}(P) = \min\{k \in \mathbb{N} | a_k \neq 0\}$.
Par convention la valuation du polynôme nul est $+\infty$.

Notation

L'ensemble des polynômes à coefficients dans $\mathbb{K}$, de degré inférieur ou égal à n, se note $\mathbb{K}_n[X]$: $\mathbb{K}_n[X] = \{\sum_{k=0}^{n} a_k X^k, (a_0, \cdots, a_n) \in \mathbb{K}^{n+1}\}$.

Ainsi, $\mathbb{R}_2[X] = \{aX^2 + bX + c, (a, b, c) \in \mathbb{R}^3\}$. Un élément $aX^2 + bX + c$ de $\mathbb{R}_2[X]$ est de degré 2 si $a \neq 0$, de degré 1 si $a = 0$ et $b \neq 0$, de degré 0 si $a = b = 0$ et $c \neq 0$ et de degré $-\infty$ si $a = b = c = 0$. $\mathbb{K}_0[X]$ est l'ensemble des polynômes constants. Il est constitué des polynômes constants non nuls qui sont les polynômes de degré 0 et du polynôme nul qui est de degré $-\infty$.

Polynômes : Construction des polynômes

On définit maintenant dans $\mathbb{K}[X]$ deux lois internes d'addition et de produit. Nous aimerons pouvoir écrire ceci :

$$\Big(\sum_{k=0}^{n} a_k X^k\Big) + \Big(\sum_{k=0}^{n} b_k X^k\Big) = \sum_{k=0}^{n} (a_k + b_k) X^k$$

et

$$\Big(\sum_{i=0}^{n} a_i X^i\Big) \times \Big(\sum_{j=0}^{n} b_j X^j\Big) = \sum_{0 \leq i,j \leq n} a_i b_j X^{i+j}$$

On regroupe les termes de même degré k

$$= \sum_{k=0}^{2n} \overbrace{\sum_{\substack{0 \leq i,j \leq n \\ i+j=k}} a_i b_j X^k}$$

On élimine j via la relation $j = k - i$

$$= \sum_{k=0}^{2n} \overbrace{\sum_{i=0}^{k} a_i b_{k-i} X^k}^{} .$$

Scanné avec CamScanner

Polynômes : Construction des polynômes

Définition (Anneau $\mathbb{K}[X]$)

Soient $P = (a_k)_{k\in\mathbb{N}}, Q = (b_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$.

- On appelle somme de P et Q la suite $(a_k + b_k)_{k\in\mathbb{N}}$, notée $P + Q$. Il s'agit bien d'un polynôme.
- On appelle produit de P et Q la suite $\left(\sum_{i=0}^{k} a_i b_{k-i}\right)_{k\in\mathbb{N}}$, notée $P \times Q$ ou PQ. Il s'agit bien d'un polynôme.
  En particulier, pour tout $\lambda \in \mathbb{K}$, λP est le polynôme $(\lambda a_k)_{k\in\mathbb{N}}$.

Le triplet $(\mathbb{K}[X], +, \times)$ est alors un anneau commutatif d'élément neutre le polynôme nul 0 pour $+$ et le polynôme constant 1 pour $\times$.

Polynômes : Construction des polynômes

Démonstration : Fixons une fois pour toutes $P = (a_k)_{k\in\mathbb{N}}, Q = (b_k)_{k\in\mathbb{N}}, R = (c_k)_{k\in\mathbb{N}} \in \mathbb{K}[X]$.

- **Lois internes** : Il s'agit de vérifier que la somme et le produit de deux polynômes sont bien des polynômes, i.e. des suites **presques nulles**. Notons N un rang à partir duquel : $a_k = b_k = 0$. Alors : $a_k + b_k = 0$ pour $k \geq N$, donc $P + Q$ est bien un polynôme. D'autre part, pour tout $k \geq 2N$, on a :

$$\sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{N-1} a_i \underbrace{b_{k-i}}_{=0 \text{ car } k-i>k-N\geq N} + \sum_{i=N}^{k} \underbrace{a_i}_{=0} b_{k-i} = 0.$$

  D'où PQ est un polynôme.

- **Multiplication par un scalaire :** Soit $\lambda \in \mathbb{K}$. Pour tout $k \in \mathbb{N}$, le coefficient de degré k de λP vaut : $0.a_0 + \cdots + 0.a_{k-1} + \lambda.a_k = \lambda a_k$, donc : $\lambda P = (\lambda a_k)_{k\in\mathbb{N}}$. En particulier : $1 \times P = P$.

Scanné avec CamScanner

Polynômes : Construction des polynômes

- **Propriétés de** $+$: Il est facile de vérifier que $(\mathbb{K}[X], +)$ est groupe commutatif d'élément neutre 0. L'inverse pour $+$ d'un polynôme $P = (a_k)_{k\in\mathbb{N}}$ est le polynôme $(-a_k)_{k\in\mathbb{N}}$ noté $-P$.
- **Commutativité de** $\times$: Pour tout $k \in \mathbb{N}$, on a :
$$\sum_{i=0}^{k} a_i b_{k-i} \overbrace{=}^{j=k-i} \sum_{j=0}^{k} b_j a_{k-j} \text{ et donc } PQ = QP.$$
- **Associativité de** $\times$: Pour tout $k \in \mathbb{N}$, le coefficient de degré k de $(PQ)R$ est :
$$\sum_{i=0}^{k}\Big(\sum_{j=0}^{i} a_j b_{i-j}\Big)c_{k-i} = \sum_{0\le j\le i\le k} a_j b_{i-j} c_{k-i} = \sum_{j=0}^{k} a_j\Big(\sum_{i=j}^{k} b_{i-j} c_{k-i}\Big)$$
$$\overbrace{=}^{l=i-j} \sum_{j=0}^{k} a_j\Big(\sum_{l=0}^{k-j} b_l c_{(k-j)-l}\Big),$$
donc est égal au coeffcient de degré k de $P(QR)$. Ainsi $(PQ)R = P(QR)$.

Polynômes : Construction des polynômes

- **Distributivité de** $\times$ **sur** $+$: Pour tout $k \in \mathbb{N}$, le coefficient de degré k de $P(Q+R)$ est :
$$\sum_{i=0}^{k} a_i(b_{k-i} + c_{k-i}) = \sum_{i=0}^{k} a_i b_{k-i} + \sum_{i=0}^{k} a_i c_{k-i},$$
donc est égal au coefficient de degré k de $(PQ) + (PR)$. Ainsi : $P(Q+R) = (PQ) + (PR)$.

▶ On va maintenant se diriger vers une notation définitive des polynômes (une notation de la forme $P = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$) et abandonner la notation $P = (a_n)_{n\in\mathbb{N}}$.

Scanné avec CamScanner

Théorème (Notation polynomiale)

Dans $\mathbb{K}[X]$, *on choisit de noter* X *le polynôme* $(0,1,0,0,\cdots)$.

- *pour tout* $k \in \mathbb{N}$: $X^k = (0,\cdots,0,1,0,0,\cdots)$, *polynôme dans lequel le* 1 *est en position degré* k.

$$1 = (1,0,0,\cdots), \quad X = (0,1,0,0,\cdots)$$
$$X^2 = (0,0,1,0,0,\cdots), \quad X^3 = (0,0,0,1,0,0,\cdots)\cdots$$

- *Pour tout polynôme non nul* $P = (a_k)_{k\in\mathbb{N}}$ *de degré* n : $P = \sum_{k=0}^{n} a_k X^k$.

  On peut aussi écrire que : $P = \sum_{k=0}^{\infty} a_k X^k$ *et cette écriture est unique.*

  Une telle somme est ***finie*** *contrairement aux apparences car la suite* $(a_k)_{k\in\mathbb{N}}$ *est presque nulle. Cette notation "infinie" rend de précieux services de rédaction.*

Démonstration.

Une récurrence simple permet de montrer que :
$\forall k \in \mathbb{N}^*$, $X^k = (0,\cdots,0,\underbrace{1,}_{k^e}0,0,\cdots)$. □

Attention : L'indéterminée X n'est pas un nombre ! Elle n'a pas de valeur. Elle représente la suite presque nulle $(0,1,0,0,\cdots)$.

▶ Dès que le contexte fait intervenir l'anneau $\mathbb{K}[X]$, la lettre majuscule X est une notation réservée (au même titre que la lettre i des nombres complexes). On n'écrira donc **JAMAIS** des phrases du type "en posant $X = \cdots$" qui n'ont aucun sens ! Autrement dit, il ne faut pas confondre l'indéterminée X avec l'inconnue x.

Scanné avec CamScanner

Polynômes : Construction des polynômes

Explication : En fait, **les polynômes ne sont pas des fonctions**. Notons par exemple P le polynôme $3X^2 + 4X + 1$. Calculer $P(5)$ c'est transformer 5 en un autre nombre conformément à certaines opérations (puissances, multiplication par un réel, et addition). Or il y a un tas de mondes mathématiques dans lesquels on sait calculer les puissances, multiplier par un réel et additionner les objets :

- le corps $\mathbb{R}$ bien sûr, d'où la possibilité de calculer $P(5)$
- l'anneau $\mathcal{M}_n(\mathbb{R})$, d'où la possibilité de calculer $P(A)$ pour tout $A \in \mathcal{M}_n(\mathbb{R})$.
- l'anneau $\mathbb{R}^{\mathbb{R}}$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$, d'où la possibilité de noter $P(\exp)$ la fonction $x \mapsto 3e^{2x} + 4e^x + 1$.

Finalement, on ne sait toujours pas ce qu'est le polynôme $P = 3X^2 + 4X + 1$, mais ce n'est pas la gentille fonction $x \mapsto 3x^2 + 4x + 1$ en tout cas.

Polynômes : Propriétés des degrés

Théorème (Degré d'une somme)

Pour tous $P, Q \in \mathbb{K}[X]$, *on a :* $\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}$.
De plus, si $\deg(P) \neq \deg(Q)$, *alors :* $\deg(P+Q) = \max\{\deg(P), \deg(Q)\}$.

Démonstration.

- Le résultat est évident lorsque P ou Q est nul. En effet, si par exemple $P = 0$, alors $\deg(P) = -\infty$ et donc $\max\{\deg(P), \deg(Q)\} = \deg(Q)$. D'autre part, $P + Q = Q$ et donc $\deg(P+Q) = \deg(Q)$. Ainsi : $\deg(P+Q) = \max\{\deg(P), \deg(Q)\} \leq \max\{\deg(P), \deg(Q)\}$.
- Supposons $P \neq 0$ et $Q \neq 0$ et notons m le degré de P et n celui de Q, ainsi que $P = (a_k)_{k\in\mathbb{N}}$ et $Q = (b_k)_{k\in\mathbb{N}}$. Pour tout $k > \max\{m, n\}$: $a_k + b_k = 0$, donc : $\deg(P+Q) \leq \max\{m, n\} = \max\{\deg(P), \deg(Q)\}$.

□

Scanné avec CamScanner

Théorème (Degré d'un produit)

Pour tous $P, Q \in \mathbb{K}[X]$, on a :

$$\deg(PQ) = \deg(P) + \deg(Q).$$

En particulier, si $\lambda \neq 0$:

$$\deg(\lambda P) = \deg(P).$$

Démonstration.

C'est immédiat lorsque P ou Q est nul. Supposons-les donc tous deux non nuls et notons m le degré de P et n celui de Q, ainsi que $P = (a_k)_{k\in\mathbb{N}}$, $Q = (b_k)_{k\in\mathbb{N}}$ et $PQ = (c_k)_{k\in\mathbb{N}}$. On a : $c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} =$

$$\sum_{i=0}^{m-1} a_i \overbrace{b_{m+n-i}}^{=0 \text{ car } m+n-i>n} + a_m b_n + \sum_{i=m+1}^{m+n} \overbrace{a_i}^{=0} b_{m+n-i} = a_m b_n.$$

Comme, $a_m \neq 0$ et $b_n \neq 0$, alors $c_{m+n} \neq 0$ et donc : $\deg(PQ) \geq m + n$.
Inversement, pour tout $k > m + n$:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{m} a_i \overbrace{b_{k-i}}^{=0 \text{ car } k-i>n} + \sum_{i=m+1}^{k} \overbrace{a_i}^{=0} b_{k-i} = 0,$$

donc $\deg(PQ) \leq m + n$. D'où le résultat. □

Scanné avec CamScanner

Polynômes : Intégrité de $\mathbb{K}[X]$

Théorème

$\mathbb{K}[X]$ *est intègre :* $\forall P, Q \in \mathbb{K}[X], \Big(PQ = 0 \Rightarrow P = 0 \, ou \, Q = 0\Big)$.

Démonstration.

Pout tous $P, Q \in \mathbb{K}[X]$ tels que $PQ = 0$: $\deg(P) + \deg(Q) = -\infty$, donc nécessairement : $\deg(P) = -\infty$ ou $\deg(Q) = -\infty$, i.e. : $P = 0$ ou $Q = 0$. □

Autre méthode : Raisonnons par contraposition et montrons que $\forall P, Q \in \mathbb{K}[X], \Big(P \neq 0 \text{ et } Q \neq 0 \Rightarrow PQ \neq 0\Big)$. Soit $P, Q \in \mathbb{K}[X]$. Supposons que $P \neq 0$ et $Q \neq 0$. Alors : $\deg(P), \deg(Q) \in \mathbb{N}$. Donc : $\deg(PQ) = \deg(P) + \deg(Q) \in \mathbb{N}$. En particulier, $PQ \neq 0$. D'où le résultat.

Polynômes : Intégrité de $\mathbb{K}[X]$

On déduit du théorème précédent les polynômes qui sont simplifiables pour la multiplication : ce sont les polynômes non nuls.

Théorème

$\forall (P, Q, R) \in (\mathbb{K}[X])^3, \Big(P \times Q = P \times R \, et \, P \neq 0 \Rightarrow Q = R\Big)$.

Démonstration.

Soit $(P, Q, R) \in (\mathbb{K}[X])^3$ tel que $P \neq 0$. Par intégrité de l'anneau $\mathbb{K}[X]$:

$$PQ = PR \Rightarrow P(Q - R) = 0 \Rightarrow Q - R = 0 \Rightarrow Q = R.$$

□

Explication : Ainsi, par exemple, $(X - 1)P = 0 \Rightarrow P = 0$, car $X - 1$ n'est pas le polynôme nul (X n'est pas un nombre mais X est un polynôme et le polynôme X n'est pas le polynôme 1).

Scanné avec CamScanner

Polynômes : Inversibles de l'anneau $\mathbb{K}[X]$

Théorème

Les inversibles de l'anneau $\mathbb{K}[X]$ *sont les constantes non nulles. Ainsi* $\mathbb{K}[X]^\times = \mathbb{K}^*$.

Démonstration.

Soit $P \in \mathbb{K}[X]$. On suppose que P est inversible. Donc, il existe un polynôme $Q \in \mathbb{K}[X]$ tel que $P \times Q = 1$. Ceci impose déjà $P \neq 0$ et $Q \neq 0$ et donc P et Q ont des degrés qui sont des entiers naturels. Ensuite,

$$PQ = 1 \Rightarrow \deg(PQ) = \deg(1) \Rightarrow \deg(P) + \deg(Q) = 0.$$

Donc, nécessairement, $\deg(P) = 0$ ou encore, P est une constante non nulle.

Réciproquement, si $P = a_0 \neq 0$, alors, en posant $Q = \dfrac{1}{a_0} \in \mathbb{K}[X]$, on a $P \times Q = 1$ et donc P est inversible dans l'anneau $\mathbb{K}[X]$. □

Polynômes : L'évaluation et les fonctions polynomiales

Définition (Evaluation, fonction polynomiale)

Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. Si $P = 0$, on pose $P(\lambda) = 0$. Si $P \neq 0$, en notant n son degré et $P = \sum_{k=0}^{n} a_k X^k$, on pose $P(\lambda) = \sum_{k=0}^{n} a_k \lambda^k$.

L'application $\widetilde{P} : \mathbb{K} \to \mathbb{K}$ définie par $\widetilde{P}(x) = P(x)$ est appelée fonction polynomiale associée au polynôme P. On la note $\widetilde{P}$ quand on veut la distinguer proprement du polynôme P, mais aussi souvent P.

Remarque : Pour tout polynôme $P = \sum_{k=0}^{+\infty} a_k X^k$ avec $(a_k)_{k\in\mathbb{N}}$ presque nulle, on a clairement : $P(\lambda) = \sum_{k=0}^{+\infty} a_k \lambda^k$, cette dernière somme étant finie.

- On dit également que le nombre $P(\lambda)$ est la valeur de P en λ. Évaluer P en λ signifie calculer le nombre $P(\lambda)$.

Scanné avec CamScanner

Définition (Composition des polynômes)

Soient P et Q deux polynômes de $\mathbb{K}[X]$. Si $P = 0$, on pose $P \circ Q = 0$. Si $P \neq 0$, on note $n \geq 0$ son degré et l'on écrit P sous la forme $P = \sum_{k=0}^{n} a_k X^k$. On pose alors $P \circ Q = \sum_{k=0}^{n} a_k Q^k$, avec la convention $Q^0 = 1$. Le polynôme $P \circ Q$ est également noté $P(Q)$.

La notation usuelle P=P(X) : Lorsque $Q = X$, on a $P(Q) = P \circ Q = \sum_{k=0}^{n} a_k X^k = P$ et on peut donc écrire que $P(X) = P$.

Théorème (Degré d'une composée)

Si Q n'est pas constant :

$$\deg(P \circ Q) = \deg(P) \times \deg(Q).$$

Démonstration.

On suppose Q non constant et on pose : $m = \deg(P)$. Par produit, on a : $\deg(Q^k) = k \deg(Q)$ pour tout $k \in \{0, \cdots, m\}$. Donc, comme $\deg(Q) \geq 1$, la suite $(\deg(Q^k))_{0 \leq k \leq m}$ est strictement croissante. Finalement, par somme :

$$\deg(P \circ Q) = \deg(\sum_{k=0}^{m} a_k Q^k) \overset{a_m \neq 0}{=} \deg(Q^m) = m \deg(Q) = \deg(P) \times \deg(Q).$$

□

Scanné avec CamScanner

Polynômes : Dérivation des polynômes

Définition (Dérivation des polynômes)

Soit $P \in \mathbb{K}[X]$. On définit le polynôme dérivé du polynôme P, noté P', de la manière suivante :

- Si $\deg(P) \leq 0$, on pose $P' = 0$.
- Si $n = \deg(P) \geq 1$ et si $P = \sum_{k=0}^{n} a_k X^k$, on pose $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

On définit ensuite pour tout $n \in \mathbb{N}$ le $n^{\text{ème}}$ polynôme dérivé de P, noté $P^{(n)}$. Pour commencer : $P^{(0)} = P$ et pour tout $n \in \mathbb{N}$: $P^{(n+1)} = (P^{(n)})'$. Pour $n = 1$ et $n = 2$, on préfère les notations P' et P'' aux notations $P^{(1)}$ et $P^{(2)}$.

Polynômes : Propriétés de la dérivation des polynômes

- Autrement dit, pour tout polynôme $P = \sum_{k=0}^{+\infty} a_k X^k \in \mathbb{K}[X]$ avec $(a_k)_{k\in\mathbb{N}}$ presque nulle, on a : $P' = \sum_{k=1}^{+\infty} k a_k X^{k-1} = \sum_{\ell=0}^{+\infty} (\ell+1) a_{\ell+1} X^{\ell}$.

Théorème

Soient $P, Q \in \mathbb{K}[X]$ et $n \in \mathbb{N}$.

1. ***Degré :*** $\begin{cases} \deg(P^{(n)}) = \deg(P) - n & \text{si : } n \leq \deg(P) \\ P^{(n)} = 0, & \text{sinon.} \end{cases}$
2. ***Somme :*** $(P+Q)^{(n)} = P^{(n)} + Q^{(n)}$.
3. ***Produit :*** $(PQ)' = P'Q + PQ'$. *Plus généralement :* $(PQ)^{(n)} = \sum_{k=0}^{n} C_n^k P^{(k)} Q^{(n-k)}$ *(formule de Leibniz).*
4. ***Composition :*** $(P \circ Q)' = Q' \times P' \circ Q$.

Scanné avec CamScanner

Démonstration : Introduisant les coefficients de P et Q :

$$P = \sum_{k=0}^{+\infty} a_k X^k \text{ et } Q = \sum_{k=0}^{+\infty} b_k X^k.$$

- **Degré :** Posons : $d = \deg(P)$. Si $d \leq 0$: $P' = 0$. Si au contraire $d \geq 1$: $P' = \sum_{k=0}^{+\infty} k a_k X^{k-1}$ avec $d a_d \neq 0$, donc : $\deg(P') = d - 1$. On généralise par récurrence aux cas des dérivées successives.
- **Somme :** Evident.
- **Produit :** Montrons d'abord la formule : $(PQ)' = P'Q + PQ'$. D'après la définition du produit sur $\mathbb{K}[X]$, on a : $PQ = \Big(\sum_{k=0}^{+\infty} a_k X^k\Big)\Big(\sum_{k=0}^{+\infty} b_k X^k\Big) = \sum_{n=0}^{+\infty} \Big(\sum_{k=0}^{n} a_k b_{n-k}\Big) X^n$. Ainsi :

$(PQ)' = \sum_{n=1}^{+\infty} n(\sum_{k=0}^{n} a_k b_{n-k}) X^{n-1}$ et donc

$$(PQ)' = \sum_{n=1}^{+\infty} n a_0 b_n X^{n-1} + \sum_{k=1}^{+\infty} (\sum_{n=k}^{+\infty} n a_k b_{n-k} X^{n-1})$$

$$= a_0 Q' + \sum_{k=1}^{+\infty} a_k (\sum_{n=k}^{+\infty} (n-k+k) b_{n-k} X^{n-1})$$

$$= a_0 Q' + \sum_{k=1}^{+\infty} a_k (\sum_{n=k}^{+\infty} (n-k) b_{n-k} X^{n-1}) + \sum_{k=1}^{+\infty} k a_k (\sum_{n=k}^{+\infty} b_{n-k} X^{n-1})$$

$$= a_0 Q' + \sum_{k=1}^{+\infty} a_k (\sum_{\ell=0}^{+\infty} \ell b_\ell X^{\ell-1+k}) + \sum_{k=1}^{+\infty} k a_k (\sum_{\ell=0}^{+\infty} b_\ell X^{\ell+k-1})$$

$$= a_0 Q' + \sum_{k=1}^{+\infty} a_k X^k (\sum_{\ell=1}^{+\infty} \ell b_\ell X^{\ell-1}) + \sum_{k=1}^{+\infty} k a_k X^{k-1} (\sum_{\ell=0}^{+\infty} b_\ell X^\ell)$$

$$= a_0 Q' + \sum_{k=1}^{+\infty} a_k X^k Q' + \sum_{k=1}^{+\infty} k a_k X^{k-1} Q = PQ' + P'Q.$$

Scanné avec CamScanner

Polynômes : Propriétés de la dérivation des polynômes

La formule de Leibniz s'en déduit par récurrence sur n.

- **Initialisation :** Pour $n = 0$, rien à faire !
- **Hérédité :** Soit $n \in \mathbb{N}$. Faisons l'hypothèse que la formule de Leibniz : $(PQ)^{(n)} = \dots$ est vraie pour tous $P, Q \in \mathbb{K}[X]$. Alors pour tous $P, Q \in \mathbb{K}[X]$:

$$
\begin{aligned}
(PQ)^{(n+1)} &= ((PQ)')^{(n)} = (P'Q + PQ')^{(n)} = (P'Q)^{(n)} + (PQ')^{(n)} \\
&= \sum_{k=0}^{n} C_n^k (P')^{(k)} Q^{(n-k)} + \sum_{\ell=0}^{n} C_n^\ell P^{(\ell)} (Q')^{(n-\ell)} \\
&= \sum_{k=0}^{n} C_n^k P^{(k+1)} Q^{(n-k)} + \sum_{\ell=0}^{n} C_n^\ell P^{(\ell)} Q^{(n+1-\ell)} \\
&= \sum_{k=1}^{n+1} C_n^{k-1} P^{(k)} Q^{(n+1-k)} + \sum_{\ell=0}^{n} C_n^\ell P^{(\ell)} Q^{(n+1-\ell)}
\end{aligned}
$$

Polynômes : Propriétés de la dérivation des polynômes

En décomposant les sommes précédentes de la façon suivante :

$$
\begin{aligned}
&(PQ)^{(n+1)} \\
&= P^{(n+1)} Q^{(0)} + \sum_{k=1}^{n} C_n^{k-1} P^{(k)} Q^{(n+1-k)} + \sum_{k=1}^{n} C_n^k P^{(k)} Q^{(n+1-k)} \\
&\quad + P^{(0)} Q^{(n+1)} \\
&= P^{(n+1)} Q^{(0)} + \sum_{k=1}^{n} \left(C_n^{k-1} + C_n^k \right) P^{(k)} Q^{(n+1-k)} + P^{(0)} Q^{(n+1)}
\end{aligned}
$$

et en utilisant la formule de Pascal $C_n^{k-1} + C_n^k = C_{n+1}^k$, on obtient :

$$
\begin{aligned}
(PQ)^{(n+1)} &= P^{(n+1)} Q^{(0)} + \sum_{k=1}^{n} C_{n+1}^k P^{(k)} Q^{(n+1-k)} + P^{(0)} Q^{(n+1)} \\
&= \sum_{k=0}^{n+1} C_{n+1}^k P^{(k)} Q^{(n+1-k)}.
\end{aligned}
$$

D'où le résultat.

Scanné avec CamScanner

Polynômes : Propriétés de la dérivation des polynômes

- **Composition :** Tout d'abord, montrons par récurrence que $\forall P \in \mathbb{K}[X], \forall n \in \mathbb{N}^* : (P^n)' = nP'P^{n-1}$.
  - **Initialisation :** Pour $n = 1$, rien à faire !
  - **Hérédité :** Soit $n \in \mathbb{N}^*$. Supposons la propriété est vraie à l'ordre n et montrons-là à l'ordre $n+1$. On a : $(P^{n+1})' = (P^n \times P)' = (P^n)'P + P^nP' = (nP'P^{n-1}) \times P + P^nP' = nP'P^n + P'P^n = (n+1)P'P^n$. D'où le résultat.

Passons maintenant à la preuve du fait que $(P \circ Q)' = Q' \times P' \circ Q$.

Par définition : $P \circ Q = \sum_{k=0}^{+\infty} a_k Q^k$, donc : $(P \circ Q)' = \sum_{k=0}^{+\infty} a_k (Q^k)'$.

Or : $(Q^k)' = kQ'Q^{k-1}$ pour tout $k \in \mathbb{N}^*$, donc :

$$(P \circ Q)' = \sum_{k=0}^{+\infty} a_k k Q' Q^{k-1} = Q' \times P' \circ Q.$$

Polynômes : Propriétés de la dérivation des polynômes

Proposition (Formule de Taylor pour les polynômes)

Pour tous $n \in \mathbb{N}$, $P \in \mathbb{K}_n[X]$ et $\lambda \in \mathbb{K}$, on a :

$$P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(\lambda)}{k!}(X - \lambda)^k.$$

Démonstration : Un polynôme P de $\mathbb{K}_n[X]$ s'écrit $P = \sum_{i=0}^{n} a_i X^i$. Par linéarité de la dérivation, pour tout k entre 0 et n, on a

$$P^{(k)} = \sum_{i=0}^{n} a_i (X^i)^{(k)} = \sum_{i=k}^{n} a_i \frac{i!}{(i-k)!} X^{i-k}.$$

Scanné avec CamScanner

Polynômes : Propriétés de la dérivation des polynômes

D'où après évaluation en λ : $P^{(k)}(\lambda) = \sum_{i=k}^{n} a_i \frac{i!}{(i-k)!}\lambda^{i-k}$ et donc

$$\sum_{k=0}^{n} \frac{P^{(k)}(\lambda)}{k!}(X-\lambda)^k = \sum_{k=0}^{n} \frac{1}{k!}\Big(\sum_{i=k}^{n} a_i \frac{i!}{(i-k)!}\lambda^{i-k}\Big)(X-\lambda)^k$$

$$= \sum_{i=0}^{n}\Big(\sum_{k=0}^{i} a_i \frac{i!}{k!(i-k)!}\lambda^{i-k}(X-\lambda)^k\Big)$$

$$= \sum_{i=0}^{n} a_i\Big(\sum_{k=0}^{i} C_i^k \lambda^{i-k}(X-\lambda)^k\Big) = \sum_{i=0}^{n} a_i\Big(X-\lambda+\lambda\Big)^i$$

$$= \sum_{i=0}^{n} a_i X^i = P(X),$$

où l'on a appliqué la formule du binôme à l'avant-dernière ligne.

Polynômes : Relation de divisibilité

Définition (Divisibilité, diviseur, multiple)

Soient $A, B \in \mathbb{K}[X]$. On dit que A divise B, ou que A est un diviseur de B, ou que B est divisible par A, ou que B est un multiple de A, s'il existe $P \in \mathbb{K}[X]$ pour lequel : $B = AP$. Cette relation se note $A|B$.

Exemples

Pour tout $n \in \mathbb{N}$, $X^{2n+1}+1$ est divisible par $X+1$.

- *En effet,*

$$X^{2n+1}+1 = X^{2n+1} - (-1)^{2n+1} = (X+1)\sum_{k=0}^{2n}(-1)^k X^{2n-k}.$$

Scanné avec CamScanner

Polynômes : Relation de divisibilité

Théorème (Propriétés de la relation de divisibilité)

Soient $A, B, C, D \in \mathbb{K}[X]$.

- *La relation de divisibilité $|$ est réflexive et transitive dans $\mathbb{K}[X]$, c'est même une relation d'ordre sur l'ensemble des polynômes **unitaires ou nuls** de $\mathbb{K}[X]$. Elle est en revanche seulement réflexive et transitive sur $\mathbb{K}[X]$ car pour tous $A, B \in \mathbb{K}[X]$: $A|B$ et $B|A \Leftrightarrow \exists \lambda \in \mathbb{K}^* / A = \lambda B$. On dit alors que A et B sont **associés** (sur $\mathbb{K}$).*
- *Si : $D|A$ et $D|B$, alors : $D|(AU + BV)$ pout tous $U, V \in \mathbb{K}[X]$.*
- *Si : $A|B$ et $C|D$, alors : $AC|BD$. En particulier, si : $A|B$, alors : $A^k|B^k$ pour tout $k \in \mathbb{N}$.*

Remarque : La relation de divisibilité restreinte à l'ensemble des polynômes **unitaires** est une relation d'ordre. En effet, deux polynômes unitaires associés sont égaux, ce qui prouve l'antisymétrie.

Polynômes : Relation de divisibilité

Démonstration : La relation de divisibilité est réflexive et transitive. En effet :

- Soit $A \in \mathbb{K}[X]$. On a : $A = 1 \times A$ avec $1 \in \mathbb{K}[X]$. Donc, $A|A$.
- Soit $(A, B, C) \in (\mathbb{K}[X])^3$ tel que $A|B$ et $B|C$. Il existe $(Q_1, Q_2) \in (\mathbb{K}[X])^2$ tel que $B = Q_1 A$ et $C = Q_2 B$. Ainsi, $C = Q_2 Q_1 A$ avec $Q_2 Q_1 \in \mathbb{K}[X]$ et donc $A|C$.

Par contre, la relation de divisibilité n'est pas anti-symétrique. En effet, si : $A = \lambda B$ avec $\lambda \in \mathbb{K}^*$, on a aussi : $B = \frac{1}{\lambda} A$, donc $A|B$ et $B|A$.

