Algèbre linéaire

Contents

1 Algèbres

K désigne un corps.

1.1 Définition

$(A, +, ., \times)$ est une K-algèbre si

1) $(A, +, .)$ est un K-espace vectoriel.
2) $(A, +, \times)$ est un anneau.
3) Si x et y sont des éléments de A et λ un scalaire :

$$\lambda . (xy) = x (\lambda . y) = (\lambda . x) y$$

1.2 Exemples

Soit K un corps ; exemples de K-algèbres :

1) K, $K[X]$.
2) $K^X = \mathcal{F}(X, K)$ pour la multiplication usuelle.
3) $M_n(K)$; $(L(E), +, \circ)$ si E est un K-espace vectoriel.

1.3 Sous-algèbres

B est une sous-algèbre de $(A, +, ., \times)$ si :

1) B est stable par combinaison linéaire.
2) B est stable par multiplication.
3) $1_A \in B$.

Conséquence

B est stable pour les 3 opérations, et constitue une algèbre pour les opérations induites.

Remarque

Pour montrer qu'un ensemble est une algèbre, on montre en général que c'est une sous-algèbre d'une algèbre connue.

1.4 Morphisme d'algèbres

Soit A et B deux K-algèbres ; $f : A \to B$ est un morphisme d'algèbres si

- f est une application linéaire
- et un morphisme d'anneaux.

Concrètement, on vérifie que :

1) f est une application linéaire.
2) f est un morphisme multiplicatif.
3) $f(1_A) = 1_B$.

2 Sous-espaces vectoriels

E désigne un $K-$espace vectoriel.

2.1 Définition d'un sous-espace vectoriel

2.1.1 Définition

F est un sous-espace vectoriel de E si

- F est non vide.
- F est stable par l'addition.
- F est stable par la multiplication par les scalaires.

2.1.2 Somme de deux vecteurs

Soit F un sous-espace vectoriel de E ; soit x et y des éléments de E.

Que dire de $x+y$ si les deux sont dans F, un seul des deux, aucun des deux ? Un dessin !

Réponse

- si $x \in F$ et $y \in F$, alors $x+y \in F$
- si $x \in F$ et $y \notin F$, alors $x+y \notin F$; en effet,

$$y = (x+y) - x$$

Si $x+y$ était dans F, y serait dans F.

- si $x \notin F$ et $y \notin F$, on ne peut pas conclure ; exemples : $x = y$ et $x = -y$.

2.2 Somme

2.2.1 Définition

Soit $F_1, ..., F_q$ des sous-espaces vectoriels de E ; soit

$$\begin{array}{cccc} f & : & F_1 \times ... \times F_q & \rightarrow & E \\ & & (x_1, ..., x_q) & \rightarrow & x_1 + ... + x_q \end{array}$$

L'image de f est notée $F_1 + ... + F_q$; on l'appelle somme de $F_1, ..., F_q$.

On montre facilement que f est une application linéaire, ce qui entraine que $F_1 + ... + F_q$ est un sous-espace vectoriel de E.

Exercice

Montrer que $F_1+...+F_q$ est le plus petit sous-espace vectoriel de E contenant $F_1 \cup ... \cup F_q$.

2.2.2 Image d'une somme

Exercice

Soit $u \in L(E,F)$ et E_1, E_2 deux sous-espaces de E.

- comparer $u(E_1 + E_2)$ et $u(E_1) + u(E_2)$.
- comparer $u(E_1 \cap E_2)$ et $u(E_1) \cap u(E_2)$.
- comparer $u(E_1 \cup E_2)$ et $u(E_1) \cup u(E_2)$.

Réponse

La linéarité ne sert que pour le premier.

$u(E_1 + E_2) = u(E_1) + u(E_2)$.

$u(E_1 \cap E_2) \subset u(E_1) \cap u(E_2)$.

$u(E_1 \cup E_2) = u(E_1) \cup u(E_2)$, mais en général ce ne sont pas des sous-espaces vectoriels.

2.3 Somme directe

2.3.1 Définition : somme directe

On dit que la somme $F_1+...+F_q$ est directe si f est injective, ou $\ker f = \{0\}$; ce qui signifie que tout vecteur de la somme se décompose de manière unique.

Dans ce cas, on la note

$$F_1 \oplus ... \oplus F_q$$

2.3.2 Supplémentaires

Soit $F_1, ..., F_q$ des sous-espaces vectoriels de E.

On dit qu'ils sont supplémentaires dans E s'ils sont en somme directe, et que leur somme est E.
Ils sont donc supplémentaires si et seulement si f est un isomorphisme.

2.3.3 Existence

Théorème

Si E est de dimension finie, tout sous-espace F possède un supplémentaire dans E.

Démonstration

Soit $(e_1, ..., e_p)$ une base de F, que l'on complète en une base $(e_1, ..., e_n)$ de E.

Alors $(e_{p+1}, ..., e_n)$ engendre un supplémentaire de F dans E.

2.3.4 Caractérisation

Exercice

La somme $F_1 + ... + F_q$ est directe si et seulement si pour tout j, $2 \leq j \leq q$,

$$(F_1 + ... + F_{j-1}) \cap F_j = \{0\}$$

Démonstration

Supposons que la somme n'est pas directe.

