

Cours d'algèbre du second semestre de L1

(écrit par Jean-Yves Ducloux)

TABLE DES MATIÈRES

Ch. 1. Polynômes	
I. L'anneau $\mathbb{K}[X]$	1
II. Racines d'un polynôme	5
III. Fractions rationnelles	9
Ch. 2. Matrices sur $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}	
I. Systèmes linéaires	15
II. Calcul matriciel	21
Ch. 3. Espaces vectoriels sur $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}	
I. Règles de calcul	29
II. Constructions	31
III. Bases et dimension	35
Ch. 4. Applications linéaires sur $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}	
I. Applications linéaires	43
II. Utilisation des matrices	48

Sources :

- Liret et Martinais, *Mathématiques pour le DEUG. Algèbre 1^{ère} année*. Éd. Dunod. [512 LIR]
- E. Ramis, C. Deschamps, J. Odoux, Cours de mathématiques [51 L RAM] :
[512 RAM], [514 RAM], [515 RAM], [517 RAM], [517 RAM], niveau L1 seul dans [51 L1 RAM]
- R. L. Burden, J. D. Faires, *Numerical analysis*, ch. 6 [519.6 BUR].
- Marc Hindry, *Cours de Mathématiques, Première Année*. Université Paris 7.
(<http://www.imj-prg.fr/~marc.hindry/Cours-L1.pdf>)

Ch. 1. Polynômes

Plan

- I. L'anneau $\mathbb{K}[X]$
- II. Racines d'un polynôme
- III. Fractions rationnelles

Dans tout ce chapitre, \mathbb{K} désigne \mathbb{R} ou \mathbb{C} (ou plus généralement un « corps commutatif »).

I. L'ANNEAU $\mathbb{K}[X]$

1. Polynômes et fonctions polynomiales

Définition

(a) Un *polynôme à coefficients dans \mathbb{K}* est une suite $P = (a_k)_{k \geq 0}$ d'éléments de \mathbb{K} pour laquelle il existe $n \in \mathbb{N}$ tel que : $\forall k > n \quad a_k = 0$.

On le notera $P = a_n X^n + \dots + a_1 X + a_0$ au lieu de $(a_k)_{k \geq 0}$.

Les nombres a_0, a_1, \dots, a_n s'appellent les *coefficients de P* .

(b) À chaque polynôme $P = a_n X^n + \dots + a_1 X + a_0$ à coefficients dans \mathbb{K} , on associe l'application notée ici $f_P: \mathbb{K} \rightarrow \mathbb{K}$ définie par :

$$f_P(x) = \underbrace{a_n x^n + \dots + a_1 x + a_0}_{\text{noté } P(x)} \text{ pour tout } x \in \mathbb{K}.$$

Une *fonction polynomiale sur \mathbb{K}* est une application f de \mathbb{K} dans \mathbb{K} telle qu'il existe un polynôme P à coefficients dans \mathbb{K} pour lequel $f = f_P$.

(c) Le *degré* d'un polynôme $P = a_n X^n + \dots + a_1 X + a_0$ non nul, noté $\deg P$, est le plus grand $d \in \mathbb{N}$ tel que $a_d \neq 0$. Par convention on pose : $\deg 0 := -\infty$.

Remarque

Soit P un polynôme non-nul de degré d à coefficients dans \mathbb{R} :

$$P = a_d X^d + \dots + a_1 X + a_0 \text{ avec } a_0, \dots, a_d \in \mathbb{R} \text{ et } a_d \neq 0.$$

On a : $|P(x)| = |x|^d \left| a_d + \frac{a_{d-1}}{x} + \dots + \frac{a_0}{x^d} \right| \xrightarrow{x \rightarrow +\infty} +\infty$ si $d \geq 1$ et $\underbrace{P(0)}_{a_0} \neq 0$ si $d = 0$.

En particulier : $f_P \neq 0$. (On n'utilisera plus la notation « f_P ».)

Ainsi, lorsque $\mathbb{K} = \mathbb{R}$:

si une fonction polynomiale réelle $x \mapsto a_n x^n + \dots + a_1 x + a_0$ est nulle, alors $a_0 = \dots = a_n = 0$.

Notations

(a) On note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} .

Il contient \mathbb{K} vu comme ensemble des polynômes a_0 pour lesquels on peut choisir $n = 0$
« polynômes constants »

(b) Étant donné $N \in \mathbb{N}$, on note $\mathbb{K}_N[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} qui sont non-nuls de degré inférieur ou égal à N , ou nuls.

(La convention $\deg 0 = -\infty$ permet d'appeler $\mathbb{K}_N[X]$ l'ensemble des polynômes de degré $\leq N$.)

Ainsi : $\mathbb{K}_N[X] = \{a_N X^N + \dots + a_1 X + a_0 ; a_0, a_1, \dots, a_N \in \mathbb{K}\}$.

Définition

Soient $P = a_p X^p + \dots + a_1 X + a_0$ et $Q = b_q X^q + \dots + b_1 X + b_0$ deux éléments de $\mathbb{K}[X]$.

On prolonge les coefficients en posant : $a_k = 0$ pour $k > p$ et $b_l = 0$ pour $l > q$.

(a) On note : $P + Q := \sum_{k=0}^{\max(p,q)} (a_k + b_k) X^k$ ←-[suite $(a_k + b_k)_{k \geq 0}$]

(b) On note : $PQ := \sum_{k=0}^{p+q} \left(\sum_{i+j=k} a_i b_j \right) X^k$. ←[suite $(c_k)_{k \geq 0}$ avec $c_k = \sum_{i=0}^k a_i b_{k-i}$]

Concrètement :
$$PQ = \sum_{k=0}^{p+q} (a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0) X^k$$

$$= a_p b_q X^{p+q} + (a_p b_{q-1} + a_{p-1} b_q) X^{p+q-1} + \dots + a_0 b_0.$$

(c) Soit $\alpha \in \mathbb{K}$. On note : $\alpha P = (\alpha a_p) X^p + \dots + (\alpha a_1) X + (\alpha a_0)$. ←[suite $(\alpha a_k)_{k \geq 0}$]

Il s'agit du cas particulier du produit du polynôme constant α par P .

(d) Les puissances de P sont définies par récurrence : $P^0 = 1$ et $P^n = P^{n-1} P$ pour $n \geq 1$.

Remarque

On définit « l'indéterminée » X par : $X = (x_k)_{k \geq 0}$ où $x_0 = 0$, $x_1 = 1$ et $x_k = 0$ si $k \geq 2$.

Quand $P=X$, on a par récurrence sur $n \geq 0$: $P^n = (\delta_n(k))_{k \geq 0}$ avec $\delta_n(k) = \begin{cases} 1 & \text{si } k = n \\ 0 & \text{sinon} \end{cases}$.

Il en résulte qu'un polynôme $P = (a_k)_{k \geq 0}$ à coefficients dans \mathbb{K} avec $a_k = 0$ pour $k > n$ s'écrit effectivement $P = a_n X^n + \dots + a_1 X + a_0$ où X^k représente maintenant la puissance k^e de X qu'on vient de calculer.

Proposition

Soient $P, Q \in \mathbb{K}[X]$, $\alpha, x \in \mathbb{K}$ et $n \in \mathbb{N}$. On a posé $\deg 0 := -\infty$.

(a) On a : $(P + Q)(x) = P(x) + Q(x)$, $(PQ)(x) = P(x)Q(x)$, et $(\alpha P)(x) = \alpha P(x)$.

(b) On a : $\deg(P + Q) \leq \max(\deg(P), \deg(Q))$ et $\deg(PQ) = \deg(P) + \deg(Q)$.

(c) Si $PQ = 0$ alors $P = 0$ ou $Q = 0$.

(d) On a : $(P + Q)^n = \sum_{k=0}^n \binom{n}{k} P^{n-k} Q^k$ « formule du binôme de Newton ».

DÉMONSTRATION

(a) Immédiat.

(b) On suppose d'abord que $P = 0$ ou $Q = 0$. On a : $P + Q \in \{P, Q\}$ et $PQ = 0$.

Donc $\deg(P + Q) \in \{\deg(P), \deg(Q)\}$ et $\deg(PQ) = -\infty = \deg(P) + \deg(Q)$.

On suppose maintenant que $P \neq 0$ et $Q \neq 0$:

$$P = a_p X^p + \dots + a_1 X + a_0 \text{ avec } a_p \neq 0 \text{ et } Q = b_q X^q + \dots + b_1 X + b_0 \text{ avec } b_q \neq 0.$$

Donc $P + Q = (a_r + b_r) X^r + (a_{r-1} + b_{r-1}) X^{r-1} + \dots + (a_0 + b_0)$ en posant $r = \max(p, q)$ et $PQ = \underbrace{a_p b_q}_{\neq 0} X^{p+q} + (a_p b_{q-1} + a_{p-1} b_q) X^{p+q-1} + \dots + a_0 b_0$. Cela fournit le résultat.

(c) Si $PQ = 0$, alors $\deg(P) + \deg(Q) = -\infty$ d'après (b), puis $P = 0$ ou $Q = 0$.

(d) L'égalité se démontre par récurrence comme dans le cas de $(u + v)^n$ avec $u, v \in \mathbb{C}$. □

Définition

Soient $P = a_p X^p + \dots + a_1 X + a_0$ et Q deux éléments de $\mathbb{K}[X]$.

(a) On note : $P' = p a_p X^{p-1} + \dots + 2 a_2 X + a_1 \in \mathbb{K}[X]$.

On définit les dérivées successives par récurrence : $P^{(0)} = P$ et $P^{(n)} = (P^{(n-1)})'$ pour $n \geq 1$.

(b) On note : $P(Q) = a_p Q^p + \dots + a_1 Q + a_0 \in \mathbb{K}[X]$.

Exemple

On prend $P = X^2 + X + 1$ et $Q = X^2$.

On a : $P' = 2X + 1$ et $P(X^2) = (X^2)^2 + (X^2) + 1 = X^4 + X^2 + 1$.

On a aussi : $P(X) = X^2 + X + 1 = P$.

Proposition

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

(a) On a : $(\alpha P + \beta Q)' = \alpha P' + \beta Q'$.

(b) On a : $(PQ)^{(n)} = \sum_{k=0}^n \binom{n}{k} P^{(n-k)} Q^{(k)}$ « formule de Leibniz ».

DÉMONSTRATION

Exercice. □

Définition-Proposition

(a) Une *loi de composition* sur un ensemble E est une application $\star: E \times E \rightarrow E$.
Suivant l'usage, on notera ici $x \star y$ l'image par \star de (x, y) .

(b) Un *anneau* est un triplet $(A, +, \times)$, où A est un ensemble, $+$ et \times sont des lois de composition sur A , avec

- (i) $(x + y) + z = x + (y + z)$ pour tous $x, y, z \in A$;
- (ii) il existe $0_A \in A$ tel que pour tout $x \in A$, on a : $0_A + x = x + 0_A = x$;
- (iii) pour tout $x \in A$ il existe $x' \in A$ tel que : $x + x' = x' + x = 0_A$;
- (iv) $x + y = y + x$ pour tous $x, y \in A$;
- (v) $(x \times y) \times z = x \times (y \times z)$ pour tous $x, y, z \in A$;
- (vi) $x \times (y + z) = (x \times y) + (x \times z)$ et $(x + y) \times z = (x \times z) + (y \times z)$ pour $x, y, z \in A$;
- (vii) il existe $1_A \in A$ tel que pour tout $x \in A$, on a : $1_A \times x = x \times 1_A = x$.

Dans ce cas, l'élément 0_A du (ii) est unique (immédiat) appelé *zéro de $(A, +)$* , pour chaque $x \in A$ l'élément x' de A du (iii) est unique (admis) appelé *opposé de x* et noté $-x$, l'élément 1_A du (vii) est unique (immédiat) et appelé *élément unité de A* .

(c) On dit qu'un anneau $(A, +, \times)$ est *commutatif* si pour tous $x, y \in A$, on a : $x \times y = y \times x$.

(d) Un *corps* est un anneau $(K, +, \times)$ qui vérifie :

$$K \neq \{0\} \text{ et pour tout } x \in K \setminus \{0\} \text{ il existe } x' \in K \text{ tel que } x \times x' = x' \times x = 1_K.$$

Dans ce cas, pour chaque $x \in K \setminus \{0\}$ l'élément x' de K est unique (admis) et noté x^{-1} .

DÉMONSTRATION

Vérification des unicités annoncées : exercice. □

Proposition

(a) L'ensemble $\mathbb{K}[X]$ muni de l'addition et de la multiplication des polynôme est un anneau commutatif de zéro le polynôme 0 et d'élément unité le polynôme constant 1.

(b) Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ munis des lois $+$ et \times usuelles sont des corps commutatifs.

DÉMONSTRATION

Exercice. □

2. Division euclidienne

Définition

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

On dit que B *divise* A (ou A *est multiple de* B), et note $B \mid A$, si :

$$\text{il existe } Q \in \mathbb{K}[X] \text{ tel que } A = BQ.$$

Quand $B \neq 0$ et B ne divise pas A , on va disposer du reste dans la division de A par B :

Théorème

Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$.

Il existe un unique $(Q, R) \in \mathbb{K}[X]^2$ tel que :

$$A = BQ + R \text{ et } \deg R < \deg B \quad \text{« division euclidienne de } A \text{ par } B \text{ ».}$$

Dans ce cas, R s'appelle *le reste* et Q s'appelle *le quotient*, de la division de A par B .

II. RACINES D'UN POLYNÔME

1. Racines avec leur multiplicité

Définition

Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$.

On dit que r est racine de P (ou zéro de la fonction $x \mapsto P(x)$) si $P(r) = 0$.

Exemple

• Quelles sont les racines « évidentes » (rationnelles) du polynôme réel $2X^3 - 5X^2 - 3X + 9$?

• On considère plus généralement : $P = a_n X^n + \dots + a_1 X + a_0$ où $n \geq 1$ et $a_0, \dots, a_n \in \mathbb{Z}$.

On suppose que $r = \frac{p}{q} \in \mathbb{Q}$ vérifie $P(r) = 0$ avec p et q de seuls diviseurs communs -1 et 1 .

On a : $a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$

$$\text{donc } \begin{cases} a_0 q^n = p(-a_n p^{n-1} - \dots - a_1 q^{n-1}) & \text{puis } p \mid a_0 q^n \\ a_n p^n = q(-a_{n-1} p^{n-1} - \dots - a_0 q^{n-1}) & \text{puis } q \mid a_n p^n \end{cases}$$

donc, par le lemme de Gauss : $p \mid a_0$ et $q \mid a_n$.

• Les racines rationnelles de $2X^3 - 5X^2 - 3X + 9$ sont dans $\{\pm 1, \pm 3, \pm 9, \pm \frac{1}{2}, \pm \frac{3}{2}, \pm \frac{9}{2}\}$. On constate que $\frac{3}{2}$ est effectivement une racine de $2X^3 - 5X^2 - 3X + 9$.

Proposition

Soient $P \in \mathbb{K}[X]$ et $r \in \mathbb{K}$.

On a : r est racine de P si et seulement si $X - r$ divise P .

DÉMONSTRATION

(\Leftarrow) On suppose que $X - r$ divise P .

Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)Q$. Donc $P(r) = 0$.

(\Rightarrow) On suppose que $P(r) = 0$.

Division euclidienne : $P = (X - r)Q + R$ avec $(Q, R) \in \mathbb{K}[X]^2$ et $\deg R < 1$.

Donc $P(r) = R(r)$ et R est constant. D'où $R = 0$, ce qui montre que $X - r$ divise P . \square

Corollaire

Un polynôme non-nul $P \in \mathbb{K}[X] \setminus \{0\}$ de degré n a au plus n racines dans \mathbb{K} .

(On verra plus tard que quand P a n racines comptées avec multiplicité $(x_1, \alpha_1), \dots, (x_p, \alpha_p)$, où $p \in \mathbb{N}$ et $\alpha_1, \dots, \alpha_p \in \mathbb{N} \setminus \{0\}$ vérifient $\alpha_1 + \dots + \alpha_p = n$, il existe $\lambda \in \mathbb{K} \setminus \{0\}$ tel que :
$$P = \lambda(X - x_1)^{\alpha_1} \dots (X - x_p)^{\alpha_p}.$$

DÉMONSTRATION

Récurrence sur $n \in \mathbb{N}$.

(i) Si $n = 0$: P est constant non-nul donc n'a pas de racine.

(ii) Soit $n \geq 0$ tel que tout polynôme non-nul de degré n a au plus n racines.

On se donne un polynôme non-nul P de degré $n + 1$. On suppose que P possède au moins une racine r (sinon il n'y a rien à faire). Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)Q$. On applique l'hypothèse de récurrence à Q et constate que P a au plus $n + 1$ racines.

(iii) D'où le résultat. \square

Remarque

On suppose ici que $\mathbb{K} = \mathbb{R}$ ou \mathbb{C} (*).

Soit $P \in \mathbb{K}[X] \setminus \{0\}$. En notant $d = \deg P$, le polynôme P a au plus d racines. En particulier, comme on l'a déjà vu dans le cas réel, l'application $f_P : x \in \mathbb{K} \mapsto P(x) \in \mathbb{K}$ est non-nulle.

Par contre quand \mathbb{K} est fini, le polynôme non-nul $P := \prod_{x \in \mathbb{K}} (X - x)$ vérifie $f_P = 0$.

(*) (ou plus généralement que \mathbb{K} est un corps commutatif infini)

Définition-Proposition

Soient $P \in \mathbb{K}[X] \setminus \{0\}$ et $r \in \mathbb{K}$.

(a) On appelle *ordre de multiplicité de r dans P* l'unique $m \in \mathbb{N}$ tel que :

$$(X - r)^m \text{ divise } P \quad \text{et} \quad (X - r)^{m+1} \text{ ne divise pas } P \text{ (existe).}$$

$m \geq 1$: « r est racine de P » ;

$m = 1$: « r est racine simple de P » ;

$m = 2$: « r est racine double de P » ;

$m \geq 2$: « r est racine multiple de P ».

(b) Lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}^{(**)}$ l'ordre de multiplicité m de r dans P est caractérisé par :

$$P(r) = P'(r) = \dots = P^{(m-1)}(r) = 0 \quad \text{et} \quad P^{(m)}(r) \neq 0.$$

En particulier, on a : $m \geq 2 \iff P(r) = P'(r) = 0$.

Par convention : l'ordre de multiplicité de r dans 0 est $+\infty$ (dérivées de 0 nulles en r).

DÉMONSTRATION

(a) Le polynôme $(X - r)^0$ divise P et $(X - r)^k$ ne divise pas P quand $k > \deg P$.

Ainsi il existe un plus grand $m \in \mathbb{N}$ tel que $(X - r)^m$ divise P .

(b) On suppose que $\underbrace{1 + \dots + 1}_{n \text{ fois}} \neq 0$ pour tout $n \in \mathbb{N} \setminus \{0\}$ (par exemple $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}).

On montre $P(r) = P'(r) = \dots = P^{(m-1)}(r) = 0$ et $P^{(m)}(r) \neq 0$ (ce qui déterminera m).

Il existe $Q \in \mathbb{K}[X]$ tel que $P = (X - r)^m Q$. Donc $Q(r) \neq 0$ car $(X - r)^{m+1}$ ne divise pas P .

Formule de Leibniz : $((X - r)^m Q)^{(p)} = \sum_{k=0}^p \binom{p}{k} \underbrace{((X - r)^m)^{(k)}}_{m \cdots (m-k+1)(X-r)^{m-k}} Q^{(p-k)}$ pour $p \in \{0, \dots, m\}$.

D'où : $P(r) = P'(r) = \dots = P^{(m-1)}(r) = 0$ et $P^{(m)}(r) = \underbrace{m! Q(r)}_{\neq 0}$. □

Exemple ($\mathbb{K} = \mathbb{R}$ ou \mathbb{C})

On prend $P = X^3 + pX + q$ avec $p, q \in \mathbb{K}$.

La division euclidienne de P par P' donne : $P = P' \times (\frac{1}{3}X) + \frac{2}{3}pX + q$. D'où, pour $r \in \mathbb{K}$:

$$\begin{cases} P(r) = 0 \\ P'(r) = 0 \end{cases} \iff \begin{cases} \overbrace{P'(r)}^{3r^2+p} = 0 \\ \frac{2}{3}pr + q = 0 \end{cases} \iff \begin{cases} pr = -\frac{3}{2}q \\ 3r^2 + p = 0 \end{cases} \iff \left(\begin{cases} p \neq 0 \\ r = -\frac{3q}{2p} \\ 3(-\frac{3q}{2p})^2 + p = 0 \end{cases} \text{ ou } \begin{cases} p = 0 \\ q = 0 \\ r = 0 \end{cases} \right).$$

Ainsi P a une racine multiple dans \mathbb{K} si et seulement si : $4p^3 + 27q^2 = 0$.

2. Polynômes irréductibles

Définition

Un *polynôme irréductible à coefficients dans \mathbb{K}* est un élément P de $\mathbb{K}[X]$ non-constant tel que les seules égalités $P = AB$ avec $A, B \in \mathbb{K}[X]$ s'obtiennent quand A ou B est constant.

Remarques (immédiates)

1. Tout polynôme de degré 1 est irréductible.

(Si $\deg P = 1$ et $P = AB$, on a : $\deg A + \deg B = 1$ donc $\deg A = 0$ ou $\deg B = 0$.)

2. Un polynôme à coefficients dans \mathbb{K} de degré 2 ou 3 est irréductible si et seulement si il n'a aucune racine dans \mathbb{K} .

$$\left(\begin{array}{l} \text{Si } \deg P \in \{2, 3\} \text{ et } P = AB \text{ avec } A \text{ et } B \text{ non-constants :} \\ \underbrace{\deg A}_{\geq 1} + \underbrace{\deg B}_{\geq 1} \leq 3 \text{ donc } A \text{ ou } B \text{ est de degré 1 de la forme } \lambda(X - r) \text{ avec } \lambda, r \in \mathbb{K}. \\ \text{Si } \deg P \in \{2, 3\} \text{ et } P = (X - r)C \text{ avec } r \in \mathbb{K} \text{ et } C \in \mathbb{K}[X] : \\ \deg(X - r) = 1 \text{ et } \deg C \in \{1, 2\} \text{ donc } X - r \text{ et } C \text{ sont non-constants.} \end{array} \right)$$

(**) (ou plus généralement quand \mathbb{K} est un corps commutatif dans lequel $\underbrace{1 + \dots + 1}_{n \text{ fois}} \neq 0$ pour tout $n \in \mathbb{N} \setminus \{0\}$)

- Par exemple :
- $X^2 + 1$ n'est pas irréductible dans $\mathbb{C}[X]$;
 - $X^2 + 1$ est irréductible dans $\mathbb{R}[X]$ et dans $\mathbb{Q}[X]$;
 - $X^2 - 2$ n'est pas irréductible dans $\mathbb{R}[X]$;
 - $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$ (exemple du début du paragraphe 1).

Proposition

- (a) Soient $A, B \in \mathbb{K}[X]$ sans diviseur commun non constant.
 Il existe $U, V \in \mathbb{K}[X]$ tels que $AU + BV = 1$ « théorème de Bézout ».
- (b) Soient $A, B \in \mathbb{K}[X]$ et $P \in \mathbb{K}[X]$ irréductible.
 Si $P \mid AB$, alors $P \mid A$ ou $P \mid B$ « lemme d'Euclide ».

DÉMONSTRATION

(a) Tout d'abord : $A \neq 0$ et $B \neq 0$. On raisonne par récurrence sur $n := \deg A + \deg B$.

(i) Si $n = 0$: $B = b_0$ puis on prend $U = 1$ et $V = \frac{1}{b_0}(1 - A)$.

(ii) Soit $n \geq 1$ tel que le résultat est acquis au niveau de $n - 1$.

Supposons par exemple que $\deg A \geq \deg B$.

On effectue la division euclidienne de A par B : $A = QB + R$.

Si $R = 0$: B est un diviseur commun de A et B donc B est constant, et on fait comme au (i).

Si $R \neq 0$: $\deg B > \deg R$ où R et B n'ont pas de diviseur commun non constant, ce qui donne $U_0R + BV_0 = 1$ puis $U_0A + B(V_0 - QU_0) = 1$ enfin on prend $U := U_0$ et $V := V_0 - QU_0$.

(b) On suppose que $P \mid AB$, et $P \nmid A$.

Comme P est irréductible, le seul diviseur unitaire de P et A est 1. Donc $\text{pgcd}(A, P) = 1$.

Bézout : il existe $U, V \in \mathbb{K}[X]$ tels que $AU + PV = 1$, donc $\underbrace{BA}U + BPV = B$ et $P \mid B$. □

divisible par P

Théorème

Soit $P \in \mathbb{K}[X] \setminus \{0\}$.

(a) Il existe $\lambda \in \mathbb{K} \setminus \{0\}$, $k \in \mathbb{N}$, des polynômes unitaires irréductibles distincts P_1, \dots, P_k et $\alpha_1, \dots, \alpha_k \in \mathbb{N} \setminus \{0\}$, tels que : $P = \lambda \underbrace{P_1^{\alpha_1} \dots P_k^{\alpha_k}}_{1 \text{ quand } k = 0}$.

(b) La décomposition du (a) est « unique à l'ordre près »^(*) au sens où pour toute autre décomposition $P = \mu Q_1^{\beta_1} \dots Q_l^{\beta_l}$, on a : $\mu = \lambda$ et $\{(Q_1, \beta_1), \dots, (Q_l, \beta_l)\} = \{(P_1, \alpha_1), \dots, (P_k, \alpha_k)\}$.

(c) Quand P est décomposé comme au (a), les éléments de $\mathbb{K}[X]$ qui divisent P sont les polynômes de la forme $\mu P_1^{\beta_1} \dots P_k^{\beta_k}$ avec $\mu \in \mathbb{K} \setminus \{0\}$ et $0 \leq \beta_1 \leq \alpha_1, \dots, 0 \leq \beta_k \leq \alpha_k$.

DÉMONSTRATION

(a) On montre l'existence d'une décomposition de P en polynômes irréductibles.

Récurrence sur $n \geq 0$: (H_n) existence d'une décomposition en polynômes irréductibles pour tous les polynômes non-nuls de degré $\leq n$.

(i) Cas $n = 0$: $k = 0$ convient. Donc (H_0) est vraie.

(ii) On suppose que (H_n) est vraie et se donne $Q \in \mathbb{K}[X] \setminus \{0\}$ de degré $n + 1$:

- soit Q est irréductible et se décompose en $\mu \tilde{Q}^1$ où $Q = \mu \tilde{Q}$ avec \tilde{Q} unitaire irréductible ;
- soit Q n'est pas irréductible et il existe $A, B \in \mathbb{K}[X] \setminus \{0\}$ tels que $Q = AB$, puis en appliquant (H_n) au niveau de A et de B on décompose Q en polynômes irréductibles.

On en déduit que (H_{n+1}) est vraie.

(iii) Ainsi, pour chaque $n \geq 1$, (H_n) est vraie et en particulier P possède une décomposition en polynômes irréductibles.