Réciproquemen, supposons que : $A|B$ et $B|A$. Il existe alors $P, Q \in \mathbb{K}[X]$ pour lesquels : $A = PB$ et $B = QA$, donc : $A = PQA$. Deux cas se présentent :

- Si $A = 0$: $B = QA = 0$, donc $A = \lambda B$ pour $\lambda = 1$.
- Si au contraire $A \neq 0$: $PQ = 1$ par intégrité de $\mathbb{K}[X]$. Donc, les polynômes P et Q sont des inversibles de l'anneau $\mathbb{K}[X]$ et donc : P et Q sont des constantes non nulles. Ainsi, il existe $\lambda \in \mathbb{K}^*$ tel que $A = \lambda B$.

Scanné avec CamScanner

Polynômes : Relation de divisibilité

Théorème

Soient A et B deux polynômes non nuls tels que $B|A$. Alors, $\deg(B) \leq \deg(A)$.

Démonstration.

Comme $B|A$, alors il existe $Q \in \mathbb{K}[x]$ tel que $A = QB$. Puisque $A \neq 0$, on a nécessairement $Q \neq 0$. Ainsi, $\deg(A), \deg(B), \deg(Q)$ sont des entiers naturels. Donc : $\deg(A) = \deg(QB) = \deg(Q) + \deg(B) \geq \deg(B)$. D'où le résultat. □

Polynômes : Division euclidienne

Théorème (Division euclidienne)

Soient $A, B \in \mathbb{K}[X]$ avec $B \neq 0$. Il existe un et un seul couple de polynômes $(Q, R) \in (\mathbb{K}[\mathbb{X}])^2$ pour lequel : $A = BQ + R$ et $\deg(R) < \deg(B)$. *On appelle A le dividende de la division euclidienne de A par B, B son diviseur, Q son quotient et R son reste.*

Remarque

L'unicité dans la division euclidienne sur $\mathbb{K}[X]$ permet d'affirmer qu'un polynôme $B \neq 0$ divise A si et seulement si le reste dans la division euclidienne de A par B est nul.

Scanné avec CamScanner

Polynômes : Division euclidienne

Démonstration : Raisonnons en deux temps.

- **Unicité de (Q, R) :** soient (Q_1, R_1) et (Q_2, R_2) deux couples de polynômes de $\mathbb{K}[X]$ tels que $A = BQ_1 + R_1$ et $A = BQ_2 + R_2$, avec $\deg(R_1) < \deg(B)$ et $\deg(R_2) < \deg(B)$. On a donc $BQ_1 + R_1 = BQ_2 + R_2$, d'où l'égalité $B(Q_1 - Q_2) = R_2 - R_1$ avec $\deg(R_2 - R_1) \leqslant \max(\deg(R_1), \deg(R_2)) < \deg(B)$. Raisonnons par l'absurde et supposons que $Q_1 \neq Q_2$. Alors $\deg(Q_1 - Q_2) \geqslant 0$. Ce qui entraine que $\deg(R_2 - R_1) = \deg(B(Q_1 - Q_2)) = \deg(B) + \deg(Q_1 - Q_2) \geqslant \deg(B)$. Contradiction. Ainsi $Q_1 = Q_2$, puis $R_1 = A - BQ_1 = A - BQ_2 = R_2$.

Polynômes : Division euclidienne

- **Existence de (Q, R) :** Raisonnons par récurrence sur le degré de A. Notons $m = \deg(B) \geqslant 0$ et $B = b_m X^m + \cdots + b_0$ avec $b_m \neq 0$. Soient n un entier naturel et $HR(n)$ la propriété suivante : pour tout polynôme A de degré inférieur ou égal à n, il existe un couple (Q, R) de polynômes à coefficients dans $\mathbb{K}$ tels que $A = BQ + R$ et $\deg(R) < \deg(B)$. L'hypothèse $HR(0)$ est vraie : en effet, $A = a_0 \in \mathbb{K}$. Si $m \geqslant 1$, on pose $Q = 0$ et $R = A$; si $m = 0$, on pose $Q = a_0/b_0$ et $R = 0$. On a bien dans tous les cas $A = BQ + R$ et $\deg(R) < \deg(B)$. Soit $n \geqslant 0$ Supposons $HR(n)$ vérifiée. Soit A un polynôme de degré $n+1 : A = a_{n+1}X^{n+1} + \cdots + a_1 X + a_0$ Si $n + 1 < m = \deg(B)$, il suffit de poser $R = A$ et $Q = 0$. Si $n + 1 \geqslant m = \deg(B)$, posons $A_1 = A - (a_{n+1}/b_m) X^{n+1-m} B$. On a $\deg(A_1) \leqslant n$, donc d'après $HR(n)$, il existe un couple de polynômes (Q_1, R_1) tels que $A_1 = Q_1 B + R_1$ avec $\deg(R_1) < \deg(B)$. Posons $R = R_1$ et $Q = Q_1 + (a_{n+1}/b_m) X^{n+1-m}$. On a bien $A = BQ + R$ et $\deg(R) < \deg(B)$. D'où le résultat.

Scanné avec CamScanner

Polynômes : Division euclidienne

Parmi les exemples fondamentaux de division euclidienne, on retiendra l'exemple de la division d'un polynôme P par $X - \lambda$, où λ est un élément de $\mathbb{K}$.

Théorème (Division par $X - \lambda$)

Soient $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$. Le reste de la division euclidienne de P par $X - \lambda$ est $P(\lambda)$.

Démonstration.

La division euclidienne de P par $X - \lambda$ s'écrit : $P = (X - \lambda)Q + R$ pour certains $(Q, R) \in \mathbb{K}[X]^2$ avec : $\deg(R) < 1$, donc en fait R est un polynôme constant. Evaluons en λ : $P(\lambda) = (\lambda - \lambda)Q(\lambda) + R(\lambda) = R$ □

Polynômes : Division euclidienne

Exemples

Pour tout $n \in \mathbb{N}$, le reste de division euclidienne de X^n par $X^2 - 3X + 2$ vaut : $(2^n - 1)X - (2^n - 2)$.

- *En effet, soit $n \in \mathbb{N}$. La division euclidienne de X^n par $X^2 - 3X + 2$ s'écrit : $X^n = (X - 1)(X - 2)Q + aX + b$ pour certain $Q \in \mathbb{R}[X]$ et $a, b \in \mathbb{R}$. Evaluons en $1 : 1 = a + b$, puis en $2 : 2^n = 2a + b$. Après calcul, on obtient : $a = 2^n - 1$ et $b = 2 - 2^n$.*

Cette méthode peut être adaptée au calcul du reste dans la division euclidienne d'un polynôme P par $(X - a)^2$. Il faudra dans ce cadre faire appel à la dérivation.

Scanné avec CamScanner

▶ Déterminons de deux manières le reste R dans la division euclidienne d'un polynôme $P \in \mathbb{K}[X]$ par $B = (X-a)^2$ où $a \in \mathbb{K}$.

- Il existe $Q \in \mathbb{K}[X]$ et $R = \alpha X + \beta \in \mathbb{K}_1[X]$ tels que $P = (X-a)^2 Q + \alpha X + \beta$. On en déduit, après évaluation en a, que $P(a) = \alpha a + \beta$. De plus, $P' = 2(X-a)Q + (X-a)^2 Q' + \alpha$ et donc, après évaluation en a, on obtient : $\alpha = P'(a)$. D'où $R = P'(a)X + P(a) - aP'(a) = P(a) + (X-a)P'(a)$.
- D'après la formule de Taylor en a, pour $n = \deg(P)$ (on peut supposer $n \geqslant 2$ car sinon $Q = 0$ et $R = P$) $P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^k =$ $P(a) + P'(a)(X-a) + (X-a)^2 \sum_{k=2}^{n} \frac{P^{(k)}(a)}{k!}(X-a)^{k-2}$. On en déduit, par unicité dans la division euclidienne, que $R = P(a) + P'(a)(X-a)$.

Exercice

Pour $n \in \mathbb{N}$, on pose $P_n = X^n - 1$. Effectuer la division euclidienne de P_n par P_m.

Solution

Soit $(m,n) \in \mathbb{N}^2$. La division euclidienne de n par m s'écrit $n = qm + r$ où $(q,r) \in \mathbb{N}^2$ et $0 \leq r < m$. On écrit $X^n - 1 = X^{qm+r} - 1$ et donc

$$X^n - 1 = X^{qm+r} - X^r + X^r - 1 = X^r\Big((X^m)^q - 1\Big) + X^r - 1$$
$$= X^r\Big(1 + X^m + (X^m)^2 + \cdots + (X^m)^{q-1}\Big)(X^m - 1) + X^r - 1.$$

Puisque $\deg(X^r - 1) \leq r < m$ (si $r \geq 1$ $\deg(X^r - 1) = r$ et si $r = 0$, $\deg(X^r - 1) = -\infty$), la division euclidienne est achevée. Le quotient est $Q = X^r\Big(1 + X^m + (X^m)^2 + \cdots + (X^m)^{q-1}\Big)$ et le reste est $R = X^r - 1$.

Scanné avec CamScanner

Polynômes : PGCD et PPCM

Définition (Diviseur/multiple commun)

Soient $A_1, \cdots, A_r \in \mathbb{K}[X]$.

- On appelle divieur commun de $A_1, \cdots, A_r$ tout polynôme de $\mathbb{K}[X]$ qui divise à la fois $A_1, \cdots, A_r$.
- On appelle multiple commun de $A_1, \cdots, A_r$ tout polynôme de $\mathbb{K}[X]$ qui divisible à la fois par $A_1, \cdots, A_r$.

Théorème (PGCD de deux polynômes)

- *Soient $AB \in \mathbb{K}[X]$ avec $A \neq 0$ et $B \neq 0$. On appelle plus grand commun diviseur ou (PGCD) de A et B tout diviseur commun de A et B de degré maximal.*
- *On convient que 0 est le seul PGCD de 0 et 0.*

Polynômes : PGCD et PPCM

Démonstration.

Justifions l'existence d'un PGCD dans le cas où : $A \neq 0$. Or l'ensemble des **degrés** des diviseurs commun non nuls de A et B contient 0 (car A et B sont divisibles par 1) et il est majoré par $\deg(A)$. Donc, cet ensemble possède un plus grand élément car partie non vide et majorée de $\mathbb{N}$. □

Exemples

Pour tout $A \in \mathbb{K}[X]$, les PGCD de A et 0 sont exactement les associés de A.

▶ *En effet, si $A \neq 0$, les diviseurs communs de A et 0 sont exactement les diviseurs de A et les diviseurs de A de degré maximal sont exactement ses associés.*

Scanné avec CamScanner

Théorème (Idée fondamentale de l'algorithme d'Euclide)

Pour tous $A, B, K \in \mathbb{K}[X]$, $A + BK$ et B ont les mêmes diviseurs communs que A et B, et donc aussi les mêmes PGCD.

Explication : En particulier, pour tous $A, B \in \mathbb{K}[X]$ avec $B \neq 0$, en notant R le reste de la division euclidienne de A par B, B et R ont les mêmes diviseurs communs que A et B.

Démonstration.

Tout diviseur commun de A et B divise aussi $A + BK$ et B, et inversement, tout diviseur commun de $A + BK$ et B divise aussi $A = (A + BK) - BK$ et B. □

Théorème (Unicité du PGCD de deux polynômes)

Soient $A, B \in \mathbb{K}[X]$.

- *Les PGCD de A et B sont associés. Un seul d'entre eux est donc unitaire (ou nul si $A = B = 0$) et on l'appelle **LE** PGCD de A et B et on le note $A \wedge B$.*
- *Les diviseurs communs de A et B sont exactement les diviseurs de $A \wedge B$.*

Démonstration :

Nous allons metre en oeuvre dans cette preuve un algorithme de calcul du PGCD qu'on appelle *l'algorithme d'Euclide*. Soient $A, B \in \mathbb{K}[X]$. On peut supposer que : $\deg(B) \leq \deg(A)$ sans perte de généralité. On définit une suite de polynômes $R_0, R_1, R_2, \cdots$ de la manière suivante :

- Au départ, on pose : $R_0 = A$ et $R_1 = B$.

Scanné avec CamScanner

- Ensuite, pour $k \in \mathbb{N}$, **TANT QUE :** $R_{k+1} \neq 0$, on note R_{k+2} le reste de la division euclidienne de R_k par R_{k+1}, et en particulier, on a : $\deg(R_{k+2}) < \deg(R_{k+1})$.

A l'issue de cette construction : $\deg(R_0) > \deg(R_1) > \deg(R_2) > \cdots$, et comme il n'existe qu'un nombre **FINI** d'entiers naturels entre 0 et $\deg(R_0)$, on obtient forcément $\deg(R_N) = -\infty$ pour un certain $N \in \mathbb{N}^*$ i.e. $R_N = 0$ et l'algorithme se termine. Or, en vertu de l'idée fondamentale de l'algorithme d'Euclide, $A = R_0$ et $B = R_1$ ont les mêmes diviseurs communs et le mêmes PGCD que R_1 et R_2, puis que R_2 et $R_3 \cdots$ et enfin que R_{N-1} et $R_N = 0$. Les PGCD de R_{N-1} et 0 étant exactement les associés de R_{N-1}, les diviseurs communs de A et B sont ainsi exactement les diviseurs de R_{N-1} et leurs PGCD sont exactement les associés de R_{N-1}. En particulier, les PGCD de A et B sont associés.

Algorithme d'Euclide

Comme on vient de le voir, l'algorithme d'Euclide est un algorithme de calcul du PGCD de deux polynômes. Il a été montré en particulier que : $A \wedge B$ est associé au dernier reste non nul dans l'algorithme d'Euclide.

- Calculons $(X^5 - X^4 + X^3 - X^2 + X - 1) \wedge (X^2 - 1)$.

$X^5 - X^4 + X^3 - X^2 + X - 1$	$X^2 - 1$
$-\left(X^5 - X^3\right)$	$X^3 - X^2 + 2X - 2$
$-X^4 + 2X^3 - X^2 + X - 1$	
$-\left(-X^4 + X^2\right)$	
$2X^3 - 2X^2 + X - 1$	
$-\left(2X^3 - 2X\right)$	
$-2X^2 + 3X - 1$	
$-\left(-2X^2 + 2\right)$	
$3X - 3$	

Scanné avec CamScanner

D'où $X^5 - X^4 + X^3 - X^2 + X - 1 = (X^3 - X^2 + 2X - 2)(X^2 - 1) + 3X - 3$ puis, on a $X^2 - 1 = \frac{1}{3}(3X - 3)(X + 1) + 0$. Le pgcd est le dernier reste non nul, donc $(X^5 - X^4 + X^3 - X^2 + X - 1) \wedge (X^2 - 1) = X - 1$,

Remarque

- *$A \wedge B$ est un polynôme unitaire.*
- *Si $A|B$ et $A \neq 0$, $A \wedge B = \frac{1}{\mathrm{dom}(A)} A$, où $\mathrm{dom}(A)$ est le coefficient dominant de A.*

Théorème (Relations de Bézout pour deux polynômes)

*Soient $A, B \in \mathbb{K}[X]$. Il existe des polynômes $U, V \in \mathbb{K}[X]$ pour lesquels : $A \wedge B = AU + BV$. Une telle relation est appelé **une** relation de Bézout de A et B.*

Attention : Les polynômes U et V ne sont pas uniques. En fait, Si A et B sont non constants, on a de plus unicité des polynômes U et V lorsque l'on impose la condition supplémentaire $\deg(U) < \deg(B)$ et $\deg(V) < \deg(A)$.

Démonstration : Si B divise A, un PGCD de A et B est B ou encore $A \wedge B = \frac{1}{\mathrm{dom}(B)} B = 0 \times A + \frac{1}{\mathrm{dom}(B)} B$. Dans ce cas, les polynômes $U = 0$ et $V = \frac{1}{\mathrm{dom}(B)}$ conviennent.

Sinon, avec les notations de l'algorithme d'Euclide exposé plus haut, on a $A \wedge B = \frac{1}{\mathrm{dom}(R_{N-1})} R_{N-1}$.

Scanné avec CamScanner

A partir de l'égalité, $R_{N-3} = Q_{N-3}R_{N-2} + R_{N-1}$, on obtient une égalité de la forme : $A \wedge B = \frac{1}{\text{dom}(R_{N-1})} R_{N-1} = R_{N-3}U_{N-3} + R_{N-2}V_{N-3}$, où $U_{N-3} = \frac{1}{\text{dom}(R_{N-1})}$ et $V_{N-3} = -\frac{1}{\text{dom}(R_{N-1})} Q_{N-3}$ sont des polynômes. Puis en remontant dans l'algorithme, par récurrence, on peut écrire $A \wedge B$ sous la forme $A \wedge B = R_k U_k + R_{k+1} V_k$ pour tout $k \in \{0, \cdots, N-3\}$, où U_k et V_k sont des polynômes. En particulier, pour $k = 0$, il existe deux polynômes U et V tels que

$$A \wedge B = R_0 U + R_1 V = AU + BV.$$

Exercice

Déterminer deux polynômes U et V tels que
$U \times (X^2 + X + 1) + V \times (X^2 - X + 1) = 1.$

Solution

$X^2 + X + 1 = 1 \times (X^2 - X + 1) + 2X$ puis
$X^2 - X + 1 = (\frac{X}{2} - \frac{1}{2}) \times (2X) + 1$. Donc,

$$\begin{aligned} 1 &= (X^2 - X + 1) - (\frac{X}{2} - \frac{1}{2}) \times (2X) \\ &= (X^2 - X + 1) - (\frac{X}{2} - \frac{1}{2})[(X^2 + X + 1) - (X^2 - X + 1)] \\ &= (-\frac{X}{2} + \frac{1}{2})(X^2 + X + 1) + (\frac{X}{2} + \frac{1}{2})(X^2 - X + 1). \end{aligned}$$

Les polynômes $U = -\frac{X}{2} + \frac{1}{2}$ et $V = \frac{X}{2} + \frac{1}{2}$.

Scanné avec CamScanner

Polynômes : PGCD et PPCM

Théorème (Factorisation par un diviseur commun)

Soient $A, B, C \in \mathbb{K}[X] \setminus \{0\}$ *avec* C *unitaire. Alors,*
$(CA) \wedge (CB) = C(A \wedge B)$.

Démonstration.

C divise CA et CB et donc C divise $(CA) \wedge (CB)$. Il existe un polynôme non nul Q tel que $(CA) \wedge (CB) = CQ$. CQ divise CA et donc Q divise A ($CA = Q_1 CQ$ puis $A = Q_1 Q$ car $C \neq 0$). De même, Q divise B et donc Q divise $A \wedge B$.
Inversement, $C(A \wedge B)$ divise CA et CB puis $C(A \wedge B)$ divise $(CA) \wedge (CB) = CQ$ et finalement $A \wedge B$ divise Q.
En résumé, Q divise $A \wedge B$ et $A \wedge B$ divise Q. Donc, il existe $\lambda \in \mathbb{K}^*$ tel que $Q = \lambda(A \wedge B)$. Enfin, CQ est unitaire car égal à $(CA) \wedge (CB)$ et C est unitaire. Donc Q est unitaire puis $\lambda = 1$ puis $Q = A \wedge B$ et finalement $(CA) \wedge (CB) = C(A \wedge B)$. □

Polynômes : PGCD et PPCM

Théorème

Soient $A, B \in \mathbb{K}[X] \setminus \{0\}$. *En posant* $D = A \wedge B$, *il existe* $A_1, B_1 \in \mathbb{K}[X] \setminus \{0\}$ *tel que* $A = DA_1$ *et* $B = DB_1$ *et* $A_1 \wedge B_1 = 1$.

Démonstration.

Puisque D divise A et B, il existe deux polynômes A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. De plus,
$D = A \wedge B = (DA_1) \wedge (DB_1) = D(A_1 \wedge B_1)$ puis $A_1 \wedge B_1 = 1$ après simplification par le polynôme non nul D. □

Scanné avec CamScanner

Polynômes : PGCD et PPCM

Définition (PPCM de deux polynômes)

Soient $A, B \in \mathbb{K}[X]$. On appelle plus petit commun multiple (ou PPCM) de A et B tout polynôme $M \in \mathbb{K}[X]$ satisfaisant les deux assertions :

- M est multiple commun de A et B,
- M divise tout multiple commun de A et B.

Théorème (Existence et unicité du PPCM)

Soient $A, B \in \mathbb{K}[X]$. Les polynômes A et B possèdent un unique PPCM UNITAIRE OU NUL appelé LE PPCM de A et B et noté $A \vee B$, et les autres PPCM sont les associés de $A \vee B$, i.e. les polynômes $\lambda(A \vee B)$, λ décrivant $\mathbb{K}^*$.

Polynômes : PGCD et PPCM

Proposition

Soient $A, B \in \mathbb{K}[X]$. Si $A = PA_1$ et $B = PB_1$ avec $P, A_1, B_1 \in \mathbb{K}[X]$ et P unitaire, alors : $A \vee B = (A_1 \vee B_1)P$.

Démonstration.

Soient $M = A \vee B$ et $M_1 = A_1 \vee B_1$. Comme $A_1|M_1$ et $B_1|M_1$, on a $A = PA_1|PM_1$ et $B = PB_1|PM_1$. Donc, PM_1 est un multiple commun à A et B, et par suite $M|PM_1$.
Réciproquement, puisque M est un multiple de $A = PA_1$, on peut écrire $M = PQ$. On a alors $PA_1|PQ$ et $PB_1|PQ$ ce qui entraine, puisque $P \neq 0$, $A_1|Q$ et $B_1|Q$. Donc, $M_1|Q$. Ce qui prouve que $PM_1|PQ = M$.
En conclusion $M = PM_1$, puisque ce sont deux polynômes unitaires (ou nuls) associés.

□

Scanné avec CamScanner

Polynômes : Polynômes premiers entre eux

Définition (Polynômes premiers entre eux)

Soient $A, B \in \mathbb{K}[X]$. On dit que A et B sont premiers entre eux lorsque leurs seuls diviseurs communs sont les constantes non nulles, autrement dit lorsque $A \wedge B = 1$.

Exemples

Pour tous a et b dans $\mathbb{K}$, $(X-a) \wedge (X-b) = 1$ si et seulement si $a \neq b$.

- *Prouvons ($\Rightarrow$) par contraposition : si $a = b$, on a $(X-a) \wedge (X-b) = X - a \neq 1$.*

Prouvons l'implication ($\Leftarrow$). Soit D un diviseur commun à $X-a$ et $X-b$. Comme D divise aussi $(X-b)-(X-a) = a-b \neq 0$, D est une constante non nulle. Ainsi $(X-a) \wedge (X-b) = 1$.

Polynômes : Polynômes premiers entre eux

Théorème (Théorème de Bezout)

Soient $A, B \in \mathbb{K}[X]$. Alors $A \wedge B = 1$ si et seulement si $\exists U, V \in \mathbb{K}[X]$, $AU + BV = 1$.

Démonstration.

Posons $D = A \wedge B$.

Si $D = 1$, alors l'algorithme d'Euclide et plus spécialement de sa remontée, assure l'existence de deux polynômes U et V tels que $AU + BV = 1$.

Réciproquement, supposons qu'il existe deux polynômes U et V tels que $AU + BV = 1$. Ainsi, un diviseur unitaire commun à A et B divise encore $AU + BV = 1$. Ceci montre que $D = 1$. □

- On précisera plus loin ce théorème : on montrera que si $\deg(A) > 1$ et $\deg(B) > 1$, on peut imposer au couple (U, V) la condition supplémentaire $\deg(U) < \deg(B)$ et $\deg(V) < \deg(A)$ et qu'un tel couple (U, V) est unique.

Scanné avec CamScanner

Théorème (Théorème de Gauss)

Soient $A, B, C \in \mathbb{K}[X]$. *Alors* $\Big(A \wedge B = 1 \quad et \quad A|BC\Big) \Rightarrow \Big(A|C\Big)$.

Démonstration.

Puisque $A|BC$, il existe $A_1 \in \mathbb{K}[X]$ tel que $BC = AA_1$. Comme $A \wedge B = 1$, il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $AU + BV = 1$. On multiple les deux membres de la dernière égalité par C et on obtient $C = ACU + BCV = ACU + AA_1V = A(CU + A_1V)$ et donc $A|C$. □

Lemme

Soient A_1, A_2 *et* B *dans* $\mathbb{K}[X]$ *tels que* $A_1 \wedge A_2 = 1$, $A_1|B$ *et* $A_2|B$. *Alors* $A_1A_2|B$.

Démonstration.

Comme $A_1|B$, il existe $Q_1 \in \mathbb{K}[X]$ tel que $B = A_1Q_1$. Puisque $A_1 \wedge A_2 = 1$ et $A_2|B$, on déduit du théorème de Gauss que $A_2|Q_1$ et donc que $A_1A_2|B$. □

On en déduit le résultat suivant par une récurrence évidente sur l'entier $m \in \mathbb{N}^*$.

Proposition

Soient $A_1, A_2, \cdots, A_m$ *et* B *dans* $\mathbb{K}[X]$ *tels que, pour tout* $i, j \in \{1, \cdots, m\}$ *vérifiant* $i \neq j$, $A_i \wedge A_j = 1$ *et* $A_i|B$. *Alors* $A_1A_2 \cdots A_m|B$.

Scanné avec CamScanner

Polynômes : Polynômes premiers entre eux

Lemme

Si A et B sont deux polynômes premiers entre eux, alors $A \vee B$ et AB sont associés.

Démonstration.

Posons $P = A \vee B$. Il est évident que $P|AB$.
Réciproquement, on a $A|P$ et $B|P$. Il existe donc $Q_1 \in \mathbb{K}[X]$ tel que $P = BQ_1$. Comme $A|P$ et $A \wedge B = 1$, on en déduit d'après le théorème de Gauss que $A|Q_1$. Il existe donc un polynôme $Q_2 \in \mathbb{K}[X]$ tel que $Q_1 = AQ_2$, ce qui donne $P = ABQ_2$. D'où $AB|P$. Ce qui prouve que P et AB sont associés. □

Polynômes : Polynômes premiers entre eux

Théorème (Lien entre PPCM et PGCD)

Soient $A, B \in \mathbb{K}[X]$. Les polynômes AB et $(A \wedge B)(A \vee B)$ sont associés.

Démonstration.

Le résultat étant évident si $AB = 0$, on peut supposer A et B non nuls, et unitaires quitte à les diviser par leurs coefficients dominants.
Soit $D = A \wedge B$. Prenons A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$ et $A_1 \wedge B_1 = 1$. Comme A_1 et B_1 sont unitaires et premiers entre eux, on a d'après le lemme précédent : $A_1 \vee B_1 = A_1B_1$. Alors,
$A \vee B = (DA_1) \vee (DB_1) = D(A_1 \vee B_1) = DA_1B_1$ et par suite $D(A \vee B) = AB$. □

Scanné avec CamScanner

Polynômes : Polynômes premiers entre eux

Théorème

Soient $A, B, C \in \mathbb{K}[X]$. *On a :*

$$\Big(A \wedge B = 1 \quad et \quad A \wedge C = 1\Big) \Leftrightarrow A \wedge (BC) = 1.$$

Démonstration.

($\Rightarrow$) Supposons $A \wedge B = A \wedge C = 1$. Il existe donc des polynômes U_1, V_1, U_2, V_2 tels que : $AU_1 + BV_1 = 1 \quad$ et $\quad AU_2 + CV_2 = 1$. En multipliant ces deux égalités, on obtient une relation de type $AU + (BC)V = 1$, ce qui prouve que $A \wedge (BC) = 1$.

($\Leftarrow$) La réciproque est évidente, puisque $A \wedge B$ et $A \wedge C$ sont des diviseurs communs a A et BC □

Polynômes : Racines d'un polynôme

Définition (Racine d'un polynôme)

Soient $P \in \mathbb{K}[X]$ et $\lambda \in \mathbb{K}$. On dit que λ est une racine de P (dans $\mathbb{K}$) lorsque $P(\lambda) = 0$, autrement dit lorsque λ est un zéro de la fonction $\widetilde{P} : \mathbb{K} \to \mathbb{K}$.

Théorème

Soient $P \in \mathbb{K}[X]$ *et* $\lambda \in \mathbb{K}$. λ *est une racine de* P *si et seulement si* $X - \lambda | P$.

Démonstration.

Effectuons la division euclidienne de P par $X - \lambda \neq 0$: on a vu (à la page 39) qu'elle s'écrit $P = (X - \lambda)Q + P(\lambda)$. Comme $X - \lambda | P$ si et seulement si le reste R dans la division euclidienne de P par $X - \lambda$ est nul, on voit directement que $X - \lambda | P$ si et seulement si $P(\lambda) = 0$, c'est-à-dire λ est racine de P. □

Scanné avec CamScanner

Polynômes : Racines d'un polynôme

Le résultat précédent se généralise au cas de $m \geq 1$ racines par des arguments d'arithmétique.

Proposition

Si $a_1, \cdots, a_m$ sont des racines deux à deux distinctes de $P \in \mathbb{K}[X]$, alors $(X - a_1) \cdots (X - a_m) | P$.

Démonstration.

Puisque $a_i \neq a_j$ pour $i \neq j$, les polynômes $X - a_i$ sont deux à deux premiers entre eux et divisent P, on en déduit que : $(X - a_1) \cdots (X - a_m) | P$. □

Polynômes : Racines d'un polynôme

Nous sommes maintenant en mesure d'établir le résultat central de ce paragraphe : le degré d'un polynôme non nul P de $\mathbb{K}[X]$ est un majorant du nombre de ses racines dans $\mathbb{K}$.

Théorème

Tout polynôme P non nul à coefficients dans $\mathbb{K}$ admet au plus $\deg(P)$ racines dans $\mathbb{K}$.

Démonstration.

Si P n'admet aucune racine dans $\mathbb{K}$, le résultat est clair. Dans le cas contraire, notons $a_1, \cdots, a_m$ les racines (deux à deux distinctes) dans $\mathbb{K}$ du polynôme P. D'après la proposition précédente, il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - a_1) \cdots (X - a_m)Q$, ainsi $\deg(P) = m + \deg(Q)$ et comme $(P \neq 0) \Rightarrow (Q \neq 0)$, on a $\deg(Q) \geq 0$, d'où l'inégalité $m \leq \deg(P)$. □

- On en déduit immédiatement que le seul polynôme admettant une infinité de racines dans $\mathbb{K}$ est le polynôme nul.

Scanné avec CamScanner

Polynômes : Racines d'un polynôme

Remarque

On utilise souvent le théorème précédent pour démontrer qu'un polynôme P est nul :

- *soit en exhibant $n+1$ racines lorsque l'on sait que* $\deg(P) \leq n$,
- *soit, plus radicalement, en exhibant une infinité de racines de P.*

Exemples

Déterminons les polynômes P de $\mathbb{K}[X]$ vérifiant $P(X+1) = P(X)$.

▶ *Raisonnons par analyse-synthèse. Soit P un tel polynôme et posons $Q = P - P(0)$. On prouve sans peine que $Q(X+1) = Q(X)$ et $Q(0) = 0$. On en déduit par une récurrence immédiate que $\forall n \in \mathbb{N}, Q(n) = 0$. Le polynôme Q admet donc une infinité de racines : $Q = 0$ et donc P est constant. Réciproquement, il est clair qu'un polynôme P constant vérifie $P(X+1) = P(X)$.*

Polynômes : Racines d'un polynôme

▶Nous avons maintenant les outils pour mieux comprendre les liens entre polynômes et fonctions polynomiales dans le cas où le corps de base est $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Théorème (Identification polynôme/fonction polynômiale)

Pour tous $P, Q \in \mathbb{K}[X]$, si les fonctions polynômiales $\widetilde{P}$ et $\widetilde{Q}$ sont égales, alors les polynômes P et Q eux mêmes le sont.

