LES NOUVEAUX

Précis

BRÉAL

Mathématiques

Algèbre et géométrie

MP

Cours

Méthodes

Exercices résolus

D. GUININ • B. JOPPIN

Nouveau programme

Bréal
L'ÉDITEUR DES PRÉPAS

Reproduction interdite © Bréal

Copyrighted material

LES NOUVEAUX

Précis

BRÉAL

Algèbre et géométrie

MP

Daniel GUININ

Professeur en classes préparatoires scientifiques - 2e année

Bernard JOPPIN

Professeur en classes préparatoires scientifiques - 1re année

1, rue de Rome - 93561 Rosny-sous-Bois cedex

Bréal éditions

Copyrighted material

LES NOUVEAUX

Précis

BRÉAL

Titres disponibles dans la filière MP

Mathématiques 2e année

- Analyse MP
- Algèbre et géométrie MP

Physique 2e année

- Mécanique MP - PC
- Électromagnétisme MP
- Électronique MP - PT
- Optique MP - PC - PSI - PT
- Thermodynamique MP

Chimie 2e année

- Chimie MP - PT

Exercices 2e année

- Mathématiques MP
- Physique MP

Maquette : Insolencre & 16 iS.
Couverture : Sophie Martinet.
Réalisation : 16 iS.

© Bréal 2004
Toute reproduction même partielle interdite.
Dépôt légal : août 2004.
ISBN 2 7495 0388 4

Copyrighted material

Cet ouvrage est conforme aux **nouveaux programmes** mis en place à la rentrée 2004.

Les Nouveaux Précis Bréal sont le reflet d'une évolution des habitudes de travail des étudiants en prépas scientifiques MP ou MP*.

Rigueur, méthode et clarté sont sans doute les leitmotivs de cette évolution. La mise en page et l'apport de couleur accompagnent, en la soulignant, la structure du contenu divisé en trois parties complémentaires :

- Le **Cours** est composé des définitions, théorèmes et propriétés nécessaires et suffisants. L'objectif est clair : tout le programme, rien que le programme. Tous les théorèmes, ainsi que les principales propriétés, sont démontrés en détail. Parfois, une démonstration simple à établir pourra faire l'objet d'un premier exercice d'application stimulant.

- Les **Méthodes** constituent la principale innovation des Nouveaux Précis. Étudiants et professeurs savent combien le plus délicat, lorsque l'on aborde un problème, est souvent la phase de démarrage : *par quel bout le prendre ?* Deux temps composent cette nouvelle rubrique.

  L'essentiel explicite, en une fiche de synthèse, les démarches les plus courantes. Des mises en œuvre illustrent ces démarches par des exercices classiques, voire «incontournables».

  De (rares) chapitres sont essentiellement composés de méthodes et ne comportent alors pas cette rubrique.

- Les **Exercices**, beaucoup plus nombreux que dans les éditions précédentes, sont classés selon leur degré de difficulté : du niveau 1, qui correspond à des exercices souvent proches du cours, au niveau 3, moins «transparents». Le niveau 2 propose des sujets de colles raisonnables. Dans tous les cas, ces exercices sont calibrés en fonction de ce que l'on peut véritablement attendre d'un étudiant en vue de la préparation immédiate des concours. Les indications apportent, comme c'est souvent le cas en colle, un coup de pouce qui peut être bienvenu lorsque l'on travaillle seul.

  Tous les exercices ont une solution, détaillée ou plus succincte.

Il nous a paru indispensable d'accorder à ces deux dernières parties, les Méthodes et les Exercices, une place importante, équivalente à celle du Cours, au fil des huit chapitres que comporte ce tome consacré à l'algèbre et à la géométrie.

Cet équilibre permettra aux étudiants de MP et MP* de disposer d'un outil de travail complet, adapté au rythme progressif et soutenu de la préparation aux concours.

Les auteurs

This One
WZF4-F19-BOUP

Copyrighted material

Sommaire

Sommaire

Copyrighted material

CHAPITRE

1

Groupes (compléments) Congruences Anneau $\mathbb{Z}/n\mathbb{Z}$ Arithmétique

A. Groupes, sous-groupes, morphismes

1. Groupes

Définition 1

Soit G un ensemble non vide muni d'une loi de composition interne notée $*$. (1)
On dit que $(G, *)$ est un groupe lorsque l'opération $*$:
est associative,
admet un élément neutre,
et quand tout élément admet un symétrique.
Un groupe $(G, *)$ est dit **commutatif** (2) lorsque l'opération $*$ est commutative.

(1) «opération» est synonyme de loi de composition interne.

(2) «Groupe abélien» est synonyme de groupe commutatif.

Notations et propriétés

1) L'opération d'un groupe est souvent notée (3)
$+$ quand elle est commutative ou $\cdot$ sans information sur sa commutativité
2) Dans un groupe $(G, +)$, le symétrique de $g \in G$ est appelé son opposé et noté $(-g)$.
3) Dans un groupe $(G, \cdot)$, on note en général ab le «produit» $a \cdot b$ de a et b dans G.
Le symétrique de $g \in G$ est appelé son inverse et noté g^{-1}.
Étant donné a et b dans G, on a $(ab)^{-1} = b^{-1}a^{-1}$.
4) Dans un groupe $(G, \cdot)$, $\forall (a, b, c) \in G^3$, $ac = bc \Rightarrow a = b$ et $ca = cb \Rightarrow a = b$. (4)

(3) Cela quand il n'y a pas de risque de confusion avec des opérations usuelles.

(4) Tout élément est simplifiable.

2. Sous-groupes

Définition 2

Une partie non vide H de G est un **sous-groupe** d'un groupe $(G, \cdot)$ quand elle est :
stable pour l'opération de G et
stable pour le passage au symétrique.

Théorème 1

Une partie non vide H de G est un sous-groupe de $(G, \cdot)$ si et seulement si :
$$H \cdot H^{-1} \subset H \quad \text{c'est-à-dire} \quad \forall (x, y) \in H^2,\ xy^{-1} \in H.$$

Propriétés

Soit $(G, \cdot)$ un groupe d'élément neutre e. Tout sous-groupe de G contient e.

1) Un sous-groupe H de G est un groupe pour l'opération induite sur H. (5)
2) Pour toute famille $(H_t)_{t \in I}$ de sous-groupes de $(G, \cdot)$, $\bigcap_{t \in I} H_t$ est un sous-groupe de $(G, \cdot)$.
3) Le sous-groupe **engendré par** $A \subset G$, noté $\mathrm{gr}(A)$, est l'intersection des sous-groupes contenant A. (6)
A est un sous-groupe si et seulement si $A = \mathrm{gr}(A)$. $\mathrm{gr}(\varnothing) = \{e\}$.

(5) L'opération induite est encore notée $\cdot$

(6) $\mathrm{gr}(A)$ est le plus petit sous-groupe contenant A.

3. Morphismes de groupes

Définition 3

Soit $(G_1, \cdot)$ et $(G_2, *)$ des groupes et f une application de G_1 dans G_2.
f est un **morphisme** de $(G_1, \cdot)$ dans $(G_2, *)$ quand :
$$\forall (x, y) \in G_1^2,\ f(xy) = f(x) * f(y).$$

Copyrighted material

Définitions – Notations

1) $\mathrm{Hom}\left(G_1, G_2\right)$ est l'ensemble des morphismes de $\left(G_1, \bullet\right)$ dans $\left(G_2, *\right)$.
2) Un **isomorphisme** est un morphisme bijectif. $G_1 \cong G_2$ exprime qu'il existe un isomorphisme de $\left(G_1, \bullet\right)$ dans $\left(G_2, *\right)$.
3) Un **endomorphisme** est un morphisme d'un groupe dans lui-même. $\mathrm{End}(G)$ est l'ensemble des endomorphismes de $(G, \bullet)$.
4) Un **automorphisme** est un endomorphisme bijectif. $\mathrm{Aut}(G)$ est l'ensemble des automorphismes de $(G, \bullet)$.

Sous-groupes et morphismes

Soit $\left(G_1, \bullet\right)$ et $\left(G_2, *\right)$ des groupes d'éléments neutres e_1 et e_2 et $f \in \mathrm{Hom}\left(G_1, G_2\right)$.

1) $f\left(e_1\right) = e_2$.
2) Pour tout $x \in G_1$, $f\left(x^{-1}\right) = \left(f(x)\right)^{-1}$.
3) Si H_1 est un sous-groupe de $\left(G_1, \bullet\right)$, alors $f\left(H_1\right)$ est un sous-groupe de $\left(G_2, *\right)$.
4) Si H_2 est un sous-groupe de $\left(G_2, *\right)$, alors $f^{-1}\left(H_2\right)$ [7] est un sous-groupe de $\left(G_1, \bullet\right)$.

[7] $f^{-1}(H_2)$ désigne l'image réciproque de H_2 par f : $f^{-1}(H_2) = \{x \in G_1 \,/\, f(x) \in H_2\}$.

Noyau et image

f étant un morphisme de $\left(G_1, \bullet\right)$ dans $\left(G_2, *\right)$,

1) Le sous-groupe $f\left(G_1\right)$ de G_2 est l'**image** du morphisme f, il est noté $\mathrm{Im}\, f$.
2) Le sous-groupe $f^{-1}\left(\{e_2\}\right)$ de G_1 est le **noyau** du morphisme f, il est noté $\mathrm{Ker}\, f$.
3) f est injectif si et seulement si $\mathrm{Ker}\, f = \{e_1\}$.

Composition de morphismes

1) Soit $\left(G_1, \bullet\right)$, $\left(G_2, \bullet\right)$ et $\left(G_3, \bullet\right)$ des groupes.
   Si $f_1 \in \mathrm{Hom}\left(G_1, G_2\right)$ et $f_2 \in \mathrm{Hom}\left(G_2, G_3\right)$ alors $f_2 \circ f_1 \in \mathrm{Hom}\left(G_1, G_3\right)$. [8]
2) Si $\mathfrak{S}(E)$ est l'ensemble des permutations d'un ensemble E, $(\mathfrak{S}(E), \circ)$ est un groupe.
3) Étant donné un groupe $(G, \bullet)$ et $f \in \mathrm{Aut}(G)$, f^{-1} est un automorphisme de G. [9]

[8] Si $(G, \bullet)$ est un groupe, $\mathrm{End}(G)$ est une partie de G^G stable par la loi $\circ$.

[9] $(\mathrm{Aut}(G), \circ)$ est un groupe.

B. Congruences – Anneau $\mathbb{Z}$ / $n\mathbb{Z}$

1. Sous-groupes de $(\mathbb{Z}, +)$ [10]

[10] Pour l'addition et la multiplication usuelles, l'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau intègre.

Propriété 1

Division euclidienne

Étant donné $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, il existe un couple unique $(q, r) \in \mathbb{Z}^2$ d'entiers tel que :

$$a = bq + r \quad , \quad 0 \leqslant r < b.$$

Théorème 2

Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$, avec $n \in \mathbb{Z}$. [11]

Tout sous-groupe non nul de $(\mathbb{Z}, +)$ est l'ensemble des multiples de son plus petit élément strictement positif.

[11] Voir Algèbre et Géométrie, MPSI, chapitre 8.

Copyrighted material

2. Congruence modulo n

Propriété 2

Soit n un entier naturel. La relation $\mathcal{R}_n$ définie sur $\mathbb{Z}$ par :

$$x \mathcal{R}_n y \iff x - y \in n\mathbb{Z}$$

est une relation d'équivalence.

☞ L'ensemble $n\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$. Il contient 0, il est stable pour le passage à l'opposé et il est stable pour l'addition. Il vient alors que la relation $\mathcal{R}_n$ est :

- réflexive : pour tout $x \in \mathbb{Z}$, $x - x = 0 \in n\mathbb{Z}$ donc $x \mathcal{R}_n x$; (12)
- symétrique : si $x \mathcal{R}_n y$, c'est-à-dire $x - y \in n\mathbb{Z}$, on a $y - x \in n\mathbb{Z}$, donc $y \mathcal{R}_n x$,
- transitive : étant donné x, y, z dans $\mathbb{Z}$ tels que $x \mathcal{R}_n y$ et $y \mathcal{R}_n z$, on a :

$x - y \in n\mathbb{Z}$ et $y - z \in n\mathbb{Z}$, donc $x - z = (x - y) + (y - z) \in n\mathbb{Z}$, c'est-à-dire $x \mathcal{R}_n z$.

(12) Le sous-groupe $n\mathbb{Z}$ contient 0,
il est stable pour le passage à l'opposé,
et il est stable pour l'addition.

Remarque

Si $n = 0$, deux entiers sont équivalents si et seulement si ils sont égaux.

Si $n = 1$, deux entiers quelconques sont équivalents. (13)

(13) Pour ces raisons, on supposera $n \geqslant 2$ dans la suite de cette section.

Définition 4

Cette relation d'équivalence est appelée la relation de **congruence modulo** n.

On note $x \equiv y \bmod n$ l'équivalence de x et y. (14)

(14) $x \equiv y \bmod n$ exprime que $x - y$ est un multiple (entier relatif) de n.

Propriété 3

$x \equiv y \bmod n$ équivaut à : x et y ont le **même reste** dans la division euclidienne par n. (15)

(15) $n \in \mathbb{N}$, $n \geqslant 2$.

☞ a) Si x et y ont le même reste dans la division euclidienne par n, il existe k et k' dans $\mathbb{Z}$ et $r \in [\![0, n-1]\!]$ tels que : $x = kn + r$, $y = k'n + r$. Il vient alors $x - y = (k - k')n$ donc $x \equiv y \bmod n$.

b) Supposons que $x \equiv y \bmod n$.

Dans les divisions euclidiennes de x et y par n, on a : $x = kn + r$, $y = k'n + r'$, avec k, k' dans $\mathbb{Z}$ et r, r' dans $[\![0, n-1]\!]$, d'où :

$$x - y = (k - k')n + (r - r').$$

De $x - y \in n\mathbb{Z}$ et $(k - k')n \in n\mathbb{Z}$, on déduit alors $|r - r'| \in n\mathbb{N}$ et, avec $|r - r'| \leqslant n - 1$, il vient $r - r' = 0$.

Les entiers x et y ont donc le même reste dans la division euclidienne par n.

Remarques

1) Tout $x \in \mathbb{Z}$ est équivalent à l'un des éléments de $[\![0, n-1]\!]$.
2) Deux éléments distincts de $[\![0, n-1]\!]$ ne sont pas équivalents.

Définition 5

Les éléments de $[\![0, n-1]\!]$ sont les **représentants canoniques** des classes d'équivalence modulo n. L'ensemble de ces classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.

On l'appelle l'**ensemble-quotient** de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$.

Remarques

1) La classe d'équivalence de $x \in \mathbb{Z}$ pour la relation de congruence modulo n est notée $\overline{x}$ quand il n'y a pas d'ambiguïté.
2) $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. $\mathbb{Z}/n\mathbb{Z}$ est un ensemble fini de cardinal n.

Copyrighted material

3. Opérations canoniques dans $\mathbb{Z} / n\mathbb{Z}$

3.1 – Compatibilité des opérations de $\mathbb{Z}$ avec les congruences

Propriété 4

On dit que l'addition de $\mathbb{Z}$ est **compatible** avec la congruence modulo n pour traduire la propriété :

$$x \equiv x' \bmod n \quad \text{et} \quad y \equiv y' \bmod n \quad \Rightarrow \quad x + y \equiv x' + y' \bmod n.$$

☞ Soit x, x', y, y' des entiers relatifs et $n \in \mathbb{N}$. On suppose $x \equiv x' \bmod n$ et $y \equiv y' \bmod n$.
Il existe k et k' dans $\mathbb{Z}$ tels que $x = x' + kn$ et $y = y' + k'n$. On a donc :
$x + y = x' + y' + (k + k')n$, avec $k + k' \in \mathbb{Z}$, c'est-à-dire $x + y \equiv x' + y' \bmod n$.

Propriété 5

On dit que la multiplication de $\mathbb{Z}$ est **compatible** avec la congruence modulo n pour traduire la propriété :

$$x \equiv x' \bmod n \quad \text{et} \quad y \equiv y' \bmod n \quad \Rightarrow \quad xy \equiv x'y' \bmod n.$$

☞ Soit x, x', y, y' des entiers relatifs et $n \in \mathbb{N}$. On suppose $x \equiv x' \bmod n$ et $y \equiv y' \bmod n$.
Il existe k et k' dans $\mathbb{Z}$ tels que $x = x' + kn$ et $y = y' + k'n$.
$xy = x'y' + (y'k + x'k' + kk'n)n$ et $y'k + x'k' + kk'n \in \mathbb{Z}$ donne $xy \equiv x'y' \bmod n$.

3.2 – Opérations dans $\mathbb{Z}/n\mathbb{Z}$

Définition 6

Étant donné un entier naturel n, l'application :

$$s : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad x \mapsto \overline{x}.$$ ✎(16)

est la **surjection canonique** de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

✎(16) La classe d'équivalence de $x \in \mathbb{Z}$ est $s(x) = \overline{x}$.

Propriété 6

On définit sur $\mathbb{Z}/n\mathbb{Z}$ des lois de composition internes par :

$$\forall x \in \mathbb{Z}, \ \forall y \in \mathbb{Z}, \quad \overline{x} + \overline{y} = \overline{x + y} \qquad \overline{x}\,\overline{y} = \overline{xy}.$$ ✎(17)

✎(17) Les addition et multiplication ainsi définies sur $\mathbb{Z}/n\mathbb{Z}$ seront appelées les opérations **canoniques** ou **usuelles** sur $\mathbb{Z}/n\mathbb{Z}$.

☞ Soit a, b dans $\mathbb{Z}/n\mathbb{Z}$ et x, x', y, y' dans $\mathbb{Z}$ tels que $\overline{x} = \overline{x'} = a$ et $\overline{y} = \overline{y'} = b$.
$\overline{x + y} = \overline{x' + y'}$ exprime la compatibilité de l'addition de $\mathbb{Z}$ avec la congruence modulo n, donc $\overline{x} + \overline{y}$ ne dépend pas des représentants choisis pour a et b : il ne dépend que de a et b. De même, $\overline{x}\,\overline{y}$ ne dépend que de a et b.

Propriété 7

Muni de son addition canonique, $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif.
Son élément neutre est $\overline{0}$. Le symétrique de $\overline{x}$ est $\overline{-x}$: $-\overline{x} = \overline{-x}$.

☞ Étant donné a et b dans $\mathbb{Z}/n\mathbb{Z}$, il existe x et y dans $\mathbb{Z}$ tels que $a = \overline{x}$ et $b = \overline{y}$.
La commutativité de l'addition de $\mathbb{Z}$ donne : $a + b = \overline{x} + \overline{y} = \overline{x + y} = \overline{y + x} = \overline{y} + \overline{x} = b + a$, ce qui montre la commutativité de l'addition canonique de $\mathbb{Z}/n\mathbb{Z}$.
Soit de plus $c = \overline{z} \in \mathbb{Z}/n\mathbb{Z}$, on a : $(a + b) + c = (\overline{x} + \overline{y}) + \overline{z} = \overline{x + y} + \overline{z} = \overline{(x + y) + z}$ et, avec l'associativité de l'addition de $\mathbb{Z}$, il vient $(a + b) + c = a + (b + c)$, ce qui montre l'associativité de l'addition canonique de $\mathbb{Z}/n\mathbb{Z}$.
$a + \overline{0} = \overline{x} + \overline{0} = \overline{x + 0} = \overline{x} = a$ montre que $\overline{0}$ est élément neutre.

Copyrighted material

Étant donné $a = \overline{x}$ dans $\mathbb{Z}/n\mathbb{Z}$, considérons $a' = \overline{-x}$.
$a + a' = \overline{x} + \overline{-x} = \overline{x - x} = \overline{0}$ montre que $\overline{-x}$ est le symétrique de $\overline{x}$.

Propriété 8

La multiplication usuelle de $\mathbb{Z}/n\mathbb{Z}$ est commutative, associative et $\overline{1}$ est élément neutre.

☞ Étant donné $a = \overline{x}$ et $b = \overline{y}$ éléments de $\mathbb{Z}/n\mathbb{Z}$,

$$ab = \overline{x}\,\overline{y} = \overline{xy} = \overline{yx} = \overline{y}\,\overline{x} = ba.$$

Soit de plus $c = \overline{z} \in \mathbb{Z}/n\mathbb{Z}$, on a :

$$(ab)c = (\overline{x}\,\overline{y})\,\overline{z} = \overline{xy}\,\overline{z} = \overline{(xy)z} = \overline{x(yz)} = \overline{x}\,\overline{yz} = \overline{x}\,(\overline{y}\,\overline{z}) = a(bc),$$

ce qui montre l'associativité de la multiplication canonique de $\mathbb{Z}/n\mathbb{Z}$.

Pour tout $a = \overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $a\,\overline{1} = \overline{x}\,\overline{1} = \overline{x1} = \overline{x} = a$, montre que $\overline{1}$ est élément neutre pour la multiplication canonique.

Propriété 9

Muni de ces addition et multiplication, $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif. (18)

(18) Compte tenu des propriétés 7 et 8, il reste à prouver la distributivité de la multiplication par rapport à l'addition.

☞ Soit $a = \overline{x}$, $b = \overline{y}$ et $c = \overline{z}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Avec $a(b + c) = \overline{x}(\overline{y} + \overline{z}) = \overline{x}\,\overline{(y + z)} = \overline{x(y + z)}$ et $\overline{x(y + z)} = \overline{xy + xz} = \overline{xy} + \overline{xz}$, il vient :

$$a(b + c) = ab + ac.$$

Remarque

Pour $n \geqslant 2$, on a $\overline{0} \neq \overline{1}$, $\mathbb{Z}/n\mathbb{Z}$ contient au moins deux éléments et n'est donc pas réduit à $\{\overline{0}\}$. Pour $n = 1$, $\mathbb{Z}/1\mathbb{Z}$ est réduit à $\{\overline{0}\}$, c'est l'anneau nul. (19)

(19) Ce cas sera, en général, écarté.

Propriété 10

Étant donné $n \in \mathbb{N}$, la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux (20) pour les opérations usuelles de $\mathbb{Z}$ et de $\mathbb{Z}/n\mathbb{Z}$.

(20) La notion de morphismes d'anneaux a été introduite en Algèbre-Géométrie, MPSI, chapitre 6. On en retrouvera la définition dans le chapitre 2 de ce tome.

C'est un résumé de $s(x + y) = s(x) + s(y)$, $s(xy) = s(x)s(y)$ et $s(1) = \overline{1}$.

Exemple 1 Tables de Pythagore de l'addition et de la multiplication de $\mathbb{Z}/4\mathbb{Z}$ et de $\mathbb{Z}/5\mathbb{Z}$.

Par exemple, le reste dans la division par 4 de $3 + 2$ est 1. Donc, dans $\mathbb{Z}/4\mathbb{Z}$: $\overline{3} + \overline{2} = \overline{1}$.

De même, le reste dans la division de 4×3 par 5 est 2. Donc, dans $\mathbb{Z}/5\mathbb{Z}$: $\overline{4} \cdot \overline{3} = \overline{2}$.

$\mathbb{Z}/4\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\mathbb{Z}/5\mathbb{Z}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Copyrighted material

4. Morphismes de $\mathbb{Z}$ dans un anneau

Soit A un anneau et f un morphisme d'anneaux de $\mathbb{Z}$ dans A.

Théorème 3

Si le noyau de f contient $n\mathbb{Z}$, avec $n \in \mathbb{N} \setminus \{0\}$ [21], alors il existe une application $\overline{f}$ de $\mathbb{Z}/n\mathbb{Z}$ dans A telle que : $f = \overline{f} \circ s$ où s est la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.
En outre, cette application $\overline{f}$ est un morphisme d'anneaux.

[21] Dans le cas où $n = 1$, f est l'application nulle ainsi que $\overline{f}$ et ce résultat ne présente pas alors un grand intérêt.

☞ a) Soit x et y dans $\mathbb{Z}$ tels que $x \equiv y \bmod n$. Alors, $x - y \in \operatorname{Ker} f$ et par suite, $f(x) = f(y)$.
Ainsi l'image $f(x)$ ne dépend que de $\overline{x} = s(x)$ et on définit une application $\overline{f}$ de $\mathbb{Z}/n\mathbb{Z}$ dans A en posant $\forall \overline{x} \in \mathbb{Z}/n\mathbb{Z}$, $\overline{f}(\overline{x}) = f(x)$.

b) Soit $\overline{a}$ et $\overline{b}$ dans $\mathbb{Z}/n\mathbb{Z}$. En utilisant les propriétés du morphisme d'anneaux f, il vient :

$$\overline{f}(\overline{a} + \overline{b}) = \overline{f}(\overline{a+b}) = f(a+b) = f(a) + f(b) = \overline{f}(\overline{a}) + \overline{f}(\overline{b}),$$
$$\overline{f}(\overline{a} \cdot \overline{b}) = \overline{f}(\overline{ab}) = f(ab) = f(a)f(b) = \overline{f}(\overline{a})\overline{f}(\overline{b}),$$
$$\overline{f}(\overline{1}) = f(1) = 1_A.$$

Ce qui montre que $\overline{f}$ est un morphisme entre les anneaux $\mathbb{Z}/n\mathbb{Z}$ et A.

Propriété 11

Avec les notations du théorème précédent,

si $\operatorname{Ker} f = n\mathbb{Z}$, alors $\overline{f}$ est injective.

☞ Soit $a \in \mathbb{Z}$ tel que $\overline{f}(\overline{a}) = 0_A$ c'est-à-dire $f(a) = 0_A$.
On a donc $a \in \operatorname{Ker} f = n\mathbb{Z}$. Il s'ensuit $s(a) = \overline{a} = \overline{0}$.
Ainsi, $\overline{f}(\overline{a}) = 0_A \Rightarrow \overline{a} = \overline{0}$ donc $\operatorname{Ker}(\overline{f}) = \{\overline{0}\}$ ce qui prouve que $\overline{f}$ est injectif.

Corollaire

Si f est un morphisme d'anneaux de $\mathbb{Z}$ dans A de noyau $n\mathbb{Z}$ avec $n \in \mathbb{N} \setminus \{0\}$ [22] :

$f(\mathbb{Z})$ est isomorphe $\mathbb{Z}/n\mathbb{Z}$.

[22] Dans le cas où $n = 1$: $f(\mathbb{Z}) = \{0_A\}$ et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}\}$.

☞ On applique la propriété ci-dessus à l'application g de $\mathbb{Z}$ dans $f(\mathbb{Z})$ induite par f.
g permet de construire un morphisme $\overline{g}$ injectif de $\mathbb{Z}/n\mathbb{Z}$ dans $f(\mathbb{Z})$ tel que $g = \overline{g} \circ s$. La surjectivité de g assure alors la surjectivité de $\overline{g}$.
$\overline{g}$ est ainsi un isomorphisme entre les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $f(\mathbb{Z})$.

C. Génération d'un sous-groupe

1. Sous-groupes cycliques

Définition 7

Une partie A de G est **génératrice** de $(G, \cdot)$ quand $\operatorname{gr}(A) = G$. [23]

Définition 8

Un groupe est **monogène** quand il admet une partie génératrice réduite à un élément. [24]
Un groupe $(G, \cdot)$ est dit **cyclique** quand il est monogène et fini.

[23] $\operatorname{gr}(A)$, sous-groupe engendré par A, est l'intersection de tous les sous-groupes de G contenant A. C'est aussi le plus petit sous-groupe de G contenant A. Voir Algèbre-Géométrie, MPSI, chapitre 6.

[24] Si $\{a\}$ est une partie génératrice de $(G, \cdot)$, on note $G = \operatorname{gr}(a)$.

Copyrighted material

Propriété 12

Avec $A \subset G$, le sous-groupe engendré par A est l'ensemble des produits d'un nombre fini d'éléments de A ou d'inverses d'éléments de A.

Exemple 2 Le groupe des isométries d'un espace euclidien E_2 de dimension 2 est engendré par les réflexions.

Tout déplacement est la composée de deux réflexions. ✎(25)

Si f est un antidéplacement, considérons une réflexion s.

$f \circ s$ est alors un déplacement, donc de la forme $f \circ s = s_1 \circ s_2$ où s_1 et s_2 sont des réflexions.

On en déduit que $f = s_1 \circ s_2 \circ s$ est composée de réflexions.

✎(25) Algèbre et Géométrie, MPSI, chapitre 16.

Exemple 3 L'ensemble $\mathbb{U}_n$ des racines $n^{\text{èmes}}$ de l'unité est un sous-groupe du groupe multiplicatif $\mathbb{U}$ (nombres complexes de module 1). Il est engendré par $\omega_n = e^{\frac{2i\pi}{n}}$.

Propriété 13

Soit $(G, \cdot)$ un groupe et $g \in G$.

$\varphi_g : \mathbb{Z} \to G,\ n \mapsto g^n$ est un morphisme de groupes de $(\mathbb{Z}, +)$ dans $(G, \cdot)$.

L'image $\varphi_g(\mathbb{Z})$ de ce morphisme est le **sous-groupe engendré par** g.

Remarques

1) g^n est le produit de n termes égaux à g pour $n \geqslant 2$.

$g^1 = g$, $g^0 = e$, ✎(26) g^{-1} est l'inverse de g.

Pour $n \geqslant 2$, g^{-n} est le produit de n termes égaux à g^{-1}.

2) Si la loi du groupe G est notée additivement, le morphisme φ_g est défini par $n \mapsto ng$.

ng est la somme de n termes égaux à g pour $n \geqslant 2$.

$1g = g$, $0g = 0$ élément neutre de G, $(-1)g$ est l'opposé de g.

Pour $n \geqslant 2$, $(-n)g$ est la somme de n termes égaux à $-g$.

3) Le noyau et l'image de φ_g sont des sous-groupes de $(\mathbb{Z}, +)$ et de $(G, \cdot)$.

✎(26) e élément neutre du groupe.

Définition 9

Avec les notations précédentes,

a) si $\operatorname{Ker}\varphi_g = \{0\}$, on dit que g est d'**ordre infini** ;

b) si $\operatorname{Ker}\varphi_g = p\mathbb{Z}$, avec $p \in \mathbb{N}^*$, on dit que g est d'**ordre** p.

Propriété 14

Soit g est un élément d'ordre $p \in \mathbb{N}^*$ d'un groupe G.

Le sous-groupe engendré par g est $\operatorname{gr}(g) = \{e, g, \ldots, g^{p-1}\}$, de cardinal p.

a) Divisons n quelconque dans $\mathbb{Z}$ par p : $n = pq + r$, avec $r \in [\![0, p-1]\!]$.

Il vient $g^n = (g^p)^q g^r$ et donc $g^n = g^r$, d'où $\operatorname{gr}(g) = \{e, g, \ldots, g^{p-1}\}$.

b) Soit r et r' dans $[\![0, p-1]\!]$, $r' \leqslant r$. Si $g^r = g^{r'}$, on a $g^{r-r'} = e$ et $r - r' \in [\![0, p-1]\!]$.

Par définition, on a $p = \inf\{k \in \mathbb{N}^*,\ g^k = e\}$ donc $r - r' = 0$ et $r = r'$.

Les g^r, $0 \leqslant r < p$, sont donc deux à deux distincts ; d'où $\operatorname{Card}\big(\operatorname{gr}(g)\big) = p$.

Copyrighted material

Corollaire

$(G, \cdot)$ de cardinal p est cyclique si et seulement si il existe un élément g d'ordre p.

Théorème 4

Si g est un élément d'ordre $p \in \mathbb{N}^*$ d'un groupe G, les groupes $\mathbb{Z}/p\mathbb{Z}$ et $\mathrm{gr}(g)$ sont isomorphes. [27]

[27] Lorsque $p = 1$, chacun des groupes $\mathbb{Z}/p\mathbb{Z}$ et $\mathrm{gr}(g)$ est réduit à son élément neutre.

☞ L'application f_g de $\mathbb{Z}$ dans G définie par $z \mapsto g^z$ est un morphisme de $(\mathbb{Z}, +)$ dans G dont le noyau est $p\mathbb{Z}$ par définition de l'ordre de g.

Comme dans le théorème **3**, il existe une application $\overline{f}_g$ de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathrm{gr}(g)$ telle que $f_g = \overline{f}_g \circ s$ où s est la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.

Avec, pour tout $(z_1, z_2) \in \mathbb{Z}^2$, $g^{z_1+z_2} = g^{z_1} g^{z_2}$, il vient :

$$\overline{f}_g\left(\overline{z_1} + \overline{z_2}\right) = f_g(z_1 + z_2) = g^{z_1+z_2} = g^{z_1} g^{z_2} = f_g(z_1) f_g(z_2) = \overline{f}_g\left(\overline{z_1}\right)\overline{f}_g\left(\overline{z_2}\right).$$

$\overline{f}_g$ est ainsi un morphisme entre les groupes $(\mathbb{Z}/p\mathbb{Z}, +)$ et G.

Comme dans la propriété **11**, ce morphisme est injectif et, comme dans le corollaire de cette propriété, le morphisme $\overline{f}_g$ induit un isomorphisme de $\mathbb{Z}/p\mathbb{Z}$ sur $f_g(\mathbb{Z}) = \mathrm{gr}(g)$.

2. Théorème de Lagrange

Soit G un groupe d'élément neutre e et H un sous-groupe de G.

Propriété 15

Dans G, la relation définie par $x \underset{H}{\sim} y \iff y^{-1}x \in H$ est une relation d'équivalence.

☞ $x^{-1}x = e \in H$ montre que la relation est réflexive.

$x \underset{H}{\sim} y$ s'écrit $y^{-1}x \in H$. Puisque H est un sous-groupe, il en résulte $\left(y^{-1}x\right)^{-1} \in H$ c'est-à-dire $x^{-1}y \in H$. Donc $y \underset{H}{\sim} x$ et la relation $\underset{H}{\sim}$ est symétrique.

$x \underset{H}{\sim} y$ et $y \underset{H}{\sim} z$ donnent $y^{-1}x \in H$ et $z^{-1}y \in H$, donc $\left(z^{-1}y\right)\left(y^{-1}x\right) \in H$, d'où $z^{-1}x \in H$, c'est-à-dire $z \underset{H}{\sim} x$ et la relation est transitive.

Définition 10

Pour la relation $\underset{H}{\sim}$, la classe d'équivalence de $x \in G$ est le sous-ensemble xH. [28]

xH est la classe à gauche de x modulo H. L'ensemble de ces classes à gauche est noté G/H.

[28] La classe d'équivalence de e est H lui-même.

Propriété 16

Les classes à gauche modulo H ont le même cardinal que H.

☞ L'application $H \to xH$, $h \mapsto xh$ est clairement une bijection.

Théorème 5

Théorème de Lagrange

Étant donné un groupe fini G et H un sous-groupe de G, le cardinal de H divise celui de G.

☞ Les classes d'équivalence modulo H forment une partition de G.

Toutes les classes d'équivalence modulo H ont le même cardinal que H.

En notant r le nombre de ces classes, il vient $\mathrm{Card}\, G = r\, \mathrm{Card}\, H$.

Corollaire

Dans un groupe fini G, l'ordre de tout élément g est un diviseur de $\mathrm{Card}\, G$.

Copyrighted material

3. Caractéristique d'un anneau

Théorème 6

Étant donné un anneau $(A, +, \cdot)$, il existe un unique morphisme de $(\mathbb{Z}, +, \cdot)$ vers $(A, +, \cdot)$. Il est défini par $\varphi(n) = n1_A$.

☞ a) Si $\varphi : \mathbb{Z} \to A$ est un morphisme d'anneaux, on a nécessairement :

$$\varphi(n) = \varphi(n \cdot 1) = n\,\varphi(1) = n1_A.$$

b) Il est aisé de vérifier que, pour $\begin{cases} \varphi : & \mathbb{Z} & \to & A \\ & n & \mapsto & n1_A \end{cases}$ on a $\varphi(1) = 1_A$ et, pour tout $(m, n) \in \mathbb{Z}^2$, $\varphi(m+n) = \varphi(m) + \varphi(n)$, $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Définition 11

a) Si $\operatorname{Ker}\varphi = \{0\}$, on dit que $(A, +, \cdot)$ est de **caractéristique nulle**.

b) Si $\operatorname{Ker}\varphi = n\mathbb{Z}$, avec $n \in \mathbb{N}^*$, on dit que $(A, +, \cdot)$ est de **caractéristique** n. [29]

[29] Si la caractéristique n'est pas nulle, c'est le plus petit des entiers $k \in \mathbb{N}^*$ tels que $k1_A = 0_A$.

Propriété 17

Si $(A, +, \cdot)$ est de caractéristique non nulle n, on a, pour tout $a \in A$, $na = 0_A$.

☞ En effet, $na = n(1_A \cdot a) = (n1_A) \cdot a = 0_A \cdot a = 0_A$

Propriété 18

Si l'anneau est de caractéristique nulle, A est infini. [30]

[30] Le morphisme ϕ étant injectif, le sous-ensemble $\phi(\mathbb{Z})$ de A est infini comme $\mathbb{Z}$.

Propriété 19

La caractéristique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est n.

D. Produit de groupes

1. Définition

Soit G_1 et G_2 des groupes d'éléments neutres e_1 et e_2.

Propriété 20

Sur $G_1 \times G_2$, on considère l'opération définie par $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$. Pour cette opération, $G_1 \times G_2$ est un groupe, appelé **produit** des groupes G_1 et G_2. [31]

[31] Le groupe produit $G_1 \times G_2$ est commutatif si et seulement si G_1 et G_2 sont commutatifs.

L'élément neutre en est (e_1, e_2). L'inverse de (x_1, x_2) est (x_1^{-1}, x_2^{-1}).

Remarque

Si G_1 et G_2 sont d'ordres finis, il en est de même pour $G_1 \times G_2$ et l'ordre du groupe produit est égal au produit des ordres de G_1 et G_2.

Propriété 21

Les projections canoniques $p_1 : G_1 \times G_2 \to G_1$ et $p_2 : G_1 \times G_2 \to G_2$ définies par $p_1(x_1, x_2) = x_1$ et $p_2(x_1, x_2) = x_2$ sont des morphismes surjectifs de groupes.

Les injections canoniques $q_1 : G_1 \to G_1 \times G_2$ et $q_2 : G_2 \to G_1 \times G_2$ définies par $q_1(x_1) = (x_1, e_2)$ et $q_2(x_2) = (e_1, x_2)$ sont des morphismes injectifs de groupes.

Copyrighted material

Corollaire

Le groupe $G_1 \times G_2$ contient des sous-groupes respectivement isomorphes à G_1 et à G_2.

q_1 induit un isomorphisme de G_1 sur $\operatorname{Im} q_1 = G_1 \times \{e_2\}$ et q_2 induit un isomorphisme de G_2 sur $\operatorname{Im} q_2 = \{e_1\} \times G_2$.

Remarques

Pour tout $x = (x_1, x_2) \in G_1 \times G_2$, on peut écrire :

- $x = (p_1(x), p_2(x))$,
- $x = q_1(x_1)q_2(x_2) = q_2(x_2)q_1(x_1)$.

Propriété 22

Soit G un groupe et H_1, H_2 des sous-groupes de G. Alors l'ensemble H_1H_2 est un sous-groupe de G si et seulement si $H_1H_2 = H_2H_1$.

a) Supposons que H_1H_2 soit un sous-groupe.

Étant donné $x_1 \in H_1$ et $x_2 \in H_2$, on peut écrire $x_2x_1 = (x_1^{-1}x_2^{-1})^{-1}$.

Inverse d'un élément de H_1H_2, x_2x_1 est alors dans H_1H_2, d'où $H_2H_1 \subset H_1H_2$.

Soit $x \in H_1H_2$. [32] Avec $x^{-1} \in H_1H_2$, il existe $x_1 \in H_1$ et $x_2 \in H_2$ tels que $x^{-1} = x_1x_2$.

Il s'ensuit $x = x_2^{-1}x_1^{-1}$, donc $x \in H_2H_1$, puis $H_1H_2 \subset H_2H_1$.

En conclusion, si H_1H_2 est un sous-groupe, alors $H_1H_2 = H_2H_1$.

b) Supposons que $H_1H_2 = H_2H_1$.

L'élément neutre e de G est dans H_1 et dans H_2, il est donc dans H_1H_2.

Soit x_1, y_1 dans H_1 et x_2, y_2 dans H_2. On a $(x_1x_2)(y_1y_2)^{-1} = x_1(x_2y_2^{-1}y_1^{-1})$.

Avec $(x_2y_2^{-1})y_1^{-1} \in H_2H_1$ et $H_2H_1 = H_1H_2$, il existe $u_1 \in H_1$ et $u_2 \in H_2$ tels que $x_2y_2^{-1}y_1^{-1} = u_1u_2$. Il s'ensuit $(x_1x_2)(y_1y_2)^{-1} = (x_1u_1)u_2 \in H_1H_2$.

On en déduit que H_1H_2 est un sous-groupe de G.

[32] Dans l'hypothèse, les sous-groupes H_1 et H_2 ne jouent pas des rôles symétriques.

2. Théorème d'isomorphisme

Théorème 7

Soit G, G_1 et G_2 des groupes. Alors G est isomorphe au groupe produit $G_1 \times G_2$ si et seulement si il contient des sous-groupes H_1 et H_2 isomorphes à G_1 et G_2, et tels que :

(1) $\forall h_1 \in H_1, \forall h_2 \in H_2, h_1h_2 = h_2h_1$, [33]

(2) $H_1 \cap H_2 = \{e\}$ [34]

(3) $G = H_1H_2$.

[33] Cette hypothèse contient $H_1H_2 = H_2H_1$.

[34] e élément, neutre de G.

a) Supposons G isomorphe à $G_1 \times G_2$. À un isomorphisme près, on peut se placer dans le cas où $G = G_1 \times G_2$.

Les injections canoniques q_1 et q_2 de G_1 et G_2 dans $G_1 \times G_2$ montrent l'existence de sous-groupes $H_1 = \operatorname{Im} q_1$ et $H_2 = \operatorname{Im} q_2$ isomorphes à G_1 et G_2. [35]

Étant donné $h_1 \in H_1$ et $h_2 \in H_2$, il existe $x_1 \in G_1$ et $x_2 \in G_2$ tels que $h_1 = (x_1, e_2)$ et $h_2 = (e_1, x_2)$, d'où $h_1h_2 = h_2h_1$.

$H_1 = G_1 \times \{e_2\}$ et $H_2 = \{e_1\} \times G_2$ donne $H_1 \cap H_2 = \{(e_1, e_2)\} = \{e\}$ où e est l'élément neutre de G.

Enfin, on a $G = H_1H_2$ (remarque du corollaire de la propriété 21).

b) On suppose que G contient des sous-groupes H_1 et H_2 satisfaisant aux conditions de l'énoncé. Pour $g \in G$, il existe $h_1 \in H_1$ et $h_2 \in H_2$ tels que $g = h_1h_2$.

[35] Corollaire de la propriété 21.

Copyrighted material

Avec $h_1' \in H_1$ et $h_2' \in H_2$ tels que $g = h_1'h_2'$, on a $h_1h_2 = h_1'h_2'$, d'où $h_1'^{-1}h_1 = h_2'h_2^{-1}$.

Alors $H_1 \cap H_2 = \{e\}$ donne $h_1'^{-1}h_1 = e$ et $h_2'h_2^{-1} = e$, c'est-à-dire $h_1 = h_1'$ et $h_2 = h_2'$.

- Ainsi tout élément de G s'écrit d'une manière unique comme produit d'un élément de H_1 et d'un élément de H_2.

Soit ϕ_1 un isomorphisme de H_1 dans G_1 et ϕ_2 un isomorphisme de H_2 dans G_2.

Considérons l'application ϕ de G dans $G_1 \times G_2$ définie par $g = h_1h_2 \mapsto \big(\phi_1(h_1), \phi_2(h_2)\big)$.

$g = h_1h_2$ et $g' = h_1'h_2'$ donne $gg' = h_1h_2h_1'h_2'$, donc $gg' = h_1h_1'h_2h_2'$ par hypothèse (1).

- On en déduit que ϕ est un morphisme de groupes.

$\phi(h_1h_2) = (e_1, e_2)$ équivaut à $\phi_1(h_1) = e_1$ et $\phi_2(h_2) = e_2$, d'où $h_1 = h_2 = e$ puisque ϕ_1 et ϕ_2 sont injectifs. Il s'ensuit que ϕ est injectif.

Soit $x = (x_1, x_2) \in G_1 \times G_2$. Il existe $h_1 \in H_1$ et $h_2 \in H_2$ tels que $x_1 = \phi_1(h_1)$ et $x_2 = \phi_2(h_2)$ puisque ϕ_1 et ϕ_2 sont surjectifs. Alors $x = \big(\phi_1(h_1), \phi_2(h_2)\big) = \phi(h_1h_2)$ montre que ϕ est surjectif.

- En conclusion, ϕ est un isomorphisme de G sur $G_1 \times G_2$.

Exemple 4 Groupe de Klein : c'est le produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il est commutatif, d'ordre 4.

Considérons l'ensemble $V = \{e, a, b, c\}$ muni de l'opération définie par la table suivante :

$\times$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

e est neutre, $a^2 = e$, $b^2 = e$ et $c^2 = e$ montre que tout élément est inversible, étant son propre inverse. La symétrie du tableau assure la commutativité de l'opération.
$(ab)c = c^2 = e$, $a(bc) = a^2 = e$ et la symétrie des rôles joués par a, b et c suffisent pour s'assurer de l'associativité.

Ce groupe V n'est pas cyclique et n'est donc pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

Le sous-groupe $H_1 = \{e, a\}$ engendré par a et le sous-groupe $H_2 = \{e, b\}$ engendré par b sont isomorphes à $\mathbb{Z}/2\mathbb{Z}$.

$ab = ba = c$ suffit à vérifier que $V = H_1H_2$ et de plus $H_1 \cap H_2 = \{e\}$.

On en déduit que le groupe de Klein et V sont isomorphes.

Théorème 8

Lemme chinois

Étant donné des entiers p et q premiers entre eux, le groupe $\mathbb{Z}/pq\mathbb{Z}$ est isomorphe au produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. ✎(36)

✎(36) Les opérations de groupes sont notées additivement.

☞ Dans $\mathbb{Z}/pq\mathbb{Z}$ on distingue les sous-groupes H_1 et H_2 engendrés respectivement par $\overline{q}$ et $\overline{p}$:

$$H_1 = \big\{k\overline{q}/k \in \mathbb{Z}\big\} \ , \ H_2 = \big\{k\overline{p}/k \in \mathbb{Z}\big\}.$$

En remarquant que $k\overline{q} = \overline{0}$ équivaut à $p \mid k$, il vient que $\overline{q}$ est d'ordre p (dans $\mathbb{Z}/pq\mathbb{Z}$), et que :

$$\operatorname{Card} H_1 = p \ , \ H_1 = \big\{k\overline{q}/k \in [\![0, p-1]\!]\big\}.$$

De même, $\overline{p}$ est d'ordre q et :

$$\operatorname{Card} H_2 = q \ , \ H_2 = \big\{k\overline{p}/k \in [\![0, q-1]\!]\big\}.$$

Le théorème 4 nous dit alors que H_1 est isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et H_2 isomorphe à $\mathbb{Z}/q\mathbb{Z}$.

Pour $\overline{x} \in H_1 \cap H_2$, il existe k et k' dans $\mathbb{Z}$ tels que $\overline{x} = k\overline{q} = k'\overline{p}$. Alors $pq \mid kq - k'p$ donc $p \mid kq$ et puisque $p \wedge q = 1$, le théorème de Gauss donne $p \mid k$ c'est-à-dire qu'il existe $\ell \in \mathbb{Z}$ tel que $k = p\ell$. Il en résulte enfin $\overline{x} = \ell\overline{pq} = \overline{0}$, et ainsi $H_1 \cap H_2 = \{\overline{0}\}$.

D'après le théorème de Bézout, pour tout $n \in \mathbb{Z}$, il existe u et v entiers tels que $n = up + vq$, on a donc $\overline{n} = u\overline{p} + v\overline{q}$ et il s'ensuit $\mathbb{Z}/pq\mathbb{Z} \subset H_1 + H_2$ donc $\mathbb{Z}/pq\mathbb{Z} = H_1 + H_2$.

Puisqu'il s'agit ici de groupes commutatifs, on a retrouvé les conditions du théorème d'isomorphisme, donc $\mathbb{Z}/pq\mathbb{Z}$ est isomorphe au produit $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Copyrighted material

E. Compléments d'arithmétique

1. Éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N} \setminus \{0, 1\}$

Théorème 9

Pour $x \in \mathbb{Z}$, la classe $\overline{x}$ est un générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si $x \wedge n = 1$.

☞ Pour tout $(k, x) \in \mathbb{Z}^2$, on a $s(kx) = ks(x)$ (ou $\overline{kx} = k\overline{x}$).
En particulier, $s(k) = ks(1)$, $\overline{k} = k\overline{1}$, donc $\overline{1}$ est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.
Étant donné $x \in \mathbb{Z}$, $\overline{x}$ est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ si et seulement si il existe $u \in \mathbb{Z}$ tel que $u\overline{x} = \overline{1}$, c'est-à-dire $\overline{ux} = \overline{1}$, ou encore : $\exists v \in \mathbb{Z},\ ux - 1 = vn$.
Le théorème de Bézout permet alors de conclure.

Théorème 10

Les éléments inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ sont les générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

☞ $\overline{x}$ est inversible quand il existe une classe $\overline{u}$ telle que $\overline{u} \cdot \overline{x} = \overline{1}$. Comme $\overline{u} \cdot \overline{x} = \overline{ux}$, on est ramené au même point que dans la démonstration précédente.

Théorème 11

$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

☞ L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si ses éléments non nuls sont inversibles, c'est-à-dire si et seulement si pour tout $k \in [\![1, n-1]\!]$, on a $k \wedge n = 1$, et ceci est équivalent au fait que n est premier.

Définition 12

Étant donné un entier $n \in \mathbb{N}^*$, l'**indicateur d'Euler** de n est le nombre d'entiers compris entre 1 et n et premiers avec n. On le note $\varphi(n)$. [37]

[37] Pour $n \in \mathbb{N}$, $n \geqslant 2$, $\varphi(n)$ est le nombre d'éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exemple 5 Si A est un anneau intègre de caractéristique $p \neq 0$, alors p est un nombre premier.
Soit f l'unique morphisme d'anneaux de Z dans A.
$f(\mathbb{Z})$ est un sous-anneau de A donc sans diviseur de 0_A.
Isomorphe à $f(\mathbb{Z})$, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est sans diviseur de 0, et par suite, p est premier.

Propriété 23

Pour tout $n \in \mathbb{N}^* \setminus \{0, 1\}$, le groupe multiplicatif $\mathbb{U}_n$ des racines $n^{\text{ièmes}}$ de 1 est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$. [38]

[38] Plus généralement, deux groupes cycliques de même ordre sont isomorphes.

☞ Le groupe $\mathbb{U}_n$ est cyclique, engendré par $\omega = e^{2i\frac{\pi}{n}}$. On conclut avec le théorème 4.

Corollaire

Les générateurs de $\mathbb{U}_n$ sont les éléments $\omega^k = e^{2i\frac{k\pi}{n}}$ tels que $k \wedge n = 1$.

Définition 13

Les générateurs de $\mathbb{U}_n$ sont appelés les **racines primitives** $n^{\text{ièmes}}$ de 1. [39]

[39] Toute racine primitive $n^{\text{ième}}$ est un élément d'ordre n de $\mathbb{U}_n$.

Copyrighted material

2. Théorèmes classiques

Théorème 12

Théorème de Wilson

Un entier $p \geqslant 2$ est premier si et seulement si $(p-1)! \equiv -1 \bmod p$. (40)

(40) Il est équivalent de dire que $\overline{(p-1)!} = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$.

☞ a) Condition nécessaire. Supposons p premier.

$\overline{(p-1)!}$ est le produit des $\overline{x}$ pour $x \in [\![1, p-1]\!]$, tous inversibles car $\mathbb{Z}/p\mathbb{Z}$ est un corps. On groupe deux à deux ces termes, sauf ceux qui sont leur propre inverse, pour obtenir des produits partiels égaux à $\overline{1}$.

$\overline{x}$ est son propre inverse si et seulement si $\overline{x}^2 = \overline{1}$, c'est-à-dire $(\overline{x}+\overline{1})(\overline{x}-\overline{1}) = \overline{0}$, ce qui est le cas pour $\overline{1}$ et pour $-\overline{1} = \overline{p-1}$. On a donc $\overline{(p-1)!} = -\overline{1}$.

b) Condition suffisante. On suppose que $(p-1)! \equiv -1 \bmod p$.

Soit a un diviseur premier de p et b tel que $p = ab$. On a $2 \leqslant a \leqslant p$ et $1 \leqslant b \leqslant p-1$.

$(p-1)! \equiv -1 \bmod p$ donne $a(p-1)! \equiv -a \bmod p$.

Or $a(p-1)! = ab \prod_{k \in [\![1, p-1]\!] \setminus \{b\}} k \equiv 0 \bmod p$. Donc $a \equiv 0 \bmod p$.

Multiple de p compris entre 2 et p, a est égal à p et p est premier.

Théorème 13

Théorème de Fermat-Euler

Quels que soient a et n dans $\mathbb{N} \setminus \{0, 1\}$, $\quad a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$.

☞ Le groupe G des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre $\varphi(n)$ et il contient $\overline{a}$.

L'application de G dans G définie par $g \mapsto \overline{a} \cdot g$ est une bijection.

On a donc $\prod_{g \in G} g = \prod_{g \in G} \overline{a} \cdot g$. Par suite, $\prod_{g \in G} g = \overline{a}^{\varphi(n)} \prod_{g \in G} g$, d'où $\overline{a}^{\varphi(n)} = \overline{1}$.

Corollaire

Théorème de Fermat

Si p est un entier naturel premier et $a \in \mathbb{N}^*$ n'est pas multiple de p : $\quad a^{p-1} \equiv 1 \bmod p$.

☞ a non multiple de p équivaut à $a \wedge p = 1$. Si p est premier, tous les entiers compris entre 1 et $p-1$ sont premiers avec p. Ainsi, $\varphi(p) = p-1$.

Exemple 6 Avec $n = 561$, on peut avoir $a \wedge n = 1$ et $a^{n-1} \equiv 1 \bmod n$ alors que n n'est pas premier.

La décomposition en produit de facteurs premiers de 561 est $561 = 3 \times 11 \times 17$.

$a \in \mathbb{N}^*$ est premier avec 561 si et seulement si il n'est pas multiple de 3, ni de 11, ni de 17.

On a $a^2 \equiv 1 \bmod(3)$, $a^{10} \equiv 1 \bmod(11)$ et $a^{16} \equiv 1 \bmod(17)$. (41)

560 est un multiple commun à 2, 10 et 16. On en déduit (compatibilité des congruences avec la multiplication) $a^{560} \equiv 1 \bmod(3)$, $a^{560} \equiv 1 \bmod(11)$ et $a^{560} \equiv 1 \bmod(17)$.

$a^{560} - 1$ est un multiple de 3, 11 et 17, donc de leur produit, d'où $a^{560} \equiv 1 \bmod(561)$.

(41) Théorème de Fermat.

Théorème 14

Théorème chinois

Soit m et n dans $\mathbb{N}^*$, $m \wedge n = 1$, a et b dans $\mathbb{Z}$, et

(S) $\quad x \in \mathbb{Z}, \quad x \equiv a \bmod m, \quad x \equiv b \bmod n$.

a) Pour tout couple (a, b) d'entiers, le système (S) admet des solutions entières.

b) Si x_0 est une solution de (S), les solutions sont les entiers x tels que :

$$x \equiv x_0 \bmod mn$$

Copyrighted material

a) Par le théorème de Bézout, il existe des entiers u et v tels que $um + vn = 1$.
Alors $(a-b)um + (a-b)vn = a - b$ et $b + (a-b)vn = a + (b-a)um$.
En posant $(a-b)v = k$, $(b-a)u = k'$ et $x = a + k'm = b + kn$, on obtient :

$$x \equiv a \bmod m \text{ et } x \equiv b \bmod n.$$

b) Soit x et x' des solutions de (S). $\begin{cases} x \equiv a \bmod m\,, & x' \equiv a \bmod m \\ x \equiv b \bmod n\,, & x' \equiv b \bmod n \end{cases}$

Alors $x - x' \equiv 0 \bmod m$ et $x - x' \equiv 0 \bmod n$.
Divisible par m et n premiers entre eux, $x - x'$ est divisible par mn. [42]

[42] Théorème de Gauss.

Corollaire

Étant donné des entiers m et n premiers entre eux, pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ (resp. $\dot{x}$) (resp. $\ddot{x}$) la classe de x modulo mn (resp. m) (resp. n). Alors on définit un isomorphisme Φ du groupe additif $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$ en posant :

$$\forall x \in \mathbb{Z},\quad \Phi(\overline{x}) = \left(\dot{x}, \ddot{x}\right)$$ [43]

[43] Ceci nous donne une nouvelle preuve du lemme chinois (théorème 8).

Remarquons d'abord que $x' \equiv x \bmod mn$ donne évidemment $x' \equiv x \bmod m$ et $x' \equiv x \bmod n$ donc $\left(\dot{x}, \ddot{x}\right) = \left(\dot{x}', \ddot{x}'\right)$. Ainsi on définit bien une application de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$ en posant :

$$\Phi\left(\overline{x}\right) = \left(\dot{x}, \ddot{x}\right)$$ [44]

[44] L'image de $\overline{x}$ ne dépend pas du représentant choisi pour la classe $\overline{x}$.

Par définition des opérations dans $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$ on a, pour tous $\overline{x}$, $\overline{y}$ de $\mathbb{Z}/mn\mathbb{Z}$, $\Phi\left(\overline{x} + \overline{y}\right) = \Phi\left(\overline{x}\right) + \Phi\left(\overline{y}\right)$, donc Φ est un morphisme de groupes.

Si $\overline{x} \in \operatorname{Ker}\Phi$, on a $x \equiv 0 \bmod m$ et $x \equiv 0 \bmod n$ et, puisque $m \wedge n = 1$, il vient $x \equiv 0 \bmod mn$ c'est-à-dire $\overline{x} = \overline{0}$. Ainsi $\operatorname{Ker}\Phi = \left\{\overline{0}\right\}$ et Φ est injective.

D'après le théorème chinois, pour tout $\left(\dot{a}, \ddot{b}\right) \in \mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$, il existe $\overline{x} \in \mathbb{Z}/mn\mathbb{Z}$ tel que $\dot{x} = \dot{a}$, $\ddot{x} = \ddot{b}$ c'est-à-dire tel que $\Phi\left(\overline{x}\right) = \left(\dot{a}, \ddot{b}\right)$. Ainsi Φ est surjective, ce qui achève la preuve.

Remarque

En définissant le produit dans $\mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$ par :

$$\left(\dot{x}, \ddot{y}\right)\left(\dot{x}', \ddot{y}'\right) = \left(\dot{x}\dot{x}', \ddot{y}\ddot{y}'\right) = \left(\dot{\widehat{xx'}}, \ddot{\widehat{yy'}}\right),$$

on munit $\mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$ d'une structure d'anneau d'élément neutre $\left(\dot{1}, \ddot{1}\right)$. [45]

[45] Il s'agit de l'anneau produit des anneaux $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$, voir chapitre 2 de ce tome.

Il est alors immédiat que pour tous $\overline{x}$, $\overline{y}$ de $\mathbb{Z}/mn\mathbb{Z}$:

$$\Phi\left(\overline{x}, \overline{y}\right) = \Phi\left(\overline{x}\right)\,\Phi\left(\overline{y}\right)$$

et que $\qquad \Phi\left(\overline{1}\right) = \left(\dot{1}, \ddot{1}\right)$

donc Φ est un isomorphisme d'anneaux de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\,\mathbb{Z} \times \mathbb{Z}\,/n\mathbb{Z}$.

Exemple 7 Recherche d'une solution particulière de (S)

Avec les notations du théorème chinois, $x_0 = umb + vna$ est une solution.

Avec $um + vn = 1$, on a $vn \equiv 1 \bmod m$, et avec $x_0 = umb + vna$, on a $x_0 \equiv vna \bmod m$.
La compatibilité de la multiplication avec la congruence modulo m donne $vna \equiv a \bmod m$ et, par transitivité, il vient $x_0 \equiv a \bmod m$. On vérifie de même que $x_0 \equiv b \bmod n$.

3. Indicateur d'Euler

Théorème 15

L'indicateur d'Euler est une fonction arithmétique multiplicative :

$$\forall (m, n) \in \mathbb{N}^2,\ m \geqslant 2,\ n \geqslant 2,\quad m \wedge n = 1 \ \Rightarrow\ \varphi(mn) = \varphi(m)\,\varphi(n)$$

Copyrighted material

☞ Conservons les notations du corollaire du théorème chinois.

En désignant par $\mathbb{U}(\mathbb{Z}/mn\mathbb{Z})$ (resp. $\mathbb{U}(\mathbb{Z}/m\mathbb{Z})$) (resp. $(\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$) l'ensemble des éléments inversibles de $\mathbb{Z}/mn\mathbb{Z}$ (resp. $\mathbb{Z}/m\mathbb{Z}$) (resp. $\mathbb{Z}/n\mathbb{Z}$), il apparaît clairement que $\overline{x}$ est inversible dans $\mathbb{Z}/mn\mathbb{Z}$ si et seulement si $\dot{x}$ et $\ddot{x}$ sont inversibles dans $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ respectivement, donc que Φ induit une bijection de $\mathbb{U}(\mathbb{Z}/mn\mathbb{Z})$ sur $\mathbb{U}(\mathbb{Z}/m\mathbb{Z}) \times \mathbb{U}(\mathbb{Z}/n\mathbb{Z})$. ✎(46)

✎(46) $\mathbb{U}(\mathbb{Z}/m\mathbb{Z})\times\mathbb{U}(\mathbb{Z}/m\mathbb{Z})$ est le groupe des inversibles de l'anneau produit $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, voir chapitre 2 de ce tome.

Il en résulte :

$$\varphi(mn) = \operatorname{Card}\mathbb{U}(\mathbb{Z}/mn\mathbb{Z}) = \operatorname{Card}\mathbb{U}(\mathbb{Z}/m\mathbb{Z}) \times \operatorname{Card}\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$$
$$= \varphi(m)\,\varphi(n).$$

Propriété 24

Soit p un nombre premier et $\alpha \in \mathbb{N}^*$. Alors :

$$\varphi(p^\alpha) = (p-1)p^{\alpha-1}.$$

☞ Si $\alpha = 1$, on a vu que $\varphi(p) = p - 1$.

Pour $\alpha \geqslant 2$, les éléments non inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$ sont les classes des entiers $k \in [\![\, 0, p^\alpha - 1 \,]\!]$ qui sont multiples de p. Leur nombre est $p^{\alpha-1}$.

Le nombre d'éléments inversibles est donc $p^\alpha - p^{\alpha-1}$, c'est-à-dire $(p-1)p^{\alpha-1}$.

Exemple 8 Calcul de $\phi(816)$

On a $816 = 2^4 \times 3 \times 17$.

φ étant multiplicative et les entiers 2^4, 3, 17 étant deux à deux premiers entre eux, il vient :

$$\varphi(816) = \varphi(2^4)\,\varphi(3)\,\varphi(17) = 2^3 \times 2 \times 16 = 256.$$

Copyrighted material

L'essentiel

I. Ordre d'un élément, ordre d'un groupe

✔ **Si l'on veut** préciser ou exploiter l'ordre d'un élément g d'un groupe G,

- **on peut** et c'est souvent le moyen le plus efficace, revenir à la définition de l'ordre p de g : $g^p = e$ (élément neutre de G) et, pour tout n tel que $g^n = e$, on a $p|n$.

  → Voir *Mise en œuvre*, exercices 1, 2, 3, 4

✔ **Si l'on veut** décrire le sous-groupe engendré par un élément g,

- **on peut** le considérer comme l'image du morphisme $(\mathbb{Z}, +) \to (G, \cdot)$, $n \mapsto g^n$;
- **on peut** utiliser le théorème de Lagrange : l'ordre de g divise $\operatorname{Card} G$.

  → Voir *Mise en œuvre*, exercices 1, 2, 3, 4

II. Congruences et divisibilié

✔ **Si l'on veut** calculer le reste modulo n de a^b,

- **on peut** utiliser le théorème de Fermat $a^{p-1} \equiv 1 \bmod p$ pour p premier et $a \wedge p = 1$,

  → Voir *Mise en œuvre*, exercice 5
- **on peut** calculer le reste r modulo n de a et étudier les puissances successives de r. Si on a $r \neq 0$, alors il existe un entier q tel que $r^q \equiv 1 \bmod n$.

  → Voir *Mise en œuvre*, exercice 6

✔ **Si l'on veut** étudier un problème de divisibilité par n,

- **on peut** transcrire le problème en termes de classes d'équivalence dans $\mathbb{Z}/n\mathbb{Z}$,

  → Voir *Mise en œuvre*, exercices 6, 7, 10
- **on peut** étudier la divisibilité par un ou plusieurs facteur premier,

  → Voir *Mise en œuvre*, exercices 5, 6, 7, 9
- **on peut** utiliser les critères familiers de divisibilité par 2, 3 ou 5, ou en établir d'autres.

  → Voir *Mise en œuvre*, exercice 8

Mise en œuvre

I. Ordre d'un élément, ordre d'un groupe

Ex. 1

On considère un entier $n \in \mathbb{N} \setminus \{0, 1\}$ et le groupe additif $\mathbb{Z}/n\mathbb{Z}$.

1) Soit $a \in [\![0, n-1]\!]$, montrer que l'ordre de l'élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est $\dfrac{n}{n \wedge a}$.

2) Étant donné d diviseur de n, montrer que le nombre d'éléments $\overline{a}$ d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est $\varphi(d)$ où φ est la fonction indicatrice d'Euler.

3) Montrer que $\sum_{d \mid n} \varphi(d) = n$, c'est-à-dire que la somme des $\varphi(d)$ quand d décrit l'ensemble des diviseurs de n est égale à n.

Indications

1) L'ordre p de $\overline{a}$ est $p = \min\{k \in \mathbb{N}^* / n \mid ka\}$. On détermine cet ensemble.

3) Observer que les ensembles $A_d = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z}, \overline{a} \text{ d'ordre } d\}$ constituent, pour d décrivant l'ensemble des diviseurs de n, une partition de $\mathbb{Z}/n\mathbb{Z}$.

Solution

1) Posons $A = \{k \in \mathbb{N}^*, n \mid ka\}$.
Avec $d = n \wedge a$, on a $n = dm$, $a = da'$ et $m \wedge a' = 1$.
Il en résulte :

$$n \mid ka \Leftrightarrow m \mid ka',$$

d'où finalement $A = m\mathbb{N}^*$. On en déduit que $\overline{a}$ est d'ordre $m = \dfrac{n}{n \wedge a}$.

2) d étant un diviseur de n, posons $n = dq$. Alors $\overline{a}$ est d'ordre d si et seulement si :

$$n \wedge a = \frac{n}{d} = q, \text{ soit aussi } q \mid a \text{ et } d \wedge \frac{a}{q} = 1.$$

En remarquant que $0 \leqslant \dfrac{a}{q} \leqslant \dfrac{n-1}{q} < d$, on en déduit que $\overline{a}$ est d'ordre d si et seulement si : $a \in \{qr / 0 \leqslant r < d, d \wedge r = 1\}$.
Il reste à remarquer que cet ensemble est de cardinal $\varphi(d)$ pour conclure.

3) Puisque l'ordre de tout élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est un diviseur de n, on a :

$$\mathbb{Z}/n\mathbb{Z} = \bigcup_{d \in \mathcal{D}_n} A_d$$

où $\mathcal{D}_n$ désigne l'ensemble des diviseurs de n.
D'autre part, il est clair que pour $d \neq d'$ on a $A_d \cap A_{d'} = \emptyset$, donc les A_d constituent une partition de $\mathbb{Z}/n\mathbb{Z}$ et on en déduit :

$$n = \sum_{d \in \mathcal{D}_n} \operatorname{Card} A_d = \sum_{d \in \mathcal{D}_n} \varphi(d).$$

Commentaires

C'est le théorème de Gauss.

$A = \{mj, j \in \mathbb{N}^*\}$.

$\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $0 \leqslant a \leqslant n-1$.

D'après la première question. Il est clair que $q = n \wedge a$ donne $q \mid a$ donc $a = qr$ et $dq \wedge qr = q$ équivaut à $d \wedge r = 1$.

Par définition de φ, si $d \geqslant 2$,
$\{r, 0 \leqslant r < d, d \wedge r = 1\} = \{r, 1 \leqslant r \leqslant d, d \wedge r = 1\}$
et si $d = 1$, $\{r, 0 \leqslant r < 1, 1 \wedge r = 1\} = \{0\}$.
A_d est défini en indications : c'est l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.

D'après le 2), on a $\operatorname{Card} A_d = \varphi(d)$.

Copyrighted material

Ex. 2

Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$ et $d \in \mathbb{N}$ un diviseur de n.

1) Soit g un générateur de G. Montrer que, pour $r \in \mathbb{N}$, l'ordre de g^r est $\dfrac{n}{n \wedge r}$.

2) On pose $q = \dfrac{n}{d}$ et on considère l'application $f_q : G \to G, x \mapsto x^q$.

Montrer que $\operatorname{Im} f_q$ est un sous-groupe d'ordre d de G.

3) Montrer qu'il existe un sous-groupe de G et un seul qui soit d'ordre d.

Indications

1) Étudier les entiers naturels m tels que $\left(g^r\right)^m = e$ élément neutre de G.

2) Étant donné $k \in \mathbb{N}$, l'application $f_k : G \to G, x \mapsto x^k$ est un endomorphisme (un groupe cyclique est commutatif).

3) On prouvera que $\operatorname{Im} f_q = \operatorname{Ker} f_d$.

Solution

1) Posons $d = n \wedge r$, $n = dn'$ et $r = dr'$.

Pour tout $m \in \mathbb{N}$, on a $(g^r)^m = e$ si et seulement si n divise rm, c'est-à-dire n' divise $r'm$. Et ceci équivaut à n' divise m. Ainsi :

$$\frac{n}{n \wedge r} = n' = \inf\left\{m \in \mathbb{N}, (g^r)^m = e\right\}.$$

2) Soit q le quotient de n par d. L'application f_q est un morphisme, donc $\operatorname{Im} f_q$ est un sous-groupe de G.

g étant un générateur de G, l'ordre de g^q est d.

Avec $\operatorname{Im} f_q = \left\{\left(g^k\right)^q,\ k \in [\![0, n-1]\!]\right\} = \left\{\left(g^q\right)^k,\ k \in [\![0, n-1]\!]\right\}$, l'image de f_q est le sous groupe engendré par g^q qui est d'ordre d. Ainsi $\operatorname{Im} f_q$ est un sous-groupe d'ordre d.

3) Soit H un sous-groupe d'ordre d.

Pour tout $h \in H$, on a $h^d = e$, c'est-à-dire $h \in \operatorname{Ker} f_d$, donc $H \subset \operatorname{Ker} f_d$.

$\forall x \in G, (x^q)^d = x^n = e$ montre que $\operatorname{Im} f_q \subset \operatorname{Ker} f_d$.

$\left(g^k\right)^d = e$ si et seulement si $kd \equiv 0 \bmod n$, ce qui montre que :

$$g^k \in \operatorname{Ker} f_d \Leftrightarrow q \mid k,\ 0 \leqslant k \leqslant n-1$$

donc $\operatorname{Ker} f_d$ est d'ordre d.

Ainsi il vient $\operatorname{Im} f_q = \operatorname{Ker} f_d$ donc $H \subset \operatorname{Im} f_q$. Ayant le même cardinal, ces sous-groupes sont les mêmes.

Commentaires

$r' \wedge n' = 1$.

Théorème de Gauss.

C'est la définition de l'ordre de g^r.

Question précédente avec $n \wedge q = q$.

$G = \{g^k, k \in [\![0, n-1]\!]\}$ donne $\operatorname{Im} f_q = \{(g^k)^q, k \in [\![0, n-1]\!]\}$

La question posée revient à prouver que $H = \operatorname{Im} f_q$.

Comme $\operatorname{Im} f_q$.

Ex. 3

À l'aide d'une partition de $\mathbb{U}_n$ (groupe des racines $n^{\text{èmes}}$ de 1), montrer que $\displaystyle\sum_{d \mid n} \varphi(d) = n$, où $n \in \mathbb{N}$, $n \geqslant 2$.

La somme porte sur les diviseurs de n dans $\mathbb{N}$ et φ est la fonction indicatrice d'Euler.

Indications

Avec $\omega = \exp\left(\dfrac{2i\pi}{n}\right)$, le groupe cyclique $\mathbb{U}_n$ admet $\varphi(n)$ générateurs : les ω^k pour $k \in [\![1, n]\!]$, $k \wedge n = 1$.

Solution

Si $d \in \mathbb{N}^*$ est un diviseur de n, alors $\mathbb{U}_d$ est un sous-groupe de $\mathbb{U}_n$.

Dans le groupe cyclique $\mathbb{U}_n$, $\mathbb{U}_d$ est le seul sous-groupe d'ordre d.

Tout élément d'ordre d engendre $\mathbb{U}_d$. Pour $r \in [\![1, n]\!]$, posons :

$$D_r = \{\omega^k,\ k \in [\![1, r-1]\!],\ k \wedge r = 1\} \text{ et } D_1 = \{1\}.$$

On obtient alors une partition de $\mathbb{U}_n$ par $\mathbb{U}_n = \bigcup_{d|n} D_d$.

On en déduit $n = \sum_{d|n} \varphi(d)$.

Commentaires

$\omega^d=1$ implique $\omega^n=1$.

Voir l'exercice précédent.

D_r est l'ensemble des générateurs de $\mathbb{U}_r$.

On classe les éléments de $\mathbb{U}_n$ selon leur ordre.
Card $D_d=\phi(d)$.

Ex. 4

1) Soit H et K des groupes finis et $(h, k) \in H \times K$.
Montrer que l'ordre de (h, k) est le PPCM des ordres de h et de k.

2) Soit H et K des groupes cycliques. Montrer que le groupe $H \times K$ est cyclique si et seulement si les ordres m et n de H et K sont premiers entre eux.

Indications

1) $H \times K$ est canoniquement muni d'une structure de groupe. L'élément neutre est $e = (e_H, e_K)$.

2) Le groupe $H \times K$ est d'ordre mn.

Solution

1) Notons r et s les ordres de h et k et considérons r', s' tels que :

$$r \vee s = rr' \text{ et } r \vee s = ss'.$$

On a :

$$(h, k)^{r \vee s} = \left(h^{r \vee s}, k^{r \vee s}\right) = \left(h^{rr'}, k^{ss'}\right) = (e_H, e_K).$$

L'ordre q de (h, k) divise donc $r \vee s$.
Avec $(h, k)^q = e$, c'est-à-dire $\left(h^q, k^q\right) = (e_H, e_K)$, il vient :

$$h^q = e_H$$

donc r divise q, et $k^q = e_K$ donc s divise q. Alors $r \vee s$ divise q, et finalement $q = r \vee s$.

2) Le groupe produit $H \times K$ est cyclique si et seulement si il existe un élément d'ordre mn.
L'ordre de $(h, k) \in H \times K$ est $r \vee s$.
En outre, r divise m et s divise n.
Soit m' et n' définis par $m = m'r$ et $n = n's$. L'ordre de (h, k) est alors mn si et seulement si $mn = r \vee s$.
Cela se lit $m'n'rs = r \vee s$, d'où $m' = n' = 1$ et $rs = r \vee s$.
Ainsi $r = m$, $s = n$ et $m \wedge n = 1$.

Commentaires

$h^r=e_H$ et $k^s=e_K$.

$H\times K$ est d'ordre mn.

r ordre de h et s ordre de k.
Théorème de Lagrange.

$rs=(r\vee s)(r\wedge s)$, donc $m'n'(r\wedge s)=1$.
Avec la question précédente, la condition est suffisante.

Copyrighted material

II. Congruences, $\mathbb{Z}/n\mathbb{Z}$

Ex. 5

Théorème de Fermat, exemple, contre-exemple.

Soit a un entier naturel, $a > 1$.

1) Montrer que $a^{13} - 1$ est divisible par 546.

2) Montrer que $4^{14} - 1$ est divisible par 15, bien que 15 ne soit pas premier.

Indications

On note que $546 = 2 \times 3 \times 7 \times 13$ (décomposition en produit de facteurs premiers).

Étudier le reste dans la division de 4^2 par 15.

Solution

1) $a^{13} - a$ est divisible par 13.

$$a^{13} - a = a(a^{12} - 1) = a(a^6 - 1)(a^6 + 1)$$
$$= (a^7 - a)(a^6 + 1)$$

donc $a^{13} - a$ est divisible par 7.

$$a^{13} - a = a(a^2 - 1)(a^4 + a^2 + 1)(a^6 + 1)$$
$$= (a^3 - a)(a^4 + a^2 + 1)(a^6 + 1)$$

donc $a^{13} - a$ est divisible par 3.