(b) On montre l'unicité de la décomposition en partant de $P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k} = \mu Q_1^{\beta_1} \dots Q_l^{\beta_l}$ avec $\lambda, \mu \in \mathbb{K} \setminus \{0\}$, $\underbrace{P_1, \dots, P_k}_{\text{distincts}}, \underbrace{Q_1, \dots, Q_l}_{\text{distincts}}$ unitaires irréductibles et $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l \in \mathbb{N} \setminus \{0\}$.

(*) (les autres décompositions s'obtiennent en « changeant l'ordre dans lequel on écrit $(P_1, \alpha_1), \dots, (P_k, \alpha_k)$ »)

Le lemme d'Euclide montre que chaque P_j ($1 \leq j \leq k$) divise un des polynômes Q_1, \dots, Q_l , noté Q_{i_j} , puis $P_j = Q_{i_j}$ par irréductibilité de Q_{i_j} . Donc : $\{P_1, \dots, P_k\} \subseteq \{Q_1, \dots, Q_l\}$. De même : $\{Q_1, \dots, Q_l\} \subseteq \{P_1, \dots, P_k\}$. D'où $l = k$. Après simplification : $\lambda P_1^{\alpha_1} \dots P_k^{\alpha_k - \beta_{i_k}} = \mu Q_{i_1}^{\beta_{i_1}} \dots Q_{i_{k-1}}^{\beta_{i_{k-1}}}$ si $\alpha_k > \beta_{i_k}$, ou, $\lambda P_1^{\alpha_1} \dots P_{k-1}^{\alpha_{k-1}} = \mu Q_{i_1}^{\beta_{i_1}} \dots Q_{i_k}^{\beta_{i_k} - \alpha_k}$ si $\alpha_k < \beta_{i_k}$, chacun de ces deux cas menant à une contradiction comme ci-dessus. Ainsi $\alpha_k = \beta_{i_k}$. Ensuite $\alpha_{k-1} = \beta_{i_{k-1}}, \dots, \alpha_1 = \beta_{i_1}, \mu = \nu$.

(c) On cherche maintenant les diviseurs de P . Ceux proposés conviennent.

Soit $B \in \mathbb{K}[X]$ qui divise P . Donc $B \neq 0$ et il existe $C \in \mathbb{K}[X] \setminus \{0\}$ tel que $P = BC$. Quitte à ajouter des Q_i^0 , on peut écrire $B = \mu Q_1^{\beta_1} \dots Q_l^{\beta_l}$ et $C = \nu Q_1^{\gamma_1} \dots Q_l^{\gamma_l}$, avec $\lambda, \mu \in \mathbb{K} \setminus \{0\}$, Q_1, \dots, Q_l unitaires irréductibles distincts et $\beta_1, \dots, \beta_l, \gamma_1, \dots, \gamma_l \in \mathbb{N}$, $\beta_1 + \gamma_1 \neq 0, \dots, \beta_l + \gamma_l \neq 0$. Donc $P = \mu\nu Q_1^{\beta_1 + \gamma_1} \dots Q_l^{\beta_l + \gamma_l}$ puis par unicité de la décomposition en polynômes irréductibles : $l = k$ et $Q_1 = P_{j_1}$ et ... et $Q_k = P_{j_k}$ et $\beta_1 + \gamma_1 = \alpha_{j_1}$ et ... et $\beta_k + \gamma_k = \alpha_{j_k}$. D'où le résultat. \square

Remarque

Soient $P = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k} \in \mathbb{K}[X] \setminus \{0\}$ comme ci-dessus et $r \in \mathbb{K}$.

On a : r est racine de P si et seulement si $X - r$ est l'un des P_i , $1 \leq i \leq k$.

Dans ce cas α_i est la multiplicité de la racine r de P .

(D'après le (c) du théorème, la multiplicité de r dans P est le plus grand $m \in \mathbb{N}$ tel que $(X - r)^m$ s'écrive $\mu P_1^{\beta_1} \dots P_k^{\beta_k}$ avec $\mu \in \mathbb{K} \setminus \{0\}$ et $0 \leq \beta_1 \leq \alpha_1, \dots, 0 \leq \beta_k \leq \alpha_k$.
Or $X - r$ est unitaire irréductible. On utilise l'unicité de la décomposition.)

Théorème (« théorème de d'Alembert-Gauss »)

Tout polynôme non-constant à coefficients dans \mathbb{C} a au moins une racine dans \mathbb{C} .

DÉMONSTRATION

Admise (difficile). \square

Corollaire (important)

(a) Les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes de degré 1.

En particulier, tout $P \in \mathbb{C}[X] \setminus \{0\}$ s'écrit de manière unique à l'ordre près sous la forme

$$P = \lambda (X - r_1)^{\alpha_1} \dots (X - r_m)^{\alpha_m}$$

avec $\lambda \in \mathbb{C} \setminus \{0\}$, $\{r_1, \dots, r_m\} \subseteq \mathbb{C}$, et $\alpha_1, \dots, \alpha_m \in \mathbb{N} \setminus \{0\}$.
distincts

(b) Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 dont le discriminant est strictement négatif.

En particulier, tout $P \in \mathbb{R}[X] \setminus \{0\}$ s'écrit de manière unique à l'ordre près sous la forme

$$P = \lambda (X - r_1)^{\alpha_1} \dots (X - r_m)^{\alpha_m} (X^2 + u_1X + v_1)^{\beta_1} \dots (X^2 + u_nX + v_n)^{\beta_n}$$

avec $\lambda \in \mathbb{R} \setminus \{0\}$, $\{r_1, \dots, r_m\} \subseteq \mathbb{R}$, $\{(u_1, v_1), \dots, (u_n, v_n)\} \subseteq \mathbb{R}^2$ tels que les $X^2 + u_kX + v_k$ ($1 \leq k \leq n$) n'ont pas de racine réelle, et $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in \mathbb{N} \setminus \{0\}$.
distincts couples distincts

DÉMONSTRATION

(a) Tout polynôme $P \in \mathbb{C}[X]$ de degré 1 est irréductible (déjà vu).

Soit $P \in \mathbb{C}[X]$ irréductible. D'après le théorème de d'Alembert-Gauss, P a un diviseur de la forme $X - r$ avec $r \in \mathbb{C}$, donc par irréductibilité on a $P = \lambda(X - r)$ pour un $\lambda \in \mathbb{C}$.

(b) Tout $P \in \mathbb{R}[X]$ de degré 1, ou de degré 2 sans racine réelle, est irréductible (déjà vu).

Soit $P \in \mathbb{R}[X]$ irréductible.

Si P a une racine $r \in \mathbb{R}$, on a comme ci-dessus $P = \lambda(X - r)$ pour un $\lambda \in \mathbb{R}$.

Sinon, d'après le théorème de d'Alembert-Gauss, P a une racine $r \in \mathbb{C} \setminus \mathbb{R}$.

Donc il existe $A \in \mathbb{C}[X]$ tel que : $P = (X - r)A$.

Comme P est à coefficients réels, on a : $P(\bar{r}) = \overline{P(r)} = 0$, puis $A(\bar{r}) = 0$.

Donc il existe $B \in \mathbb{C}[X]$ tel que : $A = (X - \bar{r})B$. On a : $P = (X^2 - 2\operatorname{Re}(r)X + |r|^2)B$.

De plus : $B \in \mathbb{R}[X]$ par existence de la division euclidienne dans $\mathbb{R}[X]$ et unicité dans $\mathbb{C}[X]$.

Ainsi $\underbrace{P}_{\text{irréductible}} = (X^2 - 2\operatorname{Re}(r)X + |r|^2)B$ puis $P = \lambda(X^2 - 2\operatorname{Re}(r)X + |r|^2)$ pour un $\lambda \in \mathbb{R}$. \square

Exemple

On obtient les décompositions en polynômes irréductibles unitaires suivantes :

$$\begin{aligned}
 - \underbrace{X^4 + 1}_{4 \text{ racines connues}} &= \underbrace{(X - e^{i\frac{\pi}{4}})(X - e^{-i\frac{\pi}{4}})}_{4 \text{ facteurs irréductibles connus}} \underbrace{(X - e^{i\frac{3\pi}{4}})(X - e^{-i\frac{3\pi}{4}})}_{\substack{X^2 - \sqrt{2}X + 1 \\ X^2 + \sqrt{2}X + 1}} \text{ dans } \mathbb{C}[X]; \\
 - X^4 + 1 &= (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1) \text{ dans } \mathbb{R}[X].
 \end{aligned}$$

Par contre $X^4 + 1$ est irréductible dans $\mathbb{Q}[X]$. En effet un facteur irréductible de $X^4 + 1$ dans $\mathbb{Q}[X]$ de degré < 4 devrait être un diviseur particulier de $X^4 + 1$ dans $\mathbb{R}[X]$ de la forme $\lambda(X^2 - \sqrt{2}X + 1)$ avec $\lambda \in \mathbb{R} \setminus \{0\}$ ou $\mu(X^2 + \sqrt{2}X + 1)$ avec $\mu \in \mathbb{R} \setminus \{0\}$, donc hors de $\mathbb{Q}[X]$. [En effet, on a $\sqrt{2} \notin \mathbb{Q}$ car le polynôme $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$.]

III. FRACTIONS RATIONNELLES

Comment dériver 1000 fois et comment intégrer une fonction rationnelle $f: [a, b] \rightarrow \mathbb{R}$?

Méthode : on écrit f comme somme de fonctions rationnelles f_1, \dots, f_n « plus simples ».

$$\left(\begin{array}{l}
 \text{Pour dériver, on utilisera les éléments simples sur } \mathbb{C}. \text{ Pour intégrer un élément simple } f_m \\
 (1 \leq m \leq n) \text{ de seconde espèce, on cherche } \alpha \in \mathbb{R}, \text{ puis } \beta \in \mathbb{R} \text{ et } \gamma > 0, \text{ tels que :} \\
 f_m(x) = \frac{\mu x + \nu}{(x^2 + u_l x + v_l)^j} = \alpha \frac{2x + u_l}{(x^2 + u_l x + v_l)^j} + \beta \frac{1}{((x + \frac{u_l}{2})^2 + \gamma^2)^j} \text{ pour tout } x \in \mathbb{R}. \\
 \text{Les primitives } \int \frac{2x + u_l}{(x^2 + u_l x + v_l)^j} dx \text{ se calculent à l'aide du CV : } t = x^2 + u_l x + v_l. \\
 \text{Le calcul des primitives } \int \frac{dx}{((x + \frac{u_l}{2})^2 + \gamma^2)^j} \text{ se ramène à celui de } \int \frac{dx}{((x + \frac{u_l}{2})^2 + \gamma^2)^{j-1}} \text{ en intégrant} \\
 \text{par parties à partir de } \int \underbrace{1}_{\text{dérivée de } x \mapsto x + \frac{u_l}{2}} \times \frac{1}{((x + \frac{u_l}{2})^2 + \gamma^2)^{j-1}} dx.
 \end{array} \right)$$

1. Fractions rationnelles

Définition

(a) Une *fraction rationnelle à coefficients dans \mathbb{K}* est un « quotient » $F = \frac{A}{B}$ (en un sens qu'on pourrait préciser) où $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$.

(b) À chaque fraction rationnelle $F = \frac{a_p X^p + \dots + a_1 X + a_0}{b_q X^q + \dots + b_1 X + b_0}$ à coefficients dans \mathbb{K} , on associe l'application notée ici abusivement f_F et définie par :

$$f_F(x) = \frac{a_p x^p + \dots + a_1 x + a_0}{b_q x^q + \dots + b_1 x + b_0} \text{ pour (au moins) tout } x \in \mathbb{K} \text{ tel que } b_q x^q + \dots + b_1 x + b_0 \neq 0.$$

[L'application f_F est définie sur cet ensemble pour l'écriture $\frac{A}{B}$ irréductible et B unitaire.]

Une *application rationnelle sur \mathbb{K}* est une application f d'une certaine partie de \mathbb{K} dans \mathbb{K} telle qu'il existe une fraction rationnelle F à coefficients dans \mathbb{K} pour laquelle $f = f_F$.

(c) Le *degré* d'une fraction rationnelle $F = \frac{A}{B}$ avec $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$, noté $\deg F$, est défini par : $\deg F := \deg A - \deg B$.

Remarque (hors programme)

On appelle « quotient d'un élément A de $\mathbb{K}[X]$ par un élément B de $\mathbb{K}[X] \setminus \{0\}$ » l'ensemble :

$$\frac{A}{B} := \{(A_0, B_0) \in \mathbb{K}[X] \times (\mathbb{K}[X] \setminus \{0\}) \mid AB_0 = A_0 B\} \text{ (il contient } (A, B)\text{)}.$$

Par définition on a donc : $\frac{A}{B} = \frac{PA}{PB}$ pour tout $P \in \mathbb{K}[X] \setminus \{0\}$.

Chaque notion attachée à $\frac{A}{B}$ devra être indépendante du choix de (A, B) dans $\frac{A}{B}$.

Par exemple on peut noter : $(\frac{A}{B})(x) := \frac{A(x)}{B(x)}$ pour certains $x \in \mathbb{K}$, et $(\frac{A}{B})' := \frac{A'B - AB'}{B^2}$ car pour $(A_0, B_0) \in \frac{A}{B}$, on a : $\frac{A_0(x)}{B_0(x)} = \frac{A(x)}{B(x)}$ quand $B_0(x)B(x) \neq 0$, et $\frac{A'_0 B_0 - A_0 B'_0}{B_0^2} = \frac{A'B - AB'}{B^2}$.

(En effet : $AB_0 = A_0 B$ donc $A'_0 B_0 B^2 + AB' B_0^2 = (A'_0 B + A_0 B')B_0 B = (A'B_0 + AB'_0)B_0 B = A'B B_0^2 + A_0 B'_0 B^2$.)

Notation

On note $\mathbb{K}(X)$ l'ensemble des fractions rationnelles à coefficients dans \mathbb{K} .

En « identifiant » A à $\frac{A}{1}$, on obtient : $\mathbb{K}[X] \subseteq \mathbb{K}(X)$ (choix de $B = 1$).

Définition-Proposition

Soient $F = \frac{A}{B}$ et $G = \frac{C}{D}$ deux éléments de $\mathbb{K}(X)$, $\alpha, x \in \mathbb{K}$ avec $B(x) \neq 0$ et $D(x) \neq 0$.

On note : $F + G := \frac{AD+BC}{BD}$, $FG := \frac{AC}{BD}$, $\alpha F = \frac{\alpha A}{B}$, et aussi $\frac{F}{G} := \frac{AD}{BC}$ quand $G \neq 0$.

Ainsi, on a : $(F + G)(x) = F(x) + G(x)$, $(FG)(x) = F(x)G(x)$, $(\alpha F)(x) = \alpha F(x)$.

Proposition

L'ensemble $\mathbb{K}(X)$ muni de l'addition et de la multiplication des fractions rationnelles est un corps commutatif de zéro le polynôme 0 et d'élément unité le polynôme constant 1.

Remarques

1. Soit $F = \frac{A}{B} \in \mathbb{K}(X) \setminus \{0\}$.

On décompose $A = \lambda P_1^{\alpha_1} \dots P_k^{\alpha_k}$ et $B = \mu P_1^{\beta_1} \dots P_k^{\beta_k}$ avec $\lambda, \mu \in \mathbb{K} \setminus \{0\}$, $P_1, \dots, P_k \in \mathbb{K}[X]$ unitaires irréductibles et $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \in \mathbb{N}$. On pose $D = P_1^{\min(\alpha_1, \beta_1)} \dots P_k^{\min(\alpha_k, \beta_k)}$.

On obtient tout de suite $A_0, B_0 \in \mathbb{K}[X] \setminus \{0\}$ sans facteur unitaire irréductible commun tels que $A = A_0 D$ et $B = B_0 D$. On a : $F = \frac{A_0}{B_0}$ « écriture de F comme fraction irréductible ».

2. Soient $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{C}[X]$ et $Q \in \mathbb{C}[X]$, $F = \frac{A}{B} \in \mathbb{C}(X)$ et $G \in \mathbb{C}(X)$.

On pose : $\overline{P} := \overline{a_n} X^n + \dots + \overline{a_1} X + \overline{a_0} \in \mathbb{C}[X]$, puis $\overline{F} := \frac{\overline{A}}{\overline{B}} \in \mathbb{C}(X)$ (cf. $\overline{PQ} = \overline{P} \overline{Q}$).

On obtient : $\overline{F+G} = \overline{F} + \overline{G}$, $\overline{FG} = \overline{F} \overline{G}$, et $\overline{F(z)} = \overline{F}(\overline{z})$ quand $z \in \mathbb{C}$ vérifie $B(z) \neq 0$.

2. Décomposition en éléments simples

Lemme

Soient $A, \tilde{B} \in \mathbb{K}[X]$ et $r \in \mathbb{K}$ tels que $\tilde{B}(r) \neq 0$.

Pour tout $\alpha \in \mathbb{N} \setminus \{0\}$ il existe $c_0, c_1, \dots, c_{\alpha-1} \in \mathbb{K}$ et $R_{\alpha-1} \in \mathbb{K}[X]$ tels que :

$$A = \tilde{B} \times (c_0 + c_1(X-r) + \dots + c_{\alpha-1}(X-r)^{\alpha-1}) + (X-r)^\alpha R_{\alpha-1}$$

« division de A par \tilde{B} suivant les puissances croissantes de $X-r$ jusqu'à l'ordre $\alpha-1$ ».

DÉMONSTRATION

On peut supposer que $A \neq 0$ (clair sinon). On note m la multiplicité de r dans A .

On vérifie par récurrence sur $n \in \mathbb{N}$ avec α fixé que :

$$(H_n) \text{ existence d'une décomposition quand } A \neq 0 \text{ et } \alpha - m \leq n.$$

(i) Si $n = 0$: on écrit $A = (X-r)^m C$ pour un certain $C \in \mathbb{K}[X]$ où $m \geq \alpha$, puis l'égalité $A = \tilde{B} \times 0 + (X-r)^\alpha ((X-r)^{m-\alpha} C)$ donne une décomposition.

(ii) Soit $n \geq 1$ tel que (H_{n-1}) est vraie. On suppose donc que $\alpha - m = n$:

$$A = \tilde{a}_m (X-r)^m + \dots + \tilde{a}_p (X-r)^p \text{ et } \tilde{B} = \tilde{b}_0 + \tilde{b}_1 (X-r) + \dots + \tilde{b}_q (X-r)^q \text{ avec } \tilde{b}_0 \neq 0.$$

On pose : $A_0 = A - \frac{\tilde{a}_m}{\tilde{b}_0} (X-r)^m \tilde{B}$. Si $A_0 \neq 0$, la multiplicité de r dans A_0 est $\geq m+1$.

D'après (H_{n-1}) , il existe $c_0, c_1, \dots, c_{\alpha-1} \in \mathbb{K}$ et $R_{\alpha-1} \in \mathbb{K}[X]$ tels que :

$$A_0 = \tilde{B} \times (c_0 + c_1(X-r) + \dots + c_{\alpha-1}(X-r)^{\alpha-1}) + (X-r)^\alpha R_{\alpha-1}.$$

$$\text{Ainsi : } A = \tilde{B} \times (c_0 + c_1(X-r) + \dots + (c_m + \frac{\tilde{a}_m}{\tilde{b}_0})(X-r)^m + \dots + c_{\alpha-1}(X-r)^{\alpha-1}) + (X-r)^\alpha R_{\alpha-1}.$$

(iii) D'où le résultat. □

Théorème (« théorème de décomposition en éléments simples » sur $\mathbb{K} = \mathbb{R}$ ou \mathbb{C})

Soient $A \in \mathbb{K}[X]$ et $B \in \mathbb{K}[X] \setminus \{0\}$. On pose : $F := \frac{A}{B}$.

(a) On suppose que $\mathbb{K} = \mathbb{C}$. On décompose B :

$$B = \gamma (X-r_1)^{\alpha_1} \dots (X-r_m)^{\alpha_m}$$

avec $\gamma \in \mathbb{C} \setminus \{0\}$, $\{r_1, \dots, r_m\} \subseteq \mathbb{C}$, et $\alpha_1, \dots, \alpha_m \in \mathbb{N} \setminus \{0\}$.

La fraction rationnelle F est somme de manière unique :

- d'un polynôme $E \in \mathbb{C}[X]$ appelé *partie entière de F* ;
- « d'éléments simples » $\frac{\lambda}{(X-r_k)^i}$ avec $\lambda \in \mathbb{C}$, $1 \leq k \leq m$, $1 \leq i \leq \alpha_k$.

$$\left[F = E + \sum_{k=1}^m \left(\frac{\lambda_{k,1}}{X-r_k} + \dots + \frac{\lambda_{k,\alpha_k}}{(X-r_k)^{\alpha_k}} \right) \right]$$

Quand A n'est pas divisible par $X - r_k$ l'élément simple $\frac{\lambda}{(X-r_k)^{\alpha_k}}$ vérifie $\lambda \neq 0$.

(b) On suppose que $\mathbb{K} = \mathbb{R}$. On décompose B :

$$B = \gamma (X - r_1)^{\alpha_1} \dots (X - r_m)^{\alpha_m} (X^2 + u_1X + v_1)^{\beta_1} \dots (X^2 + u_nX + v_n)^{\beta_n}$$

avec $\gamma \in \mathbb{R} \setminus \{0\}$, $\{r_1, \dots, r_m\} \subseteq \mathbb{R}$, $\{(u_1, v_1), \dots, (u_n, v_n)\} \subseteq \mathbb{R}^2$ tels que les $X^2 + u_kX + v_k$ ($1 \leq k \leq n$) n'ont pas de racine réelle, et $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in \mathbb{N} \setminus \{0\}$.

La fraction rationnelle F est somme de manière unique :

- d'un polynôme $E \in \mathbb{R}[X]$ appelé *partie entière de F* ;
- « d'éléments simples de 1^{re} espèce » $\frac{\lambda}{(X-r_k)^i}$ avec $\lambda \in \mathbb{R}$, $1 \leq k \leq m$, $1 \leq i \leq \alpha_k$;
- « d'éléments simples de 2^e espèce » $\frac{\mu X + \nu}{(X^2 + u_lX + v_l)^j}$ avec $\mu, \nu \in \mathbb{R}$, $1 \leq l \leq n$, $1 \leq j \leq \beta_l$.

$$\left[F = E + \sum_{k=1}^m \left(\frac{\lambda_{k,1}}{X-r_k} + \dots + \frac{\lambda_{k,\alpha_k}}{(X-r_k)^{\alpha_k}} \right) + \sum_{l=1}^n \left(\frac{\mu_{l,1}X + \nu_{l,1}}{X^2 + u_lX + v_l} + \dots + \frac{\mu_{l,\beta_l}X + \nu_{l,\beta_l}}{(X^2 + u_lX + v_l)^{\beta_l}} \right) \right]$$

Quand A n'est pas divisible par $X - r_k$ (resp. par $X^2 + u_lX + v_l$) l'élément simple $\frac{\lambda}{(X-r_k)^{\alpha_k}}$ (resp. $\frac{\mu X + \nu}{(X^2 + u_lX + v_l)^{\beta_l}}$) vérifie $\lambda \neq 0$ (resp. $(\mu, \nu) \neq (0, 0)$).

(c) Le polynôme E du (a) ou du (b) est le quotient de la division euclidienne de A par B . Il est nul si $\deg(A) < \deg(B)$, et non-nul avec un degré égal à $\deg(A) - \deg(B)$ sinon.

DÉMONSTRATION (idées)

(a) • On montre l'existence d'une décomposition sur \mathbb{C} par récurrence sur m .

(i) On suppose que $m = 0$. On a : $F \in \mathbb{K}[X]$ et la décomposition est évidente.

(ii) On se donne $m \geq 1$ pour lequel la décomposition est obtenue quand B a $m - 1$ racines.

On utilise le lemme avec $\tilde{B} := \frac{B}{(X-r_m)^{\alpha_m}}$, $r = r_m$ et $\alpha = \alpha_m$:

$$A = \tilde{B} \times (c_0 + c_1(X-r) + \dots + c_{\alpha_m-1}(X-r)^{\alpha_m-1}) + (X-r)^{\alpha_m} R_{\alpha_m-1}.$$

Donc $F = \frac{c_0 + c_1(X-r) + \dots + c_{\alpha_m-1}(X-r)^{\alpha_m-1}}{(X-r_m)^{\alpha_m}} + \frac{R_{\alpha_m-1}}{\tilde{B}}$, puis on applique l'hypothèse de récurrence.

On en déduit que la décomposition est obtenue quand B a m racines.

(iii) Ainsi l'existence est obtenue.

• Unicité sur \mathbb{C} ? On se donne $E \in \mathbb{C}[X]$ et $\lambda_{k,i} \in \mathbb{C}$ tels que

$$E + \sum_{k=1}^m \left(\frac{\lambda_{k,1}}{X-r_k} + \dots + \frac{\lambda_{k,\alpha_k}}{(X-r_k)^{\alpha_k}} \right) = 0.$$

On fixe un k . On multiplie par $(X - r_k)^{\alpha_k}$ puis prend la valeur en r_k . On obtient $\lambda_{k,\alpha_k} = 0$.

On recommence en multipliant par $(X - r_k)^{\alpha_k - 1}$ ce qui donne $\lambda_{k,\alpha_k - 1} = 0$. Puis ... $\lambda_{k,1} = 0$.

Enfin $E = 0$.

• Si $\lambda = 0$: en multipliant F décomposé par B , on constate que A est divisible par $X - r_k$.

(b) • On montre l'existence d'une décomposition sur \mathbb{R} en utilisant la décomposition sur \mathbb{C} .

On considère un élément simple $\frac{\lambda}{(X-r_k)^i}$. Si $r_k \in \mathbb{R}$, on a : $\bar{F} = F$ donc $\lambda \in \mathbb{R}$ par unicité.

On suppose que $r_k \notin \mathbb{R}$. Comme $\bar{F} = F$, on a : $\frac{\bar{\lambda}}{(X-\bar{r}_k)^i}$ est un élément simple de F sur \mathbb{C} .

On décompose sur \mathbb{R} : $\frac{\lambda}{(X-r_k)^i} + \frac{\bar{\lambda}}{(X-\bar{r}_k)^i}$ qui vaut $\frac{\lambda(X-\bar{r}_k)^i + \bar{\lambda}(X-r_k)^i}{((X-r_k)(X-\bar{r}_k))^i}$, est somme d'éléments simples de 2^e espèce (diviser suffisamment de fois $\lambda(X-\bar{r}_k)^i + \bar{\lambda}(X-r_k)^i$ par $(X-r_k)(X-\bar{r}_k)$).

• Unicité sur \mathbb{R} ? On se donne $E \in \mathbb{R}[X]$ et $\lambda_{k,i}, \mu_{l,j}, \nu_{l,j} \in \mathbb{R}$ tels que

$$E + \sum_{k=1}^m \left(\frac{\lambda_{k,1}}{X-r_k} + \dots + \frac{\lambda_{k,\alpha_k}}{(X-r_k)^{\alpha_k}} \right) + \sum_{l=1}^n \left(\frac{\mu_{l,1}X + \nu_{l,1}}{X^2 + u_lX + v_l} + \dots + \frac{\mu_{l,\beta_l}X + \nu_{l,\beta_l}}{(X^2 + u_lX + v_l)^{\beta_l}} \right) = 0.$$

Comme ci-dessus, on obtient $\lambda_{k,i} = 0$ pour tous les k, i .

