Algèbre

Martin Mugnier

DD ENSAE-HEC, 2019

Chapitre 1: Espaces vectoriels, Applications linéaires, Matrices

Définition

*On appelle un **groupe** la donnée d'un ensemble $\mathbb{K}$ et d'une opération $\underset{\mathbb{K}}{+}$ telle que*

- $\underset{\mathbb{K}}{+}$ *est une loi de composition interne sur* $\mathbb{K}$: $\forall (a, b) \in \mathbb{K}^2, a \underset{\mathbb{K}}{+} b \in \mathbb{K}$,
- *associative :* $\forall (a, b, c) \in \mathbb{K}^3, (a \underset{\mathbb{K}}{+} b) \underset{\mathbb{K}}{+} c = a \underset{\mathbb{K}}{+} (b \underset{\mathbb{K}}{+} c)$
- *possède un élément neutre :* $\exists 0_{\mathbb{K}} \in \mathbb{K} : \forall a \in \mathbb{K},\ a \underset{\mathbb{K}}{+} 0_{\mathbb{K}} = 0_{\mathbb{K}} \underset{\mathbb{K}}{+} a = a$
- *tout élément de* $\mathbb{K}$ *possède un symétrique :*

$$\forall a \in \mathbb{K}, \exists (-a) \in \mathbb{K},\ a \underset{\mathbb{K}}{+} (-a) = (-a) \underset{\mathbb{K}}{+} (a) = 0_{\mathbb{K}}$$

Si de plus $\underset{\mathbb{K}}{+}$ *est commutative alors* $(\mathbb{K}, \underset{\mathbb{K}}{+})$ *est dit "groupe abélien".*

Structure d'espace vectoriel

Définition

*On appelle espace vectoriel sur $\mathbb{K}$, un ensemble E, dont les éléments sont appellés **vecteurs**, muni de deux opérations : **une loi interne** (appellée addition et notée $\underset{E}{+}$) et une **loi externe** (appellée multiplication par un scalaire et notée, $\underset{E}{\times}$) telles que :*

i) $(E, \underset{E}{+})$ *est un groupe abélien,*

ii) $\forall \lambda \in \mathbb{K}, \forall (x, y) \in E^2, \lambda \underset{E}{\times} (x \underset{E}{+} y) = \lambda \underset{E}{\times} x \underset{E}{+} \lambda \underset{E}{\times} y$

iii) $\underset{E}{\times}$ *est exo-distributive à gauche par rapport à* $\underset{K}{+}$,

iv) $\underset{E}{\times}$ *est exo-associative à gauche pa rapport à* $\underset{K}{\times}$,

v) $\forall x \in E,\ 1_{\mathbb{K}} \underset{E}{\times} x = x$

Dans la suite, $0_E =$ élément neutre pour $\underset{E}{+}$, pour tout $x \in E$, $-x$ désigne son symétrique pour $\underset{E}{+}$.

Structure d'espace vectoriel

Ici, $\mathbb{K} = \mathbb{R}$.

Proposition

Si $(E, \underset{E}{+}, \underset{E}{\times})$ *est un* $\mathbb{K} - e.v.$ *alors*

1. $\forall x \in E, 0_{\mathbb{K}} \underset{E}{\times} x = 0_E$
2. $\forall \mu \in \mathbb{K}, \mu \underset{E}{\times} 0_E = 0_E$
3. $\forall \mu \in \mathbb{K}, \forall x \in E,\ \mu \underset{E}{\times} (-x) = -(\mu \underset{E}{\times} x)$
4. $\forall \mu \in \mathbb{K}, \forall x \in E, (-\mu) \underset{E}{\times} x = -(\mu \underset{E}{\times} x)$
5. $\forall \mu \in \mathbb{K} - \{0_{\mathbb{K}}\}, \forall (x, y) \in E^2,\ \mu \underset{E}{\times} x = \mu \underset{E}{\times} y \implies x = y$

A montrer.

