Algèbre linéaire I

D. HÄFNER

22 juin 2017

Chapitre 1

Groupes, anneaux, corps

1.1 Lois de composition interne

1.1.1 Définition

Définition 1.1.1 (Loi de composition interne) *Soit E un ensemble. On appelle loi de composition interne (en abrégé l.c.i.) dans E une application*

$$* : \begin{array}{c} E \times E \to E \\ (a,b) \mapsto a * b. \end{array}$$

Exemple 1.1.1 *i)*

$$\times : \begin{array}{c} \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ (a,b) \mapsto a \times b. \end{array}$$

ii)

$$+ : \begin{array}{c} \mathbb{R} \times \mathbb{R} \to \mathbb{R} \\ (a,b) \mapsto a + b. \end{array}$$

iii) Soit E un ensemble et E^E l'ensemble des applications de E dans E. Alors on a la loi interne

$$\circ : \begin{array}{c} E^E \times E^E \to E^E \\ (f,g) \mapsto f \circ g. \end{array}$$

Définition 1.1.2 *Une partie F de E est stable par la l.c.i., si :*

$$\forall (a,b) \in F^2 \quad a * b \in F.$$

Exemple 1.1.2 *i) La partie $\mathbb{R}_-$ de $\mathbb{R}$ est stable par $+$.*

ii) La partie $\mathbb{R}_+$ de $\mathbb{R}$ est stable par $\times$.

iii) La partie $\mathbb{R}_-$ n'est pas stable par $\times$.

1.1.2 Propriétés élémentaires

Définition 1.1.3 *Soit E un ensemble et $*$ une l.c.i. dans E.*

i) On dit que la loi est commutative si

$$\forall (a,b) \in E^2 \quad a * b = b * a.$$

ii) On dit que la loi est associative si

$$\forall (a,b,c) \in E^3 \quad a * (b * c) = (a * b) * c.$$

iii) On dit que $e \in E$ est un élément neutre si

$$\forall a \in E \quad a * e = e * a = a.$$

iv) Si E possède un élément neutre pour la loi $*$, un élément a de E est dit symétrisable s'il existe un élément $a' \in E$ tel que

$$a * a' = a' * a = e.$$

a' est appelé symétrique de a.

Remarque 1.1.1 *Si $*$ est associative, on peut écrire sans ambigu¨ıté $a * b * c$.*

Proposition 1.1.1 *Soit E un ensemble et $*$ une l.c.i. sur E.*

i) Il existe au plus un élément neutre dans E.

ii) Si E possède un élément neutre et si la l.c.i. est associative, chaque élément de E possède au plus un symétrique.

Preuve

i) S'il existait deux éléments neutres e et f, on aurait
$f * e = f$, car e est neutre,
$f * e = e$, car f est neutre. Donc $e = f$.

ii) Si un élément a possède deux symétriques a' et a'', on a :

$$a'' * a * a' = (a'' * a) * a' = e * a' = a', \quad a'' * a * a' = a'' * (a * a') = a'' * e = a'',$$

donc $a' = a''$.

□

Notations

Le plus souvent, une l.c.i. associative est notée de façon additive : $a + b$ ou multiplicative : ab. La notation additive n'est employée que pour une l.c.i. commutative. Aussi on va noter dans la suite a^{-1} le symétrique de a.

1.2 Groupes

1.2.1 Définition de base

Définition 1.2.1 (Groupe) *On appelle groupe un ensemble G muni d'une loi de composition interne $*$ telle que*

(G1) $*$ *est associative :* $\forall (a,b,c) \in G^3 \quad a*(b*c) = (a*b)*c$.

(G2) G possède un élément neutre e : $\forall a \in G \quad a*e = e*a = a$.

(G3) Tous les éléments de G sont symétrisables :

$$\forall a \in G,\ \exists a' \in G \quad a*a' = a'*a = e.$$

Si de plus $*$ est commutative, le groupe est dit commutatif ou abélien.

Remarque 1.2.1 (historique) *La notion de groupe a été introduite par Evariste Galois (1811-1832).*

Exemple 1.2.1 *i)* $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$.

ii) $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$.

iii) $(\mathcal{S}(E),\circ)$, *où E est un ensemble et $\mathcal{S}(E)$ est l'ensemble des bijections de E dans E. En particulier si $E = \mathbb{N}_n = \{1,...,n\}$ on appelle $\mathcal{S}_n := \mathcal{S}(\mathbb{N}_n)$ le groupe de permutations sur n éléments.*

Exercice 1.2.1 *Vérifier que les exemples ci-dessus forment effectivement des groupes.*

Prorpiétés

i) Un groupe est non vide : il contient au moins son élément neutre.

ii) L'élément neutre est unique.

iii) Le symétrique d'un élément est unique.

iv) Pour tout élément a de G,

$$ax = ay \Rightarrow x = y.$$

(il suffit de miltiplier à gauche par a^{-1}). De même

$$xa = ya \Rightarrow x = y.$$

(Multiplication à droite par a^{-1}.)

v) Pour tout $(a,b) \in G^2$, l'équation $ax = b$ a une solution unique $x = a^{-1}b$. De même l'équation $xa = b$ a une solution unique : $x = ba^{-1}$.

vi) $\forall (a,b) \in G^2 \quad (ab)^{-1} = b^{-1}a^{-1}$.

1.2.2 Sous-groupes

Définition 1.2.2 *Soit G un groupe. On dit qu'un sous-ensemble H de G est un sous-groupe de G lorsque les trois conditions suivantes sont vérifiées :*

i) L'ensemble H n'est pas vide.

ii) Pour tous a et b de H, le produit ab est aussi dans H.

iii) Pour tout a de H, l'inverse a^{-1} est aussi dans H.

Proposition 1.2.1 *Soit G un groupe. Un sous-ensemble de H de G est un sous-groupe de G ssi les deux conditions suivantes sont vérifiées :*

i) L'ensemble H n'est pas vide.

iv) Pour tous a et b de H, le produit ab^{-1} est aussi dans H.

Preuve

- Supposons d'abord que H est un sous-groupe de G, c. à.d. qu'il vérfie $i)$ $ii)$ et $iii)$. Il faut alors montrer que $iv)$ est vérifiée. Soient $a, b \in H$. Par $iii)$ on sait que $b^{-1} \in H$. On applique alors $ii)$ à a et b^{-1} et on trouve $ab^{-1} \in H$.
- Supposons maintenant que H vérifie $i)$ et $iv)$. Il faut montrer que H vérifie $ii)$ et $iii)$. On va montrer préalablement que $e \in H$. Comme H n'est pas vide il contient un élément c et on peut appliquer $iv)$ pour trouver que $cc^{-1} = e \in H$. Montrons maintenant que H vérifie $iii)$. Soit $a \in H$. On a alors $a^{-1} = ea^{-1} \in H$. Montrons finalement que H vérifie $ii)$. Soit $a, b \in H$. Par $iii)$ (déjà montré) on sait que $b^{-1} \in H$. Donc par $iv)$ $ab = a(b^{-1})^{-1} \in H$.

□

Remarque 1.2.2 *En pratique on va appliquer le plus souvent la proposition pour montrer qu'un sous-ensemble H est en fait un sous-groupe.*

Proposition 1.2.2 *Soit G un groupe et H un sous-groupe de G. La restriction à H de la loi de composition sur G fait de H un groupe.*

Preuve

Il faut d'abord vérifier que H est stable par la loi de composition interne de G ce qui est assuré par $ii)$. L'associativité de cette restriction est évidente. Dans la preuve de la proposition précédente nous avons montré en passage que le neutre de G est un élément de H. Il est évidemment neutre pour la loi de composition interne restreinte à H. Enfin $iii)$ garantit que le symétrique de chaque élément de H est un élément de H. □

Exercice 1.2.2 *Montrer les assertions suivantes.*

i) Soit G un groupe. $\{e\}$ et G sont des sous-groupes de G.

ii) L'intersection de deux sous-groupes de G est un sous-groupe de G.

iii) $\mathcal{U} = \{z \in \mathbb{C};\ |z| = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

iv) $\mathcal{U}_n = \{z \in \mathbb{C};\ z^n = 1\}$ est un sous-groupe de $(\mathcal{U}, \times)$.

1.2.3 Morphismes de groupes

Définition 1.2.3 *Soient $(G,*)$ et $(G',\times)$ deux groupes. On dit que $f : G \to G'$ est un morphisme de groupes si*

$$\forall (x,y) \in G^2 \quad f(x*y) = f(x) \times f(y).$$

Exemple 1.2.2

$$\begin{array}{rcl} (\mathbb{Z},+) & \to & (\mathbb{R}_+^*,\times) \\ n & \mapsto & 2^n \end{array}$$

$$\begin{array}{rcl} (\mathbb{R}_+,\times) & \to & (\mathbb{R},+) \\ x & \mapsto & \ln x \end{array}$$

$$\begin{array}{rcl} (\mathbb{C},\times) & \to & (\mathbb{C},\times) \\ z & \mapsto & \overline{z} \end{array}$$

Exercice 1.2.3 *Vérifier que les applications ci-dessus sont effectivement des morphismes de groupe.*

Proposition 1.2.3 *Soit G et G' deux groupes d'éléments neutres respectifs e et e', et $f : G \to G'$ un morphisme. Alors on a*

$$f(e) = e' \tag{1.2.1}$$

$$\forall x \in G,\ f(x^{-1}) = (f(x))^{-1}. \tag{1.2.2}$$

Preuve

(1.2.1). On a $f(e) = f(ee) = f(e)f(e)$ et $f(e) = f(e)e'$, d'où $f(e)f(e) = f(e)e'$. Multiplication à gauche avec $(f(e))^{-1}$ donne le résultat.

(1.2.2). En effet $f(xx^{-1}) = f(x)f(x^{-1})$ et $f(xx^{-1}) = f(e) = e'$, d'où $f(x)f(x^{-1}) = e'$. Multiplication à gauche avec $(f(x))^{-1}$ donne le résultat. □

1.2.4 Noyau d'un morphisme de groupes

Soit G et G' deux groupes d'éléments neutres respectifs e et e', et $f : G \to G'$ un morphisme de groupes.

Définition 1.2.4 *On appelle noyau de f l'ensemble des éléments de G qui ont pour image l'élément neutre de G'. On le note*

$$\mathrm{Ker}\, f = \{x \in G;\ f(x) = e'\} = f^{-1}(\{e'\}).$$

Proposition 1.2.4 *i)* $\mathrm{Ker}\, f$ *est un sous-groupe de G.*

ii) $\mathrm{Ker}\, f = \{e\}$ *ssi f est injectif.*

Preuve

i) On vérifie les conditions i) et iv) de la Proposition 1.2.1. Ker f n'est pas vide puisque $f(e) = e'$. Ensuite soient $x, y \in \text{Ker}\, f$. On calcule $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = e'(e')^{-1} = e'e' = e'$.

ii) Soit f injectif. Clairement $\{e\} \subset \text{Ker}\, f$. Soit maintenant $x \in \text{Ker}\, f$. On a $f(x) = e' = f(e)$. f étant injectif on trouve $x = e$.
Soit maintenant $\text{Ker}\, f = \{e\}$. Soient $x, y \in G$. Si $f(x) = f(y)$, alors multiplication à droite par $f(x)^{-1}$ donne
$e' = (f(x))^{-1}f(y) = f(x^{-1})f(y) = f(x^{-1}y)$,
c.à.d. $x^{-1}y \in \text{Ker}\, f$. Comme $\text{Ker}\, f = \{e\}$ on trouve $x = y$.

□

Exemple 1.2.3 *L'application*

$$f : \begin{array}{ccc} (\mathbb{R}_+, +) & \to & (\mathbb{C}^*, \times) \\ x & \mapsto & e^{ix} \end{array}$$

est un morphisme de groupes, dont le noyau est

$$\text{Ker}\, f = \{x \in \mathbb{R};\, e^{ix} = 1\} = 2\pi\mathbb{Z},$$

sous-groupe de $(\mathbb{R}, +)$.

1.2.5 Image d'un morphisme de groupes

Soient G et G' deux groupes d'éléments neutres e et e', et $f : G \to G'$ un morphisme de groupes.

Définition 1.2.5 *On appelle image de f l'ensemble des éléments de G' qui ont un antécédent dans G. On la note*

$$\text{Im}f = \{y \in G';\, \exists x \in G\, y = f(x)\} = f(G).$$

Proposition 1.2.5 *i)* Imf *est un sous-groupe de* G'.
ii) Im$f = G'$ *ssi* f *est surjectif.*

Preuve

i) De nouveau on vérifie i) et iv) de la Proposition 1.2.1. Imf est non vide puisque $e' = f(e) \in \text{Im}f$. Soient $f(x)$, $f(y) \in$ Imf. Alors $f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in$ Imf.

ii) $f(G) = G'$ est la définition même de la surjectivité de f.

□

Exemple 1.2.4 *L'image du morphisme*

$$f : \begin{array}{ccc} (\mathbb{R}_+, +) & \to & (\mathbb{C}^*, \times) \\ x & \mapsto & e^{ix} \end{array}$$

est Im$f = \mathcal{U} = \{z \in \mathbb{C};\, |z| = 1\}$, *qui est un sous-groupe de* $(\mathbb{C}^*, \times)$.

1.3 Anneaux et corps

1.3.1 Anneaux

Définition 1.3.1 *On appelle anneau un ensemble A muni de deux l.c.i., notées respectivement $+$ et $\times$, telles que*

(A1) $(A,+)$ est un groupe abélien. Le neutre est noté 0_A (élément nul).

(A2) La l.c.i. $\times$ est associative.

(A3) A possède un élément neutre pour le l.c.i. $\times$, notée $\mathbb{1}_A$ (élément unité).

(A4) $\times$ est distributive par rapport à $+$, c.à.d.

$$\forall (a,b,c) \in A^3 \quad a(b+c) = ab + ac \quad et \quad (b+c)a = ba + ca.$$

Si de plus $\times$ est commutatif, l'anneau est dit commutatif.

Exemple 1.3.1 *i)* $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$
ii) $(\mathbb{R}^{\mathbb{N}},+,\times)$, $(\mathbb{R}^{\mathbb{R}},+,\times)$.

Propriétés
- On peut définir dans un anneau une l.c.i., notée $-$, par

$$\forall (a,b) \in A^2 \quad a - b := a + (-b).$$

- $\forall a \in A \quad a0_A = 0_A a = 0_A$. En effet $a0_A = a(0_A + 0_A) = a0_A + a0_A \Rightarrow a0_A = 0_A$.
- La réciproque n'est pas toujours vraie : on appelle diviseurs de zéro des éléments non nuls dont le produit est 0_A.

Exemple 1.3.2 *Dans l'anneau $\mathbb{R}^{\mathbb{R}}$, les fonctions $f : x \mapsto x + |x|$ et $g : x \mapsto x - |x|$ sont des diviseurs de zéro, car fg est la fonction nulle, alors que ni f ni g ne sont nulles.*

1.3.2 Anneau des entiers relatifs

Multiples et diviseurs d'un entier

Soit $(a,b) \in \mathbb{Z}^2$; s'il existe $n \in \mathbb{Z}$ tel que $a = nb$, on dit que :
- a est un miltiple de b.
- b est un diviseur de a (ou "b divise a, notation $b|a$).

L'ensemble des multiples de b est noté $b\mathbb{Z}$.