On fixe un l . On introduit une racine s_l de $X^2 + u_l X + v_l$ (non-réelle). On multiplie par $(X^2 + u_l X + v_l)^{\beta_l}$ et prend la valeur en s_l . Donc : $\mu_{l,\beta_l} s_l + \nu_{l,\beta_l} = 0$ puis $\mu_{l,\beta_l} = 0$ et $\nu_{l,\beta_l} = 0$. La multiplication par $(X^2 + u_l X + v_l)^{\beta_l - 1}$ donne $\mu_{l,\beta_l - 1} = \nu_{l,\beta_l - 1} = 0$. Puis ... $\mu_{l,1} = \nu_{l,1} = 0$. Enfin $E = 0$.

• Si $\lambda = 0$: on constate comme ci-dessus que A est divisible par $X - r_k$.

Si $\mu = \nu = 0$: en multipliant F par B , on constate que A est divisible par $X^2 + u_l X + v_l$.

(c) À la fois dans (a) et dans (b), on obtient en multipliant F décomposé par B :

$$A = BE + R \text{ avec } \deg R \leq \deg B - 1.$$

Il s'agit du résultat de la division euclidienne de A par B . □

Algorithmes (l'algorithme du (b) n'est pas au programme mais peut être utilisé)

On reprend les notations du théorème. (Idée : calcul des DL de $x \mapsto F(x)$ en $+\infty$ et en r_k .)

a) On suppose que $\deg(A) \geq \deg(B)$ (sinon $E = 0$) et note :

$$A = a_p X^p + \dots + a_1 X + a_0 \text{ et } B = b_q X^q + \dots + b_1 X + b_0, \text{ avec } a_p \neq 0 \text{ et } b_q \neq 0.$$

Division euclidienne de A par B : son quotient Q vérifie $Q = E$ (cf. le th. (c)).

Astuce : on utilise dans ce calcul autant de coefficients de A et de B , à partir de a_p et b_q , qu'on en attend dans E .

b) Soit $k \in \{1, \dots, m\}$. On pose $X = r_k + Y$ et $\tilde{B} := \frac{B}{Y^{\alpha_k}}$. On écrit A et \tilde{B} ainsi :

$$A = \tilde{a}_0 + \tilde{a}_1 Y + \dots + \tilde{a}_p Y^p \text{ et } \tilde{B} = \tilde{b}_0 + \tilde{b}_1 Y + \dots + \tilde{b}_{q-\alpha_k} Y^{q-\alpha_k} \text{ où } \tilde{b}_0 \neq 0.$$

La fraction rationnelle F_k somme des éléments simples de 1^{re} espèce associés à r_k s'obtient par division suivant les puissances croissantes de A par \tilde{B} , jusqu'à faire apparaître α_k coefficients dans le quotient (méthode incontournable quand $\alpha_k \geq 4$) :

$$\begin{array}{l} \begin{array}{l} \tilde{a}_0 + \tilde{a}_1 Y + \dots + \tilde{a}_p Y^p \\ \ominus \tilde{a}_0 + \frac{\tilde{a}_0 \tilde{b}_1}{\tilde{b}_0} Y + \dots \\ = \\ \ominus \tilde{a}'_1 Y + \dots + \tilde{a}'_{p'} Y^{p'} \\ = \\ \dots \quad \dots \quad \dots \\ \tilde{a}''_{\alpha_k} Y^{\alpha_k} + \dots + \tilde{a}''_{p''} Y^{p''} \end{array} \quad \left| \begin{array}{l} \tilde{b}_0 + \tilde{b}_1 Y + \dots + \tilde{b}_{q-\alpha_k} Y^{q-\alpha_k} \\ \hline \underbrace{\frac{\tilde{a}_0}{\tilde{b}_0} + \frac{\tilde{a}'_1}{\tilde{b}_0} Y + \dots}_{\tilde{Q}_k := c_0 + c_1(X-r) + \dots + c_{\alpha_k-1}(X-r)^{\alpha_k-1}} \\ \hline \text{donc } \boxed{F_k = \frac{\tilde{Q}_k}{(X-r_k)^{\alpha_k}} \text{ (cf. la dém. du th.)}} \end{array} \right. \end{array}$$

Astuce : on utilise dans ce calcul autant de coefficients de A et de \tilde{B} , à partir de \tilde{a}_0 et \tilde{b}_0 , qu'on en attend dans F_k .

Remarques

1. Après avoir utilisé les algorithmes (a), et (b) pour chaque $k \in \{1, \dots, m\}$, on peut :

- appliquer la décomposition en un $z \in \mathbb{C}$, par exemple en une racine dans \mathbb{C} d'un $X^2 + u_l X + v_l$;
- réduire au même dénominateur la décomposition en éléments simples de F obtenue pour l'instant et identifier les coefficients de son numérateur avec ceux de A ;
- réduire au même dénominateur $F - \left(E + \sum_{k=1}^m F_k \right)$ puis le simplifier lorsque $\mathbb{K} = \mathbb{R}$ et $n = 1$.

2. On peut éviter de factoriser B sous la forme $(X - r_k)^{\alpha_k} C$ pour calculer le coefficient λ de l'élément simple $\frac{\lambda}{(X - r_k)^{\alpha_k}}$. En effet, il s'écrit : $\lambda = \frac{A(r_k)}{C(r_k)} = \alpha_k! \frac{A(r_k)}{B^{(\alpha_k)}(r_k)}$.
(On utilise la formule de Leibniz pour calculer $B^{(\alpha_k)}(r_k)$ à partir de l'égalité $B = (X - r_k)^{\alpha_k} C$.)

Exemple 1

On considère : $F = \frac{X^5 + X^4 + X^2 + 1}{X^3 - X^2 - X + 1} \in \mathbb{C}(X)$.

On a : $\underbrace{X^3 - X^2 - X + 1}_{\text{s'annule en 1}} = (X - 1)(X^2 + 0X - 1) = (X + 1)(X - 1)^2$.

On note $r_1 = -1$ et $r_2 = 1$. Il existe $E \in \mathbb{C}[X]$ de degré 2 et $a, b, c \in \mathbb{C}$ uniques tels que :

$$\underbrace{\frac{X^5 + X^4 + X^2 + 1}{(X+1)(X-1)^2}}_F = E + \underbrace{\frac{a}{X+1}}_{F_1, \text{ cf. (b)}} + \underbrace{\frac{b}{(X-1)^2} + \frac{c}{X-1}}_{F_2, \text{ cf. (b)}}.$$

On commence par calculer les 3 coefficients de E :

$$\begin{array}{l} \ominus \frac{X^5 + X^4 + 0X^3 + \dots}{X^5 - X^4 - X^3 + \dots} \left| \begin{array}{l} X^3 - X^2 - X + \dots \\ X^2 + 2X + 3 \end{array} \right. \\ = \frac{2X^4 + X^3 + \dots}{2X^4 - 2X^3 + \dots} \\ \ominus \frac{2X^4 - 2X^3 + \dots}{3X^3 + \dots} \\ = \frac{\quad \quad \quad}{\quad \quad \quad} \end{array} \quad \text{donc } E = X^2 + 2X + 3.$$

On multiplie l'égalité plus haut par $X + 1$ et prend les valeurs en $x = -1$: $a = \frac{1}{2}$.

• Méthode 1

On continue en généralisant cette technique et choisissant une autre valeur particulière :

- on multiplie par $(X - 1)^2$ et prend les valeurs en $x = 1$: $b = 2$;
- valeurs en $x = 0$: $1 = 3 + a + b - c$, donc $c = \frac{9}{2}$.

• Méthode 2

On utilise l'algorithme (b) pour calculer b et c . On pose $X = 1 + Y$ et cherche 2 coefficients :

$$F = \frac{(1+Y)^5 + (1+Y)^4 + (1+Y)^2 + 1}{(1+Y)^3 - (1+Y)^2 - (1+Y) + 1} = \frac{4 + 11Y + \dots}{Y^3(2+Y)}.$$

Division suivant les puissances de Y croissantes jusqu'à obtenir 2 coefficients :

$$\begin{array}{l} \ominus \frac{4 + 11Y + \dots}{4 + 2Y} \left| \begin{array}{l} 2 + Y \\ 2 + \frac{9}{2}Y \end{array} \right. \\ = \frac{9Y + \dots}{\quad \quad \quad} \end{array} \quad \text{donc } F_2(X) = \frac{2}{Y^2} + \frac{9}{2Y} \text{ puis } b = 2 \text{ et } c = \frac{9}{2}.$$

• Finalement : $F = X^2 + 2X + 3 + \frac{\frac{1}{2}}{X+1} + \frac{2}{(X-1)^2} + \frac{\frac{9}{2}}{X-1}$.

Exemple 2

On considère : $F = \frac{1}{X^3 + 1} \in \mathbb{R}(X)$.

On a : $\underbrace{X^3 + 1}_{\text{s'annule en } -1} = (X + 1)\underbrace{(X^2 + ?)}_{X^2 - X + 1}$.

Il existe donc $\lambda, \mu, \nu \in \mathbb{R}$ uniques tels que :

$$\underbrace{\frac{1}{(X+1)(X^2 - X + 1)}}_F = \underbrace{0}_E + \frac{\lambda}{X+1} + \frac{\mu X + \nu}{X^2 - X + 1}.$$

On pourrait réduire le membre de droite au même dénominateur, puis identifier les coefficients des numérateurs (c'est tout à fait possible). D'habitude, on utilise les astuces suivantes :

- on multiplie par $X + 1$ et prend les valeurs en $x = -1$: $\lambda = \frac{1}{3}$;
- valeurs en $x = 0$: $1 = \lambda + \nu$, donc $\nu = \frac{2}{3}$;
- on multiplie par X , prend les valeurs en x et passe à $x \rightarrow +\infty$: $0 = \lambda + \mu$, donc $\mu = -\frac{1}{3}$.

(Au lieu d'utiliser les valeurs 0 et $+\infty$, on aurait aussi pu se placer dans $\mathbb{C}(X)$ et prendre une valeur complexe non-réelle, par exemple $\frac{1+i\sqrt{3}}{2}$ après avoir multiplié par $X^2 - X + 1$.)

En conclusion : $F = \frac{\frac{1}{3}}{X+1} + \frac{-\frac{1}{3}X + \frac{2}{3}}{X^2 - X + 1}$.

Plan

- I. Systèmes linéaires
- II. Calcul matriciel

I. SYSTÈMES LINÉAIRES (RAPPELS)

1. Introduction

Deux problèmes

(image réciproque d'un singleton par une application)

1. Comment passer d'une équation cartésienne d'un « sous-espace affine de \mathbb{K}^p » à une équation paramétrique qui décrit les points de ce sous-espace affine ? Par exemple :

$$(E_{\text{cart}}) \begin{cases} -4x + 12y - 5z = 1 \\ x - 3y + 2z = -1 \\ 2x - 6y + z = 1 \end{cases} \text{ dans } \mathbb{K}^3 \text{ détermine } \mathcal{S}_{E_{\text{cart}}} := \underbrace{\{(x, y, z) \in \mathbb{K}^3 \mid E_{\text{cart}}\}}_{\text{image réciproque de } \{(1, -1, 1)\} \text{ par ...}}$$

(image directe d'une application)

2. Comment passer d'une équation paramétrique d'un « sous-espace affine de \mathbb{K}^p » à une équation cartésienne de ce sous-espace affine ? Par exemple :

$$\mathcal{D}: \begin{cases} x = s - t + 1 \\ y = -s + t + 2 \end{cases}, s, t \in \mathbb{K} \text{ détermine } \mathcal{D} := \underbrace{\{(s - t + 1, -s + t + 2) ; s, t \in \mathbb{K}\}}_{\text{image directe de } \mathbb{K}^2 \text{ par ...}} \subseteq \mathbb{K}^2.$$

Une motivation

De nombreuses équations issues de la physique se résolvent numériquement (par « discrétisation ») en se ramenant à des « systèmes linéaires », cf. : <http://math.nist.gov/MatrixMarket/> (cliquer sur « Search by application area »).

But

On désire « résoudre » des équations comme (E_{cart}) au sens où on écrira $\mathcal{S}_{E_{\text{cart}}}$ sous forme paramétrique, sous réserve d'avoir $\mathcal{S}_{E_{\text{cart}}} \neq \emptyset$. On va utiliser une méthode qui permettra aussi de passer d'une forme paramétrique à une forme cartésienne. Plus précisément, on cherche :

- une forme paramétrique sans paramètre inutile (ce n'est pas le cas dans la définition de \mathcal{D} où tout s'exprime avec $u := s - t$) ;
- une forme cartésienne sans égalité inutile (ce n'est pas le cas dans l'écriture de (E_{cart}) où ligne 3 = -ligne 1 - 2 ligne 2).

2. Transformation d'un système linéaire

Définition

(a) Un système d'équations « linéaires » de n équations à p inconnues dans \mathbb{K} est du type :

$$(E) \begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = b_1 \\ \dots \\ a_{n1}x_1 + \dots + a_{np}x_p = b_n \end{cases} \text{ d'inconnue } (x_1, \dots, x_p) \in \mathbb{K}^p$$

où sont donnés $a_{11}, \dots, a_{1p}, a_{21}, \dots, a_{2p}, \dots, a_{n1}, \dots, a_{np} \in \mathbb{K}$ et $b_1, \dots, b_n \in \mathbb{K}$.

Dans la suite du I on fixe un tel système (E) et note \mathcal{S}_E l'ensemble de ses solutions dans \mathbb{K}^p .

(b) Le système d'équations linéaires homogène associé à (E) est le système suivant :

$$(H) \begin{cases} a_{11}x_1 + \dots + a_{1p}x_p = 0 \\ \dots \\ a_{n1}x_1 + \dots + a_{np}x_p = 0 \end{cases} \text{ d'inconnue } (x_1, \dots, x_p) \in \mathbb{K}^p.$$

Remarques (importantes)

1. (H) admet toujours comme solution $(0, \dots, 0)$.

2. On suppose que $\mathcal{S}_E \neq \emptyset$ et fixe une solution « particulière » (x_1^E, \dots, x_p^E) de (E) .

Pour tout $(x_1, \dots, x_p) \in \mathbb{K}^p$, on a tout de suite :

(x_1, \dots, x_p) vérifie (E) si et seulement si $(x_1 - x_1^E, \dots, x_p - x_p^E)$ vérifie (H) .

En résumé : solutions de (E) = solutions de (H) + une solution particulière de (E) .

Notations

(a) On utilisera les « matrices » suivantes :

$$A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \dots & & \dots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \text{ matrice de } (E), \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \text{ inconnue, et } B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ second membre de } (E).$$

identifiée à (x_1, \dots, x_p)

On écrira en abrégé $(E) : AX = B$.

(b) La *matrice augmentée* de (E) est la matrice $(A|B) := \left(\begin{array}{ccc|c} a_{11} & \dots & a_{1p} & b_1 \\ \dots & & \dots & \vdots \\ a_{n1} & \dots & a_{np} & b_n \end{array} \right)$, où la barre

verticale n'a aucune signification mathématique.

On résoudra (E) en travaillant sur les lignes de $(A|B)$ et sur les colonnes de A .

Exemples (cf. l'introduction de la partie I de ce chapitre)

1. L'équation (E_{cart}) $\begin{cases} -4x + 12y - 5z = 1 \\ x - 3y + 2z = -1 \\ 2x - 6y + z = 1 \end{cases}$ a pour matrice augmentée $\left(\begin{array}{ccc|c} -4 & 12 & -5 & 1 \\ 1 & -3 & 2 & -1 \\ 2 & -6 & 1 & 1 \end{array} \right)$.

d'inconnue $(x, y, z) \in \mathbb{K}^3$

2. On fixe $(x, y) \in \mathbb{K}^2$. On a : $(x, y) \in \mathcal{D} \iff (\exists (s, t) \in \mathbb{K}^2 \quad \begin{cases} x = s - t + 1 \\ y = -s + t + 2 \end{cases})$.

L'équation (E_{param}) $\begin{cases} s - t = x - 1 \\ -s + t = y - 2 \end{cases}$ a pour matrice augmentée $\left(\begin{array}{cc|c} 1 & -1 & x-1 \\ -1 & 1 & y-2 \end{array} \right)$.

d'inconnue $(s, t) \in \mathbb{K}^2$

Définition

Dans ce qui suit on va noter L_1, \dots, L_n les lignes de $(A|B)$ et C_1, \dots, C_p les colonnes de A . Étant donné $k \in \{1, \dots, n\}$ et $\alpha_1, \dots, \alpha_n \in \mathbb{K}$, on écrira « $L_k \leftarrow \alpha_1 L_1 + \dots + \alpha_n L_n$ » pour exprimer qu'on remplace la ligne L_k par $\alpha_1 L_1 + \dots + \alpha_n L_n$.

(a) Une *opération élémentaire sur les lignes* de $(A|B)$ est une des transformations suivantes :

- (i) $L_i \xleftrightarrow{\text{(échange)}} L_j$ avec $i \neq j$ « permutation de deux lignes » ;
- (ii) $L_i \leftarrow c L_i$ avec $c \neq 0$ « multiplication d'une ligne par un scalaire non-nul » ;
- (iii) $L_i \leftarrow L_i + c L_j$ avec $i \neq j$ et $c \in \mathbb{K}$ « ajout à une ligne d'un multiple d'une autre ligne ».

(b) Une *permutation de deux colonnes* de A est une transformation $C_i \xleftrightarrow{\text{(échange)}} C_j$ avec $i \neq j$.

Remarque

Pour toute opération élémentaire l sur les lignes des matrices à n lignes et p (resp. $p + 1$) colonnes et toute permutation c de deux colonnes de ces matrices, on a : $c \circ l = l \circ c$.

Lemme

Soit $(A'|B')$ une matrice obtenue à partir de $(A|B)$ après avoir effectué un nombre fini d'étapes de l'un des deux types suivants :

$L_i \leftrightarrow L_j$ avec $i \neq j$;

$L_i \leftarrow c_1 L_1 + \dots + c_i L_i + \dots + c_n L_n$ avec $1 \leq i \leq n$, $c_1, \dots, c_n \in \mathbb{K}$ et $\underline{c_i \neq 0}$.

Pour tout $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{K}^p$, le système $(E) : AX = B$ équivaut au système $(E') : A'X = B'$.

DÉMONSTRATION (idée)

En appliquant à (E) les opérations sur les lignes qui font passer de $(A|B)$ à $(A'|B')$, on constate que : si (x_1, \dots, x_p) vérifie (E) , alors (x_1, \dots, x_p) vérifie (E') .

Chaque étape se décompose en une succession d'opérations élémentaires sur les lignes.

Pour être sûr de pouvoir remonter de (E') à (E) , il reste à constater que ces opérations élémentaires sont réversibles :

- (i) $L_i \leftrightarrow L_j$ avec $i \neq j$ a pour réciproque $L_i \leftrightarrow L_j$;
- (ii) $L_i \leftarrow cL_i$ avec $c \neq 0$ a pour réciproque $L_i \leftarrow \frac{1}{c}L_i$;
- (iii) $L_i \leftarrow L_i + cL_j$ avec $i \neq j$ et $c \in \mathbb{K}$ a pour réciproque $L_i \leftarrow L_i - cL_j$. □

Exemple

On va écrire une suite de matrices augmentées associées à des systèmes linéaires équivalents.

On peut commencer la résolution de (E_{cart}) ainsi, en entourant le « pivot » :

$$\left(\begin{array}{ccc|c} -4 & 12 & -5 & 1 \\ \vdots & -3 & 2 & -1 \\ 2 & -6 & 1 & 1 \end{array} \right) \xrightarrow[\substack{\text{(pour utiliser le pivot 1, ce} \\ \text{qui n'est pas indispensable)}}]{L_1 \leftrightarrow L_2} \left(\begin{array}{ccc|c} \textcircled{1} & -3 & 2 & -1 \\ -4 & 12 & -5 & 1 \\ 2 & -6 & 1 & 1 \end{array} \right) \xrightarrow[\substack{\text{(pour amener des 0 dans } C_1 \\ \text{strictement sous la diagonale)}}]{\substack{L_2 \leftarrow L_2 + 4L_1 \\ \text{puis } L_3 \leftarrow L_3 - 2L_1}} \left(\begin{array}{ccc|c} \textcircled{1} & -3 & 2 & -1 \\ \boxed{0} & 0 & 3 & -3 \\ \boxed{0} & 0 & -3 & 3 \end{array} \right).$$

3. Méthode du pivot de Gauss

On va travailler sur les colonnes de A dans $(A|B)$ en allant de la gauche vers la droite pour se ramener à un système triangulaire. À chaque étape on va chercher un scalaire non-nul (« pivot ») vers le bas à partir du terme diagonal, et éventuellement à droite ce qui nécessitera de faire un échange de colonnes. On amène ce pivot sur la diagonale puis des 0 sous ce pivot.

Proposition (*)

a) On peut passer par une suite finie d'opérations élémentaires sur les lignes et d'échanges de deux colonnes, de la matrice A à une matrice de la forme

$$A' = \left(\begin{array}{ccc|ccc} \begin{array}{ccc} d_1 & \dots & \dots \\ 0 & \dots & \dots \\ \vdots & \dots & \dots \\ 0 & \dots & 0 \end{array} & \begin{array}{ccc} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{array} & \begin{array}{ccc} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{array} & \begin{array}{ccc} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{array} & \begin{array}{ccc} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{array} & \begin{array}{ccc} \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{array} \\ \hline \begin{array}{ccc} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{array} & \begin{array}{ccc} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{array} & \begin{array}{ccc} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{array} & \begin{array}{ccc} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{array} & \begin{array}{ccc} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{array} & \begin{array}{ccc} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{array} \end{array} \right) \text{ avec } d_1 \neq 0, \dots, d_r \neq 0.$$

b) Le système $(E) : AX = B$ d'inconnue $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix}$ équivaut au système $(E') : A'X' = B'$

d'inconnue $X' := \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_p} \end{pmatrix}$, où les transformations du (a) envoient $\left(\begin{array}{c|c} x_1 \dots x_p & \\ A & B \end{array} \right)$ sur $\left(\begin{array}{c|c} x_{j_1} \dots x_{j_p} & \\ A' & B' \end{array} \right)$.

[Noter que les lettres qui se trouvent au-dessus de A ou de A' représentent ici les noms des variables-coordonnées d'un vecteur de \mathbb{K}^n et non pas les valeurs particulières qu'elles prennent pour le vecteur X . De plus, ce sont les éventuels échanges de colonnes qui feront passer de x_1, \dots, x_p à x_{j_1}, \dots, x_{j_p} .]

c) On note \mathcal{S}_E l'ensemble des solutions de (E) et $B' = \begin{pmatrix} b'_1 \\ \vdots \\ b'_n \end{pmatrix}$.

On a : $\mathcal{S}_E \neq \emptyset \iff \underbrace{b'_{r+1} = \dots = b'_n = 0}_{n-r \text{ conditions}}$.

Dans ce cas, on obtient une équation paramétrique de \mathcal{S}_E à partir de (E') en écrivant successivement x_{j_r}, \dots, x_{j_1} en fonction des paramètres $\underbrace{t_1 := x_{j_{r+1}}, \dots, t_{p-r} := x_{j_p}}_{p-r \text{ paramètres}}$.

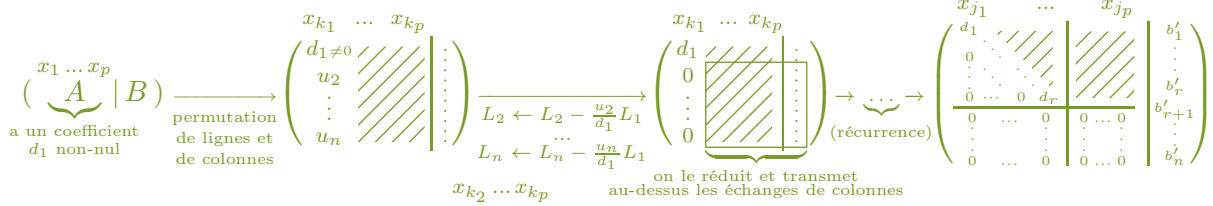
Ainsi, quand $r = n = p$ (« système de Cramer ») le système (E) a une unique solution.

(*) Pour un point de vue sans échanges de colonnes, voir la fin de ce paragraphe (« matrices échelonnées »).

Les échanges de deux colonnes peuvent permettre de minimiser les erreurs d'arrondis sur ordinateur : en travaillant sur la j^{e} colonne on choisirait comme pivot a_{i_0, j_0} avec $i_0, j_0 \geq j$ tels que $|a_{i_0, j_0}| = \max_{i', j' \geq j} |a_{i', j'}|$.

DÉMONSTRATION

(a) On écarte le cas $A = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$ qui donnerait $r = 0$ et $A' = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix}$. On a :



où on s'arrête quand le rectangle $(\tilde{A} \mid \tilde{B})$ qu'on réduit par récurrence sur n vérifie $\tilde{A} = 0$.

(b) (c) D'après le lemme du 2, et le fait qu'un échange de colonnes donne deux systèmes linéaires équivalents, (E) équivaut à :

$$(E') \begin{cases} d_1 x_{j_1} + \dots = b'_1 \\ d_1 x_{j_2} + \dots = b'_2 \\ \vdots \\ d_1 x_{j_r} + \dots = b'_r \\ 0 = b'_{r+1} \\ \vdots \\ 0 = b'_n \end{cases} \quad \text{c'est-à-dire à :} \quad \begin{cases} x_{j_{r+1}} = t_1 \\ \vdots \\ x_{j_p} = t_{p-r} \\ x_{j_r} = \frac{1}{d_r}(\dots) \\ \vdots \\ x_{j_1} = \frac{1}{d_1}(\dots) \end{cases} \quad \text{à exprimer avec } t_1, \dots, t_{p-r} \quad \square$$

$b'_{r+1} = \dots = b'_n = 0$ et $\exists t_1, \dots, t_{p-r} \in \mathbb{K}$

Remarques

1. Quand (E) a strictement plus d'inconnues que d'équations (c'est-à-dire $p > n$) et $\mathcal{S}_E \neq \emptyset$ (par exemple (E) est homogène), on a : $\underbrace{p - r}_{\text{nombre de paramètres}} > n - r \geq 0$, donc \mathcal{S}_E est infini.

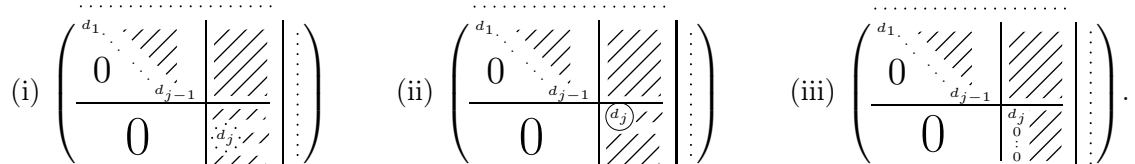
Tout système linéaire homogène dont le nombre d'inconnues est strictement supérieur au nombre d'équations admet une infinité de solutions.