Soit $(x_1, ..., x_q)$ non nul tel que

$$\sum_{k=1}^{q} x_k = 0$$

Soit alors
$$j = \max \{k / 1 \leq k \leq q,\, x_k \neq 0\}$$
Alors $j \geq 2$, $x_j \neq 0$, et $\sum_{k=1}^{j} x_k = 0$, d'où

$$x_j = -\sum_{k=1}^{j-1} x_k$$

Donc
$$x_j \in (F_1 + ... + F_{j-1}) \cap F_j \setminus \{0\}$$
On a montré que si la somme n'est pas directe, alors il existe j tel que

$$(F_1 + ... + F_{j-1}) \cap F_j \neq \{0\}$$

La réciproque est plus facile.

2.3.5 Exemple

Que dire de trois droites distinctes dans un plan ?

Réponse

Elles ne sont pas en somme directe, mais en somme directe deux à deux.

2.4 Réunion

2.4.1 Cas de deux

Exercice

Soit F, G deux sous-espaces vectoriels de E.

Si $F \cup G$ est un sous-espace vectoriel de E, montrer que l'un des deux est contenu dans l'autre.

Démonstration

On montre la contraposée.

Supposons qu'aucun des deux n'est contenu dans l'autre.

Donc l'existence de $a \in F \setminus G$ et $b \in G \setminus F$; soit

$$c = a + b$$

On sait que dans ce cas c n'appartient ni à F ni à G.

Conclusion : $F \cup G$ n'est pas un sous-espace vectoriel de E.

2.4.2 Généralisation

Soit $F_1, ..., F_q$ des sous-espaces vectoriels de E. On suppose que leur réunion F est un sous-espace vectoriel de E.

Montrer que l'un des F_j contient tous les autres.

Démonstration

Par récurrence sur q ; le cas $q = 2$ est connu ; soit $q \geq 3$; supposons la propriété au rang $q - 1$.

Supposons donc $F = F_1 \cup ... \cup F_q$; si $F = F_1 \cup ... \cup F_{q-1}$, il suffit d'appliquer l'hypothèse de récurrence.

Sinon : il existe un

$$x \in F \setminus (F_1 \cup ... \cup F_{q-1})$$

Soit $y \in F$ non nul ; considérons les

$$y_t = x + ty$$

où t décrit K ; K étant infini :

- deux des y_t appartiennent au même F_j.
- x et y appartiennent à ce même F_j.
- $x \in F_j$, donc $j = q$; donc $y \in F_q$.

Conclusion, $F = F_q$.

3 Le théorème du rang

3.1 Dimension de $F \times G$

Théorème

Si E est un $K-$espace vectoriel de dimension p et F un $K-$espace vectoriel de dimension q, $E \times F$ est un $K-$espace vectoriel de dimension $p + q$.

Démonstration

Soit $(e_1, e_2, ...e_p)$ une base de E et $(f_1, ..., f_q)$ une base de F ; on montre aisément que

$$((e_1, 0), ..., (e_p, 0), (0, f_1), ..., (0, f_q))$$

constitue une base de $E \times F$.

3.2 Dimension de $F \oplus G$

Théorème

Si F et G sont deux sous-espaces vectoriels de E en somme directe, alors

$$\dim F \oplus G = \dim F + \dim G$$

Démonstration

Il existe un isomorphisme de $F \times G$ sur $F \oplus G$:

$$(x, y) \to x + y$$

3.3 Théorème du rang

3.3.1 Théorème de l'isomorphisme induit

Si $u \in L(E, F)$ et si E' est un supplémentaire de $\ker u$ dans E :

$$E = \ker u \oplus E'$$

Alors u induit un isomorphisme u' de E' sur $\mathrm{Im} u$.

Démonstration

Il est clair que u' est une application linéaire.

Son noyau est $E' \cap \ker u = \{0\}$, donc u' est injective.

Soit $y = u(x)$ un élément de $\mathrm{Im} u$; on écrit

$$x = x_1 + x_2$$

avec $x_1 \in E'$ et $x_2 \in \ker u$. Alors

$$y = u'(x_1)$$

Ce qui montre que u' est surjectif.

3.3.2 Théorème du rang

Si E est de dimension finie, et si $u \in L(E, F)$, alors

$$\dim\ E = \dim(\ker u) + \mathrm{rg}\, u$$

Démonstration

E étant de dimension finie, on sait que $\ker u$ possède un supplémentaire E' dans E.

On peut donc utiliser l'isomorphisme induit : u' étant un isomorphisme, E' et $\mathrm{Im} u$ ont même dimension ; donc :

$$\dim E - \dim \ker u = \dim E' = \mathrm{rg} u$$

3.4 Dimension de $F + G$

Théorème (formule de Grassmann)

Soit F et G des sous-espaces vectoriels de dimensions finies de E. Alors :

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

Démonstration 1

On définit

$$f : \begin{cases} F \times G \to F + G \\ (x, y) \to x + y \end{cases}$$

Que dire de $\ker f$?