Enfin $a(a^2 - 1) = a(a-1)(a+1)$ est divisible par 2, donc $a^{13} - a$ est divisible par 2.

Divisible par les nombres premiers 2, 3, 7 et 13, $a^{13} - a$ est divisible par leur produit 576.

2) Avec $4^2 = 16 \equiv 1 \bmod 15$, il vient $(4^2)^7 \equiv 1 \bmod 15$, c'est-à-dire que $4^{14} - 1$ est divisible par 15.

Commentaires

Application du théorème de Fermat.

À partir de la décomposition précédente.

Ceci, bien que 15 ne soit pas premier. On a donc montré que le théorème de Fermat exprime une condition suffisante mais non nécessaire.

Ex. 6

Calculer le reste dans la division de 247^{343} par 7.

Indications

Les congruences modulo 7 sont efficaces. On peut utiliser le théorème de Fermat.

Solution

On voit aisément que $247 \equiv 2 \bmod 7$, donc $247^{343} \equiv 2^{343} \bmod 7$.

Compte tenu de $2^6 \equiv 1 \bmod 7$, divisons 343 par 6. Avec $343 = 6 \times 57 + 1$ et $2^{343} = (2^6)^{57} \times 2$, $(2^6)^{57} \equiv 1 \bmod 7$ donne $2^{343} \equiv 2 \bmod 7$.

On peut aussi remarquer que $343 = 7^3$. Alors $2^7 \equiv 2 \bmod 7$ donne :

$$2^{7^3} = \left(\left((2^7)\right)^7\right)^7 \equiv 2 \bmod 7.$$

En conclusion, il vient $247^{343} \equiv 2 \bmod 7$.

Commentaires

$243 = 30 \times 7 + 30 + 7$.

Théorème de Fermat.

Autre forme du théorème de Fermat.

Ex. 7

1) Étant donné un nombre premier p, déterminer les diviseurs de $\overline{0}$ dans $\mathbb{Z}/p^2\mathbb{Z}$.

2) Déterminer les entiers relatifs n tels que $2n^2 + 13n + 20$ soit divisible par 9.

Indications

Si un nombre premier divise un produit ab, alors il divise a ou b.

Avec $\overline{a} \cdot \overline{b} = \overline{0}$, il faut distinguer un facteur nul ou des facteurs diviseurs de $\overline{0}$.

Solution

1) Soit a et b entiers relatifs tels que $\overline{a}\,\overline{b} = \overline{0}$, avec $\overline{a} \neq \overline{0}$ et $\overline{b} \neq \overline{0}$.
Cela se lit aussi p^2 divise ab et p^2 ne divise ni a ni b. Ce qui est vrai si et seulement si p divise a et divise b. D'où les solutions :

$$a = kp \text{ et } b = k'p,$$

avec k et k' non multiples de p.

Les diviseurs de $\overline{0}$ dans $\mathbb{Z}/p^2\mathbb{Z}$ sont les $\overline{k}\,\overline{p}$, avec $k \in [\![1, p-1]\!]$.

2) Avec $13 \equiv 4 \bmod 9$ et $20 \equiv 2 \bmod 9$, l'équation se lit aussi :

$$\overline{2}\left(\overline{n}^2 + \overline{2n} + \overline{1}\right) = \overline{0} \text{ ou encore } \overline{2}\left(\overline{n} + \overline{1}\right)^2 = \overline{0}.$$

Avec $2 \wedge 9 = 1$, l'équation équivaut à $\left(\overline{n} + \overline{1}\right)^2 = \overline{0}$.

Les solutions sont alors les entiers n tels que $n+1 \equiv 0 \bmod 9$ ou tels que :

$$n + 1 \equiv 3 \bmod 9 \text{ ou } n + 1 \equiv 6 \bmod 9.$$

En conclusion les solutions sont les entiers $n = 3k - 1$, avec $k \in \mathbb{Z}$.

Commentaires

$\overline{x}$ désigne ici la classe de x modulo p^2.

$\overline{x}$ est ici la classe de x modulo 9.

En distinguant $\overline{n+1}=\overline{0}$ et $\overline{n+1}$ diviseur de $\overline{0}$.

Ex. 8

Quel est le reste dans la division de 761 945 par 11 ?

Indications

On peut établir un critère général de divisiblité par 11. Il ne serait pas constructif de se réfugier dans un calcul effectif de quotient et du reste.

Solution

Soit $\overline{a_r a_{r-1} \dots a_2 a_1 a_0}$ l'écriture en base 10 d'un entier A.

Avec $10 \equiv -1 \bmod 11$, il vient $a_k 10^k \equiv (-1)^k a_k \bmod 11$. Il s'ensuit :

$$A \equiv \sum_{k=0}^{r} (-1)^k a_k \bmod 11.$$

Application numérique $A = 761\,945$.

$A \equiv 5 - 4 + 9 - 1 + 6 - 7 \bmod 11$, c'est-à-dire $A \equiv 8 \bmod 11$.

Finalement, le reste dans la division de 761 945 par 11 est 8.

Commentaires

$A = \sum_{0 \leq k \leq r} a_k 10^k$.

Copyrighted material

Ex. 9

Étant donné $n \in \mathbb{N}$, $n \geqslant 2$, montrer que $h_n = \sum_{k=1}^{n} \frac{1}{k}$ n'est pas un entier.

Indications

On met h_n sous forme réduite : $h_n = \frac{a_n}{b_n}$, avec a_n et b_n dans $\mathbb{N}^*$, $a_n \wedge b_n = 1$.

Il suffit alors de trouver un diviseur premier de b_n. Le plus raisonnable est d'espérer que 2 convient.

Solution

Soit $p = \sup\left\{k \in \mathbb{N}^*, 2^k \leqslant n\right\}$. On a $h_n = \frac{1}{2^p} + g_n$, avec :

$$g_n = \sum_{k \in [\![1,n]\!] \setminus \{2^p\}} \frac{1}{k}.$$

Soit $g_n = \frac{x_n}{y_n}$ avec x_n et y_n dans $\mathbb{N}^*$, et où y_n est le plus petit multiple commun à l'ensemble des entiers $[\![1, n]\!] \setminus \{2^p\}$. Il est donc de la forme $2^{p-1}z_n$, avec $z_n \in \mathbb{N}^*$ et $z_n \wedge 2 = 1$.

Il vient alors $h_n = \frac{z_n + 2x_n}{2^p z_n}$ et il reste à noter que $z_n + 2x_n$ n'est pas divisible par 2 pour conclure.

Commentaires

$n \geqslant 2$ donne $p \geqslant 1$.

$\frac{x_n}{y_n}$ n'est pas nécessairement la forme réduite de g_n.

$z_n \wedge 2 = 1$.

Ex. 10

Soit p un entier premier, $p \geqslant 3$. Montrer que p divise le numérateur de la forme réduite de $h_p = \sum_{k=1}^{p-1} \frac{1}{k}$.

Indications

Dans $\mathbb{Z}/p\mathbb{Z}$, tout élément non nul est inversible.

En notant $F_p = \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$, l'application $\varphi : F_p \to F_p, x \mapsto -x^{-1}$ est une bijection. On pourra utiliser le théorème de Wilson.

Solution

Avec $\frac{1}{k} = \frac{u_k}{(p-1)!}$, il vient $ku_k = (p-1)!$.

Il s'ensuit $\overline{ku_k} = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$, donc $\overline{u_k} = -\overline{k}^{-1}$.

Avec $h_p = \frac{1}{(p-1)!}\sum_{k=1}^{p-1} u_k$ et $h_p = \frac{a}{b}$, il vient $\overline{b}\sum_{k=1}^{p-1}\overline{u_k} = -\overline{a}$.

L'application ϕ étant une bijection, on a $\sum_{k=1}^{p-1}\overline{u_k} = \sum_{k=1}^{p-1}\overline{k}$.

Or $\sum_{k=1}^{p-1}\overline{k}$ est la classe modulo p de $\sum_{k=1}^{p-1} k$ c'est-à-dire celle de $\frac{(p-1)p}{2}$.

$p-1$ étant pair, $\frac{(p-1)p}{2}$ est un multiple de p.

Il s'ensuit $\overline{a} = \overline{0}$, c'est-à-dire que p divise a.

Commentaires

u_k entier. Les fractions $\frac{1}{k}$ ont $(p-1)!$ pour dénominateur commun.

Théorème de Wilson.

$\frac{a}{b}$ forme réduite de h_p et théorème de Wilson.

ϕ est décrite en indications.

$p \geqslant 3$ et p premier.

Exercices

Niveau 1

Groupes

Ex. 1

Soit G un groupe fini, d'élément neutre e. On suppose que des sous-groupes H et K ont des ordres premiers entre eux. Montrer que $H \cap K = \{e\}$.

Ex. 2

Soit G un groupe multiplicatif.

On suppose qu'il existe $n \in \mathbb{N}^*$ tel que l'application $f : G \to G, x \mapsto x^n$ soit un morphisme surjectif.

Montrer que $\forall (x, y) \in G^2, x^{n-1}y = yx^{n-1}$.

Congruences, $\mathbb{Z}/n\mathbb{Z}$

Ex. 3

Résoudre le système $\begin{cases} x = 1 \bmod 9 \\ x = 2 \bmod 7 \end{cases}$

Ex. 4

Montrer que 11 divise $2 \times 5^{22} + 20 \times 3^{11}$.

Ex. 5

Déterminer les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Arithmétique

Ex. 6

1) Décomposer 5 929 en produit de facteurs premiers.

2) Quelles sont les paires d'entiers naturels dont le PGCD et le PPCM sont les racines de :

$$x^2 - 91x + 588 = 0 \text{ ?}$$

Ex. 7

Étant donné un entier $n \geqslant 2$, montrer que la somme de n entiers impairs consésutifs n'est pas un nombre premier.

Niveau 2

Avec solution détaillée

Groupes

Ex. 8

Déterminer les sous-groupes d'un groupe cyclique.

Ex. 9

Étant donné $n \in \mathbb{N} \setminus \{0, 1\}$, on note $\mathbb{P}_n$ l'ensemble des racines primitives $n^{\text{ièmes}}$ de 1.

Soit $z \in \mathbb{P}_n$ et $k \in \mathbb{N}^*$. Montrer que z^k est dans $\mathbb{P}_n$ si et seulement si $k \wedge n = 1$.

Congruences, $\mathbb{Z}/n\mathbb{Z}$

Ex. 10

Déterminer, suivant les valeurs de $n \in \mathbb{N}$, le reste dans la division par 7 de :

$$A = 851^{3n} + 851^{2n} + 851^n + 2.$$

Ex. 11

Résoudre :

$$\begin{cases} x = 2 \bmod 88 \\ x = 1 \bmod 27 \end{cases} \qquad \begin{cases} x = 3 \bmod 4 \\ x = 4 \bmod 5 \\ x = 1 \bmod 3 \end{cases}$$

Ex. 12

Montrer qu'il y a une infinité de nombres premiers congrus à -1 modulo 4.

Ex. 13

Trouver le dernier chiffre de $1987^{1991^{1993}}$.

Ex. 14

Pour $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$. Montrer que, si $n \neq m$, les entiers F_n et F_m sont premiers entre eux.

Ex. 15

Montrer qu'il y a une infinité de nombres premiers dans l'ensemble $6\,\mathbb{N}^* - 1$.

Copyrighted material

Avec éléments de solution

Ex. 16

Déterminer les éléments $(a, b) \in (\mathbb{Z}/13\mathbb{Z})^2$ tels que $a^2 + b^2 = \overline{0}$.

Ex. 17

Soit p premier, $p \geqslant 3$. On pose $F_p = \mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$.

Montrer que, pour $k \in \mathbb{N}^*$, $\sum_{x \in F_p} x^k \in \{\overline{0}, -\overline{1}\}$.

Niveau 3

Avec solution détaillée

Ex. 18

Soit p un nombre premier impair ; on pose $p = 2q + 1$.

Montrer que $(q!)^2 + (-1)^q$ est divisible par p.

Ex. 19

Soit $(G, +)$ un groupe commutatif. On donne deux éléments x et y d'ordres respectifs finis p et q premiers entre eux.

1) Montrer que le sous-groupe F de G, engendré par $z = x + y$, contient x et y.

2) Quel est le cardinal de F ?

Ex. 20

Étant donné p premier $\geqslant 3$, combien y-a-t-il de carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Ex. 21

Soit p un entier naturel premier. Montrer que le groupe (multiplicatif) G_p des éléments autres que $\overline{0}$ de $\mathbb{Z}/p\mathbb{Z}$ est cyclique.

Avec éléments de solution

Ex. 22

Montrer que, pour tout $n \in \mathbb{N}$, 19 divise $2^{2^{6n+2}} + 3$.

Ex. 23

Pour $n \in \mathbb{N}^*$, $f(n)$ désigne la somme des chiffres de n en écriture décimale.

Calculer $f \circ f \circ f\left(4\,444^{4444}\right)$.

Ex. 24

Montrer que, pour tout $n \in \mathbb{N}^*$, la partie entière de $(\sqrt{3} + 1)^{2n+1}$ est divisible par 2^{n+1}.

Ex. 25

Soit G un sous-groupe fini du groupe des bijections affines d'un espace vectoriel réel E.

1) Montrer qu'il existe un même point invariant par tout élément de G.

2) Déterminer les sous-groupes finis de $(\mathbb{C}^*, \times)$.

3) Déterminer les sous-groupes finis du groupe des similitudes directes du plan.

Copyrighted material

Indications

Ex. 8

Pour g générateur de G et H sous-groupe de G, étudier $\varphi^{-1}(H)$, avec $\varphi : \mathbb{Z} \to G, n \mapsto g^n$.

Ex. 9

Considérer $u = z^k$. Si $k \wedge n = 1$, utiliser le théorème de Gauss pour montrer que, si $u^h = 1$, alors n divise h.

Ex. 10

Utiliser d'abord le reste dans la division de 851 par 7.

Étudier la suite des restes dans la division de 2^n par 7.

Ex. 11

1) Le cours donne une méthode de résolution.

2) Résoudre le système formé par les deux premières équations. Avec la troisième, on obtient alors un nouveau problème de restes chinois.

Ex. 12

En considérant n nombres premiers $p_i \equiv -1 \bmod(4)$, l'étude des facteurs premiers de $N = -1 + 4\prod_{i=1}^{n} p_i$ met en évidence un $n+1^{\text{ème}}$ nombre premier p tel que $p \equiv -1 \bmod 4$.

Ex. 13

Considérer le premier entier d tel que : $7^d \equiv 1\ [10]$, puis la classe de 1991 modulo d.

Ex. 14

Observer que, si d divise F_n, alors d divise $2^{2^m} - 1$ pour $m > n$.

Ex. 15

Tout nombre premier (autre que 2 ou 3) est congru à 1 ou 5 modulo 6. Montrer qu'il ne peut pas y en avoir seulement un nombre fini de la forme $6n - 1$.

Ex. 16

Des représentants de $\mathbb{Z}/13\mathbb{Z}$ sont les $k \in [\![-6, 6]\!]$.

On notera que $5^2 \equiv -1 \bmod 13$.

Ex. 17

On pourra utiliser le théorème de Fermat pour justifier que l'on peut se limiter à $k \in [\![1, p-1]\!]$ et distinguer les cas particuliers $k = 1$ et $k = p - 1$.

Ex. 18

Utiliser le théorème de Wilson et $(2q)! = q! \prod_{k=1}^{q} (q+k)$.

Ex. 19

Pour montrer que $x \in F$, montrer qu'il existe $k \in \mathbb{Z}$ tel que $k \equiv 1 \bmod p$ et $k \equiv 0 \bmod q$ et qu'alors $x = kz$.

Ex. 20

Quand p est premier l'anneau $\mathbb{Z}/p\mathbb{Z}$ est intègre.

Les carrés de $\mathbb{Z}/p\mathbb{Z}$ sont les $\overline{k}^2$ pour $k \in [\![0, \frac{p-1}{2}]\!]$.

Ex. 21

Pour g d'ordre n dans G_p, comparer le nombre $\varphi(n)$ des générateurs du sous-groupe engendré par g et le nombre $\psi(n)$ des éléments de G_p qui sont d'ordre n.

On pourra utiliser $\sum_{n|p-1} \varphi(n) = p - 1$.

Ex. 22

Par récurrence. Justifier que $\overline{-3}^9 \equiv 1 \bmod 19$.

Ex. 23

Majorer $f\left(4444^{4444}\right)$ et itérer. On conclut avec les congruences modulo 9.

Ex. 24

Noter que $0 < \sqrt{3} - 1 < 1$,

et que $(\sqrt{3}+1)^{2n+1} - (\sqrt{3}-1)^{2n+1}$ est un entier.

Ex. 25

1) Pour $M \in E$, étudier l'isobarycentre de $g(M)$, $g \in G$.

2) Les éléments d'ordre fini de $\mathbb{C}^*$ sont de module 1.

3) Utiliser les deux premières questions.

Copyrighted material

Solutions des exercices

Niveau 1

Ex. 1

$H \cap K$ est un sous-groupe de H et aussi de K. D'après le théorème de Lagrange, l'ordre n de $H \cap K$ divise l'ordre de H et celui de K. Comme ces ordres sont premiers entre eux, il vient $n = 1$. Sachant que le seul sous-groupe d'ordre 1 de G est $\{e\}$, la conclusion en résulte.

Ex. 2

Étant donné $x \in G$, on considère l'application $f_x : G \to G,\ y \mapsto x^{-1}yx$.

Il s'agit de montrer que, pour tout $y \in G$, $x^{n-1}y = yx^{n-1}$, c'est-à-dire $x^{-1}yx = x^{-n}yx^n$ ou encore $f_x = f_{x^n}$. Or, pour tout $z \in G$:

$$\left(f_x(z)\right)^n = (x^{-1}zx)^n = x^{-1}z^nx = f_x(z^n)$$

et $(x^{-1}zx)^n = x^{-n}z^nx^n$ car $f : t \mapsto t^n$ est un morphisme de G : $f(x^{-1}zx) = f(x^{-1})f(z)f(x)$. Donc :

$$\forall z \in G, f_x(z^n) = f_{x^n}(z^n).$$

Comme f est surjective, pour tout $y \in G$, il existe $z \in G$ tel que $y = z^n$, donc $\forall y \in G, f_x(y) = f_{x^n}(y)$.

En conclusion, pour tout x de G, x^{n-1} commute avec tous les éléments de G.

Remarque. Si, de plus, $x \mapsto x^{n-1}$ est elle aussi surjective, le groupe G est commutatif.

Ex. 3

9 et 7 sont premiers entre eux. Une égalité de Bézout est $(-3) \times 9 + 4 \times 7 = 1$. En application du résultat relatif aux congruences simultanées, le nombre $x_0 = (-3) \times 9 \times 2 + 4 \times 7 \times 1 = -26$ est solution.

Les solutions du système sont alors $x = -26 + 63k$, $k \in \mathbb{Z}$, et la plus petite solution positive est $-26 + 63$, c'est-à-dire 37.

Ex. 4

En appliquant le théorème de Fermat, il vient $5^{11} \equiv 5 \bmod 11$.

Avec la compatibilité du produit et des congruences, il vient $5^{22} \equiv 5^2 \bmod 11$, or $25 \equiv 3 \bmod 11$, donc :

$$5^{22} \equiv 3 \bmod 11 \quad \text{et} \quad 2 \times 5^{22} \equiv 6 \bmod 11.$$

Avec $3^{11} \equiv 3 \bmod 11$ (théorème de Fermat à nouveau), il vient $20 \times 3^{11} \equiv 60 \bmod 11$ et par suite (compatibilité de l'addition et des congruences) :

$$2 \times 5^{22} + 20 \times 3^{11} \equiv 66 \bmod 11$$

c'est-à-dire $2 \times 5^{22} + 20 \times 3^{11} \equiv 0 \bmod 11$, ce qui exprime que 11 divise $2 \times 5^{22} + 20 \times 3^{11}$.

Ex. 5

La surjection canonique s de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est en particulier un morphisme de groupes (additifs).

Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Son image réciproque par s est un sous-groupe de $\mathbb{Z}$.

Il existe donc $h \in \mathbb{N}$ tel que $s^{-1}(H) = h\mathbb{Z}$. Comme s est surjective, on a alors $H = s(h\mathbb{Z})$.

De plus, comme H contient $\overline{0}$, le sous-groupe $s^{-1}(H)$ contient $s^{-1}(\overline{0}) = n\mathbb{Z}$. L'inclusion $h\mathbb{Z} \supset n\mathbb{Z}$ équivaut à h divise n. Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont ainsi les sous-groupes engendrés par les éléments $\overline{h}$, avec h diviseur de n.

Ex. 6

1) 5 929 est divible par 11 (voir *Mise en œuvre*, exercice 8) : $5\,926 = 11 \times 539$ et 539 est à nouveau divisible par $11 : 539 = 11 \times 49$. Finalement, $5\,929 = 11^2 \times 7^2$.

2) Le discriminant de $x^2 - 91x + 588$ est 5 929 et les racines sont 84 et 7. On cherche alors a et b entiers naturels tels que $a \vee b = 84$ et $a \wedge b = 7$.

En posant $a = 7a'$ et $b = 7b'$, $a \vee b = 7a'b'$ revient à trouver a' et b' tels que $a' \wedge b' = 1$ et $a'b' = 12$.

Les paires $\{a, b\}$ solutions sont donc $\{7, 84\}$ et $\{21, 28\}$.

Copyrighted material

Ex. 7

Soit $2a+1$ un entier naturel impair. La somme $S_n = \sum_{k=a}^{a+n-1} 2k+1 = n(2a+n)$ n'est pas un nombre premier.

Niveau 2

Ex. 8

Étant donné un groupe cyclique G, on note r l'ordre de G et on choisit un générateur g de ce groupe.

L'application $\begin{cases} \varphi : & \mathbb{Z} & \to & G \\ & n & \mapsto & g^n \end{cases}$ est un morphisme de groupes surjectif puisque $\mathrm{gr}(g) = G$ et de noyau $r\mathbb{Z}$ par définition de l'ordre de g. Si H est un sous-groupe de G, son image réciproque $\varphi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$.

Il existe donc $s \in \mathbb{N}$ tel que $\varphi^{-1}(H) = s\mathbb{Z}$.

Comme ce sous-groupe contient $\varphi^{-1}(0) = r\mathbb{Z}$, il vient : $s\mathbb{Z} \supset r\mathbb{Z}$ c'est-à-dire s divise r. On a donc :

$$\varphi^{-1}(H) = s\mathbb{Z} \text{ avec } s|r.$$

Puisque φ est une surjection, on a $H = \varphi\left(\varphi^{-1}(H)\right) = \varphi(s\mathbb{Z})$.

En conclusion : les sous-groupes d'un groupe cyclique d'ordre r et de générateur g sont les sous-groupes $\mathrm{gr}(g^s)$, avec $s|r$. Ce sont aussi des groupes cycliques.

Ex. 9

Posons $u = z^k$. On a évidemment $u^n = 1$.

1) Supposons que $k \wedge n = 1$.

Soit $h \in \mathbb{N}^*$ tel que $u^h = 1$. On a alors $z^{kh} = 1$, et comme z est d'ordre n, on en déduit que n divise hk. Alors n étant premier avec k, le théorème de Gauss donne que n divise h.

On a donc prouvé que n est le plus petit entier naturel non nul élément de $\{h \in \mathbb{N}^*, u^h = 1\}$. L'ordre de u est ainsi n, ce qui montre que u est dans $\mathbb{P}_n$.

2) Supposons k non premier avec n et notons d le PGCD de n et k. On a $d > 1$.

En désignant par m et h les quotients de n et k par d : $n = md$, $k = hd$, on a $0 < m < n$. On obtient alors :

$$u^m = z^{km} = z^{mhd} = z^{nh} = 1,$$

ainsi u est d'ordre strictement inférieur à n et n'est donc pas dans $\mathbb{P}_n$.

Ex. 10

Dans cet exercice, nous noterons $x = y$ pour $x = y \bmod 7$.

Le reste dans la division de 851 par 7 est 4, d'où $851 = 4$. On a donc :

$$851^{3n} + 851^{2n} + 851^n = 4^{3n} + 4^{2n} + 4^n.$$

Comme $\left(4^3\right)^n = 1^n$, $\left(4^2\right)^n = 2^n$, et $4^n = 2^{2n}$, on a $A = 851^{3n} + 851^{2n} + 851^n + 2 = 3 + 2^n(1 + 2^n)$.

Étudions les restes dans la division par 7 des puissances de 2.

$2^0 = 1$, $2^1 = 2$, $2^2 = 4$ et $2^3 = 1$ conduit à diviser n par 3 : $n = 3q + r$, $0 \leqslant r \leqslant 2$.

Il vient donc $2^n = (2^3)^q 2^r$ d'où $2^n = 2^r$ et il s'ensuit :

si $n = 0 \bmod 3$, $A = 5$,

si $n = 1 \bmod 3$, $A = 2$, et

si $n = 2 \bmod 3$, $A = 2$.

En conclusion, si n est congru à 0 modulo 3, le reste dans la division de A par 7 est 5, et, dans les autres cas, ce reste est 2.

Copyrighted material

Ex. 11

Il s'agit d'exemples du problème des restes chinois.

1) Nous avons (principe de l'algorithme d'Euclide) :

$$88 = 3 \times 27 + 7,\ 27 = 7 \times 3 + 6,\ 7 = 6 + 1.$$

On en déduit :

$$1 = 7 - 6 = 7 - (27 - 7 \times 3) = 7 \times 4 - 27 = (88 - 3 \times 27) \times 4 - 27 = 4 \times 88 - 13 \times 27.$$

Une solution particulière est donc $x_0 = 1 \times 4 \times 88 - 2 \times 13 \times 27 = -350$.

L'ensemble des solutions est donc $\{-350 + 27 \times 88\,k,\ k \in \mathbb{Z}\}$.

La plus petite solution positive est $-350 + 2\,376 = 2\,026$.

Autre méthode

On a $\begin{cases} x \equiv 2 \bmod 88 \\ x \equiv 1 \bmod 17 \end{cases}$ si et seulement si il existe $(k, k') \in \mathbb{Z}^2$ tel que :

$$\begin{cases} x = 2 + 88k \\ x = 1 + 27k' \end{cases}$$

Cela revient à trouver les couples $(k, k') \in \mathbb{Z}^2$ tels que :

$$2 + 88k = 1 + 27k', \text{ c'est-à-dire } 88k - 27k' = -1. \qquad \textbf{(1)}$$

En reprenant le calcul fait dans la première méthode, on a $4 \times 88 - 13 \times 27 = 1$.

Une solution particulière de **(1)** est donc $(-4, -13)$. Les solutions de **(1)** sont alors :

$$\{(-4 + 27\lambda, -13 + 88\,\lambda),\ \lambda \in \mathbb{Z}\}.$$

$x = 2 + 88k$ donne ensuite :

$$x = 2 + 88(-4 + 27\lambda) = -350 + 2376\lambda,\ \ \lambda \in \mathbb{Z}.$$

2) Cherchons les solutions de (S) $\begin{cases} x \equiv 3 \bmod 4 \\ x \equiv 4 \bmod 5 \end{cases}$ qui vérifient en outre :

$$x \equiv 1 \bmod 3. \qquad \textbf{(2)}$$

En utilisant l'une ou l'autre des méthodes vues en 1), le lecteur vérifiera que les solutions de (S) sont les entiers x tels que :

$$x \equiv 19 \bmod 20. \qquad \textbf{(3)}$$

Nous sommes alors ramenés à résoudre le système (S') $\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 19 \bmod 20 \end{cases}$

En définitive, les solutions sont les entiers $x \equiv 19 \bmod 60$.

Ex. 12

Mis à part 2, tout nombre premier est impair. Il est donc congru à 1 ou à -1 modulo 4.

L'ensemble des nombres premiers congrus à -1 modulo 4 n'est pas vide (il contient 3).

Montrons que s'il contient au moins n termes distincts, alors il en contient au moins $n + 1$.

Supposons donc l'existence de n nombres premiers $(p_i)_{i \in [\![1,n]\!]}$ tels que $p_i \equiv -1 \bmod(4)$.

$N = -1 + 4\prod_{i=1}^{n} p_i$ se décompose en produit de facteurs premiers qui sont tous impairs puisque N est impair.

Ces facteurs sont congrus à 1 ou à -1 modulo 4. S'ils étaient tous congrus à 1 modulo 4, il en serait de même pour leur produit N. Or N est congru à -1 modulo 4, il y a donc au moins un facteur premier de N qui est congru à -1 modulo 4.

Comme N n'est divisible par aucun des p_i, les facteurs premiers de N sont tous différents des n nombres p_i.

Nous avons donc au moins $n + 1$ éléments dans l'ensemble étudié.

Copyrighted material

Ex. 13

On a $1987 \equiv 7 \bmod 10$ donc $1987^{1991} \equiv 7^{1991} \bmod 10$ puis $1987^{1991^{1993}} \equiv 7^{1991^{1993}} \bmod 10$.

Avec $7^2 \equiv 9 \bmod 10$, il vient $7^3 = 7 \times 7^2 \equiv 7 \times 9 \bmod 10$ et $7^4 = (7^2) \equiv 9^2 \bmod 10$, c'est-à-dire :

$$7^3 \equiv 3 \bmod 10 \quad \text{et} \quad 7^4 \equiv 1 \bmod 10.$$

$1991 = 497 \times 4 + 3$ donne $1991 \equiv -1 \bmod 4$ et $1991^{1993} \equiv -1 \bmod 4$, on a donc aussi :

$$1991^{1993} = 4n + 3 \quad \text{et} \quad 7^{1991^{1993}} = 7^{4n+3} \equiv 3 \bmod 10.$$

En conclusion, $1987^{1991^{1993}} \equiv 3 \bmod 10$, c'est-à-dire que le dernier chiffre de $1987^{1991^{1993}}$ est 3.

Ex. 14

Soit m et n entiers naturels distincts. On peut choisir $m > n$.

Soit d un diviseur de F_n dans $\mathbb{N}^*$. On a $2^{2^n} + 1 \equiv 0 \bmod d$ donc $2^{2^n} \equiv -1 \bmod d$.

Il s'ensuit, pour tout $p \in 2\mathbb{N}$, $\left(2^{2^n}\right)^p = 2^{2^n p} \equiv 1 \bmod d$.

Choisissons $p = 2^{m-n} \in 2\mathbb{N}$. On obtient $2^{2^m} \equiv 1 \bmod d$ donc $F_m \equiv 2 \bmod d$.

Si d est un diviseur de F_m, on a aussi $F_m \equiv 0 \bmod d$ et par suite, si d est un diviseur commun de F_n et F_m, il vient :

$$2 \equiv 0 \ [d].$$

On a donc $d \in \{1, 2\}$. Mais le cas $d = 2$ est irrecevable car F_n est impair, donc $d = 1$. En conclusion, pour $m \neq n$, le seul diviseur commun de F_n et F_m est 1, c'est-à-dire que F_n et F_m sont premiers entre eux.

Ex. 15

Les entiers congrus à 0, 2 ou 4 modulo 6 sont pairs. Ceux qui sont congrus à 3 modulo 6 sont divisibles par 3.

Les nombres premiers, autres que 2 ou 3, sont donc congrus à 1 ou à 5 modulo 6.

Supposons qu'il y ait au moins N entiers premiers p_k de la forme $6n - 1$, avec $n \in \mathbb{N}^*$ et notons P leur produit :

$$P = \prod_{k=1}^{N} p_k .$$

Le nombre $U = 6P - 1$ n'est divisible par aucun des p_k, $k \in [\![1, N]\!]$.

Si tous les diviseurs premiers de U étaient de la forme $6n + 1$ ($\equiv 1 \bmod 6$), alors U serait aussi congru à 1 modulo 6.

Or U est congru à -1 modulo 6. On en déduit que U admet un diviseur premier de la forme $6n - 1$, avec $n \in \mathbb{N}^*$.

En conclusion, s'il y a au moins N nombres premiers de la forme $6n - 1$, $n \in \mathbb{N}^*$, alors il y en a au moins $N + 1$, ce qui montre qu'il y a une infinité de nombres premiers de cette forme.

Ex. 16

On peut identifier un élément de $[\![-6, 6]\!]$ et sa classe d'équivalence modulo 13.

Avec $5^2 \equiv -1 \bmod 13$, $a^2 + b^2 = 0$ équivaut à :

$$b^2 - 5a^2 = 0,$$

c'est-à-dire :

$$(b - 5a)(b + 5a) = 0.$$

$\mathbb{Z}/13\mathbb{Z}$ étant un corps, cela équivaut à $b = 5a$ ou $b = -5a$. Les solutions sont résumées dans le tableau suivant :

a	0	± 1	± 2	± 3	± 4	± 5	± 6
b	0	± 5	± 3	± 2	± 6	± 1	± 4

Copyrighted material

Ex. 17

Le théorème de Fermat donne $x^{p-1} = \overline{1}$, donc $x^{k+p-1} = x^k$ et on se limite à $k \in [\![1, p-1]\!]$.

Dans le cas particulier où $k = 1$, on a $\sum_{x \in F_p} x = \sum_{j \in [\![1, p-1]\!]} \overline{j}$. Avec $\frac{p(p-1)}{2}$ multiple de p, il vient :

$$\sum_{x \in F_p} x = \overline{0}.$$

Pour $k = p-1$, on a $x^{p-1} = \overline{1}$, donc :

$$\sum_{x \in F_p} x^{p-1} = \overline{p-1} = -\overline{1}.$$

Pour $k \in [\![1, p-2]\!]$, on a $(x+1)^{k+1} - x^{k+1} = \sum_{j=1}^{k+1} C_{k+1}^j x^{k+1-j}$ donc :

$$\sum_{x \in F_p} \left((x+1)^{k+1} - x^{k+1} \right) = \sum_{j=1}^{k+1} C_{k+1}^j S_{k+1-j}$$

où on a posé $S_r = \sum_{x \in F_p} x^r$ et $S_0 = \sum_{x \in F_p} \overline{1} = \overline{p-1} = -\overline{1}$.

En supposant $S_r = \overline{0}$ pour $1 \leqslant r \leqslant k-1$, il reste $-\overline{1} = (k+1)S_k + S_0$, donc $S_k = \overline{0}$ car $1 \leqslant k+1 < p$. Ainsi, par récurrence, il vient :

$$S_1 = S_2 = \cdots = S_{p-2} = \overline{0}.$$

Niveau 3

Ex. 18

$p = 2q+1$ étant premier, le théorème de Wilson nous donne $(2q)! + 1 \equiv 0 \bmod p$. Nous avons :

$$(2q)! = q! \prod_{k=1}^{q} (q+k).$$

Pour tout $k \in [\![1, q]\!]$, $p - (q+k) = q + 1 - k$ et donc $q + k \equiv -(q+1-k) \bmod p$, puis :

$$\prod_{k=1}^{q} (q+k) \equiv (-1)^q \prod_{k=1}^{q} (q+1-k) \bmod p.$$

En posant $q+1-k = j$, on a $\prod_{k=1}^{q} (q+1-k) = \prod_{j=1}^{q} j = q!$. Il s'ensuit, en reportant dans $q! \prod_{k=1}^{q} (q+k) + 1 \equiv 0 \bmod(p)$, $(-1)^q (q!)^2 + 1 \equiv 0 \bmod(p)$, d'où $(q!)^2 + (-1)^q \equiv 0 \bmod(p)$.

Ex. 19

1) Soit $k \in \mathbb{Z}$. On a $x = kz$ si et seulement si $(k-1)x + ky = 0$.

Par définition des ordres de x et y, on a, pour tout $m \in \mathbb{Z}$,

$$\left(m \equiv 0 \bmod p \;\Rightarrow\; mx = 0 \right) \quad \text{et} \quad \left(m \equiv 0 \bmod q \;\Rightarrow\; my = 0 \right).$$

Pour prouver que x appartient au sous-groupe F engendré par z, il suffit de montrer qu'il existe $k \in \mathbb{Z}$ tel que :

$$k \equiv 1 \bmod p \quad \text{et} \quad k \equiv 0 \bmod q.$$

Or, p est premier avec q, donc (théorème de Bézout) il existe $(u, v) \in \mathbb{Z}^2$ tels que $qu - pv = 1$.

Il suffit alors de choisir $k = qu = pv + 1$ pour obtenir $x \in F$.

On montre de même que y est dans F.

Copyrighted material

Remarque

x et y sont des éléments du sous-groupe F engendré par $x+y$. Les sous-groupes F_x et F_y engendrés par x et y sont donc inclus dans F. Il s'ensuit l'inclusion $F_x + F_y \subset F$.

Par ailleurs, avec $z \in F_x + F_y$, le sous-groupe engendré par z est inclus dans $F_x + F_y$. On a donc $F = F_x + F_y$.

2) On considère l'application $\Phi : F_x \times F_y \to F = F_x + F_y, \quad (u,v) \mapsto u+v$.

Elle est surjective par construction. On vérifie immédiatement que Φ est un morphisme de groupes.

Soit $(u,v) \in \operatorname{Ker}\Phi$: alors $u+v=0$ donc $u=-v \in F_x \cap F_y$ et cet élément de G a pour ordre un diviseur commun à p et q.

p et q étant premiers entre eux, cet ordre est 1, c'est-à-dire que l'élément $u=-v$ est l'élément neutre de G.

Avec $u=-v=0$, on a $\operatorname{Ker}\Phi = \{(0,0)\}$ et Φ est un morphisme injectif.

Ainsi, Φ est un injectif et surjectif, c'est donc une bijection.

En conclusion, comme les sous-groupes F_x et F_y ont pour cardinaux respectifs p et q, il vient :

$$\operatorname{Card} F = \operatorname{Card} F_x \cdot \operatorname{Card} F_y = pq.$$

Ex. 20

On note $\overline{k}$ la classe modulo p de $k \in \mathbb{Z}$.

p étant impair (entier premier supérieur ou égal à 3), on peut choisir pour représentants des éléments de $\mathbb{Z}/p\mathbb{Z}$, les p éléments $\pm k$, $\quad k \in \left[\!\left[0, \dfrac{p-1}{2}\right]\!\right]$. Les carrés dans $\mathbb{Z}/p\mathbb{Z}$ sont donc

$$\overline{k}^2,\ k \in \left[\!\left[0, \frac{p-1}{2}\right]\!\right].$$

Soit alors k et k' dans $\left[\!\left[0, \dfrac{p-1}{2}\right]\!\right]$ tels que $\overline{k}^2 - \overline{k'}^2 = \overline{0}$.

Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps (p premier) avec $\overline{k}^2 - \overline{k'}^2 = \left(\overline{k} - \overline{k'}\right)\left(\overline{k} + \overline{k'}\right)$, il vient $\overline{k} = \pm\overline{k'}$, donc $k = k'$ car ces représentants sont positifs. En conclusion, tous les carrés sont de la forme $\overline{k}^2$, $k \in \left[\!\left[0, \dfrac{p-1}{2}\right]\!\right]$ et ces $\dfrac{p+1}{2}$ éléments sont deux à deux distincts. Il y a donc $\dfrac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Ex. 21

Puisque p est premier, $F_p = \mathbb{Z}/p\mathbb{Z}$ est un corps et $G_p = F_p \setminus \{\overline{0}\}$ est un groupe multiplicatif.

Pour $p=2$, G_2 est réduit à $\overline{1}$. Il reste à examiner la situation où p est au moins égal à 3.

Si g est d'ordre n, le sous-groupe $\operatorname{gr}(g) = \left\{\overline{1}, g, \cdots, g^{n-1}\right\}$ admet pour générateurs les éléments g^k, avec $1 \leqslant k \leqslant n$ et $k \wedge n = 1$. Ces générateurs sont au nombre de $\varphi(n)$, donc $\operatorname{gr}(g)$ contient $\varphi(n)$ éléments d'ordre n.

Montrons maintenant qu'il n'y a pas d'éléments d'ordre n en dehors de $\operatorname{gr}(g)$.

On remarque d'abord que tout $x \in G_p$, d'ordre n, vérifie $x^n - \overline{1} = \overline{0}$.

Or le polynôme $X^n - \overline{1}$ de degré n, à coefficients dans le corps commutatif F_p, admet au plus n racines distinctes et tout élément h du groupe cyclique $\operatorname{gr}(g)$ d'ordre n vérifie $h^n = \overline{1}$, donc $\operatorname{gr}(g)$ est l'ensemble des racines de $X^n - \overline{1}$. Il en résulte que, si $x \in G_p$ est d'ordre n, alors x est élément de $\operatorname{gr}(g)$.

En conséquence, s'il existe un élément g d'ordre n dans G_p alors G_p contient exactement $\varphi(n)$ éléments d'ordre n. Finalement pour tout $n \in [\![1, p-1]\!]$, en notant $\psi(n)$ le nombre d'éléments de G_p qui sont d'ordre n, on a :

$$\psi(n) = 0 \ \text{ ou } \ \psi(n) = \varphi(n).$$

Or, pour tout $g \in G_p$ on a $g^{p-1} = \overline{1}$, en application du théorème de Fermat. Par suite, tout élément de G_p a un ordre qui divise $p-1$ et on en déduit :

$$\sum_{n \mid p-1} \psi(n) = p-1$$

donc $\displaystyle\sum_{n \mid p-1} \psi(n) = \sum_{n \mid p-1} \varphi(n)$ (*Mise en œuvre*, exercice 2).

Copyrighted material

Avec $0 \leqslant \psi(n) \leqslant \varphi(n)$ il vient $\psi(n) = \varphi(n)$ pour tout n divisant $p-1$. En particulier,

$$\psi(p-1) = \varphi(p-1).$$

Comme $p-2$ est premier avec $p-1$, on a $\varphi(p-1) \geqslant 1$, d'où $\psi(p-1) \geqslant 1$.

Il y a donc au moins un élément d'ordre $p-1$ dans G_p c'est-à-dire que G_p est cyclique.

Ex. 22

Posons $A_n = 2^{2^{6n+2}} + 3$. On a $A_0 = 19$ ce qui amorce la récurrence.

Supposons $A_{n-1} \equiv 0 \bmod 19$, c'est-à-dire $2^{2^{6n-4}} \equiv -3 \bmod 19$. On a :

$$2^{2^{6n+2}} = \left(2^{2^{6n-4}}\right)^{2^6} = \left(2^{2^{6n-4}}\right)^{64} = (-3)^{64} \bmod 19 = 16^{64} \bmod 19.$$

Le théorème de Fermat donne $16^{18} \equiv 1 \bmod 19$. Dans $\mathbb{Z}/19\mathbb{Z}$:

$$\overline{16}^{18} - \overline{1} = \left(\overline{16}^{9} - \overline{1}\right)\left(\overline{16}^{9} + \overline{1}\right).$$

Donc $\overline{16}^{9} = \overline{1}$ ou $\overline{16}^{9} = -\overline{1}$. Avec $\overline{-3}^{2} = \overline{9}$, puis $\overline{-3}^{4} = \overline{5}$, il vient :

$$\overline{-3}^{8} = \overline{6} \text{ puis } \overline{16}^{9} = \overline{1}.$$

Enfin, avec $64 = 9 \times 7 + 1$, on obtient :

$$\left(2^{2^{6n-4}}\right)^{64} = -3 \bmod 19.$$

Ex. 23

Une majoration de $f \circ f \circ f\left(4444^{4444}\right)$ va nous être utile.

$n = 4444^{4444}$ est inférieur à $10\,000^{5000} = 10^{20000}$, donc $m = f(n) < 9 \times 20\,000 = 18\,000$.

$r = f(m)$ est majoré par $1 + 9 \times 5 = 46$ et enfin $s = f(r)$ est majoré par $4 + 9 = 13$.

Dans la division par 9, un nombre et la somme de ses chiffres ont le même reste.

On en déduit que s et 4444^{4444} ont le même reste dans la division par 9.

Ainsi $4444 \equiv -2 \bmod 9$ donne $n \equiv (-2)^{4444} \bmod 9$, c'est-à-dire $n \equiv 2^{4444} \bmod 9$.

Avec $2^6 = 64 \equiv 1 \bmod 9$ et $4444 = 740 \times 6 + 4$, il vient $n \equiv 2^4 \bmod 9$, c'est-à-dire $n \equiv 7 \bmod 9$.

Enfin, $s \equiv 7 \bmod 9$ et $s \leqslant 13$ donne $s = 7$.

Ex. 24

Par la formule du binôme, on a :

$$E_n = \left(\sqrt{3}+1\right)^{2n+1} - \left(\sqrt{3}-1\right)^{2n+1} = 2\sum_{k=0}^{n} 3^k \mathrm{C}_{2n+1}^{2k} \in \mathbb{N}.$$

Avec $0 \leqslant \left(\sqrt{3}-1\right)^{2n+1} < 1$ et $\left(\sqrt{3}+1\right)^{2n+1} = E_n + \left(\sqrt{3}-1\right)^{2n+1}$, la partie entière de $\left(\sqrt{3}+1\right)^{2n+1}$ est E_n.

Les développements :

$$\left(\sqrt{3}+1\right)^{2n+1} = \sum_{k=0}^{n} 3^k \mathrm{C}_{2n+1}^{2k} + \sqrt{3}\sum_{k=0}^{n} 3^k \mathrm{C}_{2n+1}^{2k+1}$$

$$\text{et} \qquad \left(\sqrt{3}-1\right)^{2n+1} = -\sum_{k=0}^{n} 3^k \mathrm{C}_{2n+1}^{2k} + \sqrt{3}\sum_{k=0}^{n} 3^k \mathrm{C}_{2n+1}^{2k+1}$$

montrent que, pour $n \in \mathbb{N}$, il existe a_n et b_n dans N tels que :

$$\left(\sqrt{3}+1\right)^{2n+1} = a_n + \sqrt{3}b_n$$

$$\text{et} \quad \left(\sqrt{3}-1\right)^{2n+1} = -a_n + \sqrt{3}b_n.$$

d'où : $E_n = 2a_n$.

Copyrighted material

Pour $n \geqslant 1$, $\left(\sqrt{3}+1\right)^{2n+1} = \left(\sqrt{3}+1\right)^2\left(\sqrt{3}+1\right)^{2n-1}$ donne :

$$a_n + \sqrt{3}b_n = \left(4+2\sqrt{3}\right)\left(a_{n-1}+\sqrt{3}b_{n-1}\right),$$

donc $\sqrt{3}$ étant irrationnel, il vient :

$$\begin{cases} a_n = 2\left(2a_{n-1}+3b_{n-1}\right) \\ b_n = 2\left(a_{n-1}+2b_{n-1}\right) \end{cases}$$

Avec $a_0 = 1$ et $b_0 = 1$, ces relations définissent a_n et b_n par récurrence.

En particulier, $a_1 = 10$ et $b_1 = 6$. Si a_{n-1} et b_{n-1} sont divisibles par 2^{n-1}, alors a_n et b_n sont divisibles par 2^n. Il s'ensuit, par récurrence, que E_n est divisible par 2^{n+1}.

Ex. 25

1) Pour $M \in E$, soit $I = \dfrac{1}{\operatorname{Card} G}\displaystyle\sum_{g\in G} g(M)$. Tout $h \in G$ conserve le barycentre, donc :

$$h(I) = \frac{1}{\operatorname{Card} G}\sum_{g\in G} h\circ g(M).$$

En notant que $G \to G$, $g \mapsto h\circ g$ est une bijection, il vient $h(I) = I$, et cela pour tout $h \in G$.

2) Soit G un sous-groupe fini de $\left(\mathbb{C}^*, \times\right)$ et $n = \operatorname{Card} G$.

D'après le théorème de Lagrange, on a pour tout $z \in G$, $z^n = 1$, donc $z \in \mathbb{U}_n = \left\{e^{\frac{2ik\pi}{n}}, 0 \leqslant k \leqslant n-1\right\}$, groupe des racines $n^{\text{èmes}}$ de l'unité.

Avec $G \subset \mathbb{U}_n$ l'égalité $\operatorname{Card} G = \operatorname{Card}\mathbb{U}_n = n$ donne alors $G = \mathbb{U}_n$.

3) Soit ω l'affixe d'un point invariant par les éléments d'un sous-groupe fini G de similitudes planes directes.

Ces similitudes s ont pour formules analytiques $z \mapsto \lambda e^{i\alpha}(z-\omega)+\omega$.

On vérifie que $\psi : G \to \mathbb{C}^*$, $s \mapsto \lambda e^{i\alpha}$ est un morphisme de groupes.

Son image est un sous-groupe fini de $(\mathbb{C}^*, \times)$, donc il existe $n \in \mathbb{N}^*$ tel que $\psi(G) = \mathbb{U}_n$.

G est alors l'ensemble des rotations de centre ω et d'angles $\dfrac{2k\pi}{n}$, $k \in [\![0, n-1]\!]$.

Copyrighted material

CHAPITRE 2

Anneaux et idéaux Arithmétique des polynômes

Copyrighted material

A. Anneaux

1. Définition et règles de calcul [1]

[1] Bref rappel des notions de base relatives à un anneau.
Voir Algèbre et Géométrie, MPSI, chapitre 6.

Définition 1

Un **anneau** $(A, +, \cdot)$ est constitué d'un ensemble A non vide et de deux opérations telles que :

- $(A, +)$ est un groupe commutatif, [2]
- $\cdot$ est associative, admet un élément neutre, est distributive par rapport à $+$.

[2] $+$ est l'addition de A, $\cdot$ en est la multiplication.

Un anneau $(A, +, \cdot)$ est dit **commutatif** si sa multiplication est commutative.

L'élément neutre de l'addition est noté 0_A, celui de la multiplication est noté 1_A. [3]

Le symétrique de $a \in A$ pour $+$ (opposé de a) est noté $-a$.

S'il existe, le symétrique de $a \in A$ pour $\cdot$ (inverse de a), est noté a^{-1}.

[3] $(A, +, \cdot)$ est dit non nul quand $1_A \neq 0_A$.

1.1 – Règles de calcul

Règle 1

$\forall a \in A,\ 0_A \cdot a = a \cdot 0_A = 0_A$. Si $\text{Card}(A) > 1$, on a $0_A \neq 1_A$.

$\forall (a, b) \in A^2,\ (-a) \cdot b = a \cdot (-b) = -(a \cdot b),\quad (-1_A) \cdot a = -a,\quad (-a) \cdot (-b) = a \cdot b.$

$\forall (a, b, c) \in A^3,\quad a \cdot (b - c) = a \cdot b - a \cdot c \quad (b - c) \cdot a = b \cdot a - c \cdot a.$

$\forall (a, b) \in A^2, \forall n \in \mathbb{Z},\quad (na) \cdot b = a \cdot (nb) = n(a \cdot b).$

Règle 2

Si a et b sont des éléments de A qui commutent, on a pour tout $n \in \mathbb{N}$: [4]

(1) $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}$ [5] **(2)** $a^n - b^n = (a - b) \cdot \sum_{k=0}^{n-1} a^{n-1-k} \cdot b^k$

[4] On convient que $\forall x \in A,\ x^0 = 1_A$.

[5] Formule du binôme.

1.2 – Éléments particuliers

Propriété 1

a) L'ensemble U_A des éléments inversibles de $(A, +, \cdot)$ est stable pour la multiplication de A.

b) $(\mathrm{U}_A, \cdot)$ est un groupe.

Définition 2

a) Soit $(A, +, \cdot)$ un anneau non nul et $a \in A \setminus \{0_A\}$. On dit que a est :

- diviseur de 0_A à droite s'il existe $x \neq 0_A$ tel que $x \cdot a = 0_A$,
- diviseur de 0_A à gauche s'il existe $y \neq 0_A$ tel que $a \cdot y = 0_A$,
- diviseur de 0_A quand il est diviseur de 0_A à droite et à gauche.

b) Un anneau $(A, +, \cdot)$ est sans diviseurs de 0_A lorsque :

$$\forall (a, b) \in A^2,\ a \cdot b = 0_A \ \Rightarrow\ \left[a = 0_A \text{ ou } b = 0_A\right].$$

Définition 3

Un anneau $(A, +, \cdot)$ est dit **intègre** quand il est non nul, commutatif et sans diviseur de 0_A.

Copyrighted material

1.3 – Sous-anneaux, anneau-produit

Définition 4

Une partie B de A est un **sous-anneau** de $(A, +, \cdot)$ lorsque c'est :

(1) un sous-groupe de $(A, +)$,

(2) stable pour la multiplication de A,

(3) et contenant 1_A.

Pour les opérations induites sur B, $(B, +, \cdot)$ est alors un anneau.

Propriété 2

Soit $(A, +, \cdot)$ et $(B, +, \cdot)$ des anneaux. On munit l'ensemble $A \times B$ des opérations définies par :

quels que soient (a, b) et (a', b') dans $A \times B$,

(1) $(a, b) + (a', b') = (a + a', b + b')$,

(2) $(a, b) \cdot (a', b') = (a \cdot a', b \cdot b')$.

Alors $(A \times B, +, \cdot)$ est un anneau, appelé l'**anneau-produit** de $(A, +, \cdot)$ et $(B, +, \cdot)$.

L'élément neutre pour l'addition est $(0_A, 0_B)$ et l'élément neutre pour le produit est $(1_A, 1_B)$.

2. Morphismes d'anneaux

Définition 5

Soit $(A, +, \cdot)$ et $(B, +, \cdot)$ des anneaux et ϕ une application de A dans B. On dit que ϕ est un **morphisme d'anneaux** lorsque :

(1) ϕ est un morphisme de groupes, de $(A, +)$ dans $(B, +)$,

(2) $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ pour tout $(x, y) \in A^2$,

(3) $\phi(1_A) = 1_B$.

Le **noyau** d'un morphisme d'anneaux est le noyau du morphisme de groupes sous-jacents. En particulier un tel morphisme ϕ est injectif si et seulement si :

$$\forall a \in A,\ \phi(a) = 0_B \ \Rightarrow\ a = 0_A.$$

Avec les notations ci-dessus,

Propriété 3

a) $\phi(0_A) = 0_B$ et $\phi(-a) = -\phi(a)$ pour tout $a \in A$.

b) $\phi(na) = n\,\phi(a)$ pour tout $a \in A$ et pour tout $n \in \mathbb{Z}$.

Propriété 4

a) $\phi(a^n) = \left[\phi(a)\right]^n$ pour tout $a \in A$ et pour tout $n \in \mathbb{N}$.

b) Si a est inversible dans A, alors $\phi(a)$ est inversible dans B et :

$$\phi(a^{-1}) = \left[\phi(a)\right]^{-1}.$$

Propriété 5

a) Si A' est un sous-anneau de $(A, +, \cdot)$, alors $\phi(A')$ est un sous-anneau de $(B, +, \cdot)$.

b) Si B' est un sous-anneau de $(B, +, \cdot)$, alors $\phi^{-1}(B')$ [6] est un sous-anneau de $(A, +, \cdot)$.

[6] $\varphi^{-1}(B')$ désigne l'image réciproque de B' par φ.

Copyrighted material

B. Idéaux d'un anneau commutatif

1. Définition et propriétés

Définition 6

On dit qu'une partie non vide I de A est un **idéal** d'un anneau **commutatif** $(A, +, \cdot)$ lorsque :

(1) I est stable pour l'addition de A : $I + I \subset I$,

(2) $\forall (a, i) \in A \times I,\ ai \in I$: $IA \subset I$. ✎(7)

✎(7) Usuellement, le produit $a \cdot i$ est noté ai.

Remarque

$\{0_A\}$ et A sont des idéaux de $(A, +, \cdot)$. Ce sont les **idéaux triviaux** de l'anneau.

Tout idéal non trivial de $(A, +, \cdot)$ est appelé un **idéal propre** de l'anneau.

Propriété 6

Un idéal I de $(A, +, \cdot)$ est un sous-groupe de $(A, +)$.

☞ I est une partie non vide de A, stable pour l'addition.

De plus, pour tout $i \in I$, on a $(-1_A)i \in I$, c'est-à-dire $-i \in I$.

Propriété 7

Pour tout $a \in A$, l'ensemble aA des produits de a par tous les éléments de A ✎(8) est un idéal, appelé l'**idéal principal** engendré par a. On le note (a).

✎(8) $aA = \{ax / x \in A\}$.

☞ Soit $a \in A$. Alors aA contient $a1_a = a$.

Étant donné ab et ac dans aA, on a $ab + ac = a(b + c) \in aA$.

Étant donné $ab \in aA$ et $c \in A$, on a $c(ab) = a(bc) \in aA$.

Exemple 1 Dans l'anneau $\mathbb{Z}$ des entiers relatifs, tout sous-groupe de $(\mathbb{Z}, +)$ est un idéal.

Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$, avec $n \in \mathbb{Z}$, c'est-à-dire que c'est l'idéal principal engendré par n.

Exemple 2 **Somme d'idéaux**

Soit I et J des idéaux d'un anneau commutatif $(A, +, \cdot)$. Alors l'ensemble $I + J$ des sommes d'un élément de I et d'un élément de J est un idéal.

Il est immédiat que $I + J$ est stable pour l'addition et que 0_A appartient à $I + J$.

Étant donné $u \in I + J$, il existe $(i, j) \in I \times J$ tel que $u = i + j$.

Pour tout $a \in A$, on a : $au = a(i + j) = ai + aj$.

Comme I et J sont des idéaux, il vient $ai \in I$ et $aj \in J$ puis $au \in I + J$.

Ainsi, $I + J$ est un idéal de $(A, +, \cdot)$.

Propriété 8

Si un idéal I contient 1_A, on a $I = A$.

☞ Pour tout $a \in A$, on a $a1_A \in I$, c'est-à-dire $a \in I$, puis $A \subset I$.

Corollaire

Si un idéal I contient un élément inversible de A, alors $I = A$.

☞ On suppose que $u \in \mathbb{U}(A)$ est dans I. L'idéal I contient alors $a^{-1}a$, c'est-à-dire 1_A.

Copyrighted material

Propriété 9

L'intersection d'une familles d'idéaux d'un anneau commutatif est un idéal.

☞ Soit $(I_s)_{s\in S}$ une famille d'idéaux. Chacun des I_s étant stable pour l'addition, il en est de même pour leur intersection I.
Soit $a \in A$ et $i \in I$. Pour tout $s \in S$, on a $i \in I_s$ donc $ai \in I_s$, et il s'ensuit $ai \in I$.

Propriété 10

La réunion $\bigcup_{n\in\mathbb{N}} I_n$ d'une suite $(I_n)_{n\in\mathbb{N}}$ croissante [9] d'idéaux de $(A, +, \cdot)$ est un idéal.

[9] Au sens de l'inclusion.

☞ a) Les I_n n'étant pas vides, il en est de même pour leur réunion I.

b) Soit $i \in I$ et $a \in A$. Il existe $n \in \mathbb{N}$ tel que $i \in I_n$. Alors $ai \in I_n$ donne $a \in I$.

c) Soit i et j dans I. Il existe n et p tels que $i \in I_n$ et $j \in I_p$. Posons $q = \sup\{n, p\}$.
I_n et I_p étant inclus dans I_q, il vient $i + j \in I_q$ et donc $i + j \in I$.

Définition 7

Étant donné une partie X de A, l'intersection de tous les idéaux de $(A, +, \cdot)$ qui contiennent X est appelée l'idéal **engendré** par X. [10]

[10] C'est donc le plus petit idéal de A contenant la partie X.

Définition 8

Un idéal I de $(A, +, \cdot)$ est dit **maximal** s'il est différent de A et si, pour tout idéal J :

$$I \subset J \text{ et } I \neq J \Rightarrow J = A.$$

Exemple 3 Les idéaux maximaux de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$, avec p premier.

Les idéaux de $\mathbb{Z}$ sont les sous-groupes $n\mathbb{Z}$, avec $n \in \mathbb{N}$. Pour $n \in \mathbb{N} \setminus \{0, 1\}$, [11] l'idéal $n\mathbb{Z}$ n'est pas maximal si et seulement si : $\exists m \in \mathbb{N} \setminus \{0, 1\}$, $n\mathbb{Z} \subset m\mathbb{Z}$ et $n\mathbb{Z} \neq m\mathbb{Z}$.
Or $n\mathbb{Z} \subset m\mathbb{Z}$ équivaut à m divise n donc $n\mathbb{Z}$ n'est pas maximal si et seulement si n admet un diviseur strict. Les idéaux $n\mathbb{Z}$ non maximaux sont ainsi ceux pour lesquels n n'est pas premier.

[11] Les idéaux engendrés par 0 et par 1 sont les idéaux triviaux. Ils ne sont donc pas maximaux.

2. Idéaux et morphismes d'anneaux

Théorème 1

Soit $(A, +, \cdot)$ et $(B, +, \cdot)$ des anneaux et $\varphi : A \to B$ un morphisme d'anneaux.

a) $\operatorname{Ker}\varphi$ est un idéal de $(A, +, \cdot)$.

b) Si I est un idéal de $(A, +, \cdot)$, alors $\varphi(I)$ est un idéal de $(\varphi(A), +, \cdot)$. [12]

c) Si J est un idéal de $(B, +, \cdot)$, alors $\varphi^{-1}(J)$ est un idéal de $(A, +, \cdot)$.

[12] $\varphi(I)$ n'est pas nécessairement un idéal de $(B, +, \cdot)$, mais ceci est vrai quand φ est surjective.

☞ On sait que $\operatorname{Ker}\varphi$ est un sous-groupe de $(A, +)$, que $\varphi(I)$ est un sous-groupe de $(B, +)$, donc un sous-groupe de $(\varphi(A), +)$, et aussi que $\varphi^{-1}(J)$ est un sous-groupe de $(A, +)$. [13]

a) $\forall a \in A, \forall p \in \operatorname{Ker}\varphi$, $\varphi(ap) = \varphi(a)\varphi(p)$ donne $\varphi(ap) = \varphi(a)0_B = 0_B$ donc $ap \in \operatorname{Ker}\varphi$, d'où $A\operatorname{Ker}\varphi \subset \operatorname{Ker}\varphi$.

b) Soit $y \in \varphi(I)$ et $z \in \varphi(A)$. Il existe $x \in I$ et $t \in A$ tels que $y = \varphi(x)$, $z = \varphi(t)$.
On a donc $yz = \varphi(x)\varphi(t) = \varphi(xt)$.
Or, I étant un idéal de A, $xt \in I$ donc $\varphi(xt) \in \varphi(I)$, c'est-à-dire $yz \in \varphi(I)$.

c) Pour $x \in \varphi^{-1}(J)$ et $a \in A$, posons $y = \varphi(x)$ et $b = \varphi(a)$. On a $\varphi(xa) = \varphi(x)\varphi(a) = yb$.
Avec $y \in J$ et $b \in B$, on a $yb \in J$, c'est-à-dire $\varphi(ax) \in J$, donc $xa \in \varphi^{-1}(J)$.

[13] Pour chacun d'eux, il reste à vérifier la stabilité pour le produit par un élément de l'anneau.

Copyrighted material

3. Anneau-produit

Propriété 11

Si I et J sont des idéaux des anneaux commutatifs $(A, +, \cdot)$ et $(B, +, \cdot)$, alors $I \times J$ est un idéal de l'anneau-produit $(A \times B, +, \cdot)$.

☞ Produit de sous-groupes de $(A, +)$ et $(B, +)$, $I \times J$ est un sous-groupe de $(A \times B, +)$.
Soit $(u, v) \in I \times J$ et $(a, b) \in A \times B$. On a $(a, b) \cdot (u, v) = (au, bv)$.
Comme I est un idéal de A, on a $au \in I$ et, comme J est un idéal de B, on a $bv \in J$.
Donc $(au, bv) \in I \times J$ et $I \times J$ est bien un idéal de $A \times B$.

4. Corps

Rappelons [14] qu'un **corps** est un triplet $(K, +, \cdot)$ tel que :
(1) $(K, +, \cdot)$ est un anneau commutatif non nul,
(2) tout élément autre que 0_K est inversible.
Un morphisme de corps est un morphisme des anneaux sous-jacents.

[14] Voir Algèbre et Géométrie, MPSI, chapitre 6.

Définition 9

Un **sous-corps** d'un corps $(K, +, \cdot)$ est un sous-anneau L qui, pour les lois induites sur L par celles de K, est un corps. On dit alors que $(K, +, \cdot)$ est une **extension** du corps $(L, +, \cdot)$.

Propriété 12

Un anneau commutatif $(A, +, \cdot)$ non nul est un corps si et seulement si ses seuls idéaux sont les idéaux triviaux.

☞ a) Supposons que les seuls idéaux de $(A, +, \cdot)$ sont les idéaux triviaux $\{0_A\}$ et A.
Considérons $a \in A^* = A \setminus \{0_A\}$. L'idéal (a) engendré par a n'est pas l'idéal nul. C'est donc A. Comme l'idéal (a) est l'ensemble aA des produits de a par les éléments de A, il existe $b \in A$ tel que $a.b = 1_A$, ce qui montre que a est inversible. Ainsi, $(A, +, \cdot)$ est un corps.

b) Supposons que $(A, +, \cdot)$ soit un corps. Un idéal non nul contient un élément non nul et donc inversible. Contenant un élément inversible, un tel idéal ne peut être que A. [15]

[15] Corollaire de la propriété 8.

Exemple 4 Tout morphisme de corps est injectif.

Un morphisme f de corps K et K' étant un morphisme des anneaux sous-jacents, on a $f(0_K) = 0_{K'}$ et $f(1_K) = 1_{K'}$, donc f n'est pas l'application nulle.
Le noyau de f est un idéal de K qui n'est pas K, c'est donc $\{0_K\}$. Ainsi f est injective.

C. Arithmétique dans $\mathbb{K}[X]$

1. Division euclidienne [16]

[16] Voir Algèbre et Géométrie, MPSI, chapitre 10.

Théorème 2

Soit A et B dans $\mathbb{K}[X]$, [17] B non nul.
Il existe un couple unique (Q, R) de polynômes tel que : $A = BQ + R$, $\deg R < \deg B$.
Q est le **quotient** et R le **reste** dans la **division euclidienne** de A par B.

[17] $\mathbb{K}$ est $\mathbb{C}$ ou un sous-corps de $\mathbb{C}$.

$B \neq 0$ **divise** A lorsque le reste dans la division de A par B est nul.
A est **multiple** de B quand B **divise** A, ou quand $A = B = 0$.

Copyrighted material

2. Idéaux de $\mathbb{K}$ [X]

Propriété 13

Soit A élément de $\mathbb{K}[X]$ et (A) l'ensemble des multiples de A dans $\mathbb{K}[X]$.
(A) est un idéal de $\mathbb{K}[X]$ appelé **idéal principal engendré par** A.

C'est un cas particulier de la propriété **7**. Notons que si $A = 0$, alors $(A) = \{0\}$

Théorème 3

Dans $\mathbb{K}[X]$, tout idéal est principal.
On dit que $\mathbb{K}[X]$ est un **anneau principal**.

☞ Soit I un idéal de $\mathbb{K}[X]$.
Si $I = \{0\}$, il est engendré par 0.
Si $I \neq \{0\}$, soit D l'ensemble des degrés des éléments non nuls de I et n_0 le plus petit élément de D. Il existe $A \in I$ tel que $\deg(A) = n_0$: $\forall B \in I \setminus \{0\}$, $\deg(B) \geqslant \deg(A)$.
Formons la division euclidienne de B par A :

$$B = AQ + R,\ \deg(R) < \deg(A),$$

de $B \in I$ et $A \in I$, on déduit $AQ \in I$, puis $R = B - AQ \in I$.
Avec $\deg R < \deg A$ et $R \in I$, il vient $R = 0$ et par suite, $B \in (A)$.
On en déduit que $I \subset (A)$ et, comme il est immédiat que $(A) \subset I$, on a $I = (A)$.

Remarque

Deux générateurs d'un idéal non nul I de $\mathbb{K}[X]$ sont des polynômes associés.
En particulier, I admet un générateur unitaire unique.

3. PGCD [18]

[18] Ces propriétés ont été vues, sans la notion d'idéal, en Algèbre et Géométrie, MPSI, chapitre 10.

La somme $(A) + (B)$ des idéaux engendrés par A et B dans $\mathbb{K}[X]$ est un idéal de $\mathbb{K}[X]$.
On a $(A) + (B) \neq (0)$ si et seulement si A et B ne sont pas tous deux nuls.

Définition 10

Le **plus grand commun diviseur (PGCD)** de polynômes A et B non tous deux nuls est le générateur unitaire de l'idéal $(A) + (B)$. On le note $A \wedge B$.

Propriété 14

Le PGCD des polynômes A et B non tous deux nuls est l'unique polynôme unitaire qui appartient à $(A) + (B)$ et qui divise A et B.
Les diviseurs communs à A et B non tous deux nuls sont les diviseurs de $A \wedge B$.

Théorème 4

Théorème d'Euclide
Soit A et B deux polynômes non nuls.
S'il existe des polynômes Q et R tels que $A = BQ + R$, alors $A \wedge B = B \wedge R$.

Corollaire

Algorithme d'Euclide
Pour chercher le PGCD de A et B, on divise A par B :

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

$A \wedge B = B \wedge R$ ramène à des polynômes de degrés inférieurs à ceux du début.

Copyrighted material

4. Polynômes premiers entre eux

Définition 11

A et B dans $\mathbb{K}[X]$ sont **premiers entre eux** quand ils sont non nuls et que $A \wedge B = 1$.

Théorème 5

Théorème de Bézout

A et B non nuls sont premiers entre eux si et seulement si il existe U et V tels que $UA+VB = 1$.

Corollaire

Étant donné $(a, b) \in \mathbb{K}^2$, $X - a$ et $X - b$ sont premiers entre eux si et seulement si $a \neq b$.

Théorème 6

Théorème de Gauss

Si un polynôme A est premier avec B et divise le produit BC, alors A divise C.

Corollaire

a) $A \wedge BC = 1$ équivaut à $A \wedge B = 1$ et $A \wedge C = 1$.

b) $A \wedge B = 1$ implique $A \wedge BC = A \wedge C$.

c) A_1 divise B, A_2 divise B et $A_1 \wedge A_2 = 1$ implique A_1A_2 divise B.

d) Soit $A_1, \cdots, A_n$ des polynômes premiers entre eux deux à deux.
Si $\forall k \in \{1, \cdots, n\}$, A_k divise B, alors $A_1 \cdot A_2 \cdots A_n$ divise B.

5. PPCM

Définition 12

Si A, B sont des polynômes non nuls, le générateur unitaire de l'idéal $(A) \cap (B)$ est appelé le **plus petit commun multiple** de A et B. On le note $A \vee B$.

Théorème 7

Si A et B sont deux polynômes non nuls de coefficients dominants respectifs a et b, on a :

$$ab(A \wedge B) \cdot (A \vee B) = A \cdot B.$$

D. Divisibilité dans un anneau

1. Divisibilité dans un anneau intègre (19)

(19) Extension de la notion de divisibilité rencontrée dans les anneaux intègres $\mathbb{Z}$ et $\mathbb{K}[X]$.

Rappelons qu'un anneau A est dit intègre s'il est commutatif et si :

$$\forall (a, b) \in A^2,\ ab = 0_A \ \Rightarrow\ a = 0_A \text{ ou } b = 0_A.$$

Définition 13

Soit A un anneau intègre et a, b non nuls dans A.
On dit que a **divise** b s'il existe $c \in a$ tel que $ac = b$. On note alors $a|b$.

Copyrighted material

Propriété 15

Soit a et b non nuls dans un anneau intègre A, et (a), (b) les idéaux engendrés par a et b :
a divise b si et seulement si $(a) \supset (b)$.

☞ a) Supposons que a divise b. Il existe $c \in A$ tel que $ac = b$.
Pour tout $x \in A$, $bx = acx$ donne $bx \in aA$, donc $(b) \subset (a)$.

b) Si $(a) \supset (b)$, avec $b \in (b)$, on a $b \in (a) = aA$ et il existe $c \in A$ tel que $b = ac$.

Définition 14

Étant donné $a \in A$, les éléments au, avec u inversible dans A, sont appelés les **éléments associés** à a.

Propriété 16

Tout élément inversible dans A divise a.
Tout élément associé à a divise a.

✎(20) $\mathbb{U}(A)$ est le groupe des inversibles de A.

☞ Soit $u \in \mathbb{U}(A)$. ✎(20) Écrivons $a = 1_A a = \left(uu^{-1}\right)a = u\left(u^{-1}a\right)$. On voit ainsi que u divise a.
On a également $a = (au)u^{-1}$, ce qui montre que au divise a.

Propriété 17

Des éléments non nuls a et b d'un anneau intègre sont associés si et seulement si $aA = bA$.

☞ $(a) \supset (b)$ équivaut à a divise b, (propriété 15). Alors $(a) = (b)$, équivaut à $b|a$ et $a|b$, c'est-à-dire qu'il existe u et v dans A tels que $a = bu$ et $b = av$.

- On a donc $a = avu$, ou encore $\left(1_A - vu\right)a = 0_A$ et, puisque A n'a pas de diviseur de 0_A et que $a \neq 0_A$, il vient $1_A - vu = 0_A$, c'est-à-dire $vu = 1_A$.
Alors $a = bu$, avec u inversible, exprime que a et b sont associés.
- Si a et b sont associés, il existe u inversible tel que $a = bu$, donc $b = au^{-1}$.
On a donc $b|a$ et $a|b$; par suite $(a) = (b)$.

Définition 15

Un élément non nul a de A est qualifié d'**irréductible** lorsque ses seuls diviseurs sont les éléments inversibles de A et les éléments associés à a.

2. PGCD, PPCM

Définition 16

Un idéal I d'un anneau $(A, +, \cdot)$ est **principal** lorsque : $\exists x \in I,\ I = xA$.
Un **anneau principal** est un anneau intègre ✎(21) dont tout idéal est principal.

✎(21) Anneau commutatif et sans diviseur de zéro.

Définition 17

Soit a et b non nuls dans un anneau principal A.
Tout $d \in A$ tel que $aA + bA = dA$ est appelé un **PGCD** de a et b.

Remarques

1) Dans l'anneau principal A, il existe $d \in A$ tel que $(a) + (b) = (d)$. ✎(22)

✎(22) La somme de deux idéaux est un idéal.

Copyrighted material

2) Des PGCD de a et b sont associés. Cela découle de la propriété 17.

3) Si b divise a, alors b est un PGCD de a et b. En effet, on a $(b) \supset (a)$, donc :

$$(a) + (b) \subset (b) + (b) = (b)$$

et, avec $(b) \subset (a) + (b)$, il vient $(a) + (b) = (b)$.

Définition 18

Pour a et b non nuls dans un anneau principal A, tout $m \in A$ tel que $aA \cap bA = mA$ est appelé un **PPCM** de a et b.

Dans l'anneau principal A, il existe $m \in A$ tel que $(a) \cap (b) = (m)$. [23]

Des PPCM de a et b sont associés.

[23] Toute intersection d'idéaux est un idéal.

3. Entiers de Gauss

Définition 19

Les entiers de Gauss sont les nombres complexes $a + ib$ avec $(a, b) \in \mathbb{Z}^2$.

On note $\mathbb{Z}[i]$ l'ensemble de ces nombres.

Propriété 18

$\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$ et cet anneau $\mathbb{Z}[i]$ est principal. [24]

[24] C'est-à-dire que tout idéal de $\mathbb{Z}[i]$ est principal.

☞ Soit $z = a + ib$ et $z' = a' + ib'$, $(a, b, a', b') \in \mathbb{Z}^4$. Alors $z + z' = (a + a') + i(b + b')$ et $zz' = (aa' - bb') + i(ab' + a'b)$ sont dans $\mathbb{Z}[i]$.

Soit J un idéal non nul de $\mathbb{Z}[i]$ et $J^* = J \setminus \{0\}$. Pour $z = a + ib$, $(a, b) \in \mathbb{Z}^2$, on a $|z|^2 \in \mathbb{N}$.

L'ensemble $\left\{ |z|^2 , z \in J^* \right\}$ est une partie non vide et minorée de $\mathbb{N}$. Soit $m \in J^*$ tel que :

$$\forall z \in J^*, |m|^2 \leqslant |z|^2.$$

Pour $z \in J$, posons $\dfrac{z}{m} = s + it$, avec $(s, t) \in \mathbb{Q}^2$.

Il existe $(a, b) \in \mathbb{Z}^2$ tel que $|s - a| \leqslant \dfrac{1}{2}$ et $|t - b| \leqslant \dfrac{1}{2}$.

Posons alors $q = a + ib$ et $r = z - qm$. Il vient :

$$r = \left(\frac{z}{m} - q\right) m = \big((s - a) + (t - b)i\big) m \text{ donc } |r|^2 = \left((s - a)^2 + (t - b)^2\right) |m|^2 < |m|^2.$$

Avec $z \in J$, $m \in J$ et $q \in \mathbb{Z}[i]$, il vient $r \in J$. Le choix de m montre alors que $r = 0$ et il s'ensuit que $z = mq$. On a donc $J \subset (m)$ et, avec $(m) \subset J$, il vient $J = (m)$.