2. La matrice $(A'|B')$ dépend des opérations sur les lignes et les colonnes qu'on a utilisées. Cependant, on verra dans la suite du cours que :

- r ne dépend que de A , et sera appelé « le rang de A » ;
- \mathcal{S}_E n'a pas d'équation paramétrique avec strictement moins que $p - r$ paramètres ; (lorsque $\mathcal{S}_E: AX = B$ et $\mathcal{S}_E = \{UT + V; T \in \mathbb{K}^k\}$, on a : $k \geq \dim \overrightarrow{\mathcal{S}_E} = \dim \text{Ker } A = p - r$)
- une équation cartésienne obtenue par la méthode de Gauss à partir d'une équation paramétrique a un nombre d'égalités qui est minimal. (lorsque $\mathcal{E} = \{AT + C; T \in \mathbb{K}^p\}$ et $\mathcal{E}: UX = V$, on a : $\text{rg } U = n - \dim \overrightarrow{\mathcal{E}} = n - r$)

Algorithme 1 (« pivot total » au sens où on cherche d_j dans n'importe quelle colonne)

On détaille la méthode de la démonstration pour construire $(A' \mid B')$ comme au (b). On utilise une construction par récurrence. On construit la j^e colonne à l'étape $j \in \{1, \dots, p\}$:



(i) On choisit une colonne $C_{j'}$ avec $j \leq j' \leq p$ qui a, à partir de la j^e ligne, au moins un coefficient $d_{j'} \neq 0$ (s'il n'y a pas une telle colonne on arrête), puis on échange C_j et $C_{j'}$.

(ii) On échange la j^e ligne avec la ligne contenant d_j .

(iii) On amène des 0 strictement au-dessous de d_j par des opérations sur les lignes (composées de deux opérations élémentaires) de la forme $L_i \leftarrow c_i L_i + c_j L_j$ avec $c_i \neq 0$ quand $i > j$.

Après avoir travaillé sur toutes les colonnes en reportant les opérations sur les lignes au niveau de la colonne à droite de la barre verticale, on regarde si les membres de droite des égalités dont le membre de gauche est 0 vaut lui-même 0 (sinon le système n'a pas de solution) auquel cas on résout le système en remontant de la dernière égalité à la première égalité.

Remarques

- En pratique, on exploitera la proposition précédente en allégeant la présentation :
- lorsque $B = 0$ on ne fera pas apparaître la dernière colonne (seconds membres nuls) ;
 - on n'introduira les noms des variables au dessus des p premières colonnes qu'à partir du moment où un échange de colonnes aura été introduit (ce qui est rarement indispensable) ;
 - on résoudra « de tête » le système triangulaire correspondant à la dernière étape de la méthode de Gauss, en partant de la dernière égalité et remontant vers la première.

Exemples (cf. l'introduction de la partie I de ce chapitre)

1. Fin de la résolution de (E_{cart}) :

$$\left(\begin{array}{ccc|c} -4 & 12 & -5 & 1 \\ 1 & -3 & 2 & -1 \\ 2 & -6 & 1 & 1 \end{array} \right) \xrightarrow{\text{déjà vu}} \left(\begin{array}{ccc|c} 1 & -3 & 2 & -1 \\ 0 & 0 & 3 & -3 \\ 0 & 0 & -3 & 3 \end{array} \right) \xrightarrow{C_2 \leftrightarrow C_3} \left(\begin{array}{ccc|c} 1 & 2 & -3 & -1 \\ 0 & 3 & 0 & -3 \\ 0 & -3 & 0 & 3 \end{array} \right) \xrightarrow{L_3 \leftarrow L_3 + L_2} \left(\begin{array}{ccc|c} 1 & 2 & -3 & -1 \\ 0 & 3 & 0 & -3 \\ 0 & 0 & 0 & 0 \end{array} \right).$$

En renommant dans la conclusion la variable y en t , et calculant d'abord z puis ensuite x , on obtient l'équation paramétrique suivante de $\mathcal{S}_{E_{\text{cart}}}$:

$$\mathcal{S}_{E_{\text{cart}}} : \begin{cases} x = \frac{1}{1}(-2(-1) + 3t - 1) = 3t + 1 \\ y = t \\ z = \frac{1}{3}(-3) = -1 \end{cases}, \quad t \in \mathbb{K}.$$

2. Soit $(x, y) \in \mathbb{K}^2$. Existence de $(s, t) \in \mathbb{K}^2$ vérifiant $(E_{\text{param}}) \begin{cases} s - t = x - 1 \\ -s + t = y - 2 \end{cases} ?$

Calcul par la méthode de Gauss : $\left(\begin{array}{cc|c} 1 & -1 & x-1 \\ -1 & 1 & y-2 \end{array} \right) \xrightarrow{L_2 \leftarrow L_2 + L_1} \left(\begin{array}{cc|c} 1 & -1 & x-1 \\ 0 & 0 & x+y-3 \end{array} \right)$.

Ainsi $\mathcal{D} : \begin{cases} x = s - t + 1 \\ y = -s + t + 2 \end{cases}, s, t \in \mathbb{K}$ a pour équation cartésienne : $\mathcal{D} : x + y - 3 = 0$.

(Inutile de calculer explicitement les valeurs des paramètres s et t en fonction de x et y .)

3. Le système $(E_C) \begin{cases} 3x + 2y = 5 \\ 2x - y = 4 \end{cases}$ se résout ainsi : $\left(\begin{array}{cc|c} 3 & 2 & 5 \\ 2 & -1 & 4 \end{array} \right) \xrightarrow{L_2 \leftarrow 3L_2 - 2L_1} \left(\begin{array}{cc|c} 3 & 2 & 5 \\ 0 & -7 & 2 \end{array} \right)$.

C'est un système de Cramer d'unique solution donnée par : $\begin{cases} x = \frac{1}{3}(-2(-\frac{2}{7}) + 5) = \frac{13}{5} \\ y = -\frac{2}{7} \end{cases}$.

Définition (« méthode de Gauss sans échange de colonnes »)

(a) Une *matrice échelonnée* — suivant les lignes — est une matrice telle que le nombre de termes nuls au début de chaque ligne augmente lorsqu'on passe d'une ligne à la suivante, et ce nombre augmente même strictement lorsqu'on passe d'une ligne non nulle à la suivante.

Il s'agit d'une matrice de la forme $\left(\begin{array}{ccc|ccc|ccc|ccc} 0 & \dots & 0 & d_1 & \dots & \dots & 0 & \dots & 0 & \dots & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 \end{array} \right)$ avec $d_1 \neq 0, \dots, d_r \neq 0$.

(b) Une *matrice échelonnée réduite* est une matrice échelonnée dans laquelle les premiers termes non-nuls sur chaque ligne sont des 1 au-dessus desquels se trouvent des 0. Elle s'écrit :

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 0 & \dots & 0 & 1 & \dots & \dots & 0 & \dots & 0 & \dots & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 \end{array} \right).$$

Proposition

Il existe une unique matrice échelonnée réduite E_A qui se déduit de A par des opérations élémentaires sur les lignes.

Exemples

On considère : $U = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$, $V = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$, $W = \begin{pmatrix} 0 & -1 & 2 \\ 3 & 4 & -6 \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$.

Les sommes et produits possibles de 2 matrices différentes parmi U, V, W, X sont :

$$U + V = V + U = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix};$$

$$UV = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix} \text{ et } VU = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \text{ donc } UV \neq VU;$$

$$UW = \begin{pmatrix} -3 & -5 & 8 \\ 3 & 5 & -8 \end{pmatrix} \text{ et } VW = \begin{pmatrix} 3 & 3 & -4 \\ 6 & 6 & -8 \end{pmatrix};$$

$$WX = \begin{pmatrix} -y + 2z \\ 3x + 4y - 6z \end{pmatrix}, \text{ ce qui est compatible avec la notation } \ll (E) : AX = B \gg.$$

Remarque

Dans l'exemple ci-dessus, on pourrait calculer U^n et V^n pour $n \in \mathbb{N}$ car U et V sont carrées.

Dans le cas favorable où des matrices carrées A et B commutent on peut déduire des A^n et B^n les puissances de $A + B$. En effet, la formule du binôme se généralise facilement ainsi :

si $A, B \in \mathfrak{M}(p, \mathbb{K})$ vérifient $AB = BA$, alors $(A + B)^n = \sum_{k=0}^n \binom{n}{k} A^{n-k} B^k$ pour tout $n \in \mathbb{N}$.

Proposition

(a) Soient $A, B, C \in \mathfrak{M}_{n,p}(\mathbb{K})$, et $\lambda, \mu \in \mathbb{K}$.

$$\text{On a : } \begin{cases} 1A = A, \quad A + 0 = A \text{ et } A + (-A) = 0 \\ (A + B) + C = A + (B + C) \text{ et } A + B = B + A \\ \lambda(A + B) = (\lambda A) + (\lambda B) \text{ et } (\lambda + \mu)A = (\lambda A) + (\mu A) \\ \lambda(\mu A) = (\lambda\mu)A \end{cases}$$

(Cela s'exprimera en disant que « $(\mathfrak{M}_{n,p}(\mathbb{K}), +, \cdot)$ est un \mathbb{K} -espace vectoriel ».)

(b) Soient $A, A_1, A_2 \in \mathfrak{M}_{n,p}(\mathbb{K})$, $B, B_1, B_2 \in \mathfrak{M}_{p,q}(\mathbb{K})$, $C \in \mathfrak{M}_{q,r}(\mathbb{K})$, et $\lambda \in \mathbb{K}$.

$$\text{On a : } \begin{cases} I_n A = A = A I_p \\ (AB)C = A(BC) \\ A(B_1 + B_2) = (AB_1) + (AB_2) \text{ et } (A_1 + A_2)B = (A_1 B) + (A_2 B) \\ \lambda(AB) = (\lambda A)B = A(\lambda B) \end{cases}$$

En particulier : $(\mathfrak{M}(n, \mathbb{K}), +, \cdot)$ est un anneau.

← [non-commutatif quand $n \geq 2$]

DÉMONSTRATION

Exercice. □

Définition-Proposition

(a) Une *décomposition en blocs de taille* $\overbrace{(n_1, \dots, n_N)}^{\in \mathbb{N}^N} \times \overbrace{(p_1, \dots, p_P)}^{\in \mathbb{N}^P}$ d'une matrice $A \in \mathfrak{M}_{n,p}(\mathbb{K})$ est la donnée de matrices $A_{i,j} \in \mathfrak{M}_{n_i, p_j}(\mathbb{K})$, $i \in \{1, \dots, N\}$ et $j \in \{1, \dots, P\}$, telles que :

$$A = \begin{pmatrix} \xrightarrow{p_1} & \xrightarrow{p_P} \\ \downarrow n_1 & \downarrow n_N \\ A_{1,1} & \dots & A_{1,P} \\ \vdots & & \vdots \\ A_{N,1} & \dots & A_{N,P} \end{pmatrix} \quad \text{où les parenthèses des matrices } A_{i,j} \text{ ont été enlevées.}$$

(b) Soient $\lambda \in \mathbb{K}$ et deux matrices $A, B \in \mathfrak{M}_{n,p}(\mathbb{K})$ décomposées en blocs $(A_{i,j})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq P}}$ et $(B_{i,j})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq P}}$ de même taille. On a : $\lambda A = (\lambda A_{i,j})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq P}}$ et $A + B = (A_{i,j} + B_{i,j})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq P}}$.

(c) Soient $A \in \mathfrak{M}_{n,p}(\mathbb{K})$ et $B \in \mathfrak{M}_{p,q}(\mathbb{K})$ décomposées en blocs $A = (A_{i,j})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq P}}$ de taille $(n_1, \dots, n_N) \times (p_1, \dots, p_P)$ et $B = (B_{j,k})_{\substack{1 \leq j \leq P \\ 1 \leq k \leq Q}}$ de taille $(p_1, \dots, p_P) \times (q_1, \dots, q_Q)$.

On a la décomposition en blocs suivante : $AB = (C_{i,j})_{\substack{1 \leq i \leq N \\ 1 \leq j \leq Q}}$ avec $C_{i,j} = \sum_{k=1}^P A_{i,k} B_{k,j}$.

DÉMONSTRATION

(b) Calcul immédiat.

(c) Soit $(u, v) \in \{1, \dots, n\} \times \{1, \dots, q\}$. On peut écrire u et v sous la forme :

$$u = n_1 + \dots + n_{i-1} + r \text{ avec } 1 \leq r \leq n_i \text{ et } v = q_1 + \dots + q_{j-1} + s \text{ avec } 1 \leq s \leq q_j.$$

En notant $M(i, j)$ le coefficient d'indice (i, j) d'une matrice M , on a :

$$\begin{aligned} (AB)_{(u,v)} &= \sum_{w=1}^{p_1} A(u,w)B(w,v) + \sum_{w=p_1+1}^{p_1+p_2} A(u,w)B(w,v) + \dots + \sum_{w=p_1+\dots+p_{P-1}+1}^{p_1+\dots+p_P} A(u,w)B(w,v) \\ &= \sum_{t=1}^{p_1} A(u,t)B(t,v) + \sum_{t=1}^{p_2} A(u,p_1+t)B(p_1+t,v) + \dots + \sum_{t=1}^{p_P} A(u,p_1+\dots+p_{P-1}+t)B(p_1+\dots+p_{P-1}+t,v) \\ &= \sum_{t=1}^{p_1} A_{i,1}(r,t)B_{1,j}(t,s) + \sum_{t=1}^{p_2} A_{i,2}(r,t)B_{2,j}(t,s) + \dots + \sum_{t=1}^{p_P} A_{i,P}(r,t)B_{1,j}(t,s) \\ &= \sum_{k=1}^P \left(\sum_{t=1}^{p_k} A_{i,k}(r,t)B_{k,j}(t,s) \right) = \sum_{k=1}^P (A_{i,k}B_{k,j})(r,s) = C_{i,j}(r,s). \end{aligned}$$

D'où le résultat. □

Exemples

On va délimiter des blocs par des traits horizontaux et verticaux.

(1) Exemple de calcul pour illustrer le point (c) :

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 2 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \\ 5 & 6 \end{pmatrix} = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix} (5 \ 6) \right) = \left(\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 5 & 6 \\ -5 & -6 \end{pmatrix} \right) = \begin{pmatrix} 7 & 10 \\ 6 & 9 \\ -1 & 4 \end{pmatrix}.$$

(2) Cas des matrices augmentées :

$$P(A|B) = (PA|PB) \text{ quand } P \in \mathfrak{M}(n, \mathbb{K}), A \in \mathfrak{M}_{n,p}(\mathbb{K}) \text{ et } B \in \mathbb{K}^n.$$

2. Transposée d'une matrice, trace d'une matrice carrée

Définition (matrices rectangulaires)

$$\text{Soit } A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \in \mathfrak{M}_{n,p}(\mathbb{K}).$$

$$\text{On appelle } \textit{matrice transposée de } A \text{ la matrice } {}^tA := \begin{pmatrix} a_{11} & \dots & a_{n1} \\ \dots & \dots & \dots \\ a_{1p} & \dots & a_{np} \end{pmatrix} \in \mathfrak{M}_{p,n}(\mathbb{K}).$$

Cela signifie que : ${}^tA = (a'_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$ où $a'_{ij} := a_{ji}$ quand $1 \leq i \leq p$ et $1 \leq j \leq n$.

Proposition

Soient $A \in \mathfrak{M}_{n,p}(\mathbb{K})$ et $B \in \mathfrak{M}_{p,q}(\mathbb{K})$. On a : ${}^tB {}^tA$ est définie et ${}^t(AB) = {}^tB {}^tA$.

DÉMONSTRATION

$$\text{On pose } A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \text{ et } B = (b_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq q}}.$$

$$\text{Donc : } {}^tA = (a'_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} \text{ et } {}^tB = (b'_{ij})_{\substack{1 \leq i \leq q \\ 1 \leq j \leq p}}, \text{ avec } a'_{ij} := a_{ji} \text{ et } b'_{ij} := b_{ji}.$$

$$\text{D'une part : } AB = (c_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq q}} \text{ avec } c_{ij} = \sum_{k=1}^p a_{ik}b_{kj}, \text{ puis } {}^t(AB) = (c'_{ij})_{\substack{1 \leq i \leq q \\ 1 \leq j \leq n}} \text{ avec } c'_{ij} := c_{ji}.$$

$$\text{D'autre part : } {}^tB {}^tA = (d_{ij})_{\substack{1 \leq i \leq q \\ 1 \leq j \leq n}} \text{ avec } d_{ij} = \sum_{k=1}^p b'_{ik}a'_{kj}.$$

$$\text{Finalement : } c'_{ij} = \sum_{k=1}^p a_{jk}b_{ki} = \sum_{k=1}^p a'_{kj}b'_{ik} = d_{ij}, \text{ ce qui s'écrit } {}^t(AB) = {}^tB {}^tA.$$

Variante

$${}^t(AB)(i, j) = (AB)(j, i) = \sum_{k=1}^p A(j, k)B(k, i) = \sum_{k=1}^p ({}^tB)(i, k)({}^tA)(k, j) = ({}^tB {}^tA)(i, j). \quad \square$$

Définition (matrices carrées)

Soit $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in \mathfrak{M}(n, \mathbb{K})$.

(a) On dit que A est *symétrique* si ${}^tA = A$ (c'est-à-dire $a_{ji} = a_{ij}$ quand $1 \leq i < j \leq n$).

(b) On appelle *trace* de A , l'élément de \mathbb{K} noté $\text{tr } A$, défini par :

$$\text{tr } A = \sum_{i=1}^n a_{i,i} = a_{1,1} + \cdots + a_{n,n}.$$

Proposition

Soient $A \in \mathfrak{M}_{n,p}(\mathbb{K})$ et $B \in \mathfrak{M}_{p,n}(\mathbb{K})$. On a : $\text{tr}(AB) = \text{tr}(BA)$.

DÉMONSTRATION

On pose $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}}$ et $B = (b_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$.

On a : $AB = (c_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq q}}$ avec $c_{ij} = \sum_{k=1}^p a_{ik}b_{kj}$, donc $\text{tr}(AB) = \sum_{i=1}^n c_{i,i} = \sum_{i=1}^n \left(\sum_{k=1}^n a_{ik}b_{ki} \right)$.

On conclut en intervertissant $\sum_{i=1}^n$ et $\sum_{k=1}^n$. □

3. Matrices carrées inversibles

Définition-Proposition

(a) Soit $A \in \mathfrak{M}(n, \mathbb{K})$. On dit que A est *inversible* s'il existe $B \in \mathfrak{M}(n, \mathbb{K})$ tel que :

$$AB = I_n \text{ et } BA = I_n.$$

Dans ce cas B est unique, notée A^{-1} , et appelée *inverse* de A .

(b) On note $GL(n, \mathbb{K})$ l'ensemble des éléments inversibles de $\mathfrak{M}(n, \mathbb{K})$.

DÉMONSTRATION

On se place dans la situation du (a) avec deux « inverses » potentiels : si $B, C \in \mathfrak{M}(n, \mathbb{K})$ vérifient $AB = I_n$ et $CA = I_n$, alors $C = CI_n = C(AB) = (CA)B = I_n B = B$. □

Remarque (importante)

On suppose que $A \in \mathfrak{M}(n, \mathbb{K})$ est inversible et $B \in \mathbb{K}^n$.

Le système $(E) : AX = B$ d'inconnue $X \in \mathbb{K}^n$ équivaut à l'équation $A^{-1}(AX) = A^{-1}B$.

Il a donc pour unique solution $X := A^{-1}B$. ←[dans ce cas le nombre de paramètres $n - r$ pour les solutions est nul]

Proposition

(a) Soit $A \in \mathfrak{M}(n, \mathbb{K})$ inversible. La matrice A^{-1} est inversible et $\boxed{(A^{-1})^{-1} = A}$.

(b) Soit $A \in \mathfrak{M}(n, \mathbb{K})$ inversible. La matrice tA est inversible et $\boxed{({}^tA)^{-1} = {}^t(A^{-1})}$.

(c) Soient $A, B \in \mathfrak{M}(n, \mathbb{K})$ inversibles. La matrice AB est inversible et $\boxed{(AB)^{-1} = B^{-1}A^{-1}}$.

DÉMONSTRATION

(a) Il suffit de remarquer qu'en posant $B := A^{-1}$, on a : $A^{-1}B = I_n$ et $BA^{-1} = I_n$.

(b) D'après la fin du 2, on a : ${}^tA {}^t(A^{-1}) = {}^t(\underbrace{A^{-1}A}_{I_n}) = I_n$ et ${}^t(A^{-1}) {}^tA = {}^t(\underbrace{AA^{-1}}_{I_n}) = I_n$.
Donc tA est inversible d'inverse ${}^t(A^{-1})$.

(c) Il suffit encore de tester l'inverse proposé :
 $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$
et $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$. □

Lemme

On se donne une suite finie d'opérations élémentaires sur les lignes des matrices à n lignes. Il existe une matrice inversible $P \in \mathfrak{M}(n, \mathbb{K})$ telle que cette suite d'opérations élémentaires envoie toute matrice $M \in \mathfrak{M}_{n,p}(\mathbb{K})$ sur PM . ←[il en résulte d'ailleurs que P est l'image de I_n]

• On suppose (iii) vrai. La matrice C vérifie l'analogie du (ii) avec le rôle de A . On vient de voir que « (ii) \Rightarrow (i) ». On en déduit que C est inversible, puis $A = C^{-1}(CA) = C^{-1}$.

Ainsi (i) est vrai et $A^{-1} = C$. □

Remarques

1. La condition (iv) de la proposition signifie que I_n est l'unique matrice échelonnée réduite qui se déduit de A par des opérations élémentaires sur les lignes.

2. L'ensemble des transformations obtenues à l'issue d'une suite finie d'opérations élémentaires sur les lignes des matrices à n lignes est égal à celui des transformations $M \mapsto PM$ avec $P \in \mathfrak{M}(n, \mathbb{K})$ inversible. En effet :

(\subseteq) toute suite finie d'opérations élémentaires sur les lignes des matrices à n lignes s'écrit d'après le lemme $M \mapsto PM$ pour un certain $P \in \mathfrak{M}(n, \mathbb{K})$ inversible ;

(\supseteq) étant donné $P \in \mathfrak{M}(n, \mathbb{K})$ inversible, il existe d'après la proposition une suite finie Σ d'opérations élémentaires sur les lignes qui envoie P^{-1} sur I_n , et comme Σ est d'après le lemme de la forme $M \mapsto QM$ avec $Q \in \mathfrak{M}(n, \mathbb{K})$ inversible, l'égalité $\underbrace{QP^{-1}}_{\text{signifie que } Q=P} = I_n$ obtenue en choisissant $M = P^{-1}$ montre aussi que Σ s'écrit $M \mapsto PM$.

Algorithme (calcul de l'inverse d'une matrice par la « méthode de Gauss-Jordan »)

On suppose que A est inversible. On va construire A^{-1} par des opérations sur les lignes de A .

On applique la méthode de Gauss sans échange de colonnes sur A dans $(A|I)$ en travaillant colonne par colonne de la gauche vers la droite pour faire apparaître des zéros en dehors de la diagonale. Une dernière étape permet de faire apparaître I à gauche de la barre verticale.

On utilise une construction par récurrence. On s'intéresse à la j^{e} ligne à l'étape $j \in \{1, \dots, n\}$:

$$(i) \left(\begin{array}{ccc|c} a_1 & \dots & 0 & \boxed{} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & a_{j-1} & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & \vdots \end{array} \right) \quad (ii) \left(\begin{array}{ccc|c} a_1 & \dots & 0 & \boxed{} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & a_{j-1} & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & d_j \end{array} \right) \quad (iii) \left(\begin{array}{ccc|c} a_1 & \dots & 0 & \boxed{} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & a_{j-1} & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & d_j \end{array} \right).$$

(i) On choisit dans la j^{e} colonne à gauche de la barre verticale un coefficient $d_j \neq 0$ (existe).

(ii) On échange la j^{e} ligne de la matrice augmentée avec la ligne contenant d_j .

(iii) On amène des 0 strictement au-dessus et au-dessous de d_j par des opérations sur les lignes de la matrice augmentée de la forme $L_i \leftarrow c_i L_i + c_j L_j$ avec $c_i \neq 0$ quand $i \neq j$.

En fin de calcul on divise chacune des lignes de la matrice augmentée par son coefficient d_j . La matrice A^{-1} est la matrice qui se trouve à droite de la barre verticale.

Exemple

$A := \begin{pmatrix} 5 & 4 \\ 6 & 5 \end{pmatrix}$ est-elle inversible ? Si oui, que vaut A^{-1} ?

On a : $(A|I) = \left(\begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 6 & 5 & 0 & 1 \end{array} \right) \xrightarrow{L_2 \leftarrow 5L_2 - 6L_1} \left(\begin{array}{cc|cc} 5 & 4 & 1 & 0 \\ 0 & 1 & -6 & 5 \end{array} \right) \xrightarrow{L_1 \leftarrow L_1 - 4L_2} \left(\begin{array}{cc|cc} 5 & 0 & 25 & -20 \\ 0 & 1 & -6 & 5 \end{array} \right) \xrightarrow{L_1 \leftarrow \frac{1}{5}L_1} \left(\begin{array}{cc|cc} 1 & 0 & 5 & -4 \\ 0 & 1 & -6 & 5 \end{array} \right).$
 (On verra plus bas que le calcul de rang à mi-chemin prouve à cette étape que A est inversible.)

D'après la proposition précédente : A est inversible et $A^{-1} = \begin{pmatrix} 5 & -4 \\ -6 & 5 \end{pmatrix}$.

[On disposera aussi plus tard (en L2) d'une formule simple pour A^{-1} quand $A \in GL(2, \mathbb{K})$.]

4. Rang

La définition qui suit va utiliser la notion de rang d'une famille (v_1, \dots, v_p) avec $v_1, \dots, v_p \in \mathbb{K}^n$, qui ne sera introduite que dans le chapitre suivant. En première lecture on admettra donc que le nombre r qui apparaîtra dans l'algorithme qui va suivre la définition est indépendant de la matrice A' , et considèrera que c'est pour l'instant ce nombre qui sera appelé *rang de A* .

Définition

Soit $A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \in \mathfrak{M}_{n,p}(\mathbb{K})$.

On note : $\text{rg } A := \text{rg} \left(\left(\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1p} \\ \vdots \\ a_{np} \end{pmatrix} \right) \right) \in \mathbb{N}$.

Algorithme

On transforme $A := \begin{pmatrix} x_1 & \dots & x_p \\ a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$ en $A' = \begin{pmatrix} x_{j_1} & \dots & x_{j_r} & x_{j_{r+1}} & \dots & x_{j_p} \\ d_1 & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & \dots & \dots \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & d_r & \dots & \dots \\ \hline 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$

par la méthode de Gauss, avec $d_1 \neq 0, \dots, d_r \neq 0$.

On a : $\boxed{\text{rg } A = r}$ « calcul du rang par la méthode de Gauss ».

(Le nombre r est donc indépendant de la manière dont on applique la méthode de Gauss.)

DÉMONSTRATION

On note v_1, \dots, v_p les colonnes de A et montre que $(v_{j_1}, \dots, v_{j_r})$ est une base de $\text{Vect}(v_1, \dots, v_p)$.