On rappelle que deux polynômes sont égaux si et seulement si ils ont les mêmes coefficients.

Démonstration.

Si $\widetilde{P} = \widetilde{Q}$, la fonction $\widetilde{P - Q}$ est nulle sur $\mathbb{K}$, donc tout élément de $\mathbb{K}$ est racine de $P - Q$. Comme $\mathbb{K}$ $(= \mathbb{R}$ ou $\mathbb{C})$ est infini, $P - Q$ possède ainsi une **infinité** de racines, donc $P - Q = 0$, i.e. : $P = Q$. □

Scanné avec CamScanner

Remarque

Autrement dit, deux polynômes à coefficients dans $\mathbb{R}$ ou $\mathbb{C}$ sont égaux si et seulement si leurs fonctions polynomiales associées sont égales. Le lecteur aura remarqué que le caractère infini du corps de base $\mathbb{K}$ joue un rôle central dans cette démonstration. En effet, si l'on travaille par exemple sur $\mathbb{K} = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$, les polynômes $P_1 = X^3 + X$ et $P_2 = X^2 + X$ sont distincts bien que $\widetilde{P_1} = \widetilde{P_2}$.

Définition (Multiplicité d'une racine)

Soient $\lambda \in \mathbb{K}$ et $P \in \mathbb{K}[X]$ **non nul**.

- L'ensemble $\{k \in \mathbb{N} | (X-\lambda)^k \text{ divise } P\}$ possède un plus grand élément m appelé la multiplicité de λ dans P. On dit souvent pour résumer que m est la plus grande puissance de $X - \lambda$ qui divise P. En particulier, dire que λ n'est pas racine de P, c'est dire que λ a pour multiplicité 0 dans P. Une racine est dite *simple* si elle est de multiplicité 1, *double* si elle est de multiplicité 2.
- Plus concrètement, m est caractérisé par les deux propositions suivantes, équivalentes :
  - P est divisible par $(X-\lambda)^m$ mais **PAS** par $(X-\lambda)^{m+1}$.
  - Il existe $Q \in \mathbb{K}[X]$ pour lequel : $P = (X-\lambda)^m Q$ et $Q(\lambda) \neq 0$.

Scanné avec CamScanner

Démonstration.

Pour montrer qe l'ensemble $\mathcal{M} = \{k \in \mathbb{N} | (X-\lambda)^k \text{ divise } P\}$ possède un plus grand élément, nous allons montrer que c'est une partie non vide majorée de $\mathbb{N}$. Or déjà, $\mathcal{M}$ contient 0. Montrons ensuite que $\deg(P)$ majore $\mathcal{M}$. Pour tout $k \in \mathcal{M}$: $P = (X-\lambda)^k Q$ pour un certain $Q \in \mathbb{K}[X]$ avec $Q \neq 0$ car $P \neq 0$. En particulier : $\deg(Q) \geq 0$, donc $k \leq \deg(Q) + k = \deg(P)$. □

Théorème (Utilisation des dérivées successives pour le calcul d'une multiplicité)

Soient $P \in \mathbb{K}[X]$, $\lambda \in \mathbb{K}$ et $m \in \mathbb{N}$.
λ est de multiplicité m dans P si et seulement si, $P^{(i)}(\lambda) = 0$ pour tout $i \in \{0, \cdots, m-1\}$ ***MAIS :*** *$P^{(m)}(\lambda) \neq 0$.*

Démonstration :

$\Rightarrow |$ Supposons λ de multiplicité m dans P. Dans ce cas : $P = (X-\lambda)^m Q$ pour un certain $Q \in \mathbb{K}[X]$ avec : $Q(\lambda) \neq 0$ (première division euclidienne de P par $(X-\lambda)^m$). Mais par ailleurs, Taylor donne (deuxième division euclidienne) : $P = \sum_{i=0}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i =$

$$(X-\lambda)^m \sum_{i=m}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^{i-m} + \underbrace{\sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i}_{\text{degré} < m}.$$

Scanné avec CamScanner

Polynômes : Racines d'un polynôme

Par unicité de la division euclidienne :

$$\begin{cases} \sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i = 0 & (\clubsuit) \\ Q = \sum_{i=m}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^{i-m} & (\spadesuit) \end{cases}$$

Composons $\clubsuit$ à droite par $X+\lambda$: $\sum_{i=0}^{m-1} \frac{P^{(i)}(\lambda)}{i!}X^i = 0$ et donc par identification : $P^{(i)}(\lambda) = 0$ pour tout $i \in \{0, \cdots, m-1\}$.

Evaluons $\spadesuit$ en λ : $Q(\lambda) = \frac{P^{(m)}(\lambda)}{m!}$, donc : $P^{(m)}(\lambda) \neq 0$, car $Q(\lambda) \neq 0$.

Polynômes : Racines d'un polynôme

$\Leftarrow$ | Supposons réciproquement que :
$P(\lambda) = P'(\lambda) = \cdots = P^{(m-1)}(\lambda) = 0$ mais $P^{(m)}(\lambda) \neq 0$. D'après la formule de Taylor, on a : $P = \sum_{i=0}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i =$

$\sum_{i=m}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i = (X-\lambda)^m \sum_{i=0}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^{i-m} = (X-\lambda)^m Q$, où l'on a posé $Q = \sum_{i=0}^{+\infty} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^{i-m}$. Comme $Q(\lambda) = \frac{P^{(m)}(\lambda)}{m!} \neq 0$ par hypothèse, λ est bien de multiplicité m dans P.

Scanné avec CamScanner

Exercice

- Montrer que pour tout $n \in \mathbb{N}$, $n \geq 2$, le polynôme $P_n = 1 + \frac{1}{1!}X + \frac{1}{2!}X^2 + \cdots + \frac{1}{n!}X^n$ n'a que des racines simples dans $\mathbb{C}$.
- Montrer que pour tout $n \geq 2$, le polynôme $P_n = X^n - X + 1$ n'a que des racines simples dans $\mathbb{C}$.

Les racines appartenant à $\mathbb{C} \setminus \mathbb{R}$ d'un polynôme à coefficients réels vont toujours par deux : on peut les regrouper par paires de racines conjugués. Ce résultat repose sur le lemme suivant.

Lemme

Pour tous $Q \in \mathbb{R}[X]$ et $\lambda \in \mathbb{C}$, $\overline{Q(\lambda)} = Q(\bar{\lambda})$.

Démonstration.

Écrivons $Q = \sum_{k=0}^{n} a_k X^k$ où les a_k sont réels. On a :

$$\overline{Q(\lambda)} = \sum_{k=0}^{n} \overline{a_k \lambda^k} = \sum_{k=0}^{n} a_k \overline{\lambda^k} = \sum_{k=0}^{n} a_k \bar{\lambda}^k = Q(\bar{\lambda}), \text{ car les } a_k \text{ sont réels.} \quad \square$$

Scanné avec CamScanner

Polynômes : Racines d'un polynôme

Théorème (Racines complexes d'un polynôme réel)

Soient $P \in \mathbb{R}[X]$, $n \in \mathbb{N}^*$ et $\lambda \in \mathbb{C}$. Le nombre λ est une racine de P de multiplicité n si et seulement si le nombre $\bar{\lambda}$ est une racine de P de multiplicité n.

- Ce résultat va vous faire économiser la moitié de vos calculs. En effet, si vous parvenez à trouver une racine complexe (et non réelle) d'un polynôme réel, alors, automatiquement et sans calcul, vous en avez une autre : sa conjugué.

Démonstration.

On déduit du lemme précédent que, pour tout entier naturel k, $P^{(k)}(\bar{\lambda}) = \overline{P^{(k)}(\lambda)}$. Ainsi, $P^{(k)}(\lambda) = 0$ si et seulement si $P^{(k)}(\bar{\lambda}) = 0$. D'où le résultat. □

Polynômes : Nombre maximal de racines

Théorème (Factorisation "par les racines")

*Soient $P \in \mathbb{K}[X]$ **NON NUL** et $\lambda_1, \cdots, \lambda_r$ des racines distinctes de P de multiplicité respectives $m_1, \cdots, m_r$. Alors $(X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r}$ divise P. En particluier : $\sum_{k=1}^{r} m_k \leq \deg(P)$.*

Démonstration.

Puisque $\lambda_i \neq \lambda_j$ pour $i \neq j$, les polynômes $X - \lambda_i$ sont deux à deux premiers entre eux, et il en est donc de même des polynômes $(X-\lambda_i)^{m_i}$ qui divisent P. On en déduit que $(X-\lambda_1)^{m_1} \cdots (X-\lambda_r)^{m_r} | P$. □

Scanné avec CamScanner

Polynômes : Nombre maximal de racines

- Lorsque l'on dénombre les racines d'un polynôme, on peut :
  - soit compter le nombre de racines distinctes,
  - soit compter chaque racine avec (c'est-à-dire autant de fois que) son ordre de multiplicité ; dans ce cas, une racine d'ordre r compte comme r racines.

Exemples

Le polynôme $(X-1)(X+1)^2(X-2)^3$ *possède :*

- 3 *racines distinctes :* $-1,1,2$.
- 6 *racines comptées avec leur ordre de multiplicité :* $-1,-1,1,2,2,2$.

Conséquence : Il découle du théorème précédent que : Un polynôme **NON NUL** de degré n possède au plus n racines comptées avec leur ordre de multiplicité.

Polynômes : Racines d'un polynôme

Exemples

Déterminer les racines du polynôme $P = X^6 + X^5 + 3X^4 + 2X^3 + 3X^2 + X + 1$ *sachant que* i *en est une racine multiple.*

- *On a* $P(i) = P'(i) = 0$. *mais* $P''(i) = -8i \neq 0$. *Le nombre* i *est donc une racine de* P *de multiplicité deux. Puisque* P *est à coefficients réels,* $-i$ *est également une racine de* P *de multiplicité deux.* P *est donc divisible par* $(X-i)^2(X+i)^2 = (X^2+1)^2$. *En posant la division euclidienne, on trouve* $P = (X^2+1)^2(X^2+X+1)$. *Comme* $X^2+X+1 = (X-j)(X-j^2)$, *les racines de* P *sont* $i, -i$ *(racines d'ordre deux) et* j, j^2 *(racines simples).*

Scanné avec CamScanner

Méthode

Pour montrer qu'un polynôme P est divisible par un polynôme Q, il suffit de montrer que toutes las racines de Q dans $\mathbb{C}$ sont des racines de P avec un ordre de multiplicité au moins égal.

Exercice d'application

A quelle condition nécessaire et suffisante sur n le polynôme X^2+1 divise-t-il X^n+1 ?

Solution

Pour tout $n \in \mathbb{N}$:

$$X^2+1 \text{ divise } X^n+1 \Leftrightarrow i \text{ et } -i \text{ sont racines de } X^n+1$$
$$\Leftrightarrow i \text{ est racine de } X^n+1 \qquad (\text{car } X^n+1 \in \mathbb{R}[X])$$
$$\Leftrightarrow i^n+1=0 \Leftrightarrow e^{\frac{in\pi}{2}}=e^{i\pi}$$
$$\Leftrightarrow \frac{n\pi}{2} \equiv \pi[2\pi] \Leftrightarrow n \equiv 2[4].$$

Scanné avec CamScanner

Méthode

Pour montrer qu'un polynôme P est divisible par $(X-a)^m$, on montre que a est une racine d'ordre de multiplicité au moins m de P, et pour cela il suffit de prouver que : $P(a) = P'(a) = \cdots = P^{(m-1)}(a) = 0$.

Exercice d'application

Soit $n \in \mathbb{N}$, $n \geq 2$. On considère le polynôme P défini par $P = aX^{n+1} + bX^n + 1$. Déterminer les réels a et b pour que P soit divisible par $(X-1)^2$.

Solution

$$
\begin{aligned}
P \text{ est divisible par } (X-1)^2 &\Leftrightarrow 1 \text{ est une racine d'ordre au moins } 2 \text{ de } P \\
&\Leftrightarrow P(1) = P'(1) = 0 \\
&\Leftrightarrow \begin{cases} a+b+1=0 \\ (n+1)a+nb=0 \end{cases} \\
&\Leftrightarrow \begin{cases} a=n \\ b=-1-n. \end{cases}
\end{aligned}
$$

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Exercice

1. Quel est le reste de la division euclidienne du polynôme $A = X^n + X + b$, $n \in \mathbb{N}^*$ par $B = (X - a)^2$ où $a, b \in \mathbb{R}$.
2. Trouver a et b réels tel que le polynôme $P = X^3 + aX + b$ admette le nombre $z = 1 + i$ comme racine.
3. Montrer sans faire la division que $A = 2X^2 + X^3 - 6X^2 - X + 4$ est divisible par $B = X^2 - 1$.
4. Déterminer $n \in \mathbb{N}$ pour que le polynôme $(X + 1)^{2n+1} + X^{2n+2}$ soit divisible par le polynôme $X^2 + X + 1$.
5. Soient m, n et $p \in \mathbb{N}$. Montrer que le polynôme $X^{3m} + X^{3n+1} + X^{3p+2}$ divisible par $X^2 + X + 1$.

Polynômes : Polynômes scindés et Théorème de d'Alembert-Gauss

Nous admettrons le "**théorème fondamental de l'algèbre**" :

Théorème (d'Alembert-Gauss)

*Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine dans $\mathbb{C}$. On dit que $\mathbb{C}$ est un corps **algébriquement clos**.*

Corollaire

Soit $P \in \mathbb{C}[X]$ non constant de degré n. Il existe des nombres complexes $\lambda_1, \cdots, \lambda_n$, A tels que : $P = A \prod_{k=1}^{n} (X - \lambda_k)$.

Scanné avec CamScanner

Polynômes : Polynômes scindés et Théorème de d'Alembert-Gauss

Démonstration.

Prouvons la propriété par récurrence sur $n \geq 1$. Le résultat est clair au rang 1. Supposons le résultat acquis au rang $n \geq 1$ et considérons un polynôme P de degré $n+1$. D'après le théorème de d'Alembert-Gauss, P admet une racine $\lambda_{n+1} \in \mathbb{C}$. Ainsi, il existe $Q \in \mathbb{C}[X]$ tel que $P = (X - \lambda_{n+1})Q$. Comme $\deg(Q) = n$, on déduit de l'hypothèse au rang n l'existence de $\lambda_1, \cdots, \lambda_n$ et A dans $\mathbb{C}$ tels que : $Q = A\prod_{k=1}^{n}(X - \lambda_k)$.

D'où : $P = A\prod_{k=1}^{n+1}(X - \lambda_k)$.

L'hypothèse est donc vraie au rang $n+1$. On déduit du principe de récurrence que la propriété est vraie pour tout entier naturel non nul n. □

Polynômes : Polynômes scindés et Théorème de d'Alembert-Gauss

Définition (Polynôme scindé)

Soit $P \in \mathbb{K}[X]$. On dit que P est scindé (sur $\mathbb{K}$) s'il **N'est PAS CONSTANT** et possède exactement $\deg(P)$ racines (dans $\mathbb{K}$) comptées avec multiplicité.

Dire que P est scindé sur $\mathbb{K}$ revient donc à dire que P est de la forme : $P = A\prod_{k=1}^{r}(X - \lambda_k)^{m_k}$, où $\lambda_1, \cdots, \lambda_r$ sont les racines distinctes de P dans $\mathbb{K}$, de multiplicité respectives $m_1, \cdots, m_r$, et où A est son coefficient dominant.

- Autrement dit, un polynôme est scindé sur $\mathbb{K}$ si et seulement si il est le produit de polynômes de $\mathbb{K}[X]$ de degré un. On peut donc reformuler ainsi le théorème de d'Alembert-Gauss : tout polynôme non constant de $\mathbb{C}[X]$ est scindé sur $\mathbb{C}$.

Scanné avec CamScanner

Polynômes : Polynômes scindés et Théorème de d'Alembert-Gauss

Remarque

Deux polynômes P et Q de $\mathbb{K}[X]$ scindés sur $\mathbb{K}$ sont premiers entre eux si et seulement s'ils n'ont aucune racine commune.

Factorisation irréductible : Polynômes irréductibles

L'objectif de cette partie est de définir une classe de polynômes qui joueraient le même rôle que les nombres premiers sur $\mathbb{Z}$, puis d'en déduire l'analogue polynomial du théorème fondamental de l'arithmétique des nombres entiers.

Définition (Polynôme irréductible)

Un polynôme $P \in \mathbb{K}[X]$ est dit irréductible sur $\mathbb{K}$ si P **n'est PAS CONSTANT** et ses seuls diviseurs dans $\mathbb{K}[X]$ sont les polynômes constants et ceux de la forme λP, où $\lambda \in \mathbb{K}^*$.

Explication : Un polynôme P est irréductible s'il vérifie :

- $\deg(P) \geq 1$,
- les seuls diviseurs de P sont les éléments de $\mathbb{K}^*$ et les associés de P,

c-à-d tel que P soit non constant et que pour tout $A, B \in \mathbb{K}[X]$, on ait :
$P = AB \Rightarrow \Big(\deg(A) = 0 \text{ ou } \deg(B) = 0\Big)$.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Avant de décrire tous les irréductibles sur $\mathbb{R}$ et $\mathbb{C}$, nous passerons en revue quelques exemples.

Exemples

Tout polynôme de degré un est irréductible sur $\mathbb{K}$.

▶ *Soit P un polynôme de degré 1 et Q un diviseur de P. Il existe $Q_1 \in \mathbb{K}[X]$ tel que $P = QQ_1$. Donc $\deg(Q) \leq \deg(P)$. Ainsi Q est de degré 0 ou 1.*

- *Si $\deg(Q) = 0$, Q est constant non nul.*
- *Si $\deg(Q) = 1$, alors : $\deg(Q_1) = 0$, i.e. Q_1 est constant non nul a. Donc Q s'écrit : $Q = \frac{1}{a}P$.*

P n'est pas constant et ses seuls diviseurs sont les constantes non nulles et les polynômes de la forme λP, avec $\lambda \in \mathbb{K}^*$: P est irréductible sur $\mathbb{K}$.

Factorisation irréductible : Polynômes irréductibles

Exemples

Un polynôme de degré 2 est irréductible sur $\mathbb{K}$ si et seulement si il n'a pas de racine dans $\mathbb{K}$.

▶ *Soit $P \in \mathbb{K}[X]$ de degré 2.*

($\Rightarrow$) *Raisonnons par contraposée et supposons que P admet une racine a dans $\mathbb{K}$. Alors $X - a | P$ et donc P n'est pas irréductible.*

($\Leftarrow$) *Raisonnons par contraposée et supposons que P n'est pas irréductible. Il admet donc un diviseur unitaire Q qui est de degré 1. Ainsi, il existe $a \in \mathbb{K}$ tel que $Q = X - a | P$ d'où $P(a) = 0$. Le polynôme P admet donc une racine dans $\mathbb{K}$.*

Remarque

Un polynôme qui n'admet pas de racine dans $\mathbb{K}$ n'est pas nécessairement irréductible dans $\mathbb{K}[X]$, comme le prouve l'exemple de $(X^2 + 1)^2$ dans $\mathbb{R}[X]$.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Proposition

Les polynômes irréductibles de $\mathbb{C}[X]$ *sont les polynômes de degré* 1.

Démonstration.

On sait que tout polynôme de degré 1 est irréductible. Réciproquement, soit $P \in \mathbb{C}[X]$ irréductible. Etant **NON CONSTANT**, d'après le théorème de d'Alembert-Gauss, P possède une racine $a \in \mathbb{C}$ et donc $X - a$ divise P. L'irréductibilité de P sur $\mathbb{C}$ montre alors que P et $X - a$ sont associés, donc que P est de degré 1. □

Factorisation irréductible : Polynômes irréductibles

Proposition

Les polynômes irréductibles de $\mathbb{R}[X]$ *sont :*

- *les polynômes de degré* 1,
- *les polynômes de degré* 2 *à discriminant strictement négatif, i.e. sans racine réelle.*

Scanné avec CamScanner

Démonstration.

Soit $P \in \mathbb{R}[X]$ irréductible. Etant **NON CONSTANT**, d'après le théorème de d'Alembert-Gaus, P possède une racine a *COMPLEXE*. De plus, P étant à coefficients réels, alors $\bar{a}$ est aussi une racine de P.

- Si $a \in \mathbb{R}$, $X - a$ divise P dans $\mathbb{R}[X]$. Or, P est irréductible sur $\mathbb{R}$, donc P et $X - a$ sont associés et P est de degré 1.
- Si $a \notin \mathbb{R}$, alors $\bar{a} \neq a$, donc : $P = (X - a)(X - \bar{a})Q$ pour un certain $Q \in \mathbb{C}[X]$. En développant, on obtient : $P = (X^2 - 2Re(a)X + |a|^2)Q$, donc en réalité Q est à coefficients **RÉELS** par unicité de la division euclidienne dans $\mathbb{C}[X]$. De là, P étant irréductible sur $\mathbb{R}$, P et $X^2 - 2Re(a)X + |a|^2$ sont associés et P est de degré 2. De plus, P est bien sans racine réelle.

□

Factorisation irréductible : Polynômes irréductibles

Lemme (Euclide)

Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Si P divise un produit $\prod_{k=1}^{r} Q_k$ de $r \geq 2$ polynômes non nuls, alors il divise l'un des Q_k.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Démonstration.

On procède par récurrence sur $r \geq 2$.

- **Initialisation :** Soit P irréductible dans $\mathbb{K}[X]$. Supposons que $P|Q_1Q_2$, où Q_1 et Q_2 sont deux polynômes non nuls. Quitte à diviser par le coefficient dominant, on peut supposer que P est unitaire. Soit $D = P \wedge Q_1$. D étant un diviseur de P, il est égal à 1 ou P, puisque P est irréductible. Si $D = P$ alors $P|Q_1$. Si $D = 1$, alors $\exists U, V \in \mathbb{K}[X]$ tels que $UP + VQ_1 = 1$ et donc $P|Q_2 = UPQ_2 + VQ_1Q_2$.
- **Hérédité :** Supposons le résultat acquis pour $r - 1 \geq 2$ et soit P irréductible qui divise $\prod_{k=1}^{r} Q_k$. Si $P|Q_r$, c'est terminé, sinon il divise $\prod_{k=1}^{r-1} Q_k$ (cas $r = 2$) et l'hypothèse de récurrence permet de conclure.

□

Factorisation irréductible : Polynômes irréductibles

Théorème (Existence et unicité de la factorisation irréductible)

Tout polynôme non constant $P \in \mathbb{K}[X]$ est produit de polynômes irréductibles et une telle décomposition est unique à l'ordre près des facteurs, ce qui signifie qu'il existe une constante $A \in \mathbb{K}^*$, un entier $r \geq 1$, des polynômes unitaires $P_1, \cdots, P_r$ deux à deux distincts et irréductibles et des entiers naturels non nuls $m_1, \cdots, m_r$ tels que $P = A \prod_{k=1}^{r} P_k^{m_k}$.

L'unicité signifie que si on a une autre décomposition de même type $P = B \prod_{k=1}^{s} Q_k^{n_k}$, on a alors $B = A$, $s = r$ et il existe une permutation $\sigma \in \mathcal{S}_r$ telle que $Q_k = P_{\sigma(k)}$ et $n_k = m_{\sigma(k)}$ pour tout k compris entre 1 et r.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Démonstration :

Existence : On procède par récurrence sur le degré $n \geq 1$ de P.

- Initialisation : Pour $n = 1$, on a vu que le polynôme P est irréductible.
- Hérédité : Supposons le résultat acquis pour tous les polynômes de degré k compris entre 1 et $n-1 \geq 1$ et soit $P \in \mathbb{K}[X]$ de degré n. Si P est irréductible, c'est terminé. Sinon, P s'écrit $P = RS$ avec R, S non constants et degré compris entre 1 et $n-1$. Il suffit d'utiliser l'hypothèse de récurrence pour R et S.

Unicité : On procède également par récurrence sur le degré $n \geq 1$ de P.

- Initialisation : Pour $n = 1$, on a $P = A(X - \lambda)$ avec $A \in \mathbb{K}^*$ et $X - \lambda$ irréductible uniquement déterminés.
- Hérédité : Supposons le résultat acquis pour tous les polynômes de degré k compris entre 1 et $n-1 \geq 1$. Soit $P \in \mathbb{K}[X]$ de degré n ayant deux décompositions $P = A\prod_{k=1}^{r} P_k^{m_k} = B\prod_{k=1}^{s} Q_k^{n_k}$.

Factorisation irréductible : Polynômes irréductibles

L'identification des coefficients dominants nous donne $A = B$. Comme Q_1 est irréductible et divise $\prod_{k=1}^{r} P_k^{m_k}$, le lemme d'Euclide nous dit qu'il divise l'un des P_j, il est donc égal à ce P_j puisque ces deux polynômes sont irréductibles.

Supposons que $n_1 \leq m_j$. En divisant par $Q_1^{n_1}$, on a $Q_1^{m_j - n_1}\prod_{\substack{k=1\\k\neq j}}^{r} P_k^{m_k} = \prod_{k=2}^{s} Q_k^{n_k}$ et nécessairement $m_j = n_1$ (sinon le lemme d'Euclide nous dit Q_1 est égal à l'un des Q_k avec $k \geq 2$, ce qui n'est pas).

On note $j = \sigma(1)$ et on a $\prod_{\substack{k=1\\k\neq j}}^{r} = \prod_{k=2}^{s} Q_k^{n_k}$. L'hypothèse de récurrence permet alors de conclure.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

- La factorisation irréductible d'un polynôme non constant de $\mathbb{C}[X]$ coincide avec sa forme scindée.
- Le théorème de décomposition en facteurs irréductibles dans $\mathbb{R}[X]$ prend la forme suivante :

Théorème

Tout polynôme non constant $P \in \mathbb{R}[X]$ est produit de polynômes irréductibles de degré 1 ou 2, c-à-d qu'il existe une constante $A \in \mathbb{R}^*$, deux entiers naturels r et s, des réels $a_1, \cdots, a_r$ deux à deux distincts, des entiers naturels non nuls $n_1, \cdots, n_r$, des couples réels $(b_1, c_1), \cdots, (b_s, c_s)$ deux à deux distincts tels que $b_k^2 - 4c_k < 0$ pour tout k et des entiers naturels non nuls $m_1, \cdots, m_s$ tels que

$$P = A \prod_{k=1}^{r} (X - a_k)^{n_k} \prod_{k=1}^{s} (X^2 + b_k X + c_k)^{m_k},$$

une telle décomposition est unique à l'ordre près des facteurs.

Factorisation irréductible : Polynômes irréductibles

En pratique : Pour factoriser un polynôme P dans $\mathbb{R}[X]$, on peut, si l'on ne trouve pas de méthode plus simple, factoriser d'abord ce polynôme dans $\mathbb{C}[X]$.
On sait que si b est une racine de P dans $\mathbb{C}$, alors $\bar{b}$ est aussi une racine de P dans $\mathbb{C}$.
Soit $a_1, \cdots, a_r$ les racines réelles de P, $b_1, \bar{b}_1, \cdots, b_s, \bar{b}_s$ les racines comlexes (non réelles) de P, alors :

dans $\mathbb{C}[X]$: $P = A \prod_{k=1}^{r} (X - a_k) \prod_{k=1}^{s} (X - b_k)(X - \bar{b}_k)$, donc

dans $\mathbb{R}[X]$: $P = A \prod_{k=1}^{r} (X - a_k) \prod_{k=1}^{s} (X^2 - 2Re(b_k)X + |b_k|^2)$.

- On peut retenir que :
  - e^{it} et $e^{it'}$ sont des complexes conjugués $\Leftrightarrow \exists k \in \mathbb{Z} | t + t' = 2k\pi$.
  - $(X - b)(X - \bar{b}) = X^2 - 2Re(b)X + |b|^2 \in \mathbb{R}[X]$.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Exemples

Décomposons en produit de facteurs irréductibles sur $\mathbb{R}$ et sur $\mathbb{C}$ le polynôme $P = X^n - 1$.

- Dans $\mathbb{C}[X]$, le polynôme $X^n - 1$ est unitaire et admet n racines simples, les nombres $z_k = e^{\frac{2ik\pi}{n}}, 0 \leqslant k \leqslant n-1$. Donc,

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right).$$

Factorisation irréductible : Polynômes irréductibles

- Dans $\mathbb{R}[X]$, il y a deux cas.
  - Si $n = 2p, p \in \mathbb{N}^*$, $X^n - 1 = X^{2p} - 1$ admet 2 racines réelles : 1 et -1. En regroupant les facteurs conjugués, on obtient :

$$X^{2p} - 1 = \prod_{k=0}^{2p-1} \left(X - e^{\frac{2ik\pi}{2p}} \right)$$

$$= (X-1) \times \prod_{k=1}^{p-1} \left(X - e^{\frac{ik\pi}{p}} \right) \times (X+1) \times \prod_{k=p+1}^{2p-1} \left(X - e^{\frac{ik\pi}{p}} \right)$$

$$= (X-1)(X+1) \prod_{k=1}^{p-1} \left(X - e^{\frac{ik\pi}{P}} \right) \prod_{\ell=1}^{p-1} \left(X - e^{\frac{i(2p-\ell)\pi}{p}} \right)$$

$$= (X-1)(X+1) \prod_{k=1}^{p-1} \left(X - e^{\frac{ik\pi}{p}} \right) \left(X - e^{-\frac{ik\pi}{p}} \right)$$

$$= (X-1)(X+1) \prod_{k=1}^{p-1} \left(X^2 - 2X\cos(\frac{k\pi}{p}) + 1 \right).$$

Scanné avec CamScanner

- Si $n = 2p+1, p \in \mathbb{N}^*, X^n - 1 = X^{2p+1} - 1$ admet une seule racine réelle à savoir 1. En regroupant les facteurs conjugués, on obtient

$$X^{2p+1} - 1 = \sum_{k=0}^{2p} \left(X - e^{\frac{2ik\pi}{2p+1}} \right)$$

$$= (X-1) \times \prod_{k=1}^{p} \left(X - e^{\frac{2ik\pi}{2p+1}} \right) \times \prod_{k=p+1}^{2p} \left(X - e^{\frac{2ik\pi}{2p+1}} \right)$$

$$= (X-1) \prod_{k=1}^{p} \left(X - e^{\frac{2ik\pi}{2p+1}} \right) \left(X - e^{-\frac{2ik\pi}{2p+1}} \right)$$

$$= (X-1) \prod_{k=1}^{p} \left(X^2 - 2X \cos\left(\frac{2k\pi}{2p+1} \right) + 1 \right).$$

Exemples

Décomposons en produit de facteurs irréductibles sur $\mathbb{C}$ le polynôme $P = X^{n-1} + X^{n-2} + \cdots + X + 1$.

- *Dans $\mathbb{C}[X]$, on a*

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right) = (X-1) \prod_{k=1}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right)$$

mais aussi

$$X^n - 1 = (X-1)\left(X^{n-1} + \ldots + X + 1 \right).$$

Après simplification par le polynôme non nul $X - 1$, on obtient :

$$X^{n-1} + \ldots + X + 1 = \prod_{k=1}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right).$$

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Exercice

Déterminer la décomposition en produit de facteurs irréductibles sur $\mathbb{R}$ du polynôme $P = (X+1)^7 - X^7 - 1$ sachant que j est une racine multiple de P.

Factorisation irréductible : Polynômes irréductibles

Solution

N'oublions pas la périodicité des puissances de j $\Big((j_n)_{n\in\mathbb{N}} = (1, j, j^2, 1, j, j^2, \cdots)\Big)$ ni la relation bien connue $1 + j + j^2 = 0$.