Exemple 5 Les éléments inversibles de $\mathbb{Z}[i]$ sont 1, i, -1 ou $-i$.

Si $a + ib$, $(a, b) \in \mathbb{Z}^2$ est inversible dans $\mathbb{Z}[i]$, il existe $(c, d) \in \mathbb{Z}^2$ tel que $(a + ib)(c + id) = 1$. On en déduit $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = 1$ (en comparant les modules). Avec $a^2 + b^2$ et $c^2 + d^2$ entiers naturels, il vient $a^2 + b^2 = 1$ donc $\big(|a| = 1 \text{ et } b = 0\big)$ ou $\big(a = 0 \text{ et } |b| = 1\big)$. On a ainsi montré que :

$$\mathbb{U}\big(\mathbb{Z}[i]\big) \subset \{1, i, -1, -i\}.$$

Réciproquement, il est clair que chacun de ces quatre éléments est inversible :

$$1 \cdot 1 = 1 \ , \ (-1) \cdot (-1) = 1 \ , \ i \cdot (-i) = 1,$$

donc $\mathbb{U}\big(\mathbb{Z}[i]\big) = \{1, i, -1, -i\}$.

Copyrighted material

Exemple 6 Étant donné a et b non nuls dans $\mathbb{Z}[i]$ tels que $a = bq + r$, avec q, r dans $\mathbb{Z}[i]$, les PGCD de a et b sont les PGCD de b et r.

Soit d un PGCD de a et b et d' un PGCD de b et r. On a $(d) = (a) + (b)$, donc $d \in (a) + (b)$ et, par suite, il existe λ, μ dans $\mathbb{Z}[i]$ tels que $d = \lambda a + \mu b$. Il vient alors :

$$d = \lambda(bq + r) + \mu b = (\lambda q + \mu)b + \lambda r.$$

Donc d est dans $(b) + (r)$ c'est-à-dire dans (d').

De même, il existe u et v dans $\mathbb{Z}[i]$ tels que $d' = ub + vr$ d'où :

$$d' = ub + v(a - bq) = va + (u - vq)b.$$

Donc d' est dans $(a) + (b)$, c'est-à-dire dans (d).

Ainsi, chacun des éléments d et d' divise l'autre, ils sont donc associés.

Remarque

Si d est un PGCD de a et b, les autres sont ses associés, c'est-à-dire d, $-d$, id et $-id$.

Copyrighted material

Méthodes

L'essentiel

I. Idéaux d'un anneau commutatif

✔ **Si l'on veut** établir une propriété d'un idéal,

- **on peut** revenir à la définition, c'est souvent le meilleur moyen.

→ Voir *Mise en œuvre*, exercices 1, 2

✔ **Si l'on veut** montrer qu'un idéal I est maximal,

- **on peut** considérer un idéal contenant I et $a \in A \setminus I$.

→ Voir *Mise en œuvre*, exercice 2

II. Polynômes cyclotomiques

✔ Ces polynômes font intervenir le groupe des racines $n^{\text{èmes}}$ de 1, la fonction indicatrice d'Euler et les générateurs d'un groupe cyclique.

✔ **Si l'on veut** former le polynôme cyclotomique d'ordre n,

- **on peut** utiliser les racines primitives d'ordre n de 1 ;

→ Voir *Mise en œuvre*, exercice 3

- **on peut** utiliser les diviseurs dans $\mathbb{N}$ de n.

→ Voir *Mise en œuvre*, exercice 4

III. Polynômes à coefficients entiers ou rationnels

✔ Le choix d'étudier principalement ces polynômes est guidé par les liens naturels avec l'arithmétique des entiers.

✔ **Si l'on veut** établir la divisibilité des coefficients par p premier,

- **on peut** se ramener à un polynôme sur le corps $\mathbb{Z}/p\mathbb{Z}$:

→ Voir *Mise en œuvre*, exercice 5

- **on peut** utiliser le PGCD des coefficients, en extension du PGCD de deux entiers.

→ Voir *Mise en œuvre*, exercice 6

✔ **Si l'on veut** étudier un polynôme à coefficients rationnels,

- **on peut** se ramener à un polynôme à coefficients entiers.

→ Voir *Mise en œuvre*, exercices 6, 7, 8

IV. Polynômes de Lagrange

✔ Ce thème sera vu avec une autre approche au chapitre suivant. On en étudie la définition et un exemple d'application au calcul du reste dans la division par un polynôme scindé à racines simples.

→ Voir *Mise en œuvre*, exercices 9, 10

Copyrighted material

Mise en œuvre

I. Idéaux d'un anneau commutatif

Ex. 1

Soit A un anneau commutatif. Étant donné un idéal I, on note $\sqrt{I} = \{x \in A \,/\, \exists\, n \in \mathbb{N}^*,\ x^n \in I\}$.

1) Montrer que $\sqrt{I}$ est un idéal contenant I.

2) Soit I et J des idéaux de A. Montrer que : $I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J}$ et que $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

3) Montrer que, pour tout idéal I, $\sqrt{\sqrt{I}} = \sqrt{I}$.

4) Étant donné des idéaux I et J de A, montrer que $\sqrt{I} + \sqrt{J} \subset \sqrt{I+J}$.

Solution

1) Pour $x \in I$, on a $x \in \sqrt{I}$, donc $I \subset \sqrt{I}$.

(1) Soit $x \in \sqrt{I}$ et $a \in A$. Il existe $n \in \mathbb{N}^*$ tel que $x^n \in I$, donc $a^n x^n \in I$, et $ax \in \sqrt{I}$.

(2) Soit x, y dans $\sqrt{I}$ et p, q dans $\mathbb{N}^*$ tels que $x^p \in I$ et $y^q \in I$.

$$(x+y)^{p+q} = \sum_{k=0}^{p+q} \binom{k}{p+q} x^k y^{p+q-k}.$$

Pour $k \geqslant p$, on a $x^k \in I$ et donc $\binom{k}{p+q} x^k y^{p+q-k} \in I$.

Pour $k \leqslant p$, on a $p+q-k \geqslant q$, donc $y^k \in I$ et $\binom{k}{p+q} x^k y^{p+q-k} \in I$.

Par suite, $(x+y)^{p+q} \in I$, donc $x+y \in \sqrt{I}$.

2) (1) On suppose $I \subset J$.

Soit $x \in \sqrt{I}$. De $x^p \in I$, on déduit $x^p \in J$ puis $x \in \sqrt{J}$.

(2) De $I \cap J \subset I$ et $I \cap J \subset J$, on déduit $\sqrt{I \cap J} \subset \sqrt{I}$ et $\sqrt{I \cap J} \subset \sqrt{J}$, c'est-à-dire : $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. (i)

Soit $x \in \sqrt{I} \cap \sqrt{J}$. Il existe n et p dans $\mathbb{N}^*$ tels que $x^n \in I$ et $x^p \in J$. On a donc $x^{n+p} = x^n x^p$ dans I et dans J et donc dans $I \cap J$. Il s'ensuit :

$x \in \sqrt{I \cap J}$, puis $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cap J}$. (ii)

3) De $I \subset \sqrt{I}$, on déduit que $\sqrt{I} \subset \sqrt{\sqrt{I}}$.

Soit $x \in \sqrt{\sqrt{I}}$. Il existe $n \in \mathbb{N}^*$ tel que $x^n \in \sqrt{I}$. Il existe alors $p \in \mathbb{N}^*$ tel que $(x^n)^p \in I$, c'est-à-dire $x^{np} \in I$ et donc $x \in \sqrt{I}$.

Donc $\sqrt{\sqrt{I}} \subset \sqrt{I}$ et finalement $\sqrt{\sqrt{I}} = \sqrt{I}$.

4) $\sqrt{I} + \sqrt{J} \subset \sqrt{I+J}$ découle de $I \subset I+J$ et $J \subset I+J$.

Commentaires

$x^1 \in I$.

$a^n x^n = (ax)^n \in I$.

Formule du binôme dans l'anneau commutatif A.

I étant un idéal, $x^k y^{p+q-k} \in I$ et puisque $\binom{k}{p+q}$ est un entier, $\binom{k}{p+k} x^k y^{p+q-k} \in I$.

(i) et (ii) donnent $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Voir la première question.

$\sqrt{I} \subset \sqrt{I+J}$ et $\sqrt{J} \subset \sqrt{I+J}$.

Ex. 2

Soit A l'anneau commutatif des applications de $\mathbb{R}$ dans $\mathbb{R}$, et t un réel fixé. Notons $I = \{f \in A,\ f(t) = 0\}$.

Montrer que I est un idéal maximal.

Indications

Un idéal I de A est dit maximal quand il est différent de A et que, pour tout idéal J contenant strictement I, on a $J = A$; c'est la définition et elle contient la méthode.

Solution

1) Soit $f \in I$ et $g \in A$. On a $fg(t) = f(t)g(t) = 0$ et donc $fg \in I$.
Soit f et g dans I. $f(t) = 0$ et $g(t) = 0$ donne $(f+g)(t) = 0$, donc :
$$f + g \in I.$$
Comme la fonction nulle est dans I, il vient que I est un idéal.

2) Soit J un idéal de A contenant strictement I.

Soit $g \in J \setminus I$. Pour tout $f \in A$, considérons $\lambda = \dfrac{f(t)}{g(t)}$.
La fonction $h = f - \lambda g$ appartient à I.
Avec $f = h + \lambda g \in J$, il vient $A \subset J$, donc $J = A$.

Commentaires

$f(t)=0$.
Stabilité pour l'addition.

I est non vide.

On a $g(t)\neq 0$.

Elle prend la valeur 0 en t.
f est somme d'un élément de J et d'un élément de $I \subset J$.

II. Polynômes cyclotomiques

Ex. 3

Étant donné $n \in \mathbb{N}^*$, on note D_n l'ensemble des générateurs du groupe $\mathbb{U}_n$ et on pose $\Phi_n(X) = \prod_{\omega \in D} (X - \omega)$.

Préciser $\Phi_n(X)$ quand n est premier et expliciter Φ_n pour $1 \leqslant n \leqslant 9$.

Indications

Φ_n est appelé le polynôme cyclotomique d'indice n. Il est de degré $\varphi(n)$ où φ est la fonction indicatrice d'Euler.

Solution

Quand n est premier, on a $D_n = \mathbb{U}_n \setminus \{1\}$ donc $\Phi_n(X) = \dfrac{X^n - 1}{X - 1}$.

Pour n premier, $\Phi_n(X) = \sum_{r=0}^{n-1} X^r$. En particulier :

$$\Phi_3(X) = X^2 + X + 1,$$
$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1,$$
$$\Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,$$
$$\Phi_1(X) = X - 1 \text{ car } D_1 = \{1\},$$
$$\Phi_2(X) = X + 1 \text{ car } D_2 = \{-1\},$$
$$\Phi_4(X) = (X - i)(X + i) = X^2 + 1 \text{ car } D_4 = \{i, -1\},$$
$$\Phi_6(X) = (X + j)(X + \bar{j}) = X^2 - X + 1.$$

En effet, avec $\omega = \exp\left(\dfrac{i\pi}{3}\right)$, on a $\omega^k \in D_6$ si et seulement si $k \wedge 6 = 1$.

En notant que $D_8 = \mathbb{U}_8 \setminus \mathbb{U}_4$, il vient $\Phi_8(X) = \dfrac{X^8 - 1}{X^4 - 1} = X^4 + 1$.

De même, $D_9 = \mathbb{U}_9 \setminus \mathbb{U}_3$ donne $\Phi_9(X) = \dfrac{X^9 - 1}{X^3 - 1} = X^6 + X^3 + 1$.

Commentaires

$X^n - 1 = \prod_{\omega_k \in \mathbb{U}_n} (X - \omega_k)$.

$\mathbb{U}_2 = \{-1, 1\}$.

$\mathbb{U}_4 = \{1, -1, i, -i\}$.
$e^{i\frac{\pi}{3}} = -e^{4i\frac{\pi}{3}} = -j^2$
$e^{5i\frac{\pi}{3}} = -e^{2i\frac{\pi}{3}} = -j$

Vérification aisée.

Copyrighted material

Ex. 4

Montrer que, pour $n \in \mathbb{N}^*$, on a $X^n - 1 = \prod_{d|n} \Phi_d(X)$ où le produit porte sur les diviseurs de n dans $\mathbb{N}$.

Montrer que Φ_n est à coefficients dans $\mathbb{Z}$ et que son coefficient dominant est 1. Calculer Φ_{15}.

Indications

$\mathbb{U}_n$ est la réunion disjointe des D_d, avec d diviseur de n dans $\mathbb{N}$ et D_d ensemble des générateurs du groupe cyclique $\mathbb{U}_d$.

Solution

1) La partition $\mathbb{U}_n = \bigcup_{d|n} D_d$ donne :

$$X^n - 1 = \prod_{\omega \in \mathbb{U}_n} (X - \omega) = \prod_{d|n} \Big(\prod_{\omega \in D_d} (X - \omega) \Big) = \prod_{d|n} \Phi_d(X).$$

2) Pour $n \in \mathbb{N}^*$, on pose $\Psi_n(X) = \dfrac{X^n - 1}{\Phi_n(X)}$.

$\Phi_1(X) = X - 1$ est dans $\mathbb{Z}[X]$ et $\operatorname{dom} \Phi_1 = 1$.
Supposons que $\forall k \in \mathbb{N}^*,\ k < n \ \Rightarrow\ \Phi_k(X) \in \mathbb{Z}[X]$ et $\operatorname{dom} \Phi_k = 1$.
Alors $\Psi_n(X)$ est un produit de polynômes à coefficients entiers, donc $\Psi_n(X) \in \mathbb{Z}[X]$. Produit de polynômes de coefficient dominant 1, Ψ_n a 1 pour coefficient dominant.
Quotient de $X^n - 1$ par $\Psi_n \in \mathbb{Z}[X]$ avec $\operatorname{dom} \Psi_n = 1$, le polynôme Φ_n est à coefficients entiers et $\operatorname{dom} \Phi_n = 1$ car $\operatorname{dom}(X^n - 1) = 1$.

3) On a $\Phi_1 \Phi_3 \Phi_5 \Phi_{15} = X^{15} - 1$. Avec :

$$\Phi_1(X) = X - 1,$$

$$\Phi_3(X) = X^2 + X + 1 = \frac{X^3 - 1}{X - 1},$$

$$\Phi_5(X) = X^4 + X^3 + X^2 + X + 1 = \frac{X^5 - 1}{X - 1}.$$

il vient $\Phi_{15}(X) = \dfrac{(X-1)(X^{15}-1)}{(X^3-1)(X^5-1)} = \dfrac{X^{10} + X^5 + 1}{X^2 + X + 1}$, d'où :

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1.$$

Commentaires

On obtient une partition de $\mathbb{U}_n$ en regroupant les éléments de même ordre d et on sait que d est un diviseur de n.

C'est le produit des $\Phi_d(X)$ pour d diviseur de n, avec $1 \leqslant d < n$.
$\operatorname{dom} \Phi_1$ désigne le coefficient dominant de Φ_1.
On amorce une preuve par récurrence.

Considérer l'agorithme de la division euclidienne.

Exercice précédent.

$\frac{X^{15}-1}{X^5-1} = X^{10} + X^5 + 1$
$\frac{X^3-1}{X-1} = X^2 + X + 1.$

III. Polynômes à coefficients entiers ou rationnels

Ex. 5

1) Soit p un nombre premier. On note $\overline{a}$ la classe modulo p de $a \in \mathbb{Z}$.

Pour $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, on pose $\overline{P} = \sum_{k=0}^{n} \overline{a_k} X^k \in (\mathbb{Z}/p\mathbb{Z})[X]$.

Montrer que $P \mapsto \overline{P}$ est un morphisme des anneaux $\mathbb{Z}[X]$ et $(\mathbb{Z}/p\mathbb{Z})[X]$.

2) Soit A et B dans $\mathbb{Z}[X]$. Montrer que, si p divise tous les coefficients de AB, alors il divise tous ceux de A ou il divise tous ceux de B.

Indications

p étant premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc $(\mathbb{Z}/p\mathbb{Z})[X]$ est un anneau intègre.

Solution

1) Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et $Q = \sum_{k=0}^{n} b_k X^k \in \mathbb{Z}[X]$. Le coefficient de X^k dans $\overline{P+Q}$ est $\overline{a_k + b_k} = \overline{a_k} + \overline{b_k}$; c'est donc celui de $\overline{P} + \overline{Q}$.

Le coefficient de X^k dans $\overline{PQ}$ est $\overline{\sum_{0 \leqslant j \leqslant k} a_j b_{k-j}} = \sum_{0 \leqslant j \leqslant k} \overline{a_j b_{k-j}}$; c'est aussi celui de $\overline{P}\,\overline{Q}$.

2) p divise tous les coefficients de P équivaut à $\overline{P} = \overline{0}$.

Si p divise tous les coefficients de AB, alors $\overline{AB} = \overline{0}$, donc $\overline{A}\,\overline{B} = \overline{0}$.

Il s'ensuit $\overline{A} = \overline{0}$ ou $\overline{B} = \overline{0}$, d'où le résultat.

Commentaires

$n \geqslant \sup\{\deg P, \deg Q\}$.

En notant $\varphi : P \mapsto \overline{P}$ on vérifie $\varphi(P+Q) = \varphi(P) + \varphi(Q)$, $\varphi(PQ) = \varphi(P)\varphi(Q)$ et on note que $\varphi(1) = \overline{1}$ est une évidence.

$\overline{a_k} = \overline{0}$ si et seulement si $p \mid a_k$.

$(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre.

Ex. 6

Étant donné $P \in \mathbb{Z}[X]$, $P \neq 0$, on note $\gamma(P)$ le PGCD des coefficients de P (c'est le générateur entier naturel du sous-groupe de $(\mathbb{Z}, +)$ engendré par les coefficients de P).

1) Soit P et Q dans $\mathbb{Z}[X] \setminus \{0\}$. Montrer que, si $\gamma(P) = 1$ et $\gamma(Q) = 1$, alors $\gamma(PQ) = 1$.

2) En déduire que $\gamma(PQ) = \gamma(P)\,\gamma(Q)$.

3) Soit A et B dans $\mathbb{Q}[X]$ et non nuls, tels que $AB \in \mathbb{Z}[X]$.

Montrer qu'il existe r rationnel non nul tel que rA et $\frac{1}{r}B$ soient dans $\mathbb{Z}[X]$.

Indications

$\gamma(P)$ est appelé le contenu de P.

1) On procédera par l'absurde en utilisant l'exercice précédent.

2) On se ramènera à des polynômes de contenus égaux à 1.

Solution

1) Si un nombre premier p divise $\gamma(PQ)$, il divise tous les coefficients de PQ, donc tous ceux de P ou tous ceux de Q, ce qui est contradictoire avec $\gamma(P) = 1$ et $\gamma(Q) = 1$.

2) Pour $P \in \mathbb{Z}[X]$, $P \neq 0$, et n entier, on a $\gamma(nP) = |n|\,\gamma(P)$.

Notons $\mathcal{U} = \{P \in \mathbb{Z}[X],\ P \neq 0 \text{ et } \gamma(P) = 1\}$.

On a $\gamma(P) = n \in \mathbb{N}^*$ si et seulement si $\frac{1}{n}P$ appartient à $\mathcal{U}$.

$R = \frac{P}{\gamma(P)}$ et $S = \frac{Q}{\gamma(Q)}$ sont dans $\mathcal{U}$, donc $\gamma(RS) = 1$.

Avec $PQ = \gamma(P)\,\gamma(Q)RS$, il vient alors :

$$\gamma(PQ) = \gamma(P)\,\gamma(Q)\,\gamma(RS),$$

donc :

$$\gamma(PQ) = \gamma(P)\,\gamma(Q).$$

3) Soit a le PPCM des dénominateurs des coefficients de A. Alors aA est à coefficients entiers. Posons $P = \frac{a}{\gamma(aA)}A$.

En réduisant $\frac{a}{\gamma(aA)}$, il existe a' et b' premiers entre eux tels que :

$$A = \frac{b'}{a'}P.$$

Commentaires

Exercice précédent.

Immédiat par définition d'un contenu.

Question précédente.

P est ainsi dans $\mathcal{U}$.

a', b', c', d' entiers naturels non nuls.

Copyrighted material

De même il existe $Q \in \mathbb{U}$ et c', d' premiers entre eux tels que :

$$B = \frac{d'}{c'}Q.$$

Avec $a'c'AB = b'd'PQ$, il vient $a'c'\gamma(AB) = b'd'$.

On en déduit qu'il existe u et v dans $\mathbb{N}^*$ tels que $d' = ua'$ et $b' = vc'$. Théorème de Gauss.

Posons enfin $r = \frac{a'}{c'}$, il vient $rA = vP$ et $\frac{1}{r}B = uQ$ puis $AB = (vP)(uQ)$ est le produit de deux polynômes à coefficients entiers.

Ex. 7

Soit P un polynôme à coefficients entiers et de degré au moins 1.

Montrer que P est irréductible dans $\mathbb{Q}[X]$ si et seulement si il est irréductible dans $\mathbb{Z}[X]$.

Indications

Dans un sens, c'est banal. Pour l'autre, utiliser la fin de l'exercice précédent.

Solution

1) Si P n'est pas le produit de polynômes non constants à coefficients dans $\mathbb{Q}$, il n'est évidemment pas produit de polynômes non constants à coefficients dans $\mathbb{Z}$. — Condition nécessaire.

2) Supposons que P soit le produit de polynômes non constants A et B à coefficients rationnels. — Condition suffisante.

Il existe donc des polynômes non constants U et V à coefficients entiers tels que $AB = UV$ et $P = UV$ montre que P est réductible dans $\mathbb{Z}[X]$. — Exercice précédent, dernière question.

Commentaires

Condition nécessaire.

Condition suffisante.

Exercice précédent, dernière question.

Ex. 8

Soit $a_1, a_2, \ldots, a_q$ des entiers naturels distincts, $A = \prod_{k=1}^{q}(X - a_k)$ et $P = A - 1$.

On suppose que P est le produit QR de polynômes non constants et à coefficients entiers.

1) Montrer que A divise $Q^2 - 1$ et $R^2 - 1$ et que les quotients B et C sont constants.

2) Établir une contradiction et en déduire que P est irréductible dans $\mathbb{Q}[X]$.

Indications

1) On utilisera $P(a_k)$. On exploitera ensuite les degrés.

2) On établira que $Q^2 = 1 - A$.

En conclusion, pour tout $q \in \mathbb{N}^*$, il existe $P \in \mathbb{Z}[X]$ et de degré q qui est irréductible dans $\mathbb{Q}[X]$.

Solution

1) $P(a_k) = -1$, donc $Q(a_k)R(a_k) = -1$. Comme $Q(a_k)$ et $R(a_k)$ sont des entiers, l'un vaut 1 et l'autre vaut -1. — Q et R sont à coefficients entiers et a_k est un entier.

Ainsi, $Q^2(a_k) = 1$ et $R^2(a_k) = 1$. Prenant la valeur 0 en chacun des a_k, les polynômes $Q^2 - 1$ et $R^2 - 1$ sont divisibles par A. — Les a_k sont deux à deux distincts.

$Q^2 = 1 + AB$ et $R^2 = 1 + AC$ assure que B et C ne sont pas nuls. Il vient alors $2\deg Q = \deg A + \deg B$, $2\deg R = \deg A + \deg C$ donc : — Q et R ne sont pas constants.

$$2\deg Q + 2\deg R = 2\deg A + \deg B + \deg C.$$

Or $\deg Q + \deg R = \deg A$, on en déduit donc $\deg B = \deg C = 0$ et B, C sont constants. — $QR = A - 1$.

Commentaires

Q et R sont à coefficients entiers et a_k est un entier.

Les a_k sont deux à deux distincts.

Q et R ne sont pas constants.

$QR = A - 1$.

2) $(AB+1)(AC+1) = Q^2R^2 = P^2 = (A-1)^2$ implique $B = C = -1$.

Alors $Q^2 = R^2 = 1 - A$, ce qui est impossible car $\lim_{x \to +\infty} A(x) = +\infty$.

L'hypothèse de réductibilité de P dans $\mathbb{Z}[X]$ est donc contradictoire. L'irréductibilité de P dans $\mathbb{Q}[X]$ découle alors de son irréductibilité dans $\mathbb{Z}[X]$.

Les constantes B et C sont les racines de X^2+2X+1.

Donc $1-A$ prend des valeurs négatives.

Voir l'exercice précédent.

IV. Polynômes de Lagrange

Ex. 9

Soit $n \in \mathbb{N}^*$ et $(x_0, \ldots, x_n)$ une famille de $n+1$ éléments deux à deux distincts d'un corps K.

1) Montrer que, pour $i \in [\![0, n]\!]$, $L_i = \prod_{0 \leqslant k \leqslant n,\ k \neq i} \frac{X - x_k}{x_i - x_k}$ est l'unique élément de $K[X]$ vérifiant :

(1) $\deg L_i \leqslant n$,

(2) $L_i(x_i) = 1$,

et (3) $\forall j \in [\![0, n]\!] \setminus \{i\},\ L_i(x_j) = 0$.

2) Montrer que, pour tout $(b_0, \ldots, b_n) \in K^{n+1}$, il existe un unique $L \in K[X]$ tel que :

$$\deg L \leqslant n \quad \text{et} \quad \forall k \in [\![0, n]\!],\ L(x_k) = b_k.$$

3) Quels sont les polynômes $P \in K[X]$ tels que $\forall k \in [\![0, n]\!],\ P(x_k) = b_k$?

Indications

Cette famille de polynômes, dits polynômes interpolateurs de Lagrange, est facile à mettre en place. Elle joue un rôle important et sera vue sous un autre angle dans le chapitre «Espaces vectoriels».

Solution

1) Si L_i et M_i vérifient les propriétés (1), (2) et (3), leur différence est de degré au plus n et prend la valeur 0 en $n+1$ éléments distincts, c'est donc le polynôme nul.

Il est immédiat que L_i prend la valeur 1 en x_i et la valeur 0 en x_j, $j \neq i$.

2) L'unicité de L se prouve comme celle des L_i.

Le polynôme $b_k L_k$ prend la valeur b_k en x_k et la valeur 0 en x_j, $j \neq k$.

Alors le polynôme $L = \sum_{k=0}^{n} b_k L_k$ convient.

3) Soit $P \in K[X]$ prenant la valeur b_k en x_k, pour $k \in [\![0, n]\!]$. Alors $P - L$ prend la valeur 0 en tout x_k, $k \in [\![0, n]\!]$.

Donc $P - L$ est un multiple de $\prod_{k=0}^{n} (X - x_k)$.

Tout polynôme $P = L + Q(X) \prod_{k=0}^{n} (X - x_k)$, avec $Q \in K[X]$ convient.

Commentaires

Unicité. C'est en général le premier point à étudier.

L_i est construit «sur mesure».

On exploite les polynômes d'interpolation.

On a bien $\deg L \leqslant n$.

On a établi une condition nécessaire.

Condition suffisante.

Copyrighted material

Ex. 10

Soit a, b, c trois réels distincts et P dans $\mathbb{R}[X]$.

Calculer le reste dans la division de P par $(X-a)(X-b)(X-c)$.

Indications

Le reste R est de degré au plus égal à 2 et ses valeurs en a, b, c, sont respectivement $P(a)$, $P(b)$ et $P(c)$.

Solution

Posons $L_1 = \dfrac{(X-b)(X-c)}{(a-b)(a-c)}$ et L_2, L_3 par permutations circulaires.

$P = (X-a)(X-b)(X-c)Q + R$ donne :

$$R(a) = P(a),$$

$$R(b) = P(b),$$

et $$R(c) = P(c).$$

Avec $\deg R \leqslant 2$, il s'ensuit $R = P(a)L_1 + P(b)L_2 + P(c)L_3$.

Commentaires

Polynômes interpolateurs de a, b, c.

Q et R dans $\mathbb{R}[X]$.

Exercice précédent, 2).

Exercices

Niveau 1

Ex. 1

Soit I un idéal d'un anneau commutatif A. Montrer que la relation binaire $\mathcal{R}_I$ définie sur A par :

$$x \mathcal{R}_I y \iff x - y \in I$$

est une relation d'équivalence compatible avec les opérations de A.

Ex. 2

Sur un anneau commutatif A, soit $\mathcal{R}$ une relation d'équivalence compatible avec les opérations de A.

Montrer que la classe de 0_A est un idéal I de A et que :

$$x \mathcal{R} y \iff x - y \in I.$$

Ex. 3

Montrer que l'ensemble N des éléments nilpotents d'un anneau commutatif A est un idéal de A.

Ex. 4

Soit a, b, c deux à deux distincts dans $\mathbb{R}$. Réduire :

$$\frac{(X-b)(X-c)}{(a-b)(a-c)} + \frac{(X-c)(X-a)}{(b-c)(b-a)} + \frac{(X-a)(X-b)}{(c-a)(c-b)}.$$

Ex. 5

Soit a et b distincts dans un corps $\mathbb{K}$, et $n \in \mathbb{N}^*$.

1) Montrer qu'il existe un couple $(P, Q) \in \mathbb{K}[X]^2$ unique tel que $\deg P < 2n$, $\deg Q < 2n$ et :

$$(X-a)^{2n}P + (X-b)^{2n}Q = 1.$$

2) Montrer que P et Q vérifient :

$$P(a+b-X) = Q(X) \text{ et } Q(a+b-X) = P(X).$$

Niveau 2

Idéaux

Ex. 6

Soit E un ensemble non vide.

Pour tous sous-ensembles A et B de E, la différence symétrique de A et B est :

$$(A \setminus B) \cup (B \setminus A).$$

On la note $A \Delta B$.

1) Vérifier que $\left(\mathcal{P}(E), \Delta, \cap\right)$ est un anneau commutatif.

2) Étant donné $a \in E$, on pose :

$$I_a = \left\{X \in \mathcal{P}(E), a \notin X\right\}.$$

Montrer que I_a est un idéal de l'anneau précédent.

3) Montrer que l'idéal I_a est maximal.

Ex. 7

Soit $(K, +, \cdot)$ et $(K', +, \cdot)$ des corps.

Montrer que l'anneau-produit $K \times K'$ n'est pas un corps et déterminer les idéaux de cet anneau.

Ex. 8

Soit K un corps et A un sous-anneau de K tel que :

$$\forall x \in K^* = K \setminus \{0_K\}, x \in A \text{ ou } \frac{1}{x} \in A.$$

1) Donner un exemple de telle situation.

2) Montrer que l'ensemble M des éléments de A, non inversibles dans A, est un idéal maximal de A.

Entiers de Gauss

Ex. 9

Soit $p \in \mathbb{N}^*$ qui est la somme des carrés de deux entiers.

Montrer qu'il n'est pas irréductible dans $\mathbb{Z}[i]$.

Ex. 10

Dans $\mathbb{Z}[i]$, calculer un pgcd de $11 + 7i$ et $3 + 7i$.

Copyrighted material

Polynômes

Ex. 11

Soit $a_1, \dots, a_n$ des entiers naturels distincts. Montrer que le polynôme $P \in \mathbb{Z}[X]$:

$$P = 1 + \prod_{k=1}^{n} (X - a_k)^2$$

est irréductible dans $\mathbb{Z}[X]$.

Ex. 12

Soit $P_1, \dots, P_n$ une famille de n polynômes réels deux à deux premiers entre eux.

On considère aussi une famille $Q_1, \dots, Q_n$ de polynômes réels.

Montrer qu'il existe $Q \in \mathbb{R}[X]$ tel que :

$$\forall k \in [\![1, n]\!],\ P_k \text{ divise } Q - Q_k.$$

Niveau 3

Ex. 13

Déterminer les couples $(P, Q) \in \mathbb{R}[X]^2$ tels que :

$$P^2 + (1 - X^2)Q^2 = 1.$$

Ex. 14

Soit A, B et C dans $\mathbb{C}[X]$, deux à deux premiers entre eux et tels que $A^2 + B^2 = C^2$.

1) Montrer que $C + B$ et $C - B$ sont des carrés de polynômes dans $\mathbb{C}[X]$.

2) En déduire les expressions de A, B et C.

Ex. 15

Montrer qu'il n'existe aucun polynôme non constant à coefficients entiers relatifs ne prenant sur $\mathbb{Z}$ que des valeurs qui soient toutes des nombres premiers.

Ex. 16

Formules de Cardan-Tartaglia

Soit $T(X) = X^3 + pX + q \in \mathbb{C}[X]$ de racines x_1, x_2 et x_3.

1) Montrer qu'il existe un unique couple $(u, v) \in \mathbb{C}^2$ tel que :

$$x_1 = u + v\ ,\quad x_2 = uj + vj^2 \quad \text{et} \quad x_3 = uj^2 + vj.$$

2) Montrer que u^3, v^3 sont les racines de :

$$X^2 + qX - \frac{p^3}{27}.$$

Ex. 17

Soit d un entier naturel non nul.

1) Montrer qu'il existe un polynôme P_d réel tel que :

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} k^{2d-1} = P_d\big(n(n+1)\big).$$

2) Montrer qu'il existe un polynôme Q_d réel tel que :

$$\forall n \in \mathbb{N}^*,\ \sum_{k=1}^{n} k^{2d} = (2n+1)Q_d\big(n(n+1)\big).$$

Ex. 18

Étant donné $n \in \mathbb{N}^*$, former des polynômes de degré minimal U et V tels que $X^n U + (1 - X)^n V = 1$.

Ex. 19

Soit $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

On suppose qu'il existe $p \in \mathbb{N}^*$ tel que $\alpha^p \in \mathbb{Q}$.

On pose $n = \inf\{p \in \mathbb{N}^*,\ \alpha^p \in \mathbb{Q}\}$.

1) Montrer que $X^n - \alpha^n$ est irréductible dans $\mathbb{Q}[X]$.

2) Montrer que l'ensemble :

$$I_\alpha = \big\{P \in \mathbb{Q}[X],\ P(\alpha) = 0\big\}$$

est un idéal de $\mathbb{Q}[X]$.

3) En déduire que la famille $\big(1, \alpha, \dots, \alpha^{n-1}\big)$ est libre dans le $\mathbb{Q}$-espace vectoriel $\mathbb{R}$.

Copyrighted material

Indications

Ex. 6

1) Pour l'opération Δ, voir Algèbre et Géométrie, MPSI, chapitre 5.

2) Il suffit d'avoir compris ce qu'est la différence symétrique.

3) Pour $X \notin I_a$, considérer $Y = X \setminus \{a\}$ et $X \cap Y$.

Ex. 7

1) Étudier les éléments inversibles de $K \times K'$.

2) Pour un idéal non trivial de $K \times K'$, considérer les éléments $(k, 0_{K'})$ et $(0_K, k')$ avec k et k' non nuls dans K et K'.

Ex. 8

1) Considérer les fractions irréductibles de dénominateur impair.

2) Pour a et b dans M, montrer que $a + b \notin M$ est absurde en utilisant que ni $\frac{1}{b}$ ni $\frac{1}{a}$ ne sont dans A.

Ex. 9

Les éléments inversibles de $\mathbb{Z}[i]$ ont été vus à l'occasion de l'exemple 5 du cours.

Ex. 10

Le théorème d'Euclide (voir Algèbre et Géométrie, MPSI, chapitre 8) est utile, comme dans l'exemple 6 du cours.

Ex. 11

Avec $T = \prod_{k=1}^{n} (X - a_k)$ et $1 + T^2 = AB$, A et B n'ont pas de racine réelle. On précisera $A(a_k)$ et $B(a_k)$.

Ex. 12

Former $M_k = \prod_{j \neq k} P_j$ et écrire une égalité de Bézout entre P_k et M_k.

Ex. 13

En condition nécessaire, comparer P' et Q.

Utiliser $R \mapsto (1 - X^2)R'' - XR' + n^2 R$, avec $n = \deg P$.

Utiliser $T_n \in \mathbb{R}_n[X]$ défini par $T_n(\cos\theta) = \cos n\theta$ (polynôme de Tchebichev).

Ex. 14

1) $C - B$ et $C + B$ sont premiers entre eux.

Comparer les facteurs irréductibles de $C - B$ et A^2.

Ex. 15

Utiliser $m = P(n)$ pour $n \in \mathbb{Z}$ et former la différence $P(n + km) - P(n)$ pour $k \in \mathbb{Z}$.

Ex. 16

Utiliser les relations entre les coefficients de T et les racines x_1, x_2, x_3 et introduire l'unique polynôme $P \in \mathbb{C}_2[X]$ tel que :

$$P(1) = x_1 \ , \ P(j) = x_2 \ , \ P(j^2) = x_3 \, .$$

(Voir polynômes de Lagrange.)

Ex. 17

Calculer de deux façons $\sum_{k=1}^{n} \left(k^d(k+1)^d - k^d(k-1)^d\right)$.

Ex. 18

Cette égalité de Bézout est difficile à traiter par l'algorithme d'Euclide.

Mais une puissance convenable de $X + (1 - X)$ fait très bien l'affaire.

Ex. 19

1) Écrire la réduction en facteurs irréductibles de $X^n - a^n$ dans $\mathbb{C}[X]$ et raisonner par l'absurde.

3) Revenir à la définition d'une famille libre et utiliser que l'idéal I_a est principal.

Copyrighted material

Solutions des exercices

Niveau 1

Ex. 1

Le fait que $\mathcal{R}_I$ soit une relation d'équivalence découle de l'aspect sous-groupe additif pour tout idéal.

Réflexivité, symétrie et transitivité se traduisent par :

$$0_A \in I,\ x-y\in I \ \Rightarrow\ y-x=-(x-y)\in I.$$

$$x-y\in I,\ y-z\in I \ \Rightarrow\ x-z=(x-y)+(y-z)\in I.$$

Soit $x\,\mathcal{R}_I\,y$ et $z\in A$. De $x-y\in Y$, découle $(x+z)-(y+z)=x-y\in I$, d'où $x+z\,\mathcal{R}_I\,y+z$, c'est-à-dire la compatibilité de $\mathcal{R}_I$ avec l'addition. Seule la structure de sous-groupe intervient ici.

Soit $x\,\mathcal{R}_I\,y$ et $z\in A$. Avec $x-y\in I$ et la stabilité $AI\subset I$, il vient $zx-zy=z(x-y)\in I$, c'est-à-dire la compatibilité de $\mathcal{R}_I$ avec la multiplication.

Ex. 2

Soit x, y dans I ; $x\,\mathcal{R}\,0_A$, $y\,\mathcal{R}\,0_A$ et la compatibilité avec l'addition donne $x+y\,\mathcal{R}\,0_A$.

Soit $x\in I$ et $z\in A$. Avec $x\,\mathcal{R}\,0_A$ et la compatibilité avec la multiplication il vient $zx\,\mathcal{R}\,z0_A$, c'est-à-dire $zx\,\mathcal{R}\,0_A$ et donc $zx\in I$.

Enfin, avec $0_A\in I$, il vient que I est non vide et, avec les deux stabilités précédentes, I est un idéal de A.

Puisque $\forall y\in A,\ -y\,\mathcal{R}\,-y$, la compatibilité avec l'addition donne que pour tout $(x,y)\in A^2$, $x\,\mathcal{R}\,y$ équivaut à $x-y\,\mathcal{R}\,0_A$ soit aussi à $x-y\in I$.

Ex. 3

On a bien sûr $0_A\in A$ donc A est non vide.

Soit $x\in N$ et $z\in A$. Il existe $n\in\mathbb{N}^*$ tel que $x^n=0_A$ et, avec $(zx)^n=z^nx^n=0_A$, il vient $zx\in N$.

Soit x et y dans N. Il existe p et q dans $\mathbb{N}^*$ tels que $x^p=0_A$ et $y^q=0_A$. On applique la formule du binôme (A est commutatif) : $(x+y)^{p+q}=\sum_{k=0}^{p+q}\mathrm{C}_{p+q}^k x^k y^{p+q-k}$.

Il reste à noter que $k\geqslant p \ \Rightarrow\ x^k=0_A$ et que, pour $k\in[\![0,p]\!]$, on a $p+q-k\geqslant q$ donc $y^{p+q-k}=0_A$ pour obtenir $(x+y)^{p+q}=0_A$, donc $x+y\in N$.

Ex. 4

Posons $P=\dfrac{(X-b)(X-c)}{(a-b)(a-c)}+\dfrac{(X-c)(X-a)}{(b-c)(b-a)}+\dfrac{(X-a)(X-b)}{(c-a)(c-b)}\in\mathbb{R}[X]$.

Évitons la méthode naïve qui consiste à tout développer et réduire !

P est un polynôme de degré au plus égal à 2. C'est la somme des polynômes de Lagrange, interpolateurs de a, b et c (voir *Mise en œuvre*, exercice 9). C'est donc l'unique polynôme de degré inférieur ou égal à 2 tel que $P(a)=P(b)=P(c)=1$ donc $P=1$.

Copyrighted material

Ex. 5

1) Question classique (Algèbre et Géométrie, MPSI, chapitre 10) : si A et B sont premiers entre eux, il existe un couple (P, Q) unique d'éléments de $\mathbb{K}[X]$ tels que :

$$\deg P < \deg B,\ \deg Q < \deg A \text{ et } AP + BQ = 1.$$

Avec $A \wedge B = 1$, il existe (théorème de Bézout) U et V dans $\mathbb{K}[X]$ tels que :

$$AU + BV = 1.$$

Avec $U = BC + P$, $\deg P < \deg B$ et $V = AD + Q$, $\deg Q < \deg A$, (divisions euclidiennes), il vient :

$$AP + BQ + (C + D)AB = 1.$$

Or $\deg(AP + BQ - 1) < \deg A + \deg B = \deg AB$.

La condition $\deg\big((C + D)AB\big) < \deg AB$ implique alors $C + D = 0$, d'où :

$$AP + BQ = 1.$$

Si R et S dans $\mathbb{K}[X]$ vérifient $AR + BS = 1$, avec $\deg R < \deg B$ et $\deg S < \deg A$, il vient :

$$(P - R)A = (S - Q)B.$$

A divise $(S - Q)B$, donc divise $S - Q$ (théorème de Gauss). Avec $\deg A > \deg(S - R)$, il vient alors $S - Q = 0$, puis $P - R = 0$, ce qui donne l'unicité.

Ce théorème s'applique ici puisque $a \neq b \Rightarrow (X - a) \wedge (X - b) = 1$, donc :

$$(X - a)^{2n} \wedge (X - b)^{2n} = 1.$$

2) En substituant $a + b - X$ à X dans $(X - a)^{2n}P(X) + (X - b)^{2n}Q(X) = 1$, il vient :

$$(X - b)^{2n}P(a + b - X) + (X - a)^{2n}Q(a + b - X) = 1.$$

L'unicité donne alors $Q(a + b - X) = P(X)$ et $P(a + b - X) = Q(X)$.

Niveau 2

Ex. 6

1) Formons d'abord la fonction caractéristique de la différence symétrique $A \Delta B$. On obtient :

$$\varphi_{A\Delta B} = \varphi_A + \varphi_B - 2\,\varphi_A\,\varphi_B.$$

On vérifie alors que, quels que soient les sous-ensembles A, B et C :

$$\varphi_{A\Delta(B\Delta C)} = \varphi_{(A\Delta B)\Delta C} = \varphi_A + \varphi_B + \varphi_C - 2\,\varphi_B\,\varphi_C - 2\,\varphi_C\,\varphi_A - 2\,\varphi_A\,\varphi_B + 4\,\varphi_A\,\varphi_B\varphi_C$$

donc $A \Delta (B \Delta C) = (A \Delta B) \Delta C$: l'opération Δ est associative. (i)

Les calculs précédents sont détaillés en Algèbre-Géométrie, MPSI, chapitre 5, *Mise en œuvre*, exercice 2.

D'autre part, il est clair que :

- l'opérateur Δ est commutatif car $(A \setminus B) \cup (B \setminus A) = (B \setminus A) \cup (A \setminus B)$;
- l'ensemble vide est neutre pour Δ car $(A \setminus \varnothing) \cup (\varnothing \setminus A) = A \cup \varnothing = A$;
- tout sous -ensemble A de E est son propre symétrique car $A \setminus A = \varnothing$.

On remarquera que les trois propriétés précédentes peuvent aussi se justifier de façon tout aussi immédiate avec les fonctions caractéristiques.

Ainsi, $\big(\mathcal{P}(E), \Delta\big)$ est un groupe commutatif.

Sachant que l'opérateur $\cap$ est associatif, commutatif, et que E en est élément neutre, pour montrer que $\big(\mathcal{P}(E), \Delta, \cap\big)$ est un anneau commutatif, il reste à vérifier que l'intersection est distributive par rapport à la différence symétrique.

Le calcul donne $\varphi_{(A\cup B)\setminus(A\cap B)} = \varphi_A + \varphi_B - 2\,\varphi_A\,\varphi_B = \varphi_{A\Delta B}$ d'où la nouvelle expression :

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

On en déduit alors $\varphi_{(A\cap B)\Delta(A\cap C)} = \varphi_{A\cap(B\Delta C)}$ (voir Algèbre-Géométrie, chapitre 5, *Mise en œuvre*, exercice 3, pour un calcul détaillé), d'où finalement :

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C).$$

Copyrighted material

2) Soit A et B dans I_a. Alors a n'appartient ni à A ni à B. Il n'appartient donc pas à leur différence symétrique $A \Delta B$. Par suite, $A \Delta B \in I_a$.

Soit $A \in I_a$: a n'appartient pas à A, donc quel que soit $B \in \mathcal{P}(E)$, on a $a \notin A \cap B$, et $B \cap A \in I_a$.

Avec $I_a \neq \varnothing$ (il contient la partie vide de E), on conclut que I_a est un idéal de l'anneau $\left(\mathcal{P}(E), \Delta, \cap\right)$.

3) I_a n'est pas égal à $\mathcal{P}(E)$. En effet $\{a\} \notin I_a$.

Soit J un idéal contenant strictement I_a. Il existe $X \in \mathcal{P}(E)$ tel que $X \in J$ et $X \notin I_a$. Nous avons alors :

$$a \in X \text{ et } Y = X \setminus \{a\} \in I_a \text{ d'où } Y \in J.$$

La stabilité de J pour Δ donne $X \Delta Y \in J$ c'est-à-dire $\{a\} \in J$. Pour tout $Z \in \mathcal{P}(E)$, on a $Z \setminus \{a\} \in I_a$ d'où $Z \setminus \{a\} \in J$ puis $\left(Z \setminus \{a\}\right) \Delta \{a\} \in J$, c'est-à-dire $Z \in J$. On a donc $\mathcal{P}(E) \subset J$, soit $\mathcal{P}(E) = J$ et l'idéal I_a est bien maximal.

Ex. 7

1) Un élément (k, k') de $K \times K'$ est inversible si et seulement si k et k' sont inversibles, c'est-à-dire si et seulement si $k \neq 0_K$ et $k' \neq 0_{K'}$. Les éléments non inversibles de $K \times K'$ sont donc les couples :

$$(k, 0_{K'}) \text{ avec } k \in K \text{ et } (0_K, k') \text{ avec } k' \in K'.$$

$(1_K, 0_{K'})$ est différent de $0_{K \times K'} = (0_K, 0_{K'})$ et n'est pas inversible. L'anneau-produit n'est donc pas un corps.

2) Un idéal non trivial I de $K \times K'$ ne contient pas d'élément inversible.

Si I contenait à la fois un élément $(k, 0_{K'})$ et un élément $(0_K, k')$, avec $k \neq 0_K$ et $k' \neq 0_{K'}$ il contiendrait leur somme (k, k') qui est inversible.

Les éléments de I sont donc nécessairement de la forme :

$$(k, 0_{K'}), \text{ avec } k \in K \quad \text{ou} \quad (0_K, k'), \text{ avec } k' \in K',$$

c'est-à-dire :

$$I \subset A = K \times \{0_{K'}\} \text{ ou } I \subset B = \{0_K\} \times K'.$$

Dans le premier cas, I contient un élément $(a, 0_{K'})$ avec $a \in K$, $a \neq 0_K$. La stabilité par le produit avec tout élément de $K \times K'$ montre que I contient alors :

$$(a, 0_{K'}) \cdot (a^{-1}, 0_{K'}) = (1_K, 0_{K'}).$$

Il contient alors tous les produits $(k, k') \cdot (1_K, 0_{K'}) = (k, 0_{K'})$, donc nécessairement $I = K \times \{0_{K'}\}$.

$A = K \times \{0_{K'}\}$ est un sous-groupe de $(K \times K', +)$. Pour montrer la stabilité pour le produit par tout élément de $K \times K'$, il suffit de rappeler que :

$$(k, k') \cdot (a, 0_{K'}) = (ka, 0_{K'}).$$

Donc A est bien un idéal de $K \times K'$. L'autre cas se traite de même.

En conclusion, outre les idéaux triviaux, les idéaux propres de l'anneau-produit $K \times K'$ sont les idéaux principaux engendrés par $(1_K, 0_{K'})$ et par $(0_K, 1_{K'})$, c'est-à-dire $K \times \{0_{K'}\}$ et $\{0_K\} \times K'$.

Ex. 8

1) Dans $\mathbb{Q}$, $A = \left\{\frac{p}{q},\ p \wedge q = 1, (p, q) \in \mathbb{Z} \times \mathbb{N}^* \text{ et } q \wedge 2 = 1\right\}$ est un sous-anneau de $\mathbb{Q}$ qui vérifie la condition donnée. Avec $2 \in A$ et $\frac{1}{2} \notin A$, M n'est pas réduit à $\{0\}$. Avec $\frac{3}{5} \in A$ et $\frac{5}{3} \in A$, M est strictement inclus dans A.

2) Soit a et b dans M et non nuls. Alors $\frac{1}{a}$ et $\frac{1}{b}$ ne sont pas dans A. Somme de $a \in A$ et $b \in A$, on a :

$$a + b \in A.$$

Supposons que $a + b \notin M$, c'est-à-dire $\frac{1}{a+b} \in A$. Avec $\frac{a}{b} \in K^*$, on a :

$$\frac{a}{b} \in A \text{ ou } \frac{b}{a} \in A.$$

Si par exemple $\frac{a}{b}$ est dans A, on a $1_K + \frac{a}{b} \in A$, c'est-à-dire $\frac{a+b}{b} \in A$ d'où, avec $\frac{1}{a+b} \in A$, il vient :

$$\frac{1}{b} \in A,$$

Copyrighted material

ce qui est contradictoire avec $b \in M$. On en conclut que $a + b \in M$.

Soit $m \in M$ et $a \in A$. Alors am est élément de A, donc, si am n'est pas dans M, am est inversible dans A, c'est-à-dire que $\dfrac{1}{am} \in A$, d'où :

$$\frac{1}{m} = a\,\frac{1}{am} \in A,$$

ce qui est contradictoire avec $m \in M$. Il en résulte que $am \in M$ et, en conclusion, M est un idéal de A.

Si J est un idéal de A contenant strictement M, alors J contient un élément inversible de A, donc $J = A$.

Ex. 9

Soit $(a, b) \in \mathbb{Z}^2$ et $p = a^2 + b^2$. On a $p = (a + ib)(a - ib)$. Donc $a + ib$ et $a - ib$ divisent p.

Avec $p > 1$ on a $|a + ib|^2 > 1$, donc les éléments $a + ib$ et $a - ib$ ne sont pas inversibles (voir l'exemple 5 du cours).

Supposons p irréductible. Alors $a + ib$ est un élément associé à p.

Il existe u inversible dans $\mathbb{Z}[i]$, donc de module égal à 1, tel que $p = (a + ib)u$.

Il s'ensuit $p = |a + ib|$ donc $p^2 = a^2 + b^2$, c'est-à-dire $p^2 = p$, ce qui est impossible pour $p > 1$.

Ex. 10

Posons $a = 11 + 7i$ et $b = 3 + 7i$. Avec $a = b + 8$ et $8 = -ib + 1 + 3i$, on a :

$$a = (1 - i)b + 1 + 3i.$$

Un pgcd de a et b est un pgcd de b et $1 + 3i$.

Avec $b = 2(1 + 3i) + 1 + i$, un pgcd de b et $1 + 3i$ est un pgcd de $1 + 3i$ et $1 + i$.

Notons que $1 + 3i = (1 + i)(2 + i)$. Ainsi, un pgcd de $1 + 3i$ et $1 + i$ est $1 + i$.

En conclusion un pgcd de $11 + 7i$ et $3 + 7i$ est $1 + i$.

Ex. 11

Posons $T = \prod_{k=1}^{n} (X - a_k)$. Le polynôme P étudié est $P = 1 + T^2$.

Supposons P réductible dans $\mathbb{Z}[X]$: il existe A et B dans $\mathbb{Z}[X]$, non constants, tels que $P = AB$.

$1 + T^2 = AB$ montre que A et B n'ont aucune racine réelle. Les fonctions réelles $x \mapsto A(x)$ et $x \mapsto B(x)$ sont donc de même signe constant (puisque $A(x)B(x) > 0$).

Avec $AB = (-A)(-B)$, on peut se ramener au cas où elles sont toutes deux strictement positives sur $\mathbb{R}$.

Pour tout $k \in [\![1, n]\!]$, on a $A(a_k)B(a_k) = 1$, avec $A(a_k)$ et $B(a_k)$ entiers positifs ; il vient alors :

$$A(a_k) = B(a_k) = 1.$$

Dans la division euclidienne de A par T, le quotient Q et le reste R sont à coefficients entiers puisque le coefficient dominant de T est 1 (conséquence de l'algorithme de la division dans $\mathbb{R}[X]$).

$A = QT + R$, $A(a_k) = 1$ et $T(a_k) = 0$ donne $R(a_k) = 1$. Le polynôme $R - 1$ est de degré strictement inférieur à $\deg T = n$ et admet au moins n racines. Donc R est le polynôme constant 1.

De même, dans la division euclidienne de B par T, le reste est la constante 1. Le quotient Q_1 est aussi dans $\mathbb{Z}[X]$.

L'égalité $1 + T^2 = AB = (QT + 1)(Q_1T + 1) = 1 + (Q + Q_1)T + QQ_1T^2$ donne :

$$QQ_1T + Q + Q_1 = T.$$

On a alors $\deg(Q + Q_1) \leqslant \deg(QQ_1) < \deg(QQ_1T)$ donc :

$$\deg(Q + Q_1 + QQ_1T) = \deg(QQ_1T) \quad \text{et} \quad \deg(QQ_1T) = \deg T.$$

On en déduit :

$$\deg QQ_1 = \deg Q + \deg Q_1 = 0$$

donc :

$$\deg Q = \deg Q_1 = 0.$$

Q et Q_1 sont des polynômes constants.

Copyrighted material

Alors l'identité $(QQ_1 - 1)T + Q + Q_1 = 0$ donne :

$$Q + Q_1 = 0 \text{ et } QQ_1 = 1 \text{ donc } Q^2 = -1,$$

ce qui ne peut pas avoir lieu pour un polynôme réel Q.

On a ainsi prouvé par l'absurde que P est irréductible dans $Z[X]$.

Ex. 12

Cette propriété est le théorème chinois dans l'anneau $\mathbb{R}[X]$.

Pour $k \in [\![1, n]\!]$, soit $M_k = \prod_{j \neq k} P_j$. Comme P_k est premier avec les P_j, $j \neq k$, on a :

$$M_k \wedge P_k = 1.$$

D'après le théorème de Bézout, il existe donc U_k et V_k dans $\mathbb{R}[X]$ tels que :

$$U_k M_k + V_k P_k = 1.$$

On forme alors le polynôme $Q = \sum_{j=1}^{n} Q_j M_j U_j$.

Pour $j \neq k$, le polynôme P_k divise M_j, donc divise $S_k = \sum_{j \neq k} Q_j M_j U_j$. On a :

$$Q - Q_k = S_k + (M_k U_k - 1)Q_k.$$

Comme P_k divise $M_k U_k - 1$, il vient que P_k divise $Q - Q_k$.

Niveau 3

Ex. 13

Supposons qu'il existe une solution (P, Q). Alors $P \wedge Q = 1$ (théorème de Bézout). Par dérivation, on obtient :

$$PP' = \left(XQ + (X^2 - 1)Q'\right)Q.$$

Ainsi Q divise PP', donc, puisque $P \wedge Q = 1$, Q divise P' (théorème de Gauss).

À partir de $P^2 + (1 - X^2)Q^2 = 1$, il vient $\deg P = 1 + \deg Q$, donc Q a le même degré que P'.

Si P est constant, alors $P^2 = 1$ et $Q = 0$, et les couples $(1, 0)$, $(-1, 0)$ conviennent.

Dans la suite, on suppose $\deg P = n \geqslant 1$. Il existe alors $\lambda \in \mathbb{R}^*$ tel que $Q = \lambda P'$ d'où :

$$P^2 + \left(1 - X^2\right)\lambda^2 P'^2 = 1.$$

En comparant les termes de plus haut degré, on obtient :

$$1 - \lambda^2 n^2 = 0, \text{ donc } Q^2 = \frac{1}{n^2} P'^2.$$

Dérivons $P^2 + \frac{1}{n^2}\left(1 - X^2\right)P'^2 = 1$, il vient :

$$n^2 PP' - XP'^2 + \left(1 - X^2\right)P'P'' = 0.$$

$\mathbb{R}[X]$ étant intègre, $P' \neq 0$ donne alors :

$$\left(1 - X^2\right)P'' - XP' + n^2 P = 0.$$

L'application $\varphi : \mathbb{R}_n[X] \to \mathbb{R}_n[X]$, $R \mapsto \left(1 - X^2\right)R'' - XR' + n^2 R$ est linéaire.

En posant $r = \deg R$ et $c_r = \operatorname{dom} R$, le coefficient de X^r pour $\phi(R)$ est $\left(n^2 - r^2\right)c_r$. Il s'ensuit que $\varphi(R)$ a même degré que R lorsque $\deg R < n$. Alors $\left(\varphi(1), \varphi(X), \ldots, \varphi(X^{n-1})\right)$ est libre dans $\mathbb{R}_n[X]$.

Alors φ est de rang au moins égal à n, donc son noyau est de dimension au plus égal à 1.

Considérons le polynôme de Tchebichev défini par $\forall\, \theta \in \mathbb{R}$, $T_n(\cos\theta) = \cos n\theta$. On sait que $\deg T_n = 0$. (Voir Algèbre-Géométrie, MPSI, chapitre 1, *Mise en œuvre*, exercice 12.)

Copyrighted material

En dérivant, on a $\sin\theta\, T_n'(\cos\theta) = n\sin n\theta$ puis :

$$\cos\theta\, T_n'(\cos\theta) - \left(1-\cos^2\theta\right)T_n''(\cos\theta) = n^2\cos n\theta = n^2 T_n(\cos\theta).$$

On a donc $\left(1-X^2\right)T_n'' - XT_n' + n^2T_n^2 = 0$, puisque ce polynôme admet une infinité de racines.

Le noyau de φ est donc le sous-espace vectoriel engendré par T_n et il existe $\alpha \in \mathbb{R}$ tel que $P = \alpha T_n$.

Déterminons enfin, parmi les solutions possibles αT_n celles qui conviennent.

Avec $\sin\theta T_n'(\cos\theta) = n\sin n\theta$, on a $\left(1-\cos^2\theta\right)T_n'^2(\cos\theta) = n^2\left(1-\cos^2 n\,\theta\right) = n^2\left(1-T_n^2(\theta)\right)$, donc :

$$T_n^2 + \left(1-X^2\right)\left(\frac{1}{n}T_n'\right)^2 = 1.$$

Avec $Q = \pm\frac{1}{n}P' = \pm\frac{\alpha}{n}T_n'$, on obtient :

$$P^2 + \left(1-X^2\right)Q^2 = \alpha^2\left(T_n^2 + \left(1-X^2\right)\frac{1}{n^2}T_n'^2\right) = \alpha^2.$$

Donc (P, Q) est solution si et seulement si $\alpha = \pm 1$.

En conclusion, les solutions non constantes sont pour tout $n \in \mathbb{N}^*$, les couples :

$$\left(T_n, \frac{1}{n}T_n'\right),\ -\left(T_n, \frac{1}{n}T_n'\right),\ \left(T_n, -\frac{1}{n}T_n'\right),\ -\left(T_n, -\frac{1}{n}T_n'\right).$$

Ex. 14

1) Par hypothèse : $C^2 - B^2 = A^2$ d'où $(C-B)(C+B) = A^2$. D'autre part : $(C-B)\wedge(C+B) = C\wedge B = 1$.

Un facteur irréductible de $C-B$ est un facteur irréductible de A^2 et il figure dans la décomposition de $C-B$ avec le même exposant que dans A^2 puisqu'il n'est pas facteur irréductible de $C+B$. Cet exposant est donc pair.

On en déduit que $C-B$ est le carré d'un polynôme et il en est de même pour $C+B$.

2) a) Condition nécessaire

Posons $C+B = P^2$ et $C-B = Q^2$. Il vient alors :

$$2C = P^2 + Q^2\ ,\ 2B = P^2 - Q^2 \text{ et } A^2 = P^2Q^2$$

d'où $A = \varepsilon PQ$ avec $\varepsilon \in \{-1, 1\}$.

$B\wedge C = 1$ donne $\left(P^2-Q^2\right)\wedge\left(P^2+Q^2\right) = 1$.

Comme $\left(P^2-Q^2\right)\wedge\left(P^2+Q^2\right) = P^2\wedge Q^2 = (P\wedge Q)^2$, il vient $P\wedge Q = 1$.

b) Condition suffisante

Soit P et Q des polynômes premiers entre eux.

Posons $C = \frac{1}{2}\left(P^2+Q^2\right)$, $B = \frac{1}{2}\left(P^2-Q^2\right)$ et $A = PQ$. Il vient :

$$A^2 = C^2 - B^2.$$

$B\wedge C = \left(P^2-Q^2\right)\wedge\left(P^2+Q^2\right) = P^2\wedge Q^2 = \left(P\wedge Q\right)^2$ montre que $B\wedge C = 1$. Nous avons :

$$A\wedge C = (PQ)\wedge\left(P^2+Q^2\right).$$

Un diviseur commun à PQ et $\left(P^2+Q^2\right)$ divise :

$$P^2 + Q^2 + 2PQ \text{ et } P^2 + Q^2 - 2PQ.$$

Il divise donc :

$$(P+Q)^2\wedge(P-Q)^2 = \left((P+Q)\wedge(P-Q)\right)^2.$$

Comme $(P+Q)\wedge(P-Q) = P\wedge Q = 1$, il vient que A et C sont premiers entre eux.

Copyrighted material

Un diviseur commun à A et B divise $P^2 - Q^2$ et PQ. Il divise donc :

$$P^2 - Q^2 + 2iPQ \text{ et } P^2 - Q^2 - 2iPQ.$$

C'est donc un diviseur de $\big((P + iQ) \wedge (P - iQ)\big)^2$.

Alors, $(P + iQ) \wedge (P - iQ) = P \wedge Q = 1$ montre que $A \wedge B = 1$.

c) En conclusion, $A^2 + B^2 = C^2$ avec A, B et C deux à deux premiers entre eux, est réalisé si et seulement si :

$$A = PQ \ , \ B = \frac{1}{2}\big(P^2 - Q^2\big) \ , \ C = \frac{1}{2}\big(P^2 + Q^2\big) \quad \text{avec } P \wedge Q = 1.$$

Ex. 15

Soit $P \in \mathbb{Z}[X]$, $P = \sum a_r X^r$, où les a_r sont des entiers.

Pour $n \in \mathbb{Z}$, on pose $m = P(n)$.

Pour tout $k \in \mathbb{Z}$, $P(n + km) - P(n) = \sum a_r \big((n + km)^r - n^r\big)$ est divisible par m, donc m divise $P(n + km)$.

P n'étant pas constant, il y a une infinité de $P(n + km)$, $k \in \mathbb{Z}$, et, sauf peut-être m et $-m$, aucun d'eux n'est premier.

Ex. 16

x_1 , x_2 , x_3 étant les racines de $T(X)$, on a :

$$\begin{aligned} X^3 + pX + q &= \big(X - x_1\big(X - x_2\big)\big(X - x_3\big) \\ &= X^3 - \big(x_1 + x_2 + x_3\big)X^2 + \big(x_1x_2 + x_2x_3 + x_3x_2\big)X - x_1x_2x_3 \end{aligned}$$

d'où, en particulier, $x_1 + x_2 + x_3 = 0$.

1) ▪ Supposons qu'il existe u et v tels que $x_1 = u + v$, $x_2 = j^2u + jv$, $x_3 = ju + j^2v$ et considérons le polynôme :

$$P(X) = uX^2 + vX.$$

On obtient alors $P(1) = x_1$, $P(j) = x_2$, $P\big(j^2\big) = x_3$ donc P est l'unique polynôme de degré $\leqslant 2$ vérifiant ces conditions. Il s'écrit au moyen des polynômes de Lagrange associés au triplet $\big(1, j, j^2\big)$:

$$L_1(X) = \frac{(X - j)\big(X - j^2\big)}{(1 - j)\big(1 - j^2\big)} = \frac{1}{3}(X - j)\big(X - j^2\big).$$

$$L_2(X) = \frac{(X - 1)\big(X - j^2\big)}{(j - 1)\big(j - j^2\big)} = \frac{j}{3}(X - 1)\big(X - j^2\big).$$

$$L_3(X) = \frac{(X - 1)(X - j)}{\big(j^2 - 1\big)\big(j^2 - j\big)} = \frac{j^2}{3}(X - 1)(X - j).$$

$$P(X) = x_1L_1(X) + x_2L_2(X) + x_3L_3(X).$$

Ceci nous prouve l'unicité de (u, v) sous réserve d'existence.

▪ Pour l'existence, considérons le polynôme :

$$P(X) = x_1L_1(X) + x_2L_2(X) + x_3L_3(X).$$

Il est clair que $\deg P \leqslant 2$, donc il existe $(u, v, w) \in \mathbb{C}^3$ tel que $P(X) = uX^2 + vX + w$ et par définition des polynômes de Lagrange :

$$P(1) = x_1 \ , \ P(j) = x_2 \ , \ P\big(j^2\big) = x_3$$

c'est-à-dire $\quad u + v + w = x_1 \ , \ j^2u + jv + w = x_2 \ , \ ju + j^2v + w = x_3$.

Alors, compte tenu de $1 + j + j^2 = 0$ et de $x_1 + x_2 + x_3 = 0$, il vient $w = 0$ donc :

$$x_1 = u + v \ , \ x_2 = j^2u + jv \ , \ x_3 = ju + j^2v.$$

On a ainsi prouvé l'existence d'un couple (u, v) solution du problème.

2) Toujours avec $1 + j + j^2 = 0$, on obtient :

$$x_1x_2 + x_2x_3 + x_3x_1 = -3uv \text{ et } x_1x_2x_3 = u^3 + v^3$$

donc $X^3 + pX + q = X^3 - 3uvX - \big(u^3 + v^3\big)$ et u, v sont caractérisés par :

$$-3uv = p \ , \ u^3 + v^3 = -q.$$

Avec $u^3v^3 = -\dfrac{p^3}{27}$ et $u^3 + v^3 = -q$, u^3 et v^3 sont les racines de $X^2 + qX - \dfrac{p^3}{27}$.

Copyrighted material

Ex. 17

1) À titre d'exemple, on sait que $\sum_{k=1}^{n} k = \frac{1}{2}n(n+1)$. Ainsi, $P_1(X) = \frac{1}{2}X$.

De même, la somme $\sum_{k=1}^{n} k^3 = \frac{1}{4}n^2(n+1)^2$ est usuelle. On a donc :

$$P_3(X) = \frac{1}{4}X^2 = P_1^2(X).$$

Considérons $\sum_{k=1}^{n}\left(k^d(k+1)^d - k^d(k-1)^d\right) = \sum_{k=1}^{n} k^d(k+1)^d - \sum_{k=0}^{n-1} k^d(k+1)^d = n^d(n+1)^d$.

On a (formule du binôme) $k^d\left((k+1)^d - (k-1)^d\right) = 2k^d \sum_{i=0}^{r} C_d^{2i+1} k^{d-2i-1}$, avec r partie entière de $\frac{d-1}{2}$.

Il vient alors $\sum_{k=1}^{n}\left(k^d(k+1)^d - k^d(k-1)^d\right) = 2\sum_{i=0}^{r} C_d^{2i+1}\left(\sum_{k=1}^{n} k^{2d-2i-1}\right)$, ou aussi :

$$\sum_{k=1}^{n}\left(k^d(k+1)^d - k^d(k-1)^d\right) = 2\sum_{i=0}^{r} C_d^{2i+1} S_n(2d-2i-1),$$

en ayant posé, pour $m \in \mathbb{N}$, $S_n(m) = \sum_{k=1}^{n} k^m$. Il s'ensuit :

$$n^d(n+1)^d = 2\sum_{i=0}^{r} C_d^{2i+1} S_n(2d-2i-1) = 2dS_n(2d-1) + 2\sum_{i=1}^{r} C_d^{2i+1} S_n(2d-2i-1),$$

d'où la relation de récurrence :

$$S_n(2d-1) = \frac{1}{2d}n^d(n+1)^d - \frac{1}{d}\sum_{i=1}^{r} C_d^{2i+1} S_n(2d-2i-1).$$

Par exemple, avec $S_n(1)$ et $S_n(3)$ rappelés ci-dessus, il vient $P_3(X) = \frac{1}{6}X^3 - \frac{1}{12}X^2$. En effet :

$$\sum_{k=1}^{n} k^5 = S_n(5) = S_n(2\times 3 - 1) = \frac{1}{6}n^3(n+1)^3 - \frac{1}{3}S_n(3) = \frac{1}{6}n^3(n+1)^3 - \frac{1}{12}n^2(n+1)^2.$$

On obtient ainsi, par récurrence, l'existence d'une suite $(P_d)_{d\in\mathbb{N}^*}$ de polynômes tels que :

$$\forall n \in \mathbb{N}^*,\quad P_d\left(n(n+1)\right) = \sum_{k=1}^{n} k^{2d-1}.$$

Ils sont obtenus par $P_1(X) = \frac{1}{2}X$ et $P_d(X) = \frac{1}{2d}X^d - \frac{1}{d}\sum_{i=1}^{r} C_d^{2i+1} P_{d-i}(X)$, avec r partie entière de $\frac{d-1}{2}$.

2) Considérons $A_n = \sum_{k=1}^{n}\left(k^{d+1}(k+1)^d - k^d(k-1)^{d+1}\right) = n^{d+1}(n+1)^d$

et $B_n = \sum_{k=1}^{n}\left(k^d(k+1)^{d+1} - k^{d+1}(k-1)^d\right) = n^d(n+1)^{d+1}$.

On a $A_n + B_n = (2n+1)n^d(n+1)^d$.

Avec :

$k^{d+1}(k+1)^d + k^d(k+1)^{d+1} = (2k+1)k^d(k+1)^d$ et $k^d(k-1)^{d+1} + k^{d+1}(k-1)^d = (2k-1)k^d(k-1)^d$,

on obtient :

$$k^{d+1}(k+1)^d + k^d(k+1)^{d+1} - \left(k^d(k-1)^{d+1} + k^{d+1}(k-1)^d\right) = 2k^{d+1}\left((k+1)^d - (k-1)^d\right) + k^d\left((k+1)^d + (k-1)^d\right).$$

Copyrighted material

En développant par la formule du binôme, et en notant r la partie entière de $\frac{d-1}{2}$ et s celle de $\frac{d}{2}$, il vient :

$$A_n + B_n = 4\sum_{i=0}^{r} \mathrm{C}_d^{2i+1}\, S_n(2d-2i) + 2\sum_{i=0}^{s} \mathrm{C}_d^{2i}\, S_n(2d-2i).$$

On en déduit, par comparaison des deux expressions de $A_n + B_n$, la relation de récurrence :

$$(4d+2)S_n(2d) = (2n+1)n^d(n+1)^d - 4\sum_{i=1}^{r} \mathrm{C}_d^{2i+1}\, S_n(2d-2i) - 2\sum_{i=1}^{s} \mathrm{C}_d^{2i}\, S_n(2d-2i).$$

On sait que $S_n(2) = \sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$, d'où $Q_1(X) = \frac{1}{6}X$.

Supposons que, pour tout $q \in [\![1, d-1]\!]$, il existe $Q_q \in \mathbb{R}[X]$ tel que :

$$\sum_{k=1}^{n} k^{2q} = (2n+1)Q_q\big(n(n+1)\big),$$

alors $(4d+2)S_n(2d) = (2n+1)\Big(n^d(n+1)^d - 4\sum_{i=1}^{r} \mathrm{C}_d^{2i+1}\, Q_{d-i}\big(n(n+1)\big) - 2\sum_{i=1}^{s} \mathrm{C}_d^{2i}\, Q_{d-i}\big(n(n+1)\big)\Big)$

montre que $\sum_{k=1}^{n} k^{2d} = (2n+1)Q_d\big(n(n+1)\big)$ avec :

$$Q_d = \frac{1}{2(2d+1)}\left(X^d - 4\sum_{i=1}^{r} \mathrm{C}_d^{2i+1}\, Q_{d-i}(X) - 2\sum_{i=1}^{s} \mathrm{C}_d^{2i}\, Q_{d-i}(X)\right).$$

Par exemple, $Q_2 = \frac{1}{30}X(3X-1)$ et $Q_3 = \frac{1}{42}X\big(3X^2-3X+1\big)$.

Ex. 18

Pour tout $k \in \mathbb{N}^*$, $\big(X + (1-X)\big)^k = 1$. Il suffit alors de choisir k tel que, dans le développement par la formule du binôme, chaque terme soit divisible par X^n ou par $(1-X)^n$.

On choisit $k = 2n-1$ et on développe. Il vient :

$$1 = \sum_{k=0}^{2n-1} \mathrm{C}_{2n-1}^{k} X^k (1-X)^{2n-1-k} = \sum_{k=0}^{n-1} \mathrm{C}_{2n-1}^{k} X^k (1-X)^{2n-1-k} + \sum_{k=n}^{2n-1} \mathrm{C}_{2n-1}^{k} X^k (1-X)^{2n-1-k},$$

d'où $1 = (1-X)^n \sum_{k=0}^{n-1} \mathrm{C}_{2n-1}^{k} X^k (1-X)^{n-1-k} + X^n \sum_{k=n}^{2n-1} \mathrm{C}_{2n-1}^{k} X^{k-n} (1-X)^{2n-1-k}$.

On sait (variante du théorème de Bézout) qu'il existe un couple unique de polynômes U et V tels que :

$$X^n U + (1-X)^n V = 1 \text{ avec } \deg U < \deg(1-X)^n \text{ et } \deg V < \deg X^n.$$

Alors $U = \sum_{k=n}^{2n-1} \mathrm{C}_{2n-1}^{k} X^{k-n} (1-X)^{2n-1-k}$ et $V = \sum_{k=0}^{n-1} \mathrm{C}_{2n-1}^{k} X^k (1-X)^{n-1-k}$ conviennent.

Ex. 19

1) Montrons que $X^n - \alpha^n$ est irréductible dans $\mathbb{Q}[X]$.

Dans $\mathbb{C}[X]$, on a $X^n - \alpha^n = \prod_{k=0}^{n-1} \big(X - \alpha\,\omega_k\big)$ avec $\omega_k = \exp\left(\frac{2ik\pi}{n}\right)$.

Supposons qu'il existe A et B non constants dans $\mathbb{Q}[X]$ tels que $X^n - \alpha^n = AB$. En particulier, avec $q = \deg A$, on a $1 \leqslant q < n$. Le coefficient dominant de $X^n - \alpha^n$ étant 1, on peut imposer à A (et B) d'avoir 1 pour coefficient dominant.

Copyrighted material

Par unicité de la décomposition d'un polynôme en produit de facteurs irréductibles, il existe une famille $(\omega_{k_1}, \cdots, \omega_{k_q})$ telle que :

$$A = \prod_{j=1}^{q} (X - \alpha\,\omega_{k_j}).$$

Le terme constant a_0 de A est alors égal à :

$$(-1)^q\,\alpha^q \prod_{j=1}^{q} \omega_{k_j}.$$

Comme a_0 (rationnel) et α^q sont réels, il en est de même pour $\varepsilon = \prod_{j=1}^{q} \omega_{k_j}$.

ε étant en outre de module 1, ce ne peut être que 1 ou -1.

Alors $\alpha^q = \pm a_0$, donc $\alpha^q \in \mathbb{Q}$, ce qui n'est pas compatible avec la définition de n.

En conséquence $X^n - \alpha^n$ est irréductible dans $\mathbb{Q}[X]$.

2) I_α est non vide car il contient le polynôme nul, et non réduit à $\{0\}$ car il contient $X^n - \alpha^n$.

Il est immédiat que si $A \in I_\alpha$ et $B \in I_\alpha$ alors $(A + B)(\alpha) = 0$ donc $A + B \in I_\alpha$.