Quelques exemples : $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^n$, l'ensemble $\mathbb{R}^A$ des applications de A dans $\mathbb{R}$ où :

- l'addition est définie par : pour tout $f, g \in \mathbb{R}^A$, $f + g : x \in A \mapsto f(x) + g(x)$,
- la multiplication par un scalaire est définie par : pour tout $f \in \mathbb{R}^A$, $\lambda \in \mathbb{R}$, $\lambda f : x \mapsto \lambda f(x)$.

$\mathbb{R}^A$ est un espace vectoriel de fonctions.

Sous-espace vectoriel

Définition

Soit $(E, \underset{E}{+}, \underset{E}{\times})$ *un* $\mathbb{R} -$ *e.v.. On dit que* F *est un sous-espace vectoriel (s.e.v.) de* E *ssi :*

- $F \subset E$
- $F \neq \emptyset$
- $\forall (\alpha, \beta) \in \mathbb{R}^2,\ \forall (u, v) \in F^2, \quad \alpha \underset{E}{\times} u \underset{E}{+} \beta \underset{E}{\times} v \in F,$

i.e. F, non vide et inclus dans E est un s.e.v. de E si et seulement si il est **stable par combinaison linéaire**.

Exemple :

Fixons $E = \mathbb{R}^2$, et montrez que $F = \{(x, y) \in \mathbb{R}^2 / x + 2y = 0\}$ est un sous espace vectoriel de $\mathbb{R}^2$.

Proposition

Soit $(F_i)_{i=1,\dots,p}$ une famille de sous-espaces vectoriels de E, alors l'intersection $\cap_{i=1,\dots,p} F_i$ est un sous espace vectoriel de E.

Exemple : Considerons $F = \{(x,y,z)/x + 2y - z = 0\}$ et $G = \{(x,y,z)/x = y\}$.
Montrez que F et G sont deux sous espaces vectoriels de $\mathbb{R}^3$ et trouvez un vecteur u de $F \cap G$. Montrez que tout les éléments de $F \cap G$ peuvent se réécrire comme λu, $\lambda \in \mathbb{R}$.

Sous-espace vectoriel engendré

Définition

Soit E un $\mathbb{K}-$ e.v. et A une partie quelconque de E. L'intersection de tous les s.e.v. de E contenant A est le plus petit (au sens de l'inclusion) s.e.v. de E contenant A. On l'appelle ***s.e.v. engendré par*** *A et noté $Vect(A)$.*

Proposition

Soit E un $\mathbb{K}-$ e.v. et $A \subset E$

1) *Si $A = \emptyset$ alors $Vect(A) = \{0_E\}$.*
2) *Si A est un s.e.v. de E alors $Vect(A) = A$.*

Théorème

Si on note M l'ensemble des combinaisons linéaires associées à la famille $(x_i)_{i\in I}$ d'éléments de E, alors :

$$M = Vect\left(\cup_{i\in I}\{x_i\}\right)$$

Somme de sous-espaces vectoriels

L'union de deux s.e.v. n'est pas un s.e.v. Dans $\mathbb{R}^2$: $F = \{(x, y)/x = y\}$ et $G = \{(x, y)/x + y = 0\}$, montrez que $(1, 1) \in F \cup G$, $(1, -1) \in F \cup G$ mais $(2, 0) \notin F \cup G$.

Définition

Soient F et G deux sous espaces vectoriels de E, on définit $F + G$ par :

$$F + G = \left\{ x \in E, \quad \exists (f, g) \in F \times G : \ x = f \underset{E}{+} g \right\}.$$

- *$(F_i)_{i=1,\ldots,p}$ sont en* ***somme directe*** *quand $\forall i \in \{2, \ldots, p\}$, $F_i \cap \left[\sum_{k=1,\ldots,i-1} F_k\right] = \{0_E\}$, ce qu'on note $\oplus_{i=1,\ldots,p} F_i$.*
- *F et G sont des sous espaces* ***supplémentaires*** *quand $F \oplus G = E$.*

Proposition

Soient F et G deux s.e.v. de E, on a $F + G = Vect(F \cup G)$.