On a $P(j) = 0$. De même, on vérifie que $P'(j) = 0$. En revanche, $P''(j) = 42 \neq 0$. Ainsi, le nombre complexe j est une racine de P de multiplicité 2. Les nombres 0 et -1 sont des racines évidentes de P. Puisque $P \in \mathbb{R}[X]$, $\bar{j} = j^2$ en est également une racine de multiplicité 2. Le polynôme P est donc divisible par $Q = X(X+1)(X-j)^2(X-j^2)^2 = X(X+1)(X^2+X+1)^2$. D'autre part, en appliquant la formule du Binôme, on obtient :

$$P = \sum_{k=0}^{7} C_7^k X^k - X^7 - 1 = \sum_{k=1}^{6} C_7^k X^k.$$ P est donc de degré 6, de coefficient dominant égal à $C_7^6 = 7$. Puisque Q est unitaire de degré 6 et qu'il divisise P, on a $P = 7X(X+1)(X^2+X+1)^2$.

Scanné avec CamScanner

Factorisation irréductible : Polynômes irréductibles

Exercice

On considère le polynôme $P = X^5 - 1$.

1. Décomposer P dans $\mathbb{C}[X]$.
2. En déduire les racines de $Q = X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{C}$.
3. Décomoser Q dans $\mathbb{R}[X]$.
4. En déduire la valeur de $r_1 = \cos(\frac{2\pi}{5})$ et $r_2 = \cos(\frac{4\pi}{5})$.

Fractions rationnelles : Introduction

Soit $\mathbb{K}$ un corps commutatif. Nous savons que l'ensemble $\mathbb{K}[X]$ des polynômes à une indéterminée à coefficients dans $\mathbb{K}$ est un anneau commutatif intègre dans lequel les seuls éléments inversibles sont les polynômes de degré 0. $\mathbb{K}[X]$ n' est donc pas un corps, mais on peut construire le corps des fractions de $\mathbb{K}[X]$. Ce corps s'appelle le **corps des fractions rationnelles** à une indéterminée à coefficients dans $\mathbb{K}$. On le note $\mathbb{K}(X)$.

Scanné avec CamScanner

Fractions rationnelles : Construction

On pose comme d'habitude $\mathbb{K}[X]^* = \mathbb{K}[X] \setminus \{0\}$.

- $\mathbb{K}(X)$ est l'ensemble quotient de $\mathbb{K}[X] \times \mathbb{K}[X]^*$ par la relation d'équivalence $\mathcal{R}$: $(P, Q)\mathcal{R}(P_1, Q_1) \Leftrightarrow PQ_1 = P_1Q$. Une fraction rationnelle F de $\mathbb{K}(X)$ est donc une classe d'équivalence représentée par un couple (P, Q) d'élément de $\mathbb{K}[X]$ dans lequel $Q \neq 0$; un autre couple (P_1, Q_1) représente la même fraction rationnelle F si, et seulement si $PQ_1 = P_1Q$.
  Si (P, Q) est un représentant quelconque de F, on convient d'écrire $F = \frac{P}{Q}$; on dit que P est le numérateur et que Q est le dénominateur de la fraction rationnelle F.
- Dans $\mathbb{K}[X] \times \mathbb{K}[X]^*$ on définit l'addition et la multiplication en posant : $(P, Q) + (P_1, Q_1) = (PQ_1 + P_1Q, QQ_1)$ et $(P, Q) \cdot (P_1, Q_1) = (PP_1, QQ_1)$.

Fractions rationnelles : Construction

Les deux lois de $\mathbb{K}(X)$ sont les lois quotients et on les note aussi, $+$ et $\cdot$; alors le triplet $(\mathbb{K}(X), +, \cdot)$ est un corps commutatif. L'élément neutre pour l'addition est la fraction rationnelle nulle 0 qui est la classe des couples $(0, Q)$ tels que $Q \neq 0$. L'élément neutre pour la multiplication, appelée fraction rationnelle unité, et notée 1, est la classe des couples (Q, Q) avec $Q \neq 0$. Pour la multiplication, l'inverse de la fraction rationnelle non nulle F, classe de (P, Q) avec $P \neq 0$ et $Q \neq 0$ est la fraction rationnelle notée $\frac{1}{F}$.
L'application qui, à $P \in \mathbb{K}[X]$, associe la fraction rationnelle dont un représentant est le couple $(P, 1)$, est un morphisme injectif de l'anneau $\mathbb{K}[X]$ dans l'anneau $\mathbb{K}(X)$. On peut donc identifier $\mathbb{K}[X]$ au sous-anneau de $\mathbb{K}(X)$ constitué par les fractions rationnelles dont les représentants sont de la forme $(P, 1)$.

Scanné avec CamScanner

Fractions rationnelles : Définition, règles de calcul

On a les règles de calcul suivantes (dans lesquelles Q, Q_1 et R sont des polynômes non nuls) :

- $\dfrac{P}{Q} + \dfrac{P_1}{Q_1} = \dfrac{PQ_1 + P_1Q}{QQ_1}$.
- $\dfrac{P}{Q}\dfrac{P_1}{Q_1} = \dfrac{PP_1}{QQ_1}$.
- $\dfrac{P}{Q} = \dfrac{P_1}{Q_1} \Leftrightarrow PQ_1 = P_1Q$.
- $\dfrac{PR}{QR} = \dfrac{P}{Q}$.
- Si $P \neq 0$, $\left(\dfrac{P}{Q}\right)^{-1} = \dfrac{Q}{P}$.

Fractions rationnelles : Définition, règles de calcul

- Conjuguée d'une fraction rationnelle à coefficients complexes :
  Si (P, Q) et (P_1, Q_1) sont deux représentants d'une fraction rationnelle F à coefficients dans $\mathbb{C}$, alors $\dfrac{\overline{P}}{\overline{Q}} = \dfrac{\overline{P_1}}{\overline{Q_1}}$ puisque l'on a :

$$PQ_1 = P_1Q \Leftrightarrow \overline{P}\,\overline{Q_1} = \overline{P_1}\,\overline{Q}.$$

Cette fraction rationnelle est appelée conjuguée de F et notée $\overline{F}$.
Les propriétés sur les polynômes nous donnent immédiatement, pour $(F, G) \in \mathbb{C}(X)^2$:

$$\overline{F+G} = \overline{F} + \overline{G} \quad \text{et} \quad \overline{FG} = \overline{F}\,\overline{G}$$

Scanné avec CamScanner

Fractions rationnelles : Représentant irréductible

Définition

- On appelle *représentant irréductible* d'une fraction rationnelle F tout représentant (P, Q) de F où P et Q sont premiers entre eux.
- On appelle *représentant irréductible unitaire* d'une fraction rationnelle F tout représentant irréductible (P, Q) de F tel que Q soit un polynôme unitaire.

Proposition

- *Si* $\frac{P}{Q}$ *est une forme irréductible d'une fraction rationnelle* $F = \frac{P_1}{Q_1}$, *alors :* $\exists R \in \mathbb{K}[X] : (P_1 = RP \quad et \quad Q_1 = RQ)$.
- *Si* $\frac{P}{Q}$ *et* $\frac{P_1}{Q_1}$ *sont deux formes irréductibles d'une fraction* F, *alors :* $\exists \lambda \in \mathbb{K}^* : (P_1 = \lambda P \quad et \quad Q_1 = \lambda Q)$.
- *Toute fraction rationnelle admet un représentant irréductible unitaire et un seul.*

Fractions rationnelles : Représentant irréductible

Démonstration.

- On a $PQ_1 = QP_1$ et donc Q divise PQ_1. Comme P et Q sont premiers entre eux, on en déduit d'après le théorème de Gauss que Q divise Q_1. On peut donc trouver un polynôme $R \in \mathbb{K}[X]$ tel que $Q_1 = RQ$, et l'on a : $P_1 = \frac{PQ_1}{Q} = RP$.
- Soient (P, Q) et (P_1, Q_1) deux représentants irréductibles de F. Alors, d'après le point précédent, $Q|Q_1$ et $Q_1|Q$. Les polynômes Q et Q_1 sont donc associés et par conséquent, le polynôme R est une constante non nulle.
- L'unicité est évidente d'après ce qui précède. Pour l'existence, il suffit de prendre un représentant quelconque (P, Q), de diviser P et Q par leur PGCD et de diviser le numérateur et le dénominateur par le coefficient dominant de ce dernier (qui est non nul).

□

Scanné avec CamScanner

Fractions rationnelles : Degré d'une fraction rationnelle

Définition

Si F est une fraction rationnelle, la quantité $\deg(P) - \deg(Q) \in \mathbb{Z} \cup \{-\infty\}$ ne dépend pas du représentant (P, Q) choisi pour la fraction F. On l'appelle degré de F et on le note $\deg(F)$ ou $\deg F$. En particulier, on a $\deg 0 = -\infty$.

- On peut bien définir ainsi le degré de F car :
  - la quantité $\deg(P) - \deg(Q)$ est toujours définie puisque Q étant non nul, on a $\deg(Q) \neq -\infty$.
  - la quantité $\deg(P) - \deg(Q)$ ne dépend pas du représentant (P, Q) choisi pour la fraction rationnelle F, car si (P_1, Q_1) est un autre représentant, on a $PQ_1 = QP_1$ et donc :
    $\deg(P) + \deg(Q_1) = \deg(PQ_1) = \deg(P_1Q) = \deg(P_1) + \deg(Q)$
    c'est-à-dire, puisque $\deg(Q)$ et $\deg(Q_1)$ sont des entiers naturels :
    $\deg(P) - \deg(Q) = \deg(P_1) - \deg(Q_1)$.

Fractions rationnelles : Degré d'une fraction rationnelle

Remarque

Un polynôme P est égal à la fraction $\frac{P}{1}$ dont le degré est $\deg(P)$. Donc la définition du degré sur $\mathbb{K}(X)$ prolonge celle du degré défini sur $\mathbb{K}[X]$.

Proposition

Étant données deux fractions rationnelles F_1 et F_2 de $\mathbb{K}(X)$, on a :

1. $\deg(F_1 + F_2) \leq \max(\deg(F_1), \deg(F_2))$.
2. $\deg(F_1F_2) = \deg(F_1) + \deg(F_2)$.

Scanné avec CamScanner

Fractions rationnelles : Racines, pôles

Définition

Soit F une fraction rationnelle de forme irréductible $\frac{P}{Q}$.

- On appelle racine de F toute racine de P.
- On appelle pôle de F toute racine de Q.
- Si a est une racine (respectivement un pôle) de $F \neq 0$, l'ordre de multiplicité de a est l'ordre de multiplicité de a en tant que racine du polynôme P (respectivement Q).

Remarque

Un élément a de $\mathbb{K}$ ne peut pas être à la fois racine et pôle d'une fraction rationnelle F. Sinon, en prenant une forme irréductible $F = \frac{P}{Q}$, on aurait $P(a) = Q(a) = 0$, et donc les polynômes P et Q seraient divisibles par $X - a$, ce qui contredirait le caractère irréductible de $\frac{P}{Q}$.

Fractions rationnelles : Racines, pôles

Attention : Les racines (respectivement les pôles) d'une fraction rationnelle F ne peuvent être obtenues qu'à partir d'une forme irréductible de F. Par exemple, $F = \frac{X^3 - 1}{X^2 - 1}$ n'admet 1 ni comme racine ni comme pôle, car $F = \frac{X^2 + X + 1}{X + 1}$.

Définition

Soit F une fraction rationnelle, de forme irréductible $\frac{P}{Q}$, dont on désigne par A l'ensemble des pôles.

- Pour $\alpha \in \mathbb{K} \setminus A$, on définit $F(\alpha) = \frac{P(\alpha)}{Q(\alpha)}$.
- La fonction définie sur $\mathbb{K} \setminus A$ par $x \mapsto F(x)$ est appelée fonction rationnelle associée à la fraction rationnelle F.

Scanné avec CamScanner

Fractions rationnelles : Composition

Si $F = \dfrac{P}{Q}$ est une fraction rationnelle et R un polynôme non constant, alors le polynôme $Q \circ R$ est non nul, puisqu'il est de degré $\deg(Q)\deg(R)$. De plus, si (P_1, Q_1) est un autre représentant de la fraction F, l'égalité $PQ_1 = P_1Q$ entraîne $(P \circ R)(Q_1 \circ R) = (P_1 \circ R)(Q \circ R)$. Le quotient $\dfrac{P \circ R}{Q \circ R}$ ne dépend donc pas du représentant (P, Q) choisi pour la fraction rationnelle F. C'est une fraction rationnelle dont le degré vaut $\deg(F)\deg(R)$, que l'on l'appelle composée de F par R et que l'on note $F(R)$.

Fractions rationnelles : Décomposition en éléments simples

Proposition (Partie entière)

Toute fraction rationnelle F s'écrit de façon unique comme la somme d'un polynôme, appelé partie entière de F, et d'une fraction rationnelle de degré strictement négatif.

Démonstration.

Unicité : Supposons : $F = E_1 + F_1 = E_2 + F_2$ avec $(E_1, E_2) \in \mathbb{K}[X]^2$, $(F_1, F_2) \in \mathbb{K}(X)^2$, $\deg(F_1) < 0$ et $\deg(F_2) < 0$. Alors $E_1 - E_2$ est un polynôme, et comme il est égal à $F_2 - F_1$, son degré est strictement négatif. Donc $E_1 - E_2 = 0$ c'est-à-dire $E_1 = E_2$ et par suite $F_1 = F_2$.

Existence : Soit $F = \dfrac{P}{Q}$ une fraction rationnelle, avec $Q \neq 0$. Si l'on appelle E le quotient et R le reste de la division euclidienne de P par Q, on obtient : $F = E + \dfrac{R}{Q}$ avec $\deg(R) < \deg(Q)$, ce qui constitue l'écriture cherchée. □

Scanné avec CamScanner

Méthode

D'après la démonstration précédente, la partie entière d'une fraction rationnelle $F = \dfrac{P}{Q}$ est le quotient de la division euclidienne du numérateur P par le dénominateur Q.

Exemples

- *Si* $\deg(F)$, *alors sa partie entière est nulle.*
- *Si* F *est de degré* 0, *alors sa partie entière est le polynôme constant quotient du coefficient dominant du numérateur par celui du dénominateur.*
- *La partie entière de la fraction* $\dfrac{X^5}{(X^2+X+1)^2}$ *est* $X-2$.

Proposition (Partie polaire)

Si F *est une fraction rationnelle admettant a pour pôle d'ordre* n, *il existe un unique* n*-uplet de scalaires* $(\lambda_p)_{1\leq p\leq n}$ *et une unique fraction* F_0 *n'admettant pas a pour pôle tels que :*

$$F = \sum_{p=1}^{n} \frac{\lambda_p}{(X-a)^p} + F_0.$$

La quantité $\displaystyle\sum_{p=1}^{n} \frac{\lambda_p}{(X-a)^p}$ *s'appelle la partie polaire de* F *relative au pôle* a.

Scanné avec CamScanner

Fractions rationnelles : Décomposition en éléments simples

Méthode

Soit F une fraction rationnelle admettant a pour pôle.

- Si a est pôle d'ordre 1 de F, on peut écrire $F = \dfrac{P}{(X-a)Q_1}$ où Q_1 est un polynôme n'admettant pas a pour racine. On cherche le scalaire λ_1 tel que : $F = \dfrac{\lambda_1}{X-a} + F_0$ où F_0 est une fraction rationnelle qui n'admet pas a pour pôle. En multipliant cette égalité par $X-a$, on obtient : $\dfrac{P}{Q_1} = \lambda_1 + (X-a)F_0$ ce qui, en substituant a à X, donne $\lambda_1 = \dfrac{P(a)}{Q_1(a)}$. La partie polaire relative au pôle a est donc : $\dfrac{\lambda_1}{X-a}$ avec $\lambda_1 = \dfrac{P(a)}{Q_1(a)} = \dfrac{P(a)}{Q'(a)}$ la dernière égalité venant de la relation $Q' = (X-a)Q_1' + Q_1$.

Fractions rationnelles : Décomposition en éléments simples

- Si a est pôle d'ordre 2 de F, on peut écrire $F = \dfrac{P}{(X-a)^2 Q_2}$ où Q_2 est un polynôme n'admettant pas a pour racine. On cherche les scalaire λ_1 et λ_2 tels que : $F = \dfrac{\lambda_2}{(X-a)^2} + \dfrac{\lambda_1}{X-a} + F_0$ où F_0 est une fraction rationnelle qui n'admet pas a pour pôle. En multipliant cette égalité par $(X-a)^2$, on obtient : $\dfrac{P}{Q_2} = \lambda_2 + \lambda_1(X-a) + (X-a)^2 F_0$ ce qui, en substituant a à X, donne $\lambda_2 = \dfrac{P(a)}{Q_2(a)}$. La partie polaire relative au pôle a est donc : $\dfrac{\lambda_2}{(X-a)^2} + \dfrac{\lambda_1}{X-a}$ avec $\lambda_2 = \dfrac{P(a)}{Q_2(a)}$. Pour trouver λ_1, on peut alors retrancher $\dfrac{\lambda_2}{(X-a)^2}$ pour obtenir une fraction dont a n'est pas pôle, ou est pôle simple ce qui ramène au cas précédent.

Scanné avec CamScanner

Fractions rationnelles : Décomposition en éléments simples

- Dans le cas général, si a est pôle d'ordre n de F, alors $F = \dfrac{P}{(X-a)^n Q_n}$ avec $Q_n(a) \neq 0$ et la partie polaire relative au pôle a est : $\displaystyle\sum_{p=1}^{n} \frac{\lambda_p}{(X-a)^p}$ avec $\lambda_n = \dfrac{P(a)}{Q_n(a)}$, comme on le voit en multipliant l'égalité : $F = \displaystyle\sum_{p=1}^{n} \frac{\lambda_p}{(X-a)^p} + F_0$ par $(X-a)^n$ et en substituant a à X. Comme de plus, $Q = (X-a)^n Q_n$, alors on a $Q_n(a) = \dfrac{Q^{(n)}(a)}{n!}$ (par exemple en utilisant la formule de Leibniz ou la formule de Taylor).

Fractions rationnelles : Décomposition en éléments simples

Exemples

1. *Soit* $F = \dfrac{X^5+1}{X(X-1)^2}$.
   - *La partie polaire associée au pôle* 0 *est* $\dfrac{\lambda}{X}$ *avec* $\lambda = 1$.
   - *La partie polaire associée au pôle* 1 *est* $\dfrac{\lambda}{X-1} + \dfrac{\mu}{(X-1)^2}$ *avec* $\mu = 2$.

     Comme : $F - \dfrac{2}{(X-1)^2} = \dfrac{X^4+X^3+X^2+X-1}{X(1-X)}$ *on en déduit* $\lambda = 3$.
2. *Soit* $F = \dfrac{1}{X^5-1}$. *Si* ω *est un pôle de* F, *c'est-à-dire une racine cinquième de l'unité, alors la partie polaire associée à* ω *est* $\dfrac{\lambda}{X-\omega}$ *avec :* $\lambda = \dfrac{1}{5\omega^4} = \dfrac{\omega}{5\omega^5} = \dfrac{\omega}{5}$.

Scanné avec CamScanner

Fractions rationnelles : Décomposition en éléments simples

Théorème (Décomposition en éléments simples sur $\mathbb{C}$)

Étant donnée une fraction rationnelle $F \in \mathbb{C}(X)$ dont les pôles sont $a_1, a_2, \cdots, a_n$ distincts deux à deux et d'ordres de multiplicité respectifs $r_1, r_2, \cdots, r_n$, il existe un unique polynôme $E \in \mathbb{C}[X]$ et une unique famille de scalaires $(\lambda_{i,j})_{\substack{1\leq i\leq n \\ 1\leq j\leq r_i}}$ tels que :

$$F = E + \sum_{i=1}^{n} \left(\underbrace{\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X-a_i)^j}}_{\text{Partie polaire associé au pôle } a_i} \right).$$

Autrement dit, toute fraction rationnelle de $\mathbb{C}(X)$ est la somme de sa partie entière et des parties polaires associées à chacun de ses pôles. Cette décomposition s'appelle la décomposition en éléments simples dans $\mathbb{C}(X)$ de la fraction F.

Fractions rationnelles : Décomposition en éléments simples

Méthodes pratiques

Soit $F = \dfrac{P}{Q}$ une fraction rationnelle à coefficients complexes dont les pôles sont $a_1, a_2, \cdots, a_n$ d'ordres de multiplicité respectifs $r_1, r_2, \cdots, r_n$. Sa décomposition en éléments simples est de la forme :

$$F = E + \sum_{i=1}^{n} \left(\sum_{j=1}^{r_i} \frac{\lambda_{i,j}}{(X-a_i)^j} \right).$$

- La détermination de la partie entière E se fait à l'aide de la division euclidienne de P par Q, division limitée puisque seul le quotient nous intéresse.
- Les coefficients λ_{i,r_i} se calculent immédiatement à l'aide des formules : $\lambda_{i,r_i} = \dfrac{P(a_i)}{Q_i(a_i)} = \dfrac{r_i! P(a_i)}{Q^{(r_i)}(a_i)}$ avec $Q = (X-a_i)^{r_i} Q_i$.

Scanné avec CamScanner

Fractions rationnelles : Décomposition en éléments simples

- Si tous les pôles sont simples, on a ainsi la décomposition en éléments simples de F. Sinon, on peut retrancher à F chaque fraction $\frac{\lambda_{i,r_i}}{(X-a_i)^{r_i}}$ et recommencer avec la fraction ainsi obtenue. Mais il est souvent beaucoup plus rapide de déterminer les derniers coefficients en utilisant certaines des méthodes qui suivent :

Si la fraction est à coefficients réels

Si F est une fraction rationnelle à coefficients réels et si a est un pôle non réel de F d'ordre r, alors $\bar{a}$ est aussi un pôle d'ordre r et les coefficients des parties polaires associées à a et $\bar{a}$ sont conjugués deux à deux. En effet :

- Puisque le dénominateur Q de F est réel, si a est une racine non réelle de Q, alors $\bar{a}$ est aussi racine de Q au même ordre de multiplicité.

Fractions rationnelles : Décomposition en éléments simples

- Si $F = \sum_{i=1}^{r} \frac{\lambda_i}{(X-a)^i} + F_1$ où a n'est pas pôle de la fraction rationnelle F_1, alors $F = \overline{F} = \sum_{i=1}^{r} \frac{\overline{\lambda_i}}{(X-\bar{a})^i} + \overline{F_1}$ et la fraction rationnelle $\overline{F_1}$ n'admet pas $\bar{a}$ pour pôle. Donc, la partie polaire associée au pôle $\bar{a}$ est : $\sum_{i=1}^{r} \frac{\overline{\lambda_i}}{(X-\bar{a})^i}$ (unicité de la partie polaire).

Si la fraction est paire ou impaire

Si la fraction rationnelle F est paire ou impaire et que a est un pôle de F d'ordre n, alors $-a$ est aussi pôle de F d'ordre n et la comparaison des décompositions en éléments simples de $F(X)$ et $F(-X) = \pm F(X)$ donne des relations entre les coefficients.

Scanné avec CamScanner

Fractions rationnelles : Décomposition en éléments simples

Exemple : La fraction $F = \dfrac{4}{(X^2-1)^2}$ se décompose en éléments simples : $F = \dfrac{a}{X-1} + \dfrac{b}{X+1} + \dfrac{c}{(X-1)^2} + \dfrac{d}{(X+1)^2}$. On a :

$$F(X) = F(-X) = \frac{a}{-X-1} + \frac{b}{-X+1} + \frac{c}{(-X-1)^2} + \frac{d}{(-X+1)^2}.$$

L'unicité de la décomposition en éléments simples nous donne alors $a = -b$ et $c = d$.

- On a immédiatement $c = \dfrac{4}{(1+1)^2} = 1$, donc $c = d = 1$.
- Pour déterminer a et b, il suffit de substituer 0 à X, ce qui donne : $4 = -a + b + c + d = 2 - 2a$, donc $a = -1$ et $b = 1$.

On a donc : $F = \dfrac{-1}{X-1} + \dfrac{1}{X+1} + \dfrac{1}{(X-1)^2} + \dfrac{1}{(X+1)^2}$.

Fractions rationnelles : Décomposition en éléments simples

Si la fraction est de degré strictement négatif

Soit F une fraction rationnelle de degré strictement négatif. Si f est la restriction à $\mathbb{R}$ de sa fonction rationnelle associée, alors la fonction $x \mapsto xf(x)$ a une limite finie en l'infini : on peut ainsi trouver des relations entre les coefficients des termes en $\dfrac{1}{X-a_i}$ de la décomposition en éléments simples de F.

Exemple : Soit la fraction rationnelle $F = \dfrac{4X^3}{(X^2-1)^2}$. L'imparité de F nous dit que sa décomposition en éléments simples est du type : $F = \dfrac{a}{X-1} + \dfrac{a}{X+1} + \dfrac{b}{(X-1)^2} - \dfrac{b}{(X+1)^2}$. Alors $b = 1$ et puisque $\lim\limits_{x \to +\infty} xf(x) = 4$, on a $2a = 4$. Donc :

$$F = \frac{2}{X-1} + \frac{2}{X+1} + \frac{1}{(X-1)^2} - \frac{1}{(X+1)^2}.$$

Scanné avec CamScanner

S'il ne reste qu'un ou deux coefficients à calculer

Lorsqu'il ne reste plus qu'un ou deux coefficients à déterminer, on peut substituer à X une ou deux valeurs simples.

Exemple : Soit $F = \dfrac{X^4+1}{(X+1)^2(X^2+1)} = 1 + \dfrac{a}{(X+1)^2} + \dfrac{b}{X+1} + \dfrac{c}{X-i} - \dfrac{\bar{c}}{X+i}$. On trouve d'abord : $c = \dfrac{i^4+1}{(i+1)^2(i+i)} = \dfrac{2}{(2i)^2} = -\dfrac{1}{2}$ et $a = \dfrac{1+1}{1+1} = 1$. En substituant 0 à X, on obtient de plus : $1 = 1 + a + b - \dfrac{c}{i} + \dfrac{\bar{c}}{i} = 2 + b$ et donc $b = -1$. D'où :

$$F = \frac{X^4+1}{(X+1)^2(X^2+1)} = 1 + \frac{1}{(X+1)^2} - \frac{1}{X+1} - \frac{1}{2(X-i)} - \frac{1}{2(X+i)}.$$

Théorème (Décomposition en éléments simples sur $\mathbb{R}$)

*Soit $F = \dfrac{P}{Q} \in \mathbb{R}(X)$ **irréductible** de partie entière E. On introduit la factorisation irréductible de Q : $Q = B\prod_{i=1}^{r}(X-a_i)^{n_i}\prod_{j=1}^{s}(X^2+b_jX+c_j)^{m_j}$.*

Il existe des familles uniques $(\lambda_{i,k})_{\substack{1\le i\le r\\ 1\le k\le n_i}}$, $(u_{j,k})_{\substack{1\le j\le s\\ 1\le k\le m_j}}$ et $(v_{j,k})_{\substack{1\le j\le s\\ 1\le k\le m_j}}$ de réels telles que :

$$F = E + \sum_{i=1}^{r}\sum_{k=1}^{n_i}\frac{\lambda_{i,k}}{(X-a_i)^k} + \sum_{j=1}^{s}\sum_{k=1}^{m_j}\frac{u_{j,k}X+v_{j,k}}{(X^2+b_jX+c_j)^k}.$$

En pratique : Quand les pôles **non réels** d'une fraction **réelle** sont **simples**, on peut obtenir la décomposition en éléments simples sur $\mathbb{R}$ facilement à partir de la décomposition en éléments simples sur $\mathbb{C}$ par simple regroupement des parties polaires conjuguées.

Scanné avec CamScanner

Fractions rationnelles : Décomposition en éléments simples

Définition

Dans la décomposition en éléments simples d'une fraction rationnelle dans $\mathbb{R}(X)$, une fraction de la forme $\frac{\lambda_{i,k}}{(X-a_i)^k}$ s'appelle **un élément simple de première espèce**, une fraction de la forme $\frac{u_{j,k}X+v_{j,k}}{(X^2+b_jX+c_j)^k}$ s'appelle **un élément simple de deuxième espèce**.

Fractions rationnelles : Décomposition en éléments simples

Exemples

Décomposition en éléments simples de $\frac{P}{Q}=\frac{3X^4+5X^3+8X^2+5X+3}{(X^2+X+1)^2(X-1)}$.

- *Comme* $\deg(P)<\deg(Q)$ *alors* $E(X)=0$. *Le dénominateur est déjà factorisé sur* $\mathbb{R}$ *car* X^2+X+1 *est irréductible. La forme de la décomposition en éléments simples sur* $\mathbb{R}$ *est donc :*

$\frac{P}{Q}=\frac{aX+b}{(X^2+X+1)^2}+\frac{cX+d}{X^2+X+1}+\frac{e}{X-1}$. *Il faut ensuite mener au mieux les calculs pour déterminer les coefficients afin d'obtenir :*

$\frac{P}{Q}=\frac{2X+1}{(X^2+X+1)^2}+\frac{-1}{X^2+X+1}+\frac{3}{X-1}$.

Scanné avec CamScanner

Algèbre1
Chapitre 4: Espaces vectoriels et applications linéaires

Jawad SALHI

Faculté des Sciences et Techniques - Errachidia

A.U. 2020/2021

Plan

1. Structure d'espace vectoriel
2. Applications linéaires

Scanné avec CamScanner

Structure d'espace vectoriel : e.v et combinaisons linéaires

Dans ce chapitre, $\mathbb{K}$ est l'un des corps $\mathbb{R}$ ou $\mathbb{C}$ et I est un ensemble non vide quelconque.
La notion d'espace vectoriel introduite dans ce chapitre est un nouvel exemple fondamental de structure algébrique, après les groupes, les anneaux et les corps. Comme nous le verrons, la notion d'espace vectoriel généralise, comme son nom l'indique, les notions de vecteurs du plan et de l'espace introduites au lycée.
La théorie mathématique des espaces vectoriels s'appelle l'algèbre linéaire.

Structure d'espace vectoriel : e.v et combinaisons linéaires

Définition (Espace vectoriel)

On appelle $\mathbb{K}$-espace vectoriel ou espace vectoriel sur $\mathbb{K}$ tout triplet $(E, +, \cdot)$ vérifiant les propriétés suivantes :

- $(E, +)$ est un groupe commutatif dont l'élément neutre est noté 0_E ou 0 et appelé le vecteur nul de E,
- $\cdot$ est une application de $\mathbb{K} \times E$ dans E. À partir d'un élément λ de $\mathbb{K}$ et d'un élément x de E, $\cdot$ fournit un élément de E noté $\lambda \cdot x$ ou plus simplement λx. Par définition, cette application $\cdot$ doit satisfaire les propriétés suivantes :
  - pour tout $x \in E : 1 \cdot x = x$,
  - pour tous $x, y \in E$ et $\lambda \in \mathbb{K} : \lambda \cdot (x + y) = (\lambda \cdot x) + (\lambda \cdot y)$,
  - pour tous $x \in E$ et $\lambda, \mu \in \mathbb{K} : (\lambda + \mu) \cdot x = (\lambda \cdot x) + (\mu \cdot x)$,
  - pour tous $x \in E$ et $\lambda, \mu \in \mathbb{K} : \lambda \cdot (\mu \cdot x) = (\lambda\mu) \cdot x$.

Scanné avec CamScanner

Les éléments de E sont appelés des vecteurs, ceux de $\mathbb{K}$ des scalaires. La loi $\cdot$, qui n'est pas une loi de composition interne sur E puisqu'à travers elle des éléments de $\mathbb{K}$ agissent sur des vecteurs, est qualifiée de loi externe. La loi $+$ est appelée addition et la loi $\cdot$ est appelée multiplication par un scalaire. Le corps $\mathbb{K}$ est qualifié de corps de base pour E.