• On vérifie que la famille $(v_{j_1}, \dots, v_{j_r})$ est libre. On montre que $(\star) \alpha_1 v_{j_1} + \dots + \alpha_r v_{j_r} = 0$ d'inconnue $(\alpha_1, \dots, \alpha_r) \in \mathbb{K}^r$ a pour seule solution $(0, \dots, 0)$.

On reprend le calcul permettant de passer de A à A' en ne prenant en compte que les colonnes qui sont sous les symboles x_{j_1}, \dots, x_{j_r} . On constate à la fin du calcul que l'équation (\star) a une unique solution : $(\alpha_1, \dots, \alpha_r) = (0, \dots, 0)$.

Variante

On a : $(\star) \iff \alpha_1 v_{j_1} + \dots + \alpha_r v_{j_r} + 0v_{j_{r+1}} + \dots + 0v_{j_p} = 0 \iff A' \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

En revenant à un système linéaire, on constate que l'équation (\star) a pour seule solution $(0, \dots, 0)$.

• On vérifie maintenant que $(v_{j_1}, \dots, v_{j_r})$ engendre $\text{Vect}(v_1, \dots, v_p)$. Soit $k \in \{r+1, \dots, p\}$. On montre que l'équation $(\star\star) \alpha_1 v_{j_1} + \dots + \alpha_r v_{j_r} = v_{j_k}$ d'inconnue $(\alpha_1, \dots, \alpha_r) \in \mathbb{K}^r$ a au moins une solution. Le résultat en découlera car on aura ensuite $\underbrace{\text{Vect}(v_1, \dots, v_p)}_{\text{plus petit sous-espace vectoriel de } \mathbb{K}^n \text{ contenant } v_1, \dots, v_p} \subseteq \text{Vect}(v_{j_1}, \dots, v_{j_r})$.

On reprend le calcul permettant de passer de A à A' en ne prenant en compte que les colonnes qui sont sous les symboles x_{j_1}, \dots, x_{j_r} et x_{j_k} , et place une barrière verticale juste avant la dernière colonne. On constate que $(\star\star)$ a une solution (des 0 à droite au bons endroits).

Variante

On a : $(\star\star) \iff \alpha_1 v_{j_1} + \dots + \alpha_r v_{j_r} + 0v_{j_{r+1}} + \dots + (-1)v_{j_k} + \dots + 0v_{j_p} = 0 \iff A' \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \\ 0 \\ \vdots \\ -1 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Une remontée triangulaire fournira une solution de $(\star\star)$. \square

Remarque

Lorsqu'on adopte le point de vue de la méthode de Gauss sans permutation de colonnes, qui fournit une matrice échelonnée A' pas forcément réduite, le rang de A reste égal au nombre de pivots non nuls qui apparaissent dans la matrice A' .

Proposition

Soit $A \in \mathfrak{M}(n, \mathbb{K})$.

On a : A est inversible si et seulement si $\text{rg } A = n$.

DÉMONSTRATION

(\Rightarrow) On suppose que A est inversible. Elle vérifie la condition (iv) de la dernière proposition, et on a donc $\text{rg } A = n$ en calculant $\text{rg } A$ par la méthode de Gauss.

(\Leftarrow) On suppose que $\text{rg } A = n$. On reproduit la démonstration de l'implication (ii) \Rightarrow (iv) de la dernière proposition en remplaçant l'hypothèse (ii) par l'hypothèse « $\text{rg } A = n$ ».

La matrice PA fournit $\text{rg } A$. Elle a donc n blocs $\llcorner \llcorner$, puis (iv) est vérifié et A est inversible. \square

Proposition

Soit $A \in \mathfrak{M}_{n,p}(\mathbb{K})$. On a : $\text{rg}({}^tA) = \text{rg}(A)$.

DÉMONSTRATION (une variante sera donnée plus tard)

On calcule le rang r de A par la méthode de Gauss, ce qui donne A' avec r lignes non-nulles.

On pose : $A' = \begin{pmatrix} \xrightarrow{r} & \xrightarrow{p-r} \\ U & V \\ 0 & 0 \end{pmatrix} \downarrow r$ avec U triangulaire supérieure de termes diagonaux non-nuls.

On passe de A à A' à l'aide d'opérations élémentaires sur les lignes de matrices associées P_1, \dots, P_k dans $GL(n, \mathbb{K})$, et aussi à l'aide d'échanges $C_i \leftrightarrow C_j$ de colonnes pour lesquels on note R_1, \dots, R_L les matrices associées aux $L_i \leftrightarrow L_j$ dans $GL(p, \mathbb{K})$. On a : $P_k \dots P_1 A R_1 \dots R_L = A'$.

D'où : $P_k \dots P_1 A R_1 \dots R_L = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} U & V \\ 0 & I_{p-r} \end{pmatrix}$ avec $\begin{pmatrix} U & V \\ 0 & I_{p-r} \end{pmatrix} \in GL(p, \mathbb{K})$ vu son rang.

Cela fournit $P \in GL(n, \mathbb{K})$ et $Q \in GL(p, \mathbb{K})$ tels que : $A = P \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Q$.

On en déduit que : ${}^tA = {}^tQ \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} {}^tP$ avec ${}^tP \in GL(n, \mathbb{K})$ et ${}^tQ \in GL(p, \mathbb{K})$.

On peut donc passer de tA à $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} {}^tP$ par des opérations élémentaires sur les lignes.

La dernière matrice dont les $p - r$ dernières lignes sont nulles a un rang $\leq r$.

Ainsi $\text{rg}({}^tA) \leq \text{rg}(A)$. De même $\text{rg} A = \text{rg}({}^t({}^tA)) \leq \text{rg}({}^tA)$. Cela donne le résultat. \square

Plan

- I. Règles de calcul
- II. Constructions
- III. Bases et dimension

I. RÈGLES DE CALCUL

1. Généralités

Définition-Proposition

(a) On appelle *espace vectoriel sur \mathbb{K}* (ou \mathbb{K} -*ev*) un ensemble E muni de deux applications

$$\begin{aligned}
 E \times E &\longrightarrow E & \text{et} & & \mathbb{K} \times E &\longrightarrow E & \text{telles que :} \\
 (v, w) &\longmapsto v + w & & & (\alpha, v) &\longmapsto \underbrace{\alpha v}_{\text{noté par la suite } \alpha v}
 \end{aligned}$$

- (i) $(u + v) + w = u + (v + w)$ et $u + v = v + u$ pour tous $u, v, w \in E$;
- (ii) il existe un élément $\underbrace{0_E}_{\text{noté par la suite } 0}$ de E tel que $v + 0_E = v$ pour tout $v \in E$
et dans ce cas, compte tenu de (i) cet élément 0_E est unique ;
- (iii) pour tout $v \in E$, il existe un élément $-v$ de E tel que $v + (-v) = 0_E$
et dans ce cas, compte tenu de (i) et (ii) cet élément $-v$ est unique ;
- (iv) $\alpha(v + w) = (\alpha v) + (\alpha w)$ et $(\alpha + \beta)v = (\alpha v) + (\beta v)$
pour tous $\alpha, \beta \in \mathbb{K}$ et $v, w \in E$;
- (v) $1v = v$ et $\alpha(\beta v) = (\alpha\beta)v$ pour tous $\alpha, \beta \in \mathbb{K}$ et $v \in E$.

(b) Étant donné un \mathbb{K} -espace vectoriel $(E, +, \times)$ comme au (a), on appellera *scalaires* les éléments de \mathbb{K} et *vecteurs* les éléments de E .

On notera : $v - w = v + (-w)$ quand $v, w \in E$.

DÉMONSTRATION

Il s'agit de prouver les deux cas d'unicité signalés au (a).

(ii) Pour tout candidat $\tilde{0}$ au rôle de 0_E , on a d'après (i) :

$$\tilde{0} = \tilde{0} + 0_E = 0_E + \tilde{0} = 0_E.$$

(iii) Pour tout candidat \tilde{v} au rôle de $-v$, on a aussi d'après (i) et (ii) :

$$\tilde{v} = \tilde{v} + 0_E = \tilde{v} + (v + (-v)) = (\tilde{v} + v) + (-v) = (v + \tilde{v}) + (-v) = 0_E + (-v) = -v. \quad \square$$

Remarques

On se donne un \mathbb{K} -espace vectoriel E .

(1) Pour $\alpha \in \mathbb{K}$ et $v \in E$, on a :

$$\begin{aligned}
 0v &= 0v + (1v - v) = 0_E ; \\
 \alpha 0_E &= \alpha(0_E + 0_E) - \alpha 0_E = 0_E ; \\
 (-\alpha)v &= (-\alpha + \alpha)v - (\alpha v) = -(\alpha v).
 \end{aligned}$$

(2) Règles de simplification. Pour $\alpha, \beta \in \mathbb{K}$ et $u, v, w \in E$, on a :

$$\begin{aligned}
 u + v = u + w &\implies v = w ; && \text{(ajouter } -u \text{ à chaque membre)} \\
 \alpha v = 0_E &\implies \alpha = 0 \text{ ou } v = 0_E ; && \text{(si } \alpha \neq 0, \text{ multiplier chaque membre par } \frac{1}{\alpha}) \\
 \alpha v = \alpha w \text{ et } \alpha \neq 0 &\implies v = w ; && \text{(tout faire passer au premier membre)} \\
 \alpha v = \beta v \text{ et } v \neq 0_E &\implies \alpha = \beta. && \text{(tout faire passer au premier membre)}
 \end{aligned}$$

2. Exemples

Exemple 1

Soit $n \in \mathbb{N}$. L'ensemble \mathbb{K}^n des n -uplets (x_1, \dots, x_n) d'éléments x_1, \dots, x_n de \mathbb{K} , muni de
 $(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n)$ et $\alpha \times (x_1, \dots, x_n) := (\alpha x_1, \dots, \alpha x_n)$
est un \mathbb{K} -espace vectoriel (clair). Ses éléments sont les applications $i \mapsto x_i$ de $\{1, \dots, n\}$ dans \mathbb{K} .
Par convention, on écrira : $\mathbb{K}^0 := \{0\} \subseteq \mathbb{K}$ en « identifiant » la suite vide $()$ et 0 .

Cas particulier

Le « plan » \mathbb{R}^2 est un \mathbb{R} -espace vectoriel et la « droite » \mathbb{C}^1 est un \mathbb{C} -espace vectoriel.
Ainsi \mathbb{C} possède à la fois une structure de \mathbb{C} -espace vectoriel et de \mathbb{R} -espace vectoriel (d'ensemble \mathbb{R}^2 en définissant $x + iy$ comme le couple (x, y) quand $x, y \in \mathbb{R}$).

Exemple 2

Soient A un ensemble et E un \mathbb{K} -espace vectoriel.

L'ensemble, noté E^A , des applications de A dans E , muni des « lois » déterminées par

$$\begin{array}{ccc} f + g : A \rightarrow & E & \text{et} \quad \alpha \times f : A \rightarrow E \\ \underset{E^A}{\overset{\cap}{\cap}} & \underset{E^A}{\overset{\cap}{\cap}} & \underset{\mathbb{K}}{\overset{\cap}{\cap}} \quad \underset{E^A}{\overset{\cap}{\cap}} \quad x \mapsto f(x) + g(x) & x \mapsto \alpha(f(x)) \end{array}$$

est un \mathbb{K} -espace vectoriel, avec $0_{E^A} : A \rightarrow E$
 $x \mapsto 0$

← [exercice]

Exemple 3

En particulier, l'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites d'éléments de \mathbb{K} , est un \mathbb{K} -espace vectoriel.

Suivant l'usage, on notera $(u_n)_{n \in \mathbb{N}}$ au lieu de $u : \mathbb{N} \rightarrow \mathbb{K}$.

$$n \mapsto u_n$$

Ainsi, on a par définition : $(u_n)_{n \in \mathbb{N}} + (v_n)_{n \in \mathbb{N}} = (u_n + v_n)_{n \in \mathbb{N}}$ et $\alpha \times (u_n)_{n \in \mathbb{N}} = (\alpha u_n)_{n \in \mathbb{N}}$.

Exemple 4

Soient $n, p \in \mathbb{N}$. D'après l'exemple 2, l'ensemble $\mathfrak{M}_{n,p}(\mathbb{K})$ des matrices $n \times p$ à coefficients dans \mathbb{K} , qui est égal à $\mathbb{K}^{\{1, \dots, n\} \times \{1, \dots, p\}}$, est aussi un \mathbb{K} -espace vectoriel, avec la somme et le produit d'un scalaire par une matrice qui ont été définis dans le chapitre 2.

3. Combinaisons linéaires

Définition-Proposition

Soient E un \mathbb{K} -espace vectoriel, $p \in \mathbb{N}$ et $v_1, \dots, v_p, v, w \in E$.

(a) Une *combinaison linéaire* (ou *cl*) des vecteurs v_1, \dots, v_p est un vecteur u de E de la forme
 $u = \underbrace{\alpha_1 v_1 + \dots + \alpha_n v_p}_{0_E \text{ quand } p = 0}$ avec $\alpha_1, \dots, \alpha_p \in \mathbb{K}$.

(b) On dit que v et w sont *colinéaire* (« sur une même droite ») s'il existe $\alpha \in \mathbb{K}$ tel que $v = \alpha w$ ou $w = \alpha v$. Cela équivaut à : $v = 0_E$ ou il existe $\alpha \in \mathbb{K}$ tel que $w = \alpha v$.

DÉMONSTRATION

Il s'agit de prouver l'équivalence du (b).

(\Rightarrow) Dans le cas où $v = \alpha w$, on a : soit $\alpha = 0$ et par suite $v = 0_E$, soit $\alpha \neq 0$ et $w = \frac{1}{\alpha} v$.

(\Leftarrow) Lorsque $v = 0_E$, on a : $v = 0 w$. □

Exemple

Dans \mathbb{R}^3 , on choisit $v_1 = (0, 1, -1)$, $v_2 = (1, 0, -1)$, $v_3 = (1, -1, 0)$, et $v = (5, -2, -3)$.

Le vecteur v est combinaison linéaire de v_1, v_2, v_3 car : $v = v_1 + 2v_2 + 3v_3$.

Remarque

La notation « $\alpha_1 v_1 + \dots + \alpha_n v_p$ » avec des points de suspension est usuelle mais abusive.

On pourrait la remplacer par « $\sum_{1 \leq k \leq p} \alpha_k v_k$ » avec la définition par récurrence suivante : $\sum_{1 \leq k \leq 0} u_k :=$

0_E , et, $\sum_{1 \leq k \leq p+1} u_k = \left(\sum_{1 \leq k \leq p} u_k \right) + u_{p+1}$ pour tous $p \in \mathbb{N}$ et $(u_i)_{1 \leq i \leq p+1} \in E^{p+1}$.

II. CONSTRUCTIONS

Dans toute cette partie, on fixe un \mathbb{K} -espace vectoriel E .

1. Sous-espaces vectoriels

Définition

On dit qu'une partie F de E est un *sous-espace vectoriel* de E (ou *sous-ev* de E) si :

- (i) $0_E \in F$;
- (ii) pour tous $\alpha, \beta \in \mathbb{K}$ et $v, w \in F$, on a $\alpha v + \beta w \in F$.

Remarques

(1) Il est immédiat que : $\{0_E\}$ et E sont des sous-espaces vectoriels de E .

(2) Soient F un sous-espace vectoriel de E , $p \in \mathbb{N}$ et $v_1, \dots, v_p \in F$.

Par récurrence sur p , on constate que toute combinaison linéaire de v_1, \dots, v_p appartient à F .

Proposition

Tout sous-espace vectoriel de E est un \mathbb{K} -espace vectoriel pour l'addition et la multiplication par un scalaire dans E .^(*)

DÉMONSTRATION

Soit F un sous-espace vectoriel de E . Par restriction de l'addition et la multiplication par un scalaire dans E , on définit les applications $F \times F \longrightarrow F$ et $\mathbb{K} \times F \longrightarrow F$.

$$(v, w) \longmapsto 1v + 1w \quad (\alpha, v) \longmapsto \alpha v + 00_E$$

Comme E est un \mathbb{K} -espace vectoriel, F satisfait clairement les conditions pour être un \mathbb{K} -espace vectoriel, en prenant $0_F := 0_E$ et l'opposé de $v \in F$ égal à $\underbrace{-v}_{\text{notation relative à } E}$. \square

Exemples

1. On considère $E = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$.

(i) On a : $0 + 0 + 0 = 0$ donc $0 \in E$.

(ii) Soient $\alpha, \beta \in \mathbb{R}$ et $v = (x', y', z'), w = (x'', y'', z'') \in E$.

On a : $\alpha v + \beta w = (x, y, z)$ avec $x := \alpha x' + \beta x'', y := \alpha y' + \beta y'', z := \alpha z' + \beta z''$.

Or : $x + y + z = \alpha \underbrace{(x' + y' + z')}_{0 \text{ car } v \in E} + \beta \underbrace{(x'' + y'' + z'')}_{0 \text{ car } w \in E}$. D'où : $\alpha v + \beta w \in E$.

En conclusion : E est un sous-espace vectoriel de \mathbb{R}^3 .

2. Soit $A \in \mathfrak{M}_{n,p}(\mathbb{K})$. L'ensemble \mathcal{S}_H des solutions du système d'équations linéaires homogène $(H) : AX = 0$ d'inconnue $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{K}^p$ est un sous-ev de \mathbb{K}^p .^(**), car :

(i) on a : $A0_{\mathbb{K}^p} = 0_{\mathbb{K}^n}$ donc $0_{\mathbb{K}^p} \in \mathcal{S}_H$;

(ii) pour $\alpha, \beta \in \mathbb{K}$ et $X, Y \in \mathcal{S}_H$, on a $A(\alpha X + \beta Y) = \alpha \underbrace{AX}_0 + \beta \underbrace{AY}_0 = 0$, donc $\alpha X + \beta Y \in \mathcal{S}_H$.

3. Par définition, un polynôme à coefficients dans \mathbb{K} est une suite $P = (a_n)_{n \geq 0}$ d'éléments de \mathbb{K} pour laquelle il existe $p \in \mathbb{N}$ tel que : $a_n = 0$ pour tout $n > p$. $\leftarrow [P = a_p X^p + \dots + a_1 X + a_0]$

L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans \mathbb{K} est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$ car :

(i) $0_{\mathbb{K}^{\mathbb{N}}} \in \mathbb{K}[X]$ en prenant par exemple $p = 0$;

(ii) pour tous $\alpha, \beta \in \mathbb{K}$ et $P = (a_n)_{n \geq 0}, Q = (b_n)_{n \geq 0} \in \mathbb{K}[X]$, en fixant $p, q \in \mathbb{N}$ tels que $a_n = 0$ quand $n > p$ et $b_n = 0$ quand $n > q$ (il en existe), on constate que $\alpha a_n + \beta b_n = 0$ quand $n > \max(p, q)$, ce qui montre que $\alpha P + \beta Q \in \mathbb{K}[X]$.

(*) Cette proposition fournira de nombreux espaces vectoriels formés de fonctions réelles de la variable réelle (applications de \mathbb{R} dans \mathbb{R}) ou formés de suites de nombres réels (applications de \mathbb{N} dans \mathbb{R}).

(**) On dira qu'il s'agit d'un sous-espace vectoriel de \mathbb{K}^p donné par « équation cartésienne ».

Proposition

Soient F et G deux sous-espaces vectoriels de E .

On a : $F \cap G$ est un sous-espace vectoriel de E .

DÉMONSTRATION

(i) On a : $0_E \in F$ et $0_E \in G$ donc $0_E \in F \cap G$.

(ii) Soient $\alpha, \beta \in \mathbb{K}$ et $v, w \in F \cap G$.

On a : $\alpha \underset{F}{v} + \beta \underset{F}{w} \in F$ et $\alpha \underset{G}{v} + \beta \underset{G}{w} \in G$, donc $\alpha v + \beta w \in F \cap G$.

Il en résulte que $F \cap G$ est un sous-espace vectoriel de E . □

Remarque

On prend ici $F = (Ox)$ et $G = (Oy)$ dans \mathbb{R}^2 . Donc $F = \text{Vect}((1, 0))$ et $G = \text{Vect}((0, 1))$ sont des sous-espaces vectoriels de \mathbb{R}^2 .

On a $F \cap G = \{(0, 0)\}$, où $\{(0, 0)\}$ est un sous-espace vectoriel bien connu de \mathbb{R}^2 .

Par contre $F \cup G$ n'est pas un sous-espace vectoriel de \mathbb{R}^2 car : $1 \underset{\in F}{(1, 0)} + 1 \underset{\in G}{(0, 1)} = \underset{\notin F \cup G}{(1, 1)}$.

Exemple

Idée : des équations cartésiennes de F et G fournissent une équation cartésienne de $F \cap G$.

On considère $\Pi_1 : x + y + z = 0$ et $\Pi_2 : x + 2y = 0$ dans \mathbb{R}^3 . Comme ensembles de solutions de systèmes d'équations homogènes, Π_1 et Π_2 sont des sous-espaces vectoriels de \mathbb{R}^3 (on verra dans le prochain exemple que ce sont des plans vectoriels).

On cherche à préciser la nature du sous-espace vectoriel $\Pi_1 \cap \Pi_2$ de \mathbb{R}^3 .

On regroupe les équations cartésiennes de Π_1 et de Π_2 : $\Pi_1 \cap \Pi_2 : \begin{cases} x + y + z = 0 \\ x + 2y = 0 \end{cases}$.

On va exhiber une équation paramétrique de $\Pi_1 \cap \Pi_2$ en résolvant par la méthode de Gauss :

$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix} \xrightarrow{L_2 \leftarrow L_2 - L_1} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \end{pmatrix}$. On effectue ensuite de tête la « remontée triangulaire ».

Ainsi : $\Pi_1 \cap \Pi_2 : \begin{cases} x = -2t \\ y = t \\ z = t \end{cases}, t \in \mathbb{R}$ puis $\Pi_1 \cap \Pi_2 = \text{Vect}\left(\begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}\right)$ est une droite vectorielle.

Définition-Proposition

Soient F, G et F_1, \dots, F_k des sous-espaces vectoriels de E .

(a) On note : $F + G := \{v + w ; v \in F \text{ et } w \in G\}$.

On a : $F + G$ est un sous-espace vectoriel de E , appelé *somme de F et de G* .

On note plus généralement : $F_1 + \dots + F_k := \{v_1 + \dots + v_k ; v_1 \in F_1, \dots, v_k \in F_k\}$.

On a : $F_1 + \dots + F_k$ est un sous-espace vectoriel de E , appelé *somme de F_1, \dots, F_k* .

(b) On a : $F + G = \text{Vect}(P \cup Q)$ quand $F = \text{Vect } P$ et $G = \text{Vect } Q$ avec $P, Q \subseteq E$.

(On en déduit que $F + G = \text{Vect}(F \cup G)$.)

On a même : $F_1 + \dots + F_k = \text{Vect}(P_1 \cup \dots \cup P_k)$ quand $F_i = \text{Vect} \underbrace{P_i}_{\subseteq E}$ pour $1 \leq i \leq k$.

DÉMONSTRATION

Afin de ne pas alourdir la rédaction, on se limite ici à la démonstration du cas de $F + G$.

(a) (i) On a : $0_E = 0_E + 0_E \in F + G$.

(ii) Soient $\alpha, \alpha' \in \mathbb{K}$ et $u = \underset{F}{v} + \underset{G}{w}, u' = \underset{F}{v'} + \underset{G}{w'} \in F + G$.

On a : $\alpha u + \alpha' u' = \underbrace{(\alpha v + \alpha' v')}_{\in F} + \underbrace{(\alpha w + \alpha' w')}_{\in G}$, donc $\alpha u + \alpha' u' \in F + G$.

Il en résulte que $F + G$ est un sous-espace vectoriel de E .

(b) On a : $P \cup Q \subseteq F + G$ donc $\underbrace{\text{Vect}(P \cup Q)}_{\text{plus petit sous-ev de } E \text{ contenant } P \cup Q} \subseteq F + G$.

Soit $u = \underset{F}{v} + \underset{G}{w} \in F + G$. Comme $v \in \text{Vect } P$ et $w \in \text{Vect } Q$, on a $v, w \in \text{Vect}(P \cup Q)$ puis $u = 1v + 1w \in \text{Vect}(P \cup Q)$. Ainsi : $F + G \subseteq \text{Vect}(P \cup Q)$.

En conclusion : $F + G = \text{Vect}(P \cup Q)$. □

Exemple

Idée : des équations paramétriques de F et G donnent une équation paramétrique de $F + G$.

On reprend $\Pi_1 : x + y + z = 0$ et $\Pi_2 : x + 2y = 0$ dans \mathbb{R}^3 . On cherche à préciser $\Pi_1 + \Pi_2$.

• Méthode de Gauss pour aboutir à $\Pi_1 = \text{Vect}(v_1, \dots, v_p)$ et $\Pi_2 = \text{Vect}(w_1, \dots, w_q)$:

$$\left(\begin{array}{ccc|c} x & y & z & \\ \hline 1 & 1 & 1 & 0 \end{array} \right) \text{ donne } \Pi_1 : \begin{cases} x = -s - t \\ y = s \\ z = t \end{cases} \quad s, t \in \mathbb{R}, \text{ et } \left(\begin{array}{ccc|c} x & y & z & \\ \hline 1 & 2 & 0 & 0 \end{array} \right) \text{ donne } \Pi_2 : \begin{cases} x = -2u \\ y = u \\ z = v \end{cases} \quad u, v \in \mathbb{R}.$$

En particulier $\Pi_1 = \text{Vect} \left(\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right)$ et $\Pi_2 = \text{Vect} \left(\begin{pmatrix} -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right)$ sont des plans vectoriels.

$$\text{On a ensuite : } \Pi_1 + \Pi_2 : \begin{cases} x = -s - t - 2u \\ y = s + u \\ z = t + v \end{cases} \quad s, t, u, v \in \mathbb{R}. \text{ On va voir que : } \Pi_1 + \Pi_2 = \mathbb{R}^3.$$

• Soit $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$. On étudie l'existence de $s, t, u, v \in \mathbb{R}$ permettant de s'assurer que v vérifie l'équation paramétrique précédente de $\Pi_1 + \Pi_2$, par la méthode de Gauss :

$$\left(\begin{array}{cccc|c} -1 & -1 & -2 & 0 & x \\ 1 & 0 & 1 & 0 & y \\ 0 & 1 & 0 & 1 & z \end{array} \right) \xrightarrow{L_2 \leftarrow L_2 + L_1} \left(\begin{array}{cccc|c} -1 & -1 & -2 & 0 & x \\ 0 & -1 & -1 & 0 & x+y \\ 0 & 1 & 0 & 1 & z \end{array} \right) \xrightarrow{L_3 \leftarrow L_3 + L_2} \left(\begin{array}{cccc|c} -1 & -1 & -2 & 0 & /// \\ 0 & -1 & -1 & 0 & /// \\ 0 & 0 & -1 & 1 & /// \end{array} \right).$$

Donc : $v \in \Pi_1 + \Pi_2$.

En conclusion : $\Pi_1 + \Pi_2 = \mathbb{R}^3$.

←[variante, plus tard : extraction de base d'une famille génératrice]

Proposition

Soient F et G deux sous-espaces vectoriels de E . Les propriétés suivantes sont équivalentes :

- (i) pour tout $u \in E$, il existe $v \in F$ et $w \in G$ uniques^(***) tels que $u = v + w$;
- (ii) $E = F + G$ et $F \cap G = \{0\}$.