Somme de sous-espaces vectoriels

Proposition

$E = \oplus_{i=1,\ldots,p} F_i$ si et seulement si $\forall x \in E$, $\exists! (x_1, \ldots, x_p) \in F_1 \times \cdots \times F_p$ tel que $x = x_1 \underset{E}{+} \ldots \underset{E}{+} x_p$.

Famille libre, famille génératrice

Définition (Famille libre)

Soit $(x_1, \dots, x_k)$ *des vecteurs de* E*. On dit que* $(x_1, \dots, x_k)$ *est une* ***famille libre*** *de* E *si et seulement si pour toute combinaison linéaire associée à* $(\lambda_1, \dots, \lambda_k) \in \mathbb{R}^k$ *telle que* $\sum_{j=1}^{k} \alpha_j \underset{E}{\times} x_j = 0_E$ *alors* $\alpha_j = 0$ *pour tout* $j = 1, \dots k$*.*

Définition (Famille génératrice)

Soit $(x_1, \dots, x_k)$ *des vecteurs de* E*, on dit que* $(x_1, \dots, x_k)$ ***génère*** E *si tout vecteur* $x \in E$ *peut etre exprimé comme une combinaison linéaire de* $(x_1, \dots, x_k)$*, i.e. il existe* $(\alpha_1, \dots, \alpha_k) \in \mathbb{R}^k$ *tels que*

$$x = \sum_{j=1}^{k} \alpha_j \underset{E}{\times} x_j$$

Famille génératrice, base

Définition

$(x^1, \cdots, x^k)$ *est une* ***famille génératrice*** *pour* E *si et seulement si* $Vect\left(\cup_{i \in I}\{x_i\}\right) = E$.

Définition

Une famille $(x_1, \cdots, x_k)$ *est une* ***base*** *de* E *si et seulement si c'est une famille libre et génératrice de* E.

- Toute sous famille d'une famille libre est libre
- Toute sur famille d'une famille génératrice est génératrice
- Toute sur famille d'une famille liée est liée.

Proposition (Décomposition unique)

Une famille $(x_1, \cdots, x_k)$ *est une base de l'espace vectoriel* E *si et seulement si chaque vecteur* $x \in E$ *peut être décomposé de manière unique comme une combinaison linéaire de* $(x^1, \cdots, x^k)$. *On a alors :*

$$x = \sum_{j=1}^{k} \alpha_j \underset{E}{\times} x_j$$

Les (α_j) *sont appellés les coordonnées de* x *dans la base* $(x_1, \cdots, x_k)$.

Dimension

Définition

Un espace vectoriel E est de dimension finie si et seulement si il admet au moins une famille génératrice de cardinal fini. On appelle ce nombre la dimension de $dim(E)$.

Proposition

Si E admet une famille génératrice finie de cardinal n alors toute famille libre de E est finie et de cardinal inférieur ou égal à n. De plus, on peut échanger des vecteurs de la famille génératrice avec les vecteurs de la famille libre pour obtenir une nouvelle famille génératrice pour E.

Proposition (Théorème de la base incomplète)

Soit E un espace vectoriel de dimension finie, $\mathcal{L} = (x_i)_{i \in I}$ une famille libre et $\mathcal{G} = (y_i)_{i \in J}$ génératrice finie. Alors il existe un ensemble K tel que $K \subset J$ telle que $(\mathcal{L}, (y_i)_{i \in K})$ soit une base de E.

Dimension

Proposition

Soit E un espace vectoriel de dimension finie. Tout sous-espace vectoriel F admet au moins un suppplémentaire dans E. De plus, pour tout supplementaire S on a $dim(F) + dim(S) = dim(E)$.

Proposition

Soit E un espace vectoriel de dimension finie, F et G deux sous-espaces vectoriels de E. Alors $F + G$ et $F \cap G$ sont également de dimension finie, et on a $dim(F + G) = dim(F) + dim(G) - dim(F \cap G)$.