Réponse

$i : x \to (x, -x)$ est un isomorphisme de $F \cap G$ sur $\ker f$. D'où

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

Démonstration 2

Soit F_1 un supplémentaire de $F \cap G$ dans F : $F = F_1 \oplus (F \cap G)$; on vérifie que

$$F + G = F_1 \oplus G$$

On en déduit

$$\dim (F + G) = \dim (F_1) + \dim (G) = \dim F + \dim G - \dim (F \cap G)$$

3.5 Dimension d'une somme directe

Théorème

Soit $F_1, ..., F_q$ des sous-espaces vectoriels de dimension finie de E ; dans ce cas :

$$\dim \sum_{j=1}^{q} F_j \leq \sum_{j=1}^{q} \dim F_j$$

et il y a égalité si et seulement si la somme est directe.

Démonstration

On applique le théorème du rang à l'application :

$$\begin{array}{cccc} f & : & F_1 \times ... \times F_q & \to & F_1 + ... + F_q \\ & & (x_1, ..., x_q) & \to & x_1 + ... + x_q \end{array}$$

3.6 Exercices

Soit $u, v \in L(E, F)$ et E' un sous-espace vectoriel de E. On suppose E de dimension finie. Montrer que :

- $\dim u(E') \leq \dim E'$
- $rg(u + v) \leq rg(u) + rg(v)$

Soit $v \in L(E, F)$ et $u \in L(F, G)$. On suppose E et F de dimensions finies. Montrer que :

- $rg(u \circ v) \leq rg(u)$
- $rg(u \circ v) \leq rg(v)$

Démonstration

- On applique le théorème du rang à $u' = u_{/F}$.
- $\mathrm{Im}(u + v) \subset \mathrm{Im}u + \mathrm{Im}v$.
- $\mathrm{Im}(u \circ v) \subset \mathrm{Im}u$.
- $\mathrm{Im}(u \circ v) = u(\mathrm{Im}v)$

3.7 Les noyaux itérés

Exercice important

Soit $u \in L(E)$; on note $u^0 = \mathrm{Id}$, $F_k = \ker u^k$ et $G_k = \mathrm{Im}u^k$ pour $k \geq 0$.

a) Montrer que $(F_k)_{k \geq 0}$ est croissante et $(G_k)_{k \geq 0}$ décroissante.

b) Montrer que si $k \geq 0$ et $F_k = F_{k+1}$, alors $F_{k+1} = F_{k+2}$.

On suppose que E est de dimension finie n ; soit $a_k = \dim F_k$.

c) Montrer que $a_n = a_{n+1}$.

d) Montrer que $(a_{k+1} - a_k)$ est décroissante ; on pourra utiliser la restriction de u^k à F_{k+1}.

e) Montrer que $(F_k)_{k\geq 0}$ et $(G_k)_{k\geq 0}$ sont stationnaires à partir du même rang.

On ne suppose plus E de dimension finie.

f) Trouver un exemple où $(G_k)_{k\geq 0}$ est stationnaire, mais pas $(F_k)_{k\geq 0}$.

g) Soit $E = \mathbb{R}[X]$; $u(P) = P'$; montrer qu'il n'existe pas de $v \in \mathcal{L}(E)$ tel que $u = v^2$.

h) Montrer que si $(F_k)_{k\geq 0}$ et $(G_k)_{k\geq 0}$ sont stationnaires, elles le sont à partir du même rang (plus difficile).

Démonstration de b)

Soit $x \in F_{k+2}$; $u^{k+2}(x) = u^{k+1}(u(x)) = 0$; donc $u(x) \in F_{k+1} = F_k$; donc

$$u^k(u(x)) = 0$$

Finalement

$$x \in F_{k+1}$$

Démonstration de c)

Si par l'absurde $a_n < a_{n+1}$, alors $0 = a_0 < a_1 < ... < a_n < a_{n+1}$.

Donc, par récurrence sur k, pour $0 \leq k \leq n+1$: $a_k \geq k$; en particulier

$$a_{n+1} \geq n+1$$

Contradiction ; donc $a_n = a_{n+1}$.

Autre démonstration de c)

Si $u^n(x) \neq 0$ et $u^{n+1}(x) = 0$, on montre que la famille

$$(x, u(x), ..., u^n(x))$$

est libre.

Démonstration de d)

Avec le théorème du rang :

$$a_{k+1} - a_k = \dim u^k(F_{k+1}) = \dim\left(\mathrm{Im} u^k \cap \ker u\right)$$

Démonstration de f)

$E = \mathbb{R}[X]$; $u(P) = P'$.

Démonstration de g)

Si v existe, $\ker v \subset \ker u$ qui est de dimension 1.

- si $\ker v = (0)$, v est injectif, u aussi, contradiction.
- si $\ker v = \ker u = \ker v^2$, on utilise b) : la suite $\left(\ker v^k\right)$ est stationnaire, contradiction.

4 Interpolation de Lagrange

On fixe $n \geq 0$ et $a_0, ..., a_n \in K$, distincts.

4.1 Un isomorphisme

$$f : \left\{ \begin{array}{c} K_n[X] \to K^{n+1} \\ P \to (P(a_0), ..., P(a_n)) \end{array} \right.$$

Attention

$K_n[X]$ est de dimension $n+1$, donc $n+1$ points.

4.2 Une base adaptée

On cherche les antécédents des éléments de la base canonique. Soit

$$N = \prod_{j=0}^{n} (X - a_j)$$

et

$$N_j = \frac{N}{X - a_j} = \prod_{k \neq j} (X - a_k)$$

Exemple

$n = 2$; $N = (X - a_0)(X - a_1)(X - a_2)$; $N_0 = (X - a_1)(X - a_2)$; $N_1 = (X - a_0)(X - a_2)$; $N_2 = ...$

Que dire de $f(N_j)$?