DÉMONSTRATION

(\Rightarrow) On suppose (i) vrai. En particulier, on a : $E = F + G$.

Soit $u \in F \cap G$. On a : $u + 0_E = 0_E + u$ donc, par unicité, $u = 0_E$. Ainsi : $F \cap G = \{0\}$.

(\Leftarrow) On suppose (ii) vrai et se donne $u \in E$. En particulier, il existe au moins une décomposition $u = v + w$ avec $v \in F$ et $w \in G$.

Si $u = v + w = v' + w'$ alors $\underbrace{v - v'}_{\in F} = \underbrace{w' - w}_{\in G}$ puis $v - v', w' - w \in F \cap G$ ce qui donne $v = v'$

et $w = w'$. On en déduit l'unicité de la décomposition de u . □

Définition-Proposition

Soient F, G et F_1, \dots, F_k des sous-espaces vectoriels de E .

(a) On dit que *la somme de F et G est directe* si $F \cap G = \{0\}$.

On traduit cela en utilisant abusivement la notation $F \oplus G$ pour désigner $F + G$.

Plus généralement (c'est cohérent si $k = 2$), on dit que *la somme de F_1, \dots, F_k est directe* si, pour tous vecteurs $v_1 \in F_1, \dots, v_k \in F_k$ on a : $v_1 + \dots + v_k = 0 \implies v_1 = \dots = v_k = 0$.

On traduit cela en utilisant abusivement la notation $F_1 \oplus \dots \oplus F_k$ pour désigner $F_1 + \dots + F_k$.

(b) On dit que *F et G sont supplémentaires dans E* (ou que *G est supplémentaires de F dans E*), ce qui s'écrit $E = F \oplus G$, s'ils vérifient les (i) et (ii) de la proposition précédente.

Plus généralement, on dit que *F_1, \dots, F_k sont supplémentaires dans E* , ce qui s'écrit $E = F_1 \oplus \dots \oplus F_k$, s'ils vérifient l'une des deux propriétés équivalentes suivantes :

- (i) pour tout $u \in E$, il existe $v_1 \in F_1, \dots, v_k \in F_k$ uniques tels que $u = v_1 + \dots + v_k$;
- (ii) $E = F_1 + \dots + F_k$ et la somme de F_1, \dots, F_k est directe.

(***) Il faut interpréter l'expression « il existe $v \in F$ et $w \in G$ uniques » par « il existe $(v, w) \in F \times G$ unique ».

DÉMONSTRATION

- (a) Le cas général avec $k = 2$ est bien compatible avec le cas de la somme de F et G car :
- si $F \cap G = \{0\}$ et $(v_1, v_2) \in F \times G$ vérifie $v_1 + v_2 = 0$, alors $v_1 = -v_2 \in F \cap G = \{0\}$ puis $v_1 = v_2 = 0$;
 - si $u \in F \cap G$ et pour tout $(v_1, v_2) \in F \times G$ l'égalité $v_1 + v_2 = 0$ implique $v_1 = v_2 = 0$, alors en choisissant $v_1 = u$ et $v_2 = -u$ on constate que $u = 0$.

(b) Les idées de la proposition précédentes permettraient de démontrer encore ici l'équivalence entre (i) et (ii) (on ne détaille pas). \square

Exemples

(1) Soient $v_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}$, $v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$, $v_3 = \begin{pmatrix} 1 \\ 0 \\ \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{R}$ tel que $\lambda \neq -1$.

On constate en utilisant la méthode de Gauss que : $v_3 \notin \text{Vect}(v_1, v_2)$ et $\text{Vect}(v_1, v_2, v_3) = \mathbb{R}^3$.
On s'aperçoit donc que $\text{Vect}(v_1, v_2)$ a pour supplémentaire $\text{Vect}(v_3)$ dans \mathbb{R}^3 .

En prenant différents λ , on constate que $\text{Vect}(v_1, v_2)$ a une infinité de supplémentaires dans \mathbb{R}^3 .

(2) Soient $\Pi_1 : x + y + z = 0$ et $\Pi_2 : x + 2y = 0$ dans \mathbb{R}^3 .

On trouve par la méthode de Gauss que : $\Pi_1 \cap \Pi_2 \neq \{(0, 0, 0)\}$ (et $\Pi_1 + \Pi_2 = \mathbb{R}^3$).

Donc la somme de Π_1 et Π_2 n'est pas directe.

(3) Soient $D_1 = (Ox)$, $D_2 = (Oy)$, et $D_3 : x = y$ dans \mathbb{R}^2 .

Les droites vectorielles D_1, D_2, D_3 vérifient $D_1 \cap D_2 = D_2 \cap D_3 = D_3 \cap D_1 = \{(0, 0)\}$ et $D_1 + D_2 + D_3 = \mathbb{R}^2$ (facile).

Mais la somme de D_1, D_2 , et D_3 n'est pas directe, car : $\underbrace{(1, 0)}_{\in D_1} + \underbrace{(0, 1)}_{\in D_2} + \underbrace{(-1, -1)}_{\in D_3} = (0, 0)$.

III. BASES ET DIMENSION

Dans cette partie, on fixe à nouveau un \mathbb{K} -espace vectoriel E .

1. Familles libres. Familles génératrices. Bases

Définition

(a) Une famille numérotée de p vecteurs de E où $p \in \mathbb{N}$, est un élément (v_1, \dots, v_p) de E^p .

Plus généralement, une famille de vecteurs de E est une application $v : \underset{\text{ensemble}}{I} \rightarrow E$, qu'on notera plutôt $(v_i)_{i \in I}$.

Dans la suite de cette définition, on se donne suivant le cas : soit p vecteurs v_1, \dots, v_p de E où $p \in \mathbb{N}$, soit une famille $(v_i)_{i \in I}$ indexée par I de vecteurs de E où I est un ensemble fixé.

(b) On dit que la famille (v_1, \dots, v_p) est libre si pour tous $\alpha_1, \dots, \alpha_p \in \mathbb{K}$, on a :

$$\text{ou « les vecteurs } v_1, \dots, v_p \text{ sont linéairement indépendants »}$$

$$\alpha_1 v_1 + \dots + \alpha_p v_p = 0 \implies \alpha_1 = \dots = \alpha_p = 0.$$

Plus généralement, on dit que la famille $(v_i)_{i \in I}$ est libre si pour tous $k \in \mathbb{N}$ et $i_1, \dots, i_k \in I$, distincts les seuls $\alpha_1, \dots, \alpha_k \in \mathbb{K}$ tels que $\alpha_1 v_{i_1} + \dots + \alpha_k v_{i_k} = 0$ sont $\alpha_1 = \dots = \alpha_k = 0$.

On exprimera qu'une famille de vecteurs de E n'est pas libre en disant qu'elle est liée.

(c) On dit que la famille (v_1, \dots, v_p) est génératrice de E si pour tout $v \in E$, il existe

$$\text{ou « les vecteurs } v_1, \dots, v_p \text{ engendrent } E \text{ »}$$

$$\alpha_1, \dots, \alpha_p \in \mathbb{K} \text{ tels que : } v = \alpha_1 v_1 + \dots + \alpha_p v_p.$$

Plus généralement, on dit que la famille $(v_i)_{i \in I}$ est génératrice de E si pour tout $v \in E$, il existe $k \in \mathbb{N}$, $i_1, \dots, i_k \in I$, distincts et $\alpha_1, \dots, \alpha_k \in \mathbb{K}$ tels que : $v = \alpha_1 v_{i_1} + \dots + \alpha_k v_{i_k}$.

Ainsi, la famille $(v_i)_{i \in I}$ est génératrice de E si et seulement si $\text{Vect}(\{v_i ; i \in I\}) = E$.

Exemples

(1) Les vecteurs 1 et i du \mathbb{R} -espace vectoriel \mathbb{C} sont linéairement indépendants (sur \mathbb{R}), car : si $\alpha 1 + \beta i = 0$ avec $\alpha, \beta \in \mathbb{R}$ alors $\alpha = \beta = 0$.

Par contre, les vecteurs 1 et i du \mathbb{C} -espace vectoriel \mathbb{C} sont linéairement dépendants (sur \mathbb{C}), car : $\alpha 1 + \beta i = 0$ quand $\alpha = i$ et $\beta = -1$.

(2) Les vecteurs $f: \mathbb{R} \rightarrow \mathbb{R}$ et $g: \mathbb{R} \rightarrow \mathbb{R}$ du \mathbb{R} -espace vectoriel $\mathbb{R}^{\mathbb{R}}$ sont linéairement

$$x \mapsto \cos x \qquad x \mapsto \sin x$$

indépendants, car : si $\alpha f + \beta g = 0$ avec $\alpha, \beta \in \mathbb{R}$ alors $\begin{cases} \alpha = (\alpha f + \beta g)(0) = 0 \\ \beta = (\alpha f + \beta g)(\frac{\pi}{2}) = 0 \end{cases}$.

(3) Soient $u_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $u_3 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ dans \mathbb{R}^3 .

On étudie $(\star): \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 = 0$ et $(\star\star): \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$ à $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ fixé avec comme inconnue $(\alpha_1, \alpha_2, \alpha_3)$, et obtient par la méthode de Gauss que :

– la famille (u_1, u_2, u_3) est libre, cf. $\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{pmatrix} \xrightarrow{L_3 \leftarrow L_3 - L_1} \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ 1 & 1 & 2 \\ 0 & 2 & 1 \\ 0 & -1 & 0 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} \alpha_1 & \alpha_3 & \alpha_2 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & -1 \end{pmatrix}$;
unique solution $(0, 0, 0)$

– la famille (u_1, u_2, u_3) est génératrice de \mathbb{R}^3 , cf. $\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & | & x \\ 1 & 1 & 2 & | & y \\ 0 & 2 & 1 & | & \dots \\ 1 & 0 & 2 & | & z \end{pmatrix} \rightarrow \dots \rightarrow \begin{pmatrix} \alpha_1 & \alpha_3 & \alpha_2 & | & \dots \\ 1 & 2 & 1 & | & \dots \\ 0 & 1 & 2 & | & \dots \\ 0 & 0 & -1 & | & \dots \end{pmatrix}$.
existence d'une solution

Remarques (exercices)

(1) Dans le cas de 0, 1, ou 2 vecteurs, on constate que :

- la famille vide $(\)$ est libre (vu la convention $\sum_{1 \leq k \leq p} \alpha_k v_k = 0$ quand $p = 0$) ;
- une famille (v_1) avec $v_1 \in E$ est libre si et seulement si v_1 est non-nul ;
- deux vecteur de E sont linéairement indépendants si et seulement si ils sont non-colinéaires.

(2) Une famille $(v_i)_{i \in I}$ de vecteurs de E est liée si et seulement s'il existe un vecteur v_i , $i \in I$, qui est combinaison linéaire d'un nombre fini de vecteurs de la forme v_j avec $j \neq i$.
En particulier, toute famille de vecteurs de E dans laquelle se trouve le vecteur nul ou deux vecteurs égaux, est liée.

(3) On dira qu'une famille de vecteurs de E est « extraite » d'une famille $(v_i)_{i \in I}$ de vecteurs de E si elle est de la forme $(v_j)_{j \in J}$ avec $J \subseteq I$.

Tout famille extraite d'une famille libre de vecteurs de E , est libre. Tout famille de vecteurs de E dont une famille extraite est génératrice de E , est elle-même génératrice de E .

Notation

Soit I un ensemble. On note $E^{(I)}$ l'ensemble des familles $(v_i)_{i \in I}$ d'éléments de E indexées par I telles que la partie $J := \{i \in I \mid v_i \neq 0\}$ de I est finie. ← [par exemple : $\mathbb{K}^{(\mathbb{N})} = \mathbb{K}[X]$]

Pour un tel $(v_i)_{i \in I} \in E^{(I)}$, on pose : $\sum_{i \in I} v_i := v_{i_1} + \dots + v_{i_k}$ où $\{i_1, \dots, i_k\} := J$.
(indépendant de l'ordre sur J) distincts

On peut donc écrire $P = \sum_{n \in \mathbb{N}} a_n X^n$ pour tout $P \in \mathbb{K}[X]$ de coefficients a_n , $n \in \mathbb{N}$.

Le choix de $E = \mathbb{K}$ fournit en particulier la notation $\mathbb{K}^{(I)}$.

Proposition

Une famille finie (v_1, \dots, v_p) de vecteurs de E est libre et génératrice de E , si et seulement si, pour tout $v \in E$ il existe $(\alpha_1, \dots, \alpha_p) \in \mathbb{K}^p$ unique tel que $v = \alpha_1 v_1 + \dots + \alpha_p v_p$.

Plus généralement, une famille $(v_i)_{i \in I}$ de vecteurs de E est libre et génératrice de E , si et seulement si, pour tout $v \in E$ il existe $(\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$ unique tel que $v = \sum_{i \in I} \alpha_i v_i$.
détermine un élément de $E^{(I)}$

DÉMONSTRATION

On traite seulement le cas général.

(\Rightarrow) On suppose que $(v_i)_{i \in I}$ est libre et génératrice de E . Soit $v \in E$.

Comme $(v_i)_{i \in I}$ est génératrice de E , il existe $(\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$ tel que $v = \sum_{i \in I} \alpha_i v_i$.

On se donne une autre décomposition $v = \sum_{i \in I} \beta_i v_i$ avec $(\beta_i)_{i \in I} \in \mathbb{K}^{(I)}$. On pose :

$$\{i_1, \dots, i_k\} := \{i \in I \mid \alpha_i \neq 0\}, \quad \{j_1, \dots, j_l\} := \{i \in I \mid \beta_i \neq 0\}, \quad \text{et } \{t_1, \dots, t_m\} := \{i_1, \dots, i_k, j_1, \dots, j_l\}.$$

On a :
$$\begin{cases} v = \alpha_{i_1} v_{i_1} + \dots + \alpha_{i_k} v_{i_k} = \alpha_{t_1} v_{t_1} + \dots + \alpha_{t_m} v_{t_m} \\ v = \beta_{j_1} v_{j_1} + \dots + \beta_{j_l} v_{j_l} = \beta_{t_1} v_{t_1} + \dots + \beta_{t_m} v_{t_m} \end{cases}$$
 donc, par soustraction, $(\alpha_{t_1} - \beta_{t_1})v_{t_1} + \dots + (\alpha_{t_m} - \beta_{t_m})v_{t_m} = 0$ puis, la famille $(v_i)_{i \in I}$ étant libre, $\beta_{t_1} = \alpha_{t_1}$ et ... et $\beta_{t_m} = \alpha_{t_m}$. Cela donne l'unicité de la famille $(\alpha_i)_{i \in I}$.

(\Leftarrow) On suppose que : $\forall v \in E \quad \underbrace{\exists!}_{\text{« il existe un unique »}} (\alpha_i)_{i \in I} \in \mathbb{K}^{(I)} \quad v = \sum_{i \in I} \alpha_i v_i$.

L'existence d'un $(\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$ associé à chaque v montre que $(v_i)_{i \in I}$ est génératrice de E . L'unicité de $(\alpha_i)_{i \in I} \in \mathbb{K}^{(I)}$ quand $v = 0$ montre que $(v_i)_{i \in I}$ est libre. \square

Définition

(a) On dit qu'une famille $(v_i)_{i \in I}$ de vecteurs de E est une *base de E* si $(v_i)_{i \in I}$ est libre et génératrice de E .

(b) On suppose que E a une base finie $\mathcal{B} = (v_1, \dots, v_n)$.

Pour tout $v \in E$, les uniques scalaires $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que $v = \alpha_1 v_1 + \dots + \alpha_n v_n$ s'appellent *les coordonnées de v suivant \mathcal{B}* . On le notera : $v \Big|_{\mathcal{B}} \begin{matrix} \alpha_1 \\ \vdots \\ \alpha_n \end{matrix}$.

Exemples

(1) Le \mathbb{K} -espace vectoriel \mathbb{K}^n admet la base suivante, appelée *base canonique de \mathbb{K}^n* :

$$\mathcal{B} := (e_1, \dots, e_n) \quad \text{avec } e_1 := (1, 0, \dots, 0), e_2 := (0, 1, 0, \dots, 0), \dots, e_n := (0, \dots, 0, 1).$$

(2) Soit $(H) : AX = 0$ avec $X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{K}^p$ un système d'équations linéaires homogène.

On sait que l'ensemble \mathcal{S}_H de ses solutions est un sous-espace vectoriel de \mathbb{K}^p .

La méthode de Gauss fournit des vecteurs w_1, \dots, w_{p-r} de \mathbb{K}^p tels que :

$$\begin{aligned} - \mathcal{S}_H &= \{t_1 w_1 + \dots + t_{p-r} w_{p-r} ; t_1, \dots, t_{p-r} \in \mathbb{K}\}; & \leftarrow \text{cf. } \mathcal{S}_H : \begin{cases} x_{j_1} = \dots \\ \vdots \\ x_{j_r} = \dots \\ x_{j_{r+1}} = t_1, \dots, t_{p-r} \in \mathbb{R}. \\ \vdots \\ x_{j_p} = t_{p-r} \end{cases} \\ - \text{si } t_1 w_1 + \dots + t_{p-r} w_{p-r} = 0, & \text{ alors } \begin{cases} \text{coordonnée } j_{r+1} : t_1 + 0 + \dots + 0 = 0 \\ \vdots \\ \text{coordonnée } j_p : 0 + \dots + 0 + t_{p-r} = 0 \end{cases}, \text{ alors } t_1 = \dots = t_{p-r} = 0. \end{aligned}$$

Ainsi (w_1, \dots, w_{p-r}) est une base de \mathcal{S}_H .

(3) La famille $(X^n)_{n \geq 0}$ est une base du \mathbb{K} -espace vectoriel $\mathbb{K}[X]$.

Soit $N \in \mathbb{N}$. L'ensemble $\mathbb{K}_N[X]$ est le sous-espace vectoriel $\text{Vect}(1, X, \dots, X^N)$ de $\mathbb{K}[X]$.

La famille $(1, X, \dots, X^N)$ est une base de $\mathbb{K}_N[X]$, appelée *base canonique de $\mathbb{K}_N[X]$* .

(4) Le \mathbb{K} -espace vectoriel $\mathfrak{M}_{n,p}(\mathbb{K})$ admet la base suivante :

$$(E_{1,1}, \dots, E_{1,p}; E_{2,1}, \dots, E_{2,p}; \dots; E_{n,1}, \dots, E_{n,p}) \quad \text{avec } E_{i,j} := \underbrace{\begin{pmatrix} 0 & \downarrow & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix}}_{\substack{\text{colonne } j \\ \text{0 ailleurs qu'en l'emplacement } (i,j)}} \leftarrow \text{ligne } i$$

En effet, pour tous $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathfrak{M}_{n,p}(\mathbb{K})$ et $(x_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq p}} \in \mathbb{K}^{\{1, \dots, n\} \times \{1, \dots, p\}}$, on a :

$$A = \sum_{i,j} x_{ij} E_{ij} \iff (\forall (i,j) \in \{1, \dots, n\} \times \{1, \dots, p\}) \quad x_{ij} = a_{ij}.$$

2. Dimension. Rang

Théorème (« théorème de la base incomplète »)

On suppose que E a une famille génératrice finie (g_1, \dots, g_k) .

Toute famille libre (h_1, \dots, h_l) de E se complète à l'aide de certains vecteurs parmi g_1, \dots, g_k en une base (e_1, \dots, e_d) de E .

DÉMONSTRATION

Rappel : toute partie non-vide de $\{0, 1, \dots, N\}$, $N \in \mathbb{N}$, a un plus grand élément (par récurrence).

On note \mathcal{F} l'ensemble des éléments n de $\{l, l+1, \dots, k+l\}$ pour lesquels il existe une famille libre (e_1, \dots, e_n) de E vérifiant : $e_1 = h_1, \dots, e_l = h_l$, et e_{l+1}, \dots, e_n sont parmi g_1, \dots, g_k .

L'ensemble \mathcal{F} est non-vide, car il contient l qui correspond au cas $(e_1, \dots, e_n) = (h_1, \dots, h_l)$. Soit d le plus grand élément de \mathcal{F} et (e_1, \dots, e_d) une famille associée. Pour terminer la démonstration, il reste à vérifier que cette famille libre (e_1, \dots, e_d) est aussi génératrice de E .

Soit $i \in \{1, \dots, k\}$. Comme d est maximal, la famille (e_1, \dots, e_d, g_i) est liée. On dispose d'une égalité $\underbrace{\alpha_1 e_1 + \dots + \alpha_d e_d + \alpha g_i}_{\alpha_1, \dots, \alpha_d, \alpha \in \mathbb{K} \text{ non-tous nuls}} = 0$ donc $\alpha \neq 0$ et $g_i = -\frac{1}{\alpha}(\alpha_1 e_1 + \dots + \alpha_d e_d) \in \text{Vect}(e_1, \dots, e_d)$.

D'où : $E = \underbrace{\text{Vect}(g_1, \dots, g_k)}_{\text{plus petit sous-ev de } E \text{ contenant } g_1, \dots, g_k} \subseteq \text{Vect}(e_1, \dots, e_d)$, ce qui montre que e_1, \dots, e_d engendrent E . \square

Corollaire 1 (« théorème de la dimension »)

On suppose que E a une famille génératrice finie.

On a : E a une base finie (e_1, \dots, e_d) .

Les autres bases de E ont aussi d vecteurs.

DÉMONSTRATION

D'après le théorème de la base incomplète, on obtient une base finie $\mathcal{B} = (e_1, \dots, e_d)$ de E en complétant la famille $()$ à l'aide de vecteurs pris dans une famille génératrice finie fixée de E .

On va vérifier que :

- (i) toute base finie $\mathcal{B}' = (e'_1, \dots, e'_{d'})$ de E a d vecteurs, et pour cela quitte à échanger les rôles de \mathcal{B} et \mathcal{B}' , il suffit de prouver que $d' \leq d$:
- (ii) E n'a pas de base infinie \mathcal{B}'' .

Comme \mathcal{B}' et \mathcal{B}'' sont libres, il reste à démontrer que toute famille libre \mathcal{L} dans E a au plus d vecteurs. Une famille libre infinie dans E aurait une famille extraite formée de $d+1$ vecteurs, elle-même libre. On peut donc supposer que \mathcal{L} est finie, de la forme (h_1, \dots, h_l) .

On considère l'équation $x_1 h_1 + \dots + x_l h_l = 0$ d'inconnue $(x_1, \dots, x_l) \in \mathbb{K}^l$.

En notant $h_1 \begin{vmatrix} a_{11} \\ \vdots \\ a_{d1} \end{vmatrix} / \mathcal{B}, \dots, h_l \begin{vmatrix} a_{1l} \\ \vdots \\ a_{dl} \end{vmatrix} / \mathcal{B}$ elle équivaut à : $(H) \begin{cases} a_{11} x_1 + \dots + a_{1l} x_l = 0 \\ \vdots \\ a_{d1} x_1 + \dots + a_{dl} x_l = 0 \end{cases}$.

Si $l > d$, alors comme le nombre d'équations est strictement supérieur au nombre d'inconnues, (H) a une solution non-nulle; cela contredit la condition « (h_1, \dots, h_l) est libre ». Ainsi : $l \leq d$.

Variante

On a : $h_1, \dots, h_l \in \text{Vect}(e_1, \dots, e_d)$. Si $l > d$, on aurait donc : $(\star) h_1, \dots, h_{l+1} \in \text{Vect}(e_1, \dots, e_d)$.

Pour montrer que (\star) est fautive il reste à voir que pour tout $k \geq 0$, on a :

(H_k) pour tous $v_1, \dots, v_k \in E$ et $w_1, \dots, w_{k+1} \in \text{Vect}(v_1, \dots, v_k)$, la famille (w_1, \dots, w_{k+1}) est liée.

(i) L'assertion (H_0) , qui signifie que pour tout $w_1 \in \{0\}$ la famille (w_1) est liée, est vraie.

(ii) Soit $k \geq 1$ tel que (H_{k-1}) est vraie. On se donne $v_1, \dots, v_k \in E$ et $w_1 = \lambda_{1,1} v_1 + \dots + \lambda_{1,k} v_k, \dots, w_{k+1} = \lambda_{k+1,1} v_1 + \dots + \lambda_{k+1,k} v_k \in \text{Vect}(v_1, \dots, v_k)$. On vérifie que (w_1, \dots, w_{k+1}) est liée.

On peut supposer que $w_1 \neq 0$, puis – quitte à renuméroter les v_i – que $\lambda_{1,1} \neq 0$.

En appliquant (H_{k-1}) aux vecteurs $u_2 := w_2 - \frac{\lambda_{2,1}}{\lambda_{1,1}} w_1, \dots, u_{k+1} := w_{k+1} - \frac{\lambda_{k+1,1}}{\lambda_{1,1}} w_1$ de $\text{Vect}(v_2, \dots, v_k)$, on obtient l'existence de scalaires $\alpha_2, \dots, \alpha_{k+1} \in \mathbb{K}$ non-tous nuls, tels que $\alpha_2 u_2 + \dots + \alpha_{k+1} u_{k+1} = 0$. D'où l'égalité $\alpha_2 w_2 + \dots + \alpha_{k+1} w_{k+1} = (\alpha_2 \frac{\lambda_{2,1}}{\lambda_{1,1}} + \dots + \alpha_{k+1} \frac{\lambda_{k+1,1}}{\lambda_{1,1}}) w_1$ qui montre que (w_1, \dots, w_{k+1}) est liée. \square

Définition

(a) On dit que le \mathbb{K} -espace vectoriel E est de dimension finie s'il a une base finie (e_1, \dots, e_d) . Dans ce cas, on appelle dimension de E le nombre d , noté $\underbrace{\dim E}_{\text{ou } \dim_{\mathbb{K}} E}$, de vecteurs de ses bases.

(D'après le théorème de la dimension, ce d est bien indépendant du choix de la base.)

(b) Soient $v_1, \dots, v_p \in E$. On appelle rang de la famille (v_1, \dots, v_p) le nombre

$$\text{rg}(v_1, \dots, v_p) := \dim \text{Vect}(v_1, \dots, v_p).$$

(Cela a un sens car d'après le théorème de la dimension, $\text{Vect}(v_1, \dots, v_p)$ est de dimension finie.)

Exemples

(1) On reprend certaines définitions du paragraphe II.1. :

- $E = \{0\}$ si et seulement si $\dim E = 0$;
- E est une droite vectorielle si et seulement si $\dim E = 1$;
- E est un plan vectoriel si et seulement si $\dim E = 2$.

(2) Tout $z \in \mathbb{C}$ s'écrit de manière unique $z = x + yi$ avec $x, y \in \mathbb{R}$.

Donc $(1, i)$ est une base du \mathbb{R} -espace vectoriel \mathbb{C} . En particulier : $\dim_{\mathbb{R}} \mathbb{C} = 2$.

Par contre, comme $\mathbb{C} = \text{Vect}_{\mathbb{C}}(1)$ avec $1 \neq 0$, l'exemple 1 montre que : $\dim_{\mathbb{C}} \mathbb{C} = 1$.