Propriétés
- La somme de deux multiples de b est un multiple de b.
- L'opposé d'un multiple de b est un multiple de b.
- Tout multiple d'un multiple de b est un miltiple de b.
- Si b divise deux entiers, il divise leur somme.
- Tout diviseur d'un diviseur de a est un diviseur de a.
- 0 est un multiple de tout entier. Tout entier divise 0.
- Si b divise a et a divise b, alors $a = \pm b$.

Exercice 1.3.1 *Montrer les propriétés ci-dessus.*

Théorème 1.3.1 (Division euclidienne dans $\mathbb{Z}$) *Soit $(a,b) \in \mathbb{Z}^2$ tel que $b \neq 0$. Il existe un couple unique $(q,r) \in \mathbb{Z}^2$ tel que*

$$a = bq + r \quad et \quad 0 \leq r < |b|.$$

q est appelé quotient et r reste de la division euclidienne de a par b.

Preuve

- Existence : L'ensemble E des multiples de b inférieus ou gaux à a est une partie non vide de $\mathbb{Z}$ majorée par a. E possède donc un plus grand élément que nous noterons bq. Posons $r = a - bq$. $bq \leq a$, donc $r \geq 0$. D'autre part , $bq + |b|$ est un multiple de b supérieur à bq, donc $bq + |b| > a$, d'où $r < |b|$.
- Unicité : Supposons $a = bq + r = bq' + r'$ avec $0 \leq r < |b|$ et $0 \leq r' < |b|$. On a $b(q - q') = r' - r$, $\quad r' - r$ est donc un miltiple de b. Comme il est strictement compris entre $-|b|$ et $|b|$, il ne peut être nul. Donc $r' = r$ et par suite $q' = q$. Le couple (q,r) est donc unique.

□

1.3.3 Corps

Définition 1.3.2 *On appelle corps un anneau, non réduit à $\{0\}$, dont tout élément non nul est inversible.*

Remarque 1.3.1 *i) Dans la suite de ce cours on va toujours supposer que l'anneau dans la définition de corps est commutatif.*

ii) Si $\mathbb{K}$ est un corps, le groupe des éléments inversibles est $\mathbb{K} \setminus \{0\}$.

Exemple 1.3.3 $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.

1.4 Anneaux des polynômes $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Soit $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$. Dans ce cours on va identifier un polynôme $P = \sum_{j=0}^{n} a_j X^j$ à sa fonction polynomiale

$$P : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & \sum_{j=0}^{n} a_j x^j \end{array}$$

Remarque 1.4.1 (importante) *Soit $\mathbb{K}$ un corps. Il existe une différence entre les polynômes $\mathbb{K}[X]$ et leurs fonctions polynomiales associées. En particulier il existe un corps $\mathbb{K}$ et un polynôme non nul tels que la fonction polynomiale associée est nulle. Néanmoins si $\mathbb{K} = \mathbb{C}$ ou $\mathbb{K} = \mathbb{R}$ les deux espaces sont isomorphes au sens des espaces vecoriels (voir Chapitre 2) et nous n'allons pas faire de différence entre les polynômes et leurs fonctions polynomiales associées dans ce cas. Pour plus de détails nous renvoyons au cours d'algèbre du L3.*

Définition 1.4.1 *On appelle degré d'un polynôme non nul $P = \sum_{j=0}^{n} a_j X^j$ le plus grand entier j tel que $a_j \neq 0$. Le coefficient a_n correspondant est appelé coefficient dominant du polynôme P. Si le coefficient dominant est 1, le polynôme est dit unitaire.*

Par convention on dit que le degré du polynôme nul est $-\infty$. On convient que, pour tout $n \in \mathbb{N}$:

$$-\infty < n, \quad (-\infty) + n = n + (-\infty) = -\infty, \quad (-\infty) + (-\infty) = -\infty.$$

1.4.1 Opérations dans $\mathbb{K}[X]$

Sur $\mathbb{K}[X]$ on a deux opérations $+, \times$ donnés par l'addition et la multiplication des fonctions. On obtient

Proposition 1.4.1 *i) Soient $A, B \in \mathbb{K}[X]$. Alors*

$$\deg(A+B) \leq \max\{\deg A, \deg B\}, \quad \deg(AB) = \deg A + \deg B.$$

ii) $(\mathbb{K}[X], +, \times)$ est un anneau commutatif.

Exercice 1.4.1 *Montrer la proposition.*

1.4.2 Divisibilité dans $\mathbb{K}[X]$

Soit $(A, B) \in (\mathbb{K}[X])^2$. S'il existe $C \in \mathbb{K}[X]$ tel que $A = BC$, on dit que
- A est un *multiple* de B.
- B est un diviseur de A (ou "B" divise A", notation $B|A$).

On note $B\mathbb{K}[X]$ l'ensemble des polynômes multiples de B et $D(A)$ l'ensemble des polynômes qui divisent A.

Propriétés
- La somme de deux multiples de B est un multiple de B ;
- l'opposé d'un multiple de B est un multiple de B ;
- tout multiple d'un multiple de B est un multiple de B ;
- si B divise deux polynômes, il divise leur somme ;
- tout diviseur d'un diviseur de A est un diviseur de A ;
- 0 est un multiple de tout polynôme. Tout polynôme divise 0.

Exercice 1.4.2 *Démontrer ces propriétés.*

Théorème 1.4.1 *Soient A et B deux polynômes de $\mathbb{K}[X]$ tels que $B \neq 0$. Il existe un couple unique (Q, R) de polynômes tels que*

$$A = BQ + R \quad \deg R < \deg B.$$

Q est appelé quotient, et R reste de la division euclidienne de A par B.

Preuve

– Existence. Soit p le degré de B. Démontrons par récurrence que pour tout $n \in \mathbb{N}$, il existe un couple (Q, R) pour tout polynôme A de degré strictement inférieur à n.
  – Si $\deg(A) < p$, le couple $(0, A)$ convient : la récurrence est fondée pour tout $n \leq p$.
  – Soit n un entier supérieur ou égal à p tel qu'il existe un couple (Q, R) pour tout polynôme A de degré strictement inférieur à n, et soit A un polynôme de degré n. Posons $A = a_n X^n + ... + a_0$ et $B = b_p X^p + ... + b_0 \quad (b_p \neq 0)$. Soit $Q_1 := \frac{a_n}{b_p} X^{n-p}$. Le monôme dominant de $Q_1 B$ est $a_n X^n$, de sorte que le polynôme $A' = A - Q_1 B$ a un degré strictement inférieur à n. On peut donc lui appliquer l'hypothèse de récurrence :

$$\exists (Q, R) \in \mathbb{K}[X]^2 \quad A' = QB + R \quad \text{avec} \quad \deg R < p$$

$$A - Q_1 B = QB + R, \quad \text{d'où} \quad A = (Q_1 + Q)B + R \quad \text{avec} \quad \deg R < p.$$

  L'existence est établi pour tout polynôme A de degré n donc pour tout polynôme de degré strictement inférieur à $n + 1$.
– Unicité . Supposons $A = BQ + R = BQ' + R'$ avec $\deg R < \deg B$ et $\deg R' < \deg B$. Alors $\deg(R - R') \leq \max(\deg R, \deg R') < \deg B$. Or $R - R' = B(Q' - Q)$. D'où $\deg(Q' - Q) < 0$, ce qui signifie que $Q' - Q = 0$. On en déduit $Q = Q'$ et $R = R'$.

□

1.4.3 Racines d'un polynôme

Définition 1.4.2 *Soit $\mathbb{K} = \mathbb{C}$ ou $\mathbb{K} = \mathbb{R}$. On appelle racine de P (ou zéro) tout élément $a \in \mathbb{K}$ tel que $P(a) = 0$. Un polynôme $P \in \mathbb{K}[X]$ est dit scindé s'il est produit de polynômes de degré 1.*

Proposition 1.4.2 *Soit $P \in \mathbb{K}[X]$. Un élément $a \in \mathbb{K}$ est une racine de P ssi $(x - a)$ divise P.*

Preuve

Effectuons la division euclidienne de P par $(X - a)$.

$$P = (X - a)Q + R, \quad \deg R < 1.$$

Le polynôme P est donc constant. En remplaçant X par a, on obtient $R = P(a)$. On en déduit que P est divisible par $(X - a)$ ssi $P(a) = 0$. □

Corollaire 1.4.1 *Un polynôme de degré $n \geq 0$ possède au plus n racines.*

Preuve

Soit P un polynôme de degré n. Supposons que P possède $(n + 1)$ racines distinctes $a_1, ..., a_{n+1}$. D'après la proposition P est divisible par $(X - a_1)$: $P(X) = (X - a_1)Q_1(X)$. $P(a_2) = (a_2 - a_1)Q_1(a_2)$, d'où $Q_1(a_2) = 0$. On en déduit que Q_1 est divisible par $(X - a_2)$: $Q_1(X) = (X - a_2)Q_2(X)$, d'où $P(X) = (X - a_1)(X - a_2)Q_2(X)$: P est divisible par $(X - a_1)(X - a_2)$. Par récurrence on montre facilement que P est divisible par le produit $(X - a_1)(X - a_2)...(X - a_{n+1})$, qui est de degré $(n + 1)$: contradiction. Donc P a, au plus, n racines distinctes.

□

Définition 1.4.3 *On appelle ordre de multiplicité de la racine a, le plus grand entier m tel que P soit divisible par $(X-a)^m$. On appelle racine double une racine d'ordre 2, racine triple une racine d'ordre 3, etc.*

1.4.4 Factorisation dans $\mathbb{K}[X]$

Factorisation dans $\mathbb{C}[X]$

Théorème 1.4.2 (Théorème de d'Alembert-Gauss) *Tout polynôme non constant de $\mathbb{C}[X]$ possède au moins une racine.*

Démonstration dans le cours "analyse complexe" (M1).

Corollaire 1.4.2 *i) Tout polynôme non constant de $\mathbb{C}[X]$ est un produit de polynômes de degré 1.*

ii) Tout polynôme de degré $n \geq 0$ de $\mathbb{C}[X]$ possède exactement n racines comptées avec leur ordre de multiplicité.

Preuve

i) Raisonnons par récurrence sur le degré de P. Si P est de degré 1, le résultat est trivial. Soit $n \in \mathbb{N}^*$ tel que tout polynôme de degré n soit un produit de polynômes de degré 1 et soit P un polynôme de degré $n+1$. P n'étant pas constant, il possède d'après le théorème de de d'Alembert Gauss une racine a : il est donc divisible par $(X-a)$: $P(X) = (X-a)Q(X)$. Le polynôme Q est de degré n : d'après l'hypothèse de récurrence, c'est un produit de polynômes de degré 1. P est donc aussi un produit de polynômes de degré 1.

ii) P est donc de la forme

$$P = \lambda(X-a_1)^{m_1}(X-a_2)^{m_2}...(X-a_p)^{m_p} \quad \text{avec } \sum_{k=1}^{p} m_k = n,\ \lambda \in \mathbb{C},$$

$a_1, a_2, ..., a_p$ étant des complexes distincts 2 à 2. P a donc n racines, à condition que chaque racine a_k soit comptée m_k fois.

□

Factorisation dans $\mathbb{R}[X]$

Soit P un polynôme d'ordre $n \geq 0$ de $\mathbb{R}[X]$. P possède n racines complexes, comptées avec leur multiplicité. Si z est une racine d'ordre m :

$$P(z) = P'(z) = ... = P^{(m-1)}(z) = 0 \quad P^{(m)}(z) \neq 0.$$

En prenant le complexe conjugué on obtient :

$$P(\overline{z}) = P'(\overline{z}) = ... = P^{(m-1)}(\overline{z}) = 0 \quad P^{(m)}(\overline{z}) \neq 0.$$

$\overline{z}$ est donc aussi racine de P, avec le même ordre de multiplicité que z. Les racines de P sont donc

– soit réelles,
– soit non réelles conjugués deux à deux, avec le même ordre de multiplicité.

Dans la décomposition en produit de facteurs irréductibles de P dans $\mathbb{C}[X]$, regroupons les facteurs correspondant à deux racines non rélles conjuguées :

$$(X-z)^m(X-\overline{z})^m = (X^2+bX+c)^m \quad b=-2\mathrm{Re}(z),\ c=|z|^2.$$

On obtient un polynôme de degré 2 à coeffcients réels, irréductible dans $\mathbb{R}[X]$. Son discriminant b^2-4c est strictement négatif. Le polynôme P peut donc se décomposer dans $\mathbb{R}[X]$ sous la forme

$$P = \lambda(X-a_1)^{m_1}...(X-a_p)^{m_p}(X^2+b_1X+c_1)^{n_1}...(X^2+b_qX+c_q)^{n_q},$$

où $(a_j)_{1\leq j\ p}$ sont les racines réelles de P, et $(X^2+b_j+c_j)_{1\leq j\leq q}$ des trinômes réels à discriminant strictement négatif. Résumé :

Théorème 1.4.3 *Tout polyôme de $\mathbb{R}[X]$ est un produit :*
– *de polynômes de degré 1 ;*
– *de polynômes de degré 2 à discriminant strictement négatif.*

Corollaire 1.4.3 *Tout polynôme de degré impair de $\mathbb{R}[X]$ possède au moins une racine réelle.*

1.5 Quelques conseils pratiques

– Pour montrer qu'un ensemble E muni d'une l.c.i. est un groupe :
  – s'il s'agit d'une loi tout à fait nouvelle, il faut vérifier :
    – qu'elle est associative ;
    – qu'il existe un élément neutre ;
    – que tout élément possède un symétrique.
  – s'il s'agit de la restrcition à E de la l.c.i. d'un groupe G contenant E, il suffit de vérifier que E est un sous-groupe de G (voir ci-après).
– Pour montrer qu'une partie H d'un groupe G est un sous-groupe de G, on peut
  – utiliser la définition ;
  – appliquer la caractérisation :
    – H est non vide (on a un intérêt à montrer tout de suite que $e\in H$).
    – Si $a,b\in H$, alors $ab^{-1}\in H$.
  – montrer que c'est une intersection de sous-groupes ;
  – montrer que c'est le sous-groupe engendré par un élément ;
  – montrer que H est le noyau d'un morphisme de groupes ;
  – montrer que H est l'image d'un morphisme de groupe.
– Soient A et B deux polynômes. Pour montrer que B divise A, on peut
  – montrer que le reste de la division euclidienne de A par B est nul ;
  – si B est scindé, montrer que toute racine d'ordre m de B est une racine d'ordre $m'\geq m$ de A.
– Pour montrer que a est une racine d'ordre m du polynôme P, on peut montrer que P est divisible par $(X-a)^m$, mais pas par $(X-a)^{m+1}$.

Chapitre 2

Espaces vectoriels

Dans ce chapitre $\mathbb{K} = \mathbb{C}$ ou $\mathbb{K} = \mathbb{R}$.