De même, pour $A \in I_\alpha$ et $B \in \mathbb{Q}[X]$, on a $(AB)(\alpha) = B(\alpha)A(\alpha) = 0$ donc $AB \in I_\alpha$.

Ainsi I_α est un idéal non réduit à $\{0\}$ de $\mathbb{Q}[X]$.

3) $\mathbb{Q}[X]$ est principal, il existe donc $M \in \mathbb{Q}[X]$, unitaire, tel que I_α soit l'ensemble des multiples de M : $I_\alpha = M\,\mathbb{Q}[X]$.

Puisque $X^n - \alpha^n \in I_\alpha$, M est un diviseur de $X^n - \alpha^n$ et, puisque $X^n - \alpha^n$ est irréductible et $M \neq 1$ (sinon on aurait $I_\alpha = \mathbb{Q}[X]$), il vient $X^n - \alpha^n = M$.

Considérons alors des rationnels $\lambda_0, \cdots, \lambda_{n-1}$ tels que $\sum_{k=0}^{n-1} \lambda_k \alpha^k = 0$.

Cette relation s'écrit $P(\alpha) = 0$ en posant $P(X) = \sum_{k=0}^{n-1} \lambda_k X^k$.

Donc P appartient à I_α : il existe $U \in \mathbb{Q}[X]$ tel que $P(X) = U(X)(X^n - \alpha^n)$.

Compte tenu de $\deg P \leqslant n - 1$, on en déduit $U(X) = 0$ puis $P = 0$, ce qui donne $\lambda_0 = \lambda_1 = \cdots = \lambda_{n-1} = 0$.

On a ainsi prouvé que $(1, \alpha, \cdots, \alpha^{n-1})$ est libre dans $\mathbb{R}$ considéré comme $\mathbb{Q}$-espace vectoriel.

Copyrighted material

CHAPITRE

3

Espaces vectoriels Applications linéaires

Copyrighted material

A. Structure de $\mathbb{K}$ -algèbre

Dans ce chapitre, $\mathbb{K}$ désigne un corps de caractéristique nulle.

1. Applications multilinéaires

La notion a été introduite en Algèbre et Géométrie, MPSI, chapitre 14.

- Étant donné $p+1$ $\mathbb{K}$-espaces vectoriels $E_1, E_2, \cdots, E_p, F$, une application

$$f : E_1 \times E_2 \times \cdots \times E_p \to F$$

est dite **p-linéaire** [1] lorsque toute application partielle :

$$f_j : E_j \to F, x_j \mapsto f(a_1, \cdots, a_{j-1}, x_j, a_{j+1}, \cdots, a_n)$$

est linéaire.

[1] Si $p=2$, on dit que f est bilinéaire, et si $p=3$, on dit que f est trilinéaire.

Lorsque $F = \mathbb{K}$ on dit que f est une **forme p-linéaire**.

- L'ensemble des applications p-linéaires de E^p dans F (resp. des formes p-linéaires sur E^p) est noté $\mathcal{L}_p(E, F)$ (resp. $\mathcal{L}_p(E)$). Ce sont des $\mathbb{K}$-espaces vectoriels.

2. $\mathbb{K}$ -algèbre

Définition 1

Une **algèbre sur $\mathbb{K}$** ou **$\mathbb{K}$-algèbre** est un quadruplet $(A, +, \times, \cdot)$ tel que :

(1) $(A, +, \times)$ est un anneau ; [2]

(2) $(A, +, \cdot)$ est un $\mathbb{K}$-espace vectoriel ;

(3) $\forall \lambda \in \mathbb{K}, \forall (a, b) \in A^2, (\lambda \cdot a) \times b = a \times (\lambda \cdot b) = \lambda \cdot (a \times b)$.

Une $\mathbb{K}$-algèbre est dite commutative quand la loi interne est commutative.

[2] $\times$ est la multiplication interne et $\cdot$ la multiplication externe (à opérateurs dans $\mathbb{K}$).

Remarque

Par définition, un anneau possède un élément unité qui sera naturellement appelé unité de l'algèbre A.

Propriété 1

Si $(A, +, \times, \cdot)$ est une $\mathbb{K}$-algèbre, l'application $B : E^2 \to E, (a, b) \mapsto a \times b$ est bilinéaire.

Exemples usuels de $\mathbb{K}$-algèbres

1) L'ensemble $\mathbb{K}^{\mathbb{N}}$ des suites à valeurs dans $\mathbb{K}$ est une $\mathbb{K}$-algèbre commutative pour les lois usuelles définies par :

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}}$$

$$\lambda (x_n)_{n\in\mathbb{N}} = (\lambda x_n)_{n\in\mathbb{N}}$$

$$(x_n)_{n\in\mathbb{N}} \times (y_n)_{n\in\mathbb{N}} = (x_n y_n)_{n\in\mathbb{N}}$$

L'unité est la suite constante $(1)_{n\in\mathbb{N}}$.

2) L'ensemble $\mathcal{F}(I, \mathbb{K})$ des applications de I, intervalle de $\mathbb{R}$, dans $\mathbb{K}$ est une $\mathbb{K}$-algèbre commutative pour les lois usuelles définies par :

$$\forall x \in I, \ \forall (f, g) \in \mathcal{F}(I, \mathbb{K})^2, \ \forall \lambda \in \mathbb{K}$$

$$(f + g)(x) = f(x) + g(x)$$

$$(\lambda f)(x) = \lambda f(x)$$

$$(fg)(x) = f(x)g(x)$$

L'unité est la fonction constante égale à 1.

Copyrighted material

3) L'ensemble $\mathbb{K}[X]$ des polynômes à coefficients dans $\mathbb{K}$ est une $\mathbb{K}$-algèbre commutative pour les lois usuelles : addition, produit par un scalaire, produit des polynômes. (3)

4) L'ensemble $\mathcal{M}_n(\mathbb{K})$ des matrices à coefficients dans $\mathbb{K}$ est une $\mathbb{K}$-algèbre non commutative (dès que $n \geqslant 2$) pour les lois usuelles : addition, produit par un scalaire, produit matriciel.
L'unité est la matrice identité I_n.

5) Si E est un $\mathbb{K}$-espace vectoriel, l'ensemble $\mathcal{L}(E)$ des endomorphismes de E est une $\mathbb{K}$-algèbre non commutative (dès que E n'est pas de dimension 1) pour les lois usuelles : addition, produit par un scalaire, composition des applications.
L'unité est Id_E.

(3) On remarquera, puisque les scalaires sont identifiables aux polynômes constants, que les deux produits, interne et externe, coïncident dans ce cas.

Définition 2

Soit $(A, +, \times, \cdot)$ une $\mathbb{K}$-algèbre et B une partie non vide de A.
On dit que B est une sous-algèbre lorsque $(B, +, \times)$ est un sous-anneau de $(A, +, \times)$ et $(B, +, \cdot)$ un sous-espace vectoriel de $(A, +, \cdot)$.

On remarquera que les lois de A induisent sur B une structure de $\mathbb{K}$-algèbre. (4)

(4) L'axiome (3) est vérifié *de facto*.

Définition 3

Soit $(A, +, \times, \cdot)$ et $(A', +, \times, \cdot)$ des $\mathbb{K}$-algèbres. (5)
On dit que f est un morphisme d'algèbres de A dans A' lorsque f est un morphisme d'anneaux de $(A, +, \times)$ dans $(A', +, \times)$ et une application linéaire de $(A, +, \cdot)$ dans $(A', +, \cdot)$.

(5) Les opérations sont notées de la même façon pour les raisons de commodité évidente.

Propriété 2

L'intersection de toute famille (6) $(B_i)_{i \in I}$ de sous-algèbres d'une $\mathbb{K}$-algèbre A en un sous-algèbre de A.

(6) La notion de famille d'ensembles est présentée en Algèbre et Géométrie, MPSI, chapitre 5.

Définition 4

Étant donné une partie X d'une $\mathbb{K}$-algèbre A, la sous-algèbre engendrée par X est l'intersection de la famille des sous-algèbres de A contenant X ; c'est donc aussi la plus petite sous-algèbre de A contenant X. (7)

(7) C'est en effet une sous-algèbre de A contenant X et incluse dans toutes les autres.

B. Familles libres, génératrices Bases – Dimension

E est un $\mathbb{K}$-espace vectoriel. (8)

(8) Les notions présentées dans cette section ont, pour l'essentiel, été vues en Algèbre et Géométrie, MPSI, aux chapitres 9 et 12 dans le cadre, plus restreint, des espaces vectoriels sur $\mathbb{R}$ ou $\mathbb{C}$.

1. Combinaisons linéaires

1.1 – Familles d'éléments de E

- Une **famille** d'éléments de E indexée par un ensemble I est une application de I dans E. (9)

L'ensemble des familles d'éléments de E indexées par I est E^I.
Une famille $(c_i)_{i \in I}$ est dite finie lorsque I est un ensemble fini.

- Le **support** d'une famille $(c_i)_{i \in I}$ est le sous-ensemble $\{i \in I \ / \ c_i \neq 0\}$ noté $\mathrm{Supp}\,(c_i)_{i \in I}$.
- Une famille $(c_i)_{i \in I}$ de support fini est dite **presque nulle**.

L'ensemble des familles presque nulles d'éléments de E indexées par I est noté $E^{(I)}$.

(9) On la note, par exemple, $(c_i)_{i \in I}$.

Copyrighted material

▪ Soit $(c_i)_{i\in I}$ une famille de E et $J \subset I$. On dit que $(c_j)_{j\in J}$ est une **sous-famille de** $(c_i big)_{i\in I}$. On dit aussi que $(c_i)_{i\in I}$ est une **sur-famille** de $(c_j)_{j\in J}$.

1.2 – Combinaisons linéaires d'éléments de E

▪ Soit $(c_i)_{i\in I}$ une famille d'éléments de E. On dit que $x\in E$ est **combinaison linéaire** de $(c_i)_{i\in I}$ lorsqu'il existe une famille de scalaires $(\lambda_i)_{i\in I}$ de **support fini** J telle que $x = \sum_{j\in J} \lambda_j c_j$.

Pour $i \in I \setminus J$, on a $\lambda_i = 0$, ce qui autorise à écrire $x = \sum_{i\in I} \lambda_i c_i$.

▪ Soit A une partie de E. On dit que $x \in E$ est **combinaison linéaire** d'éléments de A lorsqu'il est combinaison linéaire de la famille $(a)_{a\in A}$ des éléments de A.

▪ L'ensemble des combinaisons linéaires d'éléments de A est le sous-espace vectoriel $\mathrm{Vect}(A)$ engendré par A. [10]

[10] $\mathrm{Vect}(A)$ est l'intersection de tous les sous-espaces vectoriels de E contenant A. C'est aussi le plus petit sous-espace vectoriel de E contenant A.

2. Familles génératrices

▪ Étant donné un sous-espace vectoriel F de E, on dit qu'une famille $(c_i)_{i\in I} \in E^I$ est **génératrice** de F lorsque $\mathrm{Vect}\left((c_i)_{i\in I}\right) = F$.

▪ Toute sur-famille d'une famille génératrice de E est encore une famille génératrice de E.

▪ Soit E et F des $\mathbb{K}$-espaces vectoriels et $u \in \mathcal{L}(E, F)$.
Si $(c_i)_{i\in I}$ est une famille génératrice de E, alors $(u(c_i) big)_{i\in I}$ est une famille génératrice de $\mathrm{Im}\, u$.

3. Familles libres, liées

Définitions

▪ Une famille finie non vide $(c_j)_{j\in J} \in E^J$ [11] est **libre** quand

$$(\forall (\lambda_j)_{j\in J} \in \mathbb{K}^J)\ .\ \left(\sum_{j\in J} \lambda_j c_j = 0_E \ \Rightarrow\ \forall j \in J,\ \lambda_j = 0\right).$$

▪ Une famille non vide $(c_i)_{i\in I} \in E^I$ est **libre** si toutes ses sous-familles finies sont libres.
On dit aussi que les éléments d'une famille libre sont **linéairement indépendants.**

▪ Une famille est dite **liée** quand elle n'est pas libre.
On dit que ses éléments sont **linéairement dépendants.**

[11] J est fini.

Propriétés

▪ Une famille à un élément (x) est libre si et seulement si $x \neq 0_E$. [12]

▪ Les éléments d'une famille libre sont deux à deux distincts.

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

▪ Une famille $(c_i)_{i\in I}$ est liée si et seulement si il existe une famille $(\lambda_i)_{i\in I}$ de scalaires, de support fini non vide [13], telle que $\sum_{i\in I} \lambda_i c_i = 0_E$

▪ Une famille $(c_i)_{i\in I}$ est liée si et seulement si il existe $k \in I$ tel que c_k soit combinaison linéaire de la famille $(c_i)_{i\in I\setminus\{k\}}$. [14]

[12] Une famille contenant 0_E est liée.

[13] $(\lambda_i)_{i\in I}$ est une famille de scalaires presque nulle mais non identiquement nulle.

[14] La difficulté pour l'utilisation de cette propriété usuelle tient à ce que, sauf information complémentaire, on ne sait pas qui est le k en question.

Copyrighted material

Propriété 3

Soit E, F des $\mathbb{K}$-espaces vectoriels; $u \in \mathcal{L}(E, F)$ et $(c_i)_{i\in I}$ une famille de E.

a) Si $(c_i)_{i\in I}$ est liée, alors $(u(c_i))_{i\in I}$ est une famille liée de F.

b) Si u est injective et si $(c_i)_{i\in I}$ est libre, alors $(u(c_i))_{i\in I}$ est une famille libre de F.

Propriété 4

Soit $(c_i)_{i\in I}$ une famille libre de E et $x \in E$ telle que les vecteurs de $\{x\} \cup \{c_i, i \in I\}$ soient liés.
Alors x est combinaison linéaire de $(c_i)_{i\in I}$, et ceci de manière unique.

Exemple 1 Dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}^{\mathbb{R}}$, la famille $F = (f_a)_{a\in\mathbb{R}}$ des fonctions $f_a : x \mapsto |x - a|$ est libre.

Soit $(a_i)_{i\in[\![1,p]\!]}$ une famille finie de réels deux à deux distincts et $(f_{a_i})_{i\in[\![1,p]\!]}$ une sous-famille finie de F. Soit alors une famille $(\lambda_i)_{i\in[\![1,p]\!]}$ de scalaires telle que :

$$\sum_{i=1}^{p} \lambda_i f_{a_i} = 0 \quad \text{c'est-à-dire} \quad \forall x \in \mathbb{R}, \sum_{i=1}^{p} \lambda_i |x - a_i| = 0.$$

S'il existait $k \in [\![1, p]\!]$ tel que $\lambda_k \neq 0$, on aurait $f_{a_k} = \sum_{\substack{i=1 \\ i\neq k}}^{p} \frac{\lambda_i}{\lambda_k} f_{a_i}$.

Or f_{a_k} n'est pas dérivable en a_k alors que les f_{a_i} sont dérivables en a_k pour $i \neq k$.
Par suite, on a $\lambda_i = 0$ pour tout $i \in [\![1, p]\!]$ et toute sous-famille finie de $(f_{a_i})_{i\in[\![1,p]\!]}$ est libre.

4. Algèbre des fonctions polynomiales sur $\mathbb{R}^n$ ou $\mathbb{C}^n$

Définition 5

Étant donné $n \in \mathbb{N}$, on note p_i, $i = 1, 2, \ldots, n$, les projections canoniques dans $\mathbb{K}^n$:

$$p_i : \mathbb{K}^n \to \mathbb{K}, (x_1, \ldots, x_n) \mapsto x_i.$$

On appelle fonctions polynomiales sur $\mathbb{K}^n$ (à valeurs dans $\mathbb{K}$) les éléments de la sous-algèbre de $\mathcal{F}(\mathbb{K}, \mathbb{K})$ engendrée par $X = \{p_i / x \in [\![1, n]\!]\}$.

Propriété 5

L'application f de $\mathbb{K}^n$ dans $\mathbb{K}$ est une fonction polynomiale si et seulement si il existe $(a_i)_{i\in\mathbb{N}^n}$ famille d'éléments de $\mathbb{K}$, de support fini J, telle que :

$$f = \sum_{i\in J} a_i p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n} \text{ (15)}$$

où on a posé $i = (i_1, i_2, \ldots, i_n)$.

(15) Pour $i \in \mathbb{N}^n \setminus J$ on a $a_i = 0$, on pourra donc aussi écrire : $f = \sum_{i\in\mathbb{N}^n} a_i p_1^{i_1} \cdots p_n^{i_n}$.

Notation

L'égalité $f = \sum_{i\in J} a_i p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}$ se lit aussi :

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{K}^n, f(x_1, \ldots, x_n) = \sum_{i\in J} a_i x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

De ce fait, la $\mathbb{K}$-algèbre des fonctions polynomiales sur $\mathbb{K}^n$ sera notée $\mathbb{K}[x_1, x_2, \ldots, x_n]$.

☞ Notons P l'ensemble des applications f de la forme $f = \sum_{i\in\mathbb{N}^n} a_i p_1^{i_1} \cdots p_n^{i_n}$ où $(a_i)_{i\in\mathbb{N}^n}$ décrit l'ensemble des familles presque nulles d'éléments de $\mathbb{K}$, indexées par $\mathbb{N}^n$.

Copyrighted material

On vérifie que P est un sous-espace vectoriel et un sous-anneau de $\mathcal{F}(\mathbb{R}^n, \mathbb{R})$.
Il est clair que P contient chacun des p_i, $1 \leqslant i \leqslant n$.
Enfin, si une sous-algèbre Q de $\mathcal{F}(\mathbb{R}^n, \mathbb{R})$ contient $\{p_i / i \in [\![1, n]\!]\}$, de par la structure de sous-anneau, Q contient tout élément de la forme :

$$p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n} \text{ avec } i = (i_1, i_2, \ldots, i_n) \in \mathbb{N}^n,$$

puis, la structure de sous-espace vectoriel montre que Q contient toute fonction polynomiale :

$$f = \sum_{i \in \mathbb{N}^n} a_i p_1^{i_1} \cdots p_n^{i_n}.$$ (16)

Ainsi, on a $P \subset Q$, et finalement P est la plus petite sous-algèbre de $\mathcal{F}(\mathbb{K}^n, \mathbb{K})$ contenant $p_1, p_2, \ldots, p_n$.

(16) $(a_i)_{i \in \mathbb{N}^n}$ famille de support fini.

5. Bases

- Une base de E est une famille $(b_i)_{i \in I}$ d'éléments de E qui est à la fois libre et génératrice de E.
- Une famille $(b_i)_{i \in I}$ est une base de E si et seulement si c'est une famille libre maximale.
- Une famille $(b_i)_{i \in I}$ est une base de E si et seulement si c'est une famille génératrice minimale.

Exemples usuels

1) La base canonique de $\mathbb{K}^n$ est $(e_i)_{1 \leqslant i \leqslant n}$ où :

$$\forall i \in [\![1, n]\!],\ e_i = (0, \ldots, 0, 1, 0, \ldots, 0) = (\delta_{k,i})_{1 \leqslant k \leqslant i}.$$ (17)

2) La base canonique de $\mathcal{M}_{n,p}(\mathbb{K})$ est la famille des matrices élémentaires : $(E_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}}$ où E_{ij} est la matrice de terme général $\delta_{k,i}\delta_{\ell,j}$, $1 \leqslant k \leqslant n$, $1 \leqslant \ell \leqslant p$.

3) La base canonique de $\mathbb{K}[x_1, x_2, \ldots, x_n]$ est $(p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n})_{(i_1, \ldots, i_n) \in \mathbb{N}^n}$. (18)
Étant donné que p_i est défini par $p_i(x_1, \ldots, x_n) = x_i$, cette base pourra être notée abusivement $(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n})_{(i_1, \ldots, i_n) \in \mathbb{N}^n}$.

(17) $\delta_{k,i}$ est le symbole de Kronecker : $\delta_{k,i} = 0$ si $k \neq i$, et $\delta_{i,i} = 1$.

(18) Notations du paragraphe 4 précédent.

6. Coordonnées

Propriété 6

Soit $(b_i)_{i \in I}$ une base de E. Pour tout vecteur $x \in E$, il existe une famille $(\lambda_i)_{i \in I}$ et une seule, de support fini, telle que $x = \sum_{i \in I} \lambda_i b_i$.

Pour tout $x \in E$, la famille $(\lambda_i)_{i \in I}$ de la propriété précédente est appelée la famille des **coordonnées** de x dans la base $(b_i)_{i \in I}$. (19)

Si $x \neq 0_E$, avec $J = \operatorname{Supp}(\lambda_i)_{i \in I}$, on a $x = \sum_{i \in I} \lambda_i b_i = \sum_{i \in J} \lambda_i b_i$.

(19) La famille des coordonnées de 0_E est la famille nulle.

Propriété 7

Détermination d'une application linéaire.
Soit E et F des $\mathbb{K}$-espaces vectoriels, $(b_i)_{i \in I}$ une base de E et $(c_i)_{i \in I} \in F^I$.

a) Il existe une application linéaire et une seule ϕ de E dans F telle que : $\forall i \in I,\ \varphi(b_i) = c_i$.

b) φ est injective si et seulement si $(c_i)_{i \in I}$ est une famille libre.

c) φ est surjective si et seulement si $(c_i)_{i \in I}$ est une famille génératrice de F.

d) φ est un isomorphisme si et seulement si $(c_i)_{i \in I}$ est une base de F.

L'application φ est déterminée de la manière suivante :

pour $x \in E$, de coordonnées $(\lambda_i)_{i \in I}$, $\varphi(x) = \varphi\left(\sum_{i \in I} \lambda_i b_i\right) = \sum_{i \in I} \lambda_i c_i$.

Copyrighted material

7. Dimension finie

Définition 6

Un $\mathbb{K}$-espace vectoriel est **de dimension finie** quand il a une famille génératrice finie. [20]

[20] Dans le cas contraire, on dit qu'il est de dimension infinie.

Propriété 8

Tout $\mathbb{K}$-espace vectoriel non nul de dimension finie admet une base finie.

Propriété 9

Si un $\mathbb{K}$-espace vectoriel E admet une famille génératrice de cardinal n, alors toute famille d'au moins $n+1$ vecteurs est liée.
Toute famille libre est de cardinal au plus n.

Propriété 10

Théorème de la dimension
Dans un $\mathbb{K}$-espace vectoriel E non nul et de dimension finie, toutes les bases ont le même nombre d'éléments.

Définition 7

Si E est un $\mathbb{K}$-espace vectoriel non nul de dimension finie, le nombre d'éléments d'une base est appelé la **dimension** de E. [21]
Il est noté $\dim_{\mathbb{K}} E$ ou $\dim E$ s'il n'y a pas d'ambiguïté.

[21] Par convention, l'espace vectoriel nul a pour dimension 0.

Propriété 11

Théorème d'échange
Soit E un $\mathbb{K}$-espace vectoriel non nul de dimension n.
Si L et G sont des parties de E respectivement libre et génératrice, on peut compléter la famille L par des éléments de G pour obtenir une base de E.

Théorème 1

Des $\mathbb{K}$-espaces vectoriels de dimensions finies sont isomorphes si et seulement si ils ont la même dimension.

Remarque

Si E est de dimension finie et si F est un $\mathbb{K}$-espace vectoriel isomorphe à E, alors F est de dimension finie et $\dim F = \dim E$.

Propriété 12

Dimension d'un sous-espace vectoriel
Un sous-espace vectoriel F d'un $\mathbb{K}$-espace vectoriel E est de dimension finie.
On a $\dim F \leqslant \dim E$ et $\dim F = \dim E$ si et seulement si $F = E$.

Théorème 2

Dimension d'un produit
Si $E_1, E_2, \ldots, E_n$ sont des $\mathbb{K}$-espaces vectoriels de dimensions finies, l'espace produit $\prod_{i=1}^{n} E_i = E_1 \times E_2 \times \cdots \times E_n$ est de dimension finie et :

$$\dim \prod_{i=1}^{n} E_i = \sum_{i=1}^{n} \dim E_i .$$

Quand $n = 2$, $E_1 \neq \{0_{E_1}\}$ et $E_2 \neq \{0_{E_2}\}$, si $(e_{1,i})_{1 \leqslant i \leqslant n_1}$ est une base de E_1 et $(e_{2,j})_{1 \leqslant j \leqslant n_2}$ est une base de E_2, une base de $E_1 \times E_2$ est :

$$\Big((e_{1,1}, 0_{E_2}), (e_{1,2}, 0_{E_2}), \ldots, (e_{1,n_1}, 0_{E_2}), (0_{E_1}, e_{2,1}), \ldots, (0_{E_1}, e_{2,n_2})\Big).$$

Copyrighted material

Théorème 3

Dimension de $\mathscr{L}(E, F)$

Si E et F sont des $\mathbb{K}$-espaces vectoriels de dimensions finies, $\mathscr{L}(E, F)$ est de dimension finie :

$$\dim \mathscr{L}(E, F) = \dim E \cdot \dim F.$$

Soit $(e_j)_{1 \leqslant j \leqslant n}$ et $(f_i)_{1 \leqslant i \leqslant p}$ des bases de E et F respectivement.

Une base de $\mathscr{L}(E, F)$ est alors $(\varphi_{ij})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}}$ où les φ_{ij} sont les éléments de $\mathscr{L}(E, F)$ caractérisés par : $\forall k \in [\![1, n]\!], \quad \varphi_{ij}(e_k) = \delta_{jk} f_i$.

Remarques

1) Soit $u \in \mathscr{L}(E, F)$, en posant $u(e_j) = \sum_{i=1}^{n} a_{ij} f_i$, on a $u = \sum_{i=1}^{p} \sum_{j=1}^{n} a_{ij} \varphi_{ij}$.

$A = [a_{ij}]$ est la matrice de u par rapport aux bases $(e_j)_{1 \leqslant j \leqslant n}$ et $(f_i)_{1 \leqslant i \leqslant p}$.

2) En notant E_{ij} les matrices élémentaires, on a $A = \sum_{i=1}^{p} \sum_{j=1}^{n} a_{ij} E_{ij}$.

E_{ij} est la matrice de φ_{ij} par rapport aux bases $(e_j)_{1 \leqslant j \leqslant n}$ et $(f_i)_{1 \leqslant i \leqslant p}$.

C. Somme de sous-espaces vectoriels

1. Somme, somme directe de deux sous-espaces [22]

[22] Ce cas a été traité en première année.

Soit F_1 et F_2 des sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E.

1.1 – Somme

- La **somme** de F_1 et F_2 est l'ensemble $F_1 + F_2 = \{x_1 + x_2 \mid x_1 \in F_1 , x_2 \in F_2\}$. [23]
- Si F_1 et F_2 sont de dimensions finies :

$$\dim(F_1 + F_2) = \dim F_1 + \dim F_2 - \dim(F_1 \cap F_2)$$

[23] F_1+F_2 est le sous-espace vectoriel engendré par $F_1 \cup F_2$.

1.2 – Somme directe

- La **somme** $F_1 + F_2$ est **directe** lorsque $F_1 \cap F_2 = \{0_E\}$; on la note alors $F_1 \oplus F_2$.
- La somme $F_1 + F_2$ est directe si et seulement si pour chaque $x \in F_1 + F_2$,
  il existe un unique $(x_1 , x_2) \in F_1 \times F_2$ tel que $x = x_1 + x_2$.
- La somme $F_1 + F_2$ est directe si et seulement si l'application φ de $F_1 \times F_2$ dans E,
  $\varphi : (x_1 , x_2) \mapsto x_1 + x_2$, est injective.
- La somme $F_1 + F_2$ est directe si et seulement si , pour tout $(x_1 , x_2) \in F_1 \times F_2$,
  $x_1 + x_2 = 0 \Rightarrow x_1 = x_2 = 0$.

1.3 – Sous-espaces supplémentaires

Soit F_1, F_2 des sous-espaces d'un $\mathbb{K}$-espace vectoriel E et $\varphi \in \mathscr{L}(F_1 \times F_2, E)$,

$$\varphi : (x_1 , x_2) \mapsto x_1 + x_2 .$$

- F_1 et F_2 sont **supplémentaires dans** E lorsque $F_1 \oplus F_2 = E$, c'est-à-dire si et seulement si :
  $F_1 + F_2 = E$ et $F_1 \cap F_2 = \{0_E\}$.
- Les sous-espaces F_1 et F_2 sont supplémentaires dans E lorsque l'application φ est bijective, donc lorsque pour tout $x \in E$, il existe un unique $(x_1 , x_2) \in F_1 \times F_2$ tel que $x = x_1 + x_2$.
- On suppose $E = F_1 \oplus F_2$. L'application $\psi : E \to F_1 \times F_2$, $x \mapsto x_1 + x_2$, où (x_1 , x_2) est l'unique couple de $F_1 \times F_2$ tel que $x = x_1 + x_2$, est linéaire. [24]

[24] ψ n'est autre que φ^{-1}.

Copyrighted material

Théorème 4

Caractérisation d'une application linéaire ✎(25)

Soit E et F des $\mathbb{K}$-espaces vectoriels, alors $f \in \mathscr{L}(E, F)$ est caractérisée par ses restrictions à des sous-espaces A et B supplémentaires dans E.

✎(25) Ce théorème et le suivant ont été vus en Algèbre et Géométrie, MPSI, au chapitre 9.

Théorème 5

Théorème noyau-image

Soit E et E' des $\mathbb{K}$-espaces vectoriels. Pour tout $f \in \mathscr{L}(E, E')$, $\operatorname{Im} f$ est isomorphe à tout supplémentaire de $\operatorname{Ker} f$. ✎(26)

✎(26) Si G est un supplémentaire de $\operatorname{Im} f$, l'application $\overline{f}$ de G dans $\operatorname{Im} f$ induite par f est un isomorphisme.

Propriété 13

Des sous-espaces G et G' supplémentaires dans un $\mathbb{K}$-espace vectoriel E d'un même sous-espace vectoriel F sont isomorphes.

☞ Soit p la projection sur G parallèlement à F. On a $\operatorname{Ker} p = F$ et $\operatorname{Im} p = G$. ✎(27)
Le théorème noyau-image assure alors que G' est isomorphe à G.

✎(27) Les projecteurs sont brièvement repris au paragraphe suivant.

2. Codimension

Définition 8

Étant donné un $\mathbb{K}$-espace vectoriel E, on dit qu'un sous-espace vectoriel est de **codimension finie** quand il admet un supplémentaire de dimension finie. ✎(28)

✎(28) E n'est pas supposé de dimension finie.

Propriété 14

Si F est un sous-espace de codimension finie d'un $\mathbb{K}$-espace vectoriel E, alors tous les supplémentaires de F dans E ont la même dimension.

☞ Soit G un supplémentaire de dimension finie de F dans E. ✎(29)
Si G' est aussi un supplémentaire de F dans E, alors G et G' sont isomorphes.
Il s'ensuit que G' est de dimension finie et $\dim G' = \dim G$.

✎(29) Il en existe un, par définition de codimension finie pour F.

Définition 9

Si F est un sous-espace de codimension finie de E, la **codimension** de F est la dimension d'un supplémentaire G de F. On note $\operatorname{codim}_E F = \dim G$.

Corollaire

Si E est un $\mathbb{K}$-espace vectoriel de dimension finie, alors tout sous-espace vectoriel F est de codimension finie et $\operatorname{codim}_E F = \dim E - \dim F$.

Hyperplans

Les hyperplans sont les sous-espaces qui admettent un supplémentaire de dimension 1.
Ce sont donc les sous-espaces de codimension égale à 1.

Exemple 2 Sous-espaces supplémentaires dans $\mathbb{R}[X]$.

Soit $\mathbb{K}[X]$ l'espace vectoriel des polynômes à coefficients dans $\mathbb{K}$, n un entier naturel et $\mathbb{K}_n[X]$ le sous-espace vectoriel formé des polynômes de degré inférieur ou égal à n.

Soit P un polynôme fixé de degré égal à $n+1$; alors l'ensemble $P\,\mathbb{K}[X]$ des multiples de P est un sous-espace vectoriel de $\mathbb{K}[X]$, de codimension finie égale à n.

- $P\,\mathbb{K}[X]$ contient le polynôme nul, il est donc non vide.

Pour tous PQ_1, PQ_2 éléments de $P\,\mathbb{K}[X]$ et tout $(\lambda_1, \lambda_2) \in \mathbb{K}^2$, on a :

$$\lambda_1 PQ_1 + \lambda_2 PQ_2 = P(\lambda_1 Q_1 + \lambda_2 Q_2) \quad \text{avec} \quad \lambda_1 Q_1 + \lambda_2 Q_2 \in \mathbb{K}[X],$$

donc :
$$\lambda_1 PQ_1 + \lambda_2 PQ_2 \in P\,\mathbb{K}[X].$$

Copyrighted material

▪ Pour tout $A \in \mathbb{K}[X]$, la division euclidienne de A par P donne l'existence de deux polynômes Q et R tels que :

$$\textbf{(1)}\ A = R + PQ \quad \text{et} \quad \textbf{(2)}\ \deg R < \deg P \ \text{ ou } \ R = 0.$$

La condition **(2)** se lit aussi $R \in \mathbb{K}_n[X]$ et alors **(1)** donne $\mathbb{K}[X] = \mathbb{K}_n[X] + P\,\mathbb{K}[X]$.

D'autre part, pour tout U non nul de $P\,\mathbb{K}[X]$, on a :

$$\deg U \geqslant \deg P \quad \text{c'est-à-dire} \quad \deg U \geqslant n+1,$$

et pour tout U non nul de $\mathbb{K}_n[X]$, $\deg U \leqslant n$. Il en résulte que $\mathbb{K}_n[X] \cap P\,\mathbb{K}[X] = \{0_{\mathbb{K}[X]}\}$. Finalement :

$$\mathbb{K}[X] = \mathbb{K}_n[X] \oplus P\,\mathbb{K}[X].$$

3. Projecteurs et involutions linéaires

3.1 – Projecteurs

▪ Un **projecteur** de E est un endomorphisme p de E tel que $p^2 = p$. [30]

[30] On dit aussi endomorphisme idempotent.

▪ Pour tout projecteur p de E, on a $E = \operatorname{Im} p \oplus \operatorname{Ker} p$.

▪ Si p est un projecteur de E, $\operatorname{Im} p$ est l'ensemble des invariants de p : $\operatorname{Im} p = \{x \in E \,/\, p(x) = x\}$.

▪ Soit $p \in \mathcal{L}(E)$, alors p est un projecteur si et seulement si $\operatorname{Id}_E - p$ est un projecteur.

▪ Si p est un projecteur de E, $\operatorname{Im} p = \operatorname{Ker}\left(\operatorname{Id}_E - p\right)$, $\operatorname{Ker} p = \operatorname{Im}\left(\operatorname{Id}_E - p\right)$

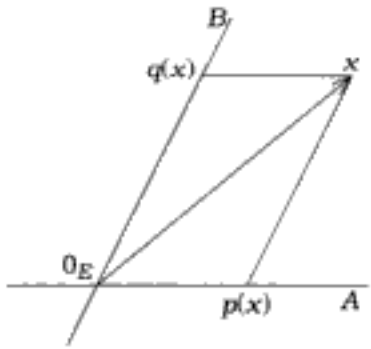
▪ Si A et B sont deux sous-espaces vectoriels supplémentaires dans E, pour tout x de E, il existe un unique $(x_1 , x_2) \in A \times B$ tel que $x = x_1 + x_2$.
Les applications :

$$p : E \to E \ , \ x \mapsto x_1$$
$$\text{et} \quad q : E \to E \ , \ x \mapsto x_2$$

sont des projecteurs tels que :

$$\operatorname{Im} p = \operatorname{Ker} q = A$$
$$\operatorname{Im} q = \operatorname{Ker} p = B$$
$$p + q = \operatorname{Id}_E \ , \ p \circ q = q \circ p = 0$$

p (resp. q) est appelé **projection sur** A (resp. B) **parallèlement à** B (resp. A).



▪ Si p est un projecteur de E alors c'est la projection sur $\operatorname{Im} p$ parallèlement à $\operatorname{Ker} p$.

3.2 – Involutions linéaires (ou symétries)

▪ Une **symétrie** de E est un endomorphisme $s \in \mathcal{L}(E)$ involutif, c'est-à-dire tel que $s^2 = \operatorname{Id}_E$. C'est donc un automorphisme tel que $s^{-1} = s$.

▪ $s \in \mathcal{L}(E)$ est une symétrie si et seulement si $p = \dfrac{1}{2}\left(s + \operatorname{Id}_E\right)$ est un projecteur.

La symétrie s et le projecteur p sont dits **associés** et on a :

$$p = \frac{1}{2}\left(s + \operatorname{Id}_E\right) . \ s = 2p - \operatorname{Id}_E$$

$$\operatorname{Im} p = \operatorname{Ker}\left(s - \operatorname{Id}_E\right) , \ \operatorname{Ker} p = \operatorname{Ker}\left(s + \operatorname{Id}_E\right)$$

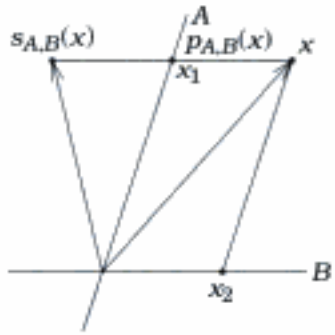
$$E = \operatorname{Im} p \oplus \operatorname{Ker} p = \operatorname{Ker}\left(s - \operatorname{Id}_E\right) \oplus \operatorname{Ker}\left(s + \operatorname{Id}_E\right)$$

▪ Si A et B sont deux sous-espaces supplémentaires dans E, pour tout x de E, il existe un unique $(x_1 , x_2) \in A \times B$ tel que $x = x_1 + x_2$.

Copyrighted material

L'application $s_{A,B} : E \to E,\ x \mapsto x_1 - x_2$ est la symétrie associée au projecteur $p_{A,B} : x \mapsto x_1$.

$s_{A,B}$ est appelée **symétrie par rapport à A, parallèlement à B.**



- Pour toute symétrie s de E, en posant :

  $A = \{x \in E \,/\, s(x) = x\}$ (invariants de s)

  $B = \{x \in E \,/\, s(x) = -x\}$ (éléments transformés en leurs opposés)

on a $E = A \oplus B$ et s est la symétrie par rapport à A parallèlement à B.

4. Somme de n sous-espaces vectoriels

Soit $F_1, F_2, \ldots, F_n$ des sous-espaces vectoriels d'un $\mathbb{K}$-espace vectoriel E.

4.1 – Somme

Définition 10

On appelle **somme** des F_i, $1 \leqslant i \leqslant n$, et on note :

$$F_1 + F_2 + \cdots + F_n \quad \text{ou} \quad \sum_{1 \leqslant i \leqslant n} F_i$$

l'ensemble des vecteurs $\sum_{i=1}^{n} x_i$ où pour tout $i \in [\![1, n]\!]$, x_i décrit F_i.

Propriété 15

$\varphi : F_1 \times F_2 \times \cdots \times F_n \to E,\ (x_1, \ldots, x_n) \mapsto x_1 + x_2 + \cdots + x_n$ est linéaire.
Son image est $F_1 + F_2 + \cdots + F_n$ qui est donc un sous-espace vectoriel de E.

Propriété 16

$F_1 + F_2 + \cdots + F_n$ est le sous-espace vectoriel de E engendré par $\bigcup_{1 \leqslant i \leqslant n} F_i$.

☞
- Pour tout $i \in [\![1, n]\!]$ et tout $x_i \in F_i$ en écrivant $x_i = 0 + \cdots + 0 + x_i + 0 + \cdots + 0$ avec $(0, \ldots, 0, x_i, 0, \ldots, 0) \in F_1 \times F_2 \times \cdots \times F_n$, on voit que $x_i \in F_1 + F_2 + \cdots + F_n$.
Ainsi $\forall i \in [\![1, n]\!]$, $\sum_{1 \leqslant j \leqslant n} F_j \supset F_i$ donc $\sum_{1 \leqslant i \leqslant n} F_i \supset \bigcup_{1 \leqslant i \leqslant n} F_i$ et, puisque $\sum_{1 \leqslant i \leqslant n} F_i$ est un sous-espace vectoriel de E, on a $\sum_{1 \leqslant i \leqslant n} F_i \supset \text{Vect}\left(\bigcup_{1 \leqslant i \leqslant n} F_i\right)$.
- Pour tout $(x_1, x_2, \ldots, x_n) \in F_1 \times F_2 \times \cdots \times F_n$, $x_1, x_2, \ldots, x_n$ sont dans $\bigcup_{1 \leqslant i \leqslant n} F_i$, donc appartiennent à $\text{Vect}\left(\bigcup_{1 \leqslant i \leqslant n} F_i\right)$ et puisqu'il s'agit là d'un sous-espace vectoriel de E, on a $x_1 + x_2 + \cdots + x_n \in \text{Vect}\left(\bigcup_{1 \leqslant i \leqslant n} F_i\right)$. Ainsi $\sum_{1 \leqslant i \leqslant n} F_i \subset \text{Vect}\left(\bigcup_{1 \leqslant i \leqslant n} F_i\right)$.

4.2 – Somme directe

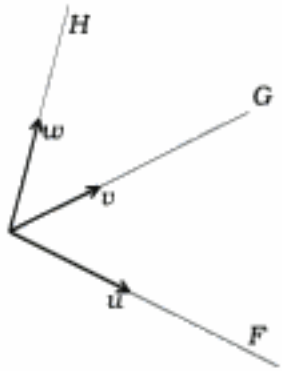
Définition 11

La somme $\sum_{1 \leqslant i \leqslant n} F_i$ est **directe** lorsque : $\forall j \in [\![1, n]\!],\ F_j \cap \sum_{\substack{1 \leqslant i \leqslant n \\ i \neq j}} F_i = \{0_E\}$.

On note alors : $\bigoplus_{1 \leqslant i \leqslant n} F_i$ ou $F_1 \oplus F_2 \oplus F_3 \oplus \cdots \oplus F_n$.

Copyright Material

Exemples



- Dans $\mathbb{R}^3$, soit trois vecteurs u, v, w formant un système libre.

$$F = \mathbb{R}u \quad , \quad G = \mathbb{R}v \quad , \quad H = \mathbb{R}w.$$

La somme $F + G + H$ est directe et égale à $\mathbb{R}^3$.

$$\mathbb{R}^3 = F \oplus G \oplus H.$$

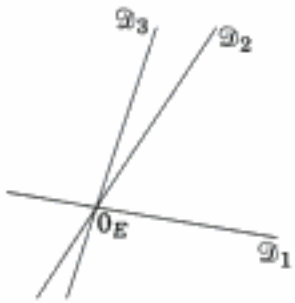
- Dans $E = \mathbb{R}_4[X]$ espace vectoriel des polynômes P tels que $\deg P \leqslant 4$, soit :

$$F = \text{Vect}\left(X^2, X^4\right) \quad , \quad G = \text{Vect}(X) \quad , \quad H = \text{Vect}\left(X^3\right).$$

La somme $F + G + H$ est directe mais n'est pas égale à $\mathbb{R}_4[X]$ car le seul polynôme constant appartenant à $F \oplus G \oplus H$ est le polynôme nul.

Remarque

Si la somme $\sum_{1 \leqslant i \leqslant n} F_i$ est directe, alors pour tout couple $(i, j) \in [\![1, n]\!]^2$ tel que $i \neq j$, on a $F_i \cap F_j = \{0_E\}$. Mais il faut prendre garde au fait que ces conditions ne permettent pas de conclure que la somme $\sum_{1 \leqslant i \leqslant n} F_i$ est directe.



Considérer, par exemple, dans le plan $\mathbb{R}^2$ trois droites vectorielles $\mathfrak{D}_1$, $\mathfrak{D}_2$, $\mathfrak{D}_3$ telles que :

$$\mathfrak{D}_1 \cap \mathfrak{D}_2 = \{0_E\}.$$
$$\mathfrak{D}_2 \cap \mathfrak{D}_3 = \{0_E\}.$$
$$\mathfrak{D}_3 \cap \mathfrak{D}_1 = \{0_E\}.$$

On a alors $\mathbb{R}^2 = \mathfrak{D}_1 \oplus \mathfrak{D}_2$ donc :

$$\mathfrak{D}_3 \cap (\mathfrak{D}_1 + \mathfrak{D}_2) = \mathfrak{D}_3 \neq \{0_E\}$$

Propriété 17

La somme $\sum_{1 \leqslant i \leqslant n} F_i$ est directe si et seulement si pour tout $x \in \sum_{1 \leqslant i \leqslant n} F_i$, il existe un unique $(x_1, x_2, \ldots, x_n) \in F_1 \times F_2 \times \ldots \times F_n$ tel que $x = x_1 + x_2 + \ldots + x_n$.

- Supposons que la somme $\sum_{1 \leqslant i \leqslant n} F_i$ soit directe. Soit alors :

$(x_1, x_2, \ldots, x_n) \in F_1 \times F_2 \times \ldots \times F_n$ et $(x'_1, x'_2, \ldots, x'_n) \in F_1 \times F_2 \times \ldots \times F_n$ tels que $x_1 + x_2 + \ldots + x_n = x'_1 + x'_2 + \ldots + x'_n$. Pour tout $i \in [\![1, n]\!]$, on a alors :

$$x_i - x'_i = \sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} x'_j - x_j \text{ donc } x_i - x'_i \in F_i \cap \sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j \text{ puis } x_i = x'_i.$$

- Supposons que pour tout $x \in \sum_{1 \leqslant i \leqslant n} F_i$ il existe $(x_1, x_2, \ldots, x_n) \in F_1 \times F_2 \times \ldots \times F_n$ unique tel que : $x = x_1 + x_2 + \ldots + x_n$.

Soit x élément de $F_i \cap \sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j$, alors il existe $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in \prod_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j$ tel que : $x = x_1 + \ldots + x_{i-1} + x_{i+1} + \ldots + x_n$.

On peut donc écrire :

$$x_1 + \ldots + x_{i-1} + 0_E + x_{i+1} + \ldots + x_n = 0_E + \ldots + 0_E + x + 0_E + \ldots + 0_E$$

avec $(x_1, \ldots, x_{i-1}, 0_E, x_{i+1}, \ldots, x_n) \in F_1 \times \ldots \times F_i \times \ldots \times F_n$,

et $(0_E, \ldots, 0_E, x, 0_E, \ldots, 0_E) \in F_1 \times \ldots \times F_i \times \ldots \times F_n$.

Copyrighted material

D'après l'hypothèse, ces n-uplets sont égaux donc $x = 0_E$ et on a : $F_i \cap \sum_{\substack{1 \leqslant j \leqslant n \\ j \neq i}} F_j = \{0_E\}$.

Propriété 18

La somme $\sum_{1 \leqslant i \leqslant n} F_i$ est directe si et seulement si l'application :

$$\varphi : F_1 \times F_2 \times \cdots \times F_n \to E, (x_1, x_2, \ldots, x_n) \mapsto x_1 + x_2 + \cdots + x_n$$

est injective. (31)

(31) C'est une autre formulation de la propriété précédente.

Propriété 19

La somme $\sum_{1 \leqslant i \leqslant n} F_i$ est directe si et seulement si :

$$\forall (x_1, x_2, \ldots, x_n) \in F_1 \times F_2 \times \cdots \times F_n,$$
$$x_1 + x_2 + \cdots + x_n = 0_E \Rightarrow x_1 = x_2 = \cdots = x_n = 0_E.$$

☞ L'application linéaire φ est injective si et seulement si son noyau est réduit à $\{0_E\}$.

Propriété 20

La somme $\sum_{1 \leqslant i \leqslant n} F_i$ est directe si et seulement si les sommes :

$$G = \sum_{1 \leqslant i \leqslant n-1} F_i \text{ et } G + F_n \text{ sont directes.}$$

☞ Supposons que les sommes $\sum_{1 \leqslant i \leqslant n-1} F_i$ et $G + F_n$ soient directes.

Soit $(x_1, \ldots, x_n) \in F_1 \times F_2 \times \cdots \times F_n$ tel que $\sum_{i=1}^{n} x_i = 0_E$.

La somme $G + F_n$ étant directe, il vient $x_n = \sum_{i=1}^{n-1} x_i = 0_E$.

Alors la somme $\sum_{1 \leqslant i \leqslant n-1} F_i$ étant directe, $\sum_{i=1}^{n-1} x_i = 0_E$ donne : $x_i = 0_E$ pour $1 \leqslant i \leqslant n-1$.

Ainsi $\sum_{1 \leqslant i \leqslant n} F_i$ est directe. La réciproque est évidente.

Exemple 3 Réunion de familles libres

Soit $F_1, \ldots, F_n$ n sous-espaces vectoriels de E tels que la somme $F = \sum_{1 \leqslant i \leqslant n} F_i$ soit directe, et $(x_i)_{i \in I}$ une famille de vecteurs «réunion» de n sous-familles $(x_i)_{i \in I_k}$, $1 \leqslant k \leqslant n$, telles que :

$$\forall k \in [\![1, n]\!], \quad \forall i \in I_k, \quad x_i \in F_k.$$

$I_1, \ldots, I_n$ réalise une partition de I : $I = \bigcup_{1 \leqslant k \leqslant n} I_k$ et $\forall k \neq \ell, \ I_k \cap I_\ell = \varnothing$.

Alors $(x_i)_{i \in I}$ est libre si et seulement si les n sous-familles $(x_i)_{i \in I_k}$ sont libres.

- Si $(x_i)_{i \in I}$ est libre, toute sous-famille est libre, c'est donc le cas pour les $(x_i)_{i \in I_k}$.
- Si les $(x_i)_{i \in I_k}$, $1 \leqslant k \leqslant n$, sont libres, soit $(\lambda_i)_{i \in I}$ une famille de scalaires de support fini telles que $\sum_{i \in I} \lambda_i x_i = 0_E$.

Posons $y_k = \sum_{i \in I_k} \lambda_i x_i$, on a alors $\sum_{i \in I} \lambda_i x_i = \sum_{k=1}^{n} y_k$ et $y_k \in F_k$.

Copyrighted material

La somme $\sum_{1\leqslant k\leqslant n} F_k$ étant directe, l'égalité $\sum_{k=1}^{n} y_k = 0_E$ donne : $y_1 = y_2 = \cdots = y_n = 0_E$.

Chaque famille $(x_i)_{i\in I_k}$ étant libre, $\sum_{i\in I_k} \lambda_i x_i = 0$, $1 \leqslant k \leqslant n$, donne enfin :

$$\forall k \in [\![1, n]\!],\ \forall i \in I_k,\ \lambda_i = 0 \text{ donc } \forall i \in I,\ \lambda_i = 0.$$

On a ainsi prouvé que $(x_i)_{i\in I}$ est libre.

4.3 – Sous-espaces supplémentaires

Définition 12

Les sous-espaces $F_1, F_2, \ldots, F_n$ sont dits **supplémentaires** dans E lorsque leur somme est directe, égale à E : $E = \bigoplus_{1\leqslant i\leqslant n} F_i$.

Propriété 21

$F_1, F_2, \ldots, F_n$ sont supplémentaires dans E si et seulement si :

$$\sum_{1\leqslant i\leqslant n} F_i = E \quad \text{et} \quad \forall i \in [\![1, n]\!],\ F_i \cap \sum_{\substack{1\leqslant j\leqslant n \\ j\neq i}} F_j = \{0_E\}.$$

Propriété 22

$F_1, F_2, \ldots, F_n$ sont supplémentaires dans E si et seulement si l'application :

$$\varphi : F_1 \times F_2 \times \cdots \times F_n \to E,\ (x_1, x_2, \ldots, x_n) \mapsto x_1 + x_2 + \cdots + x_n$$

est bijective, c'est-à-dire si et seulement si, pour tout $x \in E$, il existe un unique

$$(x_1, \ldots, x_n) \in F_1 \times F_2 \times \cdots \times F_n$$

tel que : $x = x_1 + x_2 + \cdots + x_n$.

4.4 – Sous-espaces supplémentaires et projecteurs

Propriété 23

Soit $F_1, \ldots, F_n$ des sous-espaces vectoriels supplémentaires dans E.

Pour tout $i \in [\![1, n]\!]$, soit p_i le projecteur d'image F_i et de noyau $\sum_{1\leqslant j\leqslant n,\ j\neq i} F_j$. La **famille de projecteurs** $(p_i)_{1\leqslant i\leqslant n}$ est dite **associée** à la somme directe $E = \bigoplus_{1\leqslant i\leqslant n} F_i$; elle vérifie les propriétés :

$$\textbf{(1)}\ \sum_{i=1}^{n} p_i = \mathrm{Id}_E \qquad \textbf{(2)}\ \forall (i, j) \in [\![1, n]\!]^2,\ i \neq j \ \Rightarrow\ p_i \circ p_j = 0.$$

☞ Posons $G_i = \sum_{1\leqslant j\leqslant n,\ j\neq i} F_j$, on a pour tout $i \in [\![1, n]\!]$, $E = F_i \oplus G_i$.

Tout x de E s'écrit de manière unique : $x = \sum_{j=1}^{n} x_j$, $x_j \in F_j$ donc aussi $x = x_i + x_i'$ avec :

$$x_i \in F_i \text{ et } x_i' = \sum_{1\leqslant j\leqslant n,\ j\neq i} x_j,\ x_i' \in G_i.$$

p_i est donc le projecteur qui à tout x de E associe x_i composante de x sur F_i.

L'égalité $x = \sum_{i=1}^{n} x_i$ s'écrit $x = \sum_{i=1}^{n} p_i(x)$ d'où $\sum_{i=1}^{n} p_i = \mathrm{Id}_E$. **(1)**

Si $i \neq j$, on a $F_j \subset \sum_{1\leqslant k\leqslant n,\ k\neq i} F_k$ donc $\mathrm{Im}\, p_j \subset \mathrm{Ker}\, p_i$ et $p_i \circ p_j = 0$. **(2)**

Copyrighted material

Propriété 24

Soit $(p_i)_{1\leqslant i\leqslant n}$ une famille finie d'endomorphismes de E vérifiant les propriétés **(1)** et **(2)** :

$$\textbf{(1)}\quad \sum_{i=1}^{n} p_i = \mathrm{Id}_E \qquad \textbf{(2)}\quad \forall (i,j)\in [\![1,n]\!]^2,\ i\neq j \ \Rightarrow\ p_i\circ p_j = 0.$$

Alors les sous-espaces $F_i = \mathrm{Im}\, p_i$, $1\leqslant i\leqslant n$, sont supplémentaires dans E et $(p_i)_{1\leqslant i\leqslant n}$ est la famille de projecteurs associée à la somme directe $E = \bigoplus_{1\leqslant i\leqslant n} F_i$.

☞ **(1)** donne $\sum_{i=1}^{n} p_j\circ p_i = p_j$ et, avec **(2)**, il reste $p_j^2 = p_j$: les p_j sont donc des projecteurs.

Avec **(1)**, il vient $\forall x\in E,\ x = \sum_{i=1}^{n} p_i(x)$. Or $p_i(x)\in F_i$, et il s'ensuit $E = \sum_{1\leqslant i\leqslant n} F_i$.

Soit maintenant $x_1\in F_1,\ x_2\in F_2,\ \ldots,\ x_n\in F_n$ tels que $\sum_{j=1}^{n} x_j = 0_E$.

p_j étant un projecteur, on a $F_j = \mathrm{Im}\, p_j = \mathrm{Inv}\,(p_j)$, d'où $p_j(x_j) = x_j$ donc $\sum_{j=1}^{n} p_j(x_j) = 0_E$.

En composant par p_i, il vient $\sum_{j=1}^{n} p_i\circ p_j(x_j) = 0_E$ donc, d'après la propriété **(2)**, il reste $p_i^2(x_i) = 0_E$ c'est-à-dire $x_i = 0$ car $p_i^2 = p_i$ et $x_i\in \mathrm{Im}\, p_i$.

On a ainsi prouvé que la somme $\sum_{1\leqslant i\leqslant n} F_i$ est directe : $E = \bigoplus_{1\leqslant i\leqslant n} F_i$.

Ainsi tout x de E se décompose de manière unique sous la forme : $x = \sum_{j=1}^{n} x_j\ ,\ x_j\in F_j$.

Alors $p_i(x) = p_i^2(x_i) = x_i$ et p_i est le projecteur d'image F_i, de noyau $G_i = \sum_{1\leqslant j\leqslant n,\ j\neq i} F_j$.

Exemple 4 Combinaison linéaire de projecteurs

Soit $(p_i)_{1\leqslant i\leqslant n}$ une famille de projecteurs de E associée à une somme directe $E = \bigoplus_{1\leqslant i\leqslant n} F_i$ et $(\lambda_i)_{1\leqslant i\leqslant n}\in \mathbb{K}^n$. On pose $f = \sum_{i=1}^{n} \lambda_i p_i$, et on se propose de calculer f^k pour tout $k\in\mathbb{N}^*$.

p_1 et p_2 étant permutables, (32) on a : $(\lambda_1 p_1 + \lambda_2 p_2)^k = \sum_{j=0}^{k} \binom{j}{k} \lambda_1^j \lambda_2^{k-j}\, p_1^j\circ p_2^{k-j}$.

(32) Formule du binôme. $p_i^0 = \mathrm{Id}_E$.

Sachant que $p_1\circ p_2 = 0$, il reste $(\lambda_1 p_1 + \lambda_2 p_2)^k = \lambda_1^k p_1 + \lambda_2^k p_2$.

On termine par récurrence sur n pour arriver à $f^k = \sum_{i=1}^{n} \lambda_i^k p_i$.

Théorème 6

Caractérisation d'une application linéaire (33)

Soit E et F des $\mathbb{K}$-espaces vectoriels. Une application linéaire de E dans F est caractérisée par ses restrictions à n sous-espaces $A_1,\ \ldots,\ A_n$ supplémentaires dans E.

(33) Extension du théorème 4.

☞ $E = \bigoplus_{1\leqslant i\leqslant n} A_i$.

Montrons que, étant donné $u_i\in \mathscr{L}(A_i, F)$, $1\leqslant i\leqslant n$, il existe une et une seule application linéaire f de E dans F telle que $\forall i\in [\![1,n]\!],\ f_{|A_i} = u_i$.

Copyrighted material

▪ Unicité

Supposons que f existe, alors sachant que tout x de E se décompose de manière unique sous la forme $x = \sum_{i=1}^{n} x_i$, $x_i \in A_i$, on obtient : $f(x) = \sum_{i=1}^{n} f(x_i) = \sum_{i=1}^{n} u_i(x_i)$.

Cette expression de $f(x)$ prouve l'unicité, sous réserve d'existence.

▪ Existence

On vérifie que l'application $f : E \to F$ définie par : $f : x \mapsto \sum_{i=1}^{n} u_i(x_i)$ où les x_i sont tels que $x = \sum_{i=1}^{n} x_i$ avec $\forall i \in [\![1, n]\!], x_i \in A_i$, est linéaire et telle que :

$$\forall i \in [\![1, n]\!], \quad f_{|A_i} = u_i .$$

En introduisant les projecteurs p_i associés à la somme directe $E = \bigoplus_{1 \leqslant i \leqslant n} A_i$, on a $f = \sum_{i=1}^{n} u_i \circ p_i$ ce qui prouve que $f \in \mathscr{L}(E)$ et $f_{|A_i} = u_i$.

4.5 – Sommes directes en dimension finie

Théorème 7

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Si la somme $\sum_{1 \leqslant i \leqslant n} F_i$ de n sous-espaces vectoriels de E est directe, on a :

$$\dim \bigoplus_{1 \leqslant i \leqslant n} F_i = \sum_{i=1}^{n} \dim F_i$$

et $F_1, \ldots, F_n$ sont supplémentaires dans E si et seulement si : $\sum_{i=1}^{n} \dim F_i = \dim E$.

Définition 13

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et $F_1, \ldots, F_n$ n sous-espaces vectoriels supplémentaires dans E :

$$E = \bigoplus_{i=1}^{n} F_i \text{ avec } \forall i \in [\![1, n]\!], \quad F_i \neq \{0_E\}.$$

Si $\mathscr{B}_1 = (e_1, \ldots, e_{p_1})$ est une base de F_1,
$\mathscr{B}_2 = (e_{p_1+1}, \ldots, e_{p_1+p_2})$ est une base de F_2,
$\ldots \quad \ldots \quad \ldots$
$\mathscr{B}_n = (e_{p_1+\cdots+p_{n-1}+1}, \ldots, e_{p_1+p_2+\cdots+p_n})$ est une base de F_n,

alors $\mathscr{B} = (e_i)_{1 \leqslant i \leqslant N}$ avec $N = \sum_{i=1}^{n} p_i$ est une base de E dite **adaptée à la décomposition** :

$$E = \bigoplus_{1 \leqslant i \leqslant n} F_i .$$

5. Polynômes d'interpolation de Lagrange

Théorème 8

Soit $a_0, a_1, \ldots, a_n$ $n+1$ scalaires fixés deux à deux distincts.
Pour tout $(\lambda_0, \lambda_1, \ldots, \lambda_n) \in \mathbb{K}^{n+1}$, il existe un unique polynôme P de degré inférieur ou égal à n et tel que $P(a_0) = \lambda_0 P(a_1) = \lambda_1, \ldots, P(a_n) = \lambda_n$.

☞ Considérons $u : \mathbb{K}[X] \to \mathbb{K}^{n+1}$, $u : P \mapsto (P(a_0), P(a_1), \ldots, P(a_n))$.
$P(a_0) = \lambda_0 P(a_1) = \lambda_1, \ldots, P(a_n) = \lambda_n$ se lit : $u(P) = (\lambda_0, \lambda_1, \ldots, \lambda_n)$.

Copyrighted material

- Il est clair que u est linéaire.

$\operatorname{Ker} u$ est constitué des polynômes P admettant $a_0, a_1, \ldots, a_n$ pour racines, donc en posant $N = \prod_{i=0}^{n} (X - a_i)$, $\operatorname{Ker} u$ est l'ensemble des multiples de N : $\operatorname{Ker} u = N\,\mathbb{K}[X]$.

- Avec $\deg N = n+1$, un supplémentaire de $N\,\mathbb{K}[X]$ dans $\mathbb{K}[X]$ est $\mathbb{K}_n[X]$. (34)
- La restriction $u_{|\mathbb{K}_n[X]}$ induit un isomorphisme v de $\mathbb{K}_n[X]$ sur $\operatorname{Im} u$. (35)

Il en résulte $\dim \operatorname{Im} u = \dim \mathbb{K}_n[X] = n+1$ et donc $\operatorname{Im} u = \mathbb{K}^{n+1}$, v est donc un isomorphisme de $\mathbb{K}_n[X]$ sur $\mathbb{K}^{n+1}$.

En conséquence,pour tout $(\lambda_0, \lambda_1, \ldots, \lambda_n) \in \mathbb{K}^{n+1}$, il existe un unique P dans $\mathbb{K}_n[X]$ tel que $u(P) = (\lambda_0, \lambda_1, \ldots, \lambda_n)$, il s'agit de $P = v^{-1}(\lambda_0, \lambda_1, \ldots, \lambda_n)$.

(34) Voir l'exemple 2.

(35) Théorème noyau – image.

Expression de $P = v^{-1}(\lambda_0, \lambda_1, \ldots, \lambda_n)$

Soit $(e_0, e_1, \ldots, e_n)$ la base canonique de $\mathbb{K}^{n+1}$, et pour tout $k \in [\![0, n]\!]$:

$$L_k = v^{-1}(e_k).$$

Alors $(L_0, L_1, \ldots, L_n)$ est une base de $\mathbb{K}_n[X]$. (36)

Avec $(\lambda_0, \lambda_1, \ldots, \lambda_n) = \sum_{k=0}^{n} \lambda_k e_k$, il vient : $P = v^{-1}\left(\sum_{k=0}^{n} \lambda_k e_k\right) = \sum_{k=0}^{n} \lambda_k L_k$.

L_k est l'unique polynôme de $\mathbb{K}_n[X]$ tel que $u(L_k) = e_k$, c'est-à-dire :

$$L_k(a_i) = 0 \text{ si } i \neq k \quad \text{et} \quad L_k(a_k) = 1.$$

$L_k(a_i) = 0$ pour $i \neq k$, avec $\deg L_k \leqslant n$ donne qu'il existe un scalaire μ_k tel que :

$$L_k = \mu_k \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq k}} (X - a_i)$$

alors $L_k(a_k) = 1$ donne $\mu_k = \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq k}} \frac{1}{a_k - a_i}$, d'où $L_k = \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq k}} \left(\frac{X - a_i}{a_k - a_i}\right)$.

En conséquence, l'unique polynôme P de $\mathbb{K}_n[X]$ tel que $\forall k \in [\![0, n]\!]$, $P(a_k) = \lambda_k$ est :

$$P = \sum_{k=0}^{n} \lambda_k \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq k}} \left(\frac{X - a_i}{a_k - a_i}\right).$$

(36) v^{-1} est un isomorphisme de $\mathbb{K}^{n+1}$ sur $\mathbb{K}_n[X]$.

Définition 14

Les $L_k = \prod_{\substack{0 \leqslant i \leqslant n \\ i \neq k}} \left(\frac{X - a_i}{a_k - a_i}\right)$, $0 \leqslant k \leqslant n$, sont les **polynômes d'interpolation de Lagrange** associés à la famille de scalaires deux à deux distincts $(a_k)_{0 \leqslant k \leqslant n}$.

Exemple 5 Écrire l'unique polynôme P de degré inférieur ou égal à 3, tel que :

$$P(0) = -1 \ , \ P(2) = 1 \ , \ P(-2) = 1 \ , \ P(-1) = 2.$$

Écrivons les polynômes d'interpolation de Lagrange associés à $(0, 2, -2, -1)$:

$$L_0 = \frac{(X-2)(X+2)(X+1)}{(-2)\times 2 \times 1} = -\frac{1}{4}x^3 - \frac{1}{4}x^2 + x + 1$$

$$L_1 = \frac{X(X+2)(X+1)}{2 \times 4 \times 3} = \frac{1}{24}x^3 + \frac{1}{8}x^2 + \frac{1}{12}x$$

$$L_2 = \frac{X(X-2)(X+1)}{(-2)\times(-4)\times(-1)} = -\frac{1}{8}x^3 + \frac{1}{8}x^2 + \frac{1}{4}x$$

$$L_3 = \frac{X(X-2)(X+2)}{(-1)\times(-3)\times 1} = \frac{1}{3}x^3 - \frac{4}{3}x$$

On en déduit : $P = -L_0 + L_1 + L_2 + 2L_3$, c'est-à-dire $P = \frac{5}{6}x^3 + \frac{1}{2}x^2 - \frac{10}{3}x - 1$

Copyrighted material

D. Rang d'une application linéaire

1. Théorème du rang

Théorème 9

Théorème du rang

Soit E et F des $\mathbb{K}$-espaces vectoriels et $f \in \mathscr{L}(E, F)$.

Si E est de dimension finie, alors $\operatorname{Im} f$ est de dimension finie, et on a :

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

☞ E étant de dimension finie, $\operatorname{Ker} f$ admet au moins un supplémentaire H dans E.

H est de dimension finie et isomorphe à $\operatorname{Im} f$ (théorème noyau – image).

$\operatorname{Im} f$ est donc de dimension finie et $\dim(\operatorname{Im} f) = \dim H$.

Avec $\operatorname{Ker} f \oplus H = E$, il vient $\dim(\operatorname{Ker} f) + \dim H = \dim E$, d'où :

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

Définition 15

Soit E et F des $\mathbb{K}$-espaces vectoriels et $f \in \mathscr{L}(E, F)$.

Si $\operatorname{Im} f$ est de dimension finie, $\dim(\operatorname{Im} f)$ est appelée le **rang de** f. On note $\operatorname{rg} f$ ce rang.

Remarque

Si E est de dimension finie, alors $\operatorname{Im} f$ est de dimension finie et on a :

$$\operatorname{rg} f = \dim(\operatorname{Im} f) = \dim E - \dim(\operatorname{Ker} f).$$

Théorème 10

Soit E et F des $\mathbb{K}$-espaces vectoriels et $f \in \mathscr{L}(E, F)$, avec E de dimension finie.

Si $\mathscr{B} = (e_j)_{1 \leqslant j \leqslant n}$ est une base de E, alors $\operatorname{rg} f = \operatorname{rg}\left(f(e_j)\right)_{1 \leqslant j \leqslant n}$.

On a $\operatorname{Im} f = \operatorname{Vect}\left(f(e_j)\right)_{1 \leqslant j \leqslant n}$ et [37] : $\operatorname{rg}\left(f(e_j)\right)_{1 \leqslant j \leqslant n} = \dim \operatorname{Vect}\left(f(e_j)\right)_{1 \leqslant j \leqslant n}$.

[37] Voir Algèbre – Géométrie MPSI, chapitre 12.

Remarque

Si F est également de dimension finie, $\dim F = p$, et rapporté à une base $\mathscr{B}' = (e'_i)_{1 \leqslant i \leqslant p}$,

on pose pour tout $j \in [\![1, n]\!]$, $f(e_j) = \sum_{i=1}^{p} a_{ij} e'_i$.

Alors $A = [a_{ij}]$ est la matrice de f sur le couple de bases $(\mathscr{B}, \mathscr{B}')$, le rang de la famille $\left(f(e_j)\right)_{1 \leqslant j \leqslant n}$ est aussi le rang de la matrice A, le calcul pratique de ce rang peut se faire par la **méthode du pivot de Gauss**. Ces définitions et la technique du pivot ont été présentées en première année (Voir Algèbre – Géométrie MPSI, chapitre 12).

Théorème 11

Soit E et F des $\mathbb{K}$-espaces vectoriels de même dimension finie n, et $f \in \mathscr{L}(E, F)$. Les propriétés suivantes sont équivalentes :

(1) f est injective (2) f est surjective (3) f est bijective (4) $\operatorname{rg} f = n$

☞ Il suffit de prouver **(1)** $\Longleftrightarrow$ **(2)**.

- Si f est injective, on a $\operatorname{Ker} f = \{0_E\}$ et, d'après le théorème du rang :

$$\dim \operatorname{Im} f = \dim E \quad \text{donc} \quad \dim \operatorname{Im} f = \dim F \quad \text{et} \quad \operatorname{Im} f = F.$$

Ainsi f est surjective.

Copyrighted material

▪ Si f est surjective, $\dim \operatorname{Im} f = \dim F = \dim E$ et le théorème du rang donne $\dim \operatorname{Ker} f = 0$. Ainsi f est injective.

Théorème 12

Soit E, F et G des $\mathbb{K}$-espaces vectoriels, E et F étant de dimensions finies,

$$f \in \mathscr{L}(E,F) \text{ et } g \in \mathscr{L}(F,G).$$

a) Si f est bijective, alors $\operatorname{rg}(g \circ f) = \operatorname{rg} g$.

b) Si g est bijective, alors $\operatorname{rg}(g \circ f) = \operatorname{rg} f$.

☞ a) $f \in \operatorname{Isom}(E,F)$ donc $\dim E = \dim F$. On a alors $\operatorname{Ker}(g \circ f) = f^{-1}(\operatorname{Ker} g)$ donc $\dim \operatorname{Ker}(g \circ f) = \dim \operatorname{Ker} g$. On en déduit :

$$\begin{aligned} \operatorname{rg}(g \circ f) &= \dim E - \dim \operatorname{Ker}(g \circ f) \\ &= \dim F - \dim \operatorname{Ker} g \\ &= \operatorname{rg} g \end{aligned}$$

b) $g \in \operatorname{Isom}(F,G)$.

Alors $\operatorname{Im} g \circ f = g(\operatorname{Im} f)$ donne $\dim \operatorname{Im} g \circ f = \dim \operatorname{Im} f$ c'est-à-dire $\operatorname{rg}(g \circ f) = \operatorname{rg} g$.

Théorème 13

Matrice canonique d'une application linéaire

Soit E, F des $\mathbb{K}$-espaces vectoriels de dimensions finies non nulles, $\dim E = p$, $\dim F = n$, et $f \in \mathscr{L}(E)$ de rang $r \geqslant 1$.

Alors il existe $\mathscr{B}_E$ base de E et $\mathscr{B}_F$ base de F telles que la matrice de f sur le couple de bases $(\mathscr{B}_E, \mathscr{B}_F)$ soit, en l'écrivant par blocs :

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in \mathscr{M}_{n,p}(\mathbb{K})$$

☞ Rappelons que, avec $\mathscr{B}_E = (e_j)_{1 \leqslant j \leqslant p}$, $\mathscr{B}_F = (e'_i)_{1 \leqslant i \leqslant n}$, $f(e_j) = \sum_{i=1}^{n} a_{ij} e'_i$, la matrice de f sur le couple de bases $(\mathscr{B}_E, \mathscr{B}_F)$ est la matrice A de terme général a_{ij} :

$$\operatorname{mat}_{\mathscr{B}_E, \mathscr{B}_F} f = [a_{ij}] \in \mathscr{M}_{n,p}(\mathbb{K}).$$

Soit G un supplémentaire de $\operatorname{Ker} f$ dans E : $E = G \oplus \operatorname{Ker} f$, on a ici

$$\dim \operatorname{Ker} f = p - r \ , \ \dim G = r.$$

Construisons $\mathscr{B}_E = (e_j)_{1 \leqslant j \leqslant p}$ base de E adaptée à cette somme directe : $(e_j)_{1 \leqslant j \leqslant r}$ est une base de G et $(e_j)_{r+1 \leqslant j \leqslant p}$ est une base de $\operatorname{Ker} f$.

D'après le théorème noyau-image, $(f(e_j))_{1 \leqslant j \leqslant r}$ est une base de $\operatorname{Im} f$. On pose $e'_j = f(e_j)$ pour $1 \leqslant j \leqslant r$ et on complète par $e'_{j+1}, \ldots, e'_n$ pour obtenir une base $\mathscr{B}_F$ de F.

Par construction, on a : $\operatorname{mat}_{\mathscr{B}_E, \mathscr{B}_F} f = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

2. Endomorphismes nilpotents

Définition 16

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

$u \in \mathscr{L}(E)$ est **nilpotent** si il existe $p \in \mathbb{N}$ tel que $u^p = 0$. ✎(38)

On pose alors $i = \min\{p \in \mathbb{N} \,/\, u^p = 0\}$. Cet entier i est appelé **indice** de u.

Il est caractérisé par $u^{i-1} \neq 0$, $u^i = 0$. ✎(39)

✎(38) Par convention, $u^0 = \mathrm{Id}_E$ pour tout $u \in \mathscr{L}(E)$.

✎(39) Par exemple, l'endomorphisme nul est nilpotent d'indice 1.

Copyrighted material

Propriété 25

Si E de dimension finie $n \geqslant 1$ et $u \in \mathscr{L}(E)$ est nilpotent, alors $\operatorname{rg} u \leqslant n-1$.

☞ Si u, nilpotent d'indice i, était inversible, alors $u^i = 0$ donnerait $u^{i-1} = u^{-1} \circ u^i = 0$, contrairement à la définition de i.

Alors u non inversible donne $\operatorname{rg} u < n$ c'est-à-dire $\operatorname{rg} u \leqslant n-1$. ✎(40)

✎(40) Autre solution : $u^i = 0$ donne $(\det u)^i = 0$ donc $\det u = 0$ et u n'est pas de rang n.

Propriété 26

Si E est de dimension finie n, soit $u \in \mathscr{L}(E)$ nilpotent d'indice i.

Si $x \in E$ vérifie $u^{i-1}(x) \neq 0$, alors la famille $\left(x, u(x), \ldots, u^{i-1}(x)\right)$ est libre.

☞ Il existe $x \in E$ tel que $u^{i-1}(x) \neq 0$ car par hypothèse, on a $u^{i-1} \neq 0$.

Soit des scalaires $\lambda_0, \lambda_1, \ldots, \lambda_{i-1}$ tels que $\sum_{k=0}^{i-1} \lambda_k u^k(x) = 0$. **(1)**

On compose **(1)** par u^{i-1} : $\lambda_0 u^{i-1}(x) = 0$ donc $\lambda_0 = 0$ et $\sum_{k=1}^{i-1} \lambda_k u^k(x) = 0$. **(2)**

On compose **(2)** par u^{i-2} : $\lambda_1 u^{i-1}(x) = 0$ donc $\lambda_1 = 0$ et $\sum_{k=2}^{i-1} \lambda_k u^k(x) = 0$. **(3)**

Une récurrence immédiate donne ainsi $\lambda_0 = \lambda_1 = \lambda_2 = \cdots = \lambda_{i-1} = 0$ et on a montré que $\left(u^k(x)\right)_{0 \leqslant k \leqslant i-1}$ est libre.

Corollaire 1

Si $u \in \mathscr{L}(E)$ est nilpotent d'indice i, alors $i \leqslant n$. ✎(41)

✎(41) Tout système libre de E a au plus n éléments.

Corollaire 2

Si E est de dimension finie n, alors $u \in \mathscr{L}(E)$ est nilpotent si et seulement si $u^n = 0$.