On note

$$L_j = \frac{N_j}{N_j(a_j)}$$

Images des L_j par f

$L_j(a_i) = \delta_{i,j}$; par exemple, $f(L_0) = (1, 0..., 0)$, $f(L_1) = (0, 1, 0, ..., 0)$ ...

En résumé, l'image de $(L_0, ..., L_n)$ est la base canonique de K^{n+1}.

4.3 Remarque

$N_j(a_j) = N'(a_j)$, donc

$$L_j = \frac{N_j}{N'(a_j)} = \frac{N}{N'(a_j)(X - a_j)}$$

Démonstration

$N = (X - a_j).N_j$; on dérive, et on évalue en a_j.

4.4 Expression d'un polynôme dans cette base

$$\forall P \in K_n[X], \; P = \sum_{j=0}^{n} P(a_j) L_j$$

Démonstration

On écrit

$$P = \sum_{k=0}^{n} \lambda_k L_k$$

et on évalue en chaque a_j.

Ou on constate que la différence est un polynôme de degré au plus n, qui a au moins $n+1$ racines.

Au fait, pourquoi est-ce une base ?

On peut répondre que c'est l'image de la base canonique de K^{n+1} par un isomorphisme ; ou constater que la formule précédente prouve qu'elle est génératrice, de cardinal $n+1$.

On peut aussi montrer directement qu'elle est libre.

5 Matrices équivalentes

5.1 Rang d'une matrice

Soit $A \in M_{p,q}(K)$; les colonnes de A sont des éléments de $M_{p,1}(K)$. Notons $C = (C_1, ..., C_q)$ la famille des colonnes de A.

On appelle rang de A le rang de cette famille :

$$\mathrm{rg} A = \mathrm{rg}(C_1, ..., C_q)$$

Exercice : matrices de rang 1

Toute matrice M de rang 1 s'écrit

$$M = X.Y^T$$

où X et Y sont des colonnes non nulles.

Démonstration

Les colonnes M_j de M sont proportionnelles à une colonne X :

$$M_j = y_j.X$$

Donc $m_{i,j} = x_i.y_j$; donc

$$M = X.Y^T$$

5.2 Définition : matrices équivalentes

On dit que M et M' éléments de $M_{p,q}(K)$ sont équivalentes si

$$\exists P \in GL_p(K), \exists Q \in GL_q(K), M' = P.M.Q$$

5.3 Théorème

On suppose E et F de dimensions finies ; soit $u \in L(E, F)$ de rang r.

Alors il existe une base e de E et une base f de F telles que

$$M_{e,f}(u) = J_r = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \in M_{p,q}(K)$$

Démonstration

Voir isomorphisme induit...

Soit $(e_1, ..., e_r)$ une base de E' ; $(f_1, ..., f_r)$ leurs images ; $(e_{r+1}, ..., e_q)$ une base de $\ker u$...

5.4 Caractérisation

Dans $M_{p,q}(K)$, A et B sont équivalentes si et seulement si elles ont le même rang.

A est équivalente à J_r si et seulement A est de rang r.

5.5 Transposée

Théorème

Une matrice et sa transposée ont le même rang.

Démonstration

Si $A = P.J_r.Q$, alors $A^T = Q^T.J_r.P^T$; attention, ce n'est pas le même J_r.

5.6 Caractérisation du rang

5.6.1 Lemme

Soit $A \in M_{p,q}(K)$, et r son rang.

Le rang r' d'une matrice extraite A' vérifie $r' \leq r$.

Démonstration

Si A' est obtenue en supprimant des colonnes dans A, $C' \subset C$; donc

$$\text{Vect}(C') \subset \text{Vect}(C)$$

Donc $r' \leq r$. Si on supprime aussi des lignes ?

5.6.2 Théorème

Soit $A \in M_{p,q}(K)$, et r son rang.

r est la taille maximale d'une matrice carrée extraite inversible.

Démonstration

La famille des colonnes de A, $C = (C_1, ..., C_q)$ est de rang r ; il existe donc une sous-famille libre de cardinal r ; on obtient ainsi une matrice

$$A_1 \in M_{p,r}(K)$$

de rang r.

La famille des lignes de A_1 est aussi de rang r ; elle possède donc une sous-famille libre de cardinal r ; on obtient ainsi une matrice

$$A_2 \in GL_r(K)$$

5.7 Applications

5.7.1 Exercice 1 : l'inverse faible

Soit $A \in M_{p,q}(K)$; montrer l'existence de $B \in M_{q,p}(K)$ vérifiant $ABA = A$ et $BAB = B$.

5.7.2 Exercice 2

Soit E un espace vectoriel de dimension finie ; soit $u \in L(E)$; montrer l'existence de $v \in GL(E)$ tel que $v \circ u$ soit un projecteur.