2.1 Structures d'espace vectoriel

Définition 2.1.1 *On appelle espace vectoriel sur $\mathbb{K}$ (ou $\mathbb{K}-$ espace vectoriel) un ensemble E muni de deux lois :*

- *Une loi interne, notée $+$, telle que $(E, +)$ soit un groupe abélien. L'élément neutre sera noté 0_E.*
- *Une loi externe*

$$* : \left\{ \begin{array}{ccc} \mathbb{K} \times E & \to & E, \\ (\lambda, v) & \mapsto & \lambda * v \end{array} \right.$$

telle que

(EV1) $\forall(\alpha, \beta) \in \mathbb{K}^2 \quad \forall x \in E \quad (\alpha + \beta) * x = \alpha * x + \beta * x$

(EV2) $\forall \alpha \in \mathbb{K} \quad (x, y) \in E^2 \quad \alpha * (x + y) = \alpha * x + \alpha * y$

(EV3) $\forall(\alpha, \beta) \in \mathbb{K}^2 \quad \forall x \in E \quad \alpha * (\beta * x) = (\alpha\beta) * x$

(EV4) $\forall x \in E \quad 1 * x = x$ *(1 désigne l'élément unité de $\mathbb{K}$).*

Les éléments de $\mathbb{K}$ sont appélés scalaires, ceux de E vecteurs.

Exemple 2.1.1 *i) $\mathbb{C}$ est un espace vectoriel sur $\mathbb{R}$ et sur $\mathbb{C}$!*

ii) n-uplets réels : $\mathbb{R}^n = \{(x_1, ..., x_n);\ x_1, ..., x_n \in \mathbb{R}\}$. Espace vectoriel sur $\mathbb{R}$.
- *Addition : $(1, 2, 3, 4) + (3, -1, -3, 1) = (4, 1, 0, 5)$.*
- *Multiplication externe : $(-2)(2, -1, 2, -2) = (-4, 2, -4, 4)$.*

iii) Suites de réels $\mathbb{R}^{\mathbb{N}} = \{(u_n);\ \forall n \in \mathbb{N}\, u_n \in \mathbb{R}\}$. Espace vectoriel sur $\mathbb{R}$.
- *Addition : $(2^{-n}) + (3^{-n}) = (2^{-n} + 3^{-n})$.*
- *Multiplication externe : $(-2)(2^{-n}) = (-2^{-n+1})$.*

iv) *Polynômes* $\mathbb{R}[X]$ *ou* $\mathbb{C}[X]$.
- *Addition :* $(-1+2X+3X^2)+(3X-X^2-2X^4)=-1+5X+2X^2-2X^4$.
- *Multiplication :* $(-2)(3X-X^2-2X^4)=-6X+2X^3+4X^4$.

v) *Apllications de* $\mathbb{R}$ *dans* $\mathbb{R}$ *:* $\mathbb{R}^{\mathbb{R}}$. *Espace vectoriel sur* $\mathbb{R}$.
- *Addition :* $(\cos+\sin) : x \mapsto \cos(x)+\sin(x)$.
- *Multiplication externe :* $(-2)\cos : x \mapsto -2\cos(x)$.

vi) *L'ensemble* E^X *des applications d'un ensemble* X *quelconque dans un* $\mathbb{K}-$ *espace vectoriel* E *est muni d'une structure de* $\mathbb{K}$*-espace vectoriel grâce à deux lois*

$$\left|\begin{array}{rcl} E^X \times E^X & \to & E^X, \\ (f,g) & \mapsto & f+g \end{array}\right. \qquad \forall x \in X \quad (f+g)(x)=f(x)+g(x),$$

$$\left|\begin{array}{rcl} \mathbb{K} \times E^X & \to & E^X, \\ (\alpha,g) & \mapsto & \alpha f \end{array}\right. \qquad \forall x \in X \quad (\alpha f)(x)=\alpha * f(x),$$

Exercice 2.1.1 *Soit* E *un* $\mathbb{K}-$ *espace vectoriel. Montrer que*

$$\forall x \in E \quad 0_{\mathbb{K}} * x = 0_E, \tag{2.1.1}$$

$$\forall \alpha \in \mathbb{K} \quad \alpha * 0_E = 0_E, \tag{2.1.2}$$

$$\forall (\alpha,x) \in \mathbb{K} \times E \quad (\alpha * x = 0_E \Rightarrow \alpha = 0_{\mathbb{K}} \ ou \ x = 0_E), \tag{2.1.3}$$

$$\forall x \in E \quad (-1) * x = -x, \tag{2.1.4}$$

$$\forall (\alpha,\beta) \in \mathbb{K}^2 \quad \forall x \in E \quad (\alpha-\beta) * x = \alpha * x - \beta * x, \tag{2.1.5}$$

$$\forall \alpha \in \mathbb{K} \quad \forall (x,y) \in E^2 \quad \alpha * (x-y) = \alpha * x - \alpha * y. \tag{2.1.6}$$

Définition 2.1.2 (Combinaison linéaire) *Soit* E *un espace* $\mathbb{K}-$ *vectoriel et* $(x_1,...,x_n)$ *une famille de vecteurs de* E. *On appelle* <u>combinaison linéaire</u> *des éléments de cette famille tout vecteur* $x \in E$ *qui peut s'écrire sous la forme*

$$x = \sum_{i=1}^{n} \alpha_i x_i \quad où \quad (\alpha_1,...,\alpha_n) \in \mathbb{K}^n.$$

Plus généralement, on appelle combinaison linéaire d'une famille quelconque toute combinaison linéaire d'une sous-famille finie.

2.1.1 Sous-espaces vectoriels

Définition 2.1.3 (Sous-espace vectoriel) *Soit* E *un* $\mathbb{K}-$ *espace vectoriel. On appelle*

<u>sous-espace vectoriel</u> *de* E *(en abrégé s.e.v.) toute partie* F *de* E *stable par* $+$ *et* $*$, *c.à.d. telle que*

$$\forall (x,y) \in F^2 \quad x+y \in F,$$
$$\forall \alpha \in \mathbb{K} \quad \forall x \in F \quad \alpha * x \in F$$

et qui muni des lois induites, est encore un $\mathbb{K}-$ *espace vectoriel.*

Théorème 2.1.1 *Une partie* F *d'un* $\mathbb{K}-$ *espace vectoriel* E *est un sous-espace vectoriel de* E *ssi*

- *F est non vide.*
- *F est stable par combinaison linéaire, c. à d.*

$$\forall(\alpha,\beta)\in\mathbb{K}^2 \quad \forall(x,y)\in F^2 \quad \alpha*x+\beta*y\in F.$$

Preuve

- Si F est un sous-espace vectoriel, il est non vide car c'est un sous-groupe de $(E,+)$ (il contient 0_E). Il est stable par $+$ et $*$, donc par combinaison linéaire.
- Si F est non vide et stable par combinaison linéaire, on a en particulier
  - $\forall(x,y)\in F^2 \quad x-y\in F$: F est donc un sous-groupe de $(E,+)$; c'est donc un groupe abélien.
  - F est stable par $+$ et par $*$ et les prporiétés (EV1)-(EV4) de la multiplication externe de E sont valables en particulier quand on restreint à F.

□

Exemple 2.1.2 *i) Pour tout espace vectoriel E, $\{0_E\}$ et E sont des sous-espaces vectoriels de E.*

ii) L'ensemble des vecteurs d'une droite est un sous-espace vectoriel de l'ensemble des vecteurs du plan.

iii) L'ensemble des fonctions continues est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{R}}$.

Théorème 2.1.2 *L'intersection d'une famille quelconque de sous-espaces vectoriels d'un $\mathbb{K}-$ espace vectoriel est un sous-espace vectoriel.*

Preuve

Soit $(F_i)_{i\in I}$ une famille de sous-espaces vectoriels de E, et F l'intersection de cette famille (c.à. d. l'ensemble des éléments appartenant à tous les F_i). On a

- $\forall i\in I \quad 0_E\in F_i$, donc $0_E\in F$, et F est non vide.
- De plus, si x et y sont deux éléments quelconque de F et α et β deux scalaires, $\forall i\in I \quad x\in F_i, \quad y\in F_i$, donc $\alpha x+\beta y\in F_i$ et par conséquent $\alpha x+\beta y\in F$. F est stable par combinaison linéaire. F est donc un sous-sepace vectoriel de E.

□

Exemple 2.1.3

$$X_1=\{(x_1,x_2,x_3)\in\mathbb{R}^3;\, x_1=0\}, \quad X_3=\{(x_1,x_2,x_3)\in\mathbb{R}^3;\, x_3=0\}$$

sont des sous-espaces vectoriels de $\mathbb{R}^3$ (plans passant par l'origine dans $\mathbb{R}^3$). Leur intersection

$$X_{13}=\{(x_1,x_2,x_3)\in\mathbb{R}^3;\, x_1=x_3=0\}$$

est également un sous-espace vectoriel de $\mathbb{R}$ (droite passant par l'origine).

Exercice 2.1.2 *Montrer qu'une réunion de deux sous-espaces vectoriels d'un $\mathbb{K}-$ espace vectoriel E est un sous-espace vectoriel de E ssi l'un est inclus dans l'autre.*

Définition 2.1.4 (Sous-espace vectoriel engendré par X) *Soit X une partie quelconque d'un espace vectoriel E. On appelle sous-espace vectoriel engendré par X l'intersection de tous les sous-espaces vectoriels de E contenant X.*

Il est clair qu'il s'agit du plus petit sous-espace vectoriel de E contenant X. On le note $\mathrm{Vect}(X)$.

Proposition 2.1.1 $\mathrm{Vect}(X)$ *est l'ensemble des combinaisons linéaires des éléments de X.*

Preuve

Comme il est stable par combinaison linéaire, $\mathrm{Vect}(X)$ contient toute combinaison linéaire des éléments de X. Or, l'ensemble de toutes les combinaisons linéaires est clairement un sous-espace vectoriel de E ; c'est donc les plus petit contenant X. □

Remarque 2.1.1 *En pratique on va plus utiliser la proposition que la définition.*

Exemple 2.1.4

Complexes	
Famille	*Espace engendré*
$\big(i\big)$	$\{\, z \in \mathbb{C}\,,\ Re(z) = 0 \,\}$
$\big(e^{i\pi/4}\big)$	$\{\, z \in \mathbb{C}\,,\ Re(z) = Im(z) \,\}$
$\big(1, i\big)$	$\mathbb{C}$

Couples de réels	
Famille	*Espace engendré*
$\big((0,1)\big)$	$\{\, (x,y) \in \mathbb{R}^2\,,\ x = 0 \,\}$
$\big((1,1)\big)$	$\{\, (x,y) \in \mathbb{R}^2\,, x = y \,\}$
$\big((0,1),(1,1)\big)$	$\mathbb{R}^2$

Suites de réels	
Famille	*Espace engendré*
$\big((2^n)\big)$	$\{\, (u_n)\,,\ \forall n\,,\ u_{n+1} = 2u_n \,\}$
$\big((u_n)\,,\ \exists n_0\,,\ \forall n \neq n_0\,,\ u_n = 0\big)$	$\{\, (u_n)\,,\ \exists n_0\,,\ \forall n \geqslant n_0\,,\ u_n = 0 \,\}$
$\big((u_n)\,,\ \forall n\,,\ u_n \in [0,1]\big)$	$\{\, (u_n)\,,\ \exists M\,,\ \lvert u_n\rvert \leqslant M \,\}$

Polynômes	
Famille	*Espace engendré*
$\big(X\big)$	$\{\,\lambda X\,,\ \lambda\in\mathbb{R}\,\}$
$\big(1+X, 1-X\big)$	$\{\,P\in\mathbb{R}[X]\,,\ deg(P)\leqslant 1\,\}$
$\big(P\in\mathbb{R}[X]\,,\ P(1)=1\big)$	$\mathbb{R}[X]$

Fonctions de $\mathbb{R}$ dans $\mathbb{R}$	
Famille	*Espace engendré*
$\big(\cos\big)$	$\{\,\lambda\cos\,,\ \lambda\in\mathbb{R}\,\}$
$\big(\cos,\sin\big)$	$\{\,\lambda\cos+\mu\sin\,,\ \lambda,\mu\in\mathbb{R}\,\}$
$\big(f\,,\ f(0)=1\big)$	$\mathbb{R}^{\mathbb{R}}$

Définition 2.1.5 (Somme de deux sous-espaces vectoriels) *Soit E un $\mathbb{K}-$ espace vectoriel. On appelle somme de deux sous-espaces vectoriels F et G, le sous-espace vectoriel de E engendré par leur réunion :*

$$F+G=\mathrm{Vect}(F\cup G).$$

La somme d'un élément de F et d'un élément quelconque de G est un élément de $F+G$. Comme l'ensemble de toutes ces sommes est un sous-espace vectoriel, c'est nécessairement le plus petit contenant $F\cup G$, d'où :

Proposition 2.1.2

$$F+G=\{x\in E;\ \exists(x_1,x_2)\in F\times G\quad x=x_1+x_2\}.$$

Définition 2.1.6 (Sous-espaces supplémentaires) *Soit E un $\mathbb{K}-$ espace vectoriel. Deux sous-espaces F et G sont dits supplémentaires si tout vecteur de E peut se décomposer de façon unique en la somme d'un vecteur de F et d'un vecteur de G. Si $E=F+G$ et F et G sont supplémentaires, on dit que la somme est directe et on écrit*

$$E=F\oplus G$$

Théorème 2.1.3 *Les sous-espaces vectoriels F et G sont supplémentaires ssi*

$$F+G=E,\quad F\cap G=\{0_E\}.$$

Preuve

– Si F et G sont supplémentaires, tout vecteur de E est la somme d'un vecteur de F et d'un vecteur de G, donc $F+G=E$. Soit $x \in F \cap G$; on peut écrire :
$x = x + 0_E \quad (x \in F,\, 0_E \in G)$ et $x = 0_E + x \quad (0_E \in F,\, x \in G)$. Du fait de l'unicité de la décomposition, on peut conclure que $x = 0_E$; donc $F \cap G = \{0_E\}$.
– Réciproquement, soit F et G deux sous-espaces vectoriels de E tels que $F+G=E$ et $F \cap G = \{0_E\}$. Tout vecteur de E peut se décomposer en la somme d'un vecteur de F et d'un veceur de G. Supposons que le vecteur x ait deux décompositions :

$$x = x_1 + x_2 = x_1' + x_2' \quad \text{avec } (x_1, x_1') \in F^2 \ (x_2, x_2') \in G^2.$$

On a alors $x_1 - x_1' = x_2' - x_2$, ce vecteur appartient à la fois à F et à G, il est donc nul. D'où $x_1 = x_1', \quad x_2 = x_2'$; la décomposition est unique ; F et G sont supplémentaires.

□

2.2 Applications linéaires

2.2.1 Morphismes d'espaces vectoriels

Définition 2.2.1 *Soit E et F deux espaces vectoriels sur le même corps $\mathbb{K}$. Une application f de E dans F est dite linéaire si*

$$\forall(\alpha,\beta) \in \mathbb{K}^2 \quad \forall(x,y) \in E^2 \quad f(\alpha x + \beta y) = \alpha f(x) + \beta f(y).$$

L'ensemble des applications linéaires de E dans F est noté $\mathcal{L}_{\mathbb{K}}(E,F)$ ou $\mathcal{L}(E,F)$ s'il n'y a pas d'ambigu'ite.