Corollaire 3

Si u est nilpotent d'indice n, dans un espace de dimension n, il existe des bases $\mathscr{B}$ et $\mathscr{B}'$ de E telles que :

$$\operatorname{mat}_{\mathscr{B}} u = \begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \text{ et } \operatorname{mat}_{\mathscr{B}'} u = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}.$$

En effet, si u est nilpotent d'indice n, il existe e_1 tel que $u^{n-1}(e_1) \neq 0$.

Alors, d'après la propriété 26, avec $e_k = u^{k-1}(e_1)$, le système $(e_1, \ldots, e_n)$ est une base $\mathscr{B}$ de E telle que :

$$\forall k \in [\![1, n-1]\!],\ u(e_k) = e_{k+1} \text{ et } u(e_n) = 0$$

donc $\operatorname{mat}_{\mathscr{B}} u$ a la forme indiquée et la base $\mathscr{B}'$ s'obtient en inversant l'ordre des vecteurs de base : $e'_k = e_{n+1-k}$.

Copyrighted material

E. Dual d'un espace vectoriel Formes linéaires – Hyperplans

1. Formes linéaires – Hyperplans

Définition 17

On appelle **forme linéaire** sur E [42] toute application linéaire de E dans $\mathbb{K}$.
Le $\mathbb{K}$-espace vectoriel $\mathcal{L}(E, \mathbb{K})$ des formes linéaires sur E est appelé l'espace vectoriel **dual** de E. Il est usuellement noté E^*. [43]

[42] E est un $\mathbb{K}$-espace vectoriel.

[43] Il faut distinguer E^* de $E\setminus\{0_E\}$.

Définition 18

Un **hyperplan** d'un $\mathbb{K}$-espace vectoriel E est un sous-espace vectoriel qui admet une droite vectorielle pour supplémentaire.

Propriété 27

Toute forme linéaire non nulle est surjective.

☞ Soit $f \in E^*$, on a $\operatorname{Im} f = \{0_{\mathbb{K}}\}$ ou $\operatorname{Im} f = \mathbb{K}$, donc si $f \neq 0$, il reste $\operatorname{Im} f = \mathbb{K}$.

Propriété 28

Un sous-espace vectoriel H de E est un hyperplan si et seulement si, pour tout $a \in E \setminus H$, on a $E = H \oplus \mathbb{K}a$.

☞ Montrons que la condition est nécessaire. [44]
Soit H un hyperplan de E. Il existe $b \in E \setminus \{0_E\}$ tel que $E = H \oplus \mathbb{K}b$.
Étant donné $a \in E \setminus H$, il existe $\alpha \in \mathbb{K}$ et $c \in H$ tels que $a = c + \alpha b$.
α est non nul, sinon a serait dans H.
Pour tout $x \in E$, il existe $\lambda \in \mathbb{K}$ et $y \in H$ tels que $x = y + \lambda b$.
Avec $b = \dfrac{1}{\alpha}(a - c)$, on a $x = \left(y - \dfrac{\lambda}{\alpha}c\right) + \dfrac{\lambda}{\alpha}a$, ce qui montre que $E = H + \mathbb{K}a$.
Il reste à remarquer que $a \notin H$ donne $H \cap \mathbb{K}a = \{0_E\}$ [45] pour avoir $E = H \oplus \mathbb{K}a$.

[44] La condition est suffisante, par définition d'un hyperplan.

[45] De façon générale, si $\mathcal{D}$ est une droite vectorielle et F un sous-espace de E, les seules situations possibles sont $\mathcal{D} \cap F = \{0_E\}$ et $\mathcal{D} \cap F = \mathcal{D}$.

Propriété 29

Un sous-espace vectoriel H de E est un hyperplan si et seulement si il existe une forme linéaire non nulle u telle que $\operatorname{Ker} u = H$.

☞ a) Soit H un hyperplan de E. Étant donné $a \in E \setminus H$, on a $H \oplus \mathbb{K}a = E$.
Pour tout $x \in E$, il existe $\lambda_x \in \mathbb{K}$ et $h_x \in H$ uniques tels que $x = \lambda_x a + h_x$.
On vérifie aisément que l'application $u : E \to \mathbb{K}$, $x \mapsto \lambda_x$ est une forme linéaire non nulle telle que $H = \operatorname{Ker} u$.

b) Soit u une forme linéaire non nulle. Posons $H = \operatorname{Ker} u$.
u étant non nulle, il existe $a' \in E$ tel que $u(a') \neq 0$. Avec $a = \dfrac{1}{u(a')}a'$, on a $u(a) = 1$.
Pour tout $x \in E$, on obtient $u\left(x - u(x)a\right) = 0$ et donc $x - u(x)a \in H$.
De $x = \left(x - u(x)a\right) + u(x)a$, on déduit que $x \in H + \mathbb{K}a$. Donc $E = H + \mathbb{K}a$.
Comme a n'appartient pas à H, il vient $H \cap \mathbb{K}a = \{0_E\}$ et, finalement, $E = H \oplus \mathbb{K}a$, ce qui montre que H est un hyperplan.

Copyrighted material

Propriété 30

Deux formes linéaires sur E non nulles sont liées si et seulement si elles ont le même noyau.

☞ Soit u et v des formes linéaires non nulles sur E.

a) Si u et v sont liées, il existe $\lambda \in \mathbb{K}^*$ tel que $v = \lambda u$. Il s'ensuit $\operatorname{Ker} u = \operatorname{Ker} v$.

b) On suppose que u et v ont le même noyau H. Pour $a \in E \setminus H$, on a $E = H \oplus \mathbb{K}a$.
Pour tout $x \in E$, il existe $h_x \in H$ et $\lambda_x \in \mathbb{K}$ tels que $x = h_x + \lambda_x a$.

Avec $u(x) = \lambda_x u(a)$, $v(x) = \lambda_x v(a)$ et $u(a) \neq 0$, il vient $v(x) = \dfrac{v(a)}{u(a)} u(x)$.

Par suite, on a $v = \dfrac{v(a)}{u(a)} u$.

Corollaire

Si u est une forme linéaire non nulle sur E, pour toute forme linéaire v sur E, il existe $\lambda \in \mathbb{K}$ tel que $v = \lambda u$ si et seulement si $\operatorname{Ker} u \subset \operatorname{Ker} v$. ✎(46)

✎(46) Le cas où $v = 0$ correspond à $\lambda = 0$ et $\operatorname{Ker} v = E$.

2. Dimension finie

E est maintenant un $\mathbb{K}$-espace vectoriel de dimension finie, $n \geqslant 1$, de base $B = (e_i)_{i \in [\![1,n]\!]}$.

2.1 – Bases duales

Définition 19

Soit $B = (e_i)_{i \in [\![1,n]\!]}$ une base de E. Les **formes coordonnées** associées à B sont les n formes linéaires notées e_j^*, $j \in [\![1, n]\!]$ définies par :

$$\forall (i,j) \in [\![1,n]\!]^2,\ e_j^*(e_i) = \delta_{ij}.$$

Étant donné $x = \sum_{i=1}^{n} x_i e_i$, on a $e_j^*(x) = x_j$. ✎(47)

✎(47) e_j^* est donc l'application linéaire de E dans $\mathbb{K}$ qui, à tout x de E, associe sa $j^{\text{ème}}$ coordonnée sur la base $\mathcal{B}$, ce qui explique l'appellation de « formes coordonnées ».

Théorème 14

$$\dim E^* = \dim E.$$

On sait que $\dim \mathcal{L}(E, K) = \dim E \cdot \dim \mathbb{K}$.

Théorème 15

La famille $B^* = (e_j^*)_{j \in [\![1,n]\!]}$ des formes coordonnées associées à B est une base de E^*.
B^* est appelée **base duale** de la base B.

☞ Il suffit de montrer que la famille $(e_j^*)_{j \in [\![1,n]\!]}$ est libre. ✎(48) Soit $(\lambda_i)_{1 \leqslant i \leqslant n} \in \mathbb{K}^n$ tel que $\sum_{j=1}^{n} \lambda_j e_j^* = 0$. Alors, $\forall i \in [\![1,n]\!]$, $\sum_{j=1}^{n} \lambda_j e_j^*(e_i) = 0$, d'où $\lambda_i = 0$.

✎(48) $\dim E^* = n$.

Théorème 16

Soit $f \in E^*$. La famille de ses coordonnées dans B^* est $(f(e_i))_{i \in [\![1,n]\!]}$

$$f = \sum_{i=1}^{n} f(e_i) e_i^*.$$

☞ f s'écrit d'une manière unique sous la forme $f = \sum_{j=1}^{n} \lambda_j e_j^*$.

Pour tout $i \in [\![1,n]\!]$, $f(e_i) = \sum_{j=1}^{n} \lambda_j e_j^*(e_i)$ donne $\lambda_i = f(e_i)$.

Copyrighted material

Conséquence

Toute forme linéaire f sur E s'écrit de manière unique :

$$\forall x = \sum_{i=1}^{n} x_i e_i \ , \ f(x) = a_1 x_1 + \cdots + a_n x_n$$

où les scalaires a_i sont les coordonnées de f sur la base B^*.

Théorème 17

a) Pour tout vecteur x non nul de E, il existe φ forme linéaire sur E telle que $\varphi(x) = 1$.

b) Le vecteur nul est l'unique vecteur x de E tel que $\varphi(x) = 0$ pour toute forme linéaire φ.

☞ a) Posons $e_1 = x$, il existe $e_2, \ldots, e_n$ tels que $(e_i)_{1 \leqslant i \leqslant n}$ soit une base $\mathcal{B}$ de E.

La première forme coordonnée sur cette base est solution du problème. (49)

b) Si x est non nul, il existe $\varphi \in E^*$ tel que $\varphi(x) \neq 0$, donc en supposant $\forall\ \varphi \in E^*, \varphi(x) = 0$, on a nécessairement $x = 0_E$. (50)

On a donc : $\{0_E\} = \left\{ x \in E \ / \ \forall\ \varphi \in E^*, \ \varphi(x) = 0 \right\}$.

(49) On remarquera que, pour $n \geqslant 2$, il y a une infinité de formes linéaires φ sur E telles que $\varphi(x) = 1$.

(50) La réciproque est évidente.

Théorème 18

Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $T = (\theta_i)_{i \in [\![1,n]\!]}$ une base de E^*.

Alors il existe une unique base $U = (\varepsilon_i)_{i \in [\![1,n]\!]}$ de E telle que $T = U^*$.

On dit alors que U est la base E **anté-duale** de T, ou encore que T et U sont des **bases duales**.

☞ $\varphi : E \to \mathbb{K}^n, \varphi : x \mapsto (\theta_1(x), \ldots, \theta_n(x))$ est linéaire. (51)

On a $x \in \operatorname{Ker} \varphi$ si et seulement si $\theta_i(x) = 0$ pour tout $i \in [\![1, n]\!]$.

Soit $B = (e_i)$ une base de E et $B^* = (e_i^*)$ sa base duale.

Pour tout $i \in [\![1, n]\!]$, il existe une famille $(\lambda_j)_{j \in [\![1,n]\!]} \in \mathbb{K}^n$ telle que $e_i^* = \sum_{j=1}^{n} \lambda_j \theta_j$.

$x \in \operatorname{Ker} \varphi$ implique $e_i^*(x) = \sum_{j=1}^{n} \lambda_j \theta_j(x) = 0$. Avec $x = \sum_{i=1}^{n} e_i^*(x) e_i$, il vient $x = 0_E$, d'où $\operatorname{Ker} \varphi = \{0_E\}$ et ϕ est alors un isomorphisme. (52)

En conséquence, il existe une unique famille $U = (\varepsilon_1, \ldots, \varepsilon_2) \in E^n$ telle que :

$$\forall (i, j) \in [\![1, n]\!]^2, \ \theta_j(\varepsilon_i) = \delta_{ij}$$

U est une base de E car c'est l'image par l'isomorphisme φ^{-1} de la base canonique de $\mathbb{K}^n$.

(51) Par linéarité des θ_i.

(52) $\dim E = \dim \mathbb{K}^n$.

Exemple 6 Construction d'une base duale

On considère les formes linéaires f_1, f_2 et f_3 sur $\mathbb{R}^3$ définies par :

$f_1(x) = x_1 + x_2 + x_3$, $f_2(x) = x_2 - x_3$ et $f_3(x) = 2x_1 - x_2 + x_3$ avec $x = (x_1, x_2, x_3)$.

a) Montrons que $T = (f_1, f_2, f_3)$ est une base de $(\mathbb{R}^3)^*$.

Pour cela, soit $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{R}^3$ tel que : (53) $\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3 = 0$. Il vient (54)

$$\begin{cases} \lambda_1 + 2\lambda_3 = 0 & L_1 \\ \lambda_1 + \lambda_2 - \lambda_3 = 0 & L_2 \\ \lambda_1 - \lambda_2 + \lambda_3 = 0 & L_3 \end{cases} \quad \text{donc (55)} \quad \begin{cases} \lambda_1 + 2\lambda_3 = 0 \\ 2\lambda_1 = 0 \\ \lambda_1 - \lambda_2 + \lambda_3 = 0 \end{cases}$$

puis $\lambda_1 = \lambda_2 = \lambda_3 = 0$.

(53) Il suffit de montrer que cette famille de 3 vecteurs est libre.

(54) Avec les images par $\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$ des vecteurs de la base canonique de $\mathbb{R}^3$.

(55) $L_2 \leftarrow L_2 + L_3$

Copyrighted material

b) Trouver la base U de $\mathbb{R}^3$ dont T est la duale c'est trouver les vecteurs u_1, u_2 et u_3 tels que :

$$\forall (i,j) \in [\![1,3]\!]^2,\ f_j(u_i) = \delta_{ij}$$

Nous sommes conduits à la résolution des trois systèmes : (56)

$$\begin{cases} x_1 + x_2 + x_3 = a \\ x_2 - x_3 = b \\ 2x_1 - x_2 + x_3 = c \end{cases}$$

avec, successivement, $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$

On obtient : $u_1 = \left(0, \frac{1}{2}, \frac{1}{2}\right)$, $u_2 = \left(\frac{1}{2}, \frac{1}{4}, -\frac{3}{4}\right)$, $u_3 = \left(\frac{1}{2}, -\frac{1}{4}, -\frac{1}{4}\right)$

(56) Rappelons que l'existence et l'unicité d'un tel système sont assurées. Il reste à calculer les coordonnées dans la base canonique de $\mathbb{R}^3$ de ces vecteurs.

2.2 – Sous-espaces de E et E^*

Théorème 19

Étant donné F sous-espace de E, (57) notons F^o l'ensemble des formes linéaires sur E et s'annulant sur F : $F^o = \{f \in E^* \ / \ \forall x \in F, f(x) = 0\} = \{f \in E^* \ / \ F \subset \operatorname{Ker} f\}$.

a) F^o est un sous-espace vectoriel de E^*.

b) $\dim F^o = \dim E - \dim F$.

(57) E est un $\mathbb{K}$-espace vectoriel de dimension n.

☞ Si $F = \{0_E\}$, il est clair que $F^o = E^*$ et les propositions a) et b) sont vérifiées dans ce cas.

On suppose maintenant $F \neq \{0_E\}$ donc $\dim F = p \geqslant 1$ et soit $(\varepsilon_1, \ldots, \varepsilon_p)$ une base de F que l'on complète par $(\varepsilon_{p+1}, \ldots, \varepsilon_n)$ pour obtenir $(\varepsilon_i)_{1 \leqslant i \leqslant n}$ base de E.

Considérons l'application $u : E^* \to \mathbb{K}^p, f \mapsto (f(\varepsilon_1), \ldots, f(\varepsilon_p))$. Il est immédiat que u est linéaire : $u \in \mathcal{L}(E^*, \mathbb{K}^p)$ et que $F^o \subset \operatorname{Ker} u$ avec :

$$\operatorname{Ker} u = \{f \in E^* \ / \ \forall i \in [\![1,p]\!],\ f(\varepsilon_i) = 0\}.$$

Tout x de F s'écrivant $x = \sum_{i=1}^{p} x_i \varepsilon_i$ avec $(x_1, \ldots, x_p) \in \mathbb{K}^p$, si $f \in \operatorname{Ker} u$, on obtient :

$$f(x) = \sum_{i=1}^{p} x_i f(\varepsilon_i) = 0 \text{ donc } f \in F^o.$$

On a ainsi prouvé $\operatorname{Ker} u \subset F^o$ et finalement $F^o = \operatorname{Ker} u$.

En notant $(\varepsilon_i^*)_{1 \leqslant i \leqslant n}$ la base duale de $(\varepsilon_i)_{1 \leqslant i \leqslant n}$, on constate que :

$$(u(\varepsilon_1^*), u(\varepsilon_2^*), \ldots, u(\varepsilon_p^*))$$

est la base canonique de $\mathbb{K}^p$. Donc u est surjective, soit encore $\operatorname{rg} u = p = \dim F$.

Le théorème du rang s'écrit $\dim \operatorname{Ker} u = \dim E^* - \operatorname{rg} u$ et donne enfin :

$$\dim F^o = \dim E - \dim F.$$

Corollaire 1

Équations d'un sous-espace vectoriel F de E, $F \neq E$, $F \neq \{0_E\}$.

Pour tout sous-espace vectoriel F de E, de dimension p avec $1 \leqslant p \leqslant n-1$, il existe $n-p$ formes linéaires indépendantes $f_1, f_2, \ldots, f_{n-p}$ telles que :

$$F = \bigcap_{i=1}^{n-p} \operatorname{Ker} f_i$$

c'est-à-dire telles que pour tout x de E :

$$x \in F \iff f_1(x) = 0, f_2(x) = 0, \ldots, f_{n-p}(x) = 0 \quad (S).$$

On dit que (S) est un système d'équations de F. (58)

(58) Cette propriété reste valable dans le cas où $F = \{0_E\}$. Il suffit, dans ce cas, de prendre pour $(f_1, \ldots, f_n)$ toute base de E^*.

Copyrighted material

☞ Avec les notations de la démonstration précédente, il suffit de poser $f_i = \varepsilon^*_{p+i}$ pour tout $i \in [\![p+1, n]\!]$.

Corollaire 2

Équations d'un sous-espace affine $A = a + F$ **de** E avec F sous-espace vectoriel tel que $F \neq E$, $F \neq \{0_E\}$.

Avec les notations du corollaire 1, pour tout $a \in E$, on obtient pour tout x de E :

$$x \in a + F \iff \forall i \in [\![1, n-p]\!],\ f_i(x) = f_i(a) \quad (S').$$ (59)

(59) (S') est un système d'équations de A.

☞ Il suffit de noter que $x \in A \iff x - a \in F$ et que $f_i(x-a) = f_i(x) - f_i(a)$.

Exemple 7 $\mathbb{R}^4$ est rapporté à sa base canonique $(e_i)_{1 \leqslant i \leqslant 4}$.

a) Écrire un système d'équations du plan vectoriel $P = \mathrm{Vect}(a, b)$ avec : $a = (1, 0, 1, -1)$, $b = (-1, 2, 0, 1)$.

b) Écrire un système d'équations un plan affine $A = c + P$ avec $c = (1, 1, 0, 1)$.

a) Soit $u : E^* \to \mathbb{R}^2,\ \theta \mapsto \big(\theta(a), \theta(b)\big)$.

Une forme linéaire $\theta = \sum_{i=1}^{4} \alpha_i e_i^*$ appartient à $\mathrm{Ker}\, u$ si et seulement si : $\alpha_1 + \alpha_3 - \alpha_4 = 0$ et $-\alpha_1 + 2\alpha_2 + \alpha_4 = 0$ c'est-à-dire $\alpha_3 = -2\alpha_2$ et $\alpha_4 = \alpha_1 - 2\alpha_2$, soit encore :

$$\theta = \alpha_1 \left(e_1^* + e_4^*\right) + \alpha_2 \left(e_2^* - 2e_3^* - 2e_4^*\right).$$

Une base de $\mathrm{Ker}\, u$ est donc $\left(e_1^* + e_4^*, e_2^* - 2e_3^* - 2e_4^*\right)$. D'où un système d'équations de P :

$$x_1 + x_4 = 0 \ ,\ x_2 - 2x_3 - 2x_4 = 0.$$

b) On écrit que x appartient à A si et seulement si $x - c$ appartient à P :

$$x_1 + x_4 = 2 \ ,\ x_2 - 2x_3 - 2x_4 = -1.$$

Théorème 20

Étant donné F^* sous-espace de E^*, notons F^{*o} l'intersection des noyaux des éléments de F^* :

$$F^{*o} = \left\{ x \in E \,/\, \forall f \in F^*,\ f(x) = 0 \right\}.$$

a) F^{*o} est un sous-espace vectoriel de E.

b) $\dim F^{*o} = \dim E - \dim F^*$.

☞ a) F^{*o} est un sous-espace vectoriel de E en tant qu'intersection d'une famille de sous-espaces : $F^{*o} = \bigcap_{f \in G^*} \mathrm{Ker}\, f$.

b) Si $F^* = \left\{0_{E^*}\right\}$, il est clair que $F^{*o} = E$ et l'égalité annoncée est bien vérifiée dans ce cas.

On suppose maintenant $F^* \neq \left\{0_{E^*}\right\}$ donc $\dim F^* = p \geqslant 1$ et soit $(\theta_1, \ldots, \theta_p)$ une base de F^* que l'on complète par $(\theta_{p+1}, \ldots, \theta_n)$ pour obtenir $(\theta_i)_{1 \leqslant i \leqslant n}$ base de E^*.

Considérons l'application $v : E \to \mathbb{K}^p,\ x \mapsto \big(\theta_1(x), \theta_2(x), \ldots, \theta_p(x)\big)$. Il est immédiat que v est linéaire et que $F^{*o} \subset \mathrm{Ker}\, v$ avec $\mathrm{Ker}\, v = \bigcap_{i=1}^{p} \mathrm{Ker}\, \theta_i$.

Tout f de F^* s'écrivant $f = \sum_{i=1}^{p} \lambda_i \theta_i$ avec $(\lambda_1, \ldots, \lambda_p) \in \mathbb{K}^p$, si $x \in \mathrm{Ker}\, v$ on obtient :

$$f(x) = \sum_{i=1}^{p} \lambda_i \theta_i(x) = 0 \ \text{ donc } \ x \in F^{*o}.$$

En notant $(\varepsilon_i)_{1 \leqslant i \leqslant n}$ la base de E anté-duale de $(\theta_i)_{1 \leqslant i \leqslant n}$, on constate que :

$$\big(v(\varepsilon_1), v(\varepsilon_2), \ldots, v(\varepsilon_p)\big)$$

est la base canonique de $\mathbb{K}^p$.

Copyrighted material

Donc v est surjective, soit encore $\operatorname{rg} v = p = \dim F^*$.
Le théorème du rang s'écrit $\dim \operatorname{Ker} v = \dim E - \operatorname{rg} v$ et donne enfin :

$$\dim F^{*o} = \dim E - \dim F^*.$$

Corollaire 1

Équations d'un sous-espace vectoriel (resp. affine)

Tout système d'équations $\varphi_i(x) = 0$ (resp. $\varphi_i(x) = b_i$), $1 \leqslant i \leqslant q$, dans lequel $\left(\varphi_i\right)_{1\leqslant i\leqslant q}$ est un système de E^* et $\left(b_1, \ldots, b_q\right) \in \mathbb{R}^q$ représente un sous-espace vectoriel F (resp. affine A) de E de dimension $n - q$.

- Le cas du système homogène (H) : $\varphi_i(x) = 0$, $1 \leqslant i \leqslant q$, est une transcription du théorème 20. L'ensemble des solutions de (H) est donc un sous-espace vectoriel de E de dimension $n - q$.
- Cas du système affine (S) : $\varphi_i(x) = b_i$, $1 \leqslant i \leqslant p$.

L'application $v : E \to \mathbb{K}^q, x \mapsto \left(\varphi_1(x), \varphi_2(x), \ldots, \varphi_q(x)\right)$ étant surjective, il existe $a \in E$ tel que $v(a) = \left(b_1, \ldots, b_q\right)$ et alors chaque équation $\varphi_i(x) = b_i$ se lit $\varphi_i(x - a) = 0$.
L'ensemble des solutions de (S) est donc $A = a + F$, sous-espace affine de E, de direction F.

Corollaire 2

Critère d'indépendance d'une famille de formes linéaires

Soit $\phi = \left(\varphi_1, \varphi_2, \ldots, \varphi_q\right)$ une famille de formes linéaires sur E.

a) ϕ est libre si et seulement si $\bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i$ est de dimension $n - q$.

b) Si ϕ est libre, pour toute forme linéaire f sur E, on a :

$$f \in \operatorname{Vect}\left(\varphi_1, \ldots, \varphi_q\right) \iff \operatorname{Ker} f \supset \bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i.$$

☞ a) Posons $F^* = \operatorname{Vect}\left(\varphi_1, \ldots, \varphi_q\right)$, comme dans la démonstration précédente, on obtient $F^{*o} = \bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i$. On a donc $\dim \bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i = n - \dim F^* = n - \operatorname{rg} \Phi$ et il en résulte les équivalences : Φ est libre $\iff \operatorname{rg} \Phi = q \iff \dim \bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i = n - q$.

b) Supposons $f \in F^*$, on a alors $F^* = \operatorname{Vect}\left(\varphi_1, \ldots, \varphi_q, f\right)$ donc :

$$F^{*o} = \bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i \cap \operatorname{Ker} f = F^{*o} \cap \operatorname{Ker} f$$

ce qui donne $F^{*o} \subset \operatorname{Ker} f$ c'est-à-dire $\bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i \subset \operatorname{Ker} f$.

Supposons $\bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i \subset \operatorname{Ker} f$, on a de même $F^{*o} \cap \operatorname{Ker} f = F^{*o}$.

En posant $G^* = \operatorname{Vect}\left(\varphi_1, \ldots, \varphi_q, f\right)$, on obtient $F^* \subset G^*$ et :

$$G^{*o} = \bigcap_{i=1}^{q} \operatorname{Ker} \varphi_i \cap \operatorname{Ker} f = F^{*o} \cap \operatorname{Ker} f = F^{*o}$$

puis, le théorème 20 donne $\dim G^* = \dim F^* = q$, donc $G^* = F^*$ soit aussi $\varphi \in F^*$.

Exemple 8 Soit $E = \mathbb{K}_n[X]$, $a_0, a_1, \ldots, a_n$ des scalaires distincts et $\theta_i : E \to \mathbb{K}, P \mapsto P(a_i), 0 \leqslant i \leqslant n$.

Un polynôme $P \in \bigcap_{0\leqslant i\leqslant n} \operatorname{Ker} \theta_i$ a $n + 1$ racines distinctes. Avec $\deg P \leqslant n$, il vient $P = 0$.

On en déduit[60] que le système $(\theta_i)_{0\leqslant i\leqslant n}$ est libre et donc[61] une base de E^*.

[60] D'après le corollaire 2 précédent.

[61] Car $\dim E^* = n+1$.

Copyrighted material

L'essentiel

I. Somme de sous-espaces vectoriels

✔ Les sommes directes de deux sous-espaces, vues en première année, sont étendues à plusieurs sous-espaces.

✔ **Si l'on veut** montrer qu'une somme $\sum F_i$ de sous-espaces de E est directe,

- **on peut** se servir de la principale caractérisation en montrant que,
$$\text{pour } x_i \in F_i,\ \sum x_i = 0 \ \Rightarrow\ \forall i,\ x_i = 0,$$
en procédant éventuellement par récurrence ;
→ Voir *Mise en œuvre*, exercice 1
- **on peut** montrer que tout $x \in E$ s'écrit de manière unique sous la forme : $x_i \in F_i$, $x = \sum x_i$;
→ Voir *Mise en œuvre*, exercice 2
- **on peut** pour une somme de deux sous-espaces, utiliser des informations sur les dimensions.
→ Voir *Mise en œuvre*, exercice 3

II. Endomorphismes nilpotents

✔ Les endomorphismes nilpotents sont d'usage particulièrement simples en privilégiant des bases adaptées.

✔ Le théorème du rang est fondamental en dimension finie.

✔ **Si l'on veut** étudier un endomorphisme nilpotent u,

- **on peut** observer que l'endomorphisme induit par u sur un sous-espace stable est encore nilpotent.
→ Voir *Mise en œuvre*, exercice 4

✔ **Si l'on veut** calculer une puissance d'une matrice A,

- **on peut** chercher à déceler le cas particulier où A se décompose en $A = D+N$, avec D diagonale, N nilpotente, D et N permutables.
→ Voir *Mise en œuvre*, exercice 5

III. Calcul du rang

✔ **Si l'on veut** calculer le rang d'un système de vecteurs,

- **on peut** utiliser la méthode du pivot de Gauss. C'est une méthode de base.
→ Voir *Mise en œuvre*, exercice 6

✔ **Si l'on veut** calculer le rang d'un système de formes linéaires,

- **on peut** penser à évaluer la dimension de l'intersection de leurs noyaux.
→ Voir *Mise en œuvre*, exercice 7

Mise en œuvre

I. Somme de sous-espaces vectoriels

Ex. 1

Soit $f \in \mathcal{L}(E)$, $\lambda_1, \lambda_2, \ldots, \lambda_n$, n scalaires deux à deux distincts ($n \geqslant 2$).
Montrer que, si $\forall i \in [\![1, n]\!], F_i = \operatorname{Ker}(f - \lambda_i \operatorname{Id}_E)$, alors la somme $F_1 + F_2 + \ldots + F_n$ est directe.

Indications

C'est un cas particulier important de la réduction des endomorphismes qui sera vue au chapitre 5.
On procède par récurrence sur n.

Solution

Montrons d'abord que la propriété est vraie pour $n = 2$.
Soit $x_1 \in F_1$, $x_2 \in F_2$ tels que $x_1 + x_2 = 0_E$ **(1)**.
$x_i \in F_i$ se lit $f(x_i) = \lambda_i x_i$; il vient alors : $\lambda_1 x_1 + \lambda_2 x_2 = 0_E$ **(2)**.
On multiplie **(1)** par λ_2 et on retranche membre à membre avec **(2)**, il vient $(\lambda_1 - \lambda_2)x_1 = 0_E$ donc $x_1 = 0_E$. Alors **(1)** donne $x_2 = 0_E$.
Ainsi $\forall (x_1, x_2) \in F_1 \times F_2$, $x_1 + x_2 = 0_E \Rightarrow x_1 = x_2 = 0_E$.
Supposons que la propriété soit vraie pour $n - 1$ scalaires.
Soit $\lambda_1, \ldots, \lambda_n$ des scalaires deux à deux distincts et $x_1, \ldots, x_n$ des vecteurs tels que :

$$\forall i \in [\![1, n]\!], \quad x_i \in F_i \text{ et } x_1 + x_2 + \ldots + x_n = 0_E \quad \textbf{(3)}.$$

La relation **(3)** donne : $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0_E$ **(4)**.

Il s'ensuit $\displaystyle\sum_{i=1}^{n-1} (\lambda_i - \lambda_n) x_i = 0_E$.

On en déduit $\forall i \in [\![1, n-1]\!]$, $(\lambda_i - \lambda_n) x_i = 0_E$, donc

$$\forall i \in [\![1, n-1]\!], \quad x_i = 0_E \text{ car } \lambda_i - \lambda_n \neq 0.$$

Alors **(3)** donne enfin $x_n = 0_E$. La somme $\displaystyle\sum_{i=1}^{n} F_i$ est donc directe. Ce qui achève la récurrence.

Commentaires

Début de la récurrence sur n.

On applique f aux deux membres de (1).

car $\lambda_1 - \lambda_2 \neq 0$.

La somme $F_1 + F_2$ est donc directe.

Pour montrer qu'elle est récurrente.

En appliquant f.

Par combinaison linéaire de (3) et (4).

D'après l'hypothèse de récurrence.

Ex. 2

Soit E un $\mathbb{C}$-espace vectoriel et $f \in \mathcal{L}(E)$ vérifiant $f^3 = \operatorname{Id}_E$.
Montrer que $E = \operatorname{Ker}(f - \operatorname{Id}_E) \oplus \operatorname{Ker}(f - j \operatorname{Id}_E) \oplus \operatorname{Ker}(f - j^2 \operatorname{Id}_E)$.

Indications

On montre que tout x de E peut s'écrire $x = x_1 + x_2 + x_3$ d'une manière unique avec :

$$x_1 \in \operatorname{Ker}(f - \operatorname{Id}_E) \quad , \quad x_2 \in \operatorname{Ker}(f - j \operatorname{Id}_E) \quad , \quad x_3 \in \operatorname{Ker}(f - j^2 \operatorname{Id}_E).$$

Copyrighted material

Solution

- Analyse

Supposons que (x_1, x_2, x_3) soit solution de ce problème, on obtient alors :

$$\begin{aligned} x_1 + x_2 + x_3 &= x && (1)\\ x_1 + jx_2 + j^2x_3 &= f(x) && (2)\\ x_1 + j^2x_2 + jx_3 &= f^2(x) && (3) \end{aligned}$$

Par combinaison linéaire de **(1)**, **(2)** et **(3)**, on déduit :

$$x_1 = \frac{1}{3}\left[x + f(x) + f^2(x)\right] \ , \ x_2 = \frac{1}{3}\left[x + j^2 f(x) + j f^2(x)\right] \ ,$$

$$\text{et } x_3 = \frac{1}{3}\left[x + j f(x) + j^2 f^2(x)\right].$$

- Synthèse

Le triplet (x_1, x_2, x_3) ci-dessus vérifie $x_1 + x_2 + x_3 = x$. De plus :

$$f(x_1) = \frac{1}{3}\left(f(x) + f^2(x) + f^3(x)\right) = \frac{1}{3}\left(x + f(x) + f^2(x)\right) = x_1 ,$$

$$f(x_2) = \frac{1}{3}\left(f(x) + j^2 f^2(x) + j f^3(x)\right) = \frac{1}{3}\left(jx + j^3 f(x) + j^2 f^2(x)\right) = jx_2 ,$$

$$f(x_3) = \frac{1}{3}\left(f(x) + j f^2(x) + j^2 f^3(x)\right) = \frac{1}{3}\left(j^2 x + j^3 f(x) + j^4 f^2(x)\right) = j^2 x_3 .$$

Donc (x_1, x_2, x_3) est bien solution du problème et on a :

$$E = \operatorname{Ker}\left(f - \mathrm{Id}_E\right) \oplus \operatorname{Ker}\left(f - j\,\mathrm{Id}_E\right) \oplus \left(f - j^2\,\mathrm{Id}_E\right).$$

Commentaires

Condition nécessaire.

en appliquant f à (1)
en appliquant f à (2).

Sachant que $1+j+j^2=0$.

Ce triplet (x_1, x_2, x_3) est ainsi la seule solution possible.

Condition suffisante.

puisque $f^3 = \mathrm{Id}_E$.

Remarque : après l'étude du chapitre 5, cette question sera résolue par l'application du théorème de décomposition des noyaux.

Ex. 3

Soit f et g des endomorphismes d'un K-espace vectoriel E.
On suppose que $E = \operatorname{Im} f + \operatorname{Im} g$ et $E = \operatorname{Ker} f + \operatorname{Ker} g$. Montrer que ces deux sommes sont directes.

Indications

Cet exercice est un grand classique. Il met à la fois en œuvre le théorème du rang et une caractérisation de deux sous-espaces supplémentaires qui utilise leurs dimensions.

Solution

$\operatorname{Im} f + \operatorname{Im} g = E$ donne $\operatorname{rg} f + \operatorname{rg} g \geqslant n$, et

$\operatorname{Ker} f + \operatorname{Ker} g = E$ donne $(n - \operatorname{rg} f) + (n - \operatorname{rg} g) \geqslant n$, donc $\operatorname{rg} f + \operatorname{rg} g \leqslant n$.

Il en résulte $\operatorname{rg} f + \operatorname{rg} g = n$. Avec $\operatorname{Im} f + \operatorname{Im} g = E$, on a :

$$\operatorname{Im} f \oplus \operatorname{Im} g = E.$$

On a aussi :

$$\dim(\operatorname{Ker} f) + \dim(\operatorname{Ker} g) = \dim E ;$$

avec $\operatorname{Ker} f + \operatorname{Ker} g = E$, il vient $\operatorname{Ker} f \oplus \operatorname{Ker} g = E$.

Commentaires

$\dim U + \dim V \geqslant \dim(U+V)$.

Théorème du rang.

Deux sous-espaces U et V sont supplémentaires si et seulement si $E = U + V$ et $\dim U + \dim V = \dim E$.

II. Endomorphismes nilpotents

Ex. 4

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$ et $u \in \mathcal{L}(E)$.

On suppose que u est nilpotent et que $\dim(\operatorname{Ker} u) = 1$.

1) Étant donné un sous-espace vectoriel F non nul et stable par u, montrer que $\dim u(F) = \dim F - 1$.

2) Montrer que $\forall k \in [\![0, n]\!]$, $\dim\left(\operatorname{Ker} u^k\right) = k$ et $\operatorname{rg} u^k = n - k$.

3) Déterminer tous les sous-espaces de E stables par u.

Indications

1) Théorème du rang pour l'endomorphisme de F induit par u.

2) Il suffit de montrer que $\operatorname{rg} u^k = n - k$ pour $k \in [\![1, n]\!]$. C'est d'ailleurs vrai pour $k = 0$ avec $u^0 = \mathrm{Id}$.

3) Les sous-espaces $\operatorname{Ker} u^k$ sont stables par u.

Solution

1) Soit $\overline{u}$ l'endomorphisme de F induit par u.

Rappelons que $\operatorname{Ker} \overline{u} = F \cap \operatorname{Ker} u$ et $\operatorname{Im} \overline{u} = u(F)$.

Comme u est nilpotent, il en est de même pour $\overline{u}$.

Alors $\dim \operatorname{Ker} \overline{u} \geqslant 1$, donc $\operatorname{Ker} \overline{u} = \operatorname{Ker} u$.

Il s'ensuit $\dim F - 1 = \operatorname{rg} \overline{u} = \dim u(F)$.

2) Supposons que $\operatorname{rg} u^k = n - k$ pour $k \in [\![1, n-1]\!]$.

Cette propriété est vraie pour $k = 1$: $\operatorname{rg} u = \dim u(E) = \dim E - 1$.

Avec $u\left(\operatorname{Im} u^k\right) = \operatorname{Im} u^{k+1} \subset \operatorname{Im} u^k$, on applique le résultat de la première question à $F = \operatorname{Im} u^k$.

Il vient alors $\operatorname{rg}(u^{k+1}) = \operatorname{rg}(u^k) - 1 = n - k - 1$.

Remarque : l'indice de nilpotence de u est égal à n.

Il s'ensuit alors $\dim(\operatorname{Ker} u^k) = k$.

3) Les sous-espaces $\operatorname{Ker} u^k$ sont stables par u.

Soit F un sous-espace stable par u ; posons $p = \dim F$.

Pour $p \geqslant 1$, l'endomorphisme $\overline{u}$ de F induit par u est nilpotent, donc $\overline{u}^p = 0$.

Cela nous donne $F \subset \operatorname{Ker} u^p$.

Avec l'égalité des dimensions, il vient $F = \operatorname{Ker} u^p$.

Remarque : $u^n = 0$ se lit $u^k u^{n-k} = 0$, c'est-à-dire $\operatorname{Im} u^{n-k} \subset \operatorname{Ker} u^k$.

Avec l'égalité des dimensions, il vient $\operatorname{Im} u^{n-k} = \operatorname{Ker} u^k$.

Commentaires

F est stable par u.

$\operatorname{Ker} \overline{u} \subset \operatorname{Ker} u$ et $\dim(\operatorname{Ker} u) = 1$.

Théorème du rang pour $\overline{u}$.

Pour une preuve par récurrence.

Question précédente.

$\dim u(\operatorname{Im} u^k) = \dim \operatorname{Im}(u^k) - 1$.

$\operatorname{Im} u^n = \{0\}$ et $\operatorname{rg}(u^{n-1}) = 1$.

Théorème du rang pour u^k.

Une piste : ce sont peut-être les seuls !

Pour $p = 0$, $F = \{0\} = \operatorname{Ker} u^0$.

L'indice de nilpotence est au plus égal à $\dim F$.

$\dim(\operatorname{Ker} u^k) = k$.

Copyrighted material

Ex. 5

1) Soit $A \in \mathcal{M}_n(\mathbb{R})$ nilpotente d'indice i. Montrer que $i \leqslant n$.

Montrer que $A \in \mathcal{M}_n(\mathbb{R})$ est nilpotente si et seulement si $A^n = 0$.

2) Soit $A \in \mathcal{M}_n(\mathbb{R})$, triangulaire supérieure stricte, c'est-à-dire : $A = [a_{ij}]$ avec $(i \geqslant j \Rightarrow a_{ij} = 0)$.

Montrer que A est nilpotente.

3) Calculer A^n pour $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$.

Indications

L'indice de nilpotence d'une matrice carrée se définit comme celui d'un endomorphisme.

Soit f l'endomorphisme de $\mathbb{K}^n$ canoniquement associé à A. L'indice de nilpotence de A est celui de f.

Solution

1) L'étude des endomorphismes nilpotents donne les résultats annoncés.

2) Soit $f \in \mathcal{L}(\mathbb{K}^n)$ tel que $A = \mathrm{mat}_{\mathcal{B}} f$. Avec $\mathcal{B} = (e_1, \ldots, e_n)$:

$$\forall j \in [\![2, n]\!],\ f(e_j) \in \mathrm{Vect}(e_1, \ldots, e_{j-1}),\ f(e_1) = 0.$$

On en déduit, pour $3 \leqslant j \leqslant n$:

$$f^2(e_j) \in \mathrm{Vect}(f(e_1), \ldots, f(e_{j-1})) \subset \mathrm{Vect}(e_1, \ldots, e_{j-2}).$$

$$\forall j \in [\![3, n]\!], f^2(e_j) \in \mathrm{Vect}(e_1, \ldots, e_{j-2}), \text{ et } f^2(e_1) = f^2(e_2) = 0.$$

$$\forall j \in [\![k+1, n]\!],\ f^k(e_j) \in \mathrm{Vect}(e_1, \ldots, e_{j-k}),$$

$$f^k(e_1) = f^k(e_2) = \cdots = f^k(e_k) = 0.$$

D'où pour $k = n$, $f^n(e_1) = f^n(e_2) = \cdots = f^n(e_n) = 0$, c'est-à-dire $f^n = 0$ et donc $A^n = 0$.

3) On a $A = I_3 + B$ où $B = \begin{pmatrix} 0 & 2 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$.

Avec $B^3 = 0$, la formule du binôme donne :

$$A^n = \sum_{k=0}^{n} \mathrm{C}_n^k B^k = I_3 + nB + \frac{n(n-1)}{2} B^2.$$

Avec $B^2 = \begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, il vient $A^n = \begin{pmatrix} 1 & 2n & 2n^2 + n \\ 0 & 1 & 2n \\ 0 & 0 & 1 \end{pmatrix}$.

Commentaires

Corollaire 2 de la propriété 26.

$\mathcal{B}$ base canonique de $\mathbb{K}^n$.

A est triangulaire supérieure stricte.

Par récurrence.

B nilpotente d'après le 2).

I_3 et B sont permutables.

III. Calcul du rang

Ex. 6

$E = \mathbb{R}^5$ et $F = \mathbb{R}^4$ sont rapportés à leurs bases canoniques $\mathcal{B} = (e_j)_{1 \leqslant j \leqslant 5}$ et $\mathcal{B}' = (e'_i)_{1 \leqslant i \leqslant 4}$.

Soit $f \in \mathcal{L}(E, F)$ définie par $\mathrm{mat}_{\mathcal{B},\mathcal{B}'} f = A = \begin{pmatrix} 2 & 0 & 2 & 4 & 10 \\ 0 & 1 & -3 & -5 & -6 \\ 3 & 4 & -3 & -4 & 1 \\ 3 & -10 & 9 & 16 & 35 \end{pmatrix}$.

Calculer le rang de f, former une base de $\mathrm{Im}\, f$ et une base de $\mathrm{Ker}\, f$.

Indications

L'outil de travail principal est la méthode du pivot de Gauss. Parfois, des remarques judicieuses allègent la démarche. La recherche d'une base de l'image de f est intimement liée à la détermination du rang.

Solution

1) Les colonnes de la matrice A représentent les vecteurs $f(e_j)$, $1 \leqslant j \leqslant 5$.

Notons pour simplifier $f(e_j) = u_j$ et appliquons la méthode du pivot :

$$\operatorname{rg}(u_1, u_2, u_3, u_4, u_5) = \operatorname{rg}(u_1, u_2, u_3 - u_1, u_4 - 2u_1, u_5 - 5u_1),$$

d'où $\operatorname{rg} f = \operatorname{rg} A_1$ avec $A_1 = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & -5 & -6 \\ 3 & 4 & -6 & -10 & -14 \\ 3 & -10 & 6 & 10 & 20 \end{pmatrix}$.

Remarquons que : $u_3 - u_1 = 3(-e'_2 - 2e'_3 + 2e'_4)$ **(1)**

et $u_4 - 2u_1 = 5(-e'_2 - 2e'_3 + 2e'_4)$ **(2)**.

Ces vecteurs étant proportionnels, il vient $\operatorname{rg} f = \operatorname{rg} A_2$, avec :

$$A_2 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & -3 \\ 3 & 4 & -2 & -7 \\ 3 & -10 & 2 & 10 \end{pmatrix}.$$

$\operatorname{rg} f = \operatorname{rg}(u_1, u_2, u'_3, u'_4)$ avec :

$$u'_3 = \frac{1}{3}(u_3 - u_1),\ u'_4 = \frac{1}{2}(u_5 - 5u_1).$$

Ensuite, $\operatorname{rg}(u_1, u_2, u'_3, u'_4) = \operatorname{rg}(u_1, u_2, u'_3 + u_2, u'_4 + 3u_2)$, d'où :

$$\operatorname{rg} f = \operatorname{rg} A_3 \quad \text{avec} \quad A_3 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3 & 4 & 2 & 5 \\ 3 & -10 & -8 & -20 \end{pmatrix}.$$

Avec $u'_3 + u_2 = 2(e'_3 - 4e'_4)$ **(3)** et $u'_4 + 3u_2 = 5(e'_3 - 4e'_4)$ **(4)**, il vient :

$$\operatorname{rg} f = \operatorname{rg}(u_1, u_2, u'_3 + u_2) = \operatorname{rg} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 4 & 2 \\ 3 & -10 & 8 \end{pmatrix}$$

c'est-à-dire $\operatorname{rg} f = 3$. Il en résulte $\dim \operatorname{Im} f = 3$ et $\dim \operatorname{Ker} f = 2$.

2) Avec la même méthode et les mêmes calculs,

$$\operatorname{rg}(u_1, u_2, u_3) = \operatorname{rg}(u_1, u_2, u'_3) = \operatorname{rg}(u_1, u_2, u'_3 + u_2) = 3$$

donc (u_1, u_2, u_3) est une base de $\operatorname{Im} f$.

$$u_1 = f(e_1) = 2e'_1 + 3e'_3 + 3e'_4$$
$$u_2 = f(e_2) = e'_2 + 4e'_3 - 10e'_4$$
$$u_3 = f(e_3) = 2e'_1 - 3e'_2 - 3e'_3 + 9e'_4.$$

3) Les égalités **(1)** et **(2)** donnent : $5(u_3 - u_1) - 3(u_4 - 2u_1) = 0$, c'est-à-dire $f(e_1 + 5e_3 - 3e_4) = 0$ donc $\varepsilon_1 = e_1 + 5e_3 - 3e_4 \in \operatorname{Ker} f$.

Commentaires

Par exemple, $f(e_1) = 2e'_1 + 3e'_3 + 3e'_4$.

$u'_3 = -e'_2 - 2e'_3 + 2e'_4$
$u'_4 = -3e'_2 - 7e'_3 + 10e'_4$.

De nouveau, la méthode du pivot.

On se ramène à une forme triangulaire.

$u_1 + 5u_3 - 3u_4 = 0$.

Copyrighted material

Remarquons aussi que dans la matrice A_1, on a :

$$\text{col}\,(2) - \text{col}\,(4) + \text{col}\,(5) = 0$$

donc $f(-3e_1 + e_2 - e_4 + e_5) = 0$ d'où $\varepsilon_2 = -3e_1 + e_2 - e_4 + e_5 \in \text{Ker}\, f$.

Le système $(\varepsilon_1\,,\varepsilon_2)$ est libre et constitue donc une base de $\text{Ker}\, f$.

On pourrait trouver un second vecteur du noyau en utilisant (3) et (4).

$u_2 - u_4 + 2u_1 + u_5 - 5u_1 = 0$.

Vérification immédiate.

Ex. 7

Étant donné a, b, c réels distincts, on considère les formes linéaires φ_i, $1 \leqslant i \leqslant 4$, définies sur $E = \mathbb{R}_3[X]$ par :

$$\forall P \in \mathbb{R}_3[X],\ \varphi_1(P) = P(a)\ ,\ \varphi_2(P) = P(b)\ ,\ \varphi_3(P) = P(c)\ ,\ \varphi_4(P) = \int_a^b P(t)\mathrm{d}t.$$

1) Trouver une condition nécessaire et suffisante portant sur (a, b, c) pour que le système $(\varphi_i)_{1 \leqslant i \leqslant 4}$ soit lié.

2) Cette condition étant réalisée, exprimer φ_4 comme combinaison linéaire de $(\varphi_1\,,\varphi_2\,,\varphi_3)$.

Indications

1) Si $(\varphi_1\,,\varphi_2\,,\cdots,\varphi_q)$ est une famille de formes linéaires sur E, $\mathbb{K}$ espace vectoriel de dimension n, on a :

$$\text{rg}\,(\varphi_1\,,\varphi_2\,,\cdots,\varphi_q) = n - \dim\left(\bigcap_{i=1}^{q} \text{Ker}\,\varphi_i\right).$$

$(\varphi_1\,,\varphi_2\,,\varphi_3)$ est libre donc $(\varphi_1\,,\varphi_2\,,\varphi_3\,,\varphi_4)$ est liée si et seulement si $\text{rg}\,(\varphi_1\,,\varphi_2\,,\varphi_3\,,\varphi_4) = 3$.

Solution

1) Notons $F = \bigcap_{i=1}^{3} \text{Ker}\,\varphi_i$. Un polynôme $P \in \mathbb{R}_3[X]$ est élément de F si et seulement si il admet a, b et c pour racines, donc si et seulement si il est divisible par $(X-a)(X-b)(X-c)$. S'agissant de polynômes de degré $\leqslant 3$, on en déduit que $F = \{\lambda(X-a)(X-b)(X-c) \,/\, \lambda \in \mathbb{R}\}$, puis on obtient $\text{rg}\,(\varphi_1\,,\varphi_2\,,\varphi_3) = 4 - \dim F = 3$.

Alors le système $(\varphi_1\,,\varphi_2\,,\varphi_3\,,\varphi_4)$ est lié si et seulement si $F \subset \text{Ker}\,\varphi_4$ c'est-à-dire si et seulement si $\varphi_4\big((X-a)(X-b)(X-c)\big) = 0$.

Cette condition s'écrit : $\displaystyle\int_a^b (x-a)(x-b)(x-c)\mathrm{d}x = 0.$

Avec le changement de variable défini par $x = \dfrac{a+b}{2} + \dfrac{b-a}{2}u$, il vient :

$$I = \int_a^b (x-a)(x-b)(x-c)\mathrm{d}x$$

$$= \left(\frac{b-a}{2}\right)^3 \int_{-1}^{1} (u^2-1)\left(\frac{a+b}{2} - c + \frac{b-a}{2}u\right)\mathrm{d}u = 0.$$

Sachant que $\displaystyle\int_{-1}^{1} u\mathrm{d}u = \int_{-1}^{1} u^3\mathrm{d}u = 0$ on obtient alors :

$$I = \left(\frac{b-a}{2}\right)^3 \left(\frac{a+b}{2} - c\right) \int_{-1}^{1} (u^2-1)\mathrm{d}u$$

$$= -\frac{1}{6}(b-a)^3\left(\frac{a+b}{2} - c\right).$$

En conséquence, $(\varphi_i)_{1 \leqslant i \leqslant 4}$ est lié si et seulement si $c = \dfrac{a+b}{2}$.

Commentaires

car a, b, c sont deux à deux distincts.

Soit aussi $F = \text{Vect}\,\big((X-a)(X-b)(X-c)\big)$

$\dim \mathbb{R}_3[X] = 4$.

Voir le corollaire 2 du théorème 19.

Pour ramener l'intervalle d'intégration à $[-1,1]$.

$b - a \neq 0$.

2) On suppose maintenant $c = \dfrac{a+b}{2}$ donc, d'après le 1), il existe α, β, γ réels tels que $\varphi_4 = \alpha\,\varphi_1 + \beta\,\varphi_2 + \gamma\varphi_3$ c'est-à-dire tels que :

$$\forall P \in \mathbb{R}_3[X],\ \int_a^b P(t)\mathrm{d}t = \alpha P(a) + \beta P(b) + \gamma P(c).$$

Avec les polynômes de Lagrange L_a, L_b, L_c associés au triplet (a, b, c), on obtient :

$$\alpha = \int_a^b L_a(t)\mathrm{d}t\ ,\ \beta = \int_a^b L_b(t)\mathrm{d}t\ ,\ \gamma = \int_a^b L_c(t)\mathrm{d}t$$

soit :

$$\alpha = \frac{2}{(a-b)^2}\int_a^b (x-b)\left(x - \frac{a+b}{2}\right)\mathrm{d}x$$
$$= \frac{b-a}{4}\int_{-1}^1 (u-1)u\mathrm{d}u = \frac{b-a}{6},$$
$$\beta = \frac{2}{(a-b)^2}\int_a^b (x-a)\left(x - \frac{a+b}{2}\right)\mathrm{d}x$$
$$= \frac{b-a}{4}\int_{-1}^1 (u+1)u\mathrm{d}u = \frac{b-a}{6},$$
$$\gamma = -\frac{4}{(a-b)^2}\int_a^b (x-a)(x-b)\mathrm{d}x$$
$$= -\frac{b-a}{2}\int_{-1}^1 \left(u^2-1\right)\mathrm{d}u = \frac{2}{3}(b-a).$$

En conclusion, pour tout polynôme P de degré $\leqslant 3$, on a :

$$\int_a^b P(t)\mathrm{d}t = \frac{b-a}{6}\left(P(a) + 4P\left(\frac{a+b}{2}\right) + P(b)\right).$$

$$L_a = \frac{(X-b)(X-c)}{(a-b)(a-c)} = \frac{2(X-b)\left(X-\frac{a+b}{2}\right)}{(a-b)^2}.$$

$$L_b = \frac{(X-a)(X-c)}{(b-a)(b-c)} = \frac{2(X-a)\left(X-\frac{a+b}{2}\right)}{(a-b)^2}.$$

$$L_c = \frac{(X-a)(X-b)}{(c-a)(c-b)} = -4\frac{(X-a)(X-b)}{(a-b)^2}.$$

$$x = \frac{a+b}{2} + \frac{b-a}{2}u$$

Relation connue sous le nom de « formule des trois niveaux ».

Copyrighted material

Exercices

Pour les exercices faisant appel au calcul matriciel, on peut se référer au livre Algèbre et Géométrie, MPSI, chapitre 13, et pour des exercices de niveau 1, aux chapitres 9 et 12 (Espaces vectoriels et applications linéaires, Dimension finie) et chapitre 14 (Déterminants) de ce même ouvrage.

Niveau 2

Ex. 1

Soit E et F des $\mathbb{K}$-espaces vectoriels de dimension finie et G un sous-espace de E. On pose :

$$A = \{u \in \mathcal{L}(E,F),\ \operatorname{Ker} u \supset G\}.$$

Montrer que A est un sous-espace vectoriel de $\mathcal{L}(E,F)$ et calculer sa dimension.

Ex. 2

Soit E un $\mathbb{C}$-espace vectoriel, $\dim E = 3$, et $f \in \mathcal{L}(E)$ tel que $f^2 = f^3$, et $\dim \operatorname{Ker}(f - \mathrm{Id}_E) = 1$. Montrer qu'il existe une base de E dans laquelle la matrice de f est de la forme $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \lambda \\ 0 & 0 & 0 \end{pmatrix}$ avec $\lambda \in \{0,1\}$.

Ex. 3

Quelles sont les sous-algèbres de dimension finie de $\mathcal{C}(\mathbb{R},\mathbb{R})$?

Ex. 4

Soit $A \in \mathcal{M}_{3,2}(\mathbb{R})$ et $B \in \mathcal{M}_{2,3}(\mathbb{R})$ telles que :

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

1) Vérifier que AB est idempotente.

Calculer $\operatorname{rg} A$ et $\operatorname{rg} B$.

2) Montrer que $BA = I_2$.

Ex. 5

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n \in \mathbb{N}^*$.

1) Montrer que pour tout $f \in \mathcal{L}(E)$:

$$\operatorname{rg} f^2 = \operatorname{rg} f - \dim(\operatorname{Ker} f \cap \operatorname{Im} f). \quad \textbf{(1)}$$

2) En déduire : $\dim \operatorname{Ker} f^2 \leqslant 2 \dim \operatorname{Ker} f$. **(2)**

Ex. 6

Soit $(a_k)_{k \in [\![1,p]\!]}$ une famille de p réels distincts et $(m_k)_{k \in [\![1,p]\!]}$ une famille de p entiers naturels non nuls et tels que $\sum_{i=1}^{p} m_i = n+1$.

Montrer que les $n+1$ formes linéaires :

$$\varphi_{i,j} : P \mapsto P^{(j-1)}(a_i),\ 1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant m_i$$

forment une base du dual E^* de $E = \mathbb{R}_n[X]$.

Ex. 7

Montrer qu'il existe $(a_k)_{k \in [\![1,n]\!]} \in \mathbb{R}^n$ tel que :

$$\forall P \in \mathbb{R}_{n-1}[X],\ P = \sum_{k=1}^{n} a_k P(X+k).$$

Ex. 8

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie et a non nul dans $\mathbb{K}$. On considère $f \in \mathcal{L}(E)$ tel que :

$$f^3 - 2af^2 + a^2 f = 0.$$

1) Montrer que $\operatorname{Ker} f \oplus \operatorname{Im} f = E$.

2) Dans le cas où $\dim E = 3$, préciser la matrice de f dans une base adaptée à cette somme directe.

Niveau 3

Ex. 9

Soit $E = \mathbb{R}_n[X] = \{P \in \mathbb{R}[X] \ /\ \deg P \leqslant n\}$.

On fixe un polynôme P de degré n et $n+1$ nombre réels $a_0, a_1, \ldots, a_n$ deux à deux distincts.

Montrer que les polynômes $Q_k = P(X+a_k)$, $0 \leqslant k \leqslant n$, forment une base de $\mathbb{R}_n[X]$.

Ex. 10

Dans un $\mathbb{K}$-espace vectoriel E de dimension n, soit $(f_k)_{k \in [\![1,n]\!]}$ une famille de n endomorphismes nilpotents et deux à deux permutables.

Montrer que $f_1 \circ f_2 \circ f_3 \circ \ldots \circ f_n = 0$.

Ex. 11

Soit E un $\mathbb{K}$-espace vectoriel. On considère $f \in \mathcal{L}(E)$ tel que $f^3 = f^2 + 2f$ et on pose :

$$E_1 = \operatorname{Ker} f\ ,\ E_2 = \operatorname{Ker}(f + \mathrm{Id}_E)$$

$$E_3 = \operatorname{Ker}(f - 2\,\mathrm{Id}_E).$$

1) Prouver que $E = E_1 \oplus E_2 \oplus E_3$.

2) On note p_1, p_2, p_3 les projecteurs associés à la somme directe précédente (p_i projection sur E_i parallèlement à $E_j \oplus E_k$).

Calculer f en fonction de p_1, p_2, p_3.

Copyrighted material

En déduire qu'il existe des suites réelles $(a_n)_{\mathbb{N}^*}$, $(b_n)_{\mathbb{N}^*}$ et $(c_n)_{\mathbb{N}^*}$ telles que :

$$\forall n \in \mathbb{N}^*, f^n = a_n p_1 + b_n p_2 + c_n p_3 .$$

3) Prouver l'existence et calculer les suites réelles $(a'_n)_{\mathbb{N}^*}$, $(b'_n)_{\mathbb{N}^*}$ et $(c_n)_{\mathbb{N}^*}$ telles que :

$$\forall n \in \mathbb{N}^*, f^n = a'_n \mathrm{Id}_E + b'_n f + c'_n f^2.$$

Ex. 12

Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geqslant 1$ et $f \in \mathscr{L}(E)$ nilpotent d'indice n.

On note $\mathscr{C}(f) = \{g \in \mathscr{L}(E) / g \circ f = f \circ g\}$, $\mathscr{C}(f)$ est appelé le commutant de f.

1) Montrer que $\mathscr{C}(f)$ est une sous-algèbre de $\mathscr{L}(E)$.

2) Soit $a \in E$ tels que $f^{(n-1)}(a) \neq 0$ et φ_a l'application de $\mathscr{C}(f)$ dans E définie par :

$$\forall g \in \mathscr{C}(f),\ \varphi_a(g) = g(a).$$

Montrer que φ_a est un isomorphisme de $\mathbb{K}$-espaces vectoriels.

3) En déduire que $\mathscr{C}(f) = \mathrm{Vect}\left(\mathrm{Id}_E, f, \ldots, f^{n-1}\right)$.

Ex. 13

Soit E un $\mathbb{K}$-espace vectoriel de dimension 4 et $f \in \mathscr{L}(E)$ tel que $f^3 = 0$, $f^2 \neq 0$.

1) Calculer le rang de f.

2) Montrer qu'il existe une base $(e_i)_{1 \leqslant i \leqslant 4}$ de E telle que :

$$\mathrm{mat}_{(e_i)} f = A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ex. 14

1) Montrer que pour tout $n \in \mathbb{N}$, il existe $T_n \in \mathbb{R}[X]$, de degré n, tel que :

$$\forall x \in \mathbb{R},\ \cos nx = T_n(\cos x).$$

Que peut-on dire de la famille $(T_n)_{0 \leqslant k \leqslant n}$?

2) Soit P un polynôme à coefficients réels de degré $2n-1$ au plus. Montrer que :

$$\int_{-1}^{1} \frac{P(x)}{\sqrt{1-x^2}} \mathrm{d}x = \frac{\pi}{n} \sum_{k=1}^{n} P\left(\cos \frac{2k-1}{2n} \pi\right).$$

Ex. 15

Soit E un $\mathbb{K}$-espace vectoriel et $(F_k)_{k \in [\![1,n]\!]}$ une famille finie de sous-espaces de E.

1) On suppose que $\bigcup_{k=1}^{n} F_k$ est un sous-espace de E.

Montrer qu'il existe $(i, j) \in [\![1, n]\!]^2$ tel que $i \neq j$ et $F_i \subset F_j$.

2) Montrer que $\bigcup_{k=1}^{n} F_k$ est un sous-espace de E si et seulement si l'un des sous-espaces F_k, $1 \leqslant k \leqslant n$, contient tous les autres.

3) Les propriétés précédentes sont-elles vraies si on remplace $\mathbb{K}$ (corps de caractéristique nulle, donc infini) par un corps fini ?

Avec éléments de solution

Ex. 16

1) Soit $f \in \mathscr{L}(\mathbb{R}^3)$. On suppose que $f^2 = 0$. Montrer qu'il existe $u \in \mathbb{R}^3$ et φ une forme linéaire sur $\mathbb{R}^3$ tels que $\forall x \in \mathbb{R}^3, f(x) = \varphi(x)u$.

2) Soit E un $\mathbb{K}$-espace vectoriel et $f \in \mathscr{L}(E)$, $\mathrm{rg} f = 1$. Pour $n \in \mathbb{N}^*$, exprimer f^n en fonction de f.

Ex. 17

Soit $(a_i)_{i \in [\![0,n]\!]}$ une famille strictement croissante de réels. Pour $k \in [\![0, 3]\!]$, on considère l'espace $E_k(a)$ des applications de classe $\mathscr{C}^k$ de $[a_0, a_n]$ dand $\mathbb{R}$ dont la restriction à chaque segment $[a_{i-1}, a_i]$, $1 \leqslant i \leqslant n$, est polynomiale de degré au plus 3. Calculer la dimension de $E_k(a)$.

Ex. 18

Soit E un $\mathbb{K}$-espace vectoriel et $u \in \mathscr{L}(E)$ tel que $u^n = \mathrm{Id}_E$ avec $n \in \mathbb{N}^*$. Étant donné un sous-espace vectoriel V stable par u et un projecteur p d'image V, on pose $q = \frac{1}{n} \sum_{k=1}^{n} u^k \circ p \circ u^{n-k}$.

1) Montrer que $q \circ u = u \circ q$ et en déduire que q est un projecteur.

2) Montrer que $q \circ p = p$.

3) Montrer que $\mathrm{Ker}\, q$ est un supplémentaire de V stable par u.

Ex. 19

1) Soit $n \in \mathbb{N}^*$ et P, Q dans $\mathbb{C}[X]$, $\deg P = n$ et $\deg Q = n$. Montrer l'équivalence de **(1)** et **(2)** :

(1) P et Q ont une racine commune,

(2) il existe U et V non nuls dans $\mathbb{C}_{n-1}[X]$ tels que $UP + VQ = 0$.

2) Soit A et B dans $\mathbb{C}[X]$, $\deg A = \deg B = 2$.

On considère :

$$\phi : \left(\mathbb{C}_1[X]\right)^2 \to \mathbb{C}_3[X], (U, V) \mapsto UA + VB.$$

Montrer que φ est linéaire et écrire sa matrice dans des bases à choisir.

3) En déduire une condition nécessaire et suffisante pour que A et B aient une racine commune.

Copyrighted material

Indications

Ex. 1

Utiliser un supplémentaire H de G dans E et, pour $u \in A$, la restriction u_H de u à H.

Ex. 2

f^2 est un projecteur.

Montrer que $\operatorname{Ker}\left(f^2 - \mathrm{Id}_E\right) = \operatorname{Ker}\left(f - \mathrm{Id}_E\right)$.

Ex. 3

Soit A une sous-algèbre de $\mathscr{C}(\mathbb{R}, \mathbb{R})$, $\dim A < +\infty$.

Il faut montrer que A est constituée des fonctions constantes. Raisonner par l'absurde : en supposant f non constante, considérer la suite des puissances de f.

($f^2 = f \times f$, $f^3 = f \times f^2$ etc.)

Ex. 4

Soit $g \in \mathscr{L}(\mathbb{R}^3, \mathbb{R}^2)$ canoniquement associé à B, et $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ la base canonique de $\mathbb{R}^3$. Prouver que deux vecteurs $g(\varepsilon_i)$ forment une base de $\mathbb{R}^2$.

Ex. 5

L'image de f^2 est aussi l'image de la restriction $f_{|\operatorname{Im} f}$.

Ex. 6

La famille $\left(\varphi_{i,j}\right)_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant m_i}}$ est libre si et seulement si l'intersection des noyaux des $\varphi_{i,j}$ est réduite à $\{0_E\}$.

Ex. 7

Considérer l'endomorphisme de $\mathbb{R}_{n-1}[X]$ tel que :

$$f(P) = P(X+1) - P(X).$$

Former f^n de deux manières.

Ex. 8

1) Montrer que $\operatorname{Ker} f^2 \subset \operatorname{Ker} f$.

2) Distinguer les cas $\operatorname{rg} f \in \{1, 2\}$ et $\operatorname{rg} f = 3$.

On pourra mettre en évidence un endomorphisme nilpotent de $\operatorname{Im} f$.

Ex. 9

Les polynômes dérivés $P^{(j)}(X)$, $0 \leqslant j \leqslant n$, forment une famille de degrés échelonnés.

Avec la formule de Taylor, exprimer $Q_k(X)$ à l'aide des $P^{(j)}(X)$.

Ex. 10

f_k induit un endomorphisme nilpotent de :

$$\operatorname{Im}\left(f_1 \circ f_2 \circ \cdots \circ f_{k-1}\right).$$

Ex. 11

1) Procéder par condition nécessaire pour trouver la seule décomposition possible d'un vecteur x de E sur $E_1 + E_2 + E_3$.

Ex. 12

$\left(a, f(a), \ldots, f^{n-1}(a)\right)$ est une base de E.

Ex. 13

Montrer que $\operatorname{rg} f = 2$. Étudier f tel que $\operatorname{mat} f = A$.

Ex. 14

1) Il s'agit des polynômes de Tchebychev. Utiliser $e^{ix} = \cos x + i \sin x$.

2) Ne pas oublier de prouver l'intégrabilité sur $]-1, 1[$ de la fonction $x \mapsto \dfrac{P(x)}{\sqrt{1-x^2}}$ (voir Analyse Géométrie : Intégration sur un intervalle quelconque).

Des formes linéaires coïncident sur un espace vectoriel si et seulement si elles coïncident sur une base.

Ex. 15

1) Procéder par récurrence sur n. On montrera l'hérédité par l'absurde.

2) Procéder encore par récurrence sur n.

3) La réponse est «non». Donner un contre-exemple.

Ex. 16

1) Montrer que $f = 0$ ou bien $\operatorname{rg} f = 1$ et, dans ce cas, choisir une base de $\operatorname{Im} f$.

2) Seul $\operatorname{rg} f = 1$ est utile dans la première question.

Ex. 17

À $f \in E_k(a)$ on associe sa restriction à $[a_0, a_{n-1}]$. Étudier le noyau de l'application linéaire ainsi définie et lui appliquer le théorème du rang.

Ex. 18

1) Établir que $\operatorname{Im} q \subset V$.

3) Montrer que $\operatorname{Im} q \subset \operatorname{Ker}(\mathrm{Id}_E - p)$ et $\operatorname{Im} p \subset \operatorname{Ker}(\mathrm{Id}_E - q)$.

Ex. 19

1) Utiliser le théorème de Gauss.

2) Les bases canoniques s'imposent.

3) Faire intervenir la non-injectivité de φ.

Copyrighted material

Solutions des exercices

Niveau 2

E étant un $\mathbb{K}$-espace vectoriel, pour tout $f \in \mathscr{L}(E)$ on note $\operatorname{Inv} f$ l'espace des invariants de f :

$$\operatorname{Inv} f = \{x \in E \,/\, f(x) = x\} = \operatorname{Ker}(f - \operatorname{Id}_E).$$

Ex. 1

A contient l'application nulle. Soit $(u, v) \in A^2$ et $\lambda \in \mathbb{K}$. $\forall x \in G$, $u(x) = v(x) = 0$ implique $(\lambda u + v)(x) = 0$, donc $\operatorname{Ker}(\lambda u + v) \supset G$ et A est un sous-espace vectoriel de $\mathscr{L}(E, F)$.

Étant donné un supplémentaire H de G dans E, on considère l'application φ de A dans $\mathscr{L}(H, E)$ qui, à $u \in A$, associe sa restriction u_H à H. Il est immédiat que φ est linéaire.

- Soit $v \in \operatorname{Ker}\varphi$. Alors $v_H = 0$ et, avec $v \in A$, on a aussi $v_G = 0$, donc $v = 0$ (où v_G est la restriction à G).

φ est donc injective. Pour montrer qu'elle est surjective, considérons $w \in \mathscr{L}(H, F)$.

- Soit $p \in \mathscr{L}(E)$ la projection sur H parallèlement à G et $u = w \circ p$.

Avec $\operatorname{Ker} p = G$, on a $\operatorname{Ker} u \supset G$, donc $u \in A$. Avec $H = \operatorname{Inv} p$, il vient $u_H = w$. Ainsi, ϕ est surjective.

A et $\mathscr{L}(H, F)$ sont donc isomorphes et il s'ensuit $\dim A = \dim H \dim F = (\dim E - \dim G)\dim F$.

Ex. 2

Il est immédiat que $\operatorname{Inv} f \cap \operatorname{Ker} f = \{0\}$, donc $\dim(\operatorname{Ker} f) \leqslant 2$ puisque, par hypothèse, $\dim(\operatorname{Inv} f) = 1$.

De $f^2 = f^3$ on déduit $f^3 = f^4$, donc $f^2 = f^4$, f^2 est un projecteur, et $E = \operatorname{Inv} f^2 \oplus \operatorname{Ker} f^2$.

Montons que $f + \operatorname{Id}_E$ est injective : si $x \in E$ est tel que $f(x) = -x$, alors $f^2(x) = x$ et $f^3(x) = -x$. Puis de $f^2 = f^3$, on déduit $x = 0$.

Avec $f^2 - \operatorname{Id}_E = (f + \operatorname{Id}_E) \circ (f - \operatorname{Id}_E)$ et $f + \operatorname{Id}_E$ bijective, il vient $\operatorname{Ker}(f^2 - \operatorname{Id}_E) = \operatorname{Ker}(f - \operatorname{Id}_E)$, donc :

$$\dim \operatorname{Ker}(f^2 - \operatorname{Id}_E) = 1.$$

Comme f^2 est un projecteur, il vient $\dim \operatorname{Ker} f^2 = 2$ et $E = \operatorname{Inv} f \oplus \operatorname{Ker} f^2$.

- Si $\dim(\operatorname{Ker} f) = 2$, $\operatorname{Inv} f$ et $\operatorname{Ker} f$ sont supplémentaires, donc f est un projecteur et il existe une base dans laquelle la matrice est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

- Si $\dim(\operatorname{Ker} f) = 1$, avec $\operatorname{Ker} f \subset \operatorname{Ker} f^2$ et $\dim(\operatorname{Ker} f^2) = 2$, il existe $e_3 \in \operatorname{Ker} f^2 \setminus \operatorname{Ker} f$.

Alors $f(e_3) = e_2$ est un vecteur non nul de $\operatorname{Ker} f$ et (e_2, e_3) est une base de $\operatorname{Ker} f^2$.

Si e_1 est une base de $\operatorname{Inv} f$, puisque $E = \operatorname{Inv} f \oplus \operatorname{Ker} f^2$, (e_1, e_2, e_3) est une base de E dans laquelle la matrice de f est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

Ex. 3

Soit A une sous-algèbre de dimension finie de $\mathscr{C}(\mathbb{R}, \mathbb{R})$ et f un élément de A.

- Supposons f non constante, il existe alors $(a, b) \in \mathbb{R}^2$, $a < b$, tel que $f(a) \neq f(b)$. L'application f étant continue on a, d'après le théorème des valeurs intermédiaires :

$$[f(a), f(b)] \subset f([a, b]) \quad \text{donc} \quad f(\mathbb{R}) \supset [f(a), f(b)]$$

et ce segment n'étant pas réduit à un point, f prend une infinité de valeurs distinctes.

- A étant de dimension finie, il existe $p \in \mathbb{N}^*$ tel que $(1, f, f^2, \ldots, f^p)$ soit lié.

Il existe donc $(\lambda_0, \lambda_1, \ldots, \lambda_p) \in \mathbb{R}^{p+1} \setminus \{(0, 0, \ldots, 0)\}$ tel que $\sum_{i=0}^{p} \lambda_i f^i = 0$.

Copyrighted material

Pour tout $x \in \mathbb{R}$, on a alors $\sum_{i=0}^{p} \lambda_i \big(f(x)\big)^i = 0$ d'où pour tout $y \in f(\mathbb{R})$, $\sum_{i=0}^{p} \lambda_i y^i = 0$.

Ainsi le polynôme $P = \sum_{i=0}^{p} \lambda_i X^i$ a une infinité de racines, c'est donc le polynôme nul, ce qui est contradictoire avec :

$$(\lambda_0, \lambda_1, \cdots, \lambda_n) \neq (0, 0, \cdots, 0).$$

En conséquence, f est constante. $\mathscr{C}(\mathbb{R}, \mathbb{R})$ contient une seule sous-algèbre de dimension finie, c'est la sous-algèbre des fonctions constantes.

Ex. 4

1) On vérifie que $(AB)^2 = AB$.

- Notons $e = (e_1, e_2)$ et $\varepsilon = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$ les bases canoniques de $\mathbb{R}^2$ et $\mathbb{R}^3$ respectivement.

Soit $f \in \mathscr{L}(\mathbb{R}^2, \mathbb{R}^3)$ et $g \in \mathscr{L}(\mathbb{R}^3, \mathbb{R}^2)$ telles que $A = \mathrm{mat}_{e,\varepsilon}(f)$ et $B = \mathrm{mat}_{\varepsilon,e}(g)$ alors AB est la matrice sur la base ε de $h = f \circ g \in \mathscr{L}(\mathbb{R}^3)$.