5.7.3 Réponses

Si $A = P.J_r.Q$, il suffit de choisir $B = Q^{-1}.J_r.P^{-1}$; si $M_B(u) = P.J_r.Q$, il suffit de choisir

$$M_B(v) = Q^{-1}P^{-1}$$

6 Déterminants

6.1 Déterminant triangulaire par blocs

Théorème

Soit $M = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$ une matrice triangulaire par blocs ; on suppose A et C carrées ; alors

$$\det M = \det A . \det C$$

Démonstration

$$M=\left[\begin{array}{cc} A & B \\ 0 & C \end{array}\right]=\left[\begin{array}{cc} I_r & 0 \\ 0 & C \end{array}\right]\cdot\left[\begin{array}{cc} I_r & B \\ 0 & I_s \end{array}\right]\cdot\left[\begin{array}{cc} A & 0 \\ 0 & I_s \end{array}\right]$$

6.2 Déterminant de Vandermonde

6.2.1 Il est non nul

Soit $n \geq 1$ et $a_0, ..., a_n \in K$, distincts ; le déterminant suivant est non nul :
$$\left|\begin{array}{cccc} 1 & a_0 & . & a_0^n \\ . & & & . \\ . & & & . \\ 1 & a_n & . & a_n^n \end{array}\right|$$

Démonstration

Soit $C=\sum_{k=0}^n \lambda_k C_k$ une combinaison linéaire des colonnes ; soit

$$P=\sum_{k=0}^n \lambda_k X^k$$

Si $C=0$, que dire de P ?

Réponse

Si $C=0$, P possède $n+1$ racines, les a_k ; étant de degré au plus n, il est nul ; donc les λ_k sont nuls.

On a montré que la famille des colonnes $(C_0, ..., C_n)$ est libre, ce qui prouve que le déterminant est non nul.

6.2.2 La valeur exacte

Théorème

On montre qu'il vaut
$$\prod_{i<j}(a_j-a_i)$$

Démonstration

C'est clair si $a_0, ..., a_n$ ne sont pas distincts. On les suppose donc distincts et on procède par récurrence sur n.

Le résultat est évident pour $n=1$; soit $n \geq 2$; supposons la propriété vérifiée au rang $n-1$; on remplace dans le déterminant a_n par X ; on obtient un polynôme $P \in K_n[X]$ dont on connaît n racines distinctes $a_0, ..., a_{n-1}$; de plus, le coefficient de X^n dans P est donné par l'hypothèse de récurrence.

6.2.3 Une application

Exercice

Soit $n \geq 1$ et $\lambda_1, ..., \lambda_n$ n complexes ; on suppose que

$$\forall k, 1 \leq k \leq n, \sum_{j=1}^n \lambda_j^k=0$$

Montrer que les λ_j sont nuls.

Démonstration

Supposons par l'absurde qu'ils ne sont pas tous nuls ; on peut supprimer ceux qui sont nuls, regrouper ensemble les λ_j qui sont identiques, les réindexer, et on obtient :

$$\forall k, 1 \leq k \leq q, \sum_{j=1}^{q} n_j.\lambda_j^k = 0$$

où q est le nombre de λ_j non nuls distincts, et n_j le nombre de fois que la suite de départ $\lambda_1, ..., \lambda_n$ contient λ_j.

Le vecteur $(n_1, ..., n_q)$ est donc solution d'un système linéaire homogène, dont le déterminant est non nul, car $\lambda_1, ..., \lambda_q$ sont distincts ; donc

$$(n_1, ..., n_q) = 0$$

Or les n_j sont des entiers non nuls, contradiction ; conclusion, tous les λ_j sont nuls.

7 Comatrice

7.1 Définition

Soit $A \in M_n(K)$; on note $D_{i,j}$ le déterminant de la matrice obtenue à partir de A en supprimant la ligne i et la colonne j ; la comatrice de A est

$$\left((-1)^{i+j}.D_{i,j}\right)$$

7.2 Comatrice et inverse

Théorème

Pour tout $A \in M_n(K)$:

$${}^t\mathrm{Com}(A).A = A.{}^t\mathrm{Com}(A) = \det(A).I_n$$

Si de plus A est inversible

$$A^{-1} = \frac{1}{\det A}.{}^t\mathrm{Com}A$$

Exemple

Soit $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$; si $\det A$ est non nul, $A^{-1} = ?$

$$A^{-1} = \frac{1}{ad - bc}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix}$$

7.3 Exercice : les inversibles de $M_n(\mathbb{Z})$

Soit $A \in M_n(\mathbb{Z})$.

Montrer que A est inversible et $A^{-1} \in M_n(\mathbb{Z})$ si et seulement si $\det A = \pm 1$.

Démonstration

Supposons $A^{-1} \in M_n(\mathbb{Z})$.

Alors $A.A^{-1} = I_n$; donc $\det A.\det A^{-1} = 1$; c'est le produit de deux entiers, donc $\det A = \pm 1$.

Supposons $\det A = \pm 1$.

$A \in M_n(\mathbb{Z})$, donc $\mathrm{Com}A \in M_n(\mathbb{Z})$; donc $A^{-1} \in M_n(\mathbb{Z})$.

7.4 Exercice : rang de la comatrice

Soit $A \in M_n(K)$; soit r son rang, et r' le rang de Com$A$.

- cas où $r = n$: $r' = n$.
- cas où $r \leq n-2$: Com$A = 0$.
- cas où $r = n-1$. ${}^t\mathrm{Com}(A).A = \det(A).I_n = 0$, donc l'image de A est contenue dans le noyau de ${}^t\mathrm{Com}(A)$; donc $r' \leq 1$; de plus, $\mathrm{Com}(A)$ n'est pas nulle, donc

$$r' = 1$$

8 Hyperplans

8.1 Définitions

$E^* = L(E, K)$: l'ensemble des formes linéaires.