Remarque 2.2.1 *i) Une application $f : E \to F$ entre espaces vectoriels est donc linéaire si c'est un morphisme pour chacune des deux lois $+$ et $*$.*

ii) On a donc en particulier

$$f(0_E) = 0_E, \quad \forall x \in E \quad f(-x) = -f(x).$$

Exemple 2.2.1 *i) L'application*

$$f : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (2x+3y, x-y) \end{array} \right.$$

est linéaire.

ii) L'application

$$D : \left\{ \begin{array}{rcl} C^1(\mathbb{R}) & \to & C(\mathbb{R}) \\ f & \mapsto & f' \end{array} \right.$$

est linéaire.

iii) L'application

$$E : \left\{ \begin{array}{rcl} \mathbb{K}[X] & \to & \mathbb{R} \\ P & \mapsto & P(0) \end{array} \right.$$

est linéaire.

iv) La linéarité d'une application donnée peut dépendre du corps $\mathbb{K}$*. Par exemple*

$$f : \left\{ \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C}, \\ z & \mapsto & \overline{z} \end{array} \right.$$

est $\mathbb{R}-$ *linéaire, mais elle n'est pas* $\mathbb{C}-$ *linéaire.*

Théorème 2.2.1 *Soit* E *et* F *deux* $\mathbb{K}$*-espaces vectoriels.* $\mathcal{L}(E,F)$ *est un sous-espace vectoriel de* F^E*.*

Preuve

L'application nulle est linéaire. Toute combinaison linéaire d'applications linéaires est linéaire :

Soit $(f,g) \in \mathcal{L}(E,F)^2 \quad (\lambda,\mu) \in \mathbb{K}^2 \quad \forall (x,y) \in E^2 \quad \forall (\alpha,\beta) \in \mathbb{K}^2$

$$\begin{array}{rcl} (\lambda f + \mu g)(\alpha x + \beta y) & = & \lambda f(\alpha x + \beta y) + \mu g(\alpha x + \beta y) \\ & = & \lambda(\alpha f(x) + \beta f(y)) + \mu(\alpha g(x) + \beta g(y)) \quad \text{(linéarité de } f \text{ et de } g\text{)} \\ & = & \alpha(\lambda f(x) + \mu g(x)) + \beta(\lambda f(y) + \mu g(y)) \\ & = & \alpha(\lambda f + \mu g)(x) + \beta(\lambda f + \mu g)(y), \end{array}$$

donc $\lambda f + \mu g$ est linéaire. □

Cas particuliers

On appelle

- Endomorphisme de E, une application linéaire de E dans E. L'ensemble des endomorphismes de E est noté $\mathcal{L}(E)$. C'est un sous-espace vectoriel de E^E.
- Isomorphisme une application linéaire bijective.
- Automorphisme de E, une application linéaire bijective de E dans E. L'ensemble des automorphismes de E dans E est noté $\mathcal{GL}(E)$.
- Forme linéaire sur E, une application linéaire de E dans $\mathbb{K}$. L'ensemble des formes linéaires sur E est noté E^*. C'est un sous-espace vectoriel de $\mathbb{K}^E$, appelé espace dual de E.

2.2.2 Noyau et image d'une application linéaire

Définition 2.2.2 *Soit* $f \in \mathcal{L}(E,F)$*.*

- *On appelle noyau de* f *l'ensemble des antécédents de* 0_F *dans* E*. On le note* $\operatorname{Ker} f$ *:*

$$\operatorname{Ker} f = \{x \in E;\ f(x) = 0_F\} = f^{-1}(\{0_F\}).$$

- *On appelle image de* f *l'ensemble des éléments de* F *qui ont un antécédent par* f *dans* E*. On le note* $\operatorname{Im} f$ *:*

$$\operatorname{Im} f = \{y \in F, \exists x \in E \quad f(x) = y\} = f(E).$$

Théorème 2.2.2 *Soit* E *et* F *deux* $\mathbb{K}-$ *espaces vectoriels et* f *une application linéaire de* E *dans* F*.*

i) $\mathrm{Ker}\, f$ *est un sous-espace vectoriel de* E.

ii) $\mathrm{Im} f$ *est un sous-espace vectoriel de* F.

iii) f *est injective ssi* $\mathrm{Ker}\, f = \{0_E\}$.

iv) f *est surjective ssi* $\mathrm{Im} f = F$.

Remarque 2.2.2 *Comparer avec Propositions 1.2.4 et 1.2.5.*

Preuve

i) $\mathrm{Ker}\, f$ est non vide, car $f(0_E) = 0_F$, donc $0_E \in \mathrm{Ker}\, f$. Montrons que $\mathrm{Ker}\, f$ est stable par combinaison linéaire. Soit $(x, y) \in (\mathrm{Ker}\, f)^2$ et $(\alpha, \beta) \in \mathbb{K}^2$. On a $f(x) = f(y) = 0_F$, d'où,

$$f(\alpha x + \beta y) = \alpha f(x) + \beta f(y) = 0_F,$$

donc $\alpha x + \beta y \in \mathrm{Ker}\, f$.

ii) $\mathrm{Im} f$ est non vide, car $f(0_E) = 0_F$, donc $0_F \in \mathrm{Im} f$. Montrons que $\mathrm{Im} f$ est stable par combinaison linéaire. Soit $(y_1, y_2) \in (\mathrm{Im} f)^2$ et $(\alpha, \beta) \in \mathbb{K}^2$. $\exists (x_1 x_2) \in E^2$, $y_1 = f(x_1)$, $y_2 = f(x_2)$; d'où

$$\alpha y_1 + \beta y_2 = \alpha f(x_1) + \beta f(x_2) = f(\alpha x_1 + \beta x_2),$$

donc $\alpha y_1 + \beta y_2 \in \mathrm{Im} f$.

iii) Si f est injective, $f(x) = f(0_E) \Rightarrow x = 0_E$, donc $\mathrm{Ker}\, f = \{0_E\}$. Réciproquement supposons que $\mathrm{Ker}\, f = \{0_E\}$. Soit $(x, y) \in E^2$ tel que $f(x) = f(y)$. Alors $f(x - y) = 0_F$, donc $x - y \in \mathrm{Ker}\, f$ par conséquent, $x - y = 0_E$. f est donc injective.

iv) La surjectivité de f équivaut, par définition, à $\mathrm{Im} f = F$.

□

2.2.3 Composition des applications linéaires

Théorème 2.2.3 *Soit* E, F, G *trois espaces vectoriels sur le même corps* $\mathbb{K}$, f *une application linéaire de* E *dans* F *et* g *une application linéaire de* F *dans* G. *Alors* $g \circ f$ *est une application linéaire de* E *dans* G.

Preuve

Soit $(\alpha, \beta) \in \mathbb{K}^2$ et $(x, y) \in E^2$. On a

$$\begin{aligned} g \circ f(\alpha x + \beta y) = g(f(\alpha x + \beta y)) &= g(\alpha f(x) + \beta f(y)) \quad \text{(linéarité de } f\text{)} \\ &= \alpha g(f(x)) + \beta g(f(y)) \quad \text{(linéarité de } g\text{)} \\ &= \alpha g \circ f(x) + \beta g \circ f(y), \end{aligned}$$

d'où $g \circ f \in \mathcal{L}(E, F)$. □

Théorème 2.2.4 *Soit* E *et* F *deux espaces vectoriels sur le même corps* $\mathbb{K}$. *La réciproque d'un isomorphisme de* E *dans* F *est un isomorphisme de* F *dans* E.

Preuve

Soit $(\alpha, \beta) \in \mathbb{K}^2$ et $(y_1, y_2) \in F^2$. On a

$$\begin{aligned} \alpha y_1 + \beta y_2 &= \alpha f(f^{-1}(y_1)) + \beta f(f^{-1}(y_2)) \\ &= f(\alpha f^{-}(y_1) + \beta f^{-1}(y_2)) \quad \text{(linéarité de } f\text{)}, \end{aligned}$$

donc $f^{-1}(\alpha y_1 + \beta y_2) = \alpha f^{-1}(y_1) + \beta f^{-1}(y_2)$.

□

Théorème 2.2.5 *Soit E, F, G trois $\mathbb{K}-$ espaces vectoriels. Les applications suivantes*

$$\left\{ \begin{array}{rcl} \mathcal{L}(E,F) & \to & \mathcal{L}(E,G) \\ f & \mapsto & g \circ f \end{array} \right. \quad et \quad \left\{ \begin{array}{rcl} \mathcal{L}(F,G) & \to & \mathcal{L}(E,G) \\ g & \mapsto & g \circ f \end{array} \right.$$

sont linéaires, c.à.d. que pour tout $(\alpha, \beta) \in \mathbb{K}^2$:

$$\begin{array}{l} \forall (f_1, f_2) \in \mathcal{L}(E,F)^2 \, \forall g \in \mathcal{L}(F,G) \quad g \circ (\alpha f_1 + \beta f_2) = \alpha(g \circ f_1) + \beta(g \circ f_2) \\ \forall \in \mathcal{L}(E,F) \, \forall (g_1, g_2) \in \mathcal{L}(E,G)^2 \quad (\alpha g_1 + \beta g_2) \circ f = \alpha(g_1 \circ f) + \beta(g_2 \circ f). \end{array}$$

Preuve : exo.

2.2.4 Anneau des endomorphismes

Spit E un $\mathbb{K}-$ espace vectoriel. D'après le théorème 2.2.1, $(\mathcal{L}(E), +, *)$ est un $\mathbb{K}-$ espace vectoriel ; en particulier, $(\mathcal{L}(E), +)$ est un groupe abélien. La composition d'applications est une loi interne dans $\mathcal{L}(E)$. Cette opération est associative. Elle possède un élément neutre qui est l'identité de E. En effet $id_E \in \mathcal{L}(E)$ et $\forall u \in \mathcal{L}(E) \quad u \circ id_E = id_E \circ u = u$. D'après le théorème 2.2.5, la composition des applications est également distributive par rapport à l'addition. On en déduit que $(\mathcal{L}(E), +, \circ)$ est un anneau.

Théorème 2.2.6 *Si E est un $\mathbb{K}-$ espace vectoriel, l'ensemble des ses endomorphismes $\mathcal{L}(E)$ est un anneau.*

Remarque 2.2.3 (Attention !)

– *L'anneau $\mathcal{L}(E)$ n'est en général pas commutatif. Exemple : $E = \mathbb{R}^2$. Soit*

$$f : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (y,x) \end{array} \right. \qquad g : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (x,0) \end{array} \right.$$

On a

$$f \circ g : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (0,x) \end{array} \right. \qquad g \circ f : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (y,0) \end{array} \right. ,$$

en particulier $f \circ g \neq g \circ f$. Aussi la formule de bionôme ne s'applique en général pas, on a seulement $(u+v)^2 = u^2 + uv + vu + v^2$ et non $(u+v)^2 = u^2 + 2uv + v^2$. Pour cette deuxième formule il faut en effet que les deux éléments commutent.

– *L'égalité $u \circ v = 0$ n'implique pas nécessairement $u = 0$ ou $v = 0$. Exemple $E = \mathbb{R}^2$. Soit*

$$u : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (x+y, x+y) \end{array} \right. \qquad v : \left\{ \begin{array}{rcl} \mathbb{R}^2 & \to & \mathbb{R}^2 \\ (x,y) & \mapsto & (x,-x) \end{array} \right.$$

Dans ce cas $u \circ v = 0$ alors que $u \neq 0$ et $v \neq 0$.

L'ensemble des éléments inversibles de l'anneau $\mathcal{L}(E)$ est l'ensemble des automorphismes de E. C'est un groupe pour la composition des applications, appelé groupe linéaire de E et noté $\mathcal{GL}(E)$:

$$\mathcal{GL}(E) = \{u \in \text{Ł}(E), \exists u^{-1} \in \text{Ł}(E) \quad uu^{-1} = u^{-1}u = id_E\}.$$

2.3 Projecteurs et symétries

2.3.1 Projection

Soit E un $\mathbb{K}-$ espace vectoriel et F, G deux sous-espaces vectoriels supplémentaires de E. On sait que tout élément de E peut s'écrire de façon unique $x = x_1 + x_2$, où $x_1 \in F$ et $x_2 \in G$.

Définition 2.3.1 (Projection) *On appelle projection sur F parallèlement à G l'application p de E dans E qui à x associe x_1. On dit aussi que p est un projecteur.*

On montre facilement que p est un endomorphisme et que

$$\text{Im}p = F; \quad \text{Ker}\, p = G.$$

Notons également que pour tout $x \in F \quad p(x) = x$.

Théorème 2.3.1 *Un endomorphisme d'un $\mathbb{K}-$ espace vectoriel E est un projecteur ssi $p \circ p = p$.*

Preuve

- Si p est la projection sur F parallèlement à G, pour tout $x = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in G$, $p(x) = x_1$ et $p \circ p(x) = p(x_1) = p(x)$, d'où $p \circ p = p$.
- Soit p un endomorphisme de E tel que $p \circ p = p$. Montrons que $\text{Im}p$ et $\text{Ker}\, p$ sont supplémentaires et que p est la projection sur $\text{Im}p$ parallèlement à $\text{Ker}\, p$. Soit $x \in E$. On a

  $$x = p(x) + (x - p(x)).$$

  Or $p(x) \in \text{Im}p$ et $x - p(x) \in \text{Ker}\, p$ car

  $$p(x - p(x)) = p(x) - p(p(x)) = 0.$$

  Donc $E = \text{Im}p + \text{Ker}\, p$. Soit $x \in \text{Im}p \cap \text{Ker}\, p$. Comme $x \in \text{Im}p$ il existe $t \in E$ tel que $x = p(t)$. Comme $x \in \text{Ker}\, p$, $p(x) = 0$. Or $p(x) = p \circ p(t) = p(t) = x$, d'où $x = 0$; donc $\text{Im}p \cap \text{Ker}\, p = \{0\}$. $\text{Im}p$ et $\text{Ker}\, p$ sont bien supplémentaires ; la projection sur $\text{Im}p$ parallèlement à $\text{Ker}\, p$ est l'application $x \mapsto p(x)$, c.à.d. p.

□

2.3.2 Symétrie

Soit F et G des sous-espaces supplémentaires de E. On sait que tout élément $x \in E$ peut s'écrire de feçon unique $x = x_1 + x_2$, où $x_1 \in F$ et $x_2 \in G$.

Définition 2.3.2 (Symétrie) *On appelle symétrie par rapport à F parallèlement à G l'application s de E dans E qui à $x = x_1 + x_2$ associe $x_1 - x_2$.*

Si l'on désigne par p_1 la projection sur F parallèlement à G, et par p_2 la projection sur G parallèlement à F, alors $s = p_1 - p_2$. s est donc un endomorphisme de E. On a

$$x \in \mathrm{Ker}\, s \Leftrightarrow x_1 - x_2 = 0 \Leftrightarrow x_1 = x_2 = 0 \Leftrightarrow x = 0.$$

Il s'ensuit que s est injectif. Aussi

$$\forall x \in E \quad x = x_1 + x_2 = s(x_1 - x_2) : \quad \mathrm{Im} s = E,$$

s est surjectif.