- Sachez que les mathématiciens ne mettent jamais de flèches au-dessus de leurs vecteurs, sauf quand ils font de la géométrie dans le plan et dans l'espace comme vous en avez fait jusqu'ici.
- Notons qu'un espace vectoriel contient toujours au moins le vecteur nul, il ne peut être vide. Si un ensemble ne contient pas de vecteur nul (élément neutre pour la loi $+$), ce n'est pas un espace vectoriel.

Exemples

Quelques exemples classiques d'espaces vectoriels (munis des lois usuelles) :

- $\mathbb{R}$, $\mathbb{C}$ *et plus généralement* $\mathbb{K}^n$;
- $\mathbb{K}[X]$, *l'ensemble des polynômes à coefficients dans* $\mathbb{K}$;
- $\mathcal{M}_{n,p}(\mathbb{K})$ *l'ensemble des matrices à coefficients dans* $\mathbb{K}$ *de taille* $n \times p$;
- $\mathcal{F}(\mathbb{R}, \mathbb{R})$ *l'ensemble des fonctions définies sur* $\mathbb{R}$ *et à valeurs dans* $\mathbb{R}$;
- *l'ensemble des suites à valeurs réelles ou complexes (que l'on pourrait noter* $\mathcal{F}(\mathbb{N}, \mathbb{K})$ *ou bien* $\mathbb{K}^{\mathbb{N}}$*).*

- Pour montrer que ces différents ensembles possèdent une structure d'espace vectoriel, on revient à la définition précédente. Il s'agit d'un résultat classique du cours qui peut être réutilisé sans démonstration le jour d'exemen.

Scanné avec CamScanner

Théorème (Règles de calcul dans un espace vectoriel)

Soit E un $\mathbb{K}$-espace vectoriel.

1. *Pour tous $x \in E$ et $\lambda \in \mathbb{K}$: $\lambda \cdot x = 0_E \Leftrightarrow \lambda = 0$ ou $x = 0_E$.*
2. *Pour tout $x \in E$: $-x = (-1) \cdot x$, où $-x$ est l'opposé de x dans E et -1 l'opposé de 1 dans $\mathbb{K}$.*

Structure d'espace vectoriel : e.v et combinaisons linéaires

Démonstration.

1. Trois étapes. Soient $x \in E$ et $\lambda \in \mathbb{K}$.
   - Comme : $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, alors après simplification dans le groupe $(E, +)$: $0 \cdot x = 0_E$.
   - Comme : $\lambda \cdot 0_E = \lambda \cdot (0_E + 0_E) = \lambda \cdot 0_E + \lambda \cdot 0_E$, alors après simplification : $\lambda \cdot 0_E = 0_E$.
   - Si : $\lambda \cdot x = 0_E$ et si : $\lambda \neq 0$, alors :

$$x = 1 \cdot x = (\frac{1}{\lambda} \times \lambda) \cdot x = \frac{1}{\lambda} \cdot (\lambda \cdot x) = \frac{1}{\lambda} \cdot 0_E = 0_E.$$

2. Pour tout $x \in E$:
   $x + (-1) \cdot x = 1 \cdot x + (-1) \cdot x = (1 - 1) \cdot x = 0 \cdot x = 0_E$, donc :
   $-x = (-1) \cdot x$.

□

Scanné avec CamScanner

Définition (Combinaisons linéaires d'un nombre fini de vecteurs)

Soient E un $\mathbb{K}$-espace vectoriel et $x_1, \cdots, x_n \in E$. On appelle combinaison linéaire de $x_1, \cdots, x_n$ tout vecteur de E de la forme : $\sum_{k=1}^{n} \lambda_k x_k$ pour certains $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$.

Attention : Une égalité de la forme $\sum_{k=1}^{n} \lambda_k x_k = \sum_{k=1}^{n} \mu_k x_k$ n'implique pas l'égalité $\lambda_k = \mu_k, \forall k \in \{1, \cdots, n\}$. En d'autres termes, on ne peut pas pratiquer d'identification systématiquement quand deux combinaisons linéaires d'une même famille de vecteurs sont égales. Par exemple : $(1,1) + 2(0,1) + 2(1,0) = (3,3) = 2(1,1) + (0,1) + (1,0)$.

Définition (Famille presque nulle de scalaires)

On dit qu'une famille $X = (x_i)_{i \in I} \in \mathbb{K}^I$ est presque nulle (ou à support fini) si l'ensemble $\text{supp}(X) = \{i \in I | x_i \neq 0\}$ est de cardinal fini. Autrement dit, une famille d'éléments de $\mathbb{K}$ indexée par I est presque nulle si tous ses éléments sont nuls **SAUF UN NOMBRE FINI D'ENTRE EUX**.

- Dans le cas où I est un ensemble **FINI**, la précision "presque nulle" est évidemment sans intérêt.

Définition (c.I. d'un nombre infini de vecteurs)

Soient E un espace vectoriel et $(x_i)_{i \in I}$ une famille de vecteurs de E. On appelle combinaison linéaire de $(x_i)_{i \in I}$ tout vecteur de E de la forme : $\sum_{i \in I} \lambda_i x_i$ où $(\lambda_i)_{i \in I}$ est une famille **PRESQUE NULLE** d'éléments de $\mathbb{K}$.

Scanné avec CamScanner

Structure d'espace vectoriel : e.v et combinaisons linéaires

Attention : Pour un nombre **FINI** de vecteurs, pas besoin de familles **PRESQUE NULLES** de scalaires !

▶ Nous pourrons maintenant parler des combinaisons linéaires d'un nombre **INFINI** de vecteurs, mais chacune de ces combinaisons linéaires reste fondamentalement une somme **FINIE**. Les vraies sommes infinies n'ont aucun sens sans une notion de passage à la limite adéquat.

Exemples

$\mathbb{K}[X]$ est l'ensemble des combinaisons linéaires de la famille $(X^k)_{k\in\mathbb{N}}$.

▶ *Rappelons à ce sujet que la notation $\sum_{k=0}^{+\infty} a_k X^k$ des polynômes, très pratique, désigne en fait une somme **FINIE**.*

Structure d'espace vectoriel : Sous-espace vectoriel

Définition (Sous-espace vectoriel)

Soient E un espace vectoriel et F une partie de E. On dit que F est un sous-espace vectoriel de E si :

- F est stable par addition : $\forall x, y \in F,\ x + y \in F$;
- F est stable par multiplication par un scalaire : $\forall \lambda \in \mathbb{K}, \forall x \in F,\ \lambda \cdot x \in F$;
- F est un $\mathbb{K}$-espace vectoriel pour les lois de E.

▶ Si F un sous-espace vectoriel de E, F est un sous-groupe additif de E, donc : $0_F = 0_E \in F$.

Exemples

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

Scanné avec CamScanner

Structure d'espace vectoriel : Sous-espace vectoriel

▶ Pour montrer qu'un ensemble muni d'une addition et d'une multiplication par un scalaire est un espace vectoriel, il suffit souvent de montrer qu'il est **SOUS**-espace d'un autre espace vectoriel connu. On se ramènera notamment aux exemples fondamentaux présentés précédemment.

Théorème (Caractérisation des sous-espaces vectoriels)

Soient E un $\mathbb{K}$-espace vectoriel et F un sous-ensemble (ou partie) de E. Les assertions suivantes sont équivalentes :

1. *F est un sous-espace vectoriel de E.*
2. $\begin{cases} 0_E \in F; \\ \forall x, y \in F, \forall \lambda \in \mathbb{K}, \lambda x + y \in F. \end{cases}$

Structure d'espace vectoriel : Sous-espace vectoriel

Démonstration.

($\Rightarrow$) Si F est un sous-espace vectoriel de E, on a vu que : $0_E = 0_F \in F$. De plus, pour tous $x, y \in E$ et $\lambda \in \mathbb{K}$, λx et y sont éléments de F car F est stable par multiplication par un scalaire, et enfin : $\lambda x + y \in F$ car F est stable par addition.
($\Leftarrow$) Si l'assertion (2) est vraie, F est stable par différence (pour $\lambda = -1$) donc est un sous-groupe additif de E. Les autres axiomes de la définition des espaces vectoriels ne requièrent aucune vérification particulière car une relation vraie sur E tout entier l'est aussi sur F. □

▶ C'est **TOUJOURS** le résultat précédent qu'il faut utiliser pour montrer qu'une partie d'un espace vectoriel en est un sous-espace vectoriel. Si on utilisait la DÉFINITION des sous-espaces vectoriels, on serait obligé de vérifier beaucoup d'axiomes dont la CARACTÉRISATION fait l'économie.

Scanné avec CamScanner

Structure d'espace vectoriel : Sous-espace vectoriel

S'en suit toute une série d'exemples qu'il convient de maîtriser parfaitement.

Exemples

Pour tout $n \in \mathbb{N}$, l'ensemble des polynômes de degré ***INFÉRIEUR OU ÉGAL*** *à n, noté $\mathbb{K}_n[X]$, est un sous-espace vectoriel de $\mathbb{K}[X]$.*

- *Soit $n \in \mathbb{N}$.*
  - *Pour commencer : $\mathbb{K}_n[X] \subset \mathbb{K}[X]$. Ensuite : $0 \in \mathbb{K}_n[X]$ car : $\deg(0) = -\infty \leq n$.*
  - *Montrons enfin que $\mathbb{K}_n[X]$ est stable par combinaison linéaire. Soient $P, Q \in \mathbb{K}_n[X]$ et $\lambda \in \mathbb{K}$. Nous savons qu'alors : $\deg(\lambda P + Q) \leq \max(\deg(P), \deg(Q)) \leq n$, donc en effet : $\lambda P + Q \in \mathbb{K}_n[X]$.*

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 !

Structure d'espace vectoriel : Sous-espace vectoriel

Exemples

L'ensemble des suites convergentes à valeurs réelles est un sous-espace vectoriel de l'ensemble des suites à valeurs réelles :

- *la suite nulle converge (vers 0) ;*
- *si $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont deux suites qui convergent respectivement vers ℓ et ℓ', λ un réel, alors la suite $(\lambda u_n + v_n)_{n\in\mathbb{N}}$ converge (vers $\lambda\ell + \ell'$). Il y a bien stabilité par combinaison linéaire.*

Scanné avec CamScanner

Exemples

$F = \{(x, y, z) \in \mathbb{R}^3 \mid x + 2y - 3z = 0\}$ *est un sous-espace vectoriel de* $\mathbb{R}^3$ *:*

- *le vecteur nul appartient bien à* F *car* $0 + 2 \cdot 0 - 3 \cdot 0 = 0$ *;*
- *si* $u = (x, y, z), v = (x', y', z') \in F$, $\lambda \in \mathbb{R}$ *alors* $\lambda u + v \in F$. *En effet,* $\lambda u + v = (\lambda x + x', \lambda y + y', \lambda z + z')$ *et :*

$$\begin{aligned}(\lambda x + x') + 2(\lambda y + y') - 3(\lambda z + z') \\ = \lambda(x + 2y - 3z) + (x' + 2y' - 3z') \\ = \lambda \cdot 0 + 0 = 0.\end{aligned}$$

Exemples

Soient $a, b, c \in \mathbb{R}$ *tels que* $(a, b) \neq (0, 0)$. *Notons* D *l'ensemble* $\{(x, y) \in \mathbb{R}^2 \mid ax + by + c = 0\}$.

- *Si* $c \neq 0$, *alors* D *n'est pas un sous-espace vectoriel de* $\mathbb{R}^2$ *car il ne contient pas le vecteur nul* $(0, 0)$.
- *Si au contraire* $c = 0$, D *est un sous-espace vectoriel de* $\mathbb{R}^2$, *en l'occurence la droite d'équation* $ax + by + c = 0$. *En effet :*
  - *Pour commencer,* D *est une partie de* $\mathbb{R}^2$ *et il est clair que* $(0, 0) \in D$.
  - *Soient* $(x, y), (x', y') \in D$ *et* $\lambda \in \mathbb{R}$. *Nous devons montrer que* $\lambda(x, y) + (x', y')$, *égal à* $(\lambda x + x', \lambda y + y')$ *par définition, est un élément de* D. *On a* $a(\lambda x + x') + b(\lambda y + y') = \lambda(ax + by) + (ax' + by') = \lambda \cdot 0 + 0 = 0$. *D'où le résultat.*

Scanné avec CamScanner

Théorème (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.

Démonstration.

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.

- Pour commencer : $F \subset E$. Ensuite : $0_E \in F_i$ pour tout $i \in I$ puisque F_i est un sous-espace vectoriel de E, donc : $0_E \in F$.
- Montrons enfin que F est stable par combinaison linéaire. 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 : $\lambda x + y \in F$.

□

Attention : ce théorème est faux pour la réunion !

Exercice

Soient F et G deux s.e.v d'un $\mathbb{K}$-espace vectoriel E. Si $F \cup G$ est un s.e.v de E, montrer que $F \subset G$ ou $G \subset F$.

Solution

Raisonnons par l'absurde et supposons que $F \not\subset G$ et $G \not\subset F$, de sorte qu'il existe $x \in F$, $x \notin G$, et il existe $y \in G$, $y \notin F$. Le vecteur $x + y$ est dans le s.e.v $F \cup G$, donc $x + y \in F$ ou $x + y \in G$. Supposons par exemple $x + y \in F$. Comme F est un s.e.v et que $x \in F$, on a $(x + y) - x \in F$, c'est-à-dire $y \in F$, ce qui est absurde. D'où le résultat.

Scanné avec CamScanner

Définition (Sous-espace vectoriel engendré par une partie)

Soient E un $\mathbb{K}$-espace vectoriel et X une partie de E.

1. L'intersection de tous les sous-espaces vectoriels de E contenant X est appelée le sous-espace vectoriel (de E) engendré par X et notée $\text{Vect}(X)$. À ce titre, $\text{Vect}(X)$ est le plus petit sous-espace vectoriel de E contenant X. Il est donné par la formule $\text{Vect}(X) = \bigcap_{\substack{X \subset F \subset E \\ F \text{ s.e.v de } E}} F$.

   En particulier, tout sous-espace vectoriel de E qui contient X contient aussi $\text{Vect}(X)$.
2. Si : $X = \{x_i | i \in I\}$, $\text{Vect}(X)$ est aussi l'ensemble des combinaisons linéaires de $(x_i)_{i \in I}$ et noté $\text{Vect}(x_i)_{i \in I}$. Autrement dit : $\text{Vect}(X) = \{\sum_{i \in I} \lambda_i x_i \mid (\lambda_i)_{i \in I} \in \mathbb{K}^I \text{ presque nulle}\}$.

Démonstration :

1. En tant qu'intersection de sous-espaces vectoriels de E contenant X, $\text{Vect}(X)$ est lui-même un sous-espace vectoriel de E contenant X, et il est inclus par définition dans tous les sous-espaces vectoriels de E contenant X, ce qui montre que tout sous-espace vectoriel de E qui contient X contient en réalité $\text{Vect}(X)$ tout entier.
2. Notons $V = \{\sum_{i \in I} \lambda_i x_i \mid (\lambda_i)_{i \in I} \in \mathbb{K}^I \text{ presque nulle}\}$ l'ensemble des combinaisons linéaires de $(x_i)_{i \in I}$. Nous voulons montrer que : $V = \text{Vect}(X)$. Or $\text{Vect}(X)$ est stable par combinaison linéaire en tant que sous-espace vectoriel de E et contient X, donc contient toute combinaison linéaire de $(x_i)_{i \in I}$, autrement dit : $V \subset \text{Vect}(X)$. Pour l'inclusion réciproque, d'après le premier point, il nous suffit de montrer que V est un sous-espace vectoriel de E contenant X.

Scanné avec CamScanner

Structure d'espace vectoriel : Sous-espace vectoriel

- Pour commencer : $V \subset E$. Ensuite, V contient 0_E car : $0_E = \sum_{i \in I} 0 \cdot x_i$, mais aussi X car pour tout $j \in I$: $x_j = 1 \cdot x_j + \sum_{i \in I, i \neq j} 0 \cdot x_i$.
- Pour la stabilité par combinaison linéaire, soient $v, w \in V$ et $\alpha \in \mathbb{K}$. Pour certaines familles presque nulles $(\lambda_i)_{i \in I}$ et $(\mu_i)_{i \in I}$ d'éléments de $\mathbb{K}$: $v = \sum_{i \in I} \lambda_i x_i$ et $w = \sum_{i \in I} \mu_i x_i$. La famille $(\alpha\lambda_i + \mu_i)_{i \in I}$ est alors elle aussi presque nulle et : $\alpha v + w = \sum_{i \in I} (\alpha\lambda_i + \mu_i) x_i$, donc : $\alpha v + w \in V$.

Structure d'espace vectoriel : Sous-espace vectoriel

Remarque (s.e.v engendré par une famille finie de vecteurs)

Soient E un $\mathbb{K}$-espace vectoriel. Si $(x_1, \cdots, x_n)$ est une famille d'un nombre fini de vecteurs de E, on a

$$\text{Vect}(x_1, \cdots, x_n) = \{\sum_{i=1}^{n} \alpha_i x_i | (\alpha_1, \cdots, \alpha_n) \in \mathbb{K}^n\}$$

et $\text{Vect}(x_1, \cdots, x_n)$ est le plus petit sous-espace vectoriel de E contenant $x_1, x_2, \cdots, x_n$; en d'autres termes, tout sous-espace vectoriel de E contenant $x_1, x_2, \cdots, x_n$ contient aussi $\text{Vect}(x_1, \cdots, x_n)$.

▶ Tout ensemble qui s'écrit sous la forme $\text{Vect}(\cdots)$ est donc un espace vectoriel. C'est une nouvelle façon de montrer qu'un ensemble possède une structure d'espace vectoriel.

Scanné avec CamScanner

Structure d'espace vectoriel : Sous-espace vectoriel

Exemples

- $\text{Vect}(0_E) = \{0_E\}$.
- $\text{Vect}(u)$ *est l'ensemble des vecteurs qui s'écrivent sous la forme* λu, *c'est-à-dire l'ensemble des vecteurs colinéaires à* u. *Si* u *est non nul, on dit alors que* $\text{Vect}(u)$ *est la droite vectorielle dirigée (ou engendrée) par* u.
- $\text{Vect}(u, v)$ *est l'ensemble des vecteurs qui s'écrivent sous la forme* $\lambda u + \mu v$. *Si* u *et* v *ne sont pas colinéaires, on dit alors que* $\text{Vect}(u, v)$ *est le plan vectoriel dirigé (ou engendré) par* u *et* v.

Structure d'espace vectoriel : Sous-espace vectoriel

Exemples

- *Soit* $(a, b) \in \mathbb{R}^2$ *non nul. Dans* $\mathbb{R}^2$, *le sous-espace vectoriel* $\text{Vect}((a, b))$ *est la droite passant par* $(0, 0)$ *dirigée par* (a, b).
- $\mathbb{K}[X] = \text{Vect}\left(X^k\right)_{k\in\mathbb{N}}$ *et pour tout* $n \in \mathbb{N}$: $\mathbb{K}_n[X] = \text{Vect}(1, X, \cdots, X^n)$.
- *Si le corps de base est* $\mathbb{R}$ *:* $\text{Vect}(1) = \{a \times 1 \mid a \in \mathbb{R}\} = \mathbb{R}$ *et* $\text{Vect}(1, i) = \{a + ib \mid a, b \in \mathbb{R}\} = \mathbb{C}$. *Si par contre le corps de base est* $\mathbb{C}$ *:* $\text{Vect}(1) = \{a \times 1 | a \in \mathbb{C}\} = \mathbb{C}$.

Scanné avec CamScanner

Théorème (Propriétés des Vect)

Soient E un $\mathbb{K}$-espace vectoriel, X et Y deux parties de E et $x, a, b \in E$.

1. ***Inclusion*** *: Si : $X \subset Y$, alors :* $\text{Vect}(X) \subset \text{Vect}(Y)$.
2. ***Ôter un vecteur*** *: Si : $x \in X$ est combinaison linéaire de $X \setminus \{x\}$:* $\text{Vect}(X) = \text{Vect}\left(X \setminus \{x\}\right)$.
3. ***Remplacer un vecteur*** *: Si b est combinaison linéaire de $X \cup \{a\}$ avec un coefficient* ***NON NUL*** *sur a :* $\text{Vect}\left(X \cup \{a\}\right) = \text{Vect}\left(X \cup \{b\}\right)$.

Démonstration :

1. Toute combinaison linéaire de X est bien sûr une combinaison linéaire de Y !
2. Soit $x \in X$ combinaison linéaire de $X \setminus \{x\}$. D'après (1) : $\text{Vect}\left(X \setminus \{x\}\right) \subset \text{Vect}(X)$. Réciproquement, $\text{Vect}\left(X \setminus \{x\}\right)$ est un sous-espace vectoriel contenant $X \setminus \{x\}$, or il contient aussi x par hypothèse, donc X tout entier, donc enfin $\text{Vect}(X)$.
3. Dans un sens, $\text{Vect}\left(X \cup \{a\}\right)$ contient X et a, donc aussi b par hypothèse, donc $X \cup \{b\}$, donc enfin $\text{Vect}\left(X \cup \{b\}\right)$. Dans l'autre sens, remarquons que par hypothèse : $b = \lambda a + x$ avec $\lambda \in \mathbb{K}$ **NON NUL** et où x est une combinaison linéaire de X. Ainsi : $a = \dfrac{b - x}{\lambda}$ donc a est combinaison linéaire de $X \cup \{b\}$ avec un coefficient **NON NUL** sur b. Comme a et b jouent des rôles symétriques, on obtient alors : $\text{Vect}\left(X \cup \{a\}\right) \subset \text{Vect}\left(X \cup \{b\}\right)$.

Scanné avec CamScanner

Théorème (Opération sur les Vect)

Soient E un $\mathbb{K}$-espace vectoriel et $x_1, x_2, \cdots, x_n \in E$. Le sous-espace vectoriel $\text{Vect}(x_1, x_2, \cdots, x_n)$ *n'est pas modifié*

1. *lorsqu'on permute $x_1, x_2, \cdots, x_n$;*
2. *lorsqu'on retire tous les x_k nuls, $k \in \{1, \cdots, n\}$;*
3. *lorsqu'à $k \in \{1, \cdots, n\}$ fixé, on remplace x_k par une combinaison linéaire de $x_1, x_2, \cdots, x_n$, à condition toutefois d'affecter x_k lui-même d'un* ***coefficient non nul****.*

Démonstration : Pour (1), utiliser la commutativité de $+$; pour (2), le fait que 0_E est neutre.

Prouvons l'assertion (3). Fixons donc $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{K}$ tels que $\lambda_k \neq 0$ et posons $V = \text{Vect}(x_1, x_2, \cdots, x_n)$ et

$$V' = \text{Vect}(x_1, x_2, \cdots, x_{k-1}, \sum_{i=1}^{n} \lambda_i x_i, x_{k+1}, \cdots, x_n).$$

- Montrons que $V \subset V'$. Commençons par remarquer que $x_k \in V'$ car, puisque $\lambda_k \neq 0$: $x_k = \frac{1}{\lambda_k} \sum_{i=1}^{n} \lambda_i x_i - \sum_{\substack{i=1 \\ i \neq k}}^{n} \frac{\lambda_i}{\lambda_k} x_i$. Or $x_1, x_2, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n \in V'$ également, donc V' contient $x_1, x_2, \cdots, x_n$. Enfin V' contient V car V est le plus petit sous-espace vectoriel de E contenant ces vecteurs.
- Montrons que $V' \subset V$. Bien sûr, V contient $x_1, x_2, \cdots, x_{k-1}, \sum_{i=1}^{n} \lambda_i x_i, x_{k+1}, \cdots, x_n$. Par conséquent V contient V' car V' est le plus petit sous-espace vectoriel de E contenant ces vecteurs.

Scanné avec CamScanner

Définition (Partie/famille génératrice)

Soient E un $\mathbb{K}$-espace vectoriel et X une partie de E. On note $\text{Vect}(X) = \text{Vect}(x)_{x\in X}$. On dit que X est une partie génératrice de E (ou $(x)_{x\in X}$ une famille génératrice de E) si tout élément de E est combinaison linéaire de X, i.e. si : $E = \text{Vect}(X)$.
Si : $X = (x_i)_{i\in I}$, on dit aussi que la famille $(x_i)_{i\in I}$ est génératrice de E ou engendre E.

Remarque

Soient E un $\mathbb{K}$-espace vectoriel et $x_1, x_2, \cdots, x_n \in E$. On dit que la famille $(x_1, x_2, \cdots, x_n)$ est une famille génératrice de E ou qu'elle engendre E si tout élément de E est combinaison linéaire de $x_1, x_2, \cdots, x_n$, autrement dit si $E = \text{Vect}(x_1, x_2, \cdots, x_n)$.

Exemples

- $(X^k)_{k\in\mathbb{N}}$ *engendre* $\mathbb{K}[X]$ *et* $(1, X, \cdots, X^n)$ *engendre* $\mathbb{K}_n[X]$ *pour tout* $n \in \mathbb{N}$.
- *Pour tout* $(x, y) \in \mathbb{R}^2$ *:* $(x, y) = x(1, 0) + y(0, 1)$*, donc la famille* $\Big((1, 0), (0, 1)\Big)$ *engendre* $\mathbb{R}^2$.
  Plus généralement, posons pour tout $n \in \mathbb{N}^*$ *:* $e_1 = (1, 0, \cdots, 0)$, $e_2 = (0, 1, 0, \cdots, 0), \cdots,$ $e_n = (0, \cdots, 0, 1)$*. La famille* $(e_1, \cdots, e_n)$ *engendre* $\mathbb{K}^n$ *car pour tout* $(x_1, \cdots, x_n) \in \mathbb{K}^n$ *:* $(x_1, \cdots, x_n) = \sum_{i=1}^{n} x_i e_i$.
- *La famille* $(1, i)$ *engendre le* $\mathbb{R}$*-espace vectoriel* $\mathbb{C}$*, mais* (1) *suffit à engendrer le* $\mathbb{C}$*-espace vectoriel* $\mathbb{C}$.

Scanné avec CamScanner

Structure d'espace vectoriel : Famille de vecteurs

En pratique : Trouver une partie génératrice d'un sous-espace vectoriel, c'est l'écrire comme un Vect.

Exemples

L'ensemble $E = \{(x, y, z, t) \in \mathbb{R}^4 \mid x + 2y - z = 0 \text{ et } x - y + t = 0\}$ *est un sous-espace vectoriel de* $\mathbb{R}^4$ *engendré par la famille* $\Big((1, 0, 1, -1), (0, 1, 2, 1)\Big)$.

- *Pour tout* $(x, y, z, t) \in \mathbb{R}^4$: $(x, y, z, t) \in E \Leftrightarrow \begin{cases} z &= x + 2y \\ t &= -x + y, \end{cases}$ *donc :*

$E = \{(x, y, x + 2y, -x + y) \mid x, y \in \mathbb{R}\} = \{x(1, 0, 1, -1) + y(0, 1, 2, 1) \mid x, y \in \mathbb{R}\} = \text{Vect}\Big((1, 0, 1, -1), (0, 1, 2, 1)\Big)$.

Ceci montre ***À LA FOIS*** E *est un sous-espace vectoriel de* $\mathbb{R}^4$ *et que* $\Big((1, 0, 1, -1), (0, 1, 2, 1)\Big)$ *engendre* E.

Structure d'espace vectoriel : Famille de vecteurs

Exemples

L'ensemble $F = \{P \in \mathbb{R}_3[X] \mid 2P(X + 1) = XP'\}$ *est un sous-espace vectoriel de* $\mathbb{R}_3[X]$ *engendré* par $X^2 - 4X + 3$.

- *Pour tout* $P = aX^3 + bX^2 + cX + d \in \mathbb{R}_3[X]$:

$P \in F \Leftrightarrow 2P(X + 1) = XP'$

$\Leftrightarrow 2a(X + 1)^3 + 2b(X + 1)^2 + 2c(X + 1) + 2d = X(3aX^2 + 2bX + c)$

$\Leftrightarrow \begin{cases} a &= 0 \\ c &= -4b \\ d &= 3b. \end{cases}$

Conclusion : $F = \Big\{bX^2 - 4bX + 3b \mid \quad b \in \mathbb{R}\Big\} = \Big\{b\Big(X^2 - 4X + 3\Big) \mid \quad b \in \mathbb{R}\Big\} = \text{Vect}\Big(X^2 - 4X + 3\Big)$. *Ceci montre* ***À LA FOIS*** F *est un sous-espace vectoriel de* $\mathbb{R}_3[X]$ *et que* $\Big(X^2 - 4X + 3\Big)$ *en est une famille génératrice.*

Scanné avec CamScanner

Le résultat qui suit n'est qu'une simple reformulation du théorème "Opération sur les Vect".

Proposition (Propriétés des familles génératrices)

Soit $x_1, \cdots, x_n \in E$. On pose $F = \text{Vect}(x_1, \cdots, x_n)$.
On ne change pas l'espace vectoriel engendré F si :

1. *on permute plusieurs vecteurs dans la famille $(x_1, \cdots, x_n)$.*
2. *on ajoute à la famille un vecteur combinaison linéaire des $x_1, \cdots, x_n$.*
3. *on multiplie l'un des vecteurs par un scalaire non nul.*
4. *on retranche à la famille un vecteur combinaison linéaire des autres.*

Démonstration.

Montrons l'assertion (4). Soient E un $\mathbb{K}$-espace vectoriel et $(x_1, x_2, \cdots, x_n)$ une famille génératrice E. Si par exemple x_n est combinaison linéaire de $x_1, x_2, \cdots, x_{n-1}$, alors on peut écrire aussitôt, en vertu des opérations sur les Vect, que $E = \text{Vect}(x_1, x_2, \cdots, x_n) = \text{Vect}(x_1, x_2, \cdots, x_{n-1}, 0_E) = \text{Vect}(x_1, x_2, \cdots, x_{n-1})$; dans ce cas $(x_1, x_2, \cdots, x_{n-1})$ est une famille génératrice de E, comme voulu. □

▶ En d'autres termes, si on rajoute à une famille génératrice de E des vecteurs de E, cette nouvelle famille reste génératrice. Si une famille génératrice de E contient des vecteurs combinaisons linéaires des autres, on peut les retirer, la nouvelle famille reste génératrice. Si l'on retire des vecteurs qui ne sont pas combinaisons linéaires des autres, la nouvelle famille ne sera en revanche plus génératrice !

Scanné avec CamScanner

Structure d'espace vectoriel : Famille de vecteurs

Définition (famille libre d'un nombre fini de vecteurs)

Soient E un $\mathbb{K}$-espace vectoriel et $x_1, \cdots, x_n \in E$. On dit que la famille $(x_1, \cdots, x_n)$ est libre ou que les vecteurs $x_1, \cdots, x_n$ sont linéairement indépendants si :

$$\forall (\lambda_1, \cdots, \lambda_n) \in \mathbb{K}^n, \Big(\sum_{i=1}^{n} \lambda_i x_i = 0_E \Rightarrow \lambda_1 = \cdots = \lambda_n = 0 \Big).$$

Quitte à remplacer λ_i par $\lambda_i - \mu_i$ dans la définition de la liberté, on peut aussi dire que $(x_1, \cdots, x_n)$ est libre si et seulement si :
$\forall (\lambda_1, \cdots, \lambda_n), (\mu_1, \cdots, \mu_n) \in \mathbb{K}^n$,
$\Big(\sum_{i=1}^{n} \lambda_i x_i = \sum_{i=1}^{n} \mu_i x_i \Rightarrow \forall i \in \{1, \cdots, n\},\ \lambda_i = \mu_i \Big)$, ce qui n'est finalement rien de plus qu'un **PRINCIPE D'IDENTIFICATION**.