Application linéaire : Définition

Définition

Soient (E, F) deux $\mathbb{R}-$espaces vectoriels. ***Une application*** $f : E \to F$ ***est linéaire*** *si et seulement si*

i)
$$\forall (u, v) \in E^2 \qquad f(u \underset{E}{+} v) = f(u) \underset{F}{+} f(v)$$

ii)
$$\forall \alpha \in \mathbb{R}, \quad \forall u \in E, \quad f(\alpha \underset{E}{\times} u) = \alpha \underset{F}{\times} f(u).$$

L'ensemble des applications linéaires de E dans F est noté $\mathcal{L}(E, F)$.
Une application linéaire de E dans E est appellée un ***endomorphisme****.*

Théorème

Soit $(e_i)_{i \in I}$ une base de E, alors f est déterminée entièrement par la donnée de $(f(e_i))_{i \in I}$.

Le noyau et l'image d'une application linéaire

Définition

i) *Soit f une application linéaire de E dans F. On appelle **noyau** de f l'ensemble des vecteurs $u \in E$ tels que $f(u) = 0$, i.e.*

$$Ker(f) = \{u \in E / f(u) = 0_F\}$$

ii) *On appelle l'image de f, l'ensemble des vecteurs $v \in F$ tels que*

$$Im(f) = \{v \in F / \exists u \in E, \quad v = f(u)\}$$

Proposition

$Ker(f)$ et $Im(f)$ sont respectivement des sous espaces vectoriels de E et de F.

Proposition

Si E et F sont de dimensions finies alors E et F sont isomorphes si et seulement si $dim(E) = dim(F)$.

Exemple : Soit f une application de $\mathbb{R}^2$ dans $\mathbb{R}^3$, définie par :

$$f(x_1, x_2) = \begin{pmatrix} x_1 - x_2 \\ x_1 + 2x_2 \\ x_1 + 2x_2 \end{pmatrix}$$

Montrer que f est linéaire. Donner $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

Théorème

Soit $f : E_1 \to E_2$ une application linéaire, où E_1 et E_2 sont de dimension finie.

1) *f est **injective** si et seulement si $Ker(f) = \{0_{E_1}\}$.*
2) *f est **surjective** si et seulement si $Im(f) = E_2$.*
3) *f est **bijective** si elle est injective et surjective, i.e. si $Ker(f) = \{0_{E_1}\}$ et $Im(f) = E_2$.*
4) ***Théorème du rang** : $dim(Ker(f)) + dim(Im(f)) = dim(E_1)$*

Si $Im(f)$ est de dimension finie r, alors on dit que le rang de f, noté $Rg(f)$ est égal à r.

Proposition

Si E et F sont de dimensions finies alors :

- $Rg(g \circ f) \leq Min(Rg(f), Rg(g))$
- *si f est surjective alors* $Rg(g \circ f) = Rg(g)$
- *si g est injective alors* $Rg(g \circ f) = Rg(f)$

Proposition

- *Si E est de dimension finie alors f est injective si et seulement si* $Rg(f) = Dim(E)$
- *Si F est de dimension finie alors f est surjective si et seulement si* $Rg(f) = Dim(F)$

Les projecteurs linéaires

Définition

Soient H et S deux sous-espaces vectoriels de E tels que $E = H \oplus S$:
$\forall x \in E, \quad \exists!(x_H, x_S) \in H \times S, x = x_H + x_S$. *L'application p_H définie par*

$$\begin{aligned} p_H : E &\to E \\ x &\mapsto x_H, \end{aligned}$$

est appellée projecteur linéaire sur H parallèlement à S.

Les projecteurs linéaires

Proposition

Si p_H *est le projecteur linéaire sur* H *parallèlement à* S*, alors*

- $p_H \in \mathcal{L}(E)$
- $Im(p_H) = H$ *et* $Ker(p_H) = S$.

Proposition

Soit $p \in \mathcal{L}(E)$, $p \circ p = p$ *si et seulement si* p *est un projecteur linéaire sur* $Im(p)$ *parallèlement à* $Ker(p)$.

Exo : à montrer.

Matrice représentative d'une application linéaire

Soit $\mathcal{U} = (u_1, \ldots, u_p)$ une base de E et $\mathcal{V} = (v_1, \ldots, v_n)$ une base de F.
Alors f est entièrement définie par l'image des vecteurs de la base $\mathcal{U}$: $(f(u_1), \ldots, f(u_p))$.