2.3.3 Caractéristaion d'une symétrie

Théorème 2.3.2 *Un endomorphisme s d'un $\mathbb{K}-$ espace vectoriel E est un endomorphisme ssi il est involutif, c.à.d. $s \circ s = id_E$.*

Preuve

- Si s est la symétrie par rapport à F parallèlement à G, pour tout $x = x_1 + x_2$ avec $x_1 \in F$ et $x_2 \in G$, $s(x) = x_1 - x_2$ et $s \circ s(x) = x_1 + x_2 = x$, d'où $s \circ s = id_E$.
- Soit s un endomorphisme de E tel que $s \circ s = id_E$. Posons $p_1 = \frac{1}{2}(id_E + s)$ et $p_2 = \frac{1}{2}(id_E - s)$. Montrons que p_1 et p_2 sont des projecteurs :

$$\begin{aligned} p_1^2 &= \frac{1}{4}(id_E + 2s + s^2) = \frac{1}{2}(id_E + s) = p_1, \\ p_2^2 &= \frac{1}{4}(id_E - 2s + s^2) = \frac{1}{2}(id_E - s) = p_2. \end{aligned}$$

  Par ailleurs $p_1 + p_2 = id_E$: si p_1 est la projection sur F parallèlement à G, p_2 est la projection sur G parallèlement à F. Or $s = p_1 - p_2$. s est donc la symétrie par rapport à F parallèlement à G. □

2.4 Quelques conseils pratiques

- Pour montrer que $(E, +, *)$ est un espace vectoriel.

  - s'il s'agit de lois tout à fait nouvelles, il faut vérifier que
    - que $(E, +)$ est un groupe abélien,
    - que la loi externe vérifie (EV1)-(EV4).
  - S'il s'agit de la restriction à E des lois d'un espace vectoriel $\mathcal{E}$, il suffit de vérifier que E est un sous-espace vectoriel de $\mathcal{E}$ (voir ci-après).
- Pour montrer qu'une partie F d'un espace vectoriel E est un sous-espace vectoriel de E, on peut
  - vérifier que F est non vide et stable par combinaison linéaire.
  - Montrer que F est un sous-espace vectoriel engendré par une famille, c.à.d. l'ensemble des combinaisons linéaires des éléments de cette famille ;
  - Montrer que F est le noyau ou l'image d'une application linéaire ;
  - Montrer que F est une intersection de sous-espaces vectoriels ;
  - Montrer que F est la somme de sous-espaces vectoriels.
- Pour montrer que deux sous-espaces vecoriels F et G de E sont supplémentaires, on peut :
  - montrer que $F + G = E$ et $F \cap G = \{0\}$;
  - montrer que tout élément de E se décompose de façon unique en somme d'un élément de F et d'un élément de G.
- Pour montrer qu'un endomorphisme est un projecteur, on peut
  - montrer que $p \circ p = p$;
  - Montrer que $\mathrm{Im} p$ et $\mathrm{Ker}\, p$ sont supplémentaires et que

$$\forall x \in \mathrm{Im} p \quad p(x) = x.$$

- Pour montrer qu'un endomorphisme s de E est une symétrie, on peut
  - montrer que $s \circ s = id_E$;
  - montrer que $\mathrm{Ker}\,(s - id_E)$ et $\mathrm{Ker}\,(s + id_E)$ sont supplémentaires.

Chapitre 3

Dimension des espaces vectoriels

Dans ce chapitre $\mathbb{K} = \mathbb{C}$ ou $\mathbb{K} = \mathbb{R}$.

3.1 Familles libres ou liées

3.1.1 Définition

Définition 3.1.1 *Soit E un $\mathbb{K}-$ espace vectoriel. Une famille finie $(x_1, ..., x_p)$ d'éléments de E est dite libre si la seule combinaison linéaire des x_i qui s'annule est celle dont tous les coefficients sont nuls. C'est à dire si*

$$\forall(\alpha_1, ..., \alpha_p) \in \mathbb{K}^p \quad \alpha_1 x_1 + ...\alpha_p x_p = 0 \Rightarrow \alpha_1 = ...\alpha_p = 0.$$

On dit aussi que les vecteurs $x_1, ..., x_p$ sont linéairement indépendants. Une famille qui n'est pas libre est dite liée. Ses éléments sont dits linéairement dépendants.

La famille $(x_1, ..., x_p)$ est alors liée ssi

$$\exists(\alpha_1, ..., \alpha_p) \in \mathbb{K}^p \quad \alpha_1 x_1 + ...\alpha_p x_p = 0 \quad \text{et} \quad \exists i \in \{1, ..., p\} \quad \alpha_i \neq 0.$$

Exemple 3.1.1 *Dans $\mathbb{R}^2$ on considère les familles*

$$A = ((1, 0), (0, 1)), \quad B = ((1, 1), (3, 3)).$$

A est libre, B est liée.

Exercice 3.1.1 *Montrer que*

i) $\emptyset$ est libre.

ii) La famille (x) à un élément est libre ssi $x \neq 0$.

iii) Toute famille contenue dans une famille libre est libre.

iv) Toute famille contenant une famille liée est liée.

v) En particulier, toute famille contenant le vecteur nul est liée.

3.1.2 Caractérisation d'une famille liée

Théorème 3.1.1 *Une famille $(x_1, ..., x_p)$ de vecteurs d'un $\mathbb{K}-$ espace vectoriel E est liée ssi l'un au moins des x_i est combinaison linéaire des $(p-1)$ autres.*

Preuve

– Si la famille $(x_1, ..., x_p)$ est liée, il existe une combinaison linéaire des éléments de la famille qui s'annule avec au moins un coefficient non nul. Soit $\alpha_1 x_1 + ...\alpha_p x_p = 0$ avec, par exemple $\alpha_p \neq 0$. On peut alors écrire

$$x_p = \sum_{j=1}^{p-1} -\frac{\alpha_j}{\alpha_p} x_j.$$

x_p est alors combinaison linéaire des $(p-1)$ autres vecteurs.

– Si l'un des vecteurs, par exemple x_p, est combinaison linéaire des autres :

$$x_p = \sum_{j=1}^{p-1} \beta_j x_j; \quad \text{on a alors} \quad \sum_{j=1}^{p-1} \beta_j x_j - x_p = 0,$$

ce qui représente une combinaison linéaire des éléments de la famille avec un coefficient égal à -1 : la famille est liée.

□

Exemple 3.1.2 *i) Une famille de deux vecteurs (x, y) est liée ssi il existe un scalaire α tel que $y = \alpha x$ ou $x = \alpha y$. On dit que x et y sont colinéaires.*

ii) Toute famille contenant plusieurs fois le même élément est liée.

iii) La famille $(x, y, x + y)$ est liée.

Exercice 3.1.2 *Dans l'espace vectoriel $\mathbb{K}[X]$ montrer qu'une famille finie de polynômes de dégrés tous distincts est libre.*

3.2 Familles génératrices

3.2.1 Définition

Définition 3.2.1 *Soit E un $\mathbb{K}-$ espace vectoriel. Une famille $(u_i)_{i\in I}$ d'éléments de E est dite génératrice si le sous-espace vectoriel qu'elle engendre est E tout entier. L'espace vectoriel est dit de dimension finie s'il existe une famille génératrice finie $(x_1, ..., x_m) \in E^m$.*

Dans ce cas tout élément x de E est alors combinaison linéaire des x_i, c.à.d. qu'il existe une famille de scalaires $(\alpha_1, ..., \alpha_m) \in \mathbb{K}^m$ telle que $x = \alpha_1 x_1 + ... + \alpha_m x_m$.

Exemple 3.2.1 *i) La famille (x_1, x_2, x_3) suivante est génératrice de $\mathbb{R}^3$:*

$$x_1 = (1, 1, -1), \quad x_2 = (1, -1, 1), \quad x_3 = (-1, 1, 1).$$

En effet :

$$\forall (a, b, c) \in \mathbb{R}^3 \quad (a, b, c) = \frac{a+b}{2} x_1 + \frac{c+a}{2} x_2 + \frac{b+c}{2} x_3.$$

ii) Soit $a \in \mathbb{K}$. La famille $(1, (X-a), (X-a)^2, (X-a)^3)$ est génératrice de $\mathbb{K}_3[X]$ (polynômes de degré inférieur ou égal à trois), car tout polynôme de degré inférieur ou égal à trois s'écrit (formule de Taylor) :

$$P = P(a) + P'(a)(X-a) + \frac{P''(a)}{2!}(X-a)^2 + \frac{P'''(a)}{3!}(X-a)^3.$$

3.2.2 Propriété fondamentale d'un e.v. de dimension finie

Théorème 3.2.1 *Dans un espace vectoriel de dimension finie, une famille libre ne peut avoir plus d'éléments qu'une famille génératrice.*

Preuve

Soit E un $\mathbb{K}-$ espace vectoriel de dimension finie et $(g_1, ..., g_m)$ une famille génératrice de E. Supposons l'existence d'une famille libre $(l_1, ..., l_{m+1})$ ayant $m+1$ éléments. Comme $(g_1, ..., g_m)$ est génératrice, on peut écrire $l_1 = \alpha_1 g_1 + ...\alpha_m g_m$. l_1 étant non nul, les α_i ne sont pas tous nuls. Quitte à effectuer une permutation d'indices, on peut supposer $\alpha_1 \neq 0$. On a alors :

$$g_1 = \frac{1}{\alpha_1} l_1 - \frac{\alpha_2}{\alpha_1} - ... - \frac{\alpha_m}{\alpha_1} g_m.$$

Toute combinaison linéaire de $(g_1, ...g_m)$ est donc combinaison linéaire de

$$(l_1, g_2, ..., g_m).$$

De ce fait la famille $(l_1, g_2, ..., g_m)$ est génératrice. Raisonnons par récurrence, supposons que l'on peut ainsi remplacer g_i par l_i jusqu'à l'indice k $(k < m)$ en conservant le caractère génératrice de la famille, et vérifions qu'on peut encore le faire à l'indice $k+1$. $(l_1, ..., l_k, g_{k+1}, ..., g_m)$ étant génératrice, on peut écrire

$$l_{k+1} = \alpha_1 l_1 + ... + \alpha_k l_k + \alpha_{k+1} g_{k+1} + ... + \alpha_m g_m.$$

La famille $(l_1, ...l_{k+1})$ étant libre, les coefficients $\alpha_{k+1}, ..., \alpha_m$ ne sont pas tous nuls. Quitte à effectuer une permutation d'indices, on peut supposer $\alpha_{k+1} \neq 0$; d'où

$$g_{k+1} = -\frac{\alpha_1}{\alpha_{k+1}} l_1 - ... - \frac{\alpha_k}{\alpha_{k+1}} l_k + \frac{1}{\alpha_{k+1}} l_{k+1} - \frac{\alpha_{k+2}}{\alpha_{k+1}} g_{k+2} - ... - \frac{\alpha_m}{\alpha_{k+1}} g_m.$$

Toute combinaison linéaire de $(l_1, ..., l_k, g_{k+1}, ..., g_m)$ est donc combinaison linéaire de

$(l_1, ..., l_{k+1}, g_{k+2}, ..., g_m)$ qui est, par conséquent, génératrice. Par récurrence on peut donc conclure que $(l_1, ..., l_m)$ est génératrice. On en déduit alors que l_{m+1} est combinaison linéaire des l_i de $i = 1$ à m, ce qui contredit la liberté de la famille $(l_1, ..., l_{m+1})$. □

3.3 Bases d'un e.v. de dimension finie

3.3.1 Définition et caractérisation

Définition 3.3.1 *On appelle <u>base</u> d'un espace vectoriel E une famille à la fois libre et génératrice.*

Théorème 3.3.1 *i) Tout espace vectoriel de dimension finie possède des bases.*

ii) Toutes les bases d'un espace vectorile E de dimension finie ont le même nombre d'éléments, appelé dimension de E et noté dim E.

Preuve

i) Soit E un $\mathbb{K}-$espace vectoriel possédant une famille génératrice à m éléments. L'ensemble $\mathcal{L}$ des cardinaux des familles libres est une partie de $\mathbb{N}$ non vide (elle contient 0, car $\emptyset$ est libre) et majorée par m. $\mathcal{L}$ a donc un plus grand élément n. Soit $(e_1, ..., e_n)$ une famille libre de n éléments. Pour tout $x \in E$, la famille $(e_1, ..., e_n, x)$ est liée. Il existe donc une combinaison linéaire nulle :

$$\alpha_1 e_1 + ...\alpha_n e_n + \beta x = 0,$$

avec au mojns un coefficient non nul. Comme $(e_1, ..., e_n)$ est libre, β est nécessairement non nul. x est donc combinaison linéaire des e_i : la famille $(e_1, ..., e_n)$ est génératrice ; c'est une base de E.

ii) Supposons l'existence de deux bases $b = (e_1, ..., e_n)$ et $b' = (e'_1, ...e'_p)$. Comme b est libre et b' génératrice, $n \leq p$. Comme b' est libre et b génératrice, $p \leq n$, d'où $n = p$. Le cardinal d'une base est donc est donc une caractéristique de l'espace vectoriel, qu l'on appelle sa dimension.

Théorème 3.3.2 *Si* dim $E = n$ *:*

i) toute famille ibre a au plus n éléments ;

ii) toute famille libre à n éléments est une base ;

iii) toute famille génératrice a au moins n éléments ;

iv) toute famille génératrice à n éléments est une base.

Preuve

Soit $b = (e_1, ..., e_n)$ une base de E.

i) b étant génératrice, une famille libre ne peut avoir plus de n éléments.

ii) On a montré dans la preuve du théorème 3.3.1, qu'une famille libre à n éléments était nécaissairement une base.

iii) b étant libre, une famille génératrice a au mojs n éléments.

iv) Supposons $n \geq 2$. Soit $(g_1, ..., g_n)$ une famille génératrice à n éléments. Si elle était liée,, l'un des g_i serait combinaison linéaire des autres qui formerait donc une famille génératrice à $n-1$ éléments, ce qui est impossible. Par conséquent, la famille $(g_1, ..., g_n)$ est libre, c'est donc une base. Si $n = 0$ ou $n = 1$, le résultat est immédiat.

□

Théorème 3.3.3 (Théorème de la base incomplète) – *Toute famille génératrice contient une base.*

– *Toute famille libre peut être prolongée en une base.*

Preuve

Soit E un espace vectoriel de dimension $n \geq 1$.

– Une famille génératrice a au moins n éléments ; si cette famille est liée, l'un au moins de ces éléments est combinaison linéaire des autres : on peut le retirer sans nuire au caractère générateur de la famille. On peut ainsi retirer des éléments jusqu'à ce qu'il n'y en ait plus que n : on a alors une base.
– Une famille libre a au plus n éléments ; si cette famille n'est pas génératrice, il existe au moins un élément de E qui n'est pas combinaison linéaire des éléments de cette famille : on peut l'adjoindre à la famille sans nuire à sa liberté. On peut ainsi compléter la famille jusqu'à ce qu'elle ait n éléments ; on obtient alors une base.

□

3.3.2 Coordonnées d'un vecteur dans une base

Soit E un $\mathbb{K}-$ espace vectoriel de dimension $n \geq 1$, et $b = (e_1, ..., e_n)$ une base de E. b étant génératrice, tout vecteur x de E s'écrit sous la forme :

$$x = \xi_1 e_1 + ... + \xi_n e_n \quad \text{avec} \quad (\xi_1, ..., \xi_n) \in \mathbb{K}^n.$$

Supposons qu'il existe une autre décompsition :

$$x = \xi'_1 e_1 + ... + \xi'_n e_n \quad \text{avec} \quad (\xi'_1, ..., \xi'_n) \in \mathbb{K}^n.$$

On aurait alors

$$(\xi_1 - \xi'_1)e_1 + ... + (\xi_n - x'_n)e_n = 0.$$

La décomposition de x sur b est donc unique ! Les scalaires $\xi_1, ..., \xi_n$ s'appellent coordonnées de x dans la base b.