- L'endomorphisme h est un projecteur de $\mathbb{R}^3$ et il est visible que les deux premières colonnes de AB sont indépendantes donc $\mathrm{rg}\, h = 2$ avec :

$$\mathrm{Im}\, h = \mathrm{Vect}\,\big(hbig(\varepsilon_1\big), h\big(\varepsilon_2\big)\big) = \mathrm{Vect}\,\big(\varepsilon_3 - \varepsilon_2, \varepsilon_3 - \varepsilon_1\big)$$

Remarque

$$\mathrm{Im}\, h = \mathrm{Vect}\,\big(h(\varepsilon_1), h(\varepsilon_2)\big) = \mathrm{Vect}\,\big(h(\varepsilon_2), h(\varepsilon_3)\big) = \mathrm{Vect}\,\big(h(\varepsilon_1), h(\varepsilon_3)\big)$$

$$\mathrm{Ker}\, h = \mathrm{Vect}\,\big(\varepsilon_1 + \varepsilon_2 - \varepsilon_3\big)$$

- De $f \circ g = h$ on déduit $\mathrm{Im}\, h = f(\mathrm{Im}\, g)$ et donc, d'après le théorème du rang appliqué à la restriction, $f_{|\mathrm{Im}\, g} \in \mathscr{L}\big(\mathrm{Im}\, g, \mathbb{R}^3\big)$:

$$\dim \mathrm{Im}\, h \leqslant \dim \mathrm{Im}\, g \quad \text{c'est-à-dire} \quad \mathrm{rg}\, g \geqslant 2.$$

Or $g \in \mathscr{L}(\mathbb{R}^3, \mathbb{R}^2)$ donne $\mathrm{rg}\, g \leqslant 2$ d'où finalement $\mathrm{rg}\, g = 2$.

- Avec $h = f \circ g$, on a $\mathrm{Im}\, h \subset \mathrm{Im}\, f$ donc $\mathrm{rg}\, f \geqslant \mathrm{rg}\, h$ c'est-à-dire $\mathrm{rg}\, f \geqslant 2$.

Or $f \in \mathscr{L}(\mathbb{R}^2, \mathbb{R}^3)$ donne $\mathrm{rg}\, f \leqslant 2$ d'où finalement $\mathrm{rg}\, f = 2$.

2) L'image par toute application linéaire d'un système lié est un système lié.

Donc $\big(h(\varepsilon_1), h(\varepsilon_2)\big) = \big(f(g(\varepsilon_1)), f(g(\varepsilon_2))\big)$ étant libre, a fortiori $\big(g(\varepsilon_1), g(\varepsilon_2)\big)$ est libre et constitue une base de $\mathbb{R}^2$. Puisque $h = f \circ g$ est un projecteur, on a alors :

$$f \circ g \circ f \circ g(\varepsilon_i) = f \circ g(\varepsilon_i) \quad \text{pour } i = 1 \text{ ou } 2.$$

Or $\mathrm{rg}\, f = 2$ avec $f \in \mathscr{L}(\mathbb{R}^2, \mathbb{R}^3)$ donne, d'après le théorème du rang, que f est injective. On déduit donc des relations précédentes que $g \circ f\big(g(\varepsilon_i)\big) = g(\varepsilon_i)$, $i = 1$ ou 2, et puisque $\big(g(\varepsilon_1), g(\varepsilon_2)\big)$ est une base de $\mathbb{R}^2$, il vient $g \circ f = \mathrm{Id}_{\mathbb{R}^2}$ donc $BA = I_2$.

Remarque. On peut faire le même raisonnement avec $(\varepsilon_1, \varepsilon_3)$ ou avec $(\varepsilon_2, \varepsilon_3)$. On peut aussi, en utilisant l'injectivité de f et la surjectivité de g, montrer que $\forall x \in \mathbb{R}^2$, $g \circ f(x) = x$.

Ex. 5

1) On a $\mathrm{Im}\, f^2 = f\big(f(E)\big) = f(\mathrm{Im}\, f)$.

D'autre part, $\mathrm{Im}\, f$ est stable par f donc $f_{|\mathrm{Im}\, f}$ induit un endomorphisme φ de $\mathrm{Im}\, f$ tel que $\mathrm{Im}\, f^2 = \mathrm{Im}\, \varphi$ ce qui donne : $\mathrm{rg}\, f^2 = \mathrm{rg}\, \varphi$.

D'après le théorème du rang appliqué à $\varphi \in \mathscr{L}(\mathrm{Im}\, f)$: $\mathrm{rg}\, \varphi = \dim \mathrm{Im}\, f - \dim \mathrm{Ker}\, \varphi$.

Avec $\mathrm{Ker}\, \varphi = ig\{x \in \mathrm{Im}\, f \,/\, f(x) = 0\big\} = \mathrm{Im}\, f \cap \mathrm{Ker}\, f$, il vient :

$$\mathrm{rg}\, f^2 = \mathrm{rg}\, f - \dim(\mathrm{Ker}\, f \cap \mathrm{Im}\, f). \quad \textbf{(1)}$$

2) Toujours avec le théorème du rang :

$$\dim \mathrm{Ker}\, f^2 = n - \mathrm{rg}\, f^2$$

$$\dim \mathrm{Ker}\, f = n - \mathrm{rg}\, f$$

donc l'égalité **(1)** donne : $\dim \mathrm{Ker}\, f^2 = \dim \mathrm{Ker}\, f + \dim(\mathrm{Ker}\, f \cap \mathrm{Im}\, f)$.

Or $\mathrm{Ker}\, f \cap \mathrm{Im}\, f \subset \mathrm{Ker}\, f$, donc $\dim(\mathrm{Ker}\, f \cap \mathrm{Im}\, f) \leqslant \dim \mathrm{Ker}\, f$, et finalement :

$$\dim \mathrm{Ker}\, f^2 \leqslant 2 \dim \mathrm{Ker}\, f. \quad \textbf{(2)}$$

Copyrighted material

Ex. 6

La famille $\Phi = \left(\varphi_{i,j}\right)_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant m_i}}$ est libre (théorème **20**, corollaire **2**) si et seulement si $\bigcap_{\substack{1\leqslant i\leqslant p\\ 1\leqslant j\leqslant m_i}} \operatorname{Ker}\varphi_{i,j} = \{0_E\}$.

Soit un polynôme P de E appartenant à cette intersection ; on a : $\forall i\in[\![1,p]\!],\ \forall k\in[\![0,m_i-1]\!],\ P^{(k)}(a_i)=0$, donc a_i est racine d'ordre m_i de P, c'est-à-dire que P est divisible par $(X-a_i)^{m_i}$.

Les a_i étant distincts, P est divisible par $Q=\prod_{i=1}^{p}(X-a_i)^{m_i}$. Or on a $\deg Q=\sum_{i=1}^{p} m_i = n+1$ et $\deg P\leqslant n$.

On en déduit $P=0$. La famille Φ est donc libre et, puisque $\operatorname{Card}\Phi = n+1 = \dim E$, c'est une base de E.

Ex. 7

Soit f l'endomorphisme de $\mathbb{R}_{n-1}[X]$ défini par : $\forall P\in\mathbb{R}_{n-1}[X],\ f(P)=P(X+1)-P(X)$.

- Premier calcul de f^n

$P(X)$ et $P(X+1)$ ont le même degré et le même coefficient dominant. On a donc $\deg f(P)\leqslant \deg P-1$.

Par récurrence, il vient $\deg f^k(P)\leqslant \deg P-k$, puis $\deg f^{n-1}(P)\leqslant 0$. Alors $f^{n-1}(P)$ est constant, puis $f^n(P)=0$.

- Second calcul de f^n

On a $f(P)=P(x+1)-P(x)$ puis $f^2(P)=P(X+2)-2P(X+1)+P(X)$.

Par récurrence, on obtient $f^r(P)=\sum_{k=0}^{r}(-1)^{r-k}\binom{k}{r}P(X+k)$ pour tout $r\in\mathbb{N}^*$.

Or on a $f^n(P)=0$. Il s'ensuit $(-1)^n P(X)=\sum_{k=1}^{n}(-1)^{n+1-k}\binom{k}{n}P(X+k)$, soit $P(X)=\sum_{k=1}^{n}(-1)^{k-1}\binom{k}{n}P(X+k)$.

Ex. 8

1) $f=-\frac{1}{a^2}\left(f-2a\operatorname{Id}_E\right)\circ f^2$ montre que $\operatorname{Ker} f^2$ est inclus dans $\operatorname{Ker} f$.

L'inclusion $\operatorname{Ker} f\subset\operatorname{Ker} f^2$ est usuelle. On a donc $\operatorname{Ker} f=\operatorname{Ker} f^2$.

Soit $y\in\operatorname{Ker} f\cap\operatorname{Im} f$. Il existe $x\in E$, $y=f(x)$. Alors $f(y)=f^2(x)$ donc $f^2(x)=0$ puisque $y\in\operatorname{Ker} f$.

Étant dans le noyau de f^2, x est aussi dans le noyau de f, d'où $y=f(x)=0$ et $\operatorname{Im} f\cap\operatorname{Ker} f=\{0\}$.

Le théorème du rang $\dim(\operatorname{Im} f)+\dim(\operatorname{Ker} f)=\dim E$ permet alors de conclure : $\operatorname{Im} f\oplus\operatorname{Ker} f=E$.

2) Le cas où $\operatorname{rg} f=0$ est banal. Dans les autres cas, f induit un automorphisme $\overline{f}$ de $\operatorname{Im} f$.

$f^3-2af^2+a^2f=0$ se lit aussi $f\circ\left(f-a\operatorname{Id}_E\right)^2=0$, donc $\overline{f}\circ\left(\overline{f}-a\operatorname{Id}_{\operatorname{Im} g}\right)^2=0$ puis $\left(\overline{f}-a\operatorname{Id}_{\operatorname{Im} f}\right)^2=0$.

- Dans le cas où $\operatorname{rg} f=1$, alors $\dim\operatorname{Ker} f=2$. Endomorphisme nilpotent d'un espace de dimension 1, $\overline{f}-a\operatorname{Id}_{\operatorname{Im} f}$ est nul. Une matrice de f est alors $\begin{pmatrix}a&0&0\\0&0&0\\0&0&0\end{pmatrix}$.

- Dans le cas où $\operatorname{rg} f=2$, alors $\dim\operatorname{Ker} f=1$. Endomorphisme nilpotent d'un espace de dimension 2, on a :

ou bien $\overline{f}-a\operatorname{Id}_{\operatorname{Im} f}=0$, et une matrice de f est évidemment $\begin{pmatrix}a&0&0\\0&a&0\\0&0&0\end{pmatrix}$;

ou bien $\overline{f}-a\operatorname{Id}_{\operatorname{Im} f}\neq 0$, et $\left(\overline{f}-a\operatorname{Id}_{\operatorname{Im} f}\right)^2=0$. Il existe alors une base (e_1,e_2) de $\operatorname{Im} f$ telle que $e_2=\left(\overline{f}-a\operatorname{Id}_{\operatorname{Im} f}\right)(e_1)$.

Alors $f(e_1)=ae_1+e_2$ et $\overline{f}^2=2a\overline{f}-a^2\operatorname{Id}_{\operatorname{Im} f}$ donne $f(e_2)=ae_2$. Une matrice de f est donc $\begin{pmatrix}a&0&0\\1&a&0\\0&0&0\end{pmatrix}$.

- Dans le cas où $\operatorname{rg} f=3$, alors f est bijective telle que $\left(f-a\operatorname{Id}_E\right)^2=0$. Si $f=a\operatorname{Id}_E$, la matrice est scalaire. Pour $f\neq a\operatorname{Id}_E$, on a $\operatorname{rg}\left(f-a\operatorname{Id}_E\right)=1$. Soit (e_1,e_2) une base de $\operatorname{Ker}\left(f-a\operatorname{Id}_E\right)$ et $e_3\notin\operatorname{Ker}\left(f-a\operatorname{Id}_E\right)$.

Copyrighted material

Posons $f(e_3) = \alpha e_1 + \beta e_2 + \gamma e_3$. Avec $f^2(e_3) = a\,\alpha\, e_1 + a\,\beta\, e_2 + \gamma f(e_3)$ et $f^2(e_3) = 2af(e_3) - a^2 e_3$,
il vient $\gamma = a$ et une matrice de f est $\begin{pmatrix} a & 0 & \alpha \\ 0 & a & \beta \\ 0 & 0 & a \end{pmatrix}$.

Niveau 3

Ex. 9

$\dim E = n+1$ et $\text{Card}\left\{Q_k \,/\, 0 \leqslant k \leqslant n\right\} = n+1$, il suffit donc de montrer que la famille $(Q_k)_{0\leqslant k\leqslant n}$ est libre.

La formule de Taylor donne pour tout $k \in [\![0, n]\!]$, $\quad Q_k(X) = \sum_{j=0}^{n} \frac{a_k^j}{j!} P^{(j)}(X)$. **(1)**

Considérons $n+1$ réels $\lambda_0, \lambda_1, \ldots, \lambda_n$ tels que $\sum_{k=0}^{n} \lambda_k Q_k(X) = 0$. **(2)**

Avec **(1)**, il vient $\sum_{k=0}^{n}\sum_{j=0}^{n} \lambda_k \frac{a_k^j}{j!} P^{(j)}(X) = 0$ soit $\sum_{j=0}^{n} \frac{P^{(j)}(X)}{j!} \sum_{k=0}^{n} \lambda_k a_k^j = 0$. **(3)**

La famille $\left(\frac{1}{j!}P^{(j)}(X)\right)_{0\leqslant j\leqslant n}$ est de degrés échelonnés : $\deg P^{(j)}(X) = n - j$ et elle comporte $n+1$ éléments.

C'est donc une base de $\mathbb{R}_n[X]$ et la relation **(3)** donne : $\forall j \in [\![0, n]\!]$, $\sum_{k=0}^{n} \lambda_k a_k^j = 0$. **(4)**

Matriciellement les relations **(4)** s'écrivent :

$$\begin{pmatrix} 1 & \cdots\cdots & 1 \\ a_0 & \cdots\cdots & a_n \\ a_0^2 & \cdots\cdots & a_n^2 \\ \vdots & & \vdots \\ a_0^n & \cdots\cdots & a_n^n \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$A = \left[a_j^i\right]_{\substack{0\leqslant i\leqslant n \\ 0\leqslant j\leqslant n}}$ est la matrice de Vandermonde des $n+1$ nombres $a_0, a_1, \ldots, a_n$.

Ceux-ci étant deux à deux distincts, A est inversible et **(4)** donne $\lambda_0 = \lambda_1 = \cdots = \lambda_n = 0$.

On a donc prouvé que $(Q_k)_{0\leqslant n}$ est une famille libre.

Ex. 10

Montrons par récurrence que $\text{rg}\left(f_1 \circ f_2 \circ \cdots \circ f_k\right) \leqslant n - k$.

- La propriété est vraie pour $k = 1$, en effet f_1 étant nilpotent, on a $\text{rg}\, f_1 \leqslant n - 1$.
- Supposons $\text{rg}\left(f_1 \circ f_2 \circ \cdots \circ f_{k-1}\right) \leqslant n - k + 1$ avec $k \leqslant n$.

Posons $F_{k-1} = f_1 \circ f_2 \circ \cdots \circ f_{k-1}$. Les f_i étant deux à deux permutables, on a $f_k \circ F_{k-1} = F_{k-1} \circ f_k$.

Il en résulte que $\text{Im}\, F_{k-1}$ est stable par f_k ; en effet, pour $y = F_{k-1}(x)$, élément de $\text{Im}\, F_{k-1}$, on a :

$$f_k(y) = f_k\left(F_{k-1}(x)\right) = F_{k-1}\left(f_k(x)\right) \text{ donc } f_k(y) \in \text{Im}\, F_{k-1}.$$

L'endomorphisme f_k de E induit donc un endomorphisme g_k de $\text{Im}\, F_{k-1}$:

$$\forall x \in \text{Im}\, F_{k-1}.\, g_k(x) = f_k(x)$$

et puisque f_k est nilpotent, il en est de même pour g_k car $g_k^n(x) = f_k^n(x) = 0$.

Puisque g_k est un endomorphisme nilpotent de $\text{Im}\, F_{k-1}$, on a $\text{rg}\, g_k \leqslant \dim \text{Im}\, F_{k-1} - 1$.

Or $\text{rg}\, g_k = \dim f_k\left(\text{Im}\, F_{k-1}\right) = \dim \text{Im}\left(f_1 \circ f_2 \circ \cdots \circ f_k\right) = \text{rg}\left(f_1 \circ f_2 \circ \cdots \circ f_k\right)$, donc :

$$\text{rg}\left(f_1 \circ f_2 \circ \cdots \circ f_k\right) \leqslant n - k.$$

On a ainsi prouvé que la propriété est récurrente.

- En conséquence, on a $\text{rg}\left(f_1 \circ f_2 \circ \cdots \circ f_n\right) \leqslant 0$, donc :

$$\text{rg}\left(f_1 \circ f_2 \circ \cdots \circ f_n\right) = 0 \quad \text{c'est-à-dire} \quad f_1 \circ f_2 \circ \cdots \circ f_n = 0.$$

Copyrighted material

Ex. 11

1) Il s'agit de montrer que, pour tout $x \in E$, il existe un unique triplet $(x_1, x_2, x_3) \in E_1 \times E_2 \times E_3$ tel que :

$$x = x_1 + x_2 + x_3 .$$

Supposons qu'un tel triplet existe, alors on a nécessairement :

$$\begin{cases} x & = & x_1 & + & x_2 & + & x_3 & \textbf{(1)} \\ f(x) & = & & - & x_2 & + & 2x_3 & \textbf{(2)} \\ f^2(x) & = & & & x_2 & + & 4x_3 & \textbf{(3)} \end{cases}$$

Par combinaison linéaire de **(2)** et **(3)**, il vient :

$$x_3 = \frac{1}{6}\left(f^2(x) + f(x)\right) \qquad \textbf{(2)} + \textbf{(3)}$$

$$x_2 = \frac{1}{3}\left(f^2(x) - 2f(x)\right) \qquad -2\times \textbf{(2)} + \textbf{(3)}$$

puis **(1)** donne : $x_1 = -\frac{1}{2}\left(f^2(x) - f(x) - 2x\right)$.

Ce calcul montre qu'il y a au plus un triplet (x_1, x_2, x_3) solution du problème. Pour prouver qu'il y en a un et un seul, il suffit donc de vérifier que le triplet que l'on vient de calculer est effectivement solution.

Par construction, x_1 , x_2 , x_3 vérifie l'équation **(1)** : $x_1 + x_2 + x_3 = x$. Il reste donc à montrer que $x_1 \in E_1$, $x_2 \in E_2$ et $x_3 \in E_3$.

En utilisant $f^3 = f^2 + 2f$, le calcul donne :

$$f(x_1) = -\frac{1}{2}\left(f^3(x) - f^2(x) - 2f(x)\right) = 0 \qquad \text{donc } x_1 \in E_1$$

$$f(x_2) = \frac{1}{3}\left(f^3(x) - 2f^2(x)\right) = -\frac{1}{3}\left(f^2(x) - 2f(x)\right) = -x_2 \qquad \text{donc } x_2 \in E_2$$

$$f(x_3) = \frac{1}{6}\left(f^3(x) + f^2(x)\right) = \frac{1}{3}\left(f^2(x) + f(x)\right) = 2x_3 \qquad \text{donc } x_3 \in E_3$$

Ainsi, pour tout $x \in E$, il existe $(x_1 , x_2 , x_3) \in E_1 \times E_2 \times E_3$ unique tel que :

$$x = x_1 + x_2 + x_3 \quad \text{donc} \quad E = E_1 \oplus E_2 \oplus E_3 .$$

2) Avec la décomposition précédente : $x = x_1 + x_2 + x_3$, il vient $f(x) = -x_2 + 2x_3$, or $x_2 = p_2(x)$ et $x_3 = p_3(x)$ donc $f = -p_2 + 2p_3$. Sachant que $p_2 \circ p_3 = p_3 \circ p_2 = 0$, la formule du binôme s'applique et donne :

$$\forall n \in \mathbb{N}^*, \quad f^n = \sum_{k=0}^{n} \mathrm{C}_n^k (-1)^k 2^{n-k} p_2^k \circ p_3^{n-k}$$

ce qui se réduit à $f^n = (-1)^n p_2 + 2^n p_3$.

Remarquons de plus que pour $n = 0$, $f^0 = \mathrm{Id}_E = p_1 + p_2 + p_3$.

3) D'après le 1), on a pour tout $x \in E$:

$$p_1(x) = x_1 = -\frac{1}{2}\left(f^2(x) - f(x) - 2x\right)$$

$$p_2(x) = x_2 = \frac{1}{3}\left(f^2(x) - 2f(x)\right)$$

$$p_3(x) = x_3 = \frac{1}{6}\left(f^2(x) + f(x)\right)$$

On en déduit : $p_1 = -\frac{1}{2}\left(f^2 - f - 2\,\mathrm{Id}_E\right)$. $p_2 = \frac{1}{3}\left(f^2 - 2f\right)$. $p_3 = \frac{1}{6}\left(f^2 + f\right)$, d'où :

$$\forall n \in \mathbb{N}^*, \ f^n = \left(\frac{2^{n-1} - 2(-1)^n}{3}\right) f + \left(\frac{2^{n-1} + (-1)^n}{3}\right) f^2 .$$

Ex. 12

1) On vérifie aisément que :

- $\mathscr{C}(f)$ contient Id_E,
- $\mathscr{C}(f)$ est stable par combinaison linéaire,
- $\mathscr{C}(f)$ est stable pour la loi $\circ$.

2) Il est clair que φ_a est linéaire : $\forall (\lambda, \mu) \in \mathbb{K}^2, \ \forall (g, h) \in \mathscr{C}(f)^2, \quad \varphi_a(\lambda g + \mu h) = \lambda\, \varphi_a(g) + \mu\, \varphi_a(b)$.

Copyrighted material

▪ Puisque $f^{n-1}(a) \neq 0$, le système $\left(e_k\right)_{1\leqslant k\leqslant n}$ tel que :

$$e_1 = a \ , \ e_2 = f(a), \ldots, e_k = f^{k-1}(a) \ldots, e_n = f^{n-1}(a),$$

est une base de E (voir la propriété 26).

Il en résulte que la famille $\left(f^k\right)_{0\leqslant k\leqslant n-1}$ est libre dans $\mathscr{C}(f)$.

En effet $\sum_{k=0}^{n-1} \lambda_k f^k = 0$, avec $\left(\lambda_0, \lambda_1, \ldots, \lambda_n\right) \in \mathbb{K}^n$, donne en particulier $\sum_{k=0}^{n-1} \lambda_k f^k(a) = 0$, d'où :

$$\lambda_0 = \lambda_1 = \ldots = \lambda_n = 0.$$

On a donc $\dim \mathscr{C}(f) \geqslant n$.

▪ Montrons maintenant que φ_a est injective.

Pour $g \in \operatorname{Ker} \varphi_a$, on a $g(a) = 0$, or g est permutable avec f, donc aussi avec toute puissance de f et il vient pour tout $k \in \mathbb{N}$, $g\left(f^k(a)\right) = f^k\left(g(a)\right) = 0$.

Ainsi $\forall k \in [\![1, n]\!], g\left(e_k\right) = 0$ d'où $g = 0$. On a prouvé que $\operatorname{Ker} \varphi_a = \{0\}$: φ_a est injective.

▪ L'injectivité de φ_a donne $\dim \operatorname{Im} \varphi_a = \dim \mathscr{C}(f) \geqslant n$.

Or $\operatorname{Im} \varphi_a \subset E$ avec $\dim E = n$, donc $\operatorname{Im} \varphi_a = E$.

Ainsi φ_a est surjective et finalement c'est un isomorphisme d'espaces vectoriels de $\mathscr{C}(f)$ sur E.

3) D'après le 2), $\left(\mathrm{Id}_E, f, \ldots, f^{n-1}\right)$ est une base de $\mathscr{C}(f)$.

Ex. 13

1) f est nilpotent et non nul donc $1 \leqslant \operatorname{rg} f \leqslant 3$.

▪ Supposons $\operatorname{rg} f = 3$, alors d'après le théorème du rang $\dim \operatorname{Ker} f = 1$.

Avec $\operatorname{Im} f^2 = f\left(f(E)\right) = \operatorname{Im}\left(f_{|\operatorname{Im} f}\right)$ on obtient : $\operatorname{rg} f^2 = \operatorname{rg} f - \dim(\operatorname{Ker} f \cap \operatorname{Im} f)$, puis :

$$0 \leqslant \operatorname{rg} f - \operatorname{rg} f^2 \leqslant \dim \operatorname{Ker} f. \quad \textbf{(1)}$$

De même $\operatorname{Im} f^3 = f\left(f^2(E)\right) = \operatorname{Im}\left(f_{|\operatorname{Im} f^2}\right)$ donne (théorème du rang) : $\operatorname{rg} f^3 = \operatorname{rg} f^2 - \dim(\operatorname{Ker} f \cap \operatorname{Im} f^2)$, d'où :

$$0 \leqslant \operatorname{rg} f^2 - \operatorname{rg} f^3 \leqslant \dim \operatorname{Ker} f. \quad \textbf{(2)}$$

De **(1)** et **(2)** on déduit $0 \leqslant \operatorname{rg} f - \operatorname{rg} f^3 \leqslant 2 \dim \operatorname{Ker} f$ donc $\operatorname{rg} f^3 \geqslant 1$, ce qui est contradictoire avec $f^3 = 0$.

▪ Supposons maintenant $\operatorname{rg} f = 1$ alors $\dim \operatorname{Ker} f = 3$ et deux cas sont possibles :

$$\operatorname{Im} f \cap \operatorname{Ker} f = \{0_E\} \quad \text{ou} \quad \operatorname{Im} f \subset \operatorname{Ker} f$$

– Pour $\operatorname{Im} f \cap \operatorname{Ker} f = \{0_E\}$, $f_{|\operatorname{Im} f}$ induit un isomorphisme de $\operatorname{Im} f$ sur $\operatorname{Im} f^2$ donc :

$$\operatorname{rg} f = \operatorname{rg} f^2 \quad \text{puis de même} \quad \operatorname{rg} f^2 = \operatorname{rg} f^3.$$

Ainsi $\operatorname{rg} f^3 = 1$ ce qui est contradictoire avec $f^3 = 0$.

– Pour $\operatorname{Im} f \subset \operatorname{Ker} f$ on a $f^2 = 0$ ce qui est encore une contradiction.

▪ En conclusion, s'il existe de tels endomorphismes on a nécessairement $\operatorname{rg} f = 2$.

On peut remarquer que la matrice A de la question suivante vérifie :

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{et} \quad A^3 = 0.$$

Il existe donc bien des endomorphismes $f \in \mathscr{L}(E)$ tels que $f^2 \neq 0$ et $f^3 = 0$.

2) ▪ Analyse

S'il existe une base $\mathscr{B} = (e_i)_{1\leqslant i\leqslant n}$ telle que $\operatorname{mat}_{\mathscr{B}} f = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$,

celle-ci vérifie les conditions :

$$\begin{cases} e_2 = f(e_1) \quad , \quad e_3 = f(e_2) = f^2(e_1) \\ (e_2, e_3) \text{ est une base de } \operatorname{Im} f \\ (e_3, e_4) \text{ est une base de } \operatorname{Ker} f \\ \operatorname{Im} f \cap \operatorname{Ker} f = \mathbb{K} e_3 \end{cases}$$

Copyrighted material

▪ Synthèse

f^2 est non nul donc il existe $e_1 \in E$ tel que $f^2(e_1) \neq 0$. On pose $e_2 = f(e_1)$ et $e_3 = f^2(e_1)$.

$f^3 = 0$ donne $\mathrm{Im} f^2 \subset \mathrm{Ker} f$ donc $e_3 \in \mathrm{Ker} f$ et $\mathrm{Ker} f$ étant de dimension 2, on peut trouver e_4 tel que (e_3, e_4) soit une base de $\mathrm{Ker} f$.

Montrons alors que (e_1, e_2, e_3, e_4) est une base de E.

Soit $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{K}^4$ tel que $\sum_{i=1}^{4} \alpha_i e_i = 0$.

Appliquons f^2 à cette égalité, il vient : $\alpha_1 e_3 = 0$ donc $\alpha_1 = 0$, puis appliquons f, il vient $\alpha_2 e_3 = 0$ donc $\alpha_2 = 0$, il reste $\alpha_3 e_3 + \alpha_4 e_4 = 0$ ce qui donne $\alpha_3 = \alpha_4 = 0$ car (e_3, e_4) est libre.

Par construction de la base $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant 4}$, on a $\mathrm{mat}_{\mathcal{B}} f = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Ex. 14

1) On a $e^{inx} = \left(e^{ix}\right)^n$ donc $\cos nx = \mathrm{Re}(\cos x + i \sin x)^n$.

La formule du binôme donne : $(\cos x + i \sin x)^n = \sum_{k=0}^{n} \mathrm{C}_n^k i^k \sin^k x \cos^{n-k} x$, d'où :

$$\cos nx = \sum_{0 \leqslant 2k \leqslant n} (-1)^k \mathrm{C}_n^{2k} \left(1 - \cos^2 x\right)^k \cos^{n-2k} x$$

et il suffit de poser $T_n = \sum_{0 \leqslant 2k \leqslant n} (-1)^k \mathrm{C}_n^{2k} \left(1 - X^2\right)^k X^{n-2k}$ pour avoir : $\cos nx = T_n(\cos x)$.

Chaque produit $\left(1 - X^2\right)^k X^{n-2k}$ étant de degré n, on a d'abord $\deg T_n \leqslant n$.

Le coefficient de X^n dans T_n est $a_n = \sum_{0 \leqslant 2k \leqslant n} \mathrm{C}_n^{2k}$, il est visiblement non nul donc $\deg T_n = n$.

Remarque.

Le calcul de a_n est classique : on pose $b_n = \sum_{0 \leqslant 2k+1 \leqslant n} \mathrm{C}_n^{2k+1}$ et la formule du binôme donne :

$$(1+1)^n = a_n + b_n \ , \ (1-1)^n = a_n - b_n \quad \text{d'où} \quad a_n = b_n = 2^{n-1}.$$

La famille $(T_k)_{0 \leqslant k \leqslant n}$ étant de degrés échelonnés, c'est une base du $\mathbb{R}$-espace vectoriel $\mathbb{R}_n[X]$.

2) La fonction P est continue donc bornée sur $[-1, 1]$, donc $f : x \mapsto \dfrac{P(x)}{\sqrt{1-x^2}}$ est continue sur $]-1, 1[$ et il existe $M \in \mathbb{R}_+^*$ tel que :

$$\forall x \in]-1, 1[, \quad |f(x)| \leqslant \frac{M}{\sqrt{1-x^2}}.$$

Au voisinage de 1, on a $\dfrac{M}{\sqrt{1-x^2}} \sim \dfrac{M}{\sqrt{2}\sqrt{1-x}}$ et on sait que $x \mapsto \dfrac{1}{\sqrt{1-x}}$ est intégrable sur $[0, 1[$. Il en résulte que $x \mapsto \dfrac{M}{\sqrt{1-x^2}}$ puis que f est intégrable sur $[0, 1]$.

De même, $x \mapsto \dfrac{1}{\sqrt{1+x}}$ est intégrable sur $]-1, 0]$ donc $x \mapsto \dfrac{M}{\sqrt{1-x^2}}$ et f le sont aussi.

On remarque maintenant que :

$$\varphi : P \mapsto \int_{-1}^{1} \frac{P(x)}{\sqrt{1-x^2}} \mathrm{d}x \quad \text{et} \quad \psi : P \mapsto \frac{\pi}{n} \sum_{k=1}^{n} P\left(\cos \frac{2k-1}{2n} \pi\right)$$

Copyrighted material

sont des formes linéaires sur $\mathbb{R}_{2n-1}[X]$, donc puisque $(T_p)_{0\leqslant p\leqslant 2n-1}$ est une base de $\mathbb{R}_{2n-1}[X]$, pour prouver l'identité annoncée, c'est-à-dire $\varphi = \psi$, il suffit de vérifier :

$$\forall p \in [\![0, 2n-1]\!]. \quad \varphi(T_p) = \psi(T_p)$$

Avec le changement de variable défini par $x = \cos t$, $t \in]0, \pi[$, on obtient :

$$\varphi(T_p) = \int_{-1}^{1} \frac{T_p(x)}{\sqrt{1-x^2}}\mathrm{d}x = \int_0^{\pi} T_p(\cos t)\mathrm{d}t = \int_0^{\pi} \cos pt\mathrm{d}t$$

donc $\varphi(T_0) = \pi$ et pour $p \in [\![1, 2n-1]\!]$. $\varphi(T_p) = 0$.

Évaluons $\psi(T_p)$:

$$\frac{n}{\pi}\,\psi\,(T_p) = \sum_{k=1}^{n} \cos\left(p\frac{2k-1}{2n}\pi\right)$$

donc

$$\begin{aligned}\frac{2n}{\pi}\sin\left(\frac{p\pi}{2n}\right)\psi\,(T_p) &= \sum_{k=1}^{n} 2\sin\frac{p\pi}{2n}\cos\left(p\frac{2k-1}{2n}\pi\right)\\ &= \sum_{k=1}^{n}\sin\left(p\frac{k\pi}{n}\right) - \sin\left(p\frac{(k-1)\pi}{n}\right)\\ &= \sin k\pi\\ &= 0\end{aligned}$$

Pour $p \in [\![1, 2n-1]\!]$, on a $\sin\frac{p\pi}{2n} \neq 0$ donc $\psi(T_p) = 0$. Pour $p = 0$, on obtient directement $\frac{n}{\pi}\,\psi\,(T_0) = n$ donc $\psi(T_0) = \pi$. L'identité $\varphi = \psi$ est donc prouvée.

Ex. 15

1) Pour $n \in \mathbb{N}$, $n \geqslant 2$, soit la propriété $\mathcal{P}(n)$: si la réunion d'une famille finie $(F_k)_{k\in[\![1,n]\!]}$ de sous-espaces de E est un sous-espace, alors il existe $(i, j) \in [\![1, n]\!]^2$ tel que $i \neq j$ et $F_i \subset F_j$.

Montrons que $\mathcal{P}(2)$ est vraie.

Soit F_1 et F_2 deux sous-espaces de E tels que $F_1 \cup F_2$ soit un sous-espace.

On a alors $F_1 \cup F_2 = F_1 + F_2$; en effet, $F_1 \cup F_2$ étant un sous-espace de E, on a $\mathrm{Vect}\,(F_1 \cup F_2) = F_1 \cup F_2$.

En supposant $F_1 \not\subset F_2$, il existe $x_1 \in F_1$, $x_1 \notin F_2$ et pour tout $x_2 \in F_2$, le vecteur $x_1 + x_2$ appartient à $F_1 + F_2$ donc à $F_1 \cup F_2$; c'est-à-dire $x_1 + x_2 \in F_1$ ou $x_1 + x_2 \in F_2$.

L'éventualité $x_1 + x_2 = x_2' \in F_2$ est à rejeter puisqu'alors on aurait $x_1 = x_2' - x_2 \in F_2$. Le seul cas possible est donc $x_1 + x_2 = x_1' \in F_1$ ce qui donne $x_2 = x_1' - x_1 \in F_1$.

On a ainsi établi que si $F_1 \not\subset F_2$ alors $F_2 \subset F_1$ et donc $\mathcal{P}(2)$ est vraie.

On suppose maintenant que $\mathcal{P}(n-1)$ est vraie, avec $n \geqslant 3$, et soit $(F_k)_{k\in[\![1,n]\!]}$ une famille de sous-espaces telle que $U_n = \bigcup_{k=1}^{n} F_k$ soit un sous-espace.

On se propose de montrer par l'absurde l'existence de (i, j) tels que $i \neq j$ et $F_i \subset F_j$.

Supposons que $\forall (i, j) \in [\![1, n]\!]^2$, $i \neq j \;\Rightarrow\; F_i \not\subset F_j$.

D'après $\mathcal{P}(n-1)$, la réunion $U_{n-1} = \bigcup_{k=1}^{n-1} F_k$ n'est alors pas un sous-espace vectoriel de E et on a donc :

$$U_{n-1} \subsetneq S = \sum_{k=1}^{n-1} F_k$$

ce qui assure l'existence d'un élément x de S n'appartenant pas à U_{n-1} : $x \in S, x \notin U_{n-1}$.

Envisageons alors deux cas : $x \in F_n$ ou $x \notin F_n$.

- Premier cas : $x \in F_n$

Puisque $F_1 \not\subset F_n$, il existe un élément y tel que $y \in F_1$ et $y \notin F_n$ et on remarque que pour tout $\lambda \in \mathbb{K} \setminus \{0\}$, $z = \lambda x + y \notin F_1 \cup F_n$. En effet, si $z \in F_1$, alors $x = \frac{1}{\lambda}(z - y) \in F_1$ donc $x \in U_{n-1}$, c'est exclu ; et si $z \in F_n$, alors $y = z - \lambda x \in F_n$, c'est exclu.

Copyrighted material

D'autre part, U_n étant un sous-espace vectoriel contenant $F_1 \cup F_n$, il contient x et y et :

$$\text{pour tout } \lambda \in \mathbb{K} \setminus \{0\},\quad z = \lambda x + y \in U_n = \bigcup_{k=1}^{n} F_k$$

et donc, finalement, pour tout $\lambda \in \mathbb{K} \setminus \{0\}$, il existe $i_\lambda \in [\![2, n-1]\!]$ tel que :

$$z = \lambda x + y \in F_{i_\lambda}$$

$[\![2, n-1]\!]$ est fini, alors que $\mathbb{K} \setminus \{0\}$ est infini, donc l'application $\lambda \mapsto i_\lambda$ n'est pas injective, et il existe λ et μ dans $\mathbb{K} \setminus \{0\}$ tels que $\lambda \neq \mu$ et $i_\lambda = i_\mu$. Alors $\lambda x + y$ et $\mu x + y$ sont éléments de F_{i_λ} donc $(\lambda - \mu)x \in F_{i_\lambda}$ ce qui, avec $\lambda - \mu \neq 0$, donne $x \in F_{i_\lambda}$ donc $x \in U_{n-1}$. C'est en contradiction avec le choix de x.

- Deuxième cas : $x \notin F_n$

Alors $x \notin U_n$ (car on sait déjà que $x \notin U_{n-1}$ et $U_n = U_{n-1} \cup F_n$) puis, sachant que $x \in S$, il existe :

$$x_1 \in F_1, x_2 \in F_2, \cdots, x_{n-1} \in F_{n-1} \text{ tels que } x = \sum_{k=1}^{n-1} k.$$

Ceci est en contradiction avec le fait que U_n est un sous-espace vectoriel. (Chacun des x_k est dans U_n mais leur somme x n'est pas dans U_n.)

Dans les deux cas, on a une situation contradictoire. Il existe donc i, j tels que $i \neq j$ et $F_i \subset F_j$.

On a ainsi prouvé que $\mathcal{P}(n-1) \Rightarrow \mathcal{P}(n)$. Il en résulte que $\mathcal{P}(n)$ est vraie pour tout $n \geqslant 2$.

2) La condition annoncée est évidemment suffisante, il reste à prouver qu'elle est nécessaire.

Soit la propriété $\mathcal{Q}(n)$: si la réunion $\bigcup_{k=1}^{n} F_k$ d'une famille de n sous-espaces de E est un sous-espace alors l'un des F_k, $1 \leqslant k \leqslant n$, contient tous les autres. La propriété $\mathcal{Q}(2)$ est vraie ($\mathcal{Q}(2)$ n'est autre que $\mathcal{P}(2)$).

Supposons $\mathcal{Q}(n-1)$ vraie et soit $(F_k)_{k \in [\![1, n]\!]}$ une famille de n sous-espaces telle que $U = \bigcup_{k=1}^{n} F_k$ soit encore un sous-espace de E. Alors d'après le 1), il existe i et j dans $[\![1, n]\!]$ tels que $i \neq j$ et $F_i \subset F_j$. À un réindexation près, on peut supposer $i = n$ et donc $j \leqslant n-1$ et on obtient :

$$U = \bigcup_{k=1}^{n} F_k = \bigcup_{k=1}^{n-1} F_k.$$

Sachant que U est un sous-espace de E, la propriété $\mathcal{Q}(n-1)$ donne que l'un des F_k, $1 \leqslant k \leqslant n-1$ contient tous les autres et donc contient aussi F_n. On a ainsi prouvé la propriété $\mathcal{Q}(n)$.

Finalement, $\mathcal{Q}(n)$ est vraie pour tout $n \geqslant 2$ (par récurrence). Il est clair qu'elle l'est aussi pour $n = 1$, mais c'est sans grand intérêt.

3) Si $\mathbb{K}$ est un corps fini, la réunion d'une famille finie de sous-espaces peut être un sous-espace sans que l'un d'eux contienne tous les autres.

Exemples

$\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$ $\quad E = \mathbb{K}^2 = \{(\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{1})\}$

$$F_1 = \{(\overline{0},\overline{0}), (\overline{1},\overline{0})\} = \text{Vect}\{(\overline{1},\overline{0})\}$$
$$F_2 = \{(\overline{0},\overline{0}), (\overline{0},\overline{1})\} = \text{Vect}\{(\overline{0},\overline{1})\}$$
$$F_3 = \{(\overline{0},\overline{0}), (\overline{1},\overline{1})\} = \text{Vect}\{(\overline{1},\overline{1})\}$$

F_1, F_2, F_3 sont trois sous-espaces de E et $E = F_1 \cup F_2 \cup F_3$. Aucun des F_i ne contient les deux autres ou est inclus dans un autre.

$\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$ $\quad E = \mathbb{K}^2 = \{(\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{0},\overline{1}), (\overline{1},\overline{1}), (\overline{2},\overline{0}), (\overline{0},\overline{2}), (\overline{1},\overline{2}), (\overline{2},\overline{1}), (\overline{2},\overline{2})\}$

$$F_1 = \{(\overline{0},\overline{0}), (\overline{1},\overline{0}), (\overline{2},\overline{0})\} = \text{Vect}\{(\overline{1},\overline{0})\}$$
$$F_2 = \{(\overline{0},\overline{0}), (\overline{0},\overline{1}), (\overline{0},\overline{2})\} = \text{Vect}\{(\overline{0},\overline{1})\}$$
$$F_3 = \{(\overline{0},\overline{0}), (\overline{1},\overline{1}), (\overline{2},\overline{2})\} = \text{Vect}\{(\overline{1},\overline{1})\}$$
$$F_4 = \{(\overline{0},\overline{0}), (\overline{1},\overline{2}), (\overline{2},\overline{1})\} = \text{Vect}\{(\overline{1},\overline{2})\}$$

$E = F_1 \cup F_2 \cup F_3 \cup F_4$.

Copyrighted material

Ex. 16

1) $f^2 = 0$ équivaut à $\operatorname{Im} f \subset \operatorname{Ker} f$, d'où $\operatorname{rg} f \leqslant 3 - \operatorname{rg} f$, puis $f = 0$ ou $\operatorname{rg} f = 1$.

Si $\operatorname{rg} f = 1$, soit u une base de $\operatorname{Im} f$. Pour tout $x \in \mathbb{R}^3$, on a $f(u) = \varphi(x)u$, avec $\varphi(x) \in \mathbb{R}$.

La linéarité de $\varphi : \mathbb{R}^3 \to \mathbb{R}$ est aisée.

2) Avec $\operatorname{rg} f = 1$, il existe $u \in E$ et $\varphi \in E^*$ tels que $\forall x \in E,\ f(x) = \varphi(x)u$.

$f^2(x) = f\big(\varphi(x)u\big) = \varphi(x)f(u) = \varphi(x)\,\varphi(u)u = \varphi(u)f(x)$ donc $f^2 = \varphi(u)f$.

Par récurrence, on obtient $f^n = \big(\varphi(u)\big)^{n-1} f$.

Ex. 17

$E_k(a)$ est un sous-espace vectoriel de $\mathscr{C}^k\big([a_0, a_n], \mathbb{R}\big)$.

Quand $n = 1$, la dimension de $E_k(a)$ est 4 (celle de $\mathbb{R}_3[X]$). Dans la suite on se limite à $n \geqslant 2$.

Posons $a' = \big(a_i\big)_{i \in [\![0, n-1]\!]}$ et on considère l'application linéaire $\Phi_k : E_k(a) \to E_k\big(a'\big)$ qui à $f \in E_k(a)$ associe sa restriction à $\big[a_0, a_{n-1}\big]$. Il est clair que Φ_k est surjective.

Une fonction polynomiale g de degré au plus 3 est caractérisée par les valeurs en a_{n-1} de $g^{(j)}$ pour $0 \leqslant j \leqslant 3$.

$\operatorname{Ker} \Phi_k$ s'identifie à $\big\{P \in \mathbb{R}_3[X],\ P^{(j)}(a_{n-1}) = 0,\ 0 \leqslant j \leqslant k\big\}$, c'est-à-dire au sous-espace de $\mathbb{R}_3[X]$ des polynômes qui ont a_{n-1} pour racine d'ordre au moins $k+1$.

$\operatorname{Ker} \Phi_3 = \{0\}$ et, pour $k < 3$, une base de $\operatorname{Ker} \Phi_k$ est $\Big(\big(X - a_{n-1}\big)^{k+1}, \ldots, \big(X - a_{n-1}\big)^3\Big)$.

Donc $\dim \operatorname{Ker} \Phi_k = 3 - k$.

Si $E_k\big(a'\big)$ est de dimension finie $d_{n-1}^{(k)}$, alors $E_k(a)$ est de dimension finie $d_n^{(k)} = d_{n-1}^{(k)} + 3 - k$ (théorème du rang).

Avec $d_1^{(k)} = 4$, il vient $d_n^{(k)} = (3-k)n + k + 1$.

Ex. 18

1) $q \circ u = \dfrac{1}{n}\displaystyle\sum_{k=1}^{n} u^k \circ p \circ u^{n+1-k} = \frac{1}{n}\sum_{k=0}^{n-1} u^{k+1} \circ p \circ u^{n-k} = u \circ \left(\frac{1}{n}\sum_{k=0}^{n-1} u^k \circ p \circ u^{n-k}\right)$.

Avec $u^0 \circ p \circ u^{n-0} = p \circ u^n = p = u^n \circ p \circ u^{n-0}$, $q \circ u = u \circ \left(\dfrac{1}{n}\displaystyle\sum_{k=1}^{n} u^k \circ p \circ u^{n-k}\right) = u \circ q$.

$\operatorname{Im}\big(p \circ u^{n-k}\big) \subset \operatorname{Im} p = V$ puis par stabilité $\operatorname{Im}\big(u^k \circ p \circ u^{n-k}\big) \subset V$, donc $\operatorname{Im} q \subset V$. Il s'ensuit $p \circ q = q$.

$$q \circ q = \frac{1}{n}\sum_{k=1}^{n} u^k \circ p \circ u^{n-k} \circ q = \frac{1}{n}\sum_{k=1}^{n} u^k \circ p \circ q \circ u^{n-k} = \frac{1}{n}\sum_{k=1}^{n} u^k \circ q \circ u^{n-k} = \frac{1}{n}\sum_{k=1}^{n} u^k \circ u^{n-k} \circ q = q.$$

2) Pour $y \in V$, on a $u^{n-k}(y) \in V$ donc $p \circ u^{n-k}(y) = u^{n-k}(y)$ donc $u^k \circ p \circ u^{n-k}(y) = u^n(y) = y$ puis $q(y) = y$.

Il s'ensuit $\forall x \in E,\ q\big(p(x)\big) = p(x)$ puis $q \circ p = p$.

3) $\big(\mathrm{Id}_E - p\big) \circ q = 0$ donne $\operatorname{Inv} q = \operatorname{Im} q \subset \operatorname{Ker}\big(\mathrm{Id}_E - p\big) = \operatorname{Inv} p = V$.

De même, $q \circ p = p$ donne $V \subset \operatorname{Inv} q$.

$\operatorname{Ker} q$ est alors un supplémentaire de V.

Enfin, $u \circ q = q \circ u$ assure que $\operatorname{Ker} q$ est stable par u.

Ex. 19

1) Si r est racine commune à P et Q, alors $P = (X - r)P_1$ et $Q = (X - r)Q_1$ donne $-Q_1P + P_1Q = 0$.

Avec $UP = -VQ$, P divise VQ. Si P et Q n'ont pas de racine commune, alors $P \wedge Q = 1$ puis P divise V.

La condition $\deg V \leqslant n - 1$ implique alors $V = 0$, ce qui est contraire à l'hypothèse.

2) La base canonique $\mathfrak{B}$ de $\big(\mathbb{C}_2[X]\big)^2$ est formée de $e_1 = (1, 0)$, $e_2 = (X, 0)$, $e_3 = (0, 1)$, $e_4 = (0, X)$.

On a $\varphi(e_1) = A$, $\varphi(e_2) = XA$, $\varphi(e_3) = B$ et $\varphi(e_4) = XB$.

Copyrighted material

Avec $A = aX^2 + bX + c$ et $B = dX^2 + eX + f$ et $\mathcal{B}'$ base canonique de $\mathbb{C}_3[X]$, la matrice de φ est :

$$\begin{pmatrix} c & 0 & f & 0 \\ b & c & e & f \\ a & b & d & e \\ 0 & a & 0 & d \end{pmatrix}.$$

3) A et B ont une racine commune si et seulement si le noyau de φ n'est pas nul, c'est-à-dire :

$$\begin{vmatrix} c & 0 & f & 0 \\ b & c & e & f \\ a & b & d & e \\ 0 & a & 0 & d \end{vmatrix} = 0.$$

Cette condition s'exprime par :

$$\begin{vmatrix} a & c \\ d & f \end{vmatrix}^2 = \begin{vmatrix} a & b \\ d & e \end{vmatrix} \times \begin{vmatrix} b & c \\ e & f \end{vmatrix}.$$

Copyrighted material

CHAPITRE 4

Calcul matriciel Systèmes linéaires

Copyrighted material

A. Matrices semblables Matrices équivalentes – Rang

1. Changement de base

Dans tout ce chapitre $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

1.1 – Matrice de passage ✎(1)

✎(1) Algèbre et Géométrie, MPSI, chapitre 13. Il s'agit ici d'un bref formulaire.

Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geqslant 1$.

$\mathfrak{B} = (e_i)_{1 \leqslant i \leqslant n}$ et $\mathfrak{B}' = (e'_i)_{1 \leqslant i \leqslant n}$ deux bases de E.

La **matrice de passage** de la base $\mathfrak{B}$ à la base $\mathfrak{B}'$, dans cet ordre, est la matrice du système $(e'_1, \ldots, e'_n)$ sur la base $\mathfrak{B}$, on la note $P_{\mathfrak{B},\mathfrak{B}'}$:

$$P_{\mathfrak{B},\mathfrak{B}'} = \mathrm{mat}_{\mathfrak{B}}(e'_1, \ldots, e'_n) \quad \text{ou} \quad P_{\mathfrak{B},\mathfrak{B}'} = \mathrm{mat}_{\mathfrak{B}}\,\mathfrak{B}' \text{ en notation abrégée.}$$

- La matrice $P_{\mathfrak{B},\mathfrak{B}'}$ est aussi la matrice, sur le couple de bases $(\mathfrak{B}', \mathfrak{B})$, de l'identité de E :

$$P_{\mathfrak{B},\mathfrak{B}'} = \mathrm{mat}_{\mathfrak{B}',\mathfrak{B}}(\mathrm{Id}_E).$$

- Toute matrice de passage est inversible :

$$P_{\mathfrak{B},\mathfrak{B}'} \in \mathrm{GL}_n(\mathbb{K}) \quad , \quad P_{\mathfrak{B},\mathfrak{B}'}^{-1} = P_{\mathfrak{B}',\mathfrak{B}}.$$

- Produit de deux matrices de passage :

$$P_{\mathfrak{B},\mathfrak{B}'} P_{\mathfrak{B}',\mathfrak{B}''} = P_{\mathfrak{B},\mathfrak{B}''}.$$

1.2 – Formules de changement de bases

- **Formule de changement de bases pour un vecteur**

Soit $x \in E$,

– dans la base $\mathfrak{B} = (e_i)_{1 \leqslant i \leqslant n}$, $x = \sum_{i=1}^{n} x_i e_i$, $X = \underset{\mathfrak{B}}{\mathrm{mat}}(x) = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

– dans la base $\mathfrak{B}' = (e'_i)_{1 \leqslant i \leqslant n}$, $x = \sum_{i=1}^{n} x'_i e'_i$, $X' = \underset{\mathfrak{B}'}{\mathrm{mat}}(x) = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$

– alors $\boxed{X = P_{\mathfrak{B},\mathfrak{B}'} X'}$ ✎(2)

✎(2) On obtient les anciennes coordonnées en fonction des nouvelles, alors que la matrice de passage donne les nouveaux vecteurs en fonction des anciens.

- **Formule de changement de bases pour une application linéaire**

Soit :

– E et F deux $\mathbb{K}$-espaces vectoriels de dimensions non nulles p et n,

– deux bases de E, $\mathcal{U}$ et $\mathcal{U}'$, et leur matrice de passage $P = P_{\mathcal{U},\mathcal{U}'} \in \mathrm{GL}_p(\mathbb{K})$,

– deux bases de F, $\mathcal{V}$ et $\mathcal{V}'$, et leur matrice passage $Q = P_{\mathcal{V},\mathcal{V}'} \in \mathrm{GL}_n(\mathbb{K})$,

– une application linéaire $f \in \mathscr{L}(E, F)$ et ses matrices associées :

$$M = \mathrm{mat}_{\mathcal{U},\mathcal{V}}(f) \quad , \quad M' = \mathrm{mat}_{\mathcal{U}',\mathcal{V}'}(f)$$

Alors $\boxed{M' = Q^{-1} M P}$

- **Formule de changement de bases pour un endomorphisme**

Soit E un $\mathbb{K}$-espace vectoriel de dimension non nulle n rapporté à deux bases $\mathfrak{B}$ et $\mathfrak{B}'$, $P = P_{\mathfrak{B},\mathfrak{B}'}$ la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$, un endomorphisme $f \in \mathscr{L}(E)$ et ses matrices associées :

$$A = \mathrm{mat}_{\mathfrak{B}}(f) \quad , \quad A' = \mathrm{mat}_{\mathfrak{B}'}(f)$$

Alors $\boxed{A' = P^{-1} A P}$

Copyrighted material

2. Matrices semblables

Définition 1

Des matrices carrées A et B de $\mathcal{M}_n(\mathbb{K})$ sont dites **semblables** [3] s'il existe une matrice inversible $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

[3] On définit ainsi une relation binaire dans $\mathrm{GL}_n(\mathbb{K})$, appelée similitude.

Propriété 1

Des matrices A et B de $\mathcal{M}_n(\mathbb{K})$ sont semblables si et seulement si, étant donné E, $\mathbb{K}$-espace vectoriel de dimension n rapporté à une base $\mathcal{B}$ et $f \in \mathcal{L}(E)$ tel que $A = \mathrm{mat}_{\mathcal{B}}(f)$, il existe $\mathcal{B}'$ base de E telle que $B = \mathrm{mat}_{\mathcal{B}'}(f)$. [4]

[4] C'est la formule de changement de base pour un endomorphisme.

Propriété 2

La similitude de matrices est une relation d'équivalence dans $\mathcal{M}_n(\mathbb{K})$.

☞ Réflexivité : $A = I_n^{-1}AI_n$ pour tout $A \in \mathcal{M}_n(\mathbb{K})$.

Symétrie : pour A et B dans $\mathcal{M}_n(\mathbb{K})$ et $P \in \mathrm{GL}_n(\mathbb{K})$, $B = P^{-1}AP \Rightarrow A = (P^{-1})^{-1}BP^{-1}$.

Transitivité : étant donné A, B, C dans $\mathcal{M}_n(\mathbb{K})$, P et Q dans $\mathrm{GL}_n(\mathbb{K})$,

$B = P^{-1}AP$ et $C = Q^{-1}BQ$ implique $C = Q^{-1}P^{-1}APQ$ donc $C = (PQ)^{-1}A(PQ)$. [5]

[5] $(PQ)^{-1} = Q^{-1}P^{-1}$.

Propriété 3

Des matrices semblables ont le même déterminant.

☞ Soit A et B dans $\mathcal{M}_n(\mathbb{K})$.

Si elles sont semblables, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

Alors, $\det B = \det P^{-1} \det A \det P$ [6] et $\det P^{-1} = \left(\det P\right)^{-1}$.

Il vient donc $\det B = \det A$. [7]

[6] Algèbre et Géométrie, MPSI, chapitre 14.

[7] On peut aussi remarquer que $A = \mathrm{mat}_{\mathcal{B}}(f)$ et $B = \mathrm{mat}_{\mathcal{B}'}(f)$ donne $\det A = \det f = \det B$.

Exemple 1 Si A et B sont semblables, alors il en est de même pour $B - \lambda I_n$ et $A - \lambda I_n$.

Soit A et B dans $\mathcal{M}_n(\mathbb{K})$ et $\lambda \in \mathbb{K}$.

Si A et B sont semblables, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

Alors $B - \lambda I_n = P^{-1}AP - \lambda I_n = P^{-1}AP - \lambda P^{-1}I_nP = P^{-1}\left(A - \lambda I_n\right)P$.

En particulier, il vient $\det\left(B - \lambda I_n\right) = \det\left(A - \lambda I_n\right)$.

Propriété 4

Soit A et B semblables dans $\mathcal{M}_n(\mathbb{K})$.

a) Pour tout $n \in \mathbb{N}^*$, A^n et B^n sont semblables.

b) Si de plus A et B sont dans $\mathrm{GL}_n(\mathbb{K})$, alors, pour tout $n \in \mathbb{Z}$, A^n et B^n sont semblables.

☞ Soit $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

a) Si, pour $n \in \mathbb{N}^*$, on a $B^n = P^{-1}A^nP$, alors $B^{n+1} = \left(P^{-1}A^nP\right)\left(P^{-1}AP\right) = P^{-1}A^{n+1}P$.

Ce qui montre la propriété. [8]

b) Si A et B sont inversibles, de $B = P^{-1}AP$ on déduit $B^{-1} = P^{-1}A^{-1}P$ donc B^{-1} et A^{-1} sont semblables. Pour tout $n \in \mathbb{N}$, on a donc B^{-n} et A^{-n} semblables [9] d'après le a).

[8] Autre méthode : $A = \mathrm{mat}_{\mathcal{B}}(f)$ et $B = \mathrm{mat}_{\mathcal{B}'}(f)$ donne $A^n = \mathrm{mat}_{\mathcal{B}}(f^n)$ et $B^n = \mathrm{mat}_{\mathcal{B}'}(f^n)$.

[9] $B^0 = I_n$ et $A^0 = I_n$ sont évidemment semblables.

Copyrighted material

Corollaire

Étant donné A et B semblables dans $\mathcal{M}_n(\mathbb{K})$, pour tout polynôme $Q \in \mathbb{K}[X]$, $Q = a_0 + \sum_{k=1}^{p} a_k X^k$, les matrices $Q(A) = a_0 I_n + \sum_{k=1}^{p} a_k A^k$ et $Q(B) = a_0 I_n + \sum_{k=1}^{p} a_k B^k$ sont semblables.

☞ Avec $B^k = P^{-1}A^kP$, il vient $Q(B) = P^{-1}\left(a_0 I_n + \sum_{k=1}^{p} a_k A^k\right)P = P^{-1}Q(A)P$.

3. Matrices équivalentes, rang

3.1 – Matrices équivalentes

Définition 2

Des matrices A et B de $\mathcal{M}_{n,p}(\mathbb{K})$ sont dites **équivalentes** s'il existe des matrices inversibles $P \in \mathrm{GL}_p(\mathbb{K})$ et $Q \in \mathrm{GL}_n(\mathbb{K})$ telles que $B = QAP$. (10)

(10) On définit ainsi une relation binaire sur $\mathcal{M}_{n,p}$ appelée l'équivalence de matrices.

Propriété 5

Les matrices A et B de $\mathcal{M}_{n,p}(\mathbb{K})$ sont équivalentes si et seulement si, étant donné E et F des $\mathbb{K}$-espaces vectoriels de dimensions p et n rapportés à des bases respectives $\mathcal{U}$ et $\mathcal{V}$ et $f \in \mathcal{L}(E, F)$ telle que $A = \mathrm{mat}_{\mathcal{U},\mathcal{V}}(f)$, il existe $\mathcal{U}'$ et $\mathcal{V}'$ bases de E et F telles que :

$$B = \mathrm{mat}_{\mathcal{U}',\mathcal{V}'}(f).$$ (11)

(11) C'est une conséquence aisée de la formule de changement de bases pour une application linéaire rappelée au début de ce chapitre.

Propriété 6

L'équivalence est une relation d'équivalence dans $\mathcal{M}_{n,p}(\mathbb{K})$. (12)

(12) Il y a un télescopage fâcheux où le mot «équivalence» a deux rôles différents... mais qui se rejoignent.

☞ Réflexivité : pour tout $A \in \mathcal{M}_{n,p}(\mathbb{K})$, $A = I_n A I_p$.

Symétrie : $B = QAP \Rightarrow A = Q^{-1}BP^{-1}$.

Transitivité : $B = QAP$ et $C = SBR$, avec Q et S dans $\mathrm{GL}_n(\mathbb{K})$, P et R dans $\mathrm{GL}_p(\mathbb{K})$, implique $C = (SQ)A(PR)$, avec $SQ \in \mathrm{GL}_n(\mathbb{K})$ et $PR \in \mathrm{GL}_n(\mathbb{K})$.

3.2 – Rang d'une matrice (13)

(13) Voir Algèbre et Géométrie, MPSI, chapitre 13.

Définition 3

Le **rang d'une matrice** est le rang du système de ses vecteurs-colonnes. On le note $\mathrm{rg}\, M$.

Propriété 7

Rang d'une application linéaire et d'une matrice associée

Soit E et F deux $\mathbb{K}$-espaces vectoriels de dimensions non nulles p et n, $\mathcal{U} = (u_j)_{j \in [\![1,p]\!]}$, $\mathcal{V} = (v_i)_{i \in [\![1,n]\!]}$ des bases de E et F, une application linéaire $f \in \mathcal{L}(E, F)$ et $M = \mathrm{mat}_{\mathcal{U},\mathcal{V}}(f)$.

On a alors : $\mathrm{rg}\, f = \mathrm{rg}\, M$. (14)

(14) En particulier, une matrice a le même rang que l'application linéaire de $\mathbb{K}^p$ dans $\mathbb{K}^n$ qui lui est canoniquement associée.

☞ Le rang de f est la dimension du sous-espace de F engendré par $\{f(u_1), \ldots, f(u_p)\}$.

Ces vecteurs ne sont autres que les images des vecteurs colonnes de M dans l'isomorphisme ϕ de $\mathbb{K}^n$ sur F dont l'image de la base canonique $(e_i)_{1 \leqslant i \leqslant n}$ est $\mathcal{V}$. (15)

(15) $\forall i \in [\![1,n]\!]$, $\phi(e_i) = v_i$.

Corollaire

Si A et B sont équivalentes dans $\mathcal{M}_{n,p}(\mathbb{K})$, alors elles ont le même rang. (16)

(16) Car elles sont associées à une même application linéaire.

Copyrighted material

Propriété 8

Si f est une application linéaire de matrice $M \in \mathcal{M}_{n,p}(\mathbb{K})$, alors :

$$\operatorname{rg} M = n \iff f \text{ surjective} \quad , \quad \operatorname{rg} M = p \iff f \text{ injective.}$$

Corollaire

Si $M \in \mathcal{M}_n(\mathbb{K})$, alors $\operatorname{rg} M = n \iff M \in \mathrm{GL}_n(\mathbb{K})$.

Propriété 9

Rang d'un produit matriciel

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,q}(\mathbb{K})$.

a) $\operatorname{rg}(AB) \leqslant \sup\{\operatorname{rg} A, \operatorname{rg} B\}$,

b) Si $A \in \mathrm{GL}_p(\mathbb{K})$: $\operatorname{rg}(AB) = \operatorname{rg} B$. Si $B \in \mathrm{GL}_p(\mathbb{K})$: $\operatorname{rg}(AB) = \operatorname{rg} A$.

3.3 – Matrice canonique d'une application linéaire

La matrice canonique d'une application linéaire a été vue au chapitre 3, au théorème 13.

Propriété 10

Une matrice $M \in \mathcal{M}_{n,p}(\mathbb{K})$ est de rang r si et seulement si elle est équivalente à : [17]

$$J_r = \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}.$$

[17] À M, on associe $f \in \mathcal{L}(\mathbb{K}^p, \mathbb{K}^n)$ et on forme la matrice canonique de f.

Théorème 1

Égalité des rangs d'une matrice et de sa transposée

$$\operatorname{rg} M = \operatorname{rg} {}^t M.$$

☞ $M \in \mathcal{M}_{n,p}(\mathbb{K})$ étant équivalente à $J_r = \begin{pmatrix} I_r & 0_{r,p-r} \\ 0_{n-r,r} & 0_{n-r,p-r} \end{pmatrix}$, ${}^t M \in \mathcal{M}_{n,p}(\mathbb{K})$ est équivalente à ${}^t J_r = J'_r = \begin{pmatrix} I_r & 0_{r,n-r} \\ 0_{p-r,r} & 0_{p-r,n-r} \end{pmatrix}$. [18]

Donc la propriété 10 donne $\operatorname{rg} M = r = \operatorname{rg} {}^t M$.

[18] $M = PJ_rQ$ donne ${}^t M = {}^t Q\, {}^t J_r\, {}^t P$ avec P et ${}^t P$ dans $\mathrm{GL}_n(\mathbb{K})$, Q et ${}^t Q$ dans $\mathrm{GL}_p(\mathbb{K})$.

Corollaire

Soit $M \in \mathcal{M}_{n,p}(\mathbb{K})$, $(c_1, \ldots, c_p)$ ses vecteurs-colonnes, $(\ell_1, \ldots, \ell_n)$ ses vecteurs-lignes.

Alors $\operatorname{rg} M = \operatorname{rg}(c_1, \ldots, c_p) = \operatorname{rg}(\ell_1, \ldots, \ell_n) \leqslant \inf(p, n)$.

Théorème 2

Caractérisation de l'équivalence des matrices

Des matrices M et M' de $\mathcal{M}_{n,p}(\mathbb{K})$ sont équivalentes si et seulement si elles ont même rang.

☞ Si elles sont équivalentes, la condition nécessaire a été vue. [19]

Si elles ont le même rang r, elles sont équivalentes à J_r donc équivalentes entre elles par transitivité de cette relation.

[19] Corollaire de la propriété 7.

Copyrighted material

B. Opérations élémentaires

1. Méthodes

1.1 – Permutations de lignes ou colonnes d'une matrice

Étant donné $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$, on note $P_\sigma(n) \in \mathrm{GL}_n(\mathbb{K})$ la matrice de la permutation σ.

$$P_\sigma(n) = \left[\delta_{i\sigma(j)}\right]$$ (20)

(20) Si E est un $\mathbb{K}$-espace vectoriel de dimension n muni d'une base $\mathcal{B}=(e_i)_{1\leqslant i\leqslant n}$, $P_\sigma(n)$ est la matrice dans cette base de l'automorphisme f_σ défini par :
$\forall i \in [\![1,n]\!]$, $f_\sigma(e_i)=e_{\sigma(i)}$.

Propriété 11

Soit $A \in \mathcal{M}_{n,p}(\mathbb{K})$.

a) $AP_\sigma(p)$ se déduit de A par la permutation $\sigma \in \mathfrak{S}_p$ sur les colonnes de A.

b) ${}^tP_\sigma(n)A$ se déduit de A par la permutation $\sigma \in \mathfrak{S}_p$ sur les lignes de A.

1.2 – Opérations élémentaires

Définition 4

On appelle opérations élémentaires sur une matrice $A \in \mathcal{M}_{n,p}(\mathbb{K})$:

a) la transposition de deux lignes ou de deux colonnes de A ;

b) l'addition à une ligne r d'une autre ligne s (donc $s \neq r$) multipliée par $\lambda \in \mathbb{K}$,
ou l'addition à une colonne r d'une autre colonne s (donc $s \neq r$) multipliée par $\lambda \in \mathbb{K}$;

c) le produit par $\lambda \in \mathbb{K}^*$ d'une ligne ou d'une colonne r. (21)

(21) $L_1, \ldots, L_n$ désignant les lignes de A et $C_1, \ldots, C_p$ ses colonnes, ces transformations peuvent être symbolisées par :
$L_r \rightleftarrows L_s$, $C_r \rightleftarrows C_s$
$L_r \leftarrow L_r + \lambda L_s$,
$C_r \leftarrow C_r + \lambda C_s$
$L_r \leftarrow \lambda L_r$, $C_r \leftarrow \lambda C_r$.

Propriété 12

Les opérations élémentaires peuvent être réalisées en effectuant le produit de A par une matrice carrée inversible. (22)

(22) Les matrices carrées inversibles détaillées ci-dessous sont dites matrices de transformations élémentaires.

a) Soit $P_{rs} \in \mathrm{GL}_n(\mathbb{K})$ la matrice de la transposition $\tau = (r, s)$ qui échange r et s.

$$P_{rs} = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & 1 & & & \\ & & & & 1 & & & & \\ & & & 1 & & 0 & & & \\ & & & & & & 1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ r \\ \\ s \\ \\ \\ \end{matrix}$$

$P_{rs}A$ est la matrice qui se déduit de A en échangeant les lignes r et s. (23)

(23) $P_{rs}=I_n-E_{rr}-E_{ss}+E_{rs}+E_{sr}$ où $(E_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}}$ est la base canonique de $\mathcal{M}_n(\mathbb{K})$.

b) Soit $r \neq s$. Alors $\left(I_n + \lambda E_{rs}\right)A$ est la matrice qui se déduit de A en ajoutant à la ligne r le produit par λ de la ligne s.

c) $\left(I_n + (\lambda - 1)E_{rr}\right)A$ est la matrice qui se déduit de A en multipliant la ligne r par λ.

d) En procédant de même avec les matrices carrées d'ordre p : P'_{rs} matrice de la transposition $\tau'_{rs} \in \mathfrak{S}_p$ échangeant r et s,

$$I_p + \lambda E'_{sr} \quad \text{et} \quad I_p + (\lambda - 1)E'_{rr} \quad \lambda \neq 0$$

on obtient les opérations élémentaires sur les colonnes de A avec :

$$AP'_{rs} \quad \text{ou} \quad A\left(I_p + \lambda E'_{sr}\right) \quad \text{ou} \quad A\left(I_p + (\lambda - 1)E'_{rr}\right).$$

Copyrighted material

2. Calcul du rang

Propriété 13

Toute opération élémentaire transforme une matrice A en une matrice de même rang que A.

Propriété 14

Étant donné $A \in \mathcal{M}_{n,p}(\mathbb{K})$ les propositions suivantes sont équivalentes :

(1) $\operatorname{rg}(A) = r$,

(2) il existe $T_1, \dots, T_q$ dans $\mathrm{GL}_n(\mathbb{K})$, $T'_1, \dots, T'_s$ dans $\mathrm{GL}_p(\mathbb{K})$, matrices de transformations élémentaires telles que : $T_q T_{q-1}, \dots, T_1 A T'_1, \dots, T'_s = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$.

Avec les notations précédentes, en posant $P = T_q T_{q-1} \cdots T_1 I_n$ et $Q = I_p T'_1 \cdots T'_s$, on a :

$$PAQ = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}.$$

P (resp. Q) s'obtient en effectuant à partir de I_n (resp. de I_p) la même suite de transformations élémentaires que celle qui a été faite sur les lignes (resp. les colonnes) à partir de A.

Exemple 2 Soit $A = \begin{pmatrix} 1 & 2 & -1 & -4 & 1 \\ -1 & -1 & 1 & 2 & 0 \\ 2 & -2 & 3 & 9 & -9 \\ 3 & 5 & -1 & -8 & 0 \end{pmatrix} \in \mathcal{M}_{5,4}(\mathbb{R})$.

Calculer le rang r de A et trouver $P \in \mathrm{GL}_4(\mathbb{R})$, $Q \in \mathrm{GL}_5(\mathbb{R})$ telles que :

$$PAQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Commençons par des transformations élémentaires sur les colonnes. [24]

[24] Une bonne calculatrice ou un logiciel tel que Maple facilitera grandement le travail.

Premières opérations :

$C_2 \longleftarrow C_2 - 2C_1$, $C_3 \longleftarrow C_3 + C_1$, $C_4 \longleftarrow C_4 + 4C_1$, $C_5 \longleftarrow C_5 - C_1$

$$A \longrightarrow A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & -2 & 1 \\ 2 & -6 & 5 & 17 & -11 \\ 3 & -1 & 2 & 4 & -3 \end{pmatrix} \quad , \quad I_5 \longrightarrow Q_1 = \begin{pmatrix} 1 & -2 & 1 & 4 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ensuite, $C_1 \longleftarrow C_1 + C_2$, $C_4 \longleftarrow C_4 + 2C_2$, $C_5 \longleftarrow C_5 - C_2$

$$A_1 \longrightarrow A_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ -4 & -6 & 5 & 5 & -5 \\ 2 & -1 & 2 & 2 & -2 \end{pmatrix} \quad , \quad Q_1 \longrightarrow Q_2 = \begin{pmatrix} -1 & -2 & 1 & 0 & 1 \\ 1 & 1 & 0 & 2 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Effectuons ensuite $C_4 \longleftarrow C_4 - C_3$, $C_5 \longleftarrow C_5 + C_3$, $C_3 \longleftarrow \frac{1}{5} C_3$,

et $C_1 \longleftarrow C_1 + 4C_3$, $C_2 \longleftarrow C_2 + 6C_3$

$$A_2 \longrightarrow A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \frac{18}{5} & \frac{7}{5} & \frac{2}{5} & 0 & 0 \end{pmatrix} \quad , \quad Q_2 \longrightarrow Q = \begin{pmatrix} -\frac{1}{5} & -\frac{4}{5} & \frac{1}{5} & -1 & 2 \\ 1 & 1 & 0 & 2 & -1 \\ \frac{4}{5} & \frac{6}{5} & \frac{1}{5} & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Puis opérons ensuite sur les lignes.

$L_4 \longleftarrow L_4 - \frac{18}{5} L_1$, $L_4 \longleftarrow L_4 - \frac{7}{5} L_2$, $L_4 \longleftarrow L_4 - \frac{2}{5} L_3$

$$A_3 \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad , \quad I_4 \longrightarrow P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\frac{18}{5} & -\frac{7}{5} & -\frac{2}{5} & 1 \end{pmatrix}$$

Copyrighted material

D'où les matrices P et Q et le rang : $r = 3$.

Remarque

Pour le calcul du rang, on peut se contenter de transformer, par une suite d'opérations élémentaires, A en :

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ \times & 1 & 0 & 0 & 0 \\ \times & \times & 1 & 0 & 0 \\ \times & \times & \times & 0 & 0 \end{pmatrix} \quad \text{ou} \quad A'' = \begin{pmatrix} 1 & \times & \times & \times & \times \\ 0 & 1 & \times & \times & \times \\ 0 & 0 & 1 & \times & \times \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

3. Calcul de l'inverse éventuelle d'une matrice carrée

Soit $A \in \mathcal{M}_n(\mathbb{K})$, les propositions suivantes sont équivalentes :

(1) A est inversible,

(2) il existe $T_1, \ldots, T_q \in \mathrm{GL}_n(\mathbb{K})$ matrices de transformations élémentaires telles que :
$$AT_1, \ldots, T_q = I_n,$$

(3) il existe $T'_1, \ldots, T'_s \in \mathrm{GL}_n(\mathbb{K})$ matrices de transformations élémentaires telles que :
$$T'_s, \ldots, T'_1 A = I_n.$$

Pratiquement,

- si on opère sur les colonnes :

  $A^{-1} = I_n T_1, \ldots, T_q$ se déduit de I_n par la suite des transformations élémentaires sur les colonnes qui font passer de A à I_n,

- si on opère sur les lignes :

  $A^{-1} = T'_s, \ldots, T'_1 I_n$ se déduit de I_n par la suite de transformations élémentaires sur les lignes qui font passer de A à I_n.

Exemple 3 Soit $A = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 3 & 2 & 3 \\ -1 & 0 & 1 & -1 \\ -2 & -1 & 4 & 0 \end{pmatrix}$. Vérifier que A est inversible et calculer A^{-1}.