Hyperplan

Un hyperplan H est le noyau d'une forme linéaire non nulle φ.

On dit alors que φ est une équation de H.

8.2 Caractérisation

Tout supplémentaire d'une droite est un hyperplan ; si E est de dimension finie n, les hyperplans sont les sous-espaces de dimension $n-1$.

8.3 Equations d'un hyperplan

8.3.1 Théorème

Elles sont proportionnelles.

Démonstration

Soit f et g deux éléments de $E^* - \{0\}$; supposons $H = \ker f = \ker g$ et montrons que (f, g) est liée.

Soit $a \in E \setminus H$; soit

$$\lambda = \frac{g(a)}{f(a)}$$

La formule

$$g = \lambda.f$$

est vérifiée sur H et au point a, donc sur E par linéarité ; en détail :

Soit $x \in E$.

$$\exists t \in K, \exists h \in H, x = h + t.a$$

Alors :

$$g(x) = g(h + t.a) = t.g(a) = t.\lambda.f(a) = \lambda.f(x)$$

8.3.2 Autre formulation

Soit f et g deux éléments de E^* ; si $\ker f \subset \ker g$, alors

$$\exists \lambda \in K, g = \lambda.f$$

8.3.3 Cas de K^n

Si $E = K^n$, les formes linéaires sont de la forme

$$\varphi : (x_1, x_2, ...x_n) \to \sum_{j=1}^{n} a_j x_j = A^T.X$$

Démonstration

$$\varphi(x_1, x_2, ...x_n) = \varphi\left(\sum_{j=1}^{n} x_j e_j\right) = \sum_{j=1}^{n} a_j x_j$$

où $(e_1, e_2, ...e_n)$ est ?

8.4 Généralisation

Exercice

Soit $q \geq 1$; soit $f, f_1, ..., f_q$ des formes linéaires sur E ; on suppose que

$$\bigcap_{j=1}^{q} \ker f_j \subset \ker f$$

Montrer que f est combinaison linéaire des f_j.

Démonstration 1

Par récurrence sur q ; le cas $q = 1$ est connu ; soit $q \geq 1$; supposons la propriété au rang q. On part de

$$\bigcap_{j=1}^{q+1} \ker f_j \subset \ker f$$

Soit

$$E' = \bigcap_{j=1}^{q} \ker f_j$$

On examine les restrictions sur E' :

$$\ker f'_{q+1} \subset \ker f'$$

D'après le cas $q = 1$:

$$f' = \lambda_{q+1} f'_{q+1}$$

Donc

$$E' \subset \ker(f - \lambda_{q+1} f_{q+1})$$

Donc, d'après l'hypothèse de récurrence :
$f - \lambda_{q+1} f_{q+1}$ est combinaison linéaire des $(f_j)_{1 \leq j \leq q}$.

Démonstration 2

C'est une conséquence directe de l'exercice 2 de factorisation, qui s'applique avec $F = K^q$.

8.5 Intersection d'hyperplans

8.5.1 Théorème

Si E est un espace de dimension finie n, l'intersection de m hyperplans est de dimension au moins $n - m$.

Démonstration

$$\begin{array}{cccc} f & : & E & \rightarrow & K^m \\ & & x & \rightarrow & (\varphi_1(x), ..., \varphi_m(x)) \end{array}$$

8.5.2 Exercice

Si E est un espace de dimension finie n, l'intersection de m hyperplans d'équations $\varphi_1, ..., \varphi_m$ est de dimension $n - r$, avec

$$r = \mathrm{rg}\,(\varphi_1, ..., \varphi_m)$$

Démonstration

Il suffit d'étudier le cas où $(\varphi_1, ..., \varphi_m)$ est libre, et de montrer que dans ce cas f est surjective.

Par contraposée : si f n'est pas surjective, $\mathrm{Im} f$ est contenu dans un hyperplan de K^m :

Il existe $a = (a_1, ..., a_m)$ non nul tel que

$$\forall x \in E, \sum_{j=1}^{m} a_j.\varphi_j\,(x) = 0$$

ce qui montre que $(\varphi_1, ..., \varphi_m)$ est liée.

9 Complément : l'opérateur Δ

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

$E = K\,[X]$; on définit Δ par

$$\Delta P = P\,(X+1) - P\,(X)$$

9.1 Noyau

$\ker \Delta = K_0\,[X]$; quel est le degré de ΔP ? Son terme dominant ?

Réponse

Si $\Delta P = 0$, alors $P\,(X) - P\,(0)$ a une infinité de racines (les entiers naturels), donc

$$P = P\,(0)$$

Si $P = a_n X^n + ...$, alors

$$\Delta P = n.a_n X^{n-1} + ...$$

Remarque

Si par exemple $K = \mathbb{Z}/p\mathbb{Z}$ (avec p premier), c'est très différent.

Un exemple d'élément du noyau non constant ?

Réponse

$$X^p - X = X\,(X-1)\,(X-2)\,...\,(X-p+1)$$

9.2 Δ est surjectif

Démonstration

Pour $n \geq 1$, on introduit

$$\Delta_n : K_n\,[X] \to K_{n-1}\,[X]$$

restriction de Δ ; Δ_n est surjectif d'après le théorème du rang ; comment en déduire que Δ est surjectif ?