On note par $\begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{pmatrix}$ les composantes de $f(u_i)$ sur la base $(v_1, \ldots, v_n)$.

Définition

On appelle matrice représentative de f sur $\mathcal{U}, \mathcal{V}$ la matrice de taille $n \times p$, notée $\mathcal{M}_{\mathcal{U},\mathcal{V}}(f)$ ou $\mathcal{M}at(f, \mathcal{U}, \mathcal{V})$ contenant en colonne les composantes des $f(u_i)$ dans la base $(v_1, \ldots, v_n)$.

Théorème

L'application $f \mapsto Mat(f, \mathcal{U}, \mathcal{V})$ est un isomorphisme de $\mathcal{L}(E, F)$ dans $\mathcal{M}_{n,p}(\mathbb{R})$.

Exemple :
Soit f une application linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^3$, définie par :

$$f(x_1, x_2) = \begin{pmatrix} x_1 - x_2 \\ x_1 + 2x_2 \\ x_1 + 2x_2 \end{pmatrix}$$

Matrice de f dans les bases canoniques de $\mathbb{R}^2$ et $\mathbb{R}^3$?

Proposition

Soit f une application linéaire de E dans F, et g une application linéaire de F dans G.

1) *Quelque soit $x \in E$, de composantes $\begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ dans $\mathcal{U} = (u_1, \ldots, u_p)$, les composantes de $f(x)$ dans $\mathcal{V} = (v_1, \ldots, v_n)$ sont données par*

$$\mathcal{M}_{\mathcal{U},\mathcal{V}}(f) \times \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$$

2) *Soient $\mathcal{U}$, $\mathcal{V}$ et $\mathcal{W}$ une base de E, et respectivement de F, G. Alors :*

$$\mathcal{M}_{\mathcal{U},\mathcal{W}}(g \circ f) = \mathcal{M}_{\mathcal{V},\mathcal{W}}(g) \times \mathcal{M}_{\mathcal{U},\mathcal{V}}(f)$$

Endomorphismes

Proposition

La matrice A associée à une application linéaire f est inversible si et seulement si f est bijective. Alors, la matrice de f^{-1} est A^{-1}. Si la matrice A est inversible, alors ses colonnes sont linéairement indépendantes.

Notation : on note $GL_n(\mathbb{R})$ l'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{R})$.

Matrice de passage, matrices equivalentes

Définition

Soient $\mathcal{U}$ *et* $\mathcal{V}$ *deux bases de E. On appelle* ***matrice de passage*** $P_{\mathcal{V},\mathcal{U}}$ *de* $\mathcal{U}$ *dans* $\mathcal{V}$*, la matrice contenant les colonnes de* $\mathcal{V}$ *(nouvelle base) dans* $\mathcal{U}$ *(ancienne base).*
C'est à dire : $P_{\mathcal{V},\mathcal{U}} = \mathcal{M}_{\mathcal{V},\mathcal{U}}(id_E)$.

Définition

Soient $A \in \mathcal{M}_{n,p}(\mathbb{R})$ *et* $\widetilde{A} \in \mathcal{M}_{n,p}(\mathbb{R})$*.* A *et* $\widetilde{A}$ *sont dites équivalentes ssi il existe* $(P, Q) \in GL_p(\mathbb{R}) \times GL_n(\mathbb{R})$ *telles que :*

$$\widetilde{A} = Q^{-1}AP.$$

Matrice de passage

Soit x un vecteur de E dont les coordonnées dans $\mathcal{U}$ sont données par $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et les coordonnées dans $\mathcal{V}$ sont données par $X' = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$.
Alors

$$X = P_{\mathcal{V},\mathcal{U}} X'.$$

Si f est un endomorphisme de E, la matrice $M_{\mathcal{U}}$ de f dans $\mathcal{U}$, et la matrice $M_{\mathcal{V}}$ de f dans $\mathcal{V}$ satisfont :

$$M_{\mathcal{V}} = P_{\mathcal{V},\mathcal{U}}^{-1} \times M_{\mathcal{U}} \times P_{\mathcal{V},\mathcal{U}}.$$