Structure d'espace vectoriel : Famille de vecteurs

En résumé :

- **FAMILLE GÉNÉRATRICE** = **EXISTENCE** pour **TOUT** vecteur d'une décomposition comme combinaison linéaire.
- **FAMILLE LIBRE** = **UNICITÉ** des coefficients dans les combinaisons linéaires, donc possibilité de pratiquer des **IDENTIFICATIONS**.

Définition (famille liée d'un nombre fini de vecteurs, couple de vecteurs colinéaires)

Soient E un $\mathbb{K}$-espace vectoriel et $x_1, \cdots, x_n, x, y \in E$.

- On dit que la famille $(x_1, \cdots, x_n)$ est liée ou que les vecteurs $x_1, \cdots, x_n$ sont linéairement dépendants si la famille $(x_1, \cdots, x_n)$ **N**'est **PAS** libre. Cela revient à dire que **L'UN AU MOINS** des vecteurs $x_1, \cdots, x_n$ est combinaison linéaire des autres.
- On dit que x et y sont colinéaires si la famille (x, y) est liée, i.e. si x ou y est un multiple de l'autre.

Scanné avec CamScanner

Structure d'espace vectoriel : Famille de vecteurs

Dire que $(x_1, \cdots, x_n)$ est liée, c'est dire que pour certains $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$:
$\Big(\sum_{i=1}^{n} \lambda_i x_i = 0_E \quad \text{et} \quad \exists i_0 \in \{1, \cdots, n\},\ \lambda_{i_0} \neq 0\Big)$, auquel cas :

$x_{i_0} = -\dfrac{1}{\lambda_{i_0}} \sum_{\substack{1 \leq i \leq n \\ i \neq i_0}} \lambda_i x_i$, i.e. x_{i_0} est "combinaison linéaire des autres".

Proposition

1. *Une famille est liée dès qu'elle contient le vecteur nul.*
2. *Une famille composée d'un seul vecteur est libre si et seulement si ce vecteur n'est pas nul.*
3. *Une famille composée de deux vecteurs est libre si et seulement s'ils ne sont pas colinéaires.*

Structure d'espace vectoriel : Famille de vecteurs

Démonstration.

1. La famille $(x_1, \cdots, x_n, 0_E)$ est liée car $0 \cdot x_1 + \cdots + 0 \cdot x_n + 1 \cdot 0_E = 0_E$.
2. Si u est non nul, la famille (u) est libre car : $\lambda u = 0_E \Rightarrow \lambda = 0$.
3. Si (u, v) est liée alors il existe $\alpha, \beta \in \mathbb{K}$ tels que $\alpha u + \beta v = 0_E$ avec $(\alpha, \beta) \neq (0, 0)$. Si α est non nul, $u = -\dfrac{\beta}{\alpha} v$. Si $\alpha = 0$, β est nécessairement non nul et alors $v = -\dfrac{\alpha}{\beta} u$. Dans les deux cas, u et v sont colinéaires. Réciproquement, si u et v sont colinéaires, on aura, par exemple, $u = \lambda v$ donc $1 \cdot u + (-\lambda) \cdot v = 0_E$, ce qui montre que la famille est liée.

□

Scanné avec CamScanner

Exemples

La famille $(\sin, \cos)$ *du* $\mathbb{R}$*-espace vectoriel* $\mathbb{R}^{\mathbb{R}}$ *est libre.*

- *Soient* $\lambda, \mu \in \mathbb{R}$ *tels que* $\lambda \sin + \mu \cos = 0$, *i.e. :*

$\forall x \in \mathbb{R}, \lambda \sin x + \mu \cos x = 0$. *Alors en particulier, pour* $x = 0$ *:*
$\lambda \sin 0 + \mu \cos 0 = 0$ *et donc* $\mu = 0$. *De plus, pour* $x = \dfrac{\pi}{2}$, *on a :*
$\lambda \sin \dfrac{\pi}{2} + \mu \cos \dfrac{\pi}{2} = 0$ *et donc* $\lambda = 0$, *comme voulu.*

Définition (famille libre/liée d'un nombre quelconque de vecteurs)

Soient E un $\mathbb{K}$-espace vectoriel et $(x_i)_{i \in I}$ une famille de vecteurs de E.

- On dit que la famille $(x_i)_{i \in I}$ est libre ou que les vecteurs x_i, i décrivant I, sont linéairement indépendants si :
  $\forall (\lambda_i)_{i \in I} \in \mathbb{K}^I$ presque nulle, $\Big(\sum_{i \in I} \lambda_i x_i = 0_E \Rightarrow \forall i \in I, \lambda_i = 0 \Big)$.
- On dit que la famille $(x_i)_{i \in I}$ est liée ou que les vecteurs x_i, i décrivant I, sont linéairement dépendants si $(x_i)_{i \in I}$ **N**'est **PAS** libre. Cela revient à dire que **L'UN AU MOINS** d'entre eux est combinaison linéaire des autres.

Scanné avec CamScanner

▶ L'expression "presque nulle" nous ramène toujours à un nombre **FINI** de vecteurs utiles, donc la liberté d'une famille **INFINIE** de vecteurs est équivalente à la liberté de **TOUTES** ses sous-familles **FINIES**. Pour montrer qu'une famille $(x_n)_{n\in\mathbb{N}}$ de vecteurs est libre, il suffit même de montrer que la famille $(x_0, \cdots, x_n)$ est libre pour tout $n \in \mathbb{N}$.

Définition

On dit qu'une famille de polynômes non nuls $(P_k)_{k\in\mathbb{N}}$ est :

- étagée en degrés si on a $\deg(P_k) < \deg(P_{k+1})$ pour tout $k \in \mathbb{N}$.
- échelonnée en degrés si on a $\deg(P_k) = k$ pour tout $k \in \mathbb{N}$.

▶ Une famille de polynômes échelonnée en degrés est étagée en degrés.
▶ Le théorème suivant est **TRÈS IMPORTANT !**

Théorème

Une famille $(P_k)_{k\in\mathbb{N}}$ de polynômes non nuls étagée en degrés est libre dans $\mathbb{K}[X]$.

Conséquence : Une famille de polynômes **NON NULS** échelonnés en degrés est libre.

Scanné avec CamScanner

Démonstration : Soit $(P_k)_{k\in\mathbb{N}}$ une famille de polynômes étagée en degrés. On vérifie par récurrence sur $n \geq 0$, que chaque famille $(P_k)_{0\leq k\leq n}$ est libre.

- Initialisation : Pour $n = 0$, P_0 est non nul, donc (P_0) est libre.
- Hérédité : Supposons le résultat acquis pour $n-1 \geq 0$ et soit $(\lambda_k)_{0\leq k\leq n}$ des scalaires tels que $\sum_{k=0}^{n} \lambda_k P_k = 0$. On a : $\lambda_n P_n = -\sum_{k=0}^{n-1} \lambda_k P_k$. Si $\lambda_n \neq 0$, alors : $\deg(P_n) = \deg(\sum_{k=0}^{n-1} \lambda_k P_k)$, ce qui est en contradiction avec $\deg(P_k) < \deg(P_n)$ pour tout k compris entre 0 et $n-1$. On a donc $\lambda_n = 0$ et $\sum_{k=0}^{n-1} \lambda_k P_k = 0$, ce qui impose $\lambda_k = 0$ pour tout k compris entre 0 et $n-1$ puisque $(\lambda_k)_{0\leq k\leq n-1}$ est libre par hypothèse de récurrence.

Théorème (Propriétés des familles libres/liées)

1. *Toute sur-famille d'une famille liée est liée.*
2. *Toute sous-famille d'une famille libre est libre.*
3. *Si on ajoute à une famille libre un vecteur **NON** combinaison linéaire des vecteurs de cette famille, alors la famille obtenue est encore libre.*

▶ Dire qu'une famille est libre, c'est dire qu'aucun de ses vecteurs n'est combinaison linéaire des autres, donc si on veut que l'ajout d'un vecteur conserve la liberté d'une famille libre, on doit faire attention de ne pas introduire de dépendance entre ses vecteurs (on ne peut donc ajouter qu'un vecteur linéairement indépendant des autres).

Scanné avec CamScanner

Démonstration :

1. Si une famille est liée, alors l'un de ses vecteurs est combinaison linéaire des autres. Quand on ajoute de nouveaux vecteurs à cette famille, ce fait ne s'en trouve pas modifié et donc la sur-famille obtenue est toujours liée.
2. Soient E un $\mathbb{K}$-espace vectoriel, $(x_1, x_2, \cdots, x_n)$ une famille libre de E et $p \leq n$. Montrons que la famille $(x_1, x_2, \cdots, x_p)$ est libre elle aussi.

   Soient $\lambda_1, \cdots, \lambda_p \in \mathbb{K}$ tels que $\sum_{k=1}^{p} \lambda_k x_k = 0_E$. Alors $\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_p x_p + 0 \cdot x_{p+1} + \cdots + 0 \cdot x_n = 0_E$. Or la famille $(x_1, x_2, \cdots, x_n)$ est libre. Par conséquent $\lambda_1 = \lambda_2 = \cdots = \lambda_p = 0$ comme voulu.
3. Soient E un $\mathbb{K}$-espace vectoriel, $(x_1, x_2, \cdots, x_n)$ une famille libre de E et $x_{n+1} \in E$ **non** combinaison linéaire de $x_1, x_2, \cdots, x_n$. Montrons que $(x_1, x_2, \cdots, x_n, x_{n+1})$ est libre elle aussi.

Soient $\lambda_1, \lambda_2, \cdots, \lambda_n, \lambda_{n+1}$ tels que $\sum_{k=1}^{n+1} \lambda_k x_k = 0_E$. Si λ_{n+1} était non nul, on aurait $x_{n+1} = -\frac{1}{\lambda_{n+1}} \sum_{k=1}^{n} \lambda_k x_k$; le vecteur x_{n+1} serait alors combinaison linéaire de $x_1, x_2, \cdots, x_n$, ce qui est faux par hypothèse. Par conséquent $\lambda_{n+1} = 0$. Du coup, on récupère l'égalité $\sum_{k=1}^{n} \lambda_k x_k = 0_E$. La liberté de $(x_1, x_2, \cdots, x_n)$ montre aussitôt que $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$. Nous avons bien prouvé que $\lambda_1 = \lambda_2 = \cdots = \lambda_n = \lambda_{n+1} = 0$.

Scanné avec CamScanner

Définition (Bases)

Soient E un $\mathbb{K}$-espace vectoriel et $\mathcal{B} = (e_i)_{i \in I}$ une famille de vecteurs de E.

- On dit que $\mathcal{B}$ est une base de E si $\mathcal{B}$ est à la fois libre et génératrice de E, i.e. si et seulement si tout vecteur de E est **D'UNE ET UNE SEULE MANIÈRE** combinaison linéaire de $\mathcal{B}$.
- Dans ce cas, pour tout $x \in E$, l'unique famille presque nulle $(x_i)_{i \in I} \in \mathbb{K}^I$ pour laquelle : $x = \sum_{i \in I} x_i e_i$ est appelée la famille des coordonnées de x dans $\mathcal{B}$.

La définition suivante est une synthèse des exemples précédents.

Définition (Bases canoniques de $\mathbb{K}^n$, $\mathbb{K}[X]$ et $\mathbb{K}_n[X]$)

- **Familles de scalaires** : Pour tout $n \in \mathbb{N}^*$, si on pose : $e_1 = (1, 0, \cdots, 0)$, $e_2 = (0, 1, 0, \cdots, 0)$, $\cdots$, $e_n = (0, \cdots, 0, 1)$, la famille $(e_1, \cdots, e_n)$ est une base de $\mathbb{K}^n$ appelée sa base canonique.
- **Polynômes** : La famille $(X^k)_{k \in \mathbb{N}}$ est une base de $\mathbb{K}[X]$ appelée sa base canonique et pour tout $n \in \mathbb{N}$, la famille $(1, X, \cdots, X^n)$ est une base de $\mathbb{K}_n[X]$ appelée sa base canonique.

Scanné avec CamScanner

Remarque

- *Que signifie "canonique" ? Réponse : "le plus naturel". De fait, les bases exhibées ci-dessus sont les plus naturelles, les plus simples, les plus faciles d'emploi auxquelles on peut penser dans* $\mathbb{K}^n$, $\mathbb{K}[X]$ *et* $\mathbb{K}_n[X]$.
- *On convient que la famille vide* $\emptyset$ *est une base de l'espace nul* $E = \{0_E\}$.

Méthode

Pour trouver une base d'un espace vectoriel, on en cherche d'abord une famille génératrice en l'écrivant comme un Vect, puis on essaie de montrer que la famille ainsi obtenue est libre.

Exemples

L'ensemble $F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y - 4z = 0\}$ *est un sous-espace vectoriel de* $\mathbb{R}^3$ *et la famille* $\mathcal{B} = \Big((4, 0, 1), (0, 4, 1)\Big)$ *en est une base.*

▶ *Dans cet exemple, tâchons de trouver nous-mêmes une base de* F, *sans aide extérieure.*

- *Commençons par chercher une famille génératrice de* F. *On a :* $F = \{(x, y, \frac{x+y}{4}) \mid x, y \in \mathbb{R}\} = \text{Vect}\Big((1, 0, \frac{1}{4}), (0, 1, \frac{1}{4})\Big) = \text{Vect}\Big((4, 0, 1), (0, 4, 1)\Big)$. *Ceci montre À LA FOIS que* F *est un sous-espace vectoriel de* $\mathbb{R}^3$ *et que la famille* $\mathcal{B}$ *est bien génératrice de* F.
- *Montrons que la famille* $\mathcal{B}$ *est libre. Soient* $\lambda, \mu \in \mathbb{R}$ *tels que* $\lambda(4, 0, 1) + \mu(0, 4, 1) = (0, 0, 0)$. *Alors :* $4\lambda = 4\mu = 0$, *donc* $\lambda = \mu = 0$ *comme voulu. C'est fini.*

Scanné avec CamScanner

Exercice

Montrer que pour tous $n \in \mathbb{N}$ et $\lambda \in \mathbb{K}$, la famille $\left(1, X-\lambda, (X-\lambda)^2, \cdots, (X-\lambda)^n\right)$ est une base de $\mathbb{K}_n[X]$ et que les coordonnées d'un polynôme $P \in \mathbb{K}_n[X]$ dans cette base sont $\left(P(\lambda), P'(\lambda), \frac{P''(\lambda)}{2} \cdots, \frac{P^{(n)}(\lambda)}{n!}\right)$.

Structure d'espace vectoriel : Famille de vecteurs

Solution

- Pour la liberté, soient $a_0, \cdots, a_n \in \mathbb{K}$. Faisons l'hypothèse que : $\sum_{i=0}^{n} a_i (X-\lambda)^i = 0$. Par composition à droite par $X+\lambda$: $\sum_{i=0}^{n} a_i X^i = 0$, donc aussitôt : $a_0 = \cdots = a_n = 0$.
- D'après la formule de Taylor : $P = \sum_{i=0}^{n} \frac{P^{(i)}(\lambda)}{i!}(X-\lambda)^i$ pour tout $P \in \mathbb{K}_n[X]$, donc $\left(1, X-\lambda, (X-\lambda)^2, \cdots, (X-\lambda)^n\right)$ engendre $\mathbb{K}_n[X]$ et la formule donne aussi les coordonnées de P.

Scanné avec CamScanner

Structure d'espace vectoriel : Dimension finie

Définition (Espace vectoriel de dimension finie)

Soit E un $\mathbb{K}$-espace vectoriel. On dit que E est de dimension finie s'il possède une partie génératrice **FINIE**, et de dimension infinie sinon.

Exemples

- $\mathbb{K}^n$ *et* $\mathbb{K}_n[X]$ *sont des espaces vectoriels de dimension finie car ils possèdent des familles génératrices finies (notamment les bases canoniques).*
- $\mathbb{K}[X]$ *est de dimension infinie. En effet, Pour toute famille* ***FINIE*** $(P_1, \cdots, P_n)$ *de polynômes non nuls, si nous posons :* $d = \max_{1 \leq i \leq n} \deg(Pi)$, *alors :* $\text{Vect}(P_1, \cdots, P_n) \subset \mathbb{K}_d[X] \neq \mathbb{K}[X]$, *donc* $(P_1, \cdots, P_n)$ *n'engendre pas* $\mathbb{K}[X]$. *Conclusion : aucune famille* ***FINIE*** *de* $\mathbb{K}[X]$ *n'engendre* $\mathbb{K}[X]$.

Structure d'espace vectoriel : Dimension finie

Passons maintenant à un théorème qui est à la base de la théorie sur la dimension des espaces vectoriels.

Théorème (Nombre maximal de vecteurs linéairement indépendants)

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie engendré par n éléments. Alors toute partie libre de E possède au plus n éléments.

Démonstration : Soient X une partie génératrice de E à n éléments et Y une partie libre de E. Supposant par l'absurde que Y possède au moins $n+1$ éléments, nous allons prouver par récurrence que pour tout $k \in \{0, \cdots, n\}$: "E est engendré par une famille de n vecteurs dont les $n-k$ premiers sont dans X et les k suivants dans Y."
On pourra conclure de la manière suivante. Pour $k = n$, E est engendré par une famille de n vecteurs de Y. En particulier, tout vecteur de Y est combinaison linéaire de ces n vecteurs, donc comme Y possède au moins $n+1$ éléments, Y est liée. Contradiction.

Scanné avec CamScanner

- Initialisation : La famille des n vecteurs de X engendre E.
- Hérédité : Soit $k \in \{0, \cdots, n-1\}$. Faisons l'hypothèse que E est engendré par $(x_1, \cdots, x_{n-k}, y_1, \cdots, y_k)$ pour certains $x_1, \cdots, x_{n-k} \in X$ et $y_1, \cdots, y_k \in Y$. Comme Y possède au moins $n+1$ éléments, nous pouvons nous donner un élément $y_{k+1} \in Y$ autre que $\underset{n-k}{y_1}, \cdots, \underset{k}{y_k}$. Par hypothèse de récurrence : $y_{k+1} = \sum_{i=1} \lambda_i x_i + \sum_{j=1} \mu_j y_j$ pour certains $\lambda_1, \cdots, \lambda_{n-k}, \mu_1, \cdots, \mu_k \in \mathbb{K}$. Comme Y est libre, il est impossible que tous les λ_i soient nuls car sinon y_{k+1} serait combinaison linéaire de $y_1, \cdots, y_k$. Quitte à modifier l'ordre des x_i, nous pouvons donc supposer : $\lambda_{n-k} \neq 0$. Ainsi, x_{n-k} est combinaison linéaire de $x_1, \cdots, x_{n-k-1}, y_1, \cdots, y_{k+1}$, donc enfin E est engendré par la famille $(x_1, \cdots, x_{n-k-1}, y_1, \cdots, y_{k+1})$ dont les $n-k-1$ premiers vecteurs sont dans X et les $k+1$ suivants dans Y.

Théorème (Théorème de la base extraite)

Soit E un $\mathbb{K}$-espace vectoriel admettant une famille génératrice finie $\mathcal{F}$. Alors $\mathcal{F}$ contient une sous-famille qui est une base de E.

- Un espace de dimension finie admet donc une base finie.

Scanné avec CamScanner

Structure d'espace vectoriel : Dimension finie

Démonstration : Raisonnons par récurrence. Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $\mathcal{P}_k$ la proposition "Toute famille génératrice de k vecteurs de E contient une sous-famille qui est une base de E".

- Initialisation : Si $k = 0$, E est engendré par 0 vecteur : $E = \{0_E\}$. La famille vide est une base de E.
- Hérédité : Supposons la propriété vraie au rang k et considérons une famille génératrice $\mathcal{F} = (x_1, \cdots, x_{k+1})$ de E. Si $\mathcal{F}$ est libre, c'est une base de E.
  Sinon $\mathcal{F}$ est liée et l'un des vecteurs de $\mathcal{F}$ est combinaison linéaire des autres. Nous pouvons retirer ce vecteur et noter $\mathcal{F}'$ la sous-famille obtenue. D'après ce qui précède, celle-ci est toujours génératrice. Comme $\mathcal{F}'$ contient k vecteurs, elle contient par hypothèse de récurrence une sous-famille $\mathcal{F}''$ qui est une base de E. $\mathcal{F}''$ étant elle-même une sous-famille de $\mathcal{F}$, la propriété est démontrée au rang $k + 1$.

Structure d'espace vectoriel : Dimension finie

▶ Si on connaît une famille génératrice de E, on peut toujours enlever des vecteurs combinaisons linéaires des autres jusqu'à obtenir une famille libre donc une base de E.

Remarque

- *Intuitivement, on a bien envie de définir la dimension d'un espace vectoriel comme le nombre de vecteurs qu'on trouve dans ses bases, mais $\cdots$ qui nous dit que toutes les bases ont le même nombre de vecteurs ? Pourquoi un espace vectoriel ne pourrait-il pas être à la fois de dimension 2 et de dimension 3 ?*
- *En principe, la notion de cardinal concerne les ensembles et les ensembles seulement, mais par abus de langage, une famille $(x_1, \cdots, x_n)$ de n objets est souvent appelée une famille de cardinal n, c'est très commode.*

Scanné avec CamScanner

Définition (Dimension)

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.

- Si : $E \neq \{0_E\}$, toutes les bases de E sont finies de même cardinal. Ce cardinal unique est appelé la dimension de E et notée $\dim E$.
- Si : $E = \{0_E\}$, on décrète par convention que : $\dim E = 0$.

Si : $\dim E = 1$, on dit que E est une droite (vectorielle), et si : $\dim E = 2$, que E est un plan (vectoriel).

Démonstration.

Supposons : $E \neq \{0_E\}$. Comme E est de dimension finie, nous avons vu plus haut que toutes les familles libres de E sont finies, donc en particulier ses bases aussi. Soient alors $\mathcal{B}$ une base de E à n éléments et $\mathcal{B}'$ une base de E à n' éléments. Comme $\mathcal{B}$ engendre E et comme $\mathcal{B}'$ est libre, nous avons vu déjà que : $n' \leq n$. De plus, par symétrie des rôles de $\mathcal{B}$ et $\mathcal{B}'$, on a aussi : $n \leq n'$. Conclusion : $n = n'$. □

Théorème

- *Pour tout* $n \in \mathbb{N}^*$ *:* $\dim \mathbb{K}^n = n$.
- *Pour tout* $n \in \mathbb{N}$ *:* $\dim \mathbb{K}_n[X] = n + 1$.

▶ À retenir : pour déterminer la dimension d'un espace vectoriel de dimension finie, il suffit d'exhiber une base de cet espace et de compter le nombre de vecteurs obtenus.

Scanné avec CamScanner

Exercice

On note $E = \mathbb{R}^{\mathbb{R}}$, $f, g, h : \mathbb{R} \to \mathbb{R}$ les applications définies par : $f(x) = 1, g(x) = e^x, h(x) = e^{-x}$ et $F = \text{Vect}(f, g, h)$. Déterminer dim F.

Solution

Par définition de F, la famille (f, g, h) engendre F. Montrons que (f, g, h) est libre. Soit $(a, b, c) \in \mathbb{R}^3$ tel que $af + bg + ch = 0$. On a :

$$\forall x \in \mathbb{R}, a + be^x + ce^{-x} = 0.$$

Par le changement de variable $t = e^x$, on déduit :

$$\forall t \in]0, +\infty[, a + bt + c\frac{1}{t} = 0,$$

c-à-d : $\forall t \in]0, +\infty[, bt^2 + at + c = 0$.
Le polynôme $bX^2 + aX + c$ s'annule donc en une infinité de réels (les réels > 0), donc c'est le polynôme nul, d'où : $a = b = c = 0$. Ainsi, (f, g, h) est libre. Enfin, puisque (f, g, h) est libre et engendre F, (f, g, h) est une base de F et on conclut que : dim $F = 3$.

Scanné avec CamScanner

Théorème (Dimension et cardinal d'une famille génératrice)

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n et $\mathcal{F}$ une famille génératrice de E. Alors $\text{Card}(\mathcal{F}) \geq n$, *et si* $\text{Card}(\mathcal{F}) = n$, *c'est une base de E.*

Démonstration.

Tout repose sur le théorème de la base extraite.

- $\mathcal{F}$ possède une sous-famille $\mathcal{F}'$ base de E qui comporte donc n vecteurs. Ainsi, $\mathcal{F}$ contient plus de n vecteurs.
- Si $\mathcal{F}$ possède n vecteurs, $\mathcal{F} = \mathcal{F}'$, ce qui fait de $\mathcal{F}$ une base de E.

□

▶ Dans la pratique, ce résultat a une importance capitale : il suffit qu'une famille soit génératrice et comporte autant de vecteurs que la dimension de E pour que celle-ci soit une base de E.

Voici maintenant l'équivalent du théorème de la base extraite pour les familles libres :

Théorème (Théorème de la base incomplète)

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n et $\mathcal{L}$ une famille libre de E. On peut compléter $\mathcal{L}$ en une base de E.

Scanné avec CamScanner

Démonstration : Soient $\mathcal{L} = (u_1, \cdots, u_k)$ une famille libre et $\mathcal{B} = (e_1, \cdots, e_n)$ une base de E.

- Si $\mathcal{L}$ est génératrice, c'est une base de E. Supposons désormais que $\mathcal{L}$ n'est pas génératrice.
- Il existe au moins un vecteur de $\mathcal{B}$ qui n'est pas une combinaison linéaire des vecteurs u_i. En effet, par l'absurde, si tous les vecteurs e_j étaient combinaisons linéaires des vecteurs u_i, on aurait $E = \text{Vect}(e_1, \cdots, e_n) \subset \text{Vect}(u_1, \cdots, u_k)$. Et comme $\text{Vect}(u_1, \cdots, u_k) \subset E$ (tous les vecteurs u_i sont dans E), on aurait $E = \text{Vect}(u_1, \cdots, u_k)$, ce qui ferait de $\mathcal{L}$ une famille génératrice de E, absurde par hypothèse.

- Soit e_{j_0} un vecteur non combinaison linéaire des vecteurs u_i. On pose $\mathcal{L}' = (u_1, \cdots, u_k, e_{j_0})$. Montrons que la famille $\mathcal{L}'$ reste libre. Pour cela, supposons que $\lambda_1 u_1 + \cdots + \lambda_k u_k + \lambda_{k+1} u_{j_0} = 0_E$. Si $\lambda_{k+1} \neq 0$, $e_{j_0} = -\dfrac{1}{\lambda_{k+1}}(\lambda_1 u_1 + \cdots + \lambda_k u_k)$ est une combinaison linéaire des vecteurs u_i. Absurde. Donc $\lambda_{k+1} = 0$. Ainsi, $\lambda_1 u_1 + \cdots + \lambda_k u_k = 0_E$. Comme $\mathcal{L}$ est libre, $\lambda_1 = \cdots = \lambda_k = 0$. On a bien montré que $\lambda_1 = \cdots = \lambda_k = \lambda_{k+1} = 0$.
- On peut poursuivre le raisonnement et ajouter à $\mathcal{L}'$ des vecteurs non combinaison linéaire jusqu'à obtenir une famille génératrice, qui restera libre (comme $\mathcal{L}'$). On aura ainsi construit une base de E contenant $\mathcal{L}$.

Scanné avec CamScanner

Théorème (Dimension et cardinal d'une famille libre)

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie n et $\mathcal{L}$ une famille libre de E. Alors $\text{Card}(\mathcal{L}) \leq n$, *et si* $\text{Card}(\mathcal{L}) = n$, *c'est une base de E.*

Démonstration.

Tout repose sur le théorème de la base incomplète.

- $\mathcal{L}$ possède une sur-famille $\mathcal{L}'$ base de E qui comporte donc n vecteurs. Ainsi, $\mathcal{L}$ contient moins de n vecteurs.
- Si $\mathcal{L}$ possède n vecteurs, $\mathcal{L} = \mathcal{L}'$, ce qui fait de $\mathcal{L}$ une base de E.

□

▶ Si on connaît une famille libre d'un espace vectoriel E qui contient $n = \dim(E)$ vecteurs, c'est une base !

En résumé

Dans un $\mathbb{K}$-espace vectoriel de dimension finie n, toute famille libre possède au plus n éléments et toute famille génératrice en possède au moins n.

Théorème (Dimension d'un s.e.v.)

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors F est de dimension finie et : $\dim F \leq \dim E$, *avec égalité si et seulement si : $F = E$.*

▶ Pour montrer que deux espaces vectoriels E et F de dimension finie sont égaux, il suffit donc de prouver que $F \subset E$ puis que $\dim F = \dim E$. La double inclusion ne sera alors pas nécessaire.

Scanné avec CamScanner

Démonstration.

Si : $F = \{0_E\}$, nous n'avons rien à démontrer. Si au contraire : $F \neq \{0_E\}$, l'ensemble $\mathcal{N}$ des nombres d'éléments des familles libres de F est non vide. Cet ensemble est par ailleurs majoré par $\dim E$ car toute famille libre de F est une famille libre de E, donc constituée d'au plus $\dim E$ vecteurs.
Conclusion : $\mathcal{N}$ possède un plus grand élément n inférieur ou égal à $\dim E$. Donnons-nous alors une famille libre $\mathcal{L}$ de F à n éléments. Pour tout $x \in F$, la famille $\mathcal{L}$ augmentée de x est liée par maximalité de n dans $\mathcal{N}$, donc comme $\mathcal{L}$ est libre, x est forcément combinaison linéaire de $\mathcal{L}$.
Conclusion : libre et génératrice, $\mathcal{L}$ est une base de F, donc enfin F est de dimension finie et : $\dim F = n \leq \dim E$. Et si : $\dim E = \dim F = n$? Dans ce cas $\mathcal{L}$ est une famille libre de E à $n = \dim E$ éléments, donc c'est déjà une base de E et : $E = \text{Vect}(\mathcal{L}) = F$. □

Exemples

Dans $\mathbb{R}^3$, *on note :* $u = (1,1,0)$, $v = (1,0,1)$, $x = (3,1,2)$ *et* $y = (1,3,-2)$. *Soient* F *et* G *les sous-espaces vectoriels de* $\mathbb{R}^3$ *suivants :*

$$F = \text{Vect}(u,v) \quad \textit{et} \quad G = \text{Vect}(x,y).$$

Montrer que $F = G$.

- *On remarque que :* $x = u + 2v$ *et* $y = 3u - 2v$. *Ainsi :* $x, y \in F$ *et par suite* $G \subset F$. *De plus, il est clair que* (u,v) *est libre et que* (x,y) *est libre, donc :* $\dim G = \dim F = 2$. *On conclut que :* $G = F$.

Scanné avec CamScanner

Structure d'espace vectoriel : Dimension finie

Théorème (Dimension d'un espace vectoriel produit)

Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. Alors $E \times F = \{(x, y) \mid x \in E, y \in F\}$ est de dimension finie et :
$\dim(E \times F) = \dim E + \dim F$.
Le résultat se généralise au cas d'un nombre fini quelconque d'espaces vectoriels.

Démonstration : Supposons E et F de dimensions non nulles et donnons-nous $(e_1, \cdots, e_m)$ une base de E et $(f_1, \cdots, f_n)$ une base de F.
Nous allons montrer que la famille
$\mathcal{B} = \Big((e_1, 0_F), \cdots, (e_m, 0_F), (0_E, f_1), \cdots, (0_E, f_n)\Big)$ est une base de $E \times F$.
Cela montrera bien que $E \times F$ est de dimension finie
$m + n = \dim E + \dim F$.