9.3 Un exemple d'isomorphisme induit

Un supplémentaire de $\ker\Delta$?

Réponse

Par exemple,

$$E' = \{P \in E / P(0) = 0\} = \text{Vect}\left(X^k\right)_{k \in \mathbb{N}^*}$$

D'où un isomorphisme Δ' induit par Δ de E' sur E.

9.4 Une base adaptée : les polynômes de Hilbert

On les définit par $H_0 = 1$, et $H_n = (\Delta')^{-1}(H_{n-1})$; pour $n \geq 1$, H_n est donc caractérisé par

$$\Delta(H_n) = H_{n-1},\ H_n(0) = 0$$

On en déduit facilement que $0, 1, ..., n-1$ sont racines de H_n ; finalement :

$$H_n = \frac{X(X-1)...(X-n+1)}{n!} = \left(\begin{array}{c} X \\ n \end{array}\right)$$

Soit Δ_n l'endomorphisme induit par Δ sur $K_n[X]$.

Quelle est sa matrice dans la base $(H_0, ..., H_n)$?

Réponse

$$M = \left[\begin{array}{ccccc} 0 & 1 & & . & 0 \\ & 0 & 1 & & . \\ & & & . & \\ . & & & . & 1 \\ 0 & . & & & 0 \end{array}\right]$$

Quelle base choisir pour que cette matrice soit celle de $D : P \to P'$?

Réponse

$$\left(\frac{X^k}{k!}\right)_{0 \leq k \leq n}$$

9.5 Calcul de Δ^n

$$\forall P \in E,\ \Delta^n P = \sum_{k=0}^{n} (-1)^{n-k} \left(\begin{array}{c} n \\ k \end{array}\right) P(X+k)$$

Démonstration

$\Delta = T - \text{Id}$, les deux commutent, on applique la formule du binôme.

9.6 Exercice

Soit $P_n = \sum_{k=0}^{n} (-1)^{n-k} H_k$; exprimer P_n en fonction de H_n.

Réponse

$(I + \Delta) P_n = H_n$; d'où $P_n = T^{-1} H_n = H_n(X-1)$.

9.7 Exercice

Montrer que $\forall n \geq 0, H_n(\mathbb{Z}) \subset \mathbb{Z}$.

Réciproquement, soit

$$P = \sum_{k=0}^{n} a_k H_k$$

Montrer que si $P(\mathbb{Z}) \subset \mathbb{Z}$, les a_k sont dans $\mathbb{Z}$.

Réponse

Si $P(\mathbb{Z}) \subset \mathbb{Z}$, d'abord $a_0 \in \mathbb{Z}$; ensuite, $(\Delta P)(\mathbb{Z}) \subset \mathbb{Z}$...

10 Complément : factorisation des endomorphismes

On suppose que E, F et G sont de dimensions finies.

10.1 Exercice 1

Soit $v \in L(F, G)$ et $w \in L(E, G)$; trouver une condition nécessaire pour qu'existe $u \in L(E, F)$ tel que

$$w = v \circ u$$

Montrer que cette condition est suffisante.

Réponse

$\mathrm{Im} w \subset \mathrm{Im} v$ est une condition nécessaire.

Réciproque : soit $(e_1, e_2, ...e_n)$ une base de E ; pour tout j, $w(e_j) \in \mathrm{Im} w \subset \mathrm{Im} v$; on peut donc choisir un antécédent f_j dans F de $w(e_j)$ par v :

$$v(f_j) = w(e_j)$$

Ensuite, on définit u par

$$\forall j, u(e_j) = f_j$$

Alors :

$$\forall j, w(e_j) = v(f_j) = v \circ u(e_j)$$

10.2 Exercice 2

Soit $u \in L(E, F)$ et $w \in L(E, G)$; trouver une condition nécessaire pour qu'existe $v \in L(F, G)$ tel que

$$w = v \circ u$$

Montrer que cette condition est suffisante.

Réponse

$\ker u \subset \ker w$ est une condition nécessaire.

Réciproque : soit $(f_1, f_2, ...f_n)$ une base de $\mathrm{Im} u$; chaque f_j a un antécédent e_j par u ; on définit v par

$$\forall j, v(f_j) = w(e_j)$$

Alors :

$$\forall j, w(e_j) = v \circ u(e_j)$$

Où sert l'hypothèse $\ker u \subset \ker w$?

Enfin, v n'étant définie que sur $\mathrm{Im} u$, il reste à la définir sur F.

Variante

Définir v sur $\mathrm{Im} u$ par $w \circ u_1^{-1}$, où u_1 est un isomorphisme induit.

Remarque

Dans cet exercice, on n'a utilisé que la dimension finie de F.

11 Complément : le résultant

Dans $K[X]$, soit

$$P = u_0 + ... + u_p X^p,\ Q = v_0 + ... + v_q X^q$$

On suppose $p \geq 1$, $q \geq 1$, $u_p \neq 0$, $v_q \neq 0$.