(3) Compte tenu des bases exhibées à la fin du paragraphe 1, on a :

$$\dim \mathbb{K}^n = n, \quad \dim \mathbb{K}_N[X] = N + 1 \quad \text{et} \quad \dim \mathfrak{M}_{n,p}(\mathbb{K}) = np.$$

Corollaire 2

On suppose que E est de dimension finie. On note d la dimension de E .

(a) Toute famille libre de E a au plus d vecteurs ;

quand elle a d vecteurs, c'est une base de E .

(b) Toute famille génératrice de E a au moins d vecteurs ;

quand elle a d vecteurs, c'est une base de E .

DÉMONSTRATION

(a) Une famille libre infinie dans E aurait une famille extraite formée de $d + 1$ vecteurs, qui serait elle-même encore libre. On se contente donc de traiter le cas des familles libres finies.

Une famille libre finie de l vecteurs de E se complète d'après le théorème de la base incomplète en une base de E qui a d vecteurs d'après le théorème de la dimension, donc $l \leq d$.

(b) Une famille génératrice de E infinie a au moins d vecteurs. On se contente donc de traiter le cas des familles génératrices finies.

Soit (g_1, \dots, g_k) une famille génératrice finie de vecteurs de E . D'après le théorème de la base incomplète, la famille $()$ se complète en une base \mathcal{B}' de E extraite de (g_1, \dots, g_k) .

D'après le théorème de la dimension, la famille \mathcal{B}' a d vecteurs. D'où le résultat. \square

Remarques

(1) On reprend l'exemple 3 du début du paragraphe 1 : $u_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $u_3 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$.

On a vu à l'aide d'un premier calcul que (u_1, u_2, u_3) est libre. On remarque que la base canonique de \mathbb{R}^3 est formée de 3 vecteurs. On peut donc maintenant utiliser le a) du corollaire 2 pour en conclure, sans autre calcul, que (u_1, u_2, u_3) est génératrice de \mathbb{R}^3 .

(2) On considère les applications $f_n : \mathbb{R} \rightarrow \mathbb{R}$, $n \in \mathbb{N}$.

$$x \mapsto x^n$$

Elles forment une famille $(f_n)_{n \in \mathbb{N}}$ qui est libre dans $\mathbb{R}^{\mathbb{R}}$ car :

si des éléments $n_1 < \dots < n_k$ de \mathbb{N} et $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ vérifient $\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k} = 0$, alors $\alpha_1 = \frac{1}{n_1!}(\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k})^{(n_1)}(0) = 0$ et ... et $\alpha_k = \frac{1}{n_k!}(\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k})^{(n_k)}(0) = 0$.

Ainsi le a) du corollaire 2, appliqué à la famille $(f_n)_{n \in \mathbb{N}}$ qui est libre et indexée par un ensemble infini, montre que $\mathbb{R}^{\mathbb{R}}$ n'est pas un espace vectoriel de dimension finie.

D'autre part, la famille $(f_n)_{n \in \mathbb{N}}$ n'est pas génératrice de $\mathbb{R}^{\mathbb{R}}$ car $\text{Vect}(\{f_n ; n \in \mathbb{N}\})$ qui est formée de fonctions dérivables ne contient donc pas l'application valeur absolue.

Proposition

On suppose que E a une base finie $\mathcal{B} = (e_1, \dots, e_n)$.

Soient $v_1 \begin{array}{c} | \\ a_{11} \\ \vdots \\ a_{n1} \\ | \end{array} \mathcal{B}, \dots, v_p \begin{array}{c} | \\ a_{1p} \\ \vdots \\ a_{np} \\ | \end{array} \mathcal{B} \in E$.

(a) On transforme $A := \begin{pmatrix} x_1 & \dots & x_p \\ a_{11} & \dots & a_{1p} \\ \dots & & \dots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$ en $A' = \begin{pmatrix} x_{j_1} & \dots & x_{j_r} & x_{j_{r+1}} & \dots & x_{j_p} \\ d_1 & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & \dots & \dots \\ \vdots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & d_r & \dots & \dots \\ \hline 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}$

par la méthode de Gauss, avec $d_1 \neq 0, \dots, d_r \neq 0$.

On a : $(v_{j_1}, \dots, v_{j_r})$ est une base de $\text{Vect}(v_1, \dots, v_p)$.

(b) En particulier : $\text{rg}(v_1, \dots, v_p) = r$ « calcul du rang par la méthode de Gauss ». (Le nombre r est donc indépendant de la manière dont on applique la méthode de Gauss.)

DÉMONSTRATION

Mêmes arguments que pour le calcul du rang d'une matrice par la méthode de Gauss. \square

Remarque (importante au niveau de la rédaction au cours des partiels et examens)

La partie a) de cette proposition n'est pas classique.

- Dans chaque exercice on la déduira des calculs simultanés de $\text{rg}(v_1, \dots, v_r)$ et $\text{rg}(v_{j_1}, \dots, v_{j_r})$:
- on a $\text{rg}(v_1, \dots, v_r) = r$ par calcul du rang par la méthode de Gauss ;
 - on a aussi $\text{rg}(v_{j_1}, \dots, v_{j_r}) = r$ en reprenant le calcul précédent et rayant les colonnes qui ne sont pas sous les symboles x_{j_1}, \dots, x_{j_r} , ce qui montrera cf. plus bas, que $(v_{j_1}, \dots, v_{j_r})$ est libre ;
 - $\text{Vect}(v_{j_1}, \dots, v_{j_r})$ est un sous-espace vectoriel de dimension r de $\text{Vect}(v_1, \dots, v_r)$ qui est aussi de dimension r , ce qui montrera cf. plus bas, que $(v_{j_1}, \dots, v_{j_r})$ engendre $\text{Vect}(v_1, \dots, v_p)$.

3. Dimension des sous-espaces vectoriels

Proposition

On suppose E de dimension finie.

Tout sous-espace vectoriel F de E est de dimension finie avec $\dim F \leq \dim E$.

De plus, si $\dim F = \dim E$, alors $F = E$.

DÉMONSTRATION

Toute famille libre (v_1, \dots, v_p) de F est libre dans E , donc vérifie : $p \leq \dim E$.

Il en existe, par exemple la famille vide. On choisit (v_1, \dots, v_p) de façon à avoir p maximal.

Soit $v \in F$. Comme p est maximal, la famille (v_1, \dots, v_p, v) est liée. On dispose d'une égalité $\alpha_1 v_1 + \dots + \alpha_p v_p + \alpha v = 0$ donc $\alpha \neq 0$ et $v = -\frac{1}{\alpha}(\alpha_1 v_1 + \dots + \alpha_p v_p) \in \text{Vect}(v_1, \dots, v_p)$.

$\alpha_1, \dots, \alpha_p, \alpha \in \mathbb{K}$ non-tous nuls

Par conséquent, (v_1, \dots, v_p) est génératrice de F et finalement (v_1, \dots, v_p) est une base de F .

En particulier : F est de dimension finie et $\dim F = p \leq \dim E$.

De plus : si $\dim F = \dim E$, alors la famille libre (v_1, \dots, v_p) de E qui est formée de $\dim E$ vecteurs est une base de E , puis $F = \text{Vect}(v_1, \dots, v_p) = E$. \square

Remarque

D'après cette proposition, les sous-espaces vectoriels de \mathbb{R}^3 ont une dimension, égale à 0 ou 1 ou 2 ou 3, le cas de la dimension 3 n'étant atteint que par \mathbb{R}^3 lui-même. Les sous-espaces vectoriels de \mathbb{R}^3 sont donc $\{0\}$, les droites vectorielles de \mathbb{R}^3 , les plans vectoriels de \mathbb{R}^3 , et \mathbb{R}^3 .

Proposition (utile)

Soient $v_1, \dots, v_p \in E$. On pose : $r = \text{rg}(v_1, \dots, v_p)$.

(a) La famille (v_1, \dots, v_p) est libre si et seulement si $r = p$.

(b) On suppose E de dimension finie, notée n .

La famille (v_1, \dots, v_p) est génératrice de E si et seulement si $r = n$.

DÉMONSTRATION

(a) La famille (v_1, \dots, v_p) , de p vecteurs, engendre $\text{Vect}(v_1, \dots, v_p)$ qui est de dimension r . Elle est libre si et seulement si elle est base de $\text{Vect}(v_1, \dots, v_p)$, ce qui équivaut (compte tenu du corollaire 2 (b) du théorème de la base incomplète) à $r = p$.

(b) La famille (v_1, \dots, v_p) est génératrice de E si et seulement si $\text{Vect}(v_1, \dots, v_p) = E$, c'est à dire (vu la proposition précédente) $\dim \text{Vect}(v_1, \dots, v_p) = \dim E$, c'est à dire $r = n$. \square

Remarque (importante)

On revient sur l'exemple 3 du début du paragraphe 1 : $u_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $u_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$, $u_3 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \in \mathbb{R}^3$.

La rédaction la plus rapide pour démontrer que (u_1, u_2, u_3) est une base de \mathbb{R}^3 consiste à prouver par la méthode de Gauss que $\text{rg}(u_1, u_2, u_3) = 3$.

Proposition

On suppose que E est de dimension finie. Soient F et G deux sous-espaces vectoriels de E , (v_1, \dots, v_p) une base de F et (w_1, \dots, w_q) une base de G .

On a : $\underline{E = F \oplus G}$ si et seulement si $(v_1, \dots, v_p, w_1, \dots, w_q)$ est une base de E .

« F et G sont supplémentaires dans E »

DÉMONSTRATION

On a $F + G = \text{Vect}(v_1, \dots, v_p) + \text{Vect}(w_1, \dots, w_q) = \text{Vect}(v_1, \dots, v_p, w_1, \dots, w_q)$.

Donc : $F + G = E$ si et seulement si $(v_1, \dots, v_p, w_1, \dots, w_q)$ engendre E .

Il reste à vérifier que : $F \cap G = \{0\}$ si et seulement si $(v_1, \dots, v_p, w_1, \dots, w_q)$ est libre.

• On suppose que $F \cap G = \{0\}$.

Soient $\alpha_1, \dots, \alpha_p, \beta_1, \dots, \beta_q \in \mathbb{K}$ tels que $\alpha_1 v_1 + \dots + \alpha_p v_p + \beta_1 w_1 + \dots + \beta_q w_q = 0$.

On a $\alpha_1 v_1 + \dots + \alpha_p v_p = -\beta_1 w_1 - \dots - \beta_q w_q \in F \cap G$. Puisque $F \cap G = \{0\}$, on en déduit que $\alpha_1 v_1 + \dots + \alpha_p v_p = 0$ et $\beta_1 w_1 + \dots + \beta_q w_q = 0$. Or (v_1, \dots, v_p) et (w_1, \dots, w_q) sont libres.

D'où $\alpha_1 = \dots = \alpha_p = \beta_1 = \dots = \beta_q = 0$.

Cela montre que la famille $(v_1, \dots, v_p, w_1, \dots, w_q)$ est libre.

• On suppose que la famille $(v_1, \dots, v_p, w_1, \dots, w_q)$ est libre.

Soit $u \in F \cap G$. Vu que (v_1, \dots, v_p) est une base de F et (w_1, \dots, w_q) est une base de G , il existe $x_1, \dots, x_p, y_1, \dots, y_q \in \mathbb{K}$ tels que $u = x_1 v_1 + \dots + x_p v_p$ et $u = y_1 w_1 + \dots + y_q w_q$. On a donc $x_1 v_1 + \dots + x_p v_p - y_1 w_1 - \dots - y_q w_q = 0$. Puisque $(v_1, \dots, v_p, w_1, \dots, w_q)$ est libre, il en résulte que $x_1 = \dots = x_p = y_1 = \dots = y_q = 0$, puis $u = 0v_1 + \dots + 0v_p = 0$.

Cela montre que $F \cap G = \{0\}$. \square

Remarque (importante)

On suppose que E est de dimension finie. Soit F un sous-espace vectoriel de E . On peut compléter une base (v_1, \dots, v_p) de F (qui est en particulier libre) à l'aide de certains vecteurs de E (par exemple les vecteurs d'une base donnée de E) en une base $(v_1, \dots, v_p, w_1, \dots, w_q)$ de E .

D'après la proposition, $G := \text{Vect}(w_1, \dots, w_q)$ est un supplémentaire de F dans E .

Corollaire (de la remarque)

On suppose que E est de dimension finie.

Tout sous-espace vectoriel F de E admet un supplémentaire G dans E .

Proposition

On suppose que E est de dimension finie.

Soient F et G deux sous-espaces vectoriels de E .

(a) On a : si $E = F \oplus G$, alors $\dim E = \dim F + \dim G$.

(b) Plus généralement : $\dim(F + G) + \dim(F \cap G) = \dim F + \dim G$.

DÉMONSTRATION

(a) Conséquence de la proposition précédente.

(b) • On se donne un sous-espace vectoriel F' de F tel que : $F = F' \oplus (F \cap G)$ (existe par la remarque précédente). D'après (a), on a : $\dim F \stackrel{(*)}{=} \dim(F') + \dim(F \cap G)$.

• On a : $F + G = F' + \underbrace{(F \cap G)}_{\subseteq G} + G = F' + G$ et $\underbrace{F'}_{\subseteq F} \cap G \subseteq F' \cap (F \cap G) = \{0\}$.

D'où : $F + G = F' \oplus G$. D'après (a), on a : $\dim(F + G) \stackrel{(**)}{=} \dim(F') + \dim G$.

• On obtient le résultat en soustrayant (*) à (**).

Variante

On complète une base (u_1, \dots, u_m) de $F \cap G$ d'une part en une base (v_1, \dots, v_p) de F et d'autre part en une base (w_1, \dots, w_q) de G , avec $(u_1, \dots, u_m) = (v_1, \dots, v_m) = (w_1, \dots, w_m)$.

On constate que $(u_1, \dots, u_m, v_{m+1}, \dots, v_p, w_{m+1}, \dots, w_q)$ est une base de $F + G$, car :

si $\alpha_1 u_1 + \dots + \alpha_m u_m + \beta_{m+1} v_{m+1} + \dots + \beta_p v_p + \gamma_{m+1} w_{m+1} + \dots + \gamma_q w_q = 0$,

alors $\alpha_1 u_1 + \dots + \alpha_m u_m + \beta_{m+1} v_{m+1} + \dots + \beta_p v_p, \alpha_1 u_1 + \dots + \alpha_m u_m + \gamma_{m+1} w_{m+1} + \dots + \gamma_q w_q \in F \cap G$
puis $\alpha_1 = \dots = \alpha_m = \beta_{m+1} = \dots = \beta_p v_p = \gamma_{m+1} = \dots = \gamma_q = 0$. \square

Définition-Proposition

On suppose que E est de dimension finie, notée n .

On dit qu'un sous-espace vectoriel H de E est un *hyperplan* si $\dim H = n - 1$, ce qui équivaut au fait que H a un supplémentaire dans E qui est une droite.

DÉMONSTRATION

(\Rightarrow) La dernière remarque montre que H a au moins un supplémentaire D dans E . Vu le b) de la proposition, ce supplémentaire D a pour dimension 1 et est donc une droite.

(\Leftarrow) Cela découle aussi du b) de la proposition. \square

Exemple

Soit $(a_1, \dots, a_n) \in \mathbb{R}^n \setminus \{0\}$. La partie $F: a_1 x_1 + \dots + a_n x_n = 0$ de \mathbb{R}^n est un hyperplan vectoriel de \mathbb{R}^n car on constate que la méthode de Gauss fournit une base (w_1, \dots, w_{n-1}) de F .

Ch. 4. Applications linéaires sur $\mathbb{K} = \mathbb{R}$ ou \mathbb{C}

Plan

- I. Applications linéaires
- II. Utilisation des matrices

I. APPLICATIONS LINÉAIRES

Dans toute cette partie, on fixe trois \mathbb{K} -espace vectoriel E, F et G .

1. Généralités

Définition

(a) On dit qu'une application $f : E \rightarrow F$ est *linéaire* si :

$$f(\alpha v + \beta w) = \alpha f(v) + \beta f(w) \text{ pour tous } \alpha, \beta \in \mathbb{K} \text{ et } v, w \in E.$$

Dans ce cas : $f(0_E) = 0_F$ en choisissant $\alpha = \beta = 0$ et $v = w = 0_E$;
 $f\left(\sum_{k=1}^p \alpha_k v_k\right) \stackrel{\text{récurrence sur } p}{=} \sum_{k=1}^p \alpha_k f(v_k)$ pour $\alpha_1, \dots, \alpha_p \in \mathbb{K}$ et $v_1, \dots, v_p \in E$.

(b) On appelle plus précisément :

- *forme linéaire sur E* une application linéaire de E dans \mathbb{K} ;
- *endomorphisme de (l'espace vectoriel) E* une application linéaire de E dans E ;
- *isomorphisme (d'espaces vectoriels) de E sur F* une bijection linéaire de E sur F ;
- *automorphisme de (l'espace vectoriel) E* une bijection linéaire de E sur E .

(c) On dit que les espaces vectoriels E et F sont isomorphes s'il existe un isomorphisme d'espaces vectoriels de E sur F .

Exemples

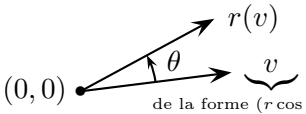
(1) Soit $A \in \mathfrak{M}_{n,p}(\mathbb{K})$. On considère $f : \mathbb{K}^p \rightarrow \mathbb{K}^n$ où $Y := AX$.

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \mapsto Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

L'application f est linéaire, car pour tous $\alpha, \beta \in \mathbb{K}$ et $V, W \in \mathbb{K}^p$ on a :

$$f(\alpha V + \beta W) = A(\alpha V + \beta W) = \alpha AV + \beta AW = \alpha f(V) + \beta f(W).$$

(2) Soit $\theta \in \mathbb{R}$. L'application $r : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ avec $\begin{cases} x' = (\cos \theta) x - (\sin \theta) y \\ y' = (\sin \theta) x + (\cos \theta) y \end{cases}$ est linéaire.
cf. l'exemple (1) ci-dessus

Géométriquement :  donc r est la rotation (vectorielle) d'angle θ .

(3) La dérivation $\delta : \mathbb{K}[X] \rightarrow \mathbb{K}[X]$ est un endomorphisme de l'espace vectoriel $\mathbb{K}[X]$.
 $P \mapsto P'$

En effet, étant donnés $\alpha, \beta \in \mathbb{K}$ et $P = a_p X^p + \dots + a_1 X + a_0, Q = b_q X^q + \dots + b_1 X + b_0 \in \mathbb{K}[X]$, en posant $n = \max(p, q)$, $a_i = 0$ quand $i > p$ et $b_j = 0$ quand $j > q$, on a :

$$\begin{aligned} \delta(\alpha P + \beta Q) &= \delta((\alpha a_n + \beta b_n)X^n + \dots + (\alpha a_1 + \beta b_1)X + (\alpha a_0 + \beta b_0)) \\ &= n(\alpha a_n + \beta b_n)X^{n-1} + \dots + 2(\alpha a_2 + \beta b_2)X + (\alpha a_1 + \beta b_1) \\ &= \alpha(na_n X^{n-1} + \dots + 2a_2 X + a_1) + \beta(nb_n X^{n-1} + \dots + 2b_2 X + b_1) \\ &= \alpha\delta(P) + \beta\delta(Q) \end{aligned}$$

(4) La transposition $t : \mathfrak{M}_{n,p}(\mathbb{K}) \rightarrow \mathfrak{M}_{p,n}(\mathbb{K})$ est linéaire (exercice!).
 $A \mapsto {}^t A$

Remarque

On suppose que E est de dimension finie, de base $\mathcal{B} = (v_1, \dots, v_n)$, et note (e_1, \dots, e_n) la base canonique de \mathbb{K}^n . D'après la proposition (a), l'unique $f \in \mathcal{L}(E, \mathbb{K}^n)$ tel que $f(v_1) = e_1$ et ... et $f(v_n) = e_n$ est un isomorphisme de E sur \mathbb{K}^n . Par linéarité, f envoie $v \Big|_{\mathcal{B}} X$ sur X .

Exemple (« changement de base »)

Les vecteurs $v_1 := \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ et $v_2 := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ de \mathbb{R}^2 sont clairement non-colinéaires. Donc (v_1, v_2) est une base de \mathbb{R}^2 . Soit $f \in \mathcal{L}(\mathbb{R}^2)$ déterminé par : $f(v_1) = 2v_2$ et $f(v_2) = v_1 + v_2$.

On cherche à calculer $f(x, y)$ pour $x, y \in \mathbb{R}$.

On exprime les vecteurs de la base canonique (e_1, e_2) de \mathbb{R}^2 à l'aide de (v_1, v_2) .

On a : $\begin{cases} 3e_1 + 2e_2 = v_1 \\ e_1 + e_2 = v_2 \end{cases}$. Présentation « à la Gauss », qui sera utile en L2 dans le cas triangulaire :

$$\left(\begin{array}{cc|c} e_1 & e_2 & \\ \hline 3 & 2 & v_1 \\ 1 & 1 & v_2 \end{array} \right) \xrightarrow{L_2 \leftarrow 3L_2 - L_1} \left(\begin{array}{cc|c} e_1 & e_2 & \\ \hline 3 & 2 & v_1 \\ 0 & -1 & -v_1 + 3v_2 \end{array} \right) \text{ donc } \begin{cases} e_1 = \frac{1}{3}(-2(-v_1 + 3v_2) + v_1) = v_1 - 2v_2 \\ e_2 = -v_1 + 3v_2 \end{cases}$$

puis $\begin{cases} f(e_1) = f(v_1) - 2f(v_2) = -2v_1 = \begin{pmatrix} -6 \\ -4 \end{pmatrix} \\ f(e_2) = -f(v_1) + 3f(v_2) = 3v_1 + v_2 = \begin{pmatrix} 10 \\ 7 \end{pmatrix} \end{cases}$.

D'où $f\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = f(xe_1 + ye_2) = xf(e_1) + yf(e_2) = \begin{pmatrix} -6x+10y \\ -4x+7y \end{pmatrix}$.

2. Noyau et image

Lemme

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

(a) L'image réciproque $f^{-1}(W) := \{v \in E \mid f(v) \in W\}$ d'un sous-espace vectoriel W de F par f , est un sous-espace vectoriel de E .

(b) L'image directe $f(V) := \underbrace{\{f(v) \mid v \in V\}}_{\text{notation pour } \{w \in F \mid \exists v \in V \ w = f(v)\}}$ d'un sous-espace vectoriel V de E par f , est un sous-espace vectoriel de F .

DÉMONSTRATION

(a) Soit W un sous-espace vectoriel de F .

(i) On a : $f(0_E) = 0_F$ (car f est linéaire) avec $0_F \in W$, donc $0_E \in f^{-1}(W)$.

(ii) Soient $\alpha, \alpha' \in \mathbb{K}$ et $v, v' \in f^{-1}(W)$. On a donc : $f(v), f(v') \in W$.

Par linéarité de f on a ensuite : $f(\alpha v + \alpha' v') = \alpha f(v) + \alpha' f(v')$ avec $\alpha f(v) + \alpha' f(v') \in W$.

D'où : $\alpha v + \alpha' v' \in f^{-1}(W)$.

Ainsi $f^{-1}(W)$ est un sous-espace vectoriel de E .

(b) Soit V un sous-espace vectoriel de E .

(i) On a : $0_F = f(0_E)$ avec $0_E \in V$, donc $0_F \in f(V)$.

(ii) Soient $\alpha, \alpha' \in \mathbb{K}$ et $w, w' \in f(V)$. Il existe $v, v' \in V$ tels que $w = f(v)$ et $w' = f(v')$.

Par linéarité de f on a : $\alpha w + \alpha' w' = \alpha f(v) + \alpha' f(v') = f(\alpha v + \alpha' v')$ avec $\alpha v + \alpha' v' \in V$.

D'où : $\alpha w + \alpha' w' \in f(V)$.

Par conséquent $f(V)$ est un sous-espace vectoriel de F . □

Définition-Proposition

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

(a) Le noyau de f , noté $\text{Ker } f$, est le sous-espace vectoriel $f^{-1}(\{0\})$ de E :

$$\text{Ker } f := \{v \in E \mid f(v) = 0\}. \quad \leftarrow \text{[équation cartésienne]}$$

(b) On a : f est injective si et seulement si $\text{Ker } f = \{0\}$.

(c) L'image de l'application f , notée $\text{Im } f$, est le sous-espace vectoriel $f(E)$ de F :

$$\text{Im } f := \{w \in F \mid \exists v \in E \ f(v) = w\}. \quad \leftarrow \text{[équation paramétrique]}$$

(d) On a : f est surjective si et seulement si $\text{Im } f = F$.

(e) Si $E = \text{Vect}(v_1, \dots, v_p)$ avec $v_1, \dots, v_p \in E$, alors $\text{Im } f = \text{Vect}(f(v_1), \dots, f(v_p))$.

DÉMONSTRATION

(a) D'après le lemme (a), $\text{Ker } f$ est un sous-espace vectoriel de E .

(b) (\Rightarrow) On suppose que f est injective. Si $v \in \text{Ker } f$, alors $f(v) = 0_F = f(0_E)$ alors, par injectivité de f , $v = 0_E$. Ainsi $\text{Ker } f \subseteq \{0\}$. Comme $\{0\} \subseteq \text{Ker } f$ d'après (a) : $\text{Ker } f = \{0\}$.

(\Leftarrow) On suppose que $\text{Ker } f = \{0\}$. Si $v, v' \in E$ vérifient $f(v) = f(v')$, alors $f(v - v') = f(v) - f(v') = 0$, alors $v - v' \in \text{Ker } f$, alors vu l'hypothèse $v = v'$. Ainsi f est injective.

(c) D'après le lemme (b), $\text{Im } f$ est un sous-espace vectoriel de F .

(d) Découle des définitions des notions de « surjectivité » et « image d'une application ».

(e) On suppose que $v_1, \dots, v_p \in E$ vérifient : $E = \text{Vect}(v_1, \dots, v_p)$. On a :

$$\begin{aligned} f(E) &= f(\{\alpha_1 v_1 + \dots + \alpha_p v_p ; \alpha_1, \dots, \alpha_p \in \mathbb{K}\}) = \{f(\alpha_1 v_1 + \dots + \alpha_p v_p) ; \alpha_1, \dots, \alpha_p \in \mathbb{K}\} \\ &= \{\alpha_1 f(v_1) + \dots + \alpha_p f(v_p) ; \alpha_1, \dots, \alpha_p \in \mathbb{K}\} = \text{Vect}(f(v_1), \dots, f(v_p)). \end{aligned}$$

D'où le résultat. □

Exemple (en « dimension infinie »)

On note ici $\mathcal{Pol}(\mathbb{K}, \mathbb{K})$ le sous-espace vectoriel $\text{Vect}(\{f_n : x \mapsto x^n ; n \in \mathbb{N}\})$ de $\mathbb{K}^{\mathbb{K}}$ formé des $p : \mathbb{K} \rightarrow \mathbb{K}$ de la forme $p : x \mapsto a_n x^n + \dots + a_1 x + a_0$ pour certains $n \in \mathbb{N}$ et $a_0, \dots, a_n \in \mathbb{K}$.

$$\begin{aligned} \text{On considère } f : \quad \mathbb{K}[X] &\longrightarrow \mathcal{Pol}(\mathbb{K}, \mathbb{K}) \\ P = a_n X^n + \dots + a_1 X + a_0 &\longmapsto (p : x \mapsto a_n x^n + \dots + a_1 x + a_0) \end{aligned}$$

L'application f est linéaire (facile), et surjective par définition de $\mathcal{Pol}(\mathbb{K}, \mathbb{K})$.