Structure d'espace vectoriel : Dimension finie

- Montrons que $\mathcal{B}$ engendre $E \times F$. Pour tout $(x, y) \in E \times F$, si nous notons $(x_1, \cdots, x_m)$ les coordonnées de x dans $(e_1, \cdots, e_m)$ et $(y_1, \cdots, y_n)$ celles de y dans $(f_1, \cdots, f_n)$, alors :

$$(x, y) = \Big(\sum_{i=1}^{m} x_i e_i, \sum_{j=1}^{n} y_j f_j\Big) = \sum_{i=1}^{m} x_i (e_i, 0_F) + \sum_{j=1}^{n} y_j (0_E, f_j).$$

- Pour la liberté, soient $\lambda_1, \cdots, \lambda_m, \mu_1, \cdots, \mu_n \in \mathbb{K}$ pour lesquels :
$\sum_{i=1}^{m} \lambda_i (e_i, 0_F) + \sum_{j=1}^{n} \mu_j (0_E, f_j) = (0_E, 0_F)$. Alors :
$\Big(\sum_{i=1}^{m} \lambda_i e_i, \sum_{j=1}^{n} \mu_j f_j\Big) = (0_E, 0_F)$, donc : $\sum_{i=1}^{m} \lambda_i e_i = 0_E$ et $\sum_{j=1}^{n} \mu_j f_j = 0_F$.
Ainsi, par liberté de $(e_i)_{1 \leq i \leq m}$ et $(f_j)_{1 \leq j \leq n}$:
$\lambda_1 = \cdots = \lambda_m = \mu_1 = \cdots = \mu_n = 0$.

Scanné avec CamScanner

Structure d'espace vectoriel : Somme de deux s.e.v

Définition (Somme de deux s.e.v.)

Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E.

- L'ensemble $F + G = \{x_1 + x_2 \mid x_1 \in F \text{ et } x_2 \in G\}$ est un sous-espace vectoriel de E appelé la somme de F et G.
- Cette somme $F + G$ est également le plus petit sous-espace vectoriel de E contenant F et G. Cela signifie que tout sous-espace vectoriel de E contenant F et G contient aussi $F + G$.

Attention : Ne confondez pas **SOMME** et **RÉUNION** ! La somme est un sous-espace vectoriel, mais pas la réunion en général.

Structure d'espace vectoriel : Somme de deux s.e.v

Démonstration.

Montrons d'abord que $F + G$ est un sous-espace vectoriel de E.

- $0_E \in F + G$ car $0_E = \underbrace{0_E}_{\in F} + \underbrace{0_E}_{\in G}$.
- Soient $x, y \in F + G$ et $\lambda \in \mathbb{K}$. Il existe $x_1, y_1 \in F$ et $x_2, y_2 \in G$ tels que $x = x_1 + x_2$ et $y = y_1 + y_2$. Donc :
  $\lambda x + y = \lambda(x_1 + x_2) + (y_1 + y_2) = (\underbrace{\lambda x_1 + y_1}_{\in F}) + (\underbrace{\lambda x_2 + y_2}_{\in G})$ car F et G sont des sous-espaces vectoriels, donc stables par combinaison linéaire. Ainsi, on a bien $\lambda x + y \in F + G$.

$F + G$ est donc un sous-espace vectoriel de E.
De plus, $F \subset F + G$ car tout vecteur $x \in F$ peut s'écrire sous la forme $x = \underbrace{x}_{\in F} + \underbrace{0_E}_{\in G}$. Idem pour G. □

Scanné avec CamScanner

Théorème (Parties génératrices d'une somme de deux s.e.v)

Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Si F est engendré par $(f_1, f_2, \cdots, f_m)$ et si G est engendré par $(g_1, g_2, \cdots, g_n)$, alors $F + G$ est engendré par $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$.

Démonstration.

Soit $x \in F + G$. Il existe alors $f \in F$ et $g \in G$ tels que $x = f + g$. Or $(f_1, f_2, \cdots, f_m)$ engendre F, donc il existe $\lambda_1, \lambda_2, \cdots, \lambda_m \in \mathbb{K}$ tels que $f = \lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_m f_m$; de même $(g_1, g_2, \cdots, g_n)$ engendre G, donc il existe $\mu_1, \mu_2, \cdots, \mu_n \in \mathbb{K}$ tels que $g = \mu_1 g_1 + \mu_2 g_2 + \cdots + \mu_n g_n$.
Finalement on obtient
$x = \lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_m f_m + \mu_1 g_1 + \mu_2 g_2 + \cdots + \mu_n g_n$. C'est le résultat voulu. □

Théorème (Formule de Grassmann)

Soient E un $\mathbb{K}$-espace vectoriel pas nécessairement de dimension finie et F et G deux sous-espaces vectoriels de dimension finie de E. La somme $F + G$ est alors elle aussi de dimension finie, et plus précisément :
$\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$.

Démonstration : Pour ne pas alourdir la preuve par l'étude de cas particuliers sans intérêt, on peut supposer que $F \cap G = \{0_E\}$, $F \cap G \neq F$ et $F \cap G \neq G$.
Toute base $(e_1, \cdots, e_p)$ de $F \cap G$ peut être complétée en une base $(e_1, \cdots, e_p, f_1, \cdots, f_q)$ de F et en une base $(e_1, \cdots, e_p, g_1, \cdots, g_r)$ de G. Par concaténation, la famille $(e_1, \cdots, e_p, f_1, \cdots, f_q, g_1, \cdots, g_r)$ est alors une famille génératrice de $F + G$, donc en particulier, $F + G$ est de dimension finie.

Scanné avec CamScanner

Structure d'espace vectoriel : Somme de deux s.e.v

Nous allons montrer qu'en réalité la famille $(e_1, \cdots, e_p, f_1, \cdots, f_q, g_1, \cdots, g_r)$ est aussi libre, et donc que c'est une base de $F+G$. La formule de Grassmann en découlera aussitôt : $\dim(F+G) = p+q+r = (p+q)+(p+r)-p = \dim F + \dim G - \dim(F \cap G)$.
Soient donc $\lambda_1, \cdots, \lambda_p, \mu_1, \cdots, \mu_q, \nu_1, \cdots, \nu_r \in \mathbb{K}^{p+q+r}$ pour lesquels :
$\underbrace{\lambda_1 e_1 + \cdots + \lambda_p e_p}_{\in F \cap G} + \underbrace{\mu_1 f_1 + \cdots, \mu_q f_q}_{\in F} + \underbrace{\nu_1 g_1 + \cdots + \nu_r g_r}_{\in G} = 0_E$.

- Pour commencer, on a $\nu_1 g_1 + \cdots + \nu_r g_r$ appartient à $F \cap G$ donc est combinaison linéaire de $e_1, \cdots, e_p$, ce qui n'est possible que si $\nu_1 = \cdots = \nu_r = 0$ par liberté de $(e_1, \cdots, e_p, g_1, \cdots, g_r)$.
- De même, $\mu_1 f_1 + \cdots + \mu_q f_q$ appartient à $F \cap G$ donc est combinaison linéaire de $e_1, \cdots, e_p$, ce qui n'est possible que si $\mu_1 = \cdots = \mu_q = 0$ par liberté de $(e_1, \cdots, e_p, f_1, \cdots, f_q)$.
- Finalement : $\lambda_1 e_1 + \cdots + \lambda_p e_p = 0_E$, donc $\lambda_1 = \cdots = \lambda_p = 0$ par liberté de $(e_1, \cdots, e_p)$.

Structure d'espace vectoriel : Somme de deux s.e.v

Définition (Somme directe de deux s.e.v)

Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. On dit que F et G sont en somme directe si tout vecteur de $F+G$ s'écrit **de manière unique** comme somme d'un élément de F et d'un élément de G. On note alors souvent $F \oplus G$ la somme $F+G$, pour indiquer qu'il y a somme directe.

▶ Le petit rond qu'on ajoute à la notation "F + G" pour indiquer que la somme est directe ne fait pas de $F+G$ et $F \oplus G$ des ensembles différents, la notation "$F \oplus G$" contient juste une INFORMATION d'unicité en plus.

Scanné avec CamScanner

Théorème (Caractérisation de la somme directe)

Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Les assertions suivantes sont équivalentes :

1. *F et G sont en somme directe.*
2. $F \cap G = \{0_E\}$.

Dans ce cas, par ailleurs, si F et G sont de dimension finie :
$\dim(F + G) = \dim F + \dim G$.

Démonstration.

- $(1 \Rightarrow 2)$ Supposons F et G en somme directe et montrons que $F \cap G = \{0_E\}$, ce qui revient à montrer que $F \cap G \subset \{0_E\}$ puisque 0_E appartient au sous-espace vectoriel $F \cap G$ de toute façon. Soit $x \in F \cap G$. Alors $x = \overbrace{x}^{\in F} + \overbrace{0_E}^{\in G} = \overbrace{0_E}^{\in F} + \overbrace{x}^{\in G}$, donc : $x = 0_E$ par définition de la somme directe.
- $(2 \Rightarrow 1)$ Supposons que : $F \cap G = \{0_E\}$. Soient $x_1, x_2 \in F$ et $y_1, y_2 \in G$ pour lesquels : $x_1 + y_1 = x_2 + y_2$. Comme : $x_1 - x_2 = y_2 - y_1 \in F \cap G = \{0_E\}$, alors $x_1 = x_2$ et $y_1 = y_2$.

La formule : $\dim(F + G) = \dim F + \dim G$ n'est enfin qu'un cas particulier de la formule de Grassmann. □

Scanné avec CamScanner

Exemples

$F = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ *et* $G = \{(x, y, z) \in \mathbb{R}^3 \mid x = y = z\}$ *sont en somme directe.*

- *On a :* $F = \{(x, y, -x - y) \mid x, y \in \mathbb{R}\} = \text{Vect}\Big((1, 0, -1), (0, 1, -1)\Big)$ *et* $G = \text{Vect}\Big((1, 1, 1)\Big)$ *et donc* F *et* G *sont bien des s.e.v de* $\mathbb{R}^3$*. Il nous reste donc de montrer que* $F \cap G = \{0_{\mathbb{R}^3}\}$*, et même que* $F \cap G \subset \{0_{\mathbb{R}^3}\}$*. Soit* $(x, y, z) \in F \cap G$*. Alors* $x + y + z = 0$ *et* $x = y = z$*. Du coup :* $x + x + x = 0$*, donc* $x = 0$ *et enfin* $x = y = z = 0$*, i.e.* $(x, y, z) = 0_{\mathbb{R}^3}$*.*

Théorème (Bases d'une somme directe de deux s.e.v)

Soient E *un* $\mathbb{K}$*-espace vectoriel et* F *et* G *deux sous-espaces vectoriels de* E *en somme directe. Si* $(f_1, f_2, \cdots, f_m)$ *est une base de* F *et* $(g_1, g_2, \cdots, g_n)$ *une base de* G*, alors* $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$ *est une base de* $F \oplus G$*. Une telle base dont les premiers vecteurs forment une base de* F *et les suivants une base de* G *est dite adaptée à la somme directe* $F \oplus G$*.*

Attention : Ce résultat est faux si on ne suppose pas la somme directe. Pour les sommes en général, on dispose seulement du résultat vu précédemment sur les familles génératrices.

Scanné avec CamScanner

Démonstration.

Nous avons déjà vu que $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$ est une famille génératrice de $F \oplus G$. Il ne nous reste donc qu'à montrer que cette famille est libre.

Soient donc $\lambda_1, \lambda_2, \cdots, \lambda_m, \mu_1, \mu_2, \cdots, \mu_n \in \mathbb{K}$ tels que $\sum_{k=1}^{m} \lambda_k f_k + \sum_{\ell=1}^{n} \mu_\ell g_\ell = 0_E$. Cette somme est une décomposition de 0_E comme somme d'un élément de F et d'un élément de G. Or la somme est directe donc il y a unicité d'une telle décomposition ; bref $\sum_{k=1}^{m} \lambda_k f_k = \sum_{\ell=1}^{n} \mu_\ell g_\ell = 0_E$. Enfin, les familles $(f_1, f_2, \cdots, f_m)$ et $(g_1, g_2, \cdots, g_n)$ étant libres, on en déduit comme voulu que $\lambda_1 = \lambda_2 = \cdots = \lambda_m = \mu_1 = \mu_2 = \cdots = \mu_n = 0$. □

Définition (Sous-espaces vectoriels supplémentaires)

Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E. Les assertions suivantes sont équivalentes :

1. Tout vecteur de E est d'une et une seule manière la somme d'un élément de F et d'un élément de G : $\forall x \in E, \exists!(f, g) \in F \times G, x = f + g$.
2. E est la somme directe de F et G : $E = F \oplus G$, ce qui revient à dire que : $E = F + G$ **ET** que F et G sont en somme directe.

On dit dans ces conditions que F et G sont supplémentaires dans E. On dit aussi que F est **UN** supplémentaire de G dans E et que G est **UN** supplémentaire de F dans E.

Scanné avec CamScanner

Démonstration.

- Supposons que, pour tout $x \in E$, il existe un unique couple $(f, g) \in F \times G$ tel que $x = f + g$ et montrons que $E = F \oplus G$. Il est clair que $E = F + G$. Soit $x \in F \cap G$. On peut alors écrire $x = x + 0_E$ avec $x \in F$ et $0_E \in G$, mais également $x = 0_E + x$ avec $0_E \in F$ et $x \in G$. L'unicité de la décomposition impose que $x = 0_E$. Donc $E = F \oplus G$.
- Réciproquement, supposons $E = F \oplus G$. Soit $x \in E$. Comme $E = F + G$, il existe $f \in F$ et $g \in G$ tels que $x = f + g$. Montrons que cette décomposition est unique. Soient $f' \in F$ et $g' \in G$ tels que $x = f' + g'$. On a alors $f + g = f' + g'$, c'est-à-dire $f - f' = g' - g$. Or $f - f' \in F$ et $g' - g \in G$. On en déduit que $f - f' \in F \cap G = \{0_E\}$. Donc $f = f'$ et, de même, $g = g'$.

□

Structure d'espace vectoriel : Somme de deux s.e.v

Théorème (Base adaptée)

Soient E un $\mathbb{K}$-espace vectoriel et F et G deux sous-espaces vectoriels de E de bases respectives $(f_1, \cdots, f_m)$ et $(g_1, \cdots, g_n)$. Alors, $E = F \oplus G$ si et seulement si la famille $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$ est une base de E. Dans ce cas, la famille $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$ est qualifiée de base adaptée.

Scanné avec CamScanner

Démonstration.

Nous avons déjà vu que si F et G sont en somme directe alors la famille $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$ est une base de $F \oplus G = E$.
Réciproquement, supposons que $(f_1, f_2, \cdots, f_m, g_1, g_2, \cdots, g_n)$ est une base de E. Alors tout $x \in E$ s'écrit d'une manière unique :
$x = \underbrace{\lambda_1 f_1 + \cdots + \lambda_m f_m}_{\in F} + \underbrace{\mu_1 g_1 + \cdots + \mu_n g_n}_{\in G}$ c'est-à-dire tout $x \in E$ s'écrit d'une manière unique $x = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in G$; donc $E = F \oplus G$. □

- Nous observerons l'importance des bases adaptées dans la prochaine partie mais remarquons déjà que ce théorème nous fournit une nouvelle méthode pour justifier que deux espaces sont supplémentaires : il suffit de montrer que la concaténation de deux bases de F et G constitue une base de E pour que ceux-ci soient supplémentaires dans E.

Théorème (Existence de supplémentaires en dimension finie)

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et F un sous-espace vectoriel de E. Alors F possède un supplémentaire dans E.
Le supplémentaire de F n'est pas unique, mais, les supplémentaires de F dans E ont tous pour dimension : $\dim E - \dim F$.

Démonstration.

Soit $(f_1, \cdots, f_m)$ une base de F et soit $n = \dim E$. D'après le théorème de la base incomplète, il existe $f_{m+1}, \cdots, f_n$ vecteurs de E tels que $(f_1, \cdots, f_m, f_{m+1}, \cdots, f_n)$ est une base de E. En posant $G = \text{Vect}(f_{m+1}, \cdots, f_n)$ on obtient, d'après le théorème précédent, un supplémentaire de F dans E. Puisque le choix de $f_{m+1}, \cdots, f_n$ n'est pas unique, le supplémentaire de F n'est pas unique ; cependant, tous les supplémentaires de F sont de dimension $n - m$, m étant la dimension de F. □

Scanné avec CamScanner

Méthode

Pour montrer que deux s.e.v F, G d'un e.v E de dimension finie sont supplémentaires dans E, on peut essayer de montrer qu'il existe une base $\mathcal{F}$ de F et une base $\mathcal{G}$ de G telles que $\mathcal{F} \cup \mathcal{G}$, obtenue par concaténation des deux bases $\mathcal{F}$ et $\mathcal{G}$, soit une base de E.

Exercice

Soit : $F = \{P \in \mathbb{R}_3[X] \mid P(X+1) = P(1-X)\}$. Montrer que $\text{Vect}(X, X^3)$ est un supplémentaire de F dans $\mathbb{R}_3[X]$.

Solution

- Nous avons besoin d'abord d'une base de F. Soit $P = aX^3 + bX^2 + cX + d \in \mathbb{R}_3[X]$. On a :

$$\begin{aligned} P \in F &\Leftrightarrow a(X+1)^3 + b(X+1)^2 + c(X+1) + d \\ &= a(1-X)^3 + b(1-X)^2 + c(1-X) + d \end{aligned}$$

$$\Leftrightarrow \begin{cases} a & = -a \\ 3a+b & = 3a+b \\ 3a+2b+c & = -3a-2b-c \\ a+b+c+d & = a+b+c+d \end{cases} \Leftrightarrow a = 0 \text{ et } 2b+c = 0.$$

  Ce calcul montre que $(1, X^2 - 2X)$ engendre F. Cette famille étant libre, c'est une base de F.

- Complétons-la en une base $(1, X^2 - 2X, X, X^3)$ de $\mathbb{R}_3[X]$. Conclusion : $\text{Vect}(X, X^3)$ est UN supplémentaire de F dans $\mathbb{R}_3[X]$.

Scanné avec CamScanner

Le résultat suivant est aussi d'un usage fréquent :

Théorème (Caractérisation de la supplémentarité en dimension finie)

Soient E un espace de dimension finie et F, G deux sous-espaces vectoriels de E. F et G sont supplémentaires dans E si et seulement si l'une des propositions suivantes est vérifiée :

1. $E = F + G$ *et* $F \cap G = \{0_E\}$.
2. $E = F + G$ *et* $\dim(E) = \dim(F) + \dim(G)$.
3. $F \cap G = \{0_E\}$ *et* $\dim(E) = \dim(F) + \dim(G)$.

▶ On a souvent recours à la dernière caractérisation. On commence par montrer que l'intersection des deux espaces est réduite à $\{0_E\}$ puis on prouve l'égalité des dimensions.

Démonstration.

Le point (1) correspond à la définition.

- Montrons que (1) $\Leftrightarrow$ (2). On suppose que $E = F + G$. On a :

$$F \cap G = \{0_E\} \Leftrightarrow \dim(F \cap G) = 0 \Leftrightarrow \dim(F + G) = \dim F + \dim G$$
$$\Leftrightarrow \dim E = \dim F + \dim G.$$

- Montrons que (2) $\Leftrightarrow$ (3). On suppose que $\dim E = \dim F + \dim G$. Remarquons que $F + G \subset E$ donc pour avoir $F + G = E$, il faut et il suffit que $\dim(F + G) = \dim(E)$. On a :

$$F \cap G = \{0_E\} \Leftrightarrow \dim(F \cap G) = 0 \Leftrightarrow \dim(F + G) = \dim F + \dim G$$
$$\Leftrightarrow \dim(F + G) = \dim E.$$

□

Scanné avec CamScanner

Exercice

On considère les deux ensembles suivants :

$$A = \{(x+y, x-y, 2y) \mid (x,y) \in \mathbb{R}^2\};$$
$$B = \{(x,y,z) \in \mathbb{R}^3 \mid 2x = y \text{ et } y = 3z\}.$$

1. Montrer que A et B sont des sous-espaces vectoriels de $\mathbb{R}^3$.
2. Montrer que $\mathbb{R}^3 = A \oplus B$.

Solution

1. On a :
   - $A = \text{Vect}\Big((1,1,0),(1,-1,2)\Big)$ est un plan vectoriel.
   - $B = \text{Vect}\Big((\frac{1}{2},1,\frac{1}{3})\Big) = \text{Vect}\Big((3,6,2)\Big)$ est une droite vectorielle.
2. Montrons maintenant que A et B sont supplémentaires :
   - $A \cap B = \{0_{\mathbb{R}^3}\}$ car si on considère $u \in A \cap B$, alors,

$$u \in A \Leftrightarrow \exists (x,y) \in \mathbb{R}^2 : u = (x+y, x-y, 2y)$$

$$u \in B \Leftrightarrow \begin{cases} 2(x+y) &= x-y, \\ x-y &= 6y \end{cases} \Leftrightarrow \begin{cases} x+3y &= 0, \\ x-7y &= 0 \end{cases} \Leftrightarrow x = y = 0$$

Donc $u = (0,0,0)$.

- $\dim A + \dim B = 2 + 1 = 3 = \dim \mathbb{R}^3$.

Nous avons ainsi démontré que $\mathbb{R}^3 = A \oplus B$.

Scanné avec CamScanner

Structure d'espace vectoriel : Somme de deux s.e.v

Exercice

$E = \mathbb{R}_4[X]$ et $F = \{P \in E \mid P(0) = P'(0) = P'(1) = 0\}$.

1. Montrer que F est un espace vectoriel, déterminer une base de F et préciser sa dimension.
2. Montrer que $G = \text{Vect}(1, X, 1 + X + X^2)$ est un supplémentaire de F dans E.

Exercice

Soit $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$ l'espace vectoriel des fonctions de $\mathbb{R}$ dans $\mathbb{R}$. On note F le sous-espace vectoriel des fonctions paires (i.e. $f(-x) = f(x)$ pour tout $x \in \mathbb{R}$) et G le sous-espace vectoriel des fonctions impaires (i.e. $f(-x) = -f(x)$ pour tout $x \in \mathbb{R}$). Montrer que F et G sont supplémentaires.

Applications linéaires : Introduction

La structure d'espace vectoriel ne devient vraiment intéressante que si l'on introduit la notion d'application linéaire. Il s'agit des applications entre espaces vectoriels qui, dans un sens que nous allons préciser, "conservent la structure d'espace vectoriel".
Dans cette partie, nous allons donner essentiellement les définitions et les résultats élémentaires de base.

Scanné avec CamScanner

Applications linéaires : Définitions et premières propriétés

Définition (Application linéaire)

Soient E et F deux $\mathbb{K}$-espaces vectoriels. On appelle application linéaire de E dans F toute application $f : E \to F$ qui préserve les combinaisons linéaires :

$$\forall x, y \in E, \forall \lambda, \mu \in \mathbb{K}, f(\lambda x + \mu y) = \lambda f(x) + \mu f(y).$$

L'ensemble des applications linéaires de E dans F est noté $\mathcal{L}(E, F)$.

- **Cas particulier où $E = F$:** Une application linéaire de E dans E est aussi appelée un endomorphisme de E. L'ensemble des endomorphismes de E est noté $\mathcal{L}(E)$.
- **Cas particulier où $F = \mathbb{K}$:** Une application linéaire de E dans $\mathbb{K}$ est aussi appelée une forme linéaire de E.

Applications linéaires : Définitions et premières propriétés

Explication : Une application linéaire n'est rien d'autre qu'un "morphisme d'espaces vectoriels", à ceci près qu'on n'emploie jamais cette expression. Bref, c'est une application qui conserve les combinaisons linéaires.

Remarque

- *Clairement :* $f(0_E) = f(0_E + 0_E) = f(0_E) + f(0_E)$, *donc après simplification :* $f(0_E) = 0_F$.
- *Ensuite, si A est un sous-espace vectoriel de E, alors $f_{|A}$ est aussi linéaire (mais sur A). En effet, s'il est vrai pour tous $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$ que :* $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$, *c'est a fortiori vrai pour tous $x, y \in A$.*
- *Enfin, pour vérifier que f est linéaire, il est suffisant de vérifier que :* $f(\lambda x + y) = \lambda f(x) + f(y)$ *pour tous $x, y \in E$ et $\lambda \in \mathbb{K}$ avec UN SEUL SCALAIRE. Dans ce cas, pour tous $x, y \in E$ et $\lambda, \mu \in \mathbb{K}$:* $f(\lambda x) = f(\lambda x + 0_E) = \lambda f(x) + f(0_E) = \lambda f(x) + 0_F = \lambda f(x)$, *puis de même :* $f(\mu y) = \mu f(y)$, *donc enfin :* $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$.

Scanné avec CamScanner

Définition (Homothétie)

Soient E un $\mathbb{K}$-espace vectoriel et $\lambda \in \mathbb{K}$. On appelle homothétie de E de rapport λ l'application λId_E, i.e. : $\begin{cases} E & \to E \\ x & \mapsto \lambda x. \end{cases}$ Cette application est un endomorphisme de E. En particulier : $Id_E \in \mathcal{L}(E)$.

Démonstration.

Pour tous $x, y \in E$ et $\alpha \in \mathbb{K}$:

$$(\lambda Id_E)(\alpha x + y) = \lambda(\alpha x + y) = \alpha(\lambda Id_E)(x) + (\lambda Id_E)(y).$$

□

Exemples

L'application $(x, y) \overset{f}{\mapsto} (x, x + y, x - 2y)$ *est linéaire de* $\mathbb{R}^2$ *dans* $\mathbb{R}^3$.

- *Pour tous* $(x, y), (x', y') \in \mathbb{R}^2$ *et* $\lambda \in \mathbb{R}$:

$$\begin{aligned} f(\lambda(x, y) + (x', y')) &= f(\lambda x + x', \lambda y + y') \\ &= \Big(\lambda x + x', (\lambda x + x') + (\lambda y + y'), (\lambda x + x') - 2(\lambda y + y')\Big) \\ &= \lambda(x, x + y, x - 2y) + (x', x' + y', x' - 2y') \\ &= \lambda f(x, y) + f(x', y'). \end{aligned}$$

Scanné avec CamScanner

Exemples

- *Soit $E = E_1 \oplus E_2$; alors tout vecteur $x \in E$ s'écrit d'une manière unique $x = x_1 + x_2$ où $x_1 \in E_1$ et $x_2 \in E_2$.*
  L'application :

$$\begin{aligned} pr_1 : \quad E &\longrightarrow E \\ x_1 + x_2 &\longmapsto x_1 \end{aligned}$$

  est une application linéaire dite projecteur sur E_1 parallèlement à E_2.
- *Soit $v_0 \neq 0$ un vecteur de E ; l'application translation définie par*

$$\begin{aligned} tr : \quad E &\longrightarrow E \\ v &\longmapsto v + v_0 \end{aligned}$$

n'est pas linéaire (noter, par exemple, que : $tr(0) = v_0 \neq 0$).

Théorème (Opérations sur les applications linéaires)

1. *Soient E et F deux $\mathbb{K}$-espaces vectoriels. Alors $\mathcal{L}(E, F)$ est un sous-espace vectoriel de F^E, donc un $\mathbb{K}$-espace vectoriel.*
2. *Soient E, F et G trois $\mathbb{K}$-espaces vectoriels. Pour tous $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, G)$: $g \circ f \in \mathcal{L}(E, G)$.*
3. *Soient E, F et G trois $\mathbb{K}$-espaces vectoriels et $f, f' \in \mathcal{L}(E, F)$ et $g, g' \in \mathcal{L}(F, G)$. Alors : $g \circ (f + f') = (g \circ f) + (g \circ f')$ et $(g + g') \circ f = (g \circ f) + (g' \circ f)$.*
4. *Soit E un $\mathbb{K}$-espace vectoriel. Alors $(\mathcal{L}(E), +, \circ)$ est un anneau, non commutatif en général, avec $1_{\mathcal{L}(E)} = Id_E$.*

Scanné avec CamScanner

Démonstration :

1. Pour commencer, on a $\mathcal{L}(E,F) \subset F^E$ et l'application nulle $x \mapsto 0_F$ de E dans F est linéaire. Soient $f, g \in \mathcal{L}(E,F)$ et $\lambda \in \mathbb{K}$. Alors, pour tous $x, y \in E$ et $\alpha \in \mathbb{K}$:

$$\begin{aligned}(\lambda f + g)(\alpha x + y) &= \lambda f(\alpha x + y) + g(\alpha x + y)\\ &= \lambda(\alpha f(x) + f(y)) + \alpha g(x) + g(y)\\ &= \alpha(\lambda f(x) + g(x)) + \lambda f(y) + g(y) = \alpha(\lambda f + g)(x) + (\lambda f + g)(y).\end{aligned}$$

2. Pour tous $x, y \in E$ et $\lambda \in \mathbb{K}$: $(g \circ f)(\lambda x + y) = g(f(\lambda x + y)) = g(\lambda f(x) + f(y)) = \lambda g(f(x)) + g(f(y)) = \lambda(g \circ f)(x) + (g \circ f)(y)$.
3. Facile.
4. L'assertion (1) montre en particulier que $(\mathcal{L}(E), +)$ est un groupe commutatif. On sait par ailleurs que la composition est une loi de composition interne sur $\mathcal{L}(E)$ via (2), qu'elle est associative, que $Id_E \in \mathcal{L}(E)$ en est l'élément neutre, et enfin que la composition est distributive sur l'addition via (3).

Deux formules à connaître

Soient E un $\mathbb{K}$-espace vectoriel, $f, g \in \mathcal{L}(E)$ et $n \in \mathbb{N}$. On suppose que f et g commutent. Alors :

$$(f+g)^n = \sum_{k=0}^{n} C_n^k f^k \circ g^{n-k}$$

et $f^n - g^n = (f-g) \circ \sum_{k=0}^{n-1} f^k \circ g^{n-k-1}$

(attention, les puissances désignent des compositions).

- Ces deux formules se démontrent ici exactement comme elles se démontrent dans $\mathbb{C}$.

Attention : Dans ces formules, il est essentiel que f et g commutent.

Scanné avec CamScanner

Applications linéaires : Définitions et premières propriétés

Théorème (Images directe et réciproque d'un s.e.v par une application linéaire)

Soient E et F deux $\mathbb{K}$-espaces vectoriels, $f \in \mathcal{L}(E,F)$, A un sous-espace vectoriel de E et B un sous-espace vectoriel de F.

1. *L'image (directe) $f(A)$ de A par f est un sous-espace vectoriel de F.*
2. *L'image réciproque $f^{-1}(B)$ de B par f est un sous-espace vectoriel de E.*

Applications linéaires : Définitions et premières propriétés

Démonstration.

1. Montrons que $f(A)$ est un sous-espace vectoriel de F. Déjà, on a $f(A) \subset F$ et de plus $0_F = f(0_E) \in f(A)$. Soient $y, y' \in f(A)$ et $\lambda \in \mathbb{K}$. Puisque $y, y' \in f(A)$, il existe $a, a' \in A$ tels que $y = f(a)$ et $y' = f(a')$. Par linéarité de f : $\lambda y + y' = \lambda f(a) + f(a') = f(\lambda a + a')$, et par ailleurs : $\lambda a + a' \in A$ car A est un sous-espace vectoriel de E, donc comme voulu : $\lambda y + y' \in f(A)$.
2. Montrons que $f^{-1}(B)$ est un sous-espace vectoriel de E. Déjà, on a $f^{-1}(B) \subset E$ et de plus $0_E \in f^{-1}(B)$ car $f(0_E) = 0_F \in B$. Soient $x, x' \in f^{-1}(B)$ et $\lambda \in \mathbb{K}$. Par linéarité de f, on a : $f(\lambda x + x') = \lambda f(x) + f(x')$. Or par définition de x et x', $f(x), f(x') \in B$ et B est un sous-espace vectoriel de E. Donc $f(\lambda x + x') \in B$, ce qui montre que $\lambda x + x' \in f^{-1}(B)$.