11.1 Lemme 1

Montrer que $P \wedge Q \neq 1$ si et seulement si il existe deux polynômes non nuls A et B tels que

$$AP = BQ,\ \deg A < q,\ \deg B < p$$

Démonstration

Supposons $D = P \wedge Q \neq 1$; écrivons $P = D.P_1$ et $Q = D.Q_1$; alors

$$D.P_1.Q_1 = Q_1.P = P_1.Q$$

Donc $A = Q_1$ et $B = P_1$ conviennent.

Pour la réciproque, on utilise le théorème de Gauss.

11.2 Lemme 2

Montrer que $P \wedge Q \neq 1$ si et seulement si

$$\left(P, XP, ...X^{q-1}P, Q, XQ, ..., X^{p-1}Q\right)$$

est liée.

On appelle résultant le déterminant suivant, de taille $p+q$:

$$Res\,(P,Q) = \begin{vmatrix} u_0 & . & . & u_p & & & \\ & . & & & . & & \\ & & u_0 & & . & . & u_p \\ v_0 & . & . & v_q & & & \\ & . & & & . & & \\ & & v_0 & & & & v_q \end{vmatrix}$$

Les $p+q$ lignes correspondent aux vecteurs de la famille $\left(P, XP, ...X^{q-1}P, Q, XQ, ..., X^{p-1}Q\right)$.

On en déduit que

$$P \wedge Q \neq 1 \Longleftrightarrow Res\,(P,Q) = 0$$

11.3 Degré 2

Soit $P = aX^2 + bX + c \in \mathbb{C}[X]$; on suppose $a \neq 0$; calculer $Res\,(P, P')$.

Réponse

$$\begin{vmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{vmatrix} = -a\left(b^2 - 4ac\right)$$

11.4 Degré 3

Soit $P = X^3 + pX + q \in \mathbb{C}[X]$; calculer $Res\,(P, P')$.

Réponse

$4p^3 + 27q^2$.

11.5 Le même par une méthode élémentaire

$$P = X^3 + pX + q \in \mathbb{C}[X]$$

On veut savoir à quelle condition P a une racine multiple.

Réponse

On calcule le reste R de la division euclidienne de P par P' :

$$R = \frac{2}{3}pX + q$$

D'où $\alpha = -\frac{3q}{2p}$; on retrouve que $P'(\alpha) = 0$ si et seulement si $4p^3 + 27q^2 = 0$.

11.6 Un ouvert de $\mathbb{C}_n[X]$

Soit U l'ensemble des polynômes de degré n ($n \geq 1$), scindés à racines simples.

Montrer que U est un ouvert de $\mathbb{C}_n[X]$.

Remarque : l'ensemble des polynômes scindés à racines simples de $\mathbb{C}_n[X]$ n'est pas un ouvert de $\mathbb{C}_n[X]$: utiliser $Q_k = X\left(\frac{X}{k} - 1\right)^2$.

Démonstration

$P \to Res(P, P')$ est une fonction polynomiale sur $\mathbb{C}_n[X]$, donc continue ; U est l'image réciproque d'un ouvert de $\mathbb{C}$: $\mathbb{C}^*$.

12 Complément : $SL_n(K)$ et les transvections

E désigne un $K-$espace vectoriel de dimension n.

12.1 Transvections

On dit qu'un élément u de $L(E)$ est une transvection si

- $\det u = 1$
- l'ensemble des vecteurs invariants est de dimension $n-1$.

Matrice d'une tranvection

$$\begin{bmatrix} I_{n-1} & C \\ 0 & 1 \end{bmatrix}$$

où C est une colonne non nulle.

On en déduit que

$$(u - \mathrm{Id})^2 = 0$$

Donc

$$D \subset H$$

où $D = \mathrm{Im}(u - \mathrm{Id})$ et $H = \mathrm{Ker}(u - \mathrm{Id})$.

12.2 Réduction

Soit u une transvection. Il existe une base B telle que

$$M_B(u) = I_n + E_{2,1}$$

Démonstration

Choisir une base e_2 de D.

12.3 $T_{i,j}(\lambda)$

Pour $i \neq j$ et $\lambda \in K^*$, on note

$$T_{i,j}(\lambda) = I_n + \lambda.E_{i,j}$$

Inverse ?

$$T_{i,j}(\lambda)^{-1} = I_n - \lambda.E_{i,j} = T_{i,j}(-\lambda)$$

12.4 Opérations élémentaires

Soit $M \in M_n(K)$.

Que dire de $T_{i,j}(\lambda).M$? $M.T_{i,j}(\lambda)$?

Réponse

$T_{i,j}(\lambda).M$ est obtenue par l'opération

$$L_i \leftarrow L_i + \lambda.L_j$$

$M.T_{i,j}(\lambda)$ est obtenue par l'opération

$$C_j \leftarrow C_j + \lambda.C_i$$

12.5 $SL_n(K)$ est engendré par l'ensemble des $T_{i,j}(\lambda)$

Démonstration

Soit $M \in SL_n(K)$. On multiplie à gauche M par des $T_{i,j}(\lambda)$ pour obtenir successivement :

- un des $m_{i,1}$ non nul, avec $i \geq 2$.
- $m_{1,1} = 1$.
- la première colonne de M égale à celle de I_n.

Par récurrence sur n, on obtient une matrice triangulaire supérieure.

Enfin, on arrive à I_n.

12.6 $SL_n(\mathbb{R})$ est connexe par arcs