On utilise le (b) de la définition-proposition pour montrer que f est injective.

Soit $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{K}[X]$ tel que l'application $p := f(P)$ est nulle.

Comme $\mathbb{R} \subseteq \mathbb{K}$, on a en particulier : $\forall x \in \mathbb{R} \quad a_n x^n + \dots + a_1 x + a_0 = 0$,

donc $a_0 = p|_{\mathbb{R}}(0) = 0$, $a_1 = p|_{\mathbb{R}}'(0) = 0$, ..., $n! a_n = p|_{\mathbb{R}}^{(n)}(0) = 0$ et a fortiori $P = 0$.

Par conséquent $\text{Ker } f = \{0\}$, ce qui prouve que f est injective.

Ainsi f est un isomorphisme de \mathbb{K} -espaces vectoriels.

Définition-Proposition

On suppose que E ou F est de dimension finie. Soit $f \in \mathcal{L}(E, F)$.

(a) L'espace vectoriel $\text{Im } f$ est ici de dimension finie.

On note : $\text{rg } f := \dim(\text{Im } f)$ « rang de f ».

(b) Si $E = \text{Vect}(v_1, \dots, v_p)$ avec $v_1, \dots, v_p \in E$, alors $\text{rg } f = \text{rg}(f(v_1), \dots, f(v_p))$.

DÉMONSTRATION

(a) Si E est de dimension finie, on va voir dans la démonstration du (b) que $\text{Im } f$ a une famille génératrice finie dont on pourra extraire une base finie.

Si F est de dimension finie, l'espace vectoriel $\text{Im } f$ qui en est un sous-espace vectoriel est aussi de dimension finie.

(b) D'après le (e) de la définition-proposition qui précède : $\text{Im } f = \text{Vect}(f(v_1), \dots, f(v_p))$.

D'où : $\text{rg } f = \dim(\text{Im } f) = \dim(\text{Vect}(f(v_1), \dots, f(v_p))) = \text{rg}(f(v_1), \dots, f(v_p))$. □

Exemple (exercice type)

$$\text{Soit } f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3 \text{ définie par } \begin{cases} x' = -4x + 12y - 5z \\ y' = x - 3y + 2z \\ z' = 2x - 6y + z \end{cases}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \longmapsto \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

(a) Équation cartésienne de $\text{Im } f$ et base de $\text{Im } f$?

Un vecteur $w = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{R}^3$ appartient à $\text{Im } f$ si et seulement si l'équation $(\star) f(v) = w$ d'inconnue $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ a au moins une solution. On étudie (\star) par la méthode de Gauss :

$$\left(\begin{array}{ccc|c} x & y & z & \\ \hline -4 & 12 & -5 & a \\ 1 & -3 & 2 & b \\ 2 & -6 & 1 & c \end{array} \right) \xrightarrow{\substack{L_2 \leftarrow 4L_2 + L_1 \\ L_3 \leftarrow 2L_3 + L_1}} \left(\begin{array}{ccc|c} x & y & z & \\ \hline -4 & 12 & -5 & a \\ 0 & 0 & 3 & a+4b \\ 0 & 0 & -3 & a+2c \end{array} \right)$$

$$\xrightarrow{C_2 \leftrightarrow C_3} \left(\begin{array}{ccc|c} x & z & y & \\ \hline -4 & -5 & 12 & a \\ 0 & 3 & 0 & a+4b \\ 0 & -3 & 0 & a+2c \end{array} \right) \xrightarrow{L_3 \leftarrow L_3 + L_2} \left(\begin{array}{ccc|c} x & z & y & \\ \hline -4 & -5 & 12 & a \\ 0 & 3 & 0 & a+4b \\ 0 & 0 & 0 & 2a+4b+2c \end{array} \right)$$

donc : $w \in \text{Im } f \iff 2a + 4b + 2c = 0 \iff a + 2b + c = 0$.

Ainsi, dans les coordonnées habituelles : $\text{Im } f$ a pour équation cartésienne $x + 2y + z = 0$.

En ne considérant que les colonnes sous x, y, z d'une part et sous x, z d'autre part, le calcul précédent donne aussi : $\dim(\text{Im } f) = \text{rg}(f(e_1), f(e_2), f(e_3)) = 2$ et $\text{rg}(f(e_1), f(e_3)) = 2$, donc $(f(e_1), f(e_3))$ engendre $\text{Im } f$ qui est de dimension 2, puis : $\text{Im } f$ a pour base $\left(\begin{pmatrix} -4 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -5 \\ 2 \\ 1 \end{pmatrix} \right)$.

(b) Équation cartésienne de $\text{Ker } f$ avec deux égalités (entre réels) et base de $\text{Ker } f$?

Un vecteur $v = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$ appartient à $\text{Ker } f$ si et seulement si $(\star\star) f(v) = 0$.

La méthode de Gauss pour résoudre $(\star\star)$ est le calcul du (a) avec un second membre nul.

$$\text{Donc : Ker } f : \begin{cases} -4x - 5z + 12y = 0 \\ 3z = 0 \end{cases}$$

Par remontée triangulaire, on obtient :

$$\text{Ker } f \begin{cases} x = 3t \\ y = t \\ z = 0 \end{cases}, t \in \mathbb{R}. \text{ Donc Ker } f = \text{Vect} \left(\underbrace{\begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}}_{\text{vecteur non-nul}} \right) \text{ puis Ker } f \text{ a pour base } \left(\begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix} \right).$$

Proposition

Soit $f \in \mathcal{L}(E, F)$. On suppose donné un supplémentaire S de $\text{Ker } f$ dans E (on sait qu'il en existe quand E est de dimension finie).

L'application $\tilde{f} : S \rightarrow \text{Im } f$ est linéaire bijective.

$$x \mapsto f(x)$$

DÉMONSTRATION

Il est clair que $f(x) \in \text{Im } f$ pour tout $x \in S$, et ensuite que \tilde{f} est linéaire.

On a : $\text{Im } \tilde{f} = \tilde{f}(S) = f(S) = f(S + \text{Ker } f) = f(E) = \text{Im } f$

et $\text{Ker } \tilde{f} = \{x \in S \mid f(x) = 0\} = S \cap \text{Ker } f = \{0\}$. Donc \tilde{f} est bijective. \square

Théorème (« théorème du rang »)

Soit $f \in \mathcal{L}(E, F)$. On suppose que E est de dimension finie.

On a : $\dim \text{Ker } f + \dim \text{Im } f = \dim \underbrace{E}_{\text{espace de départ}}$ où $\text{Ker } f$ et $\text{Im } f$ sont de dimension finie.

DÉMONSTRATION

Il existe – et on fixe – un supplémentaire S de $\text{Ker } f$ dans E .

On a d'une part $\dim E = \dim \text{Ker } f + \dim S$ car $E = \text{Ker } f \oplus S$, et d'autre part $\text{Im } f$ est de dimension finie avec $\dim S = \dim \text{Im } f$ d'après la proposition. D'où le résultat. \square

Exemple

L'application linéaire $f : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ vérifie : $\text{Ker } f = \text{Im } f = (Oy)$.

$$(x, y) \mapsto (0, x)$$

$$\text{On a bien : } \underbrace{\dim \text{Ker } f}_1 + \underbrace{\dim \text{Im } f}_1 = \underbrace{\dim \mathbb{R}^2}_2.$$

Mais $\text{Ker } f$ et $\text{Im } f$ ne sont pas supplémentaires dans \mathbb{R}^2 !

Corollaire (important)

Soit $f \in \mathcal{L}(E)$. On suppose que E est de dimension finie.

Les propriétés suivantes sont équivalentes :

(i) f est injective ; (ii) f est surjective ; (iii) f est bijective.

DÉMONSTRATION

On vient de voir que : $\dim \text{Ker } f + \dim \text{Im } f = \dim E$.

Donc : (i) $\iff \text{Ker } f = \{0\} \iff \dim \text{Ker } f = 0$
 $\iff \dim \text{Im } f = \dim E \iff \text{Im } f = E$
 \iff (ii).

On en déduit que : (i) \iff ((i) et (ii)) \iff (iii). □

Remarque

Le corollaire devient faux en enlevant l'hypothèse « E est de dimension finie ».

Par exemple, on peut montrer que la dérivation $\delta : \mathbb{K}[X] \rightarrow \mathbb{K}[X]$ définie dans le paragraphe 1, est surjective mais n'est pas injective.

II. UTILISATION DES MATRICES

Dans cette partie, on fixe trois \mathbb{K} -espaces vectoriels E, F et G de dimension finie.

On se donne des bases $\mathcal{B} = (v_1, \dots, v_p)$ de E , $\mathcal{C} = (w_1, \dots, w_n)$ de F et \mathcal{D} de G .

1. Matrice d'une application linéaire

Définition-Proposition

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

(a) La matrice de f dans les bases \mathcal{B} et \mathcal{C} est : $\text{Mat}_{\mathcal{B}, \mathcal{C}} f := \begin{pmatrix} f(v_1)/\mathcal{C} & \dots & f(v_p)/\mathcal{C} \\ \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] & \dots & \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] \end{pmatrix}$.

Il s'agit de l'unique matrice $A \in \mathfrak{M}_{n,p}(\mathbb{K})$ telle que :

$$f : v \Big|_X \Big|_{\mathcal{B}} \mapsto w \Big|_Y \Big|_{\mathcal{C}} \text{ où } \boxed{Y = AX}.$$

(b) Quand $E = F$ et $\mathcal{B} = \mathcal{C}$, on note : $\text{Mat}_{\mathcal{B}} f := \text{Mat}_{\mathcal{B}, \mathcal{B}} f$.

DÉMONSTRATION

Soit $A \in \mathfrak{M}_{n,p}(\mathbb{K})$. L'application $g : v \Big|_X \Big|_{\mathcal{B}} \mapsto w \Big|_Y \Big|_{\mathcal{C}} AX$ est linéaire (facile).

Les vecteurs $g(v_1), \dots, g(v_p)$ ont pour coordonnées $A \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, A \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ dans \mathcal{C} .

Les colonnes de A sont donc $g(v_1)/\mathcal{C}, \dots, g(v_p)/\mathcal{C}$.

Si $f = g$, alors vu ce qui précède $A = \text{Mat}_{\mathcal{B}, \mathcal{C}} f$.

Si $A = \text{Mat}_{\mathcal{B}, \mathcal{C}} f$, alors f coïncide avec g en chacun des vecteurs v_1, \dots, v_p , puis $f = g$. □

Exemples

(1) On a, par la définition du (a) : $\text{Mat}_{\mathcal{B}} \text{id}_E = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = I_p$ où $p = \dim E$.

(2) Soit $A \in \mathfrak{M}_{n,p}(\mathbb{K})$. On sait que l'application $f : \mathbb{K}^p \rightarrow \mathbb{K}^n$ est linéaire.
 $X \mapsto AX$

Par la caractérisation du (a), la matrice de f dans les bases canoniques est égale à A .

(3) Soit $\theta \in \mathbb{R}$. La rotation $r : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ déterminée par $\begin{cases} x' = (\cos \theta) x - (\sin \theta) y \\ y' = (\sin \theta) x + (\cos \theta) y \end{cases}$
 $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x' \\ y' \end{pmatrix}$

s'écrit $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. On a donc : $\text{Mat}_{\text{base canonique de } \mathbb{R}^2} r = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$.

(4) On considère l'application $\tilde{f} : \mathbb{R}_2[X] \rightarrow \mathbb{R}[X]$ qui est clairement linéaire.
 $P \mapsto (X+1)P' - P$

On cherche, à l'aide d'un calcul matriciel, une base de $\text{Ker } \tilde{f}$ et une base de $\text{Im } \tilde{f}$.

On a : $\tilde{f}(1) = -1$, $\tilde{f}(X) = 1$ et $\tilde{f}(X^2) = X^2 + 2X$.

Par conséquent : $\text{Im } \tilde{f} = \text{Vect}(\tilde{f}(1), \tilde{f}(X), \tilde{f}(X^2)) \subseteq \mathbb{R}_2[X]$.

Cela permet de définir l'application $f : \mathbb{R}_2[X] \rightarrow \mathbb{R}_2[X]$ qui est encore linéaire.
 $P \mapsto (X+1)P' - P$

On a : $\text{Ker } \tilde{f} = \text{Ker } f$ et $\text{Im } \tilde{f} = \text{Im } f$. On recherche des bases de $\text{Ker } f$ et $\text{Im } f$ en coordonnées.

Par définition, la matrice $\mathfrak{Mat}_{(1,X,X^2)} f$ est : $A := \begin{pmatrix} -1 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix}$.

On prend en compte l'autre caractérisation donnée pour $\mathfrak{Mat}_{(1,X,X^2)} f$:

$$\text{Ker } f = \left\{ P \in \mathbb{R}_2[X] \mid f(P) = 0 \right\} = \left\{ P \Big|_{/(1,X,X^2)} \begin{matrix} a_0 \\ a_1 \\ a_2 \end{matrix} \in \mathbb{R}^3 \mid A \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

On résout l'équation $A \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ d'inconnue $\begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} \in \mathbb{R}^3$ par la méthode de Gauss :

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ \textcircled{-1} & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{C_2 \leftrightarrow C_3} \begin{pmatrix} a_0 & a_2 & a_1 \\ -1 & 0 & 1 \\ 0 & \textcircled{2} & 0 \\ 0 & 1 & 0 \end{pmatrix} \xrightarrow{L_3 \leftarrow 2L_3 - L_2} \begin{pmatrix} a_0 & a_2 & a_1 \\ -1 & 0 & 1 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Donc $\text{Ker } f : \begin{cases} a_0 = t \\ a_1 = t, t \in \mathbb{R}, \text{ puis } \text{Ker } f = \{t(X+1) ; t \in \mathbb{R}\} \text{ et } \text{Ker } f \text{ a pour base } (X+1). \\ a_2 = 0 \end{cases}$

Ce calcul par Gauss montre aussi que $\text{rg}(f(1), f(X), f(X^2)) = \text{rg}(f(1), f(X^2)) = 2$.

Il en résulte que $\text{Im } f$ a pour base $(f(1), f(X^2))$, c'est-à-dire $(-1, X^2 + 2X)$.

Définition-Proposition

(a) L'application $\mathcal{L}(E, F) \rightarrow \mathfrak{M}_{n,p}(\mathbb{K})$ est un isomorphisme de \mathbb{K} -espaces vectoriels.
 $f \mapsto \mathfrak{Mat}_{\mathcal{B},\mathcal{C}} f$

Donc $\mathcal{L}(E, F)$ est de dimension finie et $\dim \mathcal{L}(E, F) = (\dim E)(\dim F)$.

Le \mathbb{K} -espace vectoriel E^* des formes linéaires sur E a d'ailleurs une base $\mathcal{B}^* = (v_1^*, \dots, v_p^*)$, appelée *base duale de \mathcal{B}* , qui est déterminée par : $v_i^*(v_i) = 1$ et $v_i^*(v_j) = 0$ quand $j \neq i$.

(b) Soient $f \in \mathcal{L}(E, F)$ et $g \in \mathcal{L}(F, G)$.

On a : $\mathfrak{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = (\mathfrak{Mat}_{\mathcal{C},\mathcal{D}} g) (\mathfrak{Mat}_{\mathcal{B},\mathcal{C}} f)$.

(c) Soit $f \in \mathcal{L}(E, F)$. On pose $A := \mathfrak{Mat}_{\mathcal{B},\mathcal{C}} f \in \mathfrak{M}_{n,p}(\mathbb{K})$.

L'application ${}^t f : F^* \rightarrow E^*$ est linéaire. De plus : $\mathfrak{Mat}_{\mathcal{C}^*,\mathcal{B}^*}({}^t f) = {}^t A$.

$$\varphi \mapsto \varphi \circ f$$

DÉMONSTRATION

(a) Il est clair que l'application $\mathfrak{Mat}_{\mathcal{B},\mathcal{C}} : \mathcal{L}(E, F) \rightarrow \mathfrak{M}_{n,p}(\mathbb{K})$ est linéaire.
 $f \mapsto \mathfrak{Mat}_{\mathcal{B},\mathcal{C}} f$

Soit $A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{np} \end{pmatrix} \in \mathfrak{M}_{n,p}(\mathbb{K})$. On note $\widetilde{w}_1, \dots, \widetilde{w}_p \in F$ tels que $\widetilde{w}_1 \Big|_{/\mathcal{C}} \begin{matrix} a_{11} \\ \vdots \\ a_{n1} \end{matrix}$ et ... et $\widetilde{w}_p \Big|_{/\mathcal{C}} \begin{matrix} a_{1p} \\ \vdots \\ a_{np} \end{matrix}$.

D'après une proposition du II 1, il existe $f \in \mathcal{L}(E, F)$ unique tel que $f(v_1) = \widetilde{w}_1$ et ... et $f(v_p) = \widetilde{w}_p$, c'est-à-dire $\mathfrak{Mat}_{\mathcal{B},\mathcal{C}} f = A$. Ainsi, l'application $\mathfrak{Mat}_{\mathcal{B},\mathcal{C}}$ est bijective.

Dans le cas où $F = \mathbb{K}$ et $\mathcal{C} = (1)$, les images des vecteurs v_1^*, \dots, v_p^* sont les vecteurs $E_{1,1}, \dots, E_{1,p}$ de $\mathfrak{M}_{1,p}(\mathbb{K})$. Cela prouve que \mathcal{B}^* est une base de E^* .

(b) On pose $A := \mathfrak{Mat}_{\mathcal{B},\mathcal{C}} f$ et $B := \mathfrak{Mat}_{\mathcal{C},\mathcal{D}} g$.

On obtient la décomposition $g \circ f : u \Big|_{/\mathcal{B}} X \xrightarrow{f} v \Big|_{/\mathcal{C}} Y \xrightarrow{g} w \Big|_{/\mathcal{D}} Z$ avec $Z = BY$ et $Y = AX$.

Donc $Z = (BA)X$, ce qui prouve que : $\mathfrak{Mat}_{\mathcal{B},\mathcal{D}}(g \circ f) = BA$.

(c) Il est clair que $\varphi \circ f \in E^*$ pour tout $\varphi \in F^*$, et ensuite que ${}^t f$ est linéaire.

Le coefficient de $\mathfrak{Mat}_{\mathcal{C}^*,\mathcal{B}^*}({}^t f)$ sur la i^e ligne et j^e colonne est la i^e coordonnée α_i de ${}^t f(w_j^*) =$

$$\sum_{i=1}^p \alpha_i v_i^* \text{ suivant } (v_1^*, \dots, v_p^*). \text{ Or : } \alpha_i = ({}^t f(w_j^*))(v_i) = w_j^* \left(\sum_{k=1}^n a_{ki} w_k \right) = a_{ji}.$$

D'où le résultat. \square

2. Utilisation du rang

Proposition

Soit $f \in \mathcal{L}(E, F)$. On pose $A := \mathfrak{Mat}_{\mathcal{B}, \mathcal{C}} f \in \mathfrak{M}_{n,p}(\mathbb{K})$.

(a) On a : $\text{rg}(A) = \text{rg}(f)$.

D'où : $\begin{cases} f \text{ est surjective si et seulement si } \text{rg}(A) = n ; \\ f \text{ est injective si et seulement si } \text{rg}(A) = p. \end{cases}$

(b) L'application f est bijective si et seulement si : $n = p$ et A est inversible.

Dans ce cas : $\mathfrak{Mat}_{\mathcal{C}, \mathcal{B}}(f^{-1}) = A^{-1}$.

(c) On a : $\text{rg}({}^t f) = \text{rg}(f)$, donc $\text{rg}({}^t A) = \text{rg}(A)$ (déjà vu).

DÉMONSTRATION

((a) On sait calculer le rang d'une matrice et d'une famille de vecteurs par la méthode de Gauss : $\text{rg} A = r = \text{rg}(f(v_1), \dots, f(v_p)) = \text{rg} f$.

Pour le reste, on utilise : $\dim F = n$ et $\dim \text{Ker} f = p - \text{rg} f$ (théorème du rang).

b) D'après (a), f est bijective si et seulement si $n = p$ et $\text{rg} A = n$, c'est à dire : $n = p$ et A est inversible. Dans ce cas, on sait que f^{-1} est linéaire. On a : $f^{-1} \circ f = \text{id}_E$ donc $\mathfrak{Mat}_{\mathcal{C}, \mathcal{B}}(f^{-1}) A = I_n$, ce qui donne le résultat en multipliant à droite par A^{-1} .

Variante (sans utiliser le rang)

Pour tout $g \in \mathcal{L}(F, E)$, on a :

$$\begin{aligned} f \text{ bijective et } f^{-1} = g &\iff g \circ f = \text{id}_E \text{ et } f \circ g = \text{id}_F \\ &\iff \underbrace{n = p}_{\text{nécessaire pour que } E \text{ et } F \text{ soient isomorphes}} \text{ et } \mathfrak{Mat}_{\mathcal{B}, \mathcal{B}}(g \circ f) = I_n \text{ et } \mathfrak{Mat}_{\mathcal{C}, \mathcal{C}}(f \circ g) = I_n \\ &\iff n = p \text{ et } (\mathfrak{Mat}_{\mathcal{C}, \mathcal{B}} g) A = I_n \text{ et } A (\mathfrak{Mat}_{\mathcal{C}, \mathcal{B}} g) = I_n \\ &\iff A \text{ inversible et } A^{-1} = \mathfrak{Mat}_{\mathcal{C}, \mathcal{B}} g \end{aligned}$$

Si f est bijective, on sait que f^{-1} est linéaire, et en appliquant ce qui précède à $g := f^{-1}$, on en déduit que A est inversible d'inverse $\mathfrak{Mat}_{\mathcal{C}, \mathcal{B}}(f^{-1})$.

Si A est inversible, on sait que son inverse est la matrice dans les bases \mathcal{C} et \mathcal{B} d'une application linéaire g , et on déduit de ce qui précède que f est bijective.

(c) D'après le théorème du rang, on a : $\text{rg}({}^t f) = \dim F - \dim \text{Ker}({}^t f)$.

Par ailleurs : $\text{Ker}({}^t f) = \{\varphi \in F^* \mid \varphi|_{\text{Im} f} = 0\}$. Soit (u_1, \dots, u_r) une base de $\text{Im} f$. On la complète en une base (u_1, \dots, u_n) de F . On note (u_1^*, \dots, u_n^*) sa base duale.

Pour tout $\varphi = \sum_{i=1}^n \alpha_i u_i^* \in F^*$, on a : $\varphi|_{\text{Im} f} = 0 \iff \alpha_1 = \dots = \alpha_r = 0$.

Ainsi $\text{Ker}({}^t f)$ a pour base $(u_{r+1}^*, \dots, u_n^*)$, ce qui donne l'égalité $\text{rg}({}^t f) = \text{rg}(f)$.

Finalement : $\text{rg}({}^t A) = \text{rg}({}^t f) = \text{rg}(f) = \text{rg}(A)$. □

Remarque

Soit $A \in \mathfrak{M}(n, \mathbb{K})$. On lui associe l'application linéaire $f : \mathbb{K}^n \rightarrow \mathbb{K}^n$.
 $X \mapsto AX$

Pour montrer que A est inversible et calculer A^{-1} , il suffit de montrer que f est bijective et calculer f^{-1} . Pour cela on peut tenter de résoudre à $Y \in \mathbb{K}^n$ fixé le système $AX = Y$ d'inconnue $X \in \mathbb{K}^n$ et de prouver qu'il a une unique solution qu'on écrira sous la forme $X = BY$ avec $B \in \mathfrak{M}(n, \mathbb{K})$. Dans ce cas, on aura : $\underbrace{A \text{ est inversible}}_{\text{car } f \text{ est bijective}} \text{ et } A^{-1} = \underbrace{B}_{\text{matrice de } f^{-1} : Y \mapsto BY}$.

3. Changement de base

On se donne deux nouvelles bases, $\mathcal{B}' = (v'_1, \dots, v'_p)$ de E et $\mathcal{C}' = (w'_1, \dots, w'_n)$ de F .

Définition-Proposition

(a) La matrice de passage de \mathcal{B} à \mathcal{B}' est :
$$\begin{pmatrix} v'_1/\mathcal{B} & \dots & v'_p/\mathcal{B} \\ \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] & \dots & \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] \end{pmatrix}.$$

(b) Il s'agit de l'unique matrice $P \in \mathfrak{M}(p, \mathbb{K})$ vérifiant :

$$\text{si } v \underset{\mathcal{B}}{\Big|} X \in E \text{ alors on a } v \underset{\mathcal{B}'}{\Big|} X' \text{ avec } \underbrace{X = PX'}_{\text{attention!}}.$$

(c) On a : P est inversible et P^{-1} est la matrice de passage de \mathcal{B}' à \mathcal{B} .

DÉMONSTRATION

(b) Comme la matrice de passage de \mathcal{B} à \mathcal{B}' est égale à $\mathfrak{Mat}_{\mathcal{B}', \mathcal{B}} \text{id}_E$, il suffit d'appliquer le résultat analogue du paragraphe 1.

(c) Puisque id_E est bijective de réciproque id_E , la matrice $\mathfrak{Mat}_{\mathcal{B}', \mathcal{B}} \text{id}_E$ est inversible et son inverse est égal à $\mathfrak{Mat}_{\mathcal{B}, \mathcal{B}'} \text{id}_E$. Compte tenu de l'égalité du début de cette démonstration, cela signifie que P est inversible et d'inverse la matrice de passage de \mathcal{B}' à \mathcal{B} . \square

Remarque

Soient $\tilde{v}_1, \dots, \tilde{v}_p \in E$. On pose $\tilde{\mathcal{B}} := (\tilde{v}_1, \dots, \tilde{v}_p)$ et $\tilde{P} := \begin{pmatrix} \tilde{v}_1/\mathcal{B} & \dots & \tilde{v}_p/\mathcal{B} \\ \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] & \dots & \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] \end{pmatrix}.$

Si on dispose d'une expression explicite des vecteurs v_1, \dots, v_p comme combinaisons linéaires de $\tilde{v}_1, \dots, \tilde{v}_p$, alors : $E = \text{Vect}(v_1, \dots, v_p) \subseteq \text{Vect}(\tilde{v}_1, \dots, \tilde{v}_p)$ ce qui donne $E = \text{Vect}(\tilde{v}_1, \dots, \tilde{v}_p)$, puis $(\tilde{v}_1, \dots, \tilde{v}_p)$ engendre E et $\text{rg } \tilde{P} = p$, enfin $\tilde{\mathcal{B}}$ est une base de E et \tilde{P} est inversible.

On inverse \tilde{P} grâce au (c) de la proposition-définition précédente : $\tilde{P}^{-1} = \begin{pmatrix} v_1/\tilde{\mathcal{B}} & \dots & v_p/\tilde{\mathcal{B}} \\ \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] & \dots & \left[\begin{array}{c} \vdots \\ \vdots \end{array} \right] \end{pmatrix}.$