Opérons sur les colonnes :

$C_2 \longleftarrow C_2 - 2C_1$. $C_3 \longleftarrow C_3 - C_1$. $C_4 \longleftarrow C_4 - C_1$

$$A \longrightarrow A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & 0 & 1 \\ -1 & 2 & 2 & 0 \\ -2 & 3 & 6 & 2 \end{pmatrix} \quad , \quad I_4 \longrightarrow B_1 = \begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$C_2 \longleftarrow -C_2$. $C_1 \longleftarrow C_1 - 2C_2$. $C_4 \longleftarrow C_4 - C_2$

$$A_1 \longrightarrow A_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 3 & -2 & 2 & 2 \\ 4 & -3 & 6 & 5 \end{pmatrix} \quad , \quad B_1 \longrightarrow B_2 = \begin{pmatrix} -3 & 2 & -1 & -3 \\ 2 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$C_3 \longleftarrow C_3 \times \frac{1}{2}$. $C_1 \longleftarrow C_1 - 3C_3$. $C_2 \longleftarrow C_2 + 2C_3$. $C_4 \longleftarrow C_4 - 2C_3$

$$A_2 \longrightarrow A_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -5 & 3 & 3 & -1 \end{pmatrix} \quad , \quad B_2 \longrightarrow B_3 = \begin{pmatrix} -\frac{3}{2} & 1 & -\frac{1}{2} & -2 \\ 2 & -1 & 0 & 1 \\ -\frac{3}{2} & 1 & \frac{1}{2} & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$C_4 \longleftarrow C_4 \times (-1)$. $C_1 \longleftarrow C_1 + 5C_4$. $C_2 \longleftarrow C_2 - 3C_4$. $C_3 \longleftarrow C_3 - 3C_4$

$$A_3 \longrightarrow I_4 \quad , \quad B_3 \longrightarrow A^{-1} = \begin{pmatrix} \frac{17}{2} & -5 & -\frac{13}{2} & 2 \\ -3 & 2 & 3 & -1 \\ \frac{7}{2} & -2 & -\frac{5}{2} & 1 \\ -5 & 3 & 3 & -1 \end{pmatrix}$$

Copyrighted material

C. Trace d'une matrice carrée, d'un endomorphisme

1. Trace d'une matrice carrée

Définition 5

On appelle **trace d'une matrice carrée** $M = [m_{ij}] \in \mathcal{M}_n(\mathbb{K})$, le scalaire, noté $\mathrm{Tr}(M)$, somme des éléments diagonaux de M : $\mathrm{Tr}(M) = \sum_{i=1}^{n} m_{ii}$.

Théorème 3

a) L'application $\mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$, $M \mapsto \mathrm{Tr}(M)$ est une forme linéaire non nulle.

b) Pour tout $A \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B \in \mathcal{M}_{p,n}(\mathbb{K})$, on a : $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

☞ a) La linéarité de l'application «trace» de $\mathcal{M}_n(\mathbb{K})$ dans $\mathbb{K}$ est immédiate.

b) Considérons $A = [a_{ij}] \in \mathcal{M}_{n,p}(\mathbb{K})$ et $B = [b_{ij}] \in \mathcal{M}_{p,n}(\mathbb{K})$.

Notons que les matrices produits $AB \in \mathcal{M}_n(\mathbb{K})$ et $BA \in \mathcal{M}_p(\mathbb{K})$ ne sont a priori pas de même ordre. Soit $C = AB \in \mathcal{M}_n(\mathbb{K})$.

Son terme général est $c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj}$ et on a $\mathrm{Tr}(AB) = \sum_{i=1}^{n} \sum_{k=1}^{p} a_{ik} b_{ki}$ et de même :

$$\mathrm{Tr}(BA) = \sum_{k=1}^{p} \sum_{i=1}^{n} b_{ki} a_{ik}.$$

On voit alors que $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

Remarque

Avec dans $\mathcal{M}_2(\mathbb{K})$: $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, on a :

$$ABC = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{et} \quad BAC = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

D'où : $\mathrm{Tr}(ABC) \neq \mathrm{Tr}(BAC)$.

En revanche, le théorème ci-dessus permet de dire que $\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB) = \mathrm{Tr}(BCA)$.

Propriété 15

Le noyau de la trace est un hyperplan de $\mathcal{M}_n(\mathbb{K})$ dont un supplémentaire est le sous-espace des matrices scalaires : $\mathcal{M}_n(\mathbb{K}) = \mathrm{Ker}(\mathrm{Tr}) \oplus \mathbb{K} I_n$.

Il suffit de remarquer que la forme linéaire Tr n'est pas la forme nulle et que $\mathrm{Tr}(I_n) = n$.

Exemple 4 Soit φ une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$ telle que : $\forall (X, Y) \in \mathcal{M}_n(\mathbb{K})^2$, $\varphi(XY) = \varphi(YX)$.

Montrer qu'il existe $\alpha \in \mathbb{K}$ tel que $\varphi = \alpha\,\mathrm{Tr}$.

Le choix de $X = E_{ij}$, $Y = E_{kl}$ donne : $XY = \delta_{jk} E_{il}$, $YX = \delta_{li} E_{kj}$. D'où :

$$\delta_{jk}\, \varphi(E_{il}) = \delta_{li}\, \varphi(E_{kj}).$$

- Pour $j = k$ et $i \neq l$, on a $\varphi(E_{il}) = 0$.
- Pour $j = k$ et $i = l$, on a $\varphi(E_{ii}) = \varphi(E_{jj})$.

Il existe donc $\alpha \in \mathbb{K}$ tel que $\forall i \in [\![1, n]\!]$, $\alpha = \varphi(E_{ii})$; ainsi $\varphi = \alpha\,\mathrm{Tr}$.

Propriété 16

Des matrices carrées semblables ont la même trace.

☞ Soit A et B dans $\mathcal{M}_n(\mathbb{K})$. Leur similitude s'exprime par l'existence de $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $B = P^{-1}AP$.

On a donc $\mathrm{Tr}(B) = \mathrm{Tr}(P^{-1}AP)$. Or $\mathrm{Tr}(P^{-1}AP) = \mathrm{Tr}(PP^{-1}A) = \mathrm{Tr}(A)$.

Copyrighted material

2. Trace d'un endomorphisme

Définition 6

Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geqslant 1$ et $f \in \mathcal{L}(E)$.
Le scalaire $\mathrm{Tr}\left(\mathrm{mat}_{\mathcal{B}}(f)\right)$ ne dépend pas de la base $\mathcal{B}$.
Il est appelé «trace de $f$fg et noté $\mathrm{Tr}(f)$.

Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux bases de E, les matrices $\mathrm{mat}_{\mathcal{B}}(f)$ et $\mathrm{mat}_{\mathcal{B}'}(f)$ sont semblables et ont donc la même trace.

Propriété 17

L'application «trace» $\mathcal{L}(E) \to \mathbb{K}, f \mapsto \mathrm{Tr}(f)$ est une forme linéaire non nulle.

Propriété 18

Quels que soient les endomorphismes f et g de E :

$$\mathrm{Tr}(f \circ g) = \mathrm{Tr}(g \circ f).$$

Propriété 19

Si $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ est une base de E et $\mathcal{B}^* = (e_i^*)_{1 \leqslant i \leqslant n}$ la base duale :

$$\mathrm{Tr}(f) = \sum_{i=1}^{n} e_i^*\left(f(e_i)\right).$$

Exemple 5 Soit $A \in \mathcal{M}_n(\mathbb{K})$ et f_A l'endomorphisme de $\mathcal{M}_n(\mathbb{K})$ défini par : $f_A : M \mapsto AM$.
Calculer $\mathrm{Tr}(f)$ en fonction de $\mathrm{Tr}(A)$.

Soit $\left(E_{ij}\right)_{(i,j) \in [\![1,n]\!]^2}$ la base de $\mathcal{M}_n(\mathbb{K})$ formée par les matrices élémentaires [25] et $\left(E_{ij}^*\right)_{(i,j) \in [\![1,n]\!]^2}$ sa base duale.

[25] C'est-à-dire la base canonique de $\mathcal{M}_n(\mathbb{K})$.

Pour $M = \left[m_{ij}\right]$ on a $f_A(M) = \left[m'_{ij}\right]$ avec $E_{ij}^*\left(f_A(M)\right) = m'_{ij} = \sum_{k=1}^{n} a_{ik} m_{kj}$, donc :

$$E_{ij}^*\left(f_A(E_{ij})\right) = \sum_{k=1}^{n} a_{ik}\delta_{kl} = a_{ii}.$$

On en déduit :

$$\mathrm{Tr}\left(f_A\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} E_{ij}^*\left(f_A(E_{ij})\right) = n\sum_{i=1}^{n} a_{ii} = n\,\mathrm{Tr}(A).$$

Théorème 4

Pour tout projecteur p d'un $\mathbb{K}$-espace vectoriel E de dimension finie, on a $\mathrm{rg}\, p = \mathrm{Tr}\, p$.

☞ Puisque p est un projecteur, on a $\mathrm{Inv}\, p \oplus \mathrm{Ker}\, p = E$.
On considère une base $\mathcal{B} = (e_1, \ldots, e_r, e_{r+1}, \ldots, e_n)$ de E telle que $(e_1, \ldots, e_r)$ soit une base de $\mathrm{Inv}\, p$ et $(e_{r+1}, \ldots, e_n)$ une base de $\mathrm{Ker}\, p$. [26]

[26] $\mathcal{B}$ est une base adaptée à la somme directe $E = \mathrm{Inv}\, p \oplus \mathrm{Ker}\, p$.

La matrice de p dans $\mathcal{B}$ est $B = \begin{pmatrix} I_r & (0) \\ (0) & (0) \end{pmatrix}$, d'où $\mathrm{rg}\, B = r = \mathrm{Tr}\, B$.

Exemple 6 Exemple d'endomorphisme f tel que $\mathrm{Tr}\, f = \mathrm{rg}\, f$, bien que f ne soit pas un projecteur.

L'endomorphisme de $\mathbb{K}^2$ dont la matrice dans la base canonique est $A = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ n'est pas idempotent car $A^2 = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$. Cependant, on a $\mathrm{Tr}\, A = 2 = \mathrm{rg}\, A$.

Copyrighted material

D. Systèmes d'équations linéaires

1. Notion d'équation linéaire

Soit E et F des $\mathbb{K}$-espaces vectoriels. [27]

[27] Les notions rappelées ci-après ont été introduites en Algèbre et Géométrie, MPSI, chapitre 14.

Définition 7

Étant donné $f \in \mathscr{L}(E,F)$ et $b \in F$, l'équation :

$(L) : x \in E, f(x) = b$ est appelée l'**équation linéaire** associée à (f, b).

$(H) : x \in E, f(x) = 0_F$ est l'**équation homogène** associée à (L).

Notation 1

On note $S(L) = \{x \in E \ / \ f(x) = b\}$ l'ensemble des solutions de (L)

et $S(H) = \{x \in E \ / \ f(x) = 0_F\}$ l'ensemble des solutions de (H).

Remarque

$S(H)$ est le noyau de f. C'est donc un sous-espace vectoriel de E.

Il contient en particulier 0_E qui est appelé la **solution banale** (ou triviale) de (H).

Définition 8

L'équation (L) est dite **possible** lorsque l'ensemble $S(L)$ n'est pas vide.

Remarque

L'équation (L) est possible si et seulement si b appartient à l'image de f.

Propriété 20

L'ensemble $S(L)$ des solutions de (L) est un sous-espace affine de E.

Si x_0 est une solution de (L), on a $S(L) = x_0 + S(H)$.

☞ Si (L) est possible, considérons $x_0 \in S(L)$. Il vient alors :

$$f(x) = b \iff f(x) = f(x_0) \iff f(x - x_0) = 0_F \iff x - x_0 \in S(H)$$

c'est-à-dire $x \in S(L) \iff x \in x_0 + S(H)$.

Propriété 21

Soit $f \in \mathscr{L}(E,F)$, $(b_1, b_2) \in F^2$, $(\lambda_1, \lambda_2) \in \mathbb{K}^2$ et les équations linéaires

$(L_1) : x \in E, f(x) = b_1$, $(L_2) : x \in E, f(x) = b_2$, $(L) : x \in E, f(x) = \lambda_1 b_1 + \lambda_2 b_2$.

Si (L_1) et (L_2) sont possibles, alors (L) est possible et $S(L) = \lambda_1 S(L_1) + \lambda_2 S(L_2)$.

☞ Soit $x_1 \in S(L_1)$ et $x_2 \in S(L_2) : f(x_1) = b_1$ et $f(x_2) = b_2$.

On a donc $f(\lambda_1 x_1 + \lambda_2 x_2) = \lambda_1 b_1 + \lambda_2 b_2$ et (L) est possible, de solution particulière :

$$\lambda_1 x_1 + \lambda_2 x_2 .$$

Il s'ensuit $S(L) = \lambda_1 x_1 + \lambda_2 x_2 + S(H)$. Or $S(H) = \lambda_1 S(H) + \lambda_2 S(H)$ d'où :

$$S(L) = \lambda_1 (x_1 + S(H)) + \lambda_2 (x_2 + S(H)) = \lambda_1 S(L_1) + \lambda_2 S(L_2).$$

Copyrighted material

2. Système d'équations linéaires

2.1 – Notations

- $E = \mathbb{K}^p$, $F = \mathbb{K}^n$ avec n et p dans $\mathbb{N}^*$.
- $\mathcal{B} = (e_1, \dots, e_p)$ et $\mathcal{B}' = (\varepsilon_1, \dots, \varepsilon_n)$ les bases canoniques de E et F.
- $A = [a_{ij}] \in \mathcal{M}_{n,p}(\mathbb{K})$, $B = [b_i] \in \mathcal{M}_{n,1}(\mathbb{K})$ et $r = \operatorname{rg} A$.
- $(c_1, \dots, c_p)$ la famille des vecteurs-colonnes de A et $b \in F$ le vecteur-colonne de B.
- $(\theta_1, \dots, \theta_n)$ la famille des formes linéaires sur E telle que pour tout $i \in [\![1, n]\!]$:

$$\theta_i = \sum_{j=1}^{p} a_{ij} e_j^* \text{ .}$$ (28)

(28) $(e_1^*, \dots, e_p^*)$ est la base duale de la base $\mathcal{B}$ de E. Chaque θ_i correspond à la ligne i de A.

- $f \in \mathcal{L}(E, F)$ canoniquement associée à A : $A = \operatorname{mat}_{\mathcal{B},\mathcal{B}'}(f)$.
- (L) l'équation linéaire associée à (f, b) et (H) l'équation homogène associée.

2.2 – Interprétations des équations *(L) et (H)*

Fonctionnelle :	$f(x) = b$	$f(x) = 0_F$	$x \in E$
Matricielle :	$AX = B$	$AX = 0$	$X \in \mathcal{M}_{n\,1}(\mathbb{K})$
Vectorielle :	$\sum_{j=1}^{p} x_j c_j = b$	$\sum_{j=1}^{p} x_j c_j = 0_F$	$(x_1, \dots, x_p) \in \mathbb{K}^p$
Analytique :	$\begin{cases} a_{1\,1}x_1 + \dots + a_{1\,p}x_p = b_1 \\ a_{2\,1}x_1 + \dots + a_{2\,p}x_p = b_2 \\ \dots\dots\dots\dots\dots \\ a_{n\,1}x_1 + \dots + a_{n\,p}x_p = b_n \end{cases}$	$\begin{cases} a_{1\,1}x_1 + \dots + a_{1\,p}x_p = 0 \\ a_{2\,1}x_1 + \dots + a_{2\,p}x_p = 0 \\ \dots\dots\dots\dots\dots \\ a_{n\,1}x_1 + \dots + a_{n\,p}x_p = 0 \end{cases}$	$(x_1, \dots, x_p) \in \mathbb{K}^p$
Duale :	$\begin{cases} \theta_1(x) = b_1 \\ \theta_2(x) = b_2 \\ \dots\dots\dots \\ \theta_n(x) = b_n \end{cases}$	$\begin{cases} \theta_1(x) = 0 \\ \theta_2(x) = 0 \\ \dots\dots\dots \\ \theta_n(x) = 0 \end{cases}$	

3. Système de Cramer

Définition 9

Avec les notations précédentes, on dit que (L) est un **système de Cramer** lorsque l'une des conditions (équivalentes) suivantes est réalisée :

(1) $n = p = r$ (2) $A \in \mathrm{GL}_n(\mathbb{K})$ (3) f est un isomorphisme.

Remarques

1) Un système de Cramer admet une solution unique $x = f^{-1}(b)$.

2) Un système de Cramer homogène admet la solution banale pour solution unique.

Théorème 5

Formules de Cramer

Avec les notations ci-dessus, la solution d'un système de Cramer est :

$$\forall j \in [\![1, n]\!],\ x_j = \frac{\det A_j(b)}{\det A}.$$

où $A_j(b)$ est la matrice obtenue à partir de A en remplaçant le vecteur-colonne c_j par b.

Copyrighted material

☞ La solution $x = (x_1, \dots, x_n)$ est caractérisée par $b = \sum_{k=1}^{n} x_k c_k$. On a donc :

$$\det A_j(b) = \det_{\mathcal{B}}\left(c_1, \dots, c_{j-1}, b, c_{j+1}, \dots, c_n\right)$$

d'où $\det A_j(b) = \sum_{k=1}^{n} x_k \det_{\mathcal{B}}\left(c_1, \dots, c_{j-1}, c_k, c_{j+1}, \dots, c_n\right)$, c'est-à-dire :

$$\det A_j(b) = x_j \det_{\mathcal{B}}\left(c_1, \dots, c_{j-1}, c_j, c_{j+1}, \dots, c_n\right) = x_j \det A.$$

Application au calcul de l'inverse d'une matrice

La solution d'un système de Cramer $AX = B$ (en écriture matricielle) est $X = A^{-1}B$.

Les expressions des x_i à l'aide des b_j donnent alors la matrice A^{-1}.

Pour $n \geqslant 3$, il est souvent pratique de déterminer l'inverse d'une matrice par le biais de la résolution d'un système linéaire.

Exemple 7 Calculer l'inverse de la matrice $A = \begin{pmatrix} 1 & 2 & 1 & & & \\ & 1 & 2 & 1 & & (0) \\ & & \ddots & \ddots & \ddots & \\ & & & \ddots & \ddots & 1 \\ (0) & & & & 1 & 2 \\ & & & & & 1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R}), \quad n \geqslant 3.$

$\det A = 1$ donc A est inversible. À la matrice A, on associe le système de Cramer :

$$(S) : \begin{cases} x_1 + 2x_2 + x_3 = y_1 & E_1 \\ x_2 + 2x_3 + x_4 = y_2 & E_2 \\ \dots \quad \dots \quad = \dots & \\ x_{n-2} + 2x_{n-1} + x_n = y_{n-2} & E_{n-2} \\ x_{n-1} + 2x_n = y_{n-1} & E_{n-1} \\ x_n = y_n & E_n \end{cases}$$

Pour $i \in [\![1, n-1]\!]$, effectuons sur les équations la combinaison linéaire symbolisée par :

$E_i \longleftarrow \sum_{k=i}^{n} (-1)^{k+i} E_k$. Il vient : $\begin{cases} x_i + x_{i+1} = \sum_{k=i}^{n} (-1)^{k+i} y_k & 1 \leqslant i \leqslant n-1 \\ x_n = y_n \end{cases}$

$$\begin{cases} x_1 + x_2 = y_1 - y_2 + y_3 + \dots + (-1)^{n+1} y_n & E'_1 \\ -x_2 - x_3 = -y_2 + y_3 + \dots + (-1)^{n+1} y_n & E'_2 \\ x_3 + x_4 = y_3 + \dots + (-1)^{n+1} y_n & E'_3 \\ \dots \quad \dots \quad \dots & \\ (-1)^n (x_{n-1} + x_n) = (-1)^n y_{n-1} + (-1)^{n+1} y_n & E'_{n-1} \\ (-1)^{n+1} x_n = (-1)^{n+1} y_n & E'_n \end{cases}$$

D'où en effectuant les combinaisons linéaires $E_i \longleftarrow \sum_{k=i}^{n} E'_k$:

$$\begin{cases} x_1 = y_1 - 2y_2 + 3y_3 + \dots + (-1)^{n+1} n y_n \\ x_2 = y_2 - 2y_3 + (-1)^n (n-1) y_n \\ \dots \quad \dots \quad \dots \quad \dots \\ x_{n-1} = y_{n-1} - 2y_n \\ x_n = y_n \end{cases}$$

Copyrighted material

Il en résulte :

$$A^{-1} = \begin{pmatrix} 1 & -2 & 3 & -4 & \dots & (-1)^n(n-1) & (-1)^{n+1}n \\ 0 & 1 & -2 & 3 & \dots & (-1)^{n-1}(n-2) & (-1)^n(n-1) \\ 0 & 0 & 1 & -2 & \dots & & (-1)^{n-1}(n-2) \\ \vdots & & & \ddots & & & \vdots \\ \vdots & & (0) & & \ddots & & \vdots \\ \vdots & & & & & 1 & -2 \\ 0 & & & & & 0 & 1 \end{pmatrix}$$

4. Système linéaire : cas général

Considérons, avec les notations du paragraphe **B**, le système linéaire défini par :

$$f(x) = b \quad \text{ou} \quad AX = B$$

$S(H)$ est un sous-espace de dimension $p - r$ de $\mathbb{K}^p$ où $r = \text{rg}(f) = \text{rg}(A)$.

Si le système (L) est possible, $S(L)$ est un sous-espace affine de direction $S(H)$.

La méthode du pivot de Gauss

Les colonnes de A forment un système de rang r. À une permutation près des inconnues $x_1, \dots, x_p$ on peut donc se ramener au cas d'un système : $AX = B$ **(1)** dans lequel les r premières colonnes de A forment un système libre. On sait alors qu'il existe une suite d'opérations élémentaires sur les lignes qui transforme A en une matrice T de la forme :

$$T = \begin{pmatrix} 1 & \times & \dots & & \dots & \dots & \times \\ 0 & 1 & & & & & \\ \vdots & & \ddots & & & & \\ \vdots & & & 1 & \times & \dots & \times \\ \vdots & & & 0 & \dots & \dots & 0 \\ \vdots & & & \vdots & \dots & \dots & \vdots \\ 0 & & & 0 & \dots & \dots & 0 \end{pmatrix}$$

Matriciellement, cela donne l'existence de $P \in \text{GL}_p(\mathbb{K})$, produit de matrices de transformations élémentaires, telle que : $T = PA$, et P étant inversible, on a :

$$AX = B \iff PAX = PB$$

C'est-à-dire que le système **(1)** a les mêmes solutions que : $TX = PB$ **(2)**.

On dit que les **systèmes (1)** et **(2)** sont **équivalents**.

Il y a lieu de remarquer que la transformation de **(1)** en **(2)** s'obtient en effectuant sur les équations de **(1)** la suite d'opérations élémentaires qui fait passer de A à T. Dans la pratique on pourra, de façon à se dispenser d'écrire les inconnues lors de ces manipulations, effectuer la suite d'opérations en question sur la matrice $A_1 = \left[A\ B\right]$, formée par les deux blocs A et B.

Au niveau de **(2)**, la discussion est facile. Ce système s'écrit :

$$\textbf{(2)} \quad \begin{cases} x_1 + \alpha_{12}x_2 + \dots + \alpha_{1p}x_p = \beta_1 \\ \quad x_2 + \dots + \alpha_{2p}x_p = \beta_2 \\ \quad \ddots \\ \quad x_r + \dots + \alpha_{rp}x_p = \beta_r \\ \quad 0 = \beta_{r+1} \\ \quad \dots \quad \dots \\ \quad 0 = \beta_n \end{cases}$$

- il est possible si et seulement si $\beta_{r+1} = \beta_{r+2} = \dots = \beta_n = 0$;
- si cette condition est réalisée, les r premières équations donnent, en cascade et de manière unique, $x_1, \dots, x_r$ en fonction de $x_{r+1}, \dots, x_p$.

Copyrighted material

Exemple 8 Résoudre dans $\mathbb{C}^4$ le système (S) $\begin{cases} x+y+z+at &= 1 & E_1 \\ x+y+az+t &= b & E_2 \\ x+ay+z+t &= b^2 & E_3 \\ ax+y+z+t &= b^3 & E_4 \end{cases}$

a et b sont des complexes donnés.

Formons le déterminant du système :

$$\begin{vmatrix} 1 & 1 & 1 & a \\ 1 & 1 & a & 1 \\ 1 & a & 1 & 1 \\ a & 1 & 1 & 1 \end{vmatrix} = (a+3)(a-1)^3$$

Donc, pour $a \notin \{1, -3\}$, on a affaire à un système de Cramer. On résoud alors en évitant soigneusement les formules de Cramer.

Pour cela, on remarque en formant $\sum_{i=1}^{4} E_i$ que la solution (x, y, z, t) vérifie :

$$x+y+z+t = \frac{1+b+b^2+b^3}{a+3} \qquad E_5$$

Par combinaisons linéaires de E_5 et E_i, $i = 1, 2, 3, 4$, on obtient :

$$x = \frac{(a+2)b^3 - 1 - b - b^2}{(a-1)(a+3)} \quad , \quad y = \frac{(a+2)b^2 - 1 - b - b^3}{(a-1)(a+3)}$$

$$z = \frac{(a+2)b - 1 - b^2 - b^3}{(a-1)(a+3)} \quad , \quad t = \frac{(a+2) - b - b^2 - b^3}{(a-1)(a+3)}$$

Dans le cas $a = 1$, il est clair que le système est possible si et seulement si $b = 1$ et alors il est équivalent à $x+y+z+t = 1$.

Dans le cas $a = -3$, le système est équivalent à :

$$\begin{cases} x+y+z-3t = 1 & E_1 \\ x+y-3z+t = b & E_2 \\ x-3y+z+t = b^2 & E_3 \\ 0 = 1+b+b^2+b^3 & E_4' \longleftarrow \sum_{i=1}^{4} E_i \end{cases}$$

Avec $1+b+b^2+b^3 = (1+b^2)(1+b)$ on voit que :

- pour $b \notin \{-1, i, -i\}$, (S) est impossible,
- pour $b \in \{-1, i, -i\}$, (S) équivaut à (S') :

$$(S') \begin{cases} x+y+z-3t = 1 \\ x+y-3z+t = b \\ x-3y+z+t = b^2 \end{cases}$$

soit encore

$$\begin{cases} x = t + \dfrac{1-b^3}{4} \\ y = t + \dfrac{1-b^2}{4} \\ z = t + \dfrac{1-b}{4} \end{cases}$$

Copyrighted material

Méthodes

L'essentiel

I. Matrices semblables et trace

✔ La trace est une forme linéaire non nulle.

✔ Propriété fondamentale : $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

✔ **Si l'on veut** utiliser que deux matrices sont semblables,

- **on peut** écrire l'égalité de leurs traces ;

  → Voir *Mise en œuvre*, exercices 1, 2, 3, 4

- **on peut** lire $B = P^{-1}AP$ sous la forme $PB = AP$.

  → Voir *Mise en œuvre*, exercice 3

✔ **Si l'on veut** étudier un problème en termes de matrices,

- **on peut** l'exprimer en termes d'endomorphismes ;

  → Voir *Mise en œuvre*, exercices 2, 5, 6, 8

- **on peut** dégager des informations venant du déterminant.

  → Voir *Mise en œuvre*, exercices 3, 4, 8

II. Trace et projecteurs

✔ Propriété fondamentale d'un projecteur : $\mathrm{Tr}\, p = \mathrm{rg}\, p$.

✔ **Si l'on veut** Montrer qu'une matrice est idempotente,

- **on peut** construire une matrice idempotente qui lui est semblable.

  → Voir *Mise en œuvre*, exercice 5

✔ **Si l'on veut** Montrer qu'une somme de matrices idempotentes est idempotente,

- **on peut** mettre en évidence des sous-espaces en somme directe.

  → Voir *Mise en œuvre*, exercice 6

III. Commutateur de deux matrices

✔ **Si l'on veut** calculer la trace d'un carré de matrice $AB - BA$,

- **on peut** mettre en œuvre la symétrie ou l'antisymétrie.

  → Voir *Mise en œuvre*, exercice 7

✔ **Si l'on veut** montrer qu'un commutateur $AB - BA$ est nilpotent,

- **on peut** étudier l'endomorphisme $M \mapsto MB - BM$.

  → Voir *Mise en œuvre*, exercice 8

Copyrighted material

Mise en œuvre

I. Matrices semblables et trace.

Ex. 1

Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, on pose $S(A) = \sum_{(i,j)\in[\![1,n]\!]^2} a_{ij}a_{ji}$.

Montrer que si A et B sont semblables, alors $S(A) = S(B)$.

Indications

La trace et le déterminant sont les mêmes pour deux matrices semblables. On tente alors d'exprimer $S(A)$ à l'aide de $\mathrm{Tr}\,A$ ou de $\det(A)$.

Solution

On a $S(A) = \sum_{i\in[\![1,n]\!]} \left(\sum_{j\in[\![1,n]\!]} a_{ij}a_{ji} \right)$.

Or $\sum_{j\in[\![1,n]\!]} a_{ij}a_{ji}$ n'est autre que le terme d'indice (i,i) de la matrice A^2.

Il s'ensuit que $S(A) = \mathrm{Tr}\left(A^2\right)$.

Les matrices semblables A^2 et B^2 ont la même trace.
L'égalité $\mathrm{Tr}\left(A^2\right) = \mathrm{Tr}\left(B^2\right)$ donne enfin $S(A) = S(B)$.

Commentaires

On décompose la somme sur $(i,j)\in[\![1,n]\!]^2$.

Si des matrices A et B sont semblables, il en est de même pour A^2 et B^2.

Ex. 2

1) Montrer que si $A \in \mathcal{M}_n(\mathbb{K})$ est de trace nulle, alors elle est semblable à une matrice de diagonale nulle.
2) Étant donné une matrice diagonale $D = \mathrm{diag}\left(d_1, \cdots, d_n\right) \in \mathcal{M}_n(\mathbb{K})$ à termes diagonaux deux à deux distincts, étudier le noyau et l'image de $\varphi \in \mathcal{L}(\mathcal{M}_n(\mathbb{K}))$ défini par $\forall M \in \mathcal{M}_n(\mathbb{K})$, $\varphi(M) = DM - MD$.
3) Soit $A \in \mathcal{M}_n(\mathbb{K})$. Montrer que $\mathrm{Tr}\,A = 0$ si et seulement si il existe R et S dans $\mathcal{M}_n(\mathbb{K})$ telles que :

$$A = RS - SR.$$

Indications

Pour la première question, on traduit en terme d'endomorphisme f de $\mathbb{K}^n$ canoniquement associé à A.
On procède par récurrence sur n. L'image de φ est l'ensemble des matrices à termes diagonaux tous nuls.

Solution

1) Soit $\mathcal{B}_0$ la base canonique de $E = \mathbb{K}^n$, on pose $A = \mathrm{mat}_{\mathcal{B}_0} f$.
Le résultat est banal pour $A = 0$ et pour $n = 1$.
Supposons $A \neq 0$, $n \geqslant 2$ et le résultat acquis pour $n-1$.
Premier cas : pour tout $x \in E$, $\left(x, f(x)\right)$ est lié. Alors f est une homothétie.
Avec $f = k\,\mathrm{Id}_E$, $\mathrm{Tr}\,f = 0$ donne $k = 0$, donc $f = 0$.
Second cas : il existe $a \in E$ tel que $\left(a, f(a)\right)$ soit libre. On complète en une base $\mathcal{B} = \left(a, f(a), e_3, \ldots, e_n\right)$.

Commentaires

Voir Algèbre et Géométrie, MPSI, chapitre 12, *Mise en œuvre*, Exercice 1.

Copyrighted mat

Dans une telle base, la matrice de f est de la forme

$$B = \begin{pmatrix} 0 & b_{12} & \cdots & b_{1n} \\ 1 & & & \\ 0 & & B' & \\ \vdots & & & \\ 0 & & & \end{pmatrix}.$$

$\operatorname{Tr} A = 0$ donne $\operatorname{Tr} B' = 0$, donc il existe $Q \in \mathrm{GL}_{n-1}(\mathbb{K})$ telle que $Q^{-1}B'Q$ soit de diagonale nulle.

B est semblable à A.
$B' \in \mathcal{M}_{n-1}(\mathbb{K})$, $\operatorname{Tr} B' = \operatorname{Tr} B = \operatorname{Tr} A$.
Hypothèse de récurrence.

Avec $P = \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix} \in \mathrm{GL}_n(\mathbb{K})$, on a $P^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & Q^{-1} \end{pmatrix}$ et $C = P^{-1}BP = \begin{pmatrix} 0 & L \\ M & Q^{-1}B'Q \end{pmatrix}$ est de trace nulle.

Et A est semblable à C.

En conséquence, la propriété est vraie pour tout $n \geqslant 1$.

Par récurrence sur n.

2) Avec $M = [m_{ij}]$, $\phi(M)$ est la matrice $[(d_i - d_j)m_{ij}]$.

M est dans le noyau de φ si et seulement si elle est diagonale. Et le sous-espace des matrices diagonales est de dimension n.

$\forall (i,j),\ i \neq j$ et $(d_i - d_j)m_{ij} = 0$ implique $m_{ij} = 0$.

Les éléments de l'image ont tous leurs termes diagonaux nuls, et l'ensemble des matrices de diagonale nulle est un sous-espace $\mathcal{M}'$ de dimension $n^2 - n$, comme $\operatorname{Im}\phi$. Donc $\operatorname{Im}\phi = \mathcal{M}'$.

Théorème du rang.

3) Si $A = RS - SR$, alors évidemment $\operatorname{Tr} A = 0$.

Si A est de trace nulle, elle est semblable à un élément A' de $\mathcal{M}'$.

Première question.

Et il existe $C \in \mathcal{M}_n(\mathbb{K})$ telle que $A' = DC - CD$.

Deuxième question.

Avec $T \in \mathrm{GL}_n(\mathbb{K})$ telle que $A = TA'T^{-1}$, il vient :
$A = TDCT^{-1} - TCDT^{-1} = (TDT^{-1})(TCT^{-1}) - (TCT^{-1})(TDT^{-1})$.

On a terminé, avec $R = TDT^{-1}$ et $S = TCT^{-1}$.

Ex. 3

Soit A et B dans $\mathcal{M}_n(\mathbb{R})$. On suppose qu'il existe $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $B = P^{-1}AP$.
Montrer qu'il existe $R \in \mathrm{GL}_n(\mathbb{R})$ telle que $B = R^{-1}AR$.
En d'autres termes : si deux matrices réelles sont semblables dans $\mathcal{M}_n(\mathbb{C})$, elle le sont dans $\mathcal{M}_n(\mathbb{R})$.

Indications

La similitude donnée s'écrit $PB = AP$. Séparer P en $P = U + iV$ avec U et V dans $\mathcal{M}_n(\mathbb{R})$.
Pour $x \in \mathbb{C}$ et U, V dans $\mathcal{M}_n(\mathbb{R})$, $x \mapsto \det(U + xV)$ est une fonction polynôme.

Solution

Avec $P = U + iV$, U et V dans $\mathcal{M}_n(\mathbb{R})$, $PB = AP$ se lit $UB + iVB = UA + iVA$.
Cela équivaut à $UB = AU$ et $VB = AV$.

A et B sont réelles, comme U et V.

Pour tout $x \in \mathbb{C}$, on a donc $(U + xV)B = A(U + xV)$.

$(U+xV)B = UB + xVB = AU + xAV = A(U+xV)$.

La fonction polynôme $f : \mathbb{C} \to \mathbb{C}$, $x \mapsto \det(U + xV)$ vérifie $f(i) \neq 0$.

$f(i) = \det(U + iV) = \det P \neq 0$.

Il existe alors $t \in \mathbb{R}$ tel que $\det(U + tV) \neq 0$, donc $U + tV$ inversible.

Si f s'annule en tout x réel, alors f est le polynôme nul, comme admettant une infinité de racines.

Alors, en posant $R = U + tV \in \mathrm{GL}_n(\mathbb{R})$, il vient $RB = AR$ donc $B = R^{-1}AR$.

Copyrighted material

Ex. 4

Soit $P \in \mathrm{GL}_n(\mathbb{C})$ et φ_P l'endomorphisme de $\mathcal{M}_n(\mathbb{C})$ défini par $\varphi_P(M) = P^{-1}MP$.
Calculer la trace et le déterminant de φ_P

Indications

Former la matrice de φ_P dans la base canonique de $\mathcal{M}_n(\mathbb{C})$. Classiquement les matrices élémentaires sont notées E_{ij} avec $(i,j) \in [\![1, n]\!]^2$. On exprime les produits $PE_{ij}P^{-1}$ à l'aide des termes de P et de P^{-1}.

La trace de φ_P s'exprimera à l'aide de $\mathrm{Tr}\, P$ et $\mathrm{Tr}\, P^{-1}$.

Solution

Posons $P = \left(p_{ij}\right)_{(i,j)\in[\![1,n]\!]^2}$ et $P^{-1} = Q = \left(q_{ij}\right)_{(i,j)\in[\![1,n]\!]^2}$.

1) Alors $QE_{kl} = \displaystyle\sum_{i,j} q_{ij}E_{ij}E_{kl} = \sum_{i} q_{ik}E_{il}$.

puis $QE_{kl}P = \displaystyle\sum_{i} q_{ik} \sum_{j} p_{lj}E_{ij}$, soit : $\varphi_P(E_{kl}) = \displaystyle\sum_{i,j} q_{ik}p_{lj}E_{ij}$.

La matrice de φ_P dans la base canonique de $\mathcal{M}_n(\mathbb{C})$ est alors :

$$A = \begin{pmatrix} q_{11}\,{}^tP & q_{12}\,{}^tP & \cdots & q_{1n}\,{}^tP \\ q_{21}\,{}^tP & q_{22}\,{}^tP & \cdots & q_{2n}\,{}^tP \\ \vdots & \vdots & & \vdots \\ q_{n1}\,{}^tP & q_{n2}\,{}^tP & \cdots & q_{nn}\,{}^tP \end{pmatrix} \in \mathcal{M}_{n^2}(\mathbb{C}).$$

On en déduit $\mathrm{Tr}\,\phi_P = \mathrm{Tr}\,P\,\mathrm{Tr}\,P^{-1}$.

2) Remarquons que $A = BC$, avec B et C dans $\mathcal{M}_{n^2}(\mathbb{C})$:

$$B = \begin{pmatrix} q_{11}I_n & q_{12}I_n & \cdots & q_{1n}I_n \\ q_{21}I_n & q_{22}I_n & \cdots & q_{2n}I_n \\ \vdots & \vdots & & \vdots \\ q_{n1}I_n & q_{n2}I_n & \cdots & q_{nn}I_n \end{pmatrix}, C = \begin{pmatrix} {}^tP & (0) & \cdots & (0) \\ (0) & {}^tP & \ddots & \vdots \\ \vdots & \ddots & \ddots & (0) \\ (0) & \cdots & (0) & {}^tP \end{pmatrix}.$$

$\det A = \det B \det C$, et $\det C = (\det P)^n$.

La méthode du pivot de Gauss permet de transformer P^{-1} en une matrice triangulaire $T = \begin{pmatrix} d_{11} & \cdots & d_{1n} \\ & \ddots & \vdots \\ & & d_{nn} \end{pmatrix}$ telle que $\det P^{-1} = \displaystyle\prod_k d_{kk}$.

En effectuant la même transformation sur les blocs de la matrice B, on obtient :

$$\det B = \begin{vmatrix} d_{11}I_n & \cdots & d_{n1}I_n \\ & \ddots & \vdots \\ & & d_{nn}I_n \end{vmatrix}.$$

Il s'ensuit $\det B = \displaystyle\prod_{k=1}^{n} d_{kk}^n = \left(\det P^{-1}\right)^n$.

En conclusion, il vient $\det A = 1$.

Commentaires

$E_{ij}E_{kl} = \delta_{jk}E_{il}$. Pour simplifier on écrit $\sum_i$ au lieu de $\sum_{i=n}^{n}$, $\sum_{i,j}$ au lieu de $\sum_{i=1}^{n}\sum_{j=1}^{n}$.

$\sum_{r,j} p_{ij}E_{il}E_{rj} = \sum_{j} p_{ij}E_{lj}$.

A est donnée par blocs.

La base canonique de $\mathcal{M}_n(\mathbb{C})$ est ordonnée dans l'ordre lexicographique des indices (i,j).

$\mathrm{Tr}\,\varphi_P = \sum_k q_{kk}\,\mathrm{Tr}\,P$.

Produit par blocs.

C est triangulaire par blocs et $\det {}^tP = \det P$.

$\det(d_{kk}I_n) = d_{kk}^n$.

II. Trace et projecteurs

Ex. 5

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Montrer que, si $\operatorname{rg} A = 1$ et $\operatorname{Tr} A = 1$, alors $A^2 = A$.

Indications

Considérer l'endormorphisme p de $\mathbb{K}^n$ canoniquement associé à A.
La trace et le rang d'un projecteur sont égaux. C'est une réciproque qui est étudiée.

Solution

Le rang de A étant 1, on a $\dim \operatorname{Ker} p = n-1$. On complète une base $(e_1, \ldots, e_{n-1})$ de $\operatorname{Ker} p$ en une base $\mathcal{B} = (e_1, \ldots, e_{n-1}, e_n)$ de $\mathbb{K}^n$.

Alors A est semblable à $B = \begin{pmatrix} 0 & \cdots & 0 & \lambda_1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$.

$\operatorname{Tr} A = 1$ implique $\operatorname{Tr} B = 1$, donc $\lambda_n = 1$ et on obtient aisément $B^2 = B$.

Il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $A = PBP^{-1}$ et il s'ensuit $A^2 = A$.

Commentaires

Exploitation de $\operatorname{rg} A = 1$.

B matrice de p dans la base $\mathcal{B}$.

Exploitation de la seconde hypothèse.

Ex. 6

Soit $(A_k)_{k \in [\![1,s]\!]}$ une famille de s éléments de $\mathcal{M}_n(\mathbb{K})$ telle que $\forall k \in [\![1,s]\!]$, $A_k^2 = A_k$ et on pose $A = \sum_{k=1}^{s} A_k$.

Montrer que $\forall (i,j) \in [\![1,s]\!]^2$, $i \neq j \Rightarrow A_i A_j = 0$ équivaut à $A^2 = A$.

Indications

Utiliser $U^2 = U \Rightarrow \operatorname{rg} U = \operatorname{Tr} U$.
Avec $p_k \in \mathcal{L}(\mathbb{K}^n)$ canoniquement associé à A_k, montrer que la somme des $\operatorname{Im} p_k$ est directe.

Solution

1) On a $A^2 = \sum_{k=1}^{s} A_k^2 + \sum_{i \neq j} A_i A_j$.

Avec $\forall (i,j) \in [\![1,s]\!]^2$, $i \neq j \Rightarrow A_i A_j = 0$, il vient $A^2 = A$.

2) Soit $p_k \in \mathcal{L}(\mathbb{K}^n)$ dont la matrice est A_k dans la base canonique de $\mathbb{K}^n$, et $p = \sum_{k=1}^{s} p_k$. Avec $A = \sum_{k=1}^{s} A_k$ il vient $\operatorname{rg} A \leqslant \sum_{k=1}^{s} \operatorname{rg} A_k$.

Par ailleurs, on a $\sum_{k=1}^{s} \operatorname{rg} A_k = \sum_{k=1}^{s} \operatorname{Tr} A_k = \operatorname{Tr} A$. Alors :

$\operatorname{rg} A \leqslant \sum_{k=1}^{s} \operatorname{rg} A_k = \operatorname{Tr} A$, donc $\operatorname{rg} A = \sum_{k=1}^{s} \operatorname{rg} A_k$ car $\operatorname{rg} A = \operatorname{Tr} A$.

$\dim \operatorname{Im}\left(\sum_{k=1}^{s} p_k\right) = \sum_{k=1}^{s} \dim(\operatorname{Im} p_k)$ implique que $\operatorname{Im} p = \bigoplus_{k=1}^{s} \operatorname{Im} p_k$.

Pour tout $x \in \mathbb{K}^n$ et tout $j \in [\![1,s]\!]$, on a :

$$p_j(x) = p\left(p_j(x)\right) = \sum_{i=1}^{s} p_i\left(p_j(x)\right).$$

L'unicité de la décomposition de $p_j(x)$ suivant les $\operatorname{Im} p_i$ donne alors $p_i\left(p_j(x)\right) = 0$ pour $i \neq j$. Ainsi, $\forall (i,j) \in [\![1,s]\!]$, $i \neq j \Rightarrow p_i \circ p_j = 0$.
ou encore, $\forall (i,j) \in [\![1,s]\!]$, $i \neq j \Rightarrow A_i A_j = 0$.

Commentaires

A priori, les A_k ne commutent pas.

La condition suffisante est banale.

A est alors la matrice de $p = \sum_{k=1}^{s} p_k$.

$\operatorname{rg}\left(\sum p_k\right) \leqslant \sum \operatorname{rg}(p_k)$.

$A_k^2 = A_k \Rightarrow \operatorname{rg} A_k = \operatorname{Tr} A_k$.

$A^2 = A \Rightarrow \operatorname{rg} A = \operatorname{Tr} A$.

p est un projecteur, donc $\operatorname{Im} p = \operatorname{Inv} p$.

La somme est directe et $p_j(x) = p_j\left(p_j(x)\right)$.

Copyrighted material

III. Commutateur de deux matrices

Ex. 7

Soit A et B deux matrices antisymétriques réelles d'ordre n.

1) Montrer que $\mathrm{Tr}(AB-BA)^4 \geqslant 0$.

2) Que peut-on dire de A et B lorsque cette trace est nulle ?

Indications

Le point clé est que $AB-BA$ est antisymétrique. Cette situation est également vraie si A et B sont symétriques.

Solution

1) Avec l'antisymétrie de A et de B, la matrice $AB-BA$ est antisymétrique.

Alors $C=(AB-BA)^2$ est symétrique.

Avec $C=\left[c_{ij}\right]$, on a $\mathrm{Tr}\left(C^2\right)=\sum_{i=1}^{n}\sum_{k=1}^{n} c_{ik}c_{ki}=\sum_{i=1}^{n}\sum_{k=1}^{n} c_{ik}^2 \geqslant 0$.

2) Le même calcul montre que $\mathrm{Tr}\left(C^2\right)=0$ alors :

$$\forall (i,k)\in[\![1,n]\!]^2,\ c_{ik}=0.$$

Posons $AB-BA=\left[d_{ij}\right]$.

Alors, pour tout $i\in[\![1,n]\!]$, $c_{ii}=\sum_{k=1}^{n} d_{ik}d_{ki}=-\sum_{k=1}^{n} d_{ik}^2$.

On en déduit $\forall (i,k)\in[\![1,n]\!]^2,\ d_{ik}=0$, c'est-à-dire $AB=BA$.

Commentaires

${}^t(AB-BA)={}^t(AB)-{}^t(BA)={}^tA{}^tB-{}^tB{}^tA$.

Si une matrice est antisymétrique, son carré est symétrique.

La trace de $(AB-BA)^4$ est celle de C^2.

car $AB-BA$ est antisymétrique.

Ex. 8

Étant donné A et B dans $\mathcal{M}_n(\mathbb{R})$, on pose $C=AB-BA$.
Montrer que si C est colinéaire à A ou à B, alors elle est nilpotente.

Indications

Si $C=\lambda A$, il suffit de montrer que A est nilpotente. Considérer l'application linéaire $\varphi : M\mapsto MB-BM$.

Solution

On suppose que $C=\lambda A$, avec $\lambda\in\mathbb{R}^*$ et $A\neq 0$.

Soit $\varphi\in\mathcal{L}\left(\mathcal{M}_n(\mathbb{R})\right)$ définie par $\varphi(M)=MB-BM$.

Alors $\lambda A=AB-BA$, s'exprime par $\varphi(A)=\lambda A$ et il vient :

$$\forall k\in\mathbb{N}^*,\ \varphi(A^k)=k\lambda A^k.$$

En effet, $\varphi\left(A^{k+1}\right)=A^k(AB)-BA^{k+1}=A^k(BA+C)-\left(BA^k\right)A$, donc :

$$\varphi\left(A^{k+1}\right)=\left(A^kB-BA^k\right)A+A^kC=\varphi(A^k)A+\lambda A^{k+1}$$

Alors $\varphi\left(A^{k+1}\right)=\left(\lambda A^k\right)A+\lambda A^{k+1}=(k+1)\lambda A^{k+1}$.

Considérons $\varphi_k=\varphi-\lambda k\,\mathrm{Id}$.

Il existe k_0 tel que φ_{k_0} est bijective.

Alors $\varphi_{k_0}\left(A^{k_0}\right)=0$ implique $A^{k_0}=0$ et A est nilpotente.

Commentaires

Si $\lambda=0$ ou $A=0$, alors $C=0$.

Preuve par récurrence.

$AB=BA+C$ par définition de C.

$C=\lambda A$.

Hypothèse de récurrence : $\varphi(A^k)=k\lambda A^k$.

Pour exploiter $\varphi(A^k)=\lambda kA^k$.

$\det\varphi_k$ est un polynôme en k de degré au plus n et n'admet donc qu'un nombre fini de valeurs d'annulation.

Exercices

Niveau 1

Ex. 1

Existe-t-il des matrices A et B dans $\mathcal{M}_n(\mathbb{K})$ telles que :

$$AB - BA = I_n \ ?$$

Donner un exemple d'endomorphismes f et g de $E = \mathbb{K}[X]$ tels que $f \circ g - g \circ f = \mathrm{Id}_E$.

Ex. 2

Montrer que les matrices :

$$A = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 1 \\ -1 & 6 \end{pmatrix}$$

sont semblables.

Ex. 3

$$A = \begin{pmatrix} 1 & -1 & 4 \\ 2 & -2 & 8 \\ 3 & -3 & 12 \end{pmatrix} \text{ et } B = \begin{pmatrix} 1 & 3 & 4 \\ 0 & -2 & 6 \\ 0 & 8 & 12 \end{pmatrix}$$

sont-elles des matrices semblables ?

Ex. 4

Montrer que, quelle que soit $A \in \mathcal{M}_2(\mathbb{K})$, les matrices A et ${}^tA$ sont semblables.

Ex. 5

Soit f un endomorphisme d'un $\mathbb{K}$-espace vectoriel de dimension finie tel que $f^2 = \lambda f$, avec $\lambda \in \mathbb{K}^*$.

Comparer $\mathrm{Tr}\, f$ et $\mathrm{rg}\, f$.

Ex. 6

Soit $(X_1, \ldots, X_q)$ et $(Y_1, \ldots, Y_p)$ des familles libres dans $\mathcal{M}_{n,1}(\mathbb{K})$.

Montrer que la famille $\left(Y_i\, {}^tX_j\right)_{(i,j) \in [\![1,p]\!] \times [\![1,q]\!]}$ est libre dans $\mathcal{M}_n(\mathbb{K})$.

Niveau 2

Ex. 7

Montrer que deux matrices idempotentes sont semblables si et seulement si elles ont le même rang.

Ex. 8

Soit $G \subset \mathcal{M}_n(\mathbb{C})$ un groupe multiplicatif. Montrer que tous les éléments de G ont le même rang.

Ex. 9

Soit $A \in \mathrm{GL}_n(\mathbb{K})$ et $B \in \mathcal{M}_n(\mathbb{K})$, avec $\mathrm{rg}\, B = 1$.

Montrer que $A + B$ est dans $\mathrm{GL}_n(\mathbb{C})$ si et seulement si :

$$\mathrm{Tr}\left(BA^{-1}\right) \neq -1.$$

Ex. 10

Soit A, B, C dans $\mathcal{M}_n(\mathbb{R})$ idempotentes.

Montrer que, si $S = A + \sqrt{2}B + \sqrt{3}C$ est idempotente, alors $B = C = 0$.

Ex. 11

Soit $A \in \mathcal{M}_n(\mathbb{K})$ telle que $A^2 = A$.

Montrer que la trace de l'endomorphisme ψ de $\mathcal{M}_n(\mathbb{K})$ défini par $\psi(M) = AM + MA$ est égale à $2n\, \mathrm{rg}\, A$.

Ex. 12

Soit p une application continue de $[0, 1]$ dans $\mathcal{M}_n(\mathbb{R})$.

On suppose que, pour tout $t \in [0, 1]$, $p(t)$ est une matrice idempotente.

Montrer que $\varphi : t \mapsto \mathrm{rg}\left(p(t)\right)$ est constante.

Ex. 13

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et G un sous-groupe d'ordre $n \in \mathbb{N}^*$ de $\mathrm{GL}_n(E)$.

Montrer que le sous-espace des vecteurs invariants par tous les éléments de G a pour dimension $\dfrac{1}{n} \displaystyle\sum_{g \in G} \mathrm{Tr}\, g$.

Avec éléments de solution

Ex. 14

Étant donné A et B dans $\mathcal{M}_n(\mathbb{K})$, résoudre l'équation :

$$X \in \mathcal{M}_n(\mathbb{K}),\ X + (\mathrm{Tr}\, X)A = B.$$

Copyrighted material

Ex. 15

Soit A et M dans $\mathcal{M}_n(\mathbb{R})$, avec :

$$\operatorname{rg} M = 1.$$

Montrer que :

$$\det\big((A+M)(A-M)\big) \leqslant \det\left(A^2\right).$$

Ex. 16

Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbb{K})$.

Montrer que si $\displaystyle\sum_{M\in G} \operatorname{Tr} M = 0$, alors $\displaystyle\sum_{M\in G} M = 0$.

Niveau 3

Ex. 17

Donner une condition nécessaire et suffisante sur les réels a et b pour que :

$$A = \begin{pmatrix} a & b & \dots & b \\ b & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & b \\ b & \dots & b & a \end{pmatrix} \in \mathcal{M}_n(\mathbb{R}) \text{ soit inversible.}$$

Calculer A^{-1} quand elle existe.

Ex. 18

Soit A et B dans $\mathcal{M}_n(\mathbb{C})$ et $M = \begin{pmatrix} A & A \\ A & B \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{C})$.

1) Calculer le rang de M en fonction de A et B.

2) Calculer M^{-1} quand elle existe.

Ex. 19

Soit f une application non constante de $\mathcal{M}_n(\mathbb{C})$ dans $\mathbb{C}$ telle que : $\forall (A,B)\in \mathcal{M}_n(\mathbb{C}) \times \mathcal{M}_n(\mathbb{C})$,

$$f(AB) = f(A)\,f(B) \quad \textbf{(1)}$$

Montrer que : $f(A) = 0 \iff (A \text{ est inversible})$.

Ex. 20

On donne $A \in \mathcal{M}_n(\mathbb{C})$.

1) Expliciter $f : \mathcal{M}_n(\mathbb{C}),\ X \mapsto \operatorname{Tr}(AX)$.

2) Montrer que, pour tout élément φ du dual $\mathcal{M}_n(\mathbb{C})^*$ de $\mathcal{M}_n(\mathbb{C})$, il existe une unique matrice $A\in\mathcal{M}_n(\mathbb{C})$ telle que φ soit l'application $X \mapsto \operatorname{Tr}(AX)$.

3) Caractériser les formes linéaires g sur $\mathcal{M}_n(\mathbb{C})$ telles que :

$$\forall (X,Y)\in \mathcal{M}_n(\mathbb{C})^2,\ g(XY) = g(YX).$$

4) Montrer que, dans tout hyperplan de $\mathcal{M}_n(\mathbb{C})$, il existe une matrice inversible.

Ex. 21

Étant donné n et p entiers naturels non nuls, on considère une famille $(A_k)_{k\in[\![1,p]\!]}$ d'éléments de $\mathrm{GL}_n(\mathbb{R})$ deux à deux distincts et telle que $\{A_1, \dots, A_p\}$ soit stable pour la multiplication.

Montrer que la trace de $\displaystyle\sum_{k=1}^{p} A_k$ est un entier naturel multiple de p.

Avec éléments de solution

Ex. 22

1) Soit $n\in\mathbb{N}$, $n \geqslant 2$. Trouver les matrices $A\in\mathcal{M}_n(\mathbb{K})$ telles que :

$$\forall M \in \mathcal{M}_n(\mathbb{K}),\ \det(A+M) = \det A + \det M.$$

2) Trouver les couples $(A,B)\in(\mathcal{M}_n(\mathbb{K}))^2$ tels que :

$$\forall M \in \mathcal{M}_n(\mathbb{K}),\ \det(A+M) = \det(B+M).$$

Ex. 23

Étant donné $p\in\mathbb{N}^*$, p premier, on considère la matrice $M\left(a_0, a_1, \dots, a_{p-1}\right) \in \mathcal{M}_p(\mathbb{Z})$ circulante (droite) à coefficients entiers.

Montrer que $\det M = \displaystyle\sum_{k=0}^{p-1} a_k \bmod p$.

Ex. 24

On considère la matrice $A \in \mathcal{M}_n(\mathbb{R})$ telle que :

$$\forall (i,j)\in[\![1,n]\!]^2,\ a_{ij} = i \wedge j.$$

Calculer $\det A$.

Ex. 25

Soit $\mathcal{D}\subset\mathcal{M}_n(\mathbb{K})$ le sous-ensemble des matrices A telles que $A^2 = 0$.

Déterminer le nombre de classes d'équivalence, pour la relation de similitude, contenues dans $\mathcal{D}$.

Copyrighted material

Indications

Ex. 7

A et B sont des matrices de projecteurs p et q. Utiliser des bases U et V adaptées à ces projecteurs.

Ex. 8

Il n'est pas dit que G est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$. En particulier, l'élément neutre J de G n'est pas supposé être I_n. Comparer le rang de $A \in G$ à celui de J.

Ex. 9

$A + B \in \mathrm{GL}_n(\mathbb{K})$ équivaut à $(A + B)A^{-1} \in \mathrm{GL}_n(\mathbb{K})$.

Utiliser les endomorphismes de $\mathbb{K}^n$ canoniquement associés à A et B.

Ex. 10

La trace d'un projecteur est un entier naturel.

$\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$ sont des irrationnels.

Ex. 11

Calculer $\psi(E_{ij})$ pour les matrices élémentaires, qui forment la base canonique de $\mathcal{M}_n(\mathbb{K})$.

On pourra se reporter à l'exemple 5 du cours. Toutefois, le résultat alors donné ne préjuge pas $A^2 = A$.

Ex. 12

p est continue signifie que les n^2 termes de $p(t)$ dont des fonctions continues de t.

Ex. 13

Vérifier que $p = \dfrac{1}{n}\sum_{g \in G} g$ est un projecteur.

Ex. 14

$h : M \mapsto (\mathrm{Tr}\, a)M$ et $f = \mathrm{Id}_E + h$, monter que f est inversible lorsque $\mathrm{Tr}\, A \neq -1$.

Ex. 15

Commencer par le cas où $m_{ij} = \delta_{1i}\delta_{1j}$ pour exprimer $\det(A + M)$ et $\det(A - M)$ à l'aide de $\det A$ et d'un cofacteur de A.

Ex. 16

On peut s'inspirer de l'exercice 13.

Ex. 17

Lorsque $\det A \neq 0$, on peut associer à la matrice A le système de Cramer : $AX = Y$.

Ex. 18

1) $\mathrm{rg}\, M = \mathrm{rg} \begin{pmatrix} A & 0 \\ 0 & B - A \end{pmatrix}$.

2) Si M est inversible, écrire le système $MX = Y$ sous la forme :

$$\begin{pmatrix} A & A \\ A & B \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix}.$$

Ex. 19

Si $\mathrm{rg}\, A = r \in [\![1, n-1]\!]$, et si K_r est une matrice nilpotente de rang r, il existe P, Q dans $\mathrm{GL}_n(\mathbb{C})$ telles que $A = PK_rQ$.

Ex. 20

4) A étant de rang r, il existe P et Q dans $\mathrm{GL}_n(\mathbb{C})$ telles que $PAQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Ex. 21

Avec $A = \sum_{k=1}^{p} A_k$, comparer A^2 et A.

Exploiter, pour $k \in [\![1, p]\!]$, l'application $A_l \mapsto A_l A_k$.

Ex. 22

Une condition nécessaire vient de $M = A$.

Deux démarches possibles ensuite : soit montrer que le rang de A est 0 soit, si $\mathrm{rg}\, A \neq 0$, exhiber une matrice M qui conduit à une contradiction

Ex. 23

$A = (a_{ij})$ et $B = (b_{ij})$ sont congrues modulo p quand $a_{ij} \equiv b_{ij} \bmod p$ pour tout (i, j).

Alors $\det A \equiv \det B \bmod p$.

p divise $\binom{k}{n}$ pour $k \in [\![1, p-1]\!]$ et $x^p \equiv x \bmod p$ pour tout $x \in \mathbb{Z}$.

Ex. 24

On peut utiliser $\sum_{d|n} \varphi(d) = n$.

Justifier $i \wedge j = \sum_{k=1}^{n} \delta_{ki}\delta_{kj}\varphi(k)$ pour i et j dans $[\![1, n]\!]$.

Ex. 25

Pour $A \in \mathcal{D}$, justifier que $\mathrm{rg}\, A$ est au plus égal à la partie entière de $\dfrac{n}{2}$.

Dans $\mathcal{D}$, des matrices sont semblables si et seulement si elles ont le même rang.

Copyrighted material

Solutions des exercices

Niveau 1

Ex. 1

1) On a, pour toutes matrices A et B dans $\mathcal{M}_n(\mathbb{K})$, $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, donc $\mathrm{Tr}(AB - BA) = 0$, alors que $\mathrm{Tr}\, I_n = n$.
La réponse est donc non.

2) On vient de montrer que, si E est de dimension finie, il n'y a pas d'endomorphismes f et g qui vérifient $f \circ g - g \circ f = \mathrm{Id}_E$. Dans $\mathbb{K}[X]$, soit $f : P \mapsto P'$ et $g : P \mapsto XP$.
Avec $f \circ g(P) = (XP)' = P + XP'$ et $g \circ f = XP'$, il vient $\big(f \circ g - g \circ f\big)(P) = P$, donc $f \circ g - g \circ f = \mathrm{Id}_E$.

Ex. 2

Le problème revient à trouver $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K})$ telle que $PB = AP$.

Avec $PB = \begin{pmatrix} -z & x+6z \\ -t & y+6t \end{pmatrix}$ et $AP = \begin{pmatrix} 3x+2y & 3z+2t \\ 4x+3y & 4z+3t \end{pmatrix}$, on obtient un système de quatre équations :

$$3x + 2y + z = 0, \quad x + 3z - 2t = 0, \quad 4x + 3y + t = 0, \quad y - 4z + 3t = 0,$$

qui a pour solutions $(x, y, z, t) = \big(-3z+2t, 4z-3t, z, t\big)$. Par exemple, $P = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$, de déterminant -2 vérifie :

$$PB = AP.$$

Ex. 3

Si des matrices sont semblables, elles ont nécessairement même trace, même rang et même déterminant. S'il est vrai que $\mathrm{Tr}\, A = \mathrm{Tr}\, B$ (mieux, elles ont la même diagonale), le rang de A est égal à 1, alors que celui de B est égal à 3.
A et B ne sont donc pas semblables.

Ex. 4

Si $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ est symétrique, alors A et ${}^tA$ sont évidemment semblables (réflexivité de la similitude).

On peut alors supposer $b \neq c$. une matrice $P = \begin{pmatrix} x & z \\ y & t \end{pmatrix} \in \mathrm{GL}_2(\mathbb{K})$ vérifie $PA = {}^tAP$ si et seulement si :

$$\begin{cases} b(y-z) = 0 \\ c(y-z) = 0 \\ cx + (d-a)y - bt = 0 \\ bt + (a-d)z - cx = 0 \end{cases}$$

Compte tenu de $b \neq c$, les deux premières conditions équivalent à $y = z$. Avec cela, les deux autres conditions sont les mêmes.

Si $b \neq 0$, une solution est (avec $x = 0$) $P = \begin{pmatrix} 0 & b \\ b & d-a \end{pmatrix}$. Si $c \neq 0$, une solution est (avec $t = 0$) $P = \begin{pmatrix} a-d & c \\ c & 0 \end{pmatrix}$.

Ex. 5

En posant $p = \dfrac{1}{\lambda} f$, la propriété $f^2 = \lambda f$ équivaut à $p^2 = p$.

Il s'ensuit $\mathrm{rg}\, p = \mathrm{Tr}\, p$ (proriété utile d'un projecteur). Avec $\mathrm{rg}\, p = \mathrm{rg}\, f$ et $\mathrm{Tr}\, p = \dfrac{1}{\lambda}\mathrm{Tr}\, f$, il vient $\mathrm{Tr}\, f = \lambda\, \mathrm{rg}\, f$.

Ex. 6

Notons que $1 \leqslant p \leqslant n$ et $1 \leqslant q \leqslant n$. On complète les familles libres $(X_1, \ldots, X_q)$ et $(Y_1, \ldots, Y_p)$ en des bases $(X_1, \ldots, X_n)$ et $(Y_1, \ldots, Y_n)$ de $\mathcal{M}_{n,1}(\mathbb{K})$.

Soit A et B les éléments de $\mathrm{GL}_n(\mathbb{K})$ dont les colonnes sont les X_j pour A et les Y_i pour B.

Copyrighted material

On notant $(E_1, \dots, E_n)$ la base canonique de $\mathcal{M}_{n,1}(\mathbb{K})$, on a $Y_i = BE_i$ et $X_j = AE_j$, d'où $Y_i\,{}^tX_j = B\left(E_i\,{}^tE_j\right){}^tA$, c'est-à-dire $Y_i\,{}^tX_j = BE_{ij}\,{}^tA$ où les E_{ij} sont les matrices de la base canonique de $\mathcal{M}_n(\mathbb{K})$.

Comme A et B sont inversibles, $\varphi : M \mapsto BM{}^tA$ est un automorphisme de $\mathcal{M}_n(\mathbb{K})$. Les images par φ de la base canonique de $\mathcal{M}_n(\mathbb{K})$ en constituent une base. Extraite d'une famille libre, la famille $\left(Y_i\,{}^tX_j\right)_{(i,j)\in[\![1,p]\!]\times[\![1,q]\!]}$ est libre.

Niveau 2

Ex. 7

A et B telles que $A^2 = A$ et $B^2 = B$ sont, dans la base canonique B de $\mathbb{K}^n$, des matrices de projecteurs p et q.

Il existe des bases U et V de $\mathbb{K}^n$ dans lesquelles les matrices de p et q sont respectivement :

$$J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \text{ et } J_{r'} = \begin{pmatrix} I_{r'} & 0 \\ 0 & 0 \end{pmatrix}$$

où r et r' sont les rangs de p et q, c'est-à-dire ceux de A et B.

On en déduit que si A et B ont même rang, elles sont semblables à une même matrice J_r, donc elles sont semblables. La réciproque est évidente.

Ex. 8

Pour $A \in \mathcal{M}_n(\mathbb{C})$, soit $f_A \in \mathcal{L}(\mathbb{C}^n)$ canoniquement associé à A (A matrice de f_A dans la base canonique de $\mathbb{C}^n$).

Soit J l'élément neutre du groupe multiplicatif G : $\forall A \in G,\ AJ = JA = A$.

Cela équivaut à $f_J \circ f_A = f_A \circ f_J = f_A$. La relation $f_A \circ f_J = f_A$ donne $\operatorname{Ker} f_J \subset \operatorname{Ker} f_A$.

Soit $B \in G$ tel que $AB = BA = J$ (inverse de A dans G) : $f_A \circ f_B = f_B \circ f_A = f_J$.

La relation $f_B \circ f_A = f_J$ donne $\operatorname{Ker} f_A \subset f_J$. Finalement, il vient $\operatorname{Ker} f_A = \operatorname{Ker} f_J$.

Alors (théorème du rang) : $\operatorname{rg} f_A = \operatorname{rg} f_J$. En conclusion, pour tout $A \in G$, $\operatorname{rg} A = \operatorname{rg} J$.

Ex. 9

Soit f et g les endomorphismes de $E = \mathbb{K}^n$ canoniquement associés à A et B.

f étant dans $\mathrm{GL}(E)$, on a $f + g \in \mathrm{GL}(E)$ si et seulement si $(f + g) \circ f^{-1} \in \mathrm{GL}(E)$, c'est-à-dire si et seulement si $g \circ f^{-1} + \mathrm{Id}_E \in \mathrm{GL}(E)$.

Avec $A \in \mathrm{GL}_n(\mathbb{K})$, on a $\operatorname{rg}\left(BA^{-1}\right) = \operatorname{rg} B = 1$, donc le noyau de $g \circ f^{-1}$ est de dimension $n - 1$.

On complète une base de $\operatorname{Ker}\left(g \circ f^{-1}\right)$ en une base $\mathcal{B} = (e_1, \dots, e_{n-1}, e_n)$ de E.

Dans $\mathcal{B}$, la matrice de $g \circ f^{-1}$ est de la forme $C = \begin{pmatrix} 0 & \cdots & 0 & \lambda_1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix}$ et on a $\operatorname{Tr} BA^{-1} = \operatorname{Tr} C = \lambda_n$.

Avec $\det\left(C + I_n\right) = 1 + \lambda_n$, il vient $A + B$ inversible si et seulement si $\lambda_n \neq -1$, c'est-à-dire $\operatorname{Tr}\left(BA^{-1}\right) \neq -1$.

Ex. 10

On a $\operatorname{Tr} S = \operatorname{Tr} A + \sqrt{2}\operatorname{Tr} B + \sqrt{3}\operatorname{Tr} C$.

A, B et C étant idempotentes, leurs traces sont des entiers naturels.

Si S est idempotente, donc de trace dans $\mathbb{N}$, l'égalité :

$$(\operatorname{Tr} A - \operatorname{Tr} S) + \sqrt{2}\operatorname{Tr} B + \sqrt{3}\operatorname{Tr} C = 0$$

signifie que $(\operatorname{Tr} A - \operatorname{Tr} S, \operatorname{Tr} B, \operatorname{Tr} C)$ est solution de l'équation $(x, y, z) \in \mathbb{Z}^3$, $x + y\sqrt{2} + z\sqrt{3} = 0$.

Or, sachant que $\sqrt{2}$, $\sqrt{3}$ et $\sqrt{6}$ sont irrationnels, il vient que $y\sqrt{2} + z\sqrt{3}$, avec $(y, z) \in \mathbb{Q}^2$, n'est rationnel que si $y = z = 0$.

B et C étant idempotentes, on a aussi $\operatorname{rg} B = \operatorname{Tr} B$ et $\operatorname{rg} C = \operatorname{Tr} C$. Alors $\operatorname{Tr} B = \operatorname{Tr} C = 0$ implique $B = C = 0$.

Copyrighted material

Ex. 11

Soit E_{ij} une matrice élémentaire de $\mathcal{M}_n(\mathbb{K})$, de terme général $\delta_{ik}\Delta_{jl}$, $1 \leqslant k \leqslant n$, $1 \leqslant l \leqslant n$.

Avec $A = [a_{ij}]$, on a $AE_{ij} = \sum_{k,l} a_{kl}E_{kl}E_{ij}$ et on sait que $E_{kl}E_{ij} = \delta_{li}E_{kj}$.

Alors $AE_{ij} = \sum_{k=1}^{n} a_{ki}E_{kj}$, de coordonnée a_{ii} sur E_{ij}. De même, la coordonnée sur E_{ij} de $E_{ij}A$ est a_{jj}.

Ainsi, la coordonnée sur E_{ij} de $\psi(E_{ij})$ est $a_{ii} + a_{jj}$. Alors, il s'ensuit $\operatorname{Tr}\psi = \sum_{i,j}(a_{ii} + a_{jj}) = 2n \operatorname{Tr} A$.

Comme A est idempotente, la relation $\operatorname{Tr} A = \operatorname{rg} A$ donne le résultat.

Ex. 12

Comme $p(t)$ est idempotente, on a $\operatorname{rg}\big(p(t)\big) = \operatorname{Tr}\big(p(t)\big)$. L'application $\phi : t \mapsto \operatorname{Tr}\big(p(t)\big)$ est continue (somme de fonctions continues). Comme elle est à valeurs entières, elle est constante (théorème des valeurs intermédiaires).

Ex. 13

Posons $p = \dfrac{1}{n}\sum_{g\in G} g$. Pour tout $h \in G$, on a $h \circ p = \dfrac{1}{n}\sum_{g\in G} h \circ g$.

Or $g \mapsto h \circ g$ est une bijection du groupe fini G. Il s'ensuit $h \circ p = p$.

Alors $p \circ p = \dfrac{1}{n}\Big(\sum_{h\in G} h\Big) \circ p = \dfrac{1}{n}\sum_{h\in G} h \circ p = p$, donc $\operatorname{Tr} p = \operatorname{rg} p$ (propriété utile pour un projecteur).

Il vient alors $\dfrac{1}{n}\sum_{g\in G} \operatorname{Tr} g = \operatorname{Tr} p = \operatorname{rg} p$. Comme l'image d'un projecteur est aussi le sous-espace des vecteurs invariants,

on a $\operatorname{rg} p = \dim\big(\operatorname{Ker}(p - \mathrm{Id}_E)\big)$. Avec $p - \mathrm{Id}_E = \dfrac{1}{n}\sum_{g\in G}(g - \mathrm{Id}_E)$, il vient $\bigcap_{g\in G} \operatorname{Ker}(g - \mathrm{Id}_E) \subset \operatorname{Ker}(p - \mathrm{Id}_E)$.

Réciproquement, pour tout $g \in G$, $g \circ p = p$ donne :

$$\operatorname{Im} p \subset \operatorname{Ker}(g - \mathrm{Id}_E) \text{ donc } \operatorname{Ker}(p - \mathrm{Id}_E) = \operatorname{Im} p \subset \bigcap_{g\in G} \operatorname{Ker}(g - \mathrm{Id}_E).$$

Ainsi $\operatorname{Ker}(p - \mathrm{Id}_E) = \bigcap_{g\in G} \operatorname{Ker}(g - \mathrm{Id}_E)$ donc $\dim\Big(\bigcap_{g\in G} \operatorname{Ker}(g - \mathrm{Id}_E)\Big) = \dfrac{1}{n}\sum_{g\in G} \operatorname{Tr} g$.

Ex. 14

Soit $h : \mathcal{M}_n(\mathbb{K}) \to \mathcal{M}_n(\mathbb{K})$, $M \mapsto (\operatorname{Tr} M)A$. Alors $h^2 = (\operatorname{Tr} A)h$ et, avec $f = \mathrm{Id}_E + h$, il vient :

$$f^2 - (2 + \operatorname{Tr} A)f + (1 + \operatorname{Tr} A)\,\mathrm{Id}_E = 0.$$

Si $\operatorname{Tr} A \neq -1$, alors f est bijective, d'inverse $f^{-1} = \dfrac{1}{1 + \operatorname{Tr} A}\big((2 + \operatorname{Tr} A)\,\mathrm{Id}_E - f\big)$, soit $f^{-1} = \mathrm{Id}_E - \dfrac{1}{1 + \operatorname{Tr} A}\,h$, donc

$f(X) = B$ admet pour solution unique $X = B - \dfrac{\operatorname{Tr} B}{1 + \operatorname{Tr} A}\,A$.

Si $\operatorname{Tr} A = -1$, alors $f^2 = f$ et f est un projecteur de noyau $\{X,\ (\operatorname{Tr} X)A = -X\}$, donc $\operatorname{Ker} f = \mathbb{R}A$.

$\operatorname{Im} f = \operatorname{Inv} f = \operatorname{Ker}(f - \mathrm{Id}_E) = \operatorname{Ker} h = \operatorname{Ker} \operatorname{Tr}$. Ainsi, si $\operatorname{Tr} B \neq 0$, l'équation n'a pas de solution et, si $\operatorname{Tr} B = 0$, l'ensemble des solutions est $B + \mathbb{R}A$.

Ex. 15

1) Premier cas : $M = J = \begin{pmatrix} 1 & & & \\ & 0 & (0) & \\ & (0) & \ddots & \\ & & & 0 \end{pmatrix}$. Alors, avec $A + M = \begin{pmatrix} 1 + a_{11} & \cdots & \cdots \\ \vdots & & \\ \vdots & & (a_{ij}) \\ \vdots & & \end{pmatrix}$, il vient

$\det(A + M) = \det A + \alpha_{11}$, où α_{11} est le cofacteur d'indice $(1, 1)$ de A.

De même, $\det(A - M) = A - \alpha_{11}$ puis $\det\big((A + M)(A - M)\big) = (\det A)^2 - \alpha_{11}^2 \leqslant (\det A)^2$.

Copyrighted material

2) Cas général : il existe P et Q dans $GL_n(R)$ telles que $M = PJQ$. En posant $B = P^{-1}AQ^{-1}$, on a :

$$\det\big((A+M)(A-M)\big) = \det\big(P(B+J)QP(B-J)Q\big) = \det P^2 \det Q^2 \det\big((B+J)(B-J)\big).$$

D'après l'étude du premier cas, $\det\big((B+J)(B-J)\big) \leqslant (\det B)^2$.

Alors $\det\big((A+M)(A-M)\big) \leqslant \det P^2 \det Q^2 (\det B)^2$, soit $\det\big((A+M)(A-M)\big) \leqslant (\det A)^2$.

Ex. 16

On notant $m = \text{Card } G$, on pose $P = \dfrac{1}{m}\sum_{M\in G} M$. On obtient $P^2 = P$. Alors $\text{rg } P = \text{Tr } P = \dfrac{1}{m}\sum_{M\in G} \text{Tr } M$.

Il s'ensuit $\text{rg } P = 0$, c'est-à-dire que $\sum_{M\in G} M = 0$.