Exemple 3.3.1 *i) Dans $\mathbb{K}^n$, la famille $(e_1, ..., e_n)$ définie par*

$$e_1 = (1, ..., 0), \quad e_2 = (0, 1, ..., 0), \quad ... \quad , e_n = (0, 0, 0, ..., 1)$$

est une base, appelée base canonique de $\mathbb{K}^n$. $\dim \mathbb{K}^n = n$. Les coordonnées de $(a_1, ..., a_n)$ dans cette base sont les scalaires $a_1, ..., a_n$.

ii) Dans $\mathbb{K}_n[X]$ (polynômes de degré infrieur ou égal à n), la famille

$$(1, X, X^2, ..., X^n)$$

est une base, appelée base canonique de $\mathbb{K}_n[X]$. $\dim \mathbb{K}_n[X] = n + 1$. Les coordonnées d'un polynôme dans cette base sont ses coefficients.

iii) Si E et F sont deux $\mathbb{K}-$ espaces vectoriels munis de bases $(e_1, ..., e_p)$ et $(f_1, ...f_n)$, la famille

$$(e_i, 0)_{i \in \{1,...,p\}}, \ (0, f_j)_{j \in \{1,...,n\}}$$

est une base de l'espace vectoriel produit $E \times F$. On a

$$\dim E \times F = \dim E + \dim F$$

Les coordonnées de (x, y) dans cette base sont celles de x suivies par celles de y.

3.4 Sous-espaces vectoriels en dimension finie

3.4.1 Dimension d'un sous-espace vectoriel

Théorème 3.4.1 *Soit E un $\mathbb{K}-$ espace vectoriel de dimension finie. Tout sous-espace vectoriel F de E est de dimension finie, et :*

$$\dim F \leq \dim E$$

Si $\dim F = \dim E$, alors $F = E$.

Preuve

Soit $n = \dim E$. Les familles libres de F sont des familles libres de E ; elles ont donc au plus n éléments. L'ensemble des cardinaux des familles libres de F est une partie non vide de $\mathbb{N}$ majorée par n ; il admet donc un plus grand élément p. Comme dans la première partie du théorème 3.3.1, on en déduit l'existence d'une base de F à p éléments. Donc $\dim F = p$ et $\dim F \leq \dim E$. Si $\dim F = \dim E$, une base de F est une famille libre de E à n éléments : c'est aussi une base de E et $F = E$. □

Remarque 3.4.1 *Ce théorème est très utile dans les applications, car il permet d'éviter d'avoir à démontrer l'autre inclusion, parfois difficile.*

3.4.2 Rang d'une famille de vecteurs

Définition 3.4.1 *Soit E un e.v. de dimension n. On appelle rang d'une famille $(x_1, ...x_p)$ de p vecteurs de E, la dimension du sous-espace vectoriel engendré par cette famille.*

On a donc :
- $rg(x_1, ..., x_p) \leq p$ car $(x_1, ..., x_p)$ est génératrice de $Vect(x_1, ..., x_p)$.
- $rg(x_1, ..., x_p) \leq n$ car $Vect(x_1, ..., x_p)$ est un sous-espace vectoriel de E.
- D'où $rg(x_1, ..., x_p) \leq \min(p, n)$.
- $rg(x_1, ..., x_p) = p$ ssi $(x_1, ..., x_p)$ est libre.
- $rg(x_1, ..., x_p) = n$ ssi $(x_1, ..., x_p)$ est génératrice de E.

3.4.3 Dimension de deux s.e.v. supplémentaires

Théorème 3.4.2 *Soit E un espace vectoriel de dimension finie. Deux sous-espaces vectoriels F et G de E sont supplémentaires ssi*

$$\dim F + \dim G = \dim E \quad et \quad F \cap G = \{0\}.$$

Preuve

Soit $(f_1, ..., f_p)$ une base de F et $(g_1, ..., g_q)$ une base de G.

– supposons F et G supplémentaires. Alors $f \cap G = \emptyset$. Comme $E = F + G$, la famille $(f_1, ..., f_p, g_1, ..., g_q)$ est génératrice de E. Montrons qu'elle est libre. Si

$$\alpha_1 f_1 + ... + \alpha_p g_p + \beta_1 g_1 + ... + \beta_q g_q = 0,$$

on en déduit

$$\alpha_1 f_1 + ... + \alpha_p f_p = -\beta_1 g_1 - ... - \beta_q g_q$$

qui appartient donc à F et à G. Comme $f \cap G = \{0\}$, on a donc $\alpha_1 f_1 + ... + \alpha_p f_p = 0$ et , puisque $(f_1, ..., f_p)$ est libre, $\alpha_1 = ... = \alpha_p = 0$. Avec le même raisonnement on montre $\beta_1 = ... = \beta_q = 0$. En définitive $(f_1, ..., f_p, g_1, ..., g_q)$ est une base de E, d'où $\dim E = p + q = \dim F + \dim G$.

– Réciproquement, supposons que $\dim F + \dim G = \dim E$ et $F \cap E = \{0\}$. On montre, comme ci-dessus, que la famille $(f_1, ..., f_p, g_1, ..., g_q)$ est libre. Son cardinal est $p + q$, c.à.d. $\dim E$. C'est donc une base de E. Tout élément de E se décompose sur cette base et par conséquent $E = F + G$. Comme $F \cap G = \{0\}$, cette somme est directe. F et G sont donc supplémentaires.

□

Remarque 3.4.2 *Ce théorème démontre en même temps que tout sous-espace vectoriel F d'un espace vectoriel E de dimension finie possède des supplémentaires : les vecteurs utilisés dans le théorème de la base incomplète pour prolonger une base de F en une base de E engendrent un supplémentaire de F.*

3.4.4 Dimension d'une somme de s.e.v.

Soit F et G deux sous-espaces vectoriels dun $\mathbb{K}-$ espace vectoriel E. Si la somme $F + G$ est directe, le théorème précédent permet d'écrire

$$\dim(F \oplus G) = \dim F + \dim G.$$

Dans le cas général on a

Théorème 3.4.3 *Soit E un $\mathbb{K}-$ espace vectoriel e dimension finie, F et G deux sous-espaces vectoriels de E. Alors*

$$\dim(F + G) = \dim F + \dim G - \dim(F \cap G).$$

Preuve

Soit F' un supplémentaire de $F \cap G$ dans F. Montrons que $F + G = F' \oplus G$. Il est clair que $F' + G \subset F + G$. De plus

$$\forall x \in F + G \quad \exists (y, z) \in F \times G \quad x = y + z$$

et $\exists (y', y'') \in F' \times (F \cap G) \quad y = y' + y''$, d'où $x = y' + y'' + z$ avec $y' \in F'$ et $y'' + z \in G$. Donc $x \in F' + G$. D'où $F + G = F' + G$. Or $F' \cap G \subset F' \cap (F \cap G)$, donc $F' \cap G = \{0\}$. La somme $F' + G$ est donc directe. De $F + G = F' \oplus G$, on déduit $\dim(F + G) = \dim F' + \dim G$. Or $\dim F' = \dim F - \dim(F \cap G)$; d'où $\dim(F + G) = \dim F + \dim G - \dim(F \cap G)$. □

3.5 Applications linéaires en dimension finie

3.5.1 Image d'une base

En dimension finie une application linéaire est entièrement déterminée par l'image d'une base.

Théorème 3.5.1 *Soit E un $\mathbb{K}-$ espace vectoriel de dimension finie p munie d'une base $b = (e_1, ..., e_p)$ et F un $\mathbb{K}-$ espace vectoriel quelconque. Pour toute famille $(y_1, ..., y_p)$ de p éléments de F il existe une et une seule application linéaire f de E dan F telle que*

$$\forall i \in \{1, ..., p\} \quad f(e_i) = y_i.$$

Preuve

Si f existe, elle associe nécessairement au vecteur $x = \xi_1 e_1 + ... + \xi_p e_p$ de E, le vecteur

$$\xi_1 f(e_1) + ... + \xi_p f(e_p) = \xi_1 y_1 + ... + \xi_p y_p.$$

Réciproquement on vérifie que l'appication ainsi définie est bien linéaire. □

3.5.2 Rang d'une application linéaire

Définition 3.5.1 *Soit E un $\mathbb{K}-$ espace vectoriel de dimension finie p muni d'une base b avec $b = (e_1, ..., e_p)$ et F un $\mathbb{K}-$ espace vectoriel quelconque. Soit $f \in \mathcal{L}(E, F)$. On appelle rang de f le rang de la famille $(f(e_1), ..., f(e_p))$, qui est aussi la dimension de* $\mathrm{Im} f$.

Théorème 3.5.2 *Soit E un espace vectoriel de dimension finie p muni d'une base $b = (e_1, ..., e_p)$ et F un $\mathbb{K}-$ espace vectoriel de dimension finie n. Soit $f \in \mathcal{L}(E, F)$:*

i) f est injective $\Leftrightarrow$ $f(b)$ est libre dans $F \Leftrightarrow rgf = p$.

ii) f est surjective $\Leftrightarrow$ $f(b)$ est génératrice de $F \Leftrightarrow rgf = n$.

iii) f est bijective $\Leftrightarrow$ $f(b)$ est une base de $F \Leftrightarrow rgf = p = n$.

Preuve

i) Suppososn f injective, et considérons une combinaison linéaire des $f(e_i)$ qui s'annule : $\alpha_1 f(e_1) + ... + \alpha_p f(e_p) = 0$. f étant linéaire, $f(\alpha_1 e_1 + ... + \alpha_p e_p) = 0$, et comme $\mathrm{Ker} f = \{0\}$, $\alpha_1 e_1 + ... + \alpha_p e_p = 0$. La famille $(e_1, ..., e_p)$ étant libre, on en déduit que $\alpha_1 = \alpha_2 = ... = \alpha_p = 0$; c.à.d. que la famille $(f(e_1), ..., f(e_p))$ est libre. Son rang est alors p. Réciproquement si $(f(e_1), ..., f(e_p))$ est libre, soit $x \in \mathrm{Ker} f$. Décomposons x sur la base b : $x = \xi_1 e_1 + ... + \xi_p e_p$. On a

$$f(x) = \xi_1 f(e_1) + ... + \xi_p f(e_p).$$

D'où $\xi_1 = ... = \xi_p = 0$ et $x = 0$. On en déduit que $\mathrm{Ker} f = \{0\}$, c.à.d. que f est injective.

ii) La famille $(f(e_1), ..., f(e_p))$ engendre $\mathrm{Im} f$. Donc f est surjective ssi elle engendre F tout entier. Son rang est alors n.

iii) f est bijective ssi elle est à la fois injective et surjective.

□

Corollaire 3.5.1 *Si E et F sont des espaces vectoriels de dimension finie, et si $\dim E = \dim F$, une application linéaire f de E dans F est bijective si et seulement si elle est injective ou surjective.*

Corollaire 3.5.2 *Deux $\mathbb{K}-$ espaces vectoriels de dimension finie sont isomorphes ssi ils ont la même dimension.*

3.5.3 Théorème du rang

Théorème 3.5.3 (Théorème du rang) *Soit E un $\mathbb{K}-$ espace vectoriel de dimension finie et F un $\mathbb{K}-$ espace vectoriel quelconque. Soit f une application linéaire de E dan F.*

i) $\mathrm{Im} f$ *est isomorphe à tout supplémentaire de* $\mathrm{Ker}\, f$ *dans* E.

ii) $\dim \mathrm{Ker}\, f + \dim \mathrm{Im} f = \dim E$.

Preuve

i) Soit G un supplémentaire de $\mathrm{Ker}\, f$ dans E, et g la restriction de f à G comme ensemble de départ et $\mathrm{Im} f$ comme ensemble d'arrivée. $\mathrm{Ker}\, g = G \cap \mathrm{Ker}\, f = \{0\}$, donc g est injective. $\mathrm{Im} g \subset \mathrm{Im} f$. Réciproquement, soit $y \in \mathrm{Im} f$, ce qui signifie que $\exists x \in E \quad y = f(x)$. Comme $E = G \oplus \mathrm{Ker}\, f, \quad x = x_1 + x_2$, avec $x_1 \in G$ et $x_2 \in \mathrm{Ker}\, f$. On a

$$f(x) = f(x_1) + f(x_2) = f(x_1) = g(x_1);$$

d'où $y \in \mathrm{Im} g$. Donc $\mathrm{Im} f \subset \mathrm{Im} g$. En définitive $\mathrm{Im} g = \mathrm{Im} f$, donc g est surjective. g est donc un isomorphisme de G dans $\mathrm{Im} f$.

ii) On en déduit que $\dim G = \dim E - \dim \mathrm{Ker}\, f$. Or $\dim G = \dim E - \dim \mathrm{Ker}\, f$. On a donc bien $\dim E = \dim \mathrm{Ker}\, f + \dim \mathrm{Im} f$.

□

3.6 Quelques conseils pratiques

- Pour montrer qu'une famille de vecteurs d'un e.v. est libre on peut
  - écire une combinaison linéaire des éléments de cette famille qui s'annule et démontrer que tous les coefficients sont nuls.
  - supposer que l'un des éléments de cette famille est combinaison des autres et aboutir à une contradiction.
- Pour montrer qu'une famille de vecteurs d'un e.v. E est génératrice, on montre que tout élément de E est combinaison linéaire des éléments de cette famille.
- Pour montrer qu'une famillle de vecteurs b d'un e.v. E est une base :
  - si on ne connaˆit pas la dimension de E, il faut montrer que b est libre et génératrice ;
  - si on sait que E est de dimension finie n, il suffit de montrer que b possède n éléments et qu'elle est libre (ou qu'elle possède n éléments et qu'elle est génératrice).
- Pour construire une base d'un e.v. de dimension finie, on peut :

  - compléter une famille libre à l'aide du théorème de la base incomplète ;
  - en particulier compléter une base d'un sous-espace vectoriel ;
  - retirer d'une famille génératrice finie, un élément qui est combinaison linéaire des autres, et recommencer jusqu'à obtenir une famille libre ;
  - réunir des bases de deux s.e.v. supplémentaires.
- Pour raisonner sur les dimensions de sous-espaces vectoriels F et G d'un e.v. de dimension finie E, on utilise les relations
  - $F \subset G \Rightarrow \dim F \leq \dim G$
  - $\dim(F+G) = \dim F + \dim G - \dim(F \cap G)$
  - $\dim(F \oplus G) = \dim F + \dim G$.
- Pour raisonner sur des applications linéaires entre deux s.e.v. E et F, l'outil essentiel est le théorème du rang :

$$\dim \operatorname{Im} f + \dim \operatorname{Ker} f = \dim E.$$

- Pour montrer qu'une application linéaire f entre deux e.v. e dimension finie est un isomrophisme, il suffit de montrer qu'elle est injective ($\operatorname{Ker} f = \{0\}$), et que $\dim E = \dim F$.