□

Scanné avec CamScanner

Applications linéaires : Noyau et image d'une application linéaire

Définition (Noyau et image d'une application linéaire)

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$.

- On appelle noyau de f, noté $\operatorname{Ker} f$, l'ensemble $f^{-1}\Big(\{0_F\}\Big) = \{x \in E \mid f(x) = 0_F\}$.
- On appelle image de f, noté $\operatorname{Im} f$, l'ensemble $f(E) = \{y \in F \mid \exists x \in E : y = f(x)\} = \{f(x), x \in E\}$.

Applications linéaires : Noyau et image d'une application linéaire

Théorème

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. Alors, $\operatorname{Ker} f$ *est un sous-espace vectoriel de E.*

Démonstration.

- Tout d'abord on a : $0_E \in \operatorname{Ker} f$, car $f(0_E) = 0_F$.
- Soient $x, y \in \operatorname{Ker} f$ et $\lambda \in \mathbb{K}$. On a : $f(\lambda x + y) \overset{f \in \mathcal{L}(E,F)}{=} \lambda f(x) + f(y) = \lambda 0_F + 0_F = 0_F$ donc $\lambda x + y \in \operatorname{Ker} f$.

□

Scanné avec CamScanner

Applications linéaires : Noyau et image d'une application linéaire

Théorème

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. L'application linéaire f est injective si et seulement si $\operatorname{Ker} f = \{0_E\}$.

- Pour montrer qu'une application linéaire $f : E \to F$ est injective, il suffit de montrer que $\operatorname{Ker} f = \{0_E\}$, c-à-d montrer que :
$\forall x \in E, \Big(f(x) = 0 \Rightarrow x = 0_E\Big)$.

Applications linéaires : Noyau et image d'une application linéaire

Démonstration.

Démontrons ce résultat par double implication.

- ($\Rightarrow$) Supposons f injective, c'est-à-dire que :
$\forall (x,y) \in E^2, f(x) = f(y) \Rightarrow x = y$ et montrons qu'alors :
$\operatorname{Ker} f = \{0_E\}$ ou encore : $\operatorname{Ker} f \subset \{0_E\}$. Or pour tout $x \in \operatorname{Ker} f$:
$f(x) = 0_F = f(0_E)$, donc comme f est injective : $x = 0_E$.
- ($\Leftarrow$) Supposons maintenant que $\operatorname{Ker} f = \{0_E\}$ et montrons que f est injective. Soient $x, x' \in E$ tels que : $f(x) = f(x')$. Alors :
$f(x - x') = f(x) - f(x') = 0_F$ par linéarité, donc :
$x - x' \in \operatorname{Ker} f = \{0_E\}$, donc : $x - x' = 0_E$, i.e. : $x = x'$.

□

Scanné avec CamScanner

Applications linéaires : Noyau et image d'une application linéaire

Exemples

Soit f l'endomorphisme de $\mathbb{R}^3$ défini par $f(x,y,z) = (2x-y, y+z, z-x)$. Étudions l'injectivité de f.

- *Déterminons pour cela son noyau. Soit $(x,y,z) \in \mathbb{R}^3$. On a :*

$$(x,y,z) \in \operatorname{Ker} f \Leftrightarrow f(x,y,z) = 0_{\mathbb{R}^3} \Leftrightarrow (2x-y, y+z, z-x) = 0_{\mathbb{R}^3}.$$

Ce qui conduit à la résolution suivante :

$$\begin{cases} 2x - y &= 0 \\ y + z &= 0 \\ z - x &= 0 \end{cases} \Leftrightarrow x = y = z = 0.$$

Ainsi : $\operatorname{Ker} f = 0_{\mathbb{R}^3}$ et f est injective.

Applications linéaires : Noyau et image d'une application linéaire

Théorème

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. Alors, $\operatorname{Im} f$ est un sous-espace vectoriel de F.

Démonstration.

- Comme $0_F = f(0_E)$, on a bien : $0_F \in \operatorname{Im} f$.
- De plus, si $x, y \in \operatorname{Im} f$ et $\lambda \in \mathbb{K}$, il existe $x', y' \in E$ tels que $x = f(x')$ et $y = f(y')$. D'où,

$$\lambda x + y = \lambda f(x') + f(y') \overset{f \in \mathcal{L}(E,F)}{=} f(\lambda x' + y') \in \operatorname{Im} f.$$

□

Scanné avec CamScanner

Applications linéaires : Noyau et image d'une application linéaire

Théorème (Familles génératrices de l'image d'une application linéaire)

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$. On suppose que E possède une famille génératrice $(x_1, x_2, \cdots, x_n)$. Alors $\Big(f(x_1), f(x_2), \cdots, f(x_n)\Big)$ est une famille génératrice de $\operatorname{Im} f$. En résumé :

$$\operatorname{Im} f = \operatorname{Vect}\Big(f(x_1), f(x_2), \cdots, f(x_n)\Big).$$

Applications linéaires : Noyau et image d'une application linéaire

Démonstration.

Soit $y \in \operatorname{Im} f$. Alors il existe $x \in E$ tel que $y = f(x)$. Or $(x_1, x_2, \cdots, x_n)$ engendre E par hypothèse, donc $x = \sum_{k=1}^{n} \lambda_k x_k$ pour certains $\lambda_1, \lambda_2, \cdots, \lambda_n \in \mathbb{K}$. Par suite : $y = f(x) = f\Big(\sum_{k=1}^{n} \lambda_k x_k\Big) = \sum_{k=1}^{n} \lambda_k f(x_k)$, ce qui montre bien que la famille $\Big(f(x_1), f(x_2), \cdots, f(x_n)\Big)$ engendre $\operatorname{Im} f$. □

Scanné avec CamScanner

Définition (Isomorphisme, espaces vectoriels isomorphes)

Soient E et F deux $\mathbb{K}$-espaces vectoriels.

- On appelle isomorphisme de E sur F toute application linéaire bijective de E sur F.
  Cas particulier où $E = F$: Un isomorphisme de E sur E est aussi appelée un automorphisme de E. L'ensemble des automorphismes de E est noté $\mathrm{GL}(E)$ et appelé le groupe linéaire de E.
- On dit que F est isomorphe à E s'il existe un isomorphisme de E sur F.

▶ Le fait que deux espaces vectoriels soient isomorphes signifie intuitivement que ces deux espaces sont "identiques" d'un strict point de vue vectoriel.

Théorème (Composition d'isomorphismes, réciproque d'un isomorphisme)

Soient E, F et G trois $\mathbb{K}$-espaces vectoriels.

1. *Si f est un isomorphisme de E sur F et g un isomorphisme de F sur G, $g \circ f$ est un isomorphisme de E sur G.*
2. *Si f est un isomorphisme de E sur F, alors f^{-1} est un isomorphisme de F sur E.*

▶ En d'autres termes, la relation d'isomorphisme entre espaces vectoriels est une relation d'équivalence (pour la réflexivité, remarquer simplement que Id_E est un isomorphisme de E pour tout $\mathbb{K}$-espace vectoriel E).

Scanné avec CamScanner

Démonstration.

1. La composée de deux applications bijectives (resp. linéaires) est bijective (resp. linéaire).
2. Nous savons que f^{-1} est bijective de F sur E. Montrons que f^{-1} est linéaire. Soient $x', y' \in F$ et $\lambda \in \mathbb{K}$. Posons alors $x = f^{-1}(x')$ et $y = f^{-1}(y')$. On a alors $x' = f(x)$ et $y' = f(y)$ et,

$$\begin{aligned} f^{-1}(\lambda x' + y') &= f^{-1}\Big(\lambda f(x) + f(y)\Big) \\ &= f^{-1}\Big(f(\lambda x + y)\Big) \\ &= \lambda x + y, \quad \text{car} \quad f^{-1} \circ f = Id_E \\ &= \lambda f^{-1}(x') + f^{-1}(y'). \end{aligned}$$

□

Le théorème qui suit montre que les $\mathbb{K}$-espaces vectoriels de dimension finie sont tous "identiques" à un $\mathbb{K}^n$.

Théorème (Effet d'un isomorphisme sur la dimension)

- *Soient E et F deux $\mathbb{K}$-espaces vectoriels. Si E est de dimension finie et si F est isomorphe à E, alors F est de dimension finie et :* $\dim E = \dim F$.
- *Réciproquement, deux $\mathbb{K}$-espaces vectoriels de* ***MÊMES*** *dimensions finies sont isomorphes. En particulier, tout $\mathbb{K}$-espace vectoriel de dimension finie $n \neq 0$ est isomorphe à $\mathbb{K}^n$.*

Scanné avec CamScanner

Démonstration :

- On peut supposer $E \neq \{0_E\}$ et noter f un isomorphisme de E sur F. De dimension finie $n \neq 0$, E possède une base $(e_1, \cdots, e_n)$. En particulier, par surjectivité de f : $F = \operatorname{Im} f = \operatorname{Vect}\Big(f(e_1), \cdots, f(e_n)\Big)$, donc F est engendré par la famille $\Big(f(e_1), \cdots, f(e_n)\Big)$ donc est de dimension finie. Nous allons en fait montrer que cette famille est libre. Il en découlera que c'est une base de F, et donc que : $\dim F = n = \dim E$. Soient $\lambda_1, \cdots, \lambda_n \in \mathbb{K}$ tels que : $\sum_{i=1}^{n} \lambda_i f(e_i) = 0_F$. Alors : $f\Big(\sum_{i=1}^{n} \lambda_i e_i\Big) = 0_F$, donc : $\sum_{i=1}^{n} \lambda_i e_i \in \operatorname{Ker} f$. Or f est injective et donc : $\sum_{i=1}^{n} \lambda_i e_i = 0_E$. Finalement comme voulu, la famille $(e_1, \cdots, e_n)$ étant libre : $\lambda_1 = \cdots = \lambda_n$.

- Soient E et F deux $\mathbb{K}$-espaces vectoriels de même dimension finie n. On peut supposer $n \neq 0$. Nous allons montrer que E est isomorphe à $\mathbb{K}^n$ et E et F seront alors isomorphes tout court.
  Comme $n \neq 0$, E possède une base $(e_1, \cdots, e_n)$. Soit alors φ l'application $(x_1, \cdots, x_n) \in \mathbb{K}^n \mapsto \sum_{i=1}^{n} x_i e_i$ de $\mathbb{K}^n$ dans E. On a, φ est linéaire. En effet, pour tous $x = (x_1, \cdots, x_n), x = (x'_1, \cdots, x'_n) \in \mathbb{K}^n$ et $\lambda \in \mathbb{K}$:

$$\varphi(\lambda x + x') = \sum_{i=1}^{n} (\lambda x_i + x'_i) e_i = \lambda \sum_{i=1}^{n} x_i e_i + \sum_{i=1}^{n} x'_i e_i = \lambda \varphi(x) + \varphi(x').$$

  De plus, φ est bijective de $\mathbb{K}^n$ sur E, car $(e_1, \cdots, e_n)$ étant une base de E alors :
  $\forall x \in E, \exists!(x_1, \cdots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^{n} x_i e_i = \varphi(x_1, \cdots, x_n)$. D'où φ est un isomorphisme de $\mathbb{K}^n$ sur E.

Scanné avec CamScanner

Remarque

L'application φ de la preuve précédente mérite qu'on s'y attarde un instant. Soient E un $\mathbb{K}$-espace vectoriel et $(e_1, \cdots, e_n)$ une famille ***QUELCONQUE*** *de E (plus forcément une base de E). L'application $(x_1, \cdots, x_n) \in \mathbb{K}^n \overset{\varphi}{\mapsto} \sum_{i=1}^{n} x_i e_i$ est toujours linéaire de $\mathbb{K}^n$ dans E.*

- *φ surjective si et seulement si :*
  $\forall x \in E, \exists (x_1, \cdots, x_n) \in \mathbb{K}^n, x = \sum_{i=1}^{n} x_i e_i$, *i.e. si et seulement si la famille $(e_1, \cdots, e_n)$ engendre E.*
- *φ est injective si et seulement si : $\operatorname{Ker}\varphi = \{0_E\}$, i.e. si et seulement si : $\forall (x_1, \cdots, x_n) \in \mathbb{K}^n, \sum_{i=1}^{n} x_i e_i = 0_E \Rightarrow x_1 = \cdots = x_n = 0$, i.e. si et seulement si la famille $(e_1, \cdots, e_n)$ est libre.*

Le théorème qui suit caractérise l'injectivité/surjectivité d'une application linéaire par l'image d'une base.

Théorème

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E, F)$. On suppose que E possède une base $(e_i)_{i \in I}$.

1. *f est surjective de E sur F si et seulement si $\left(f(e_i)\right)_{i \in I}$ engendre F.*
2. *f est injective sur E si seulement si $\left(f(e_i)\right)_{i \in I}$ est libre.*
3. *f est un isomorphisme de E sur F si et seulement si $\left(f(e_i)\right)_{i \in I}$ est une base de F.*

Démonstration :

1 On sait que : $\operatorname{Im} f = \operatorname{Vect}\left(f(e_i)\right)_{i \in I}$. Ainsi : $\operatorname{Im} f = F$ si et seulement si $\left(f(e_i)\right)_{i \in I}$ engendre F.

Scanné avec CamScanner

Applications linéaires : Isomorphisme et e. v. isomorphes

2 Supposons f injective et montrons que $\Big(f(e_i)\Big)_{i\in I}$ est libre.
Soit $(\lambda_i)_{i\in I} \in \mathbb{K}^I$ presque nulle telle que : $\sum_{i\in I} \lambda_i f(e_i) = 0_F$.
Alors : $f\Big(\sum_{i\in I} \lambda_i e_i\Big) = 0_F$ et donc : $\sum_{i\in I} \lambda_i e_i \in \operatorname{Ker} f$. Comme f est injective, alors $\sum_{i\in I} \lambda_i e_i = 0_E$ et donc : $\lambda_i = 0$ pour tout $i \in I$.
Réciproquement, supposons $\Big(f(e_i)\Big)_{i\in I}$ est libre et montrons que f est injective, i.e. que : $\operatorname{Ker} f \subset \{0_E\}$. Soient $x \in \operatorname{Ker} f$ de coordonnées $(x_i)_{i\in I}$ dans $(e_i)_{i\in I}$. Alors :
$0_F = f(x) = f\Big(\sum_{i\in I} \lambda_i e_i\Big) = \sum_{i\in I} x_i f(e_i)$, donc par hypothèse pour tout $i \in I$: $x_i = 0$, et donc a fortiori : $x = 0_E$.

Applications linéaires : Notion de rang

Définition (Application linéaire de rang fini, rang)

Soient E et F deux $\mathbb{K}$-espaces vectoriels pas nécessairement de dimension finie et $f \in \mathcal{L}(E, F)$.

- On dit que f est de rang fini si $\operatorname{Im} f$ est de dimension finie, et de rang infini sinon.
- Si f est de rang fini, on appelle rang de f , noté $\operatorname{rg}(f)$, la dimension de $\operatorname{Im} f$.

Scanné avec CamScanner

Théorème (Inégalités sur le rang et cas d'égalité)

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$.

1. *Si F est de dimension finie, f est de rang fini et : $\mathrm{rg}(f) \leq \dim F$, avec égalité si et seulement si f est surjective.*
2. *Si E est de dimension finie, f est de rang fini et : $\mathrm{rg}(f) \leq \dim E$, avec égalité si et seulement si f est injective.*

Démonstration.

1. Comme : $\mathrm{Im}\, f \subset F$, alors $\mathrm{Im}\, f$ est de dimension finie et : $\mathrm{rg}(f) = \dim \mathrm{Im}\, f \leq \dim F$, avec égalité si et seulement si : $\mathrm{Im}\, f = F$, i.e. si et seulement si f est surjective.
2. Supposons $E \neq \{0_E\}$ et donnons-nous une base $(e_1, \cdots, e_n)$ de E. Par suite : $\mathrm{Im}\, f = \mathrm{Vect}\Big(f(e_1), \cdots, f(e_n)\Big)$, donc $\mathrm{Im}\, f$ est de dimension finie et : $\mathrm{rg}(f) = \dim \mathrm{Im}\, f \leq n = \dim E$, avec égalité si et seulement si $\Big(f(e_1), \cdots, f(e_n)\Big)$ est libre, i.e. si et seulement si f est injective.

□

Scanné avec CamScanner

Applications linéaires : Notion de rang

Théorème (Applications linéaires entre e. v. de mêmes dimensions finies)

Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimensions finies ***ÉGALES*** *et $f \in \mathcal{L}(E, F)$.*

$$f \text{ est bijective} \Leftrightarrow f \text{ est injective} \Leftrightarrow f \text{ est surjective.}$$

Attention : Le théorème ne dit pas que : bijectif = surjectif = injectif en algèbre linéaire ! Elle affirme seulement que c'est vrai lorsque les espaces vectoriels de départ et d'arrivée ont **MÊME DIMENSION FINIE**.

Démonstration.

Par hypothèse : $\dim E = \dim F$. Du coup, f est injective si et seulement si : $\text{rg}(f) = \dim E$, i.e. si et seulement si : $\text{rg}(f) = \dim F$, i.e. si et seulement si f est surjective. □

Applications linéaires : Notion de rang

Remarque

Ce résultat est faux en dimension infinie. En voici un contre-exemple d'un endomorphisme surjectif qui n'est pas injectif :

$$\begin{aligned} D : \quad \mathbb{R}[X] &\longrightarrow \mathbb{R}[X] \\ P &\longmapsto D(P) = P'. \end{aligned}$$

En effet :

- *Le polynôme $X^0 = 1$ appartient à $\text{Ker}(D)$ et il n'est pas nul, donc l'endomorphisme D n'est pas injectif.*
- *Soit $Q \in \mathbb{R}[X]$. Il existe $n \in \mathbb{N}$, $a_0, \cdots, a_n \in \mathbb{R}$ tels que : $Q = \sum_{k=0}^{n} a_k X^k$. En notant $P = \sum_{k=0}^{n} \frac{a_k}{k+1} X^{k+1}$, on a $P \in \mathbb{R}[X]$ et $D(P) = P' = Q$. Ceci montre que D est surjectif.*

Scanné avec CamScanner

Exemples

En voici un autre contre-exemple d'un endomorphisme injectif qui n'est pas surjectif. :

$$f : \quad \mathbb{R}[X] \longrightarrow \mathbb{R}[X]$$
$$P \longmapsto f(P) = XP.$$

En effet :

- *Soit* $P \in \mathbb{R}[X]$ *tel que* $f(P) = 0$. *Alors :* $XP = 0$. *Or, comme l'anneau* $\mathbb{R}[X]$ *est intègre et* $X \neq 0$, *alors :* $P = 0$. *D'où* $\mathrm{Ker}\, f = \{0_{\mathbb{R}[X]}\}$ *et donc l'endomorphisme* f *est injectif.*
- *On a :* $\mathrm{Im}\, f = \{f(P), P \in \mathbb{R}[X]\} = \{XP, P \in \mathbb{R}[X]\} = \{Q \in \mathbb{R}[X] \mid Q(0) = 0\}$. *Donc par exemple* $X^0 = 1 \notin \mathrm{Im}\, f$, *ce qui montre que* $\mathrm{Im}\, f \subsetneq E$. *Il en résulte que l'endomorphisme* f *n'est pas une surjection de* E *sur* E.

Exercice

Soit $n \in \mathbb{N}^*$. On note $E = \mathbb{R}_n[X]$ et

$$f : \quad E \longrightarrow E$$
$$P \longmapsto f(P) = XP' + P.$$

Vérifier que $f \in \mathcal{L}(E)$ et montrer que f est bijectif.

Scanné avec CamScanner

Solution

- Pour tout $P \in E$, on a $\deg P \leq n$, donc : $\deg P' \leq n-1$ et $\deg(XP') \leq n$. Ainsi : $\deg(XP'+P) \leq n$ et donc $f(P) \in E$. D'autre part, soient $P, Q \in E$ et $\lambda \in \mathbb{R}$. On a : $f(\lambda P+Q) = X(\lambda P+Q)' + (\lambda P+Q) = \lambda(XP'+P) + (XQ'+Q) = \lambda f(P) + f(Q)$. Donc f est linéaire. D'où : $f \in \mathcal{L}(E)$.
- Puisque E est de dimension finie ($\dim(E) = n+1$), pour montrer que f est bijectif, il suffit de montrer que, par exemple, que f est injectif. Soit $P \in \operatorname{Ker} f$. Supposons $P \neq 0$ et notons $d = \deg P \leq n$. Il existe $a_0, \cdots, a_d \in \mathbb{R}$ avec $a_d \neq 0$, tels que $P = \sum_{k=0}^{d} a_k X^k$. Le coefficient du terme de degré d de $f(P)$ est $da_d + a_d = (d+1)a_d \neq 0$. Ce qui contredit le fait que $f(P) = 0$. Ceci montre que $\operatorname{Ker} f = \{0_E\}$ et donc f est injectif. On conclut que f est bijectif.

Exercice

Soit

$$\begin{aligned} \varphi : \quad \mathbb{R}_n[X] &\longrightarrow \mathbb{R}^{n+1} \\ P &\longmapsto \varphi(P) = (P(0), P(1), P(2), \ldots, P(n)). \end{aligned}$$

Montrer que φ est un isomorphisme.

Indication

D'abord, il est facile de vérifier que φ est linéaire.
Concernant la bijectivité, remarquer que puisque $\dim \mathbb{R}_n[X] = \dim \mathbb{R}^{n+1}$, il suffit donc de vérifier que φ est injective et pour cela, utiliser le fait qu'un polynôme non nul de degré n admet au plus n racines.

Scanné avec CamScanner

Théorème (Forme géométrique du théorème du rang)

Soient E et F deux $\mathbb{K}$-espaces vectoriels pas nécessairement de dimension finie et $f \in \mathcal{L}(E, F)$.
Si $\operatorname{Ker} f$ possède un supplémentaire I dans E, alors $f_{|I}$ est un isomorphisme de I sur $\operatorname{Im} f$.

Explication : Dans l'égalité : $E = I \oplus \operatorname{Ker} f$, $\operatorname{Ker} f$ est l'ensemble des éléments de E que f ne voit pas, donc f ne voit passer que I, et comme I ne touche $\operatorname{Ker} f$ que du bout de son zéro, f est injective sur I, donc envoie bijectivement I sur $\operatorname{Im} f$. De manière moins imagée, $\left(f_{|I}\right)^{-1}$ est l'application qui, à tout élément de $\operatorname{Im} f$, associe son unique antécédent dans I.

Démonstration.

Par restriction, $f_{|I}$ est linéaire de I dans $\operatorname{Im} f$.

- Pour l'injectivité, sachant que I et $\operatorname{Ker} f$ sont en somme directe : $\operatorname{Ker} f_{|I} = I \cap \operatorname{Ker} f = \{0_E\}$.
- Pour la surjectivité, soit $y \in \operatorname{Im} f$, disons : $y = f(x)$ pour un certain $x \in E$. Comme $E = I + \operatorname{Ker} f$, alors : $x = i + k$ pour certains $i \in I$ et $k \in \operatorname{Ker} f$, donc : $y = f(x) = f(i) + f(k) = f(i) + 0_F = f_{|I}(i)$.

□

Scanné avec CamScanner

Théorème (Théorème du rang)

Soient E et F deux $\mathbb{K}$-espaces vectoriels et $f \in \mathcal{L}(E,F)$.
Si E est de dimension finie : $\dim E = \dim \operatorname{Ker} f + \operatorname{rg}(f)$.

Morale de l'histoire : Si on connait le noyau, on connait un peu l'image (et vice versa).

- L'hypothèse selon laquelle E est de dimension finie garantit en particulier que $\operatorname{Ker} f$ et $\operatorname{Im} f$ le sont aussi.

Démonstration.

Comme E est de dimension finie, $\operatorname{Ker} f$ possède un supplémentaire I dans E. Or, d'après la forme géométrique du théorème du rang, $f_{|I}$ est un isomorphisme de I sur $\operatorname{Im} f$ et donc : $\dim I = \dim \operatorname{Im} f$. Par supplémentarité de I et $\operatorname{Ker} f$ dans E, on obtient :
$\operatorname{rg}(f) = \dim \operatorname{Im} f = \dim I = \dim E - \dim \operatorname{Ker} f$. □

Exemples

Soient E un $\mathbb{K}$-espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$. Si :
$f^3 = 0_{\mathcal{L}(E)}$, *alors :* $\operatorname{rg}(f) + \operatorname{rg}(f^2) \leq \dim E$.

- *En effet, l'égalité :* $f^3 = 0_{\mathcal{L}(E)}$ *montre que pour tout* $x \in E$: $f\left(f^2(x)\right) = 0_E$, *i.e. que :* $\operatorname{Im}(f^2) \subset \operatorname{Ker} f$ *et donc en particulier que :* $\operatorname{rg}(f^2) \leq \dim \operatorname{Ker} f$. *Appliquons alors le théorème du rang à f, ce qui est possible car E est de dimension finie pour obtenir :*
$\dim E = \dim \operatorname{Ker} f + \operatorname{rg}(f) \geq \operatorname{rg}(f) + \operatorname{rg}(f^2)$.

Scanné avec CamScanner

Applications linéaires : Existence d'applications linéaires

Pour connaitre une application en général, on n'a pas trop d'autre choix que de connaître l'ensemble de ses valeurs point par point. En revanche, pour une application linéaire, ce lot considérable d'informations peut être résumé par un nombre restreint de valeurs stratégiques. On connaît par exemple parfaitement l'application $(x, y, z) \mapsto (2x + y + z, 3x - z)$ de $\mathbb{R}^3$ dans $\mathbb{R}^2$ **SI ON SAIT QU'ELLE EST LINÉAIRE** et si on sait que : $f(1, 0, 0) = (2, 3), f(0, 1, 0) = (1, 0)$ et $f(0, 0, 1) = (1, -1)$.

- En effet, pour tout $(x, y, z) \in \mathbb{R}^3$:

$$\begin{aligned} f(x, y, z) &= f\Big(x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1)\Big) \\ &\overset{\text{Linéarité}}{=} xf(1, 0, 0) + yf(0, 1, 0) + zf(0, 0, 1) \\ &= x(2, 3) + y(1, 0) + z(1, -1) = (2x + y + z, 3x - z). \end{aligned}$$

Applications linéaires : Existence d'applications linéaires

Le théorème qui suit, fondamental, généralise ce principe. Il signifie que, pour se donner une application linéaire complètement, on peut se contenter de donner les valeurs qu'elle prend sur une base quelconque fixée de l'espace vectoriel de départ.

Théorème (Détermination d'une application linéaire par l'image d'une base)

Soient E et F deux $\mathbb{K}$-espaces vectoriels. On suppose que E possède une base $(e_1, e_2, \cdots, e_n)$. Pour toute famille $(f_1, f_2, \cdots, f_n)$ de vecteurs de F, il existe une et une seule application linéaire f de E dans F telle que : $\forall k \in \{1, \cdots, n\}, f(e_k) = f_k$.

Explication : Pour connaître/définir une application linéaire complètement, il suffit de connaître/définir les valeurs qu'elle prend sur une base de l'espace de départ.

Scanné avec CamScanner

Démonstration : Soit $(f_1, f_2, \cdots, f_n)$ une famille fixée de vecteurs de F.

- **Unicité :** Soient $f, g \in \mathcal{L}(E, F)$ telles que : $\forall k \in \{1, \cdots, n\}, f(e_k) = g(e_k) = f_k$. Montrons que $f = g$. Pour tout $x \in E$ de coordonnées $(x_1, x_2, \cdots, x_n)$ dans $(e_1, e_2, \cdots, e_n)$, on a :

$$f(x) = f\Big(\sum_{k=1}^{n} x_k e_k\Big) = \sum_{k=1}^{n} x_k f(e_k) = \sum_{k=1}^{n} x_k g(e_k)$$
$$= g\Big(\sum_{k=1}^{n} x_k e_k\Big) = g(x),$$

et donc $f = g$.

- **Existence :** Soit f l'application de E dans F qui associe, à tout vecteur x de E de coordonnées $(x_1, x_2, \cdots, x_n)$ dans $(e_1, e_2, \cdots, e_n)$, le vecteur $f(x) = \sum_{k=1}^{n} x_k f_k$ de F. Montrons que f est linéaire. Soient $x, y \in E$ et $\lambda \in \mathbb{K}$. Si $(x_k)_{1 \leq k \leq n}$ et $(y_k)_{1 \leq k \leq n}$ sont les coordonnées respectives de x et y dans $(e_1, e_2, \cdots, e_n)$, les coordonnées de $\lambda x + y$ sont $(\lambda x_k + y_k)_{1 \leq k \leq n}$. Du coup :

$$f(\lambda x + y) = \sum_{k=1}^{n} (\lambda x_k + y_k) f_k = \lambda \sum_{k=1}^{n} x_k f_k + \sum_{k=1}^{n} y_k f_k = \lambda f(x) + f(y),$$

donc f est bien linéaire. Enfin, soit $k \in \{1, \cdots, n\}$. Alors les coordonnées de e_k sont la famille $(0, \cdots, 0, 1, 0, .., 0)$ dans laquelle le 1 est placé en $k^{ème}$ position, donc aussitôt $f(e_k) = f_k$.

Scanné avec CamScanner

Applications linéaires : e. v. d'applications linéaires

Théorème (Dimension d'un espace vectoriel d'applications linéaires)

Soient E et F deux $\mathbb{K}$-espaces vectoriels de dimension finie. Alors $\mathcal{L}(E,F)$ est de dimension finie et : $\dim \mathcal{L}(E,F) = \dim E \times \dim F$.

Applications linéaires : e. v. d'applications linéaires

Démonstration :

- Si : $\dim E = 0$, la seule application linéaire de E dans F est l'application nulle qui envoie 0_E sur 0_F, donc : $\mathcal{L}(E,F) = \{0_{\mathcal{L}(E,F)}\}$ et $\dim \mathcal{L}(E,F) = 0 = \dim E \times \dim F$.
- Si : $\dim E \neq 0$, nous pouvons nous donner une base $(e_1, \cdots, e_n)$ de E. Il n'est pas trop dur de vérifier que l'application $u \overset{\varphi}{\mapsto} \Big(u(e_1), \cdots, u(e_n)\Big)$ est linéaire de $\mathcal{L}(E,F)$ dans F^n, et d'après le théorème précédent :

$$\forall (f_1, \cdots, f_n) \in F^n, \exists! u \in \mathcal{L}(E,F), \varphi(u) = (f_1, \cdots, f_n).$$

Conclusion : linéaire bijective, φ est un isomorphisme de $\mathcal{L}(E,F)$ sur F^n. Or F est de dimension finie, donc F^n aussi par produit, puis $\mathcal{L}(E,F)$ par isomorphisme. Finalement :

$$\dim \mathcal{L}(E,F) = \dim F^n = n \times \dim F = \dim E \times \dim F.$$

Scanné avec CamScanner

Bibliographie

Voici une liste d'ouvrages auxquels le texte fait référence et qui contiennent des précisions sur les notions abordées.

- ✓ **Jean-Marie Arnaudiès et Henri Fraysse,** *Cours de mathématiques 1, Algèbre,* Dunod 1987.
- ✓ **Claude Deschamps et André Warusfel,** *Mathématiques tout-en-un, 1re année Cours et exercices corrigés,* 2e édition, Dunod 2003.
- ✓ **Joseph Grifone,** *Algèbre linéaire,* CÉPADUÈS-ÉDITIONS 2011.
- ✓ **Jean-Pierre Marco et Laurent Lazzarini,** *Mathématiques L1 Cours complet avec 1000 tests et exercices corrigés,* Pearson Education 2007.

Merci pour votre attention

Scanné avec CamScanner