Niveau 3

Ex. 17

En ajoutant les lignes $L_2, L_3, \ldots, L_n$ à la ligne L_1 : $L_1 \longleftarrow \sum_{i=1}^{n} L_i$, puis en factorisant $a+(n-1)b$ dans la ligne L_1, il vient :

$$\det A = \big(a+(n-1)b\big)\begin{vmatrix} 1 & 1 & \ldots & \ldots & 1 \\ b & a & b & \ldots & b \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & b \\ b & \ldots & \ldots & b & a \end{vmatrix}$$

Pour $i = 2, 3, \ldots, n$, $L_i \longleftarrow L_i - bL_1$ donne :

$$\det A = \big(a+(n-1)b\big)\begin{vmatrix} 1 & 1 & \ldots & \ldots & 1 \\ 0 & a-b & 0 & \ldots & 0 \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \ldots & \ldots & 0 & a-b \end{vmatrix}$$

Le déterminant qui reste à calculer étant celui d'une matrice triangulaire, il vient : $\det A = \big(a+(n-1)b\big)(a-b)^{n-1}$.

A est donc inversible si et seulement si $a \neq b$ et $a+(n-1)b \neq 0$ (n est supposé $\geqslant 2$).

- Calcul de A^{-1}. Considérons le système (S) : $AX = Y$ équivalent à $X = A^{-1}Y$.

(S) est équivalent à :

$$\begin{cases} ax_1 + bx_2 + \cdots + bx_n = y_1 & (E_1) \\ bx_1 + ax_2 + bx_3 + \cdots + bx_n = y_2 & (E_2) \\ \cdots\cdots\cdots\cdots \\ bx_1 + \cdots + bx_{n-1} + ax_n = y_n & (E_n) \\ x_1 + \cdots + x_n = \dfrac{1}{a+(n-1)b}(y_1 + y_2 + \cdots + y_n) & (E_{n+1}) \end{cases}$$

(l'équation supplémentaire étant la somme des n équations de (S)).

On obtient encore un système équivalent en remplaçant chaque équation (E_i) par $(E_i) - b\big(E_{n+1}\big)$, et il en résulte :

$$\text{pour } 1 \leqslant i \leqslant n,\ (a-b)x_i = y_i - \frac{b}{a+(n-1)b}(y_1 + \cdots + y_n)$$

soit

$$x_i = \frac{1}{(a-b)\big(a+(n-1)b\big)}\left[\big(a+(n-2)b\big)y_i - b\sum_{\substack{j=1 \\ j\neq i}}^{n} y_i\right].$$

En conséquence, on a : $A^{-1} = \dfrac{1}{(a-b)\big(a+(n-1)b\big)}\begin{pmatrix} a+(n-2)b & & \\ & \ddots & (-b) \\ (-b) & & \ddots \\ & & a+(n-2)b \end{pmatrix}$.

Copyrighted material

Ex. 18

1) a) Par transformations élémentaires sur les colonnes : $C_{n+j} \longleftarrow C_{n+j} - C_j$, $1 \leqslant j \leqslant n$ (où C_k est la $k^{\text{ème}}$ colonne de M), on ne change pas le rang de M. Donc $\operatorname{rg} M = \operatorname{rg} M_1$ avec $M_1 = \begin{bmatrix} A & 0 \\ A & B-A \end{bmatrix}$.

De même, par transformations élémentaires sur les lignes : $L_{n+j} \longleftarrow L_{n+j} - L_j$, $1 \leqslant j \leqslant n$, on obtient :

$$\operatorname{rg} M_1 = \operatorname{rg} M_2 \quad \text{avec} \quad M_2 = \begin{pmatrix} A & 0 \\ 0 & B-A \end{pmatrix}.$$

Remarque Les deux affirmations précédentes peuvent aussi se déduire des identités matricielles :

$$\begin{pmatrix} A & 0 \\ A & B-A \end{pmatrix} = \begin{pmatrix} A & A \\ A & B \end{pmatrix}\begin{pmatrix} I_n & -I_n \\ 0 & I_n \end{pmatrix} \text{ et } \begin{pmatrix} A & 0 \\ 0 & B-A \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ -I_n & I_n \end{pmatrix}\begin{pmatrix} A & 0 \\ A & B-A \end{pmatrix}$$

en notant que les deux matrices $\begin{pmatrix} I_n & -I_n \\ 0 & I_n \end{pmatrix}$ et $\begin{pmatrix} I_n & 0 \\ -I_n & I_n \end{pmatrix}$ sont évidemment inversibles.

b) On montre facilement que le rang de M_2 est égal à $\operatorname{rg} A + \operatorname{rg}(B-A)$.

Par exemple, en posant $\operatorname{rg} A = r$ et $\operatorname{rg}(B-A) = s$, on sait qu'il existe P_1, Q_1 et P_2, Q_2 dans $\mathrm{GL}_n(\mathbb{C})$:

$$P_1 A Q_1 = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} = J_r \text{ et } P_2(B-A)Q = \begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix} = J_s$$

d'où $$\begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & B-A \end{pmatrix}\begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix} = \begin{pmatrix} J_r & 0 \\ 0 & J_s \end{pmatrix}$$

et puisque les matrices $P = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}$ et $Q = \begin{pmatrix} Q_1 & 0 \\ 0 & Q_2 \end{pmatrix}$ sont inversibles, on a : $\operatorname{rg} M_2 = r + s$.

En conclusion $$\operatorname{rg} M = \operatorname{rg} A + \operatorname{rg}(B-A).$$

2) On a $\operatorname{rg} A \leqslant n$ et $\operatorname{rg}(B-A) \leqslant n$ donc : $\operatorname{rg} M = 2n \iff \big(\operatorname{rg} A = n \text{ et } \operatorname{rg}(B-A) = n\big)$.

Ainsi M est inversible si et seulement si $A \in \mathrm{GL}_n(\mathbb{C})$ et il existe $D \in \mathrm{GL}_n(\mathbb{C})$ telle que $B = A + D$.

Dans ces conditions, pour X_1, X_2, Y_1, Y_2 dans $\mathcal{M}_{n,1}(\mathbb{C})$, on a :

$$\begin{pmatrix} A & A \\ A & B \end{pmatrix}\begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix} \iff \begin{cases} A(X_1+X_2) = Y_1 \\ AX_1 + BX_2 = Y_2 \end{cases} \iff \begin{cases} A(X_1+X_2) = Y_1 \\ DX_2 = Y_2 - Y_1 \end{cases}$$

$$\iff \begin{cases} X_1 = (A^{-1}+D^{-1})Y_1 - D^{-1}Y_2 \\ X_2 = D^{-1}Y_2 - D^{-1}Y_1 \end{cases}$$

$$\iff \begin{pmatrix} X_1 \\ X_2 \end{pmatrix} = \begin{pmatrix} A^{-1}+D^{-1} & -D^{-1} \\ -D^{-1} & D^{-1} \end{pmatrix}\begin{pmatrix} Y_1 \\ Y_2 \end{pmatrix}$$

On en déduit $$\begin{pmatrix} A & A \\ A & B \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1}+(B-A)^{-1} & -(B-A)^{-1} \\ -(B-A)^{-1} & (B-A)^{-1} \end{pmatrix}$$

Ex. 19

1) Supposons $f(A) = 0$.

Si A était inversible, pour tout $B \in \mathcal{M}_n(\mathbb{C})$ on pourrait écrire $B = AA^{-1}B$ et on aurait donc :

$$f(B) = f(A)\,f\left(A^{-1}B\right) = 0$$

f serait constante, nulle. Ce cas étant à rejeter par hypothèse, on en déduit que $A \notin \mathrm{GL}_n(\mathbb{C})$.

Remarque. L'implication ainsi démontrée donne par contraposition : $A \in \mathrm{GL}_n(\mathbb{C}) \;\Rightarrow\; f(A) \neq 0$.

2) Supposons que $A \notin \mathrm{GL}_n(\mathbb{C})$.

a) Un premier cas est $A = 0$.

(1) donne alors $\forall B \in \mathcal{M}_n(\mathbb{C}), f(0)\big(1 - f(B)\big) = 0$ donc $f(0) = 0$ sinon f serait constante égale à 1, ce qui est exclu par hypothèse.

b) Le cas général est $\operatorname{rg} A = r$ avec $1 \leqslant r \leqslant n-1$.

Considérons alors la matrice : $K_r = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & 1 & \ddots & \vdots \\ \vdots & & & \ddots & 0 & 0 \\ \vdots & & & & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$ où le nombre de 1 est égal à r.

K_r est nilpotente et $\operatorname{rg} K_r = r$.

Copyrighted material

Puisqu'elles sont de même rang, A et K_r sont équivalentes, c'est-à-dire qu'il existe P et Q dans $\mathrm{GL}_n(\mathbb{C})$ telles que $A = PK_rQ$ ce qui, d'après **(1)**, donne $f(A) = f(P)f(Q)f\left(K_r\right)$.

Par ailleurs, $K_r^n = 0$ donne $f\left(K_r\right)^n = 0$ et donc $f\left(K_r\right) = 0$, puis $f(A) = 0$.

Ex. 20

Soit $A = \left[a_{ij}\right] \in \mathcal{M}_n(\mathbb{C})$.

1) Pour $X = [x_{ij}]$ posons $AX = Y$, $Y = \left[y_{ij}\right]$.

Alors, pour tout $(i, k) \in [\![1, n]\!]^2$, $y_{ik} = \sum_{j=1}^{n} a_{ij}x_{jk}$ donc $\mathrm{Tr}(AX) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_{ji}$.

2) Soit $\left(E_{ij}\right)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant n}}$ la base canonique de $\mathcal{M}_n(\mathbb{C})$ (matrices élémentaires).

Étant donné $\varphi \in \mathcal{M}_n(\mathbb{C})^*$, pour tout $X = \sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij}E_{ij}$ de $\mathcal{M}_n(\mathbb{C})$, on a : $\varphi(X) = \sum_{i=1}^{n}\sum_{j=1}^{n} \varphi\left(E_{ij}\right)x_{ij}$ donc, d'après 1), $\varphi(X) = \mathrm{Tr}(AX)$ où A est la matrice de terme général $a_{ij} = \varphi(E_{ji})$.

Considérons alors l'application Φ de $\mathcal{M}_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})^*$ qui, à toute matrice A de $\mathcal{M}_n(\mathbb{C})$, associe la forme linéaire $\varphi_A \ : \ X \mapsto \mathrm{Tr}(AX)$.

Φ est évidemment linéaire et ce qui précède montre qu'elle est surjective.

En conséquence, puisque $\dim \mathcal{M}_n(\mathbb{C}) = \dim \mathcal{M}_n(\mathbb{C})^* = n^2$, on en déduit que Φ est un isomorphisme de $\mathcal{M}_n(\mathbb{C})$ sur $\mathcal{M}_n(\mathbb{C})^*$.

Finalement, pour tout $\varphi \in \mathcal{M}_n(\mathbb{C})^*$, il existe une unique matrice A de $\mathcal{M}_n(\mathbb{C})$ telle que :

$$\Phi(A) = \varphi \quad \text{c'est-à-dire telle que} \quad \forall X \in \mathcal{M}_n(\mathbb{C}),\ \varphi(X) = \mathrm{Tr}(AX).$$

3) Soit $g \in \mathcal{M}_n(\mathbb{C})^*$ telle que $\forall (X, Y) \in \mathcal{M}_n(\mathbb{C})^2$, $g(XY) = g(YX)$.

D'après le 2), il existe $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\forall X \in \mathcal{M}_n(\mathbb{C})$, $g(X) = \mathrm{Tr}(AX)$ donc :

$$\text{pour tout } (X, Y) \in \mathcal{M}_n(\mathbb{C})^2,\ \mathrm{Tr}(AXY) = \mathrm{Tr}(AYX). \quad \textbf{(1)}$$

Sachant que $E_{ij}E_{k\ell} = \delta_{jk}E_{i\ell}$ (δ_{jk} : symbole de Kronecker), on obtient :

$$A\,E_{k\ell} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{ij}E_{k\ell} = \sum_{i=1}^{n} a_{ik}E_{i\ell} \quad \text{donc} \quad \mathrm{Tr}\left(A\,E_{k\ell}\right) = a_{\ell k}.$$

Alors, avec $i \neq j$, $X = E_{ik}$ et $Y = E_{kj}$, la relation **(1)** donne $\mathrm{Tr}(A\,E_{ij}) = 0$ donc $a_{ji} = 0$ puis, avec $X = E_{ij}$ et $Y = E_{ji}$, la relation **(1)** donne : $\mathrm{Tr}(A\,E_{ii}) = \mathrm{Tr}(A\,E_{jj})$ donc $a_{ii} = a_{jj}$.

En conséquence, A est une matrice scalaire $A = \lambda I_n$ et g est définie par : $g(X) = \lambda\,\mathrm{Tr}\,X$ donc $g = \lambda\,\mathrm{Tr}$.

Inversement, on sait que, pour tout couple (X, Y) de $\mathcal{M}_n(\mathbb{C})$, on a $\mathrm{Tr}(XY) = \mathrm{Tr}(YX)$, donc une forme linéaire $g \in \mathcal{M}_n(\mathbb{C})^*$ vérifie $g(XY) = g(YX)$ pour tout (X, Y) si et seulement si il existe $\lambda \in \mathbb{C}$ tel que $g = \lambda\,\mathrm{Tr}$.

4) Tout hyperplan H de $\mathcal{M}_n(\mathbb{C})$ est le noyau d'une forme linéaire non nulle.

Il existe donc $A \in \mathcal{M}_n(\mathbb{C})$, $A \neq 0$, telle que, pour tout X de $\mathcal{M}_n(\mathbb{C})$, on ait : $X \in H \iff \mathrm{Tr}(AX) = 0$.

Posons $r = \mathrm{rg}\,A$, on sait qu'il existe P et Q dans $\mathrm{GL}_n(\mathbb{C})$ telles que : $A = P\,J_r\,Q$ avec $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ et $A \neq 0$ équivaut à $r \geqslant 1$. On a alors, pour tout $X \in \mathcal{M}_n(\mathbb{C})$: $\mathrm{Tr}(AX) = \mathrm{Tr}(P\,J_r\,QX) = \mathrm{Tr}(J_r\,QXP)$.

En considérant, par exemple, la matrice de permutation :

$$U = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \\ \vdots & & \ddots & \ddots & 0 \\ 0 & & & \ddots & 1 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix} \quad \text{on a} \quad J_rU = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \\ \vdots & & \ddots & 1 & \ddots & \\ \vdots & & & \ddots & 0 & 0 \\ \vdots & & & & \ddots & 0 \\ 0 & \dots & \dots & \dots & \dots & 0 \end{pmatrix} \quad \text{pour } r < n$$

et $J_nU = I_nU = U$ donc, dans tous les cas $\mathrm{Tr}(J_rU) = 0$, or $U = QVP$ avec $V = Q^{-1}UP^{-1}$ donc $\mathrm{Tr}(AV) = \mathrm{Tr}(J_rU) = 0$ et V, qui est inversible, appartient à H.

Copyrighted material

Ex. 21

Pour i, j et k dans $[\![1, p]\!]$, $A_iA_k = A_jA_k$ implique $A_i = A_j$ puisque A_k est inversible.

Ainsi $\varphi_k \ : \ A_i \mapsto A_iA_k$ est une application injective.

La stabilité de $U = \{A_1, \ldots, A_p\}$ pour la multiplication montre que $\varphi_k(U) \subset U$.

Il s'ensuit que φ_k est une permutation de U.

On a donc $\displaystyle\sum_{i=1}^{p} A_i = \sum_{i=1}^{p} A_iA_k = \Big(\sum_{i=1}^{p} A_i\Big)A_k$.

En posant $A = \displaystyle\sum_{i=1}^{p} a_i$, ceci nous donne $A = AA_k$ pour tout $k \in [\![1, p]\!]$.

Alors $A^2 = A\Big(\displaystyle\sum_{k=1}^{p} A_k\Big) = \sum_{k=1}^{p} AA_k = pA$, soit $\left(\frac{1}{p}A\right)^2 = \frac{1}{p}A$ ce qui montre que $\frac{1}{p}A$ est une matrice de projection.

La trace de $\frac{1}{p}A$ est donc égale à son rang et c'est ainsi un entier naturel.

Finalement $\operatorname{Tr} A = p \operatorname{Tr}\left(\frac{1}{p}A\right)$ est un entier naturel multiple de p.

Ex. 22

1) Première condition : en prenant $M = A$, il vient $\det(2A) = 2 \det A$, soit $\left(2^n - 2\right) \det A = 0$, donc $\det A = 0$.

On est ramené à $\det(A + M) = \det M$, avec A non inversible (ou de rang strictement inférieur à n).

Première démarche : soit $A_1, \ldots, A_n$ les vecteurs colonnes de A. On considère $M_i \in \mathcal{M}_n(\mathbb{K})$ dont la $i^{\text{ème}}$ colonne est $-A_i$. Alors $A + M_i$ n'est pas inversible et il s'ensuit $\det M_i = 0$.

Si A n'est pas la matrice nulle, on prend $A_i \neq 0$. On choisit des colonnes $U_j, j \in [\![1, n]\!] \setminus \{i\}$ qui complètent $-A_i$ en une famille de colonnes indépendantes, d'où $\det M_i \neq 0$ pour une contradiction.

Seconde démarche : soit $r = \operatorname{rg} A$ et P, Q dans $\mathrm{GL}_n(\mathbb{K})$ telles que $A = PJ_rQ$ avec $J_r = \begin{pmatrix} I_r & (0) \\ (0) & (0) \end{pmatrix}$.

Pour $M = P(I_n - J_r)Q$, $\det\big(PJ_rQ + P(I_n - J_r)Q\big) = \det\big(P(I_n - J_r)Q\big)$ donne $1 = \det(I_n - J_r)$, ce qui implique $J_r = 0$, donc $A = 0$.

2) En posant $U = M + B$, $\det(A + M) = \det(B + M)$ se lit $\det(A - B + U) = \det U$.

Comme en première partie, il vient $\det(A - B) = 0$ puis $A - B = 0$.

Ex. 23

$M = \begin{pmatrix} a_0 & a_1 & \ldots & a_{p-1} \\ a_{p-1} & a_0 & \ldots & a_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}$, on a $M = a_0I_p + a_1J + \ldots + a_{p-1}J^{p-1}$ avec $J = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$.

Si A et B dans $\mathcal{M}_p(\mathbb{Z})$ commutent alors $(A + B)^p = A^p + B^p \bmod p$, compte tenu de p divise C_p^k pour $1 \leqslant k \leqslant p - 1$.

Alors, si des matrices A_i commutent deux à deux, $\Big(\displaystyle\sum_i A_i\Big)^p = \sum_i A_i^p \bmod p$. En particulier :

$$M^p = a_0^pI_p + \sum_{k=1}^{p-1} a_k^pJ^{kp} \bmod p.$$

Avec $J^p = I_p$ et $\forall x \in \mathbb{Z}$, $x^p = x \bmod p$, il vient $M^p = \Big(\displaystyle\sum_{k=0}^{p-1} a_k\Big)I_p \bmod p$.

Il reste à noter que $A = B \bmod p \ \Rightarrow \ \det A = \det B \bmod p$ pour conclure : $\det M = \displaystyle\sum_{k=0}^{p-1} a_k \bmod p$.

Copyrighted material

Ex. 24

On a vu (chapitre 1) que, pour $m \in \mathbb{N}^*$, on a $m = \sum_{d|m} \varphi(d)$ où la somme porte sur les diviseurs dans $\mathbb{N}$ de m, et φ désigne la fonction indicatrice d'Euler. On a donc $i \wedge j = \sum_{k|i \text{ et } k|j} \varphi(k)$.

On pose $\Delta_{k\,i} = 1$ si k divise i et $\Delta_{k\,i} = 0$ sinon. Alors, pour i et j dans $[\![1, n]\!]$, on a :

$$i \wedge j = \sum_{k=1}^{n} \Delta_{k\,i}\, \Delta_{k\,j}\, \varphi(k).$$

On reconnaît alors le terme général du produit de matrices P et Q triangulaires dont les termes diagonaux sont tous égaux à 1 pour l'une et égaux aux $\varphi(k)$, $k \in [\![1, n]\!]$, pour l'autre.

Le déterminant de A est donc égal à $\prod_{k=1}^{n} \varphi(k)$.

Ex. 25

1) Soit $A \in \mathcal{D}$ et u l'endomorphisme de $\mathbb{K}^n$ canoniquement associé à A. Notons $r = \operatorname{rg} A = \operatorname{rg} u$.

$u^2 = 0$ équivaut à $\operatorname{Im} u \subset \operatorname{Ker} u$, ce qui implique $r \leqslant n - r$, soit $r \leqslant \frac{n}{2}$ ou $r \leqslant n'$, avec n' partie entière de $\frac{n}{2}$.

Soit $(e_1, \ldots, e_r)$ une base d'un supplémentaire de $\operatorname{Ker} u$.

$(u(e_1), \ldots, u(e_r))$ est une famille libre d'éléments qui sont encore dans $\operatorname{Ker} u$.

On la complète par $(e_{r+1}, \ldots, e_{n-r})$ pour obtenir une base de $\operatorname{Ker} u$.

Dans la base $(u(e_1), \ldots, u(e_r), e_{r+1}, \ldots, e_{n-r}, e_1, \ldots, e_r)$, la matrice de u est $J_r = \begin{pmatrix} (0) & I_r \\ (0) & (0) \end{pmatrix}$.

2) Toute matrice semblable à une matrice de carré nul est elle-même de carré nul, donc $\mathcal{D}$ est une réunion de classes de similitude.

Deux matrices de $\mathcal{D}$ de même rang r sont semblables, puisque semblables à J_r, et deux matrices semblables ont le même rang.

Pour tout $r \in [\![0, n']\!]$, la matrice J_r est de rang r et de carré nul. Il y a donc $1 + n'$ classes de similitude.

Copyrighted material

CHAPITRE 5

Réduction des endomorphismes et des matrices carrées

Copyrighted material

Dans tout ce chapitre, E est un $\mathbb{K}$-espace vectoriel non réduit à $\{0\}$, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

A. Sous-espaces stables

1. Endomorphisme induit

Définition 1

Un sous-espace vectoriel F de E est **stable par** $u \in \mathscr{L}(E)$ si et seulement si $u(F) \subset F$. (1)

(1) On dit aussi que u stabilise F. Cette notion n'est pas nouvelle : il s'agit ici d'un simple rappel.

Définition 2

Si F est un sous-espace vectoriel de E stable pour $u \in \mathscr{L}(E)$, la restriction $u_{|F}$ de u à F induit un endomorphisme de F, noté u_F, défini par : (2)

$$\forall x \in F, \quad u_F(x) = u(x).$$

(2) u_F et $u_{|F}$ ne diffèrent que par l'espace d'arrivée : $u_{|F} \in \mathscr{L}(F,E)$ et $u_F \in \mathscr{L}(F,F)$.

Théorème 1

Soit u et v deux endomorphismes de E tels que $u \circ v = v \circ u$.
Alors, $\operatorname{Im} u$ et $\operatorname{Ker} u$ sont stables par v. (3)
En particulier, pour tout $u \in \mathscr{L}(E)$, $\operatorname{Im} u$ et $\operatorname{Ker} u$ sont stables par u.

(3) Ce résultat élémentaire est d'usage très fréquent.

2. Interprétation matricielle

E est maintenant un $\mathbb{K}$-espace vectoriel de dimension finie $n \geqslant 1$.

2.1 – Caractérisation matricielle d'un sous-espace stable

Théorème 2

Étant donné un sous-espace vectoriel F de E, $F \neq \{0\}$, et $\mathscr{B} = (e_i)_{1 \leqslant i \leqslant n}$ une base de E obtenue en complétant une base $\mathscr{B}_F = (e_i)_{1 \leqslant i \leqslant p}$ de F, F est stable par $u \in \mathscr{L}(E)$ si et seulement si $\operatorname{mat}_{\mathscr{B}} u$ est de la forme $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ où $A \in \mathscr{M}_p(\mathbb{K})$. (4)

(4) On a $E = F \oplus G$ avec $G = \operatorname{Vect}(e_{p+1}, \ldots, e_n)$ et en notant p la projection sur G parallèlement à F, $p \circ u_{|G}$ induit un endomorphisme de G encore noté $p \circ u_{|G}$. En posant $\mathscr{B}_G = (e_{p+1}, \ldots, e_n)$ on a $C = \operatorname{mat}_{\mathscr{B}_G}(p \circ u_{|G})$.

☞ En posant $M = \operatorname{mat}_{\mathscr{B}} u$, on a $M = [m_{ij}]$ avec $m_{ij} = e_i^*(u(e_j))$ où $(e_i^*)_{1 \leqslant i \leqslant n}$ est la base duale de $(e_i)_{1 \leqslant i \leqslant n}$ (m_{ij} est la $i^{\text{ème}}$ coordonnée de $u(e_j)$) sur la base $\mathscr{B}$.
F est stable par u si et seulement si $\forall j \in [\![1, p]\!], u(e_j) \in \operatorname{Vect}(e_1, \ldots, e_p)$ c'est-à-dire :

$$\forall j \in [\![1, p]\!], \forall i \in [\![p+1, n]\!], e_i^*(u(e_j)) = 0$$

ou encore : $\forall j \in [\![1, p]\!], \forall i \in [\![p+1, n]\!], m_{ij} = 0.$

Propriété 1

Dans les conditions du théorème 2, il existe une base $\mathscr{B}$ de E sur laquelle la matrice de u : $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ est **triangulaire par blocs**. On a alors :

$$\det u = \det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det A \times \det C.$$

☞ Posons $M = \begin{pmatrix} A & B \\ (0) & C \end{pmatrix}$, $P = \begin{pmatrix} A & (0) \\ (0) & I_{n-p} \end{pmatrix}$, $Q = \begin{pmatrix} I_r & B \\ (0) & I_{n-p} \end{pmatrix}$, $R = \begin{pmatrix} I_p & (0) \\ (0) & C \end{pmatrix}$

où (0) représente la matrice nulle de $\mathscr{M}_{n-p,p}(\mathbb{K})$ ou $\mathscr{M}_{p,n-p}(\mathbb{K})$ suivant le cas.

Copyrighted material

On vérifie que $M = RQP$ et, par suite, $\det M = \det P \cdot \det Q \cdot \det R$.

Q est triangulaire supérieure, d'élément diagonaux égaux à 1 d'où $\det Q = 1$.

En développant $\det P$, $n-p$ fois par rapport à la dernière colonne, il vient $\det P = \det A$, et en développant $\det R$, p fois par rapport à la première colonne, on a de même $\det R = \det C$. Finalement :

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

Exemple 1 $M = \begin{pmatrix} 1 & 0 & 2 & 0 \\ 2 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_4(\mathbb{R})$ est semblable à une matrice de la forme $N = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ avec $A \in \mathcal{M}_2(\mathbb{R})$.

Soit E un $\mathbb{R}$-espace vectoriel, $\dim E = 4$, rapporté à une base $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant 4}$ et $u \in \mathcal{L}(E)$ tel que $M = \operatorname{mat}_{\mathcal{B}} u$. Par lecture de la matrice, on a $u(e_2) = e_2 + e_4$ et $u(e_4) = -e_2 + e_4$. Donc $F = \text{Vect}\,(e_2, e_4)$ est stable par u, et d'après le théorème 2, sur la base $\mathcal{B}' = (e_2, e_4, e_1, e_3)$, la matrice de u a la forme souhaitée.

En effet, $u(e_2) = e_2 + e_4$. $u(e_4) = -e_2 + e_4$ donne
$u(e_1) = 2e_2 + e_4 + e_1 - e_3$. $u(e_3) = e_4 + 2e_1 + e_3$

$$\operatorname{mat}_{\mathcal{B}'} u = \begin{pmatrix} 1 & -1 & 2 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & -1 & 1 \end{pmatrix} = N.$$

La matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$ est $P = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, c'est la matrice de la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ donc telle que $P^{-1} = {}^tP$.

Ainsi $N = P^{-1}MP = {}^tPMP$ et N se déduit de M en effectuant la permutation σ sur les lignes puis sur les colonnes (ou inversement).

2.2 – Somme directe de sous-espaces stables

Théorème 3

Soit $F_1, \ldots, F_p$ des sous-espaces vectoriels de E, supplémentaires tels que :

$$\forall i \in [\![1, p]\!], \dim F_i = n_i \geqslant 1,$$

et $\mathcal{B}$ une base de E adaptée à la somme directe $E = \bigoplus_{i=1}^{p} F_i$.

Alors chaque F_i, $1 \leqslant i \leqslant p$, est stable par $u \in \mathcal{L}(E)$ si et seulement si $\operatorname{mat}_{\mathcal{B}} u$ est de la forme $\begin{pmatrix} A_1 & & (0) \\ & A_2 & \\ (0) & & \ddots \\ & & & A_p \end{pmatrix}$ où $\forall i \in [\![1, p]\!], A_i \in \mathcal{M}_{n_i}(\mathbb{K})$. ✎(5)

✎(5) Justification analogue à celle du théorème 2.

Propriété 2

Dans les conditions du théorème 3, la matrice de u dans la base $\mathcal{B}$ est dite **diagonale par blocs**. On a alors :

$$\det u = \det \begin{pmatrix} A_1 & & (0) \\ & A_2 & \\ (0) & & \ddots \\ & & & A_p \end{pmatrix} = \prod_{i=1}^{p} \det A_i .$$

Copyrighted material

☞ Le résultat est une évidence pour $p = 1$ et il est vrai pour $p = 2$ d'après la propriété 1. Supposons-le vrai pour $p \geqslant 2$.

Soit alors $M = \begin{bmatrix} A_1 & & \\ & \ddots & (0) \\ (0) & & A_{p+1} \end{bmatrix}$ une matrice diagonale par blocs, avec $p+1$ blocs.

D'après la propriété 1, on a

$$\det M = \det A_{p+1} \cdot \begin{pmatrix} A_1 & & \\ & \ddots & (0) \\ (0) & & A_p \end{pmatrix}$$

puis, avec l'hypothèse de récurrence : $\det M = \prod_{i=1}^{p+1} \det A_i$.

Ainsi la propriété est héréditaire et elle est donc vraie pour tout $p \in \mathbb{N}^*$.

B. Polynômes d'un endomorphisme

1. Puissances d'un endomorphisme

Définition 3

Soit $u \in \mathscr{L}(E)$. On définit les puissances u^n de u, où $n \in \mathbb{N}$, par récurrence en posant :

$$u^0 = \mathrm{Id}_E \quad , \quad \forall n \in \mathbb{N},\ u^{n+1} = u \circ u^n.$$

Propriété 3

$\forall u \in \mathscr{L}(E), \forall (p, q) \in \mathbb{N}^2,\ u^p \circ u^q = u^q \circ u^p = u^{p+q}$.

Propriété 4

Noyaux itérés d'un endomorphisme

Soit $u \in \mathscr{L}(E)$.

a) La suite $\left(\operatorname{Ker} u^p\right)_{p \in \mathbb{N}}$ est croissante : $\operatorname{Ker} u^p \subset \operatorname{Ker} u^{p+1}$

b) Si l'ensemble $\{p \in \mathbb{N} / \operatorname{Ker} u^p = \operatorname{Ker} u^{p+1}\}$ n'est pas vide, il admet un plus petit élément n, appelé **indice de** u. On a alors :

$$\forall q \in \mathbb{N}.\ \operatorname{Ker} u^{n+q} = \operatorname{Ker} u^n \quad , \quad \forall q \in [\![0, n-1]\!],\ \operatorname{Ker} u^{q+1} \neq \operatorname{Ker} u^q.$$

c) Si E est de dimension finie, l'existence de n, indice de u, est assurée et $n \leqslant \dim E$.

☞ a) Résulte de l'implication : $u^p(x) = 0 \ \Rightarrow \ u^{p+1}(x) = u\left[u^p(x)\right] = 0$.

b) Par définition de n, on a : $\operatorname{Ker} u^{n+1} = \operatorname{Ker} u^n$, d'où pour $q \in \mathbb{N}$:

$x \in \operatorname{Ker} u^{n+q+1} \ \Rightarrow \ u^q(x) \in \operatorname{Ker} u^{n+1} \ \Rightarrow \ u^q(x) \in \operatorname{Ker} u^n \ \Rightarrow \ x \in \operatorname{Ker} u^{n+q}$.

Il en résulte $\operatorname{Ker} u^{n+q+1} \subset \operatorname{Ker} u^{n+q}$ donc, d'après a), $\operatorname{Ker} u^{n+q+1} = \operatorname{Ker} u^{n+q}$ puis par récurrence :

$$\forall q \in \mathbb{N},\ \operatorname{Ker} u^{n+q} = \operatorname{Ker} u^n.$$

c) S'il existe $p \in \mathbb{N}$ tel que $\operatorname{Ker} u^{p+1} \neq \operatorname{Ker} u^p$, alors, pour tout $q \leqslant p$:

$$\operatorname{Ker} u^{q+1} \neq \operatorname{Ker} u^q \ \text{ d'où } \ \dim \operatorname{Ker} u^{q+1} \geqslant 1 + \dim \operatorname{Ker} u^q.$$

De $u^0 = \mathrm{Id}_E$, on déduit $\dim \operatorname{Ker} u^0 = 0$ et, par récurrence $p \leqslant \dim \operatorname{Ker} u^p \leqslant \dim E$.

L'ensemble $\left\{p \in \mathbb{N} / \operatorname{Ker} u^{p+1} \neq \operatorname{Ker} u^p\right\}$ est fini, son nombre d'éléments est, par définition, l'indice n de u, il est majoré par la dimension de E.

Copyrighted material

Remarques

1) Si $u \in \mathcal{L}(E)$ est nilpotent, l'indice n de u existe, c'est le plus petit entier p tel que $\operatorname{Ker} u^p = E$.

2) Pour $E = \mathbb{R}[X]$ et u l'endomorphisme de E défini par $u(P) = P'$ (polynôme dérivé de P), on a : $\forall p \in \mathbb{N}^*$, $\operatorname{Ker} u^p = \mathbb{R}_{p-1}[X]$. L'endomorphisme u n'a pas d'indice.

2. Polynômes d'un endomorphisme

Définition 4

Pour $u \in \mathcal{L}(E)$ et $P \in \mathbb{K}[X]$, $P = \sum_{k=0}^{n} a_k X^k$, on pose $P(u) = \sum_{k=0}^{n} a_k u^k$ et on dit que $P(u)$ est un **polynôme de l'endomorphisme** u.

Propriété 5

$u \in \mathcal{L}(E)$ étant fixé, l'ensemble noté $\mathbb{K}[u]$ des polynômes de l'endomorphisme u est une sous-algèbre commutative de $\mathcal{L}(E)$.

☞ Par définition, on a $\mathbb{K}[u] = \varphi_u\big[\mathbb{K}[X]\big]$ où φ_u est l'application définie par :

$$\varphi_u : \mathbb{K}[X] \to \mathcal{L}(E),\ P \mapsto P(u).$$

Vérifions que φ_u est linéaire, c'est-à-dire que :

$$\forall (P, Q) \in \mathbb{K}[X]^2, \forall (\lambda, \mu) \in \mathbb{K}^2,\ \big(\lambda P + \mu Q\big)(u) = \lambda P(u) + \mu Q(u) \qquad \textbf{(1)}$$

Pour tous polynômes P, Q il existe $n \in \mathbb{N}$ tel que $P = \sum_{k=0}^{n} a_k X^k$, $Q = \sum_{k=0}^{n} b_k X^k$ ✎(6)

et on obtient alors $\big(\lambda P + \mu Q\big)(u) = \sum_{k=0}^{n} \big(\lambda a_k + \mu b_k\big) u^k = \lambda P(u) + \mu Q(u)$ d'où **(1)**.

Par définition des polynômes en u, on a $1(u) = \mathrm{Id}_E$ c'est-à-dire $\varphi_u(1) = \mathrm{Id}_E$. **(2)**

Vérifions que $\forall (P, Q) \in \mathbb{K}[X]^2, (PQ)(u) = P(u) \circ Q(u)$. **(3)**

En effet, on a $PQ = \sum_{k=0}^{n} \sum_{\ell=0}^{n} a_k b_\ell X^{k+\ell}$ donc $(PQ)(u) = \sum_{k=0}^{n} \sum_{\ell=0}^{n} a_k b_\ell u^{k+\ell}$ et d'après les règles de calcul dans l'algèbre $\mathcal{L}(E)$:

$$P(u) \circ Q(u) = \sum_{k=0}^{n} a_k u^k \circ \sum_{\ell=0}^{n} b_\ell u^\ell = \sum_{k=0}^{n} \sum_{\ell=0}^{n} a_k b_\ell u^{k+\ell} \quad \text{d'où } \textbf{(3)}.$$

Les propositions **(2)** et **(3)** montrent que φ_u est un morphisme d'anneaux. En conséquence, φ_u étant linéaire, $\operatorname{Im} \varphi_u$ est un sous-espace vectoriel de $\mathcal{L}(E)$ et puisque c'est un morphisme d'anneaux. $\operatorname{Im} \varphi_u$ est un sous-anneau de $\mathcal{L}(E)$ donc, finalement, $\mathbb{K}[u] = \operatorname{Im} \varphi_u$ est une sous-algèbre de $\mathcal{L}(E)$.

Enfin, la commutativité de $\mathbb{K}[X]$ donne celle de $\mathbb{K}[u]$ puisque $PQ = QP$ donne :

$$(PQ)(u) = (QP)(u) \quad \text{c'est-à-dire} \quad P(u) \circ Q(u) = Q(u) \circ P(u).$$

✎(6) Si $(P,Q) \neq (0,0)$ il suffit de poser $n = \max(\deg P, \deg Q)$.

Propriété 6

$u \in \mathcal{L}(E)$ étant fixé, l'ensemble noté $\mathcal{I}(u)$ des polynômes $P \in \mathbb{K}[X]$ tels que $P(u) = 0$ est un idéal de $\mathbb{K}[X]$ appelé **idéal annulateur de** u.

☞ $\mathcal{I}(u)$ est un idéal de $\mathbb{K}[X]$ puisque c'est le noyau du morphisme d'anneaux φ_u.

Propriété 7

Lorsque $\mathcal{I}(u) \neq \{0\}$, il existe un polynôme unitaire M_u unique tel que : ✎(7)

$$\mathcal{I}(u) = M_u\,\mathbb{K}[X] = \big\{M_u P \,|\, P \in \mathbb{K}[X]\big\}.$$

On dit que M_u est le **polynôme minimal de** u.

✎(7) Cela tient au fait que $\mathbb{K}[X]$ est un anneau principal.

Copyrighted material

Propriété 8

Si E est de dimension finie, tout endomorphisme u de E admet un polynôme minimal.

☞ Si $\dim E = n$, on a $\dim \mathcal{L}(E) = n^2$.
La famille $\left(u^k\right)_{0 \leqslant k \leqslant n^2}$ est donc liée et il existe $n^2 + 1$ scalaires α_k, $0 \leqslant k \leqslant n^2$, non tous nuls, tels que $\sum_{k=0}^{n^2} \alpha_k u^k = 0$. En conséquence, en posant $P = \sum_{k=0}^{n^2} \alpha_k X^k$, on a $P \neq 0$ et $P \in \mathcal{I}(u)$ donc $\mathcal{I}(u) \neq 0$.

3. Décomposition des noyaux

u est un endomorphisme de E

Théorème 4

Soit $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]$ et $D = A \wedge B$. [8] On a alors :

$$\operatorname{Ker} A(u) \cap \operatorname{Ker} B(u) = \operatorname{Ker} D(u).$$

[8] PGCD de A et B.

☞ Il existe deux polynômes A_1 et B_1 tels que $A = DA_1$ et $B = DB_1$. Alors :

$$A(u) = A_1(u) \circ D(u) \text{ donc } \operatorname{Ker} D(u) \subset \operatorname{Ker} A(u),$$
$$B(u) = B_1(u) \circ D(u) \text{ donc } \operatorname{Ker} D(u) \subset \operatorname{Ker} B(u).$$

Finalement $\operatorname{Ker} D(u) \subset \operatorname{Ker} A(u) \cap \operatorname{Ker} B(u)$. **(1)**

$D = A \wedge B$ donne l'existence de deux polynômes P et Q tels que $D = AP + BQ$, donc

$$D(u) = P(u) \circ A(u) + Q(u) \circ B(u) \text{ et } \operatorname{Ker} A(u) \cap \operatorname{Ker} B(u) \subset \operatorname{Ker} D(u). \quad \textbf{(2)}$$

(1) et **(2)** donnent la conclusion.

Théorème 5

a) Soit $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que $A \wedge B = 1$. Alors :

$$\operatorname{Ker}(AB)(u) = \operatorname{Ker} A(u) \oplus \operatorname{Ker} B(u).$$

b) Soit $A_1, A_2, \ldots, A_n$ n éléments de $\mathbb{K}[X]$ deux à deux premiers entre eux alors :

$$\operatorname{Ker}\left(A_1 A_2 \cdots A_n\right)(u) = \bigoplus_{i=1}^{n} \operatorname{Ker} A_i(u).$$

☞ a) Pour $D = 1$, on a $D(u) = \mathrm{Id}_E$ donc $\operatorname{Ker} D(u) = \{0\}$.
Du théorème 4, on déduit alors que la somme $\operatorname{Ker} A(u) + \operatorname{Ker} B(u)$ est directe.
Les inclusions $\operatorname{Ker} A(u) \subset \operatorname{Ker}(AB)(u)$ et $\operatorname{Ker} B(u) \subset \operatorname{Ker}(AB)(u)$ sont conséquences de $(AB)(u) = B(u) \circ A(u) = A(u) \circ B(u)$ d'où :

$$\operatorname{Ker} A(u) \oplus \operatorname{Ker} B(u) \subset \operatorname{Ker}(AB)(u). \quad \textbf{(1)}$$

Le théorème de Bézout donne l'existence de deux polynômes P et Q tels que $AP + BQ = 1$ d'où $\mathrm{Id}_E = A(u) \circ P(u) + B(u) \circ Q(u)$ et $\forall x \in E,\ x = A(u) \circ P(u)(x) + B(u) \circ Q(u)(x)$.
Lorsque $x \in \operatorname{Ker}(AB)(u)$, on a :

$$x_1 = A(u) \circ P(u)(x) \in \operatorname{Ker} B(u) \text{ et } x_2 = B(u) \circ Q(u)(x) \in \operatorname{Ker} A(u).$$

En effet, $B(u)(x_1) = B(u) \circ A(u) \circ P(u)(x) = P(u) \circ (AB)(u)(x) = 0$, et de même $A(u)(x_2) = 0$. On en déduit :

$$\operatorname{Ker}(AB)(u) \subset \operatorname{Ker} A(u) \oplus \operatorname{Ker} B(u). \quad \textbf{(2)}$$

Finalement : $\operatorname{Ker}(AB)(u) = \operatorname{Ker} A(u) \oplus \operatorname{Ker} B(u)$ d'après **(1)** et **(2)**.

b) Remarquons que, pour tout $p \in \{1, 2, \ldots, n-1\}$, on a $\left(A_1 A_2 \cdots A_p\right) \wedge A_{p+1} = 1$, donc, en utilisant le a), on obtient par récurrence que :

$$\operatorname{Ker}\left(A_1 A_2 \cdots A_n\right)(u) = \bigoplus_{i=1}^{n} \operatorname{Ker} A_i(u).$$

Copyrighted material

Théorème 6

a) Soit $(A, B) \in \mathbb{K}[X] \times \mathbb{K}[X]$ tel que $A \wedge B = 1$ et $(AB)(u) = 0$. Alors :

$$E = \operatorname{Ker} A(u) \oplus \operatorname{Ker} B(u).$$

b) Soit $A_1, A_2, \ldots, A_n$ n éléments de $\mathbb{K}[X]$ deux à deux premiers entre eux et tels que $(A_1 A_2 \cdots A_n)(u) = 0$. Alors : $E = \bigoplus_{i=1}^{n} \operatorname{Ker} A_i(u)$.

☞ a) $\operatorname{Ker}(AB)(u) = E$.

b) $\operatorname{Ker}(A_1 A_2 \cdots An)(u) = E$. Ce résultat est donc un corollaire du théorème 5.

Exemple 2 Si E est un $\mathbb{C}$-espace vectoriel et $u \in \mathscr{L}(E)$ tel que $u^3 = \mathrm{Id}_E$, il existe trois sous-espaces F_1, F_2 et F_3 de E, stables par u, tels que $E = F_1 \oplus F_2 \oplus F_3$ et la restriction u_i de u à chaque F_i est une homothétie.

On a ici $X^3 - 1 = (X-1)(X-j)(X-j^2) \in \mathscr{I}(u)$.

$X-1, X-j, X-j^2$ sont premiers entre eux deux à deux. Donc, d'après le théorème 6 :

$$E = \operatorname{Ker}(u - \mathrm{Id}_E) \oplus \operatorname{Ker}(u - j\,\mathrm{Id}_E) \oplus \operatorname{Ker}(u - j^2\,\mathrm{Id}_E).$$

$F_1 = \operatorname{Ker}(u - \mathrm{Id}_E)$, $F_2 = \operatorname{Ker}(u - j\,\mathrm{Id}_E)$ et $F_3 = \operatorname{Ker}(u - j^2\,\mathrm{Id}_E)$ sont stables par u car $u - \mathrm{Id}_E$, $u - j\,\mathrm{Id}_E$ et $u - j^2\,\mathrm{Id}_E$ sont permutables avec u.

$u_1 = u_{F_1}$ est l'identité de F_1

$u_2 = u_{F_2}$ est l'homothétie de rapport j

$u_3 = u_{F_3}$ est l'homothétie de rapport j^2.

C. Éléments propres d'un endomorphisme

Définition 5

Valeurs propres, spectre

Soit $u \in \mathscr{L}(E)$. $\lambda \in \mathbb{K}$ est valeur propre de u si et seulement si $u - \lambda\,\mathrm{Id}_E$ est non injectif, c'est-à-dire s'il existe $x \in E$, $x \neq 0$, $u(x) = \lambda x$.

Le spectre de $u \in \mathscr{L}(E)$, noté $\mathrm{Sp}(u)$, est l'ensemble des valeurs propres de u.

Définition 6

Vecteurs propres, sous-espace propre

$x \in E$ est vecteur propre de $u \in \mathscr{L}(E)$ si et seulement si $x \neq 0$ et il existe $\lambda \in \mathbb{K}$, tel que $u(x) = \lambda x$. ✎(9)

Pour $u \in \mathscr{L}(E)$ et $\lambda \in \mathrm{Sp}(u)$, le sous-espace propre de u associé à la valeur propre λ est le sous-espace $E_u(\lambda) = \operatorname{Ker}(u - \lambda e)$.

✎(9) Alors $\lambda \in \mathrm{Sp}(u)$.

Remarque

Si $\lambda \notin \mathrm{Sp}(u)$, on a $\operatorname{Ker}(u - \lambda\,\mathrm{Id}_E) = \{0\}$ que l'on note encore $E_u(\lambda)$.

Propriété 9

Soit $u \in \mathscr{L}(E)$ et $x \in E$, $x \neq 0$.

La droite $D = \mathrm{Vect}(x)$ est stable par u si et seulement si x est vecteur propre de u.

Copyrighted material

Propriété 10

Soit $u \in \mathcal{L}(E)$ et $(\lambda_i)_{1 \leqslant i \leqslant n}$ une famille finie de valeurs propres de u deux à deux distinctes.
Alors, la somme des sous-espaces propres associés : $E_u(\lambda_i) = \operatorname{Ker}(u - \lambda_i \operatorname{Id}_E)$ est directe.

☞ Démonstration par récurrence sur n.

- La propriété est vraie pour $n = 2$.

En effet, si $x \in E_u(\lambda_1) \cap E_u(\lambda_1)$, on a $u(x) = \lambda_1 x = \lambda_2 x$, donc :

$$(\lambda_1 - \lambda_2)x = 0 \text{ et } x = 0 \text{ car } \lambda_1 - \lambda_2 \neq 0.$$

Ainsi $E_u(\lambda_1) \cap E_u(\lambda_2) = \{0\}$ et $E_u(\lambda_1) + E_u(\lambda_2) = E_u(\lambda_1) \oplus E_u(\lambda_2)$.

- Supposons la propriété vraie pour $n \geqslant 2$.

Soit $(\lambda_i)_{1 \leqslant i \leqslant n+1}$ une famille de $n+1$ valeurs propres deux à deux distinctes.

Si $x \in E_u(\lambda_{n+1}) \cap \sum_{i=1}^{n} E_u(\lambda_i)$, on a $u(x) = \lambda_{n+1} x$, et il existe :

$$(x_1, \ldots, x_n) \in \prod_{i=1}^{n} E_u(\lambda_i) \text{ tel que } x = \sum_{i=1}^{n} x_i \text{ donc } u(x) = \sum_{i=1}^{n} \lambda_i x_i .$$

On en déduit $\sum_{i=1}^{n} (\lambda_i - \lambda_{n+1}) x_i = 0$ et la somme $\sum_{i=1}^{n} E_u(\lambda_i)$ étant directe d'après l'hypothèse de récurrence, il en résulte :

$$\forall i \in [\![1, n]\!], (\lambda_i - \lambda_{n+1}) x_i = 0 \text{ donc } \forall i \in [\![1, n]\!], x_i = 0 \text{ (car } \lambda_i - \lambda_{n+1} \neq 0).$$

Finalement $x = 0$. En posant $F = \bigoplus_{i=1}^{n} E_u(\lambda_i)$, on a ainsi $F + E_u(\lambda_{n+1}) = F \oplus E_u(\lambda_{n+1})$, d'où enfin :

$$\sum_{i=1}^{n+1} E_u(\lambda_i) = \bigoplus_{i=1}^{n+1} E_u(\lambda_i).$$

Corollaire 1

Pour λ et μ dans $\operatorname{Sp}(u)$, $\lambda \neq \mu \Rightarrow E_u(\lambda) \cap E_u(\mu) = \{0\}$. ✎(10)

✎(10) Un vecteur propre est associé à une seule valeur propre.

Corollaire 2

Si $(x_1, \ldots, x_n)$ est une famille de vecteurs propres associés à des valeurs propres deux à deux distinctes de u, cette famille est libre.

Propriété 11

Soit $u \in \mathcal{L}(E)$ et $v \in \mathcal{L}(E)$ tels que $v \circ u = u \circ v$.
Alors, tout sous-espace propre de l'un est stable par l'autre.

☞ C'est une conséquence de $v \circ (u - \lambda \operatorname{Id}_E) = (u - \lambda \operatorname{Id}_E) \circ v$ et du théorème 1.

Propriété 12

Soit $u \in \mathcal{L}(E)$ et $\lambda \in \operatorname{Sp}(u)$. Alors :

a) $\forall P \in \mathbb{K}[X]$, $P(\lambda) \in \operatorname{Sp}(P(u))$;

b) $\forall k \in \mathbb{N}$, $\lambda^k \in \operatorname{Sp}(u^k)$;

c) si $v = u - \alpha \operatorname{Id}_E$ avec $\alpha \in \mathbb{K}$, on a :

$$\lambda \in \operatorname{Sp}(u) \iff \lambda - \alpha \in \operatorname{Sp}(v) \text{ et } E_u(\lambda) = E_v(\lambda - \alpha).$$

Copyrighted material

☞ a) $P(X)-P(\lambda)$ est divisible par $X-\lambda$: $P(X)-P(\lambda)=(X-\lambda)Q(X)$, $Q(X)\in\mathbb{K}[X]$, donc :
$P(u)-P(\lambda)\,\mathrm{Id}_E = Q(u)\circ\left(u-\lambda\,\mathrm{Id}_E\right)$ et $\mathrm{Ker}\left(u-\lambda\,\mathrm{Id}_E\right)\subset\mathrm{Ker}\left(P(u)-P(\lambda)\,\mathrm{Id}_E\right)$.
Ainsi $\mathrm{Ker}(u-\lambda\,\mathrm{Id}_E)\neq\{0\}\ \Rightarrow\ \mathrm{Ker}\left(P(u)-P(\lambda)\,\mathrm{Id}_E\right)\neq\{0\}$.

b) On applique le a) avec $P(X)=X^k$.

c) Il suffit de remarquer que $u-\lambda\,\mathrm{Id}_E=v-(\lambda-\alpha)\,\mathrm{Id}_E$.

Propriété 13

Soit $u\in\mathcal{L}(E)$ et $P\in\mathbb{K}[X]$ tel que $P(u)=0$. Alors, $\mathrm{Sp}(u)\subset\left\{\lambda\in\mathbb{K},\ P(\lambda)=0\right\}$.

☞ Le spectre de l'endomorphisme nul est réduit à $\{0\}$ et $P(u)=0$, donc :
$$\lambda\in\mathrm{Sp}(u)\ \Rightarrow\ P(\lambda)\in\{0\}.$$ (11)

(11) C'est un corollaire de la propriété 12.

Corollaire

Si $u\in\mathcal{L}(E)$ est nilpotent, alors $\mathrm{Sp}(u)=\{0\}$.

☞ Il existe $p\in\mathbb{N}^*$ tel que $u^p=0$ donc $P(u)=0$ avec $P=X^p$ et la propriété 13 donne :
$$\mathrm{Sp}(u)\subset\{0\}.$$
D'autre part, $\mathrm{Ker}\,u\neq\{0\}$ donne $0\in\mathrm{Sp}(u)$ d'où finalement $\mathrm{Sp}(u)=\{0\}$.

Propriété 14

Soit $u\in\mathcal{L}(E)$.

a) On a $E_u(0)=\mathrm{Ker}\,u$. (12)

b) Si x est un vecteur propre associé à une valeur propre non nulle, alors $x\in\mathrm{Im}\,u$. (13)

(12) Définition de $E_u(0)$.

(13) $u(x)=\lambda x$ avec $\lambda\neq 0$ donne $x=\frac{1}{\lambda}u(x)$.

Propriété 15

Soit $u\in\mathrm{GL}(E)$. Alors 0 n'est pas valeur propre et $\mathrm{Sp}\left(u^{-1}\right)=\left\{\frac{1}{\lambda}\ \middle|\ \lambda\in\mathrm{Sp}(u)\right\}$. (14)

(14) Si E est de dimension finie, $u\in\mathcal{L}(E)$ est inversible si et seulement si $0\notin\mathrm{Sp}(u)$.

☞ On a $\mathrm{Ker}\,u=\{0\}$ donc $0\notin\mathrm{Sp}(u)$. Alors :
$$\lambda\in\mathrm{Sp}\left(u^{-1}\right)\iff\exists x\in E\setminus\{0\},\ u^{-1}(x)=\lambda x$$
$$\iff\exists x\in E\setminus\{0\},\ \frac{1}{\lambda}x=u(x)$$

Propriété 16

Soit $u\in\mathcal{L}(E)$, $F\neq\{0_E\}$ un sous-espace vectoriel de E stable par u et $v=u_F$ l'endomorphisme de F induit par u.
On a alors $\mathrm{Sp}(v)\subset\mathrm{Sp}(u)$ avec, pour tout $\lambda\in\mathrm{Sp}(v)$:
$$\mathrm{Ker}\left(v-\lambda\,\mathrm{Id}_F\right)=F\cap\mathrm{Ker}\left(u-\lambda\,\mathrm{Id}_E\right).$$

☞ Pour tout $\lambda\in K$, on a :
$$\begin{aligned}\mathrm{Ker}\left(v-\lambda\,\mathrm{Id}_F\right)&=\left\{x\in F\ /\ v(x)=\lambda x\right\}\\&=\left\{x\in F\ /\ u(x)=\lambda x\right\}\\&=F\cap\mathrm{Ker}\left(u-\lambda\,\mathrm{Id}_E\right).\end{aligned}$$
Donc $\mathrm{Ker}\left(v-\lambda\,\mathrm{Id}_F\right)\neq\{0\}\ \Rightarrow\ \mathrm{Ker}\left(u-\lambda\,\mathrm{Id}_E\right)\neq\{0\}$ ce qui prouve que $\mathrm{Sp}(v)\subset\mathrm{Sp}(u)$.

Propriété 17

Étant donné $a\in\mathrm{GL}(E)$, l'application :
$$I_a\ :\ \mathcal{L}(E)\to\mathcal{L}(E),\quad u\mapsto a\circ u\circ a^{-1}$$
est un automorphisme de la $\mathbb{K}$-algèbre $\mathcal{L}(E)$ dit **automorphisme intérieur** associé à a.

Copyrighted material

☞ On vérifie successivement :

- I_a est une bijection car : $\forall v \in \mathscr{L}(E),\ I_a(u) = v \iff u = a^{-1} \circ v \circ a$.
- I_a est linéaire : $I_a(\lambda u + \mu v) = \lambda I_a(u) + \mu I_a(v)$.
- I_a est un morphisme d'anneaux : $I_a(u \circ v) = I_a(u) \circ I_a(v)$.

Propriété 18

Étant donné $a \in GL(E)$ et $u \in \mathscr{L}(E)$, soit $v = a \circ u \circ a^{-1}$ l'image de u par l'automorphisme intérieur I_a. On a alors $\mathrm{Sp}(u) = \mathrm{Sp}(v)$ et pour tout $\lambda \in \mathbb{K}$:

$$E_v(\lambda) = a\big(E_u(\lambda)\big).$$

☞ Soit $x \in E$ et $\lambda \in \mathbb{K}$, on a :

$$\begin{aligned} x \in E_v(\lambda) &\iff a \circ u \circ a^{-1}(x) = \lambda x \\ &\iff u \circ a^{-1}(x) = \lambda a^{-1}(x) \\ &\iff a^{-1}(x) \in E_u(\lambda) \\ &\iff x \in a\big(E_u(\lambda)\big) \end{aligned}$$

Donc $E_v(\lambda) = a\big(E_u(\lambda)\big)$ et puisque a est un automorphisme de E, $E_v(\lambda)$ est non réduit à $\{0\}$ si et seulement si $E_u(\lambda)$ est non réduit à $\{0\}$, c'est-à-dire que $\lambda \in \mathrm{Sp}(v)$ équivaut à $\lambda \in \mathrm{Sp}(u)$.

Exemple 3 Éléments propres de $u \in \mathscr{L}(E)$: les cas usuels.

a) u est une homothétie : $u = \lambda\,\mathrm{Id}_E$, $\lambda \in \mathbb{K}$, $\mathrm{Ker}\,(u - \lambda\,\mathrm{Id}_E) = E$ et $E \neq \{0\}$, donc λ est valeur propre de u.

$P = X - \lambda$ étant annulateur de u, d'après la propriété 13, la seule valeur propre possible de u est λ et finalement : $\mathrm{Sp}(u) = \{\lambda\}$.

b) u est un projecteur avec $u \neq 0$ et $u \neq \mathrm{Id}_E$. On a ici $u^2 - u = 0$ donc $X^2 - X$ est annulateur de u et, d'après la propriété 13, $\mathrm{Sp}\,u \subset \{0, 1\}$.

Puisque u est un projecteur, on a $\mathrm{Ker}\,u = \mathrm{Im}\,(u - \mathrm{Id}_E)$ et $\mathrm{Ker}\,(u - \mathrm{Id}_E) = \mathrm{Im}\,u$. Donc $u \neq \mathrm{Id}_E$ donne $\mathrm{Ker}\,u \neq \{0\}$ et $0 \in \mathrm{Sp}(u)$ puis, $u \neq 0$ donne $\mathrm{Ker}\,(u - \mathrm{Id}_E) \neq \{0\}$ et $1 \in \mathrm{Sp}(u)$.

Finalement, $\mathrm{Sp}\,u = \{0, 1\}$ et, comme on sait que pour un projecteur $E = \mathrm{Im}\,u \oplus \mathrm{Ker}\,u$, on a ici $E = E_u(0) \oplus E_u(1)$.

c) u est une symétrie avec $u \neq \mathrm{Id}_E$ et $u \neq -\mathrm{Id}_E$.

On a $u^2 = \mathrm{Id}_E$ donc $X^2 - 1$ est annulateur de u et, avec la propriété 13, il vient :

$$\mathrm{Sp}(u) \subset \{-1, 1\}.$$

Soit v le projecteur associé à la symétrie u : $v = \dfrac{u + \mathrm{Id}_E}{2}$ donc $u = P(v)$ avec $P = 2X - 1$.

Les conditions $u \neq \mathrm{Id}_E$ et $u \neq -\mathrm{Id}_E$ donnent $v \neq \mathrm{Id}_E$ et $v \neq 0$.

Donc, d'après 2), on a $\mathrm{Sp}(v) = \{0, 1\}$ et en utilisant la propriété 12 on obtient :

$$P(0) \in \mathrm{Sp}(u) \text{ et } P(1) \in \mathrm{Sp}(u), \text{ c'est-à-dire } \{-1, 1\} \subset \mathrm{Sp}(u).$$

Finalement $\mathrm{Sp}(u) = \{-1, 1\}$;

$$E_u(1) = \mathrm{Ker}(u - \mathrm{Id}_E) = \mathrm{Ker}(v - \mathrm{Id}_E) = \mathrm{Im}\,v\,;$$

$$E_u(-1) = \mathrm{Ker}(u + \mathrm{Id}_E) = \mathrm{Ker}(v).$$

d) u est une affinité différente d'une homothétie.

Dans ce cas, il existe un projecteur v tel que $u = \lambda\,\mathrm{Id}_E + (1 - \lambda)v$ donc : $u = P(v)$ avec $P = (1 - \lambda)X + \lambda$.

Puisque u n'est pas une homothétie, on a $v \neq 0$, $v \neq \mathrm{Id}_E$ et $\lambda \neq 1$ donc $\mathrm{Sp}(v) = \{0, 1\}$ et la propriété 12 donne :

$$P(0) \in \mathrm{Sp}(u) \text{ et } P(1) \in \mathrm{Sp}(u) \text{ c'est-à-dire } \{\lambda, 1\} \subset \mathrm{Sp}(u).$$

Avec $\lambda \neq 1$ et $u - \lambda\,\mathrm{Id}_E = (1 - \lambda)v$ on obtient $\mathrm{Ker}\,(u - \lambda\,\mathrm{Id}_E) = \mathrm{Ker}\,v$, de même $u - \mathrm{Id}_E = (1 - \lambda)\big(v - \mathrm{Id}_E\big)$ donne $\mathrm{Ker}\,(u - \mathrm{Id}_E) = \mathrm{Ker}\,(v - \mathrm{Id}_E) = \mathrm{Im}\,v$, d'où finalement : $\mathrm{Sp}(u) = \{\lambda, 1\}$, $E_u(\lambda) = \mathrm{Ker}\,v$, $E_u(1) = \mathrm{Im}\,v$.

Copyrighted material

Exemple 4 Éléments propres d'un endomorphisme de rang 1

Si $u \in \mathscr{L}(E)$ est de rang 1, il existe $a \in E \setminus \{0\}$ et une forme linéaire φ non nulle tels que $\forall x \in E,\ u(x) = \varphi(x)a$. Alors $\operatorname{Im} u = \operatorname{Vect}(a)$. Le seul sous-espace propre associé à une valeur propre non nulle est donc $\operatorname{Vect} a$ (associé à la valeur propre $\varphi(a)$).

Conséquence

Si $\dim E = 1$, $\operatorname{Sp} u = \{\varphi(a)\}$, $E_u\big(\varphi(a)\big) = E$.

Si $\dim E > 1$, $\operatorname{Sp} u = \{0, \varphi(a)\}$, $E_u(0) = \operatorname{Ker}\varphi$, $E_u\big(\varphi(a)\big) = \operatorname{Vect} a$.

Exemple 5 E étant un $\mathbb{R}$-espace vectoriel, étude de $\operatorname{Sp}(u)$ où $u \in \mathscr{L}(E)$ tel que $u^2 = -\operatorname{Id}_E$.

Remarquons qu'il existe de tels endomorphismes, par exemple dans $\mathbb{R}^2$, u défini par :

$$(x, y) \mapsto (y, -x).$$

On a ici $X^2 + 1 \in \mathscr{I}(u)$, donc, par application de la propriété 13, $\operatorname{Sp}(u) = \varnothing$ car $X^2 + 1$ n'a pas de racine dans $\mathbb{R}$.

Exemple 6 Avec $E = \mathbb{K}[X]$, éléments propres de $u \in \mathscr{L}(E)$ défini par $u(P) = XP' - P$.

Si $\lambda \in \mathbb{K}$ est valeur propre de u, il existe $P = \sum_{k=0}^{n} a_k X^k$, $(a_n \neq 0)$, tel que $XP' = (\lambda + 1)P$.

On en déduit $na_n = (\lambda + 1)a_n$ d'où $\lambda = n - 1$ (car $a_n \neq 0$) : $\lambda \in \mathbb{N} \cup \{-1\}$, puis :

$$\forall k \in [\![0, n-1]\!],\ ka_k = na_k \text{ d'où } a_k = 0 \text{ et ainsi } P = a_n X^n.$$

Réciproquement, il est immédiat que $\forall\, \lambda \in \mathbb{N} \cup \{-1\},\ P_\lambda = X^{\lambda+1}$ est vecteur propre de u associé à la valeur propre λ. Ainsi $\operatorname{Sp} u = \mathbb{N} \cup \{-1\}$ et $\forall\, \lambda \in \operatorname{Sp} u,\ E_u(\lambda) = \operatorname{Vect}\left(X^{\lambda+1}\right)$.

D. Réduction en dimension finie

1. Éléments propres d'une matrice carrée

Définition 7

Soit $A \in \mathcal{M}_n(\mathbb{K})$; les éléments propres de A (valeurs propres, vecteurs propres) sont les éléments propres de $u \in \mathscr{L}(\mathbb{K}^n)$ canoniquement associé à A.

Conséquences

- $\forall\, \lambda \in \mathbb{K},\ \lambda \in \operatorname{Sp}(A) \iff \exists X \in \mathcal{M}_{n,1}(\mathbb{K}),\ X \neq 0,\ AX = \lambda X$.
- Identifions $\mathcal{M}_{n,1}(\mathbb{K})$ et $\mathbb{K}^n$. [15] $X \in \mathcal{M}_{n,1}(\mathbb{K})$ est vecteur propre de A équivaut à
$$X \neq 0 \text{ et } \exists\, \lambda \in \mathbb{K},\ AX = \lambda X.$$
- Étant donné $P \in \mathrm{GL}_n(K)$ et $B = PAP^{-1}$, on a $\operatorname{Sp}(A) = \operatorname{Sp}(B)$.

[15] Isomorphisme défini au moyen de leurs bases canoniques

2. Polynôme caractéristique

Théorème 7

Soit $A \in \mathcal{M}_n(\mathbb{K})$. $\det(A - XI_n)$ est un polynôme de degré n.

☞ $A - XI_n$ est une matrice à coefficients dans $\mathbb{K}(X)$. [16]

Posons $A = \big[a_{ij}\big]$, $A - XI_n = \big[p_{ij}(X)\big]$: $p_{ij}(X) = a_{ij}$ si $i \neq j$, $p_{ii}(X) = a_{ii} - X$. Alors :

$$\det\big(A - XI_n\big) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon_\sigma p_{1\sigma(1)} p_{2\sigma(2)} \cdots p_{n\sigma(n)}.$$

[16] Corps des fractions à coefficients dans $\mathbb{K}$.

Copyrighted material

Si $\sigma \neq \mathrm{Id}_{[\![1,n]\!]}$, $\prod_{i=1}^{n} p_{i\sigma(i)}(X)$ est un polynôme de degré $\leqslant n-1$.

Pour $\sigma = \mathrm{Id}_{[\![1,n]\!]}$, $\prod_{i=1}^{n} p_{i\sigma(i)}(X) = \prod_{i=1}^{n}(a_{ii} - X)$ est un polynôme de degré n et de coefficient dominant $(-1)^n$.

$\det(A - XI)$ est donc un polynôme de degré n et de coefficient dominant $(-1)^n$.

Propriété 19

Si A et B sont semblables, on a : $\det\left(A - XI_n\right) = \det\left(B - XI_n\right)$.

☞ Si A et B sont semblables, il existe $P \in \mathrm{GL}_n(\mathbb{K})$, $B = P^{-1}AP$, alors :
$\det\left(B - XI_n\right) = \det\left(P^{-1}\left(A - XI_n\right)P\right) = \det P^{-1} \det\left(A - XI_n\right) \det P = \det\left(A - XI_n\right)$.

Définition 8

Le **polynôme caractéristique** de $A \in \mathcal{M}_n(\mathbb{K})$ est $\chi_A(X) = \det\left(A - XI_n\right)$.

Définition 9

Soit $u \in \mathcal{L}(E)$, $\mathcal{B}$ une base de E et $A = \mathrm{mat}_{\mathcal{B}}\, u$, le polynôme $\chi_u(X) = \det\left(A - XI_n\right)$ est indépendant de la base $\mathcal{B}$ choisie. ✎(17) C'est le **polynôme caractéristique** de u.

✎(17) Il dépend de u seul.

Si $\mathcal{B}'$ est une autre base de E et $A' = \mathrm{mat}_{\mathcal{B}'}\, u$, A et A' sont semblables, donc, d'après la propriété 19, $\det\left(A - XI_n\right) = \det\left(A' - XI_n\right)$.

Théorème 8

Soit $u \in \mathcal{L}(E)$ (resp. $A \in \mathcal{M}_n(\mathbb{K})$) et $\lambda \in \mathbb{K}$. λ est valeur propre de u (resp. de A) si et seulement si λ est racine du polynôme caractéristique.

$$\lambda \in \mathrm{Sp}\, u \iff \mathrm{Ker}\left(u - \lambda\, \mathrm{Id}_E\right) \neq \{0\} \iff \det\left(u - \lambda\, \mathrm{Id}_E\right) = 0.$$

Propriété 20

Soit $u \in \mathcal{L}(E)$, (resp. $A \in \mathcal{M}_n(\mathbb{K})$).
$\chi_u(X)$ (resp. $\chi_A(X)$) est un polynôme de degré n.

- Le coefficient dominant est $(-1)^n$.
- Le coefficient de X^{n-1} est $(-1)^{n-1}\,\mathrm{Tr}\, u$ (resp. $(-1)^{n-1}\,\mathrm{Tr}\, A$).
- Le terme constant est $\det u$ (resp. $\det A$).

$$\chi_u(X) = (-1)^n X^n + (-1)^{n-1}\,\mathrm{Tr}\, u \cdot X^{n-1} + \ldots + \det u.$$

Propriété 21

$A \in \mathcal{M}_n(\mathbb{K})$: $\chi_A = \chi_{{}^tA}$.

☞ $\chi_{{}^tA}(X) = \det\left({}^tA - XI_n\right) = \det\, {}^t\left(A - XI_n\right) = \det\left(A - XI_n\right) = \chi_A(X)$.

Propriété 22

Soit $u \in \mathcal{L}(E)$, F un sous-espace de E stable par u, et $v \in \mathcal{L}(F)$ l'endomorphisme de F induit par u : $v = u_F$. Alors χ_v divise χ_u.

☞ Soit $\mathcal{B} = (e_1, e_2, \ldots, e_n)$ une base de E obtenue en complétant une base $\mathcal{B}_F = (e_1, \ldots, e_p)$ de F ; $(e_{p+1}, \ldots, e_n)$ est une base de G supplémentaire de F.

Copyrighted material

Alors $\mathrm{mat}_{\mathcal{B}} u = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} \in \mathcal{M}_n(\mathbb{K})$ avec $A = \mathrm{mat}_{\mathcal{B}_F} v \in \mathcal{M}_p(\mathbb{K})$, donc :

$$\chi_u(X) = \det \begin{pmatrix} A - XI_p & B \\ 0 & C - XI_{n-p} \end{pmatrix} = \det\left(A - XI_p\right) \cdot \det\left(C - XI_{n-p}\right)$$

soit : $$\chi_u(X) = \chi_v(X) \cdot \det\left(C - XI_{n-p}\right).$$

Théorème 9

Soit $u \in \mathcal{L}(E)$ (resp. $A \in \mathcal{M}_n(\mathbb{K})$).

Si $\lambda \in \mathbb{K}$ est **valeur propre de u (resp. de A) d'ordre m**, [18] alors $1 \leqslant \dim E_u(\lambda) \leqslant m$.

[18] C'est-à-dire que λ est racine d'ordre de multiplicité m de χ_u (resp. de χ_A).

☞
- λ valeur propre de u donne $E_u(\lambda) \neq \{0\}$ et donc $\dim E_u(\lambda) \geqslant 1$.
- La restriction v de u à $E_u(\lambda)$ est l'application $x \mapsto \lambda x$ de matrice λI_p (avec $p = \dim E_u(\lambda)$) dans toute base de $E_u(\lambda)$, donc $\chi_v = (\lambda - X)^p$. $E_u(\lambda)$ étant stable par u, on déduit de la propriété 22 que $(\lambda - X)^p$ divise χ_u et donc que $m \geqslant p$.

Remarque importante

Si u est un endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie, son polynôme caractéristique a au moins une racine.

Conséquence : le spectre de u est non vide et u admet au moins un vecteur propre.

3. Diagonalisation

Définition 10

$u \in \mathcal{L}(E)$ est **diagonalisable** si et seulement si il existe une base de E dans laquelle la matrice de u est diagonale, c'est-à-dire si et seulement si il existe une base $\mathcal{B} = \left(e_i\right)_{1 \leqslant i \leqslant n}$ de E formée de vecteurs propres de u. [19]

[19] Alors $\mathrm{mat}_{\mathcal{B}} u = \mathrm{diag}(\lambda_1, \cdots, \lambda_n)$ où, pour tout $i \in [\![1, n]\!]$, λ_i est la valeur propre associée au vecteur propre e_i.

Théorème 10

Étant donné $u \in \mathcal{L}(E)$, les propositions suivantes sont équivalentes :

(1) u est diagonalisable ;

(2) E est somme directe de sous-espaces vectoriels $E_1, E_2, \cdots, E_p$ stables par u tels que chaque endomorphisme induit u_{F_i} soit une homothétie ;

(3) E est somme directe de sous-espaces vectoriels $\left(E_i\right)_{1 \leqslant i \leqslant p}$ et il existe $\left(\lambda_i\right)_{1 \leqslant i \leqslant p} \in \mathbb{K}^p$ tel que, π_i étant la projection sur E_i parallèlement à $\bigoplus_{\substack{1 \leqslant j \leqslant p \\ j \neq i}} E_j$, on ait $u = \sum_{i=1}^{p} \lambda_i \pi_i$.

☞ **(1) ⇒ (2)**

u étant diagonalisable, il existe $\mathcal{B} = \left(e_i\right)_{1 \leqslant i \leqslant n}$ base de E formée de vecteurs propres de u.

En posant $E_i = \mathrm{Vect}\left(e_i\right)$, $1 \leqslant i \leqslant n$, on a $E = \bigoplus_{i=1}^{n} E_i$, chaque E_i est stable par u, et u_{F_i} est l'homothétie de rapport λ_i valeur propre associée à e_i.

(2) ⇒ (1)

u_{F_i} étant l'homothétie de rapport λ_i, tout vecteur non nul de E_i est vecteur propre de u associé à la valeur propre λ_i.

Une base de E, adaptée à la somme directe $E = \bigoplus_{i=1}^{p} E_i$, est donc formée de vecteurs propres de u.

Copyrighted material

(2) ⇒ (3)

Si $\mathcal{B}$ est une base de E adaptée à la somme directe $E = \bigoplus_{i=1}^{p} E_i$ on a en posant $m_i = \dim E_i$:

$$\mathrm{mat}_{\mathcal{B}}\, u = \begin{pmatrix} \lambda_1 I_{m_1} & & & (0) \\ & \lambda_2 I_{m_2} & & \\ & & \ddots & \\ (0) & & & \lambda_p I_{m_p} \end{pmatrix}$$

En observant que $\mathrm{mat}_{\mathcal{B}}\, \pi_i = \begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & I_{m_i} & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}$ il vient $u = \sum_{i=1}^{p} \lambda_i \pi_i$.

(3) ⇒ (2)

Chaque E_i est stable par chaque π_j [20] donc est stable par u.

De plus, si $x \in E_i$, on a $\pi_j(x) = 0$ si $j \neq i$ et $\pi_i(x) = x$ donc $u(x) = \lambda_i x$ et u_{E_i} est l'homothétie de rapport λ_i.

[20] $\pi_j(E_i) = \{0\}$ si $i \neq j$, $\pi_j(E_j) = E_j$.

Théorème 11

Étant donné $u \in \mathcal{L}(E)$, les propositions suivantes sont équivalentes :

(1) u est diagonalisable ;

(2) E est somme directe des sous-espaces propres de u ;

(3) le polynôme caractéristique χ_u est scindé dans $\mathbb{K}[X]$ et, pour toute valeur propre λ, on a $\dim E_u(\lambda) = m$, où m est l'ordre de multiplicité de λ.

(1) ⇒ (2)

Posons $\mathrm{Sp}(u) = \{\mu_1, \mu_2, \ldots, \mu_p\}$, $F = \bigoplus_{i=1}^{p} E_u(\mu_i)$, $\forall i \in [\![1, p]\!]$, $q_i = \dim E_u(\mu_i)$. [21]

Si $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ est une base de E formée de vecteurs propres de u, $(e_i)_{1 \leqslant i