Chapitre 4

Matrices

Dans ce chapitre on se restreint de nouveau à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

4.1 Espace vectoriel $M_{np}(\mathbb{K})$

4.1.1 Matrices à n lignes et p colonnes

Définition 4.1.1 *On appelle matrice à n lignes et p colonnes (ou de type (n,p)) à coefficients dans $\mathbb{K}$, une application*

$$A : \left\{ \begin{array}{rcl} \{1,...,n\} \times \{1,...,p\} & \to & \mathbb{K} \\ (i,j) & \mapsto & a_{ij}, \end{array} \right.$$

c.à.d. la donnée de np éléments de $\mathbb{K}$, que l'on peut disposer en tableau :

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1p} \\ a_{21} & a_{22} & ... & a_{2p} \\ ... & ... & ... & ... \\ a_{n1} & a_{n2} & ... & a_{np} \end{pmatrix}.$$

- Lorsqu'il n'y a pas d'ambigu¨ité sur les valeurs de n et p, la matrice A sera notée $A = (a_{ij})$.
- Le premier indice du coefficent a_{ij} est appelé indice de ligne et le second, indice de colonne.
- L'ensemble des matrices de type (n,p) à coefficients dans $\mathbb{K}$ est noté $\mathcal{M}_{np}(\mathbb{K})$.
- On appelle matrice carrée d'ordre n une matrice de type (n,n). Ses coefficients dont les indices de ligne et de colonne sont égaux sont appelés coefficients diagonaux. La famille des coefficents diagonaux est appelée diagonale de la matrice. L'ensemble des matrices carrées d'ordre n à coefficients dans $\mathbb{K}$ est noté $\mathcal{M}_n(\mathbb{K})$.

4.1.2 Addition des matrices

Soit $A = (a_{ij})$ et $B = b_{ij}) \in \mathcal{M}_{np}(\mathbb{K})$. On appelle somme des matrices A et B, la matrice $A + B = (c_{ij})$ définie par

$$\forall (i,j) \in \{1,...,n\} \times \{1,...,p\} \quad c_{ij} = a_{ij} + b_{ij}.$$

Exemple 4.1.1

$$\begin{pmatrix} 1 & 0 & -2 & -3 \\ 2 & -1 & 0 & 1 \\ 3 & 1 & 1 & -2 \end{pmatrix} + \begin{pmatrix} 0 & -1 & 2 & 2 \\ 1 & 1 & -1 & -1 \\ -2 & 2 & -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 & -1 \\ 3 & 0 & -1 & 0 \\ 1 & 3 & 0 & 0 \end{pmatrix}$$

Exercice 4.1.1 *Montrer que $(\mathcal{M}_{np}(\mathbb{K}), +)$ est un groupe abélien. L'élément neutre est la matrice nulle, l'opposée de A est $-A = (-a_{ij})$.*

4.1.3 Multiplication d'une matrice par un scalaire

Soit $A = (a_{ij}) \in \mathcal{M}_{np}(\mathbb{K})$ et $\alpha \in \mathbb{K}$. On appelle produit de la matrice A par le scalaire α la matrice $\alpha A = (b_{ij})$ de $\mathcal{M}_{np}(\mathbb{K})$ définie par

$$\forall (i,j) \in \{1,...,n\} \times \{1,...,p\} \quad b_{ij} = \alpha a_{ij}$$

Exemple 4.1.2

$$3 * \begin{pmatrix} 1 & 0 & -2 & -3 \\ 2 & -1 & 0 & 1 \\ 3 & 1 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 0 & -6 & -9 \\ 6 & -3 & 0 & 3 \\ 9 & 3 & 3 & -6 \end{pmatrix}$$

Exercice 4.1.2 *Montrer que $\mathcal{M}_{np}(\mathbb{K}), +, *)$ est un $\mathbb{K}-$ espace vectoriel.*

4.1.4 Base de $\mathcal{M}_{np}(\mathbb{K})$

Soit E_{ij} la matrice de $\mathcal{M}_{np}(\mathbb{K})$ dont tous les coefficients sont nuls, sauf celui de la ligne i et de la colonne j qui vaut 1.

Exercice 4.1.3 *$(E_{ij})_{1 \leq i \leq n,\, 1 \leq j \leq p}$ est une base de $\mathcal{M}_{np}(\mathbb{K})$, en particulier* $\dim \mathcal{M}_{np} = np$.

4.2 Multiplication matricielle

4.2.1 Produit de deux matrices

Soit n, p, q trois entiers strictement positifs, A une matrice de $\mathcal{M}_{np}(\mathbb{K})$ et B une matrice de $\mathcal{M}_{pq}(\mathbb{K})$ (le nombre de colonnes de A est égal au nombre de lignes de B). Posons $A = (a_{ij})$ at $B = (b_{jk})$ (par commodité, on choisit de donner le même nom à l'indice de colonne de A et à l'indice de la ligne de B, qui parcourent le même ensemble $\{1,...,p\}$). On appelle produit des matrices A et B, la matrice $AB = (c_{ik}) \in \mathcal{M}_{nq}(\mathbb{K})$ (elle a le même nombre de lignes que A et le même nombre de colonnes que B) définie par

$$\forall (i,k) \in \{1,...,n\} \times \{1,...,q\} \quad c_{ik} = \sum_{j=1}^{p} a_{ij} b_{jk}.$$

Dans la pratique, pour calculer le coefficient de la $i-$ème ligne, $k-$ ième colonne de la matrice AB, on considère la $i-$ième ligne de A, la $k-$ ième colonne de B et on fait la somme de leurs produits terme à terme :

$$c_{ik} = a_{i1} b_{1k} + a_{i2} b_{2k} + ... + a_{in} b_{nk}.$$

De cette façon on peut multiplier en particulier un vecteur ligne avec un vecteur colonne :

$$(a_1\, a_2\, a_3 ... a_n) \begin{pmatrix} b_1 \\ b_1 \\ b_3 \\ . \\ . \\ . \\ b_n \end{pmatrix} = \sum_{i=1}^{n} a_i b_i.$$

Exemple 4.2.1

$$(1\,0\,3\,2) \begin{pmatrix} 2 \\ 1 \\ -1 \\ 2 \end{pmatrix} = 2 + 0 - 3 + 4 = 3.$$

Pour la multiplication de matrices, on peut adopter la disposition :

$$\begin{array}{cc} & \begin{pmatrix} b_{1k} \\ b_{2k} \\ . \\ \\ . \\ b_{pk} \end{pmatrix} \\ \begin{pmatrix} a_{i1} & a_{i2} & ... & a_{ip} \end{pmatrix} & \begin{pmatrix} c_{ik} \end{pmatrix} \end{array}$$

Exemple 4.2.2

$$\begin{pmatrix} 1 & -1 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 3 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & 4 & -2 \\ 11 & 8 & 1 \end{pmatrix}.$$

Lemme 4.2.1 *La multiplication matricielle est associative.*

Preuve plus tard.

4.2.2 Bilinéarité

Théorème 4.2.1 *Soit n, p, q trois entiers strictement positifs. Pour toute matrice fixée $A \in \mathcal{M}_{np}(\mathbb{K})$, l'application*

$$\begin{cases} \mathcal{M}_{pq}(\mathbb{K}) & \to & \mathcal{M}_{nq}(\mathbb{K}), \\ B & \mapsto & AB \end{cases}$$

est linéaire. Pour toute matrice $B \in \mathcal{M}_{pq}(\mathbb{K})$ fixée l'application

$$\begin{cases} \mathcal{M}_{np}(\mathbb{K}) & \to & \mathcal{M}_{nq}(\mathbb{K}), \\ A & \mapsto & AB \end{cases}$$

est linéaire.

Admis.

Remarque 4.2.1 *On dit que l'application*

$$\left\{ \begin{array}{rcl} \mathcal{M}_{np}(\mathbb{K}) \times \mathcal{M}_{pq}(\mathbb{K}) & \to & \mathcal{M}_{nq}(\mathbb{K}), \\ A & \mapsto & AB \end{array} \right.$$

est bilinéaire.

4.3 Anneau des matrices carrées d'ordre n

4.3.1 Structure de $\mathcal{M}_n(\mathbb{K})$

L'ensemble des matrices carrées d'ordre n, $\mathcal{M}_n(\mathbb{K})$, est muni de deux opérations internes.

– L'addition :

$$\left\{ \begin{array}{rcl} \mathcal{M}_n(\mathbb{K})^2 & \to & \mathcal{M}_n(\mathbb{K}) \\ (A, B) & \to & A + B. \end{array} \right.$$

$\mathcal{M}_n(\mathbb{K})$ muni de cette opération est un groupe commutatif.

– La multiplication de matrices

$$\left\{ \begin{array}{rcl} \mathcal{M}_n(\mathbb{K})^2 & \to & \mathcal{M}_n(\mathbb{K}) \\ (A, B) & \to & AB. \end{array} \right.$$

Nous avons que cette opération est associative et, du fait de la bilinéarité, distributive par rapport à l'addition de $\mathcal{M}_n(\mathbb{K})$. Elle admet pour élément neutre la matrice

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

appelée matrice unité d'ordre n.

Lemme 4.3.1 $(\mathcal{M}_n(\mathbb{K}), +, \times)$ *est un anneau.*

Remarque 4.3.1 *i) La multiplication dans $\mathcal{M}_n(\mathbb{K})$ n'est pas commutative (sauf si $n = 1$). Par exemple*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

En particulier, il faudra prendre garde à n'appliquer la formule du binôme qu'à la somme de deux matrices qui commutent.

ii) Il existe dans $\mathcal{M}_n(\mathbb{K})$ des diviseurs de zéro, c.à.d. des matrices non nulles dont le produit peut être nul.

Exemple *:*

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

Il existe aussi des matrices carrées nilpotentes, c.à.d. des matrices dont une puissance est nulle :

Exemple *:*

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

4.3.2 Elements inversibles de $\mathcal{M}_n(\mathbb{K})$

Une matrice carrée $A \in \mathcal{M}_n(\mathbb{K})$ est dite inversible s'il existe une matrice $A^{-1} \in \mathcal{M}_n(\mathbb{K})$ telle que

$$AA^{-1} = A^{-1}A = I_n.$$

Comme dans tout anneau, on sait que l'ensemble des éléments inversibles de $\mathcal{M}_n(\mathbb{K})$ est un groupe multiplicatif. On l'appelle groupe linéaire et il est noté $\mathcal{GL}_n(\mathbb{K})$.

Théorème 4.3.1 *Une matrice carrée de $\mathcal{M}_n(\mathbb{K})$ est inversible si et seulement si elle est inversible à droite ou inversible à gauche.*

Preuve

Il est clair que si A est inversible, elle est inversible àÂ gauche et àÂ droite. Supposons que A est invsersible à gauche, c.à.d.

$$\exists A' \in CM_n(\mathbb{K}) \quad A'A - I_n.$$

Soit f_A l'application

$$f_A : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \to & \mathcal{M}_n(\mathbb{R}), \\ X & \mapsto & AX \end{array} \right.$$

f_A est un endormophisme de l'espace vectoriel $\mathcal{M}_n(\mathbb{K})$. Or :

$$X \in \operatorname{Ker} f_A \Rightarrow AX = 0 \Rightarrow A'AX = 0 \Rightarrow X = 0.$$

f_A est injectif, et comme c'est un endomorphisme d'un espace vectoriel de dimension finie, il est bijectif. La matrice I_n possède alors un antécédent $A'' \in \mathcal{M}_n(\mathbb{K})$ telle que $AA'' = I_n$. A est donc inversible à droite (ce qui implique que ses invserses à gauche et à droite sont égaux). On procède de même en supposant que A est inversible à droite. □

4.4 Matrice d'une application linéaire

4.4.1 Représentation matricielle d'une famille de vecteurs

Soit E un $\mathbb{K}-$ espace vectoriel de dimension $n \geq 1$, muni d'une base $b = (e_1, e_2, e_3, ..., e_n)$. On peut représenter un vecteur x de E par la matrice unicolonne, notée $M_b(x)$, formée par

ses coordonnées dans la base b :

$$\text{Si} \quad x = \sum_{i=1}^{n} \xi_i e_i, \quad M_b(x) = X = \begin{pmatrix} \xi_1 \\ \xi_2 \\ . \\ . \\ . \\ \xi_n \end{pmatrix}.$$

Plus généralement, on peut représenter une famille de p vecteurs de E ($p \in \mathbb{N}^*$) par la matrice de type (n, p) dont la j-ième colonne représente les coordonnées du $j-$ième vecteur de la famille dans la base b :

$$\text{Si} \quad x_j = \sum_{i=1}^{n} \xi_{ij} e_i, \quad M_b(x_1, ..., x_p) = \begin{pmatrix} \xi_{11} & \xi_{12} & ... & \xi_{1p} \\ \xi_{21} & \xi_{22} & ... & \xi_{2p} \\ ... & ... & ... & ... \\ \xi_{n1} & \xi_{n2} & ... & \xi_{np} \end{pmatrix}.$$

4.4.2 Représentation matricielle d'une application linéaire

Soit E un $\mathbb{K}-$ espace vectoriel de dimansion $p \geq 1$, muni d'une base $b = (e_1, ..., e_p)$ et F un $\mathbb{K}-$ espace vectoriel de dimension $n \geq 1$, muni d'une base $b' = (e'_1, ..., e'_n)$. Une application linéaire f de E dans F est caractérisée par l'image de la base b, c.à.d. par la famille de p vecteurs de F :

$$(f(e_1), ..., f(e_p)).$$

D'après ce qui précède, on peut représenter cette famille par une matrice de $\mathcal{M}_{np}(\mathbb{K})$ que l'on appelle matrice de f relativement au système de bases (b, b') et que nous noterons $M^b_{b'}(f)$:

$$\forall j \in \{1, ..., p\} \quad f(e_j) = \sum_{i=1}^{n} a_{ij} e'_i, \quad M^b_{b'}(f) = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1p} \\ a_{21} & a_{22} & ... & a_{2p} \\ ... & ... & ... & ... \\ a_{n1} & a_{n2} & ... & a_{np} \end{pmatrix}.$$

Réciproquement, toute matrice de $\mathcal{M}_{np}(\mathbb{K})$ définit une application linéaire, et une seule, d'un espace vectoriel de dimension p dans un espace vectoriel de dimension n munis chacun d'une base.

Lemme 4.4.1 *Soient E un $\mathbb{K}$ espace vectoriel de dimension p muni d'une base b et F un $\mathbb{K}-$ espace vectoriel mundi d'une base b'. Alors l'application*

$$\begin{cases} \mathcal{L}(E, F) & \to & \mathcal{M}_{np}(\mathbb{K}) \\ f & \mapsto & M^b_{b'}(f) \end{cases}$$

est bijective.

En particulier une matrice $A \in \mathcal{M}_{np}$ représente une unique application linéaire de $\mathbb{K}^p$ dans $\mathbb{K}^n$ relativement aux bases canoniques de ces espaces vectoriels ; on l'appelle application linéaire canoniquement associée à A.

Exemple 4.4.1 *Soit*

$$f : \left\{ \begin{array}{ccc} \mathbb{R}_2[X] & \to & \mathbb{R}_3[X] \\ P & \mapsto & (X+1)P - P'. \end{array} \right.$$

Soit $b = (X^2, X, 1)$ *la base canonique de* $\mathbb{R}_2[X]$ *et* $b' = (X^3, X^2, X, 1)$ *celle de* $\mathbb{R}_3[X]$. *On a*

$$f(X^2) = X^3 + X^2 - 2X, \quad f(X) = X^2 + X - 1, \quad f(1) = X + 1.$$

Donc

$$M^b_{b'}(f) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ -2 & 1 & 1 \\ 0 & -1 & 1 \end{pmatrix}.$$

4.4.3 Expression matricielle de l'application linéaire

- E $\mathbb{K}-$ espace vetoriel de dimension p muni d'une base $b = (e_1, ..., e_p)$.
- F $\mathbb{K}-$ espace vetoriel de dimension n muni d'une base $b = (e_1, ..., e_n)$.
- $f \in \mathcal{L}(E, F)$.
- $M^b_{b'}(f) =: A$.
- $X = M_b(x) = \begin{pmatrix} \xi_1 \\ \xi_2 \\ . \\ . \\ . \\ \xi_p \end{pmatrix}$, $\quad x = \sum_{i=1}^{p} \xi_j e_j$.

On a

$$f(x) = \sum_{j=1}^{p} \xi_j f(e_j) = \sum_{j=1}^{p} \sum_{i=1}^{n} a_{ij} e'_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{p} a_{ij} \right) e'_i.$$

La matrice représentant le vecteur $f(x)$ dans la base b' est donc :

$$Y = M_{b'}(f(x)) = \begin{pmatrix} y_1 \\ y_2 \\ . \\ . \\ . \\ y_n \end{pmatrix} \quad \text{où} \quad y_i = \sum_{j=1}^{p} a_{ij} \xi_j.$$

On reconnaˆit la définition d'un produit de matrices

$$Y = AX$$

L'effet de l'application linéaire f revient donc pour les matrices unicolonnes représentant les vecteurs à une multiplication à gauche par la matrice A.

4.4.4 Matrice de la somme de deux applications linéaires

Soit f et g deux applications linéaires de E dans F, représentées respectivement par les matrices A et B relativement aux bases b et b'.

$$\begin{array}{rcl} \forall x \in E \quad (f+g)(x) & = & f(x)+g(x), \quad \text{soit matriciellement} \\ Y & = & AX+BX=(A+B)X. \end{array}$$

La matrice représentant $f+g$ dans les bases b et b' étant unique, c'est nécessairement $A+B$.

$$M_{b'}^{b}(f+g) = M_{b'}^{b}(f) + M_{b'}^{b}(g).$$

On montre de même que, pour tout scalaire α :

$$M_{b'}^{b}(\alpha f) = \alpha M_{b'}^{b}(f).$$

Lemme 4.4.2

$$\left\{ \begin{array}{rcl} \mathcal{L}(E,F) & \to & \mathcal{M}_{np}(\mathbb{K}) \\ f & \mapsto & M_{b'}^{b}(f) \end{array} \right.$$

est un isomorphisme.

On a en particulier l'égalité des dimensions :

$$\dim \mathcal{L}(E,F) = \dim \mathcal{M}_{np}(\mathbb{K}) = np.$$

4.4.5 Matrice de la composée de deux applications linéaires

- E $\mathbb{K}-$ espace vectoriel de dimension $p \geq 1$, muni d'une base b.
- F $\mathbb{K}-$ espace vectoriel de dimension $n \geq 1$, muni d'une base b'.
- G $\mathbb{K}-$ espace vectoriel de dimension $q \geq 1$, muni d'une base b''.
- $f \in \mathcal{L}(E,F) \quad A = M_{b'}^{b}(f), \quad g \in \mathcal{L}(F,G) \quad B = M_{b''}^{b'}(g)$.

Soit $x \in E$, tel que $M_b(x) = X$. Alors

$$M_{b'}(f(x)) = Y = AX \quad \text{et} \quad M_{b''}(g \circ f(x)) = Z = BY = BAX.$$

La matrice représentant $g \circ f$ dans les bases b et b'' étant unique, c'est nécessairement BA :

$$M_{b''}^{b}(g \circ f) = M_{b''}^{b'}(g) M_{b'}^{b}(f). \tag{4.4.1}$$

Remarque 4.4.1 *La multiplication des matrices est définie telle que* (4.4.1) *soit vérifiée. L'associativité de la multiplication des matrices vient alors de l'associativité de la composition d'applications.*

4.4.6 Matrice carrée d'un isomorphisme

Si f est un isomorphisme de E dans F (ce qui n'est possible que si $\dim E = \dim F$), on a

$$f \circ f^{-1} = Id_F, \quad f^{-1} \circ f = Id_E.$$

D'où :

$$M_{b'}^{b}(f) M_{b}^{b'}(f^{-1}) = N_{b}^{b'}(Id_F) = I_n, \quad M_{b}^{b'}(f^{-1}) M_{b'}^{b}(f) = M_{b}^{b}(Id_E) = I_n.$$

On en déduit que la matrice $M_{b'}^{b}(f)$ est inversible et

$$(M_{b'}^{b}(f))^{-1} = M_{b}^{b'}(f^{-1}).$$

4.4.7 Matrice carrée d'un endomorphisme

Soit $u \in \mathcal{L}(E)$. On choisit la même base dans E en tant qu'espace de départ et en tant qu'espace d'arrivée. Soit $M_b(u) = M_b^b(u)$. L'application

$$\begin{cases} \mathcal{L}(E) & \to & \mathcal{M}_n(\mathbb{K}) \\ u & \mapsto & M_b(u) \end{cases}$$

est un isomorphisme d'espaces vectoriels et d'anneaux. u est un automorphisme de E ssi la matrice $M_b(u)$ est inversible et

$$(M_b(u))^{-1} = M_b(u^{-1}).$$

Terminologie
- groupe linéaire de E : ensemble des automorphismes de E.
- groupe linéaire d'ordre n de $\mathbb{K}$: ensemble des matrices inversibles d'ordre n.

L'application

$$\begin{cases} \mathcal{GL}(E) & \to & \mathcal{GL}(\mathbb{K}) \\ u & \mapsto & M_b(u) \end{cases}$$

est un isomorphisme de groupes.

4.5 Changement de bases

4.5.1 Effet d'un changement de bases sur les coordonnées d'un vecteur

Soit E un $\mathbb{K}-$ espace vectoriel de dimension $n \geq 1$, muni de deux bases $b = (e_1, ..., e_n)$ et $b' = (e'_1, ..., e'_n)$. Soit x un vecteur de E ; on peut le représenter dans chacune des bases par une matrice unicolonne :

$$\begin{aligned} \text{Si} \quad x &= \sum_{i=1}^{n} \xi e_i = \sum_{i=1}^{n} \xi'_i e'_i, \\ M_b(x) &= X = \begin{pmatrix} \xi_1 \\ . \\ . \\ . \\ \xi_n \end{pmatrix} \quad \text{et} \quad M_{b'}(x) = X' = \begin{pmatrix} \xi'_1 \\ . \\ . \\ . \\ \xi'_n \end{pmatrix}. \end{aligned}$$

Comme $x = Id_E(x)$, on peut écrire $M_b(x) = M_b^{b'}(Id_E)M_{b'}(x)$, c.à.d.

$$X = PX',$$

où P est la mtrice représenant l'identité de E relativement aux bases b' au départ et b à l'arrivée.
- La $j-$ème colonne de P représente les coordonnées de e'_j dans la base b.
- Cette matrice P est appelée matrice de passage de la base b à la base b' (attention à l'ordre !).

– Comme elle représente l'identité, une matrice de passage est inversible. L'inverse de la matrice de passage de b à b' est la matrice de passage de b' à b. Réciproquement, toute matrice de $\mathcal{GL}_n(\mathbb{K})$ peut être considérée comme la matrice de passage de la base canonique de $\mathbb{K}^n$ dans la base constituée des vecteurs colonnes.

Exemple 4.5.1 *Soit dans l'espace vectoriel $\mathbb{R}_3[X]$ les bases :*

$$b(X^3, X^2, X, 1), \quad b' = ((X-1)^3, (X-1)^2, X-1, 1).$$

Note que b' est une base parce qu'elle a quatre éléments de degrés tous distincts (voir Exercice 3.1.2). La matrice de passage de b à b' est :

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 3 & -2 & 1 & 0 \\ -1 & 1 & -1 & 1 \end{pmatrix}.$$

Soit un polynôme :

$$\begin{aligned} Q &= aX^3 + bX^2 + cX + d = a'(X-1)^3 + b'(X-1)^2 + c'(X-1) + d' \\ \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 3 & -2 & 1 & 0 \\ -1 & 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix}. \end{aligned}$$

4.5.2 Effet d'un changement de base sur la matrice d'une application linéaire

Soit E un $\mathbb{K}-$ espace vectoriel muni de deux bases b_1 et b'_1, P la matrice de passage de b_1 à b'_1, et F un $\mathbb{K}-$ espace vectoriel muni de deux bases b_2 et b'_2, Q la matrice de passage de b_2 à b'_2. Soit f une application linéaire de E dans F ; on peut la représenter matriciellement dans chacun des systèmes de bases :

$$A = M_{b_2}^{b_1}(f) \quad A' = M_{b'_2}^{b'_1}(f).$$

En remarquant que $f = Id_F \circ f \circ Id_E$, on peut écrire

$$M_{b'_2}^{b'_1} = M_{b'_2}^{b_2}(Id_F) M_{b_2}^{b_1}(f) M_{b_1}^{b'_1}(Id_E),$$

c.à.d.

$$A' = Q^{-1}AP.$$

Définition 4.5.1 *Deux matrices A et A' de $\mathcal{M}_{np}(\mathbb{K})$, telles qu'il existe $P\mathcal{GL}_p(\mathbb{K})$ et $Q \in \mathcal{GL}_n(\mathbb{K})$ vérifiant $A' = Q^{-1}AP$ sont dites <u>équivalentes</u>.*

Remarque 4.5.1 *En intreprétant P et Q comme des matrices de passage, on voit que deux matrices sont équivalentes ssi elles représentent une même application linéaire dans des bases différentes.*

4.5.3 Effet d'un changement de bases sur la matrice d'un endomorphisme

Soit E un $\mathbb{K}-$ espace vectoriel muni de deux bases b et b', et P la matrice de passage de b à b'. Soit $u \in \mathcal{L}(E)$; on peut le représenter matriciellement dans chacune des bases (en choisissant à chaque fois la mme base pour E en tant qu'espace de départ et en tant qu'espace d'arrivée).

$$A = M_b(u) \quad A' = M_{b'}(u).$$

On peut reprendre le même calcul que pour une application linéaire quelconque, en remarquant qu'ici $Q = P$. D'où

$$A' = P^{-1}AP.$$

Définition 4.5.2 *Deux matrices A et A' de $\mathcal{M}_n(\mathbb{K})$, telles qu'il existe $P \in \mathcal{GL}_n(\mathbb{K})$ vérifiant $A' = P^{-1}AP$, sont dites semblables.*

4.6 Transposition

4.6.1 Transposée d'une matrice

Soit $A \in \mathcal{M}_{np}(\mathbb{K})$. On appelle transposée de A la matrice de $\mathcal{M}_{pn}(\mathbb{K})$ dont les lignes sont les colonnes de A et vice versa. Si

$$A = (a_{ij}), \quad {}^tA = (a'_{ij}), \quad \text{où} \quad \forall (i,j) \in \{1,...,p\} \times \{1,...,n\} \quad a'_{ij} = a_{ji}.$$

Exemple :

$${}^t\begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}.$$

Théorème 4.6.1 *L'application*

$$\begin{cases} \mathcal{M}_{np}(\mathbb{K}) & \to & \mathcal{M}_{pn}(\mathbb{K}), \\ A & \mapsto & {}^tA \end{cases}$$

est un isomorphisme d'espaces vectoriels.

Preuve

On montre facilement que cette application est linéaire :

$$\forall (A,B) \in \mathcal{M}_n(\mathbb{K})^2 \quad \forall (\alpha,\beta) \in \mathbb{K}^2 \quad {}^t(\alpha A + \beta B) = \alpha {}^tA + \beta {}^tB.$$

Par ailleurs, toute matrice C de $\mathcal{M}_{pn}(\mathbb{K})$ est la transposée d'une unique matrice de $\mathcal{M}_{np}(\mathbb{K})$, qui est ${}^tC$:notre application est donc bijective. □

4.6.2 Transposée d'un produit

Théorème 4.6.2 *Pour toutes matrices $A \in \mathcal{M}_{np}(\mathbb{K})$ et $B \in \mathcal{M}_{pq}(\mathbb{K})$:*

$${}^t(AB) = {}^tB\,{}^tA.$$

Remarque 4.6.1 *Attention à l'ordre !*

Admis.

Corollaire 4.6.1 *La transposée d'une matrice carrée inversible est inversible et :*

$$^t(A^{-1}) = (^tA)^{-1}.$$

Preuve

Soit $A \in \mathcal{GL}_n(\mathbb{K})$. En transposant l'égalité $AA^{-1} = A^{-1}A = I_n$, on obtient :

$$^t(A^{-1})^tA = {}^tA^t(A^{-1}) = {}^tI_n = I_n.$$

$^t(A^{-1})$ est donc l'inverse de ^tA. □

4.6.3 Matrices carrées symétriques et antisymétriques

Soit $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$ une matrice carrée. A est dite symétrique si $^tA = A$, c.à.d. si

$$\forall (i,j) \in \{1,...,n\}^2 \quad a_{ij} = a_{ji}.$$

Les coefficients symétriques par rapport à la diagonale sont égaux. A est dite antisymétrique si $^tA = -A$, c.à.d. si

$$\forall (i,j) \in \{1,...,n\}^2 \quad a_{ij} = -a_{ji}.$$

Les coefficents symétriques par rapport à la diagonale sont opposés ; en particulier les coefficients diagonuax sont nuls.

Théorème 4.6.3 *L'ensemble $\mathcal{S}_n(\mathbb{K})$ des matrices symétriques et l'ensemble $\mathcal{A}_n(\mathbb{K})$ des matrices antisymétriques sont des sous-espaces vectoriels supplémentaires de $\mathcal{M}_n(\mathbb{K})$.*

Preuve

Soit T l'endororphisme de $\mathcal{M}_n(\mathbb{K}) : A \mapsto {}^tA$. On remarque que $\mathcal{S}_n(\mathbb{K})$ est le noyau de $T - Id$ et $\mathcal{A}_n(\mathbb{K})$ le noyau de $T + Id$. Ce sont donc bien des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$. Montrons que leur intersection est le singleton nul. Soit A une matrice carrée à la fois symétrique et antisymétrique : $^tA = A = -A$, d'où $A = 0$. Montrons ensuite que toute matrice carrée est la somme d'une matrice symétrique et d'une matrice antisymétrique :

$$\forall A \in \mathcal{M}_n(\mathbb{K}) \quad A = \frac{1}{2}(A + {}^tA) + \frac{1}{2}(A - {}^tA).$$

Or

$$\begin{aligned} {}^t(\frac{1}{2}(A + {}^tA)) &= \frac{1}{2}({}^tA + A) : \quad \text{la matrice } \tfrac{1}{2}(A + {}^tA) \text{ est symétrique.} \\ {}^t(\frac{1}{2}(A - {}^tA)) &= \frac{1}{2}({}^tA - A) : \quad \text{la matrice } \tfrac{1}{2}(A - {}^tA) \text{ est antisymétrique.} \end{aligned}$$

□

Remarque 4.6.2
- *T est la symétrie par rapport à $\mathcal{S}_N(\mathbb{K})$ parrallèlement à $\mathcal{A}_n(\mathbb{K})$.*
- *On a*

$$\dim \mathcal{S}_n(\mathbb{K}) = \frac{n(n+1)}{2}, \quad \dim \mathcal{A}_n(\mathbb{K}) = \frac{n(n-1)}{2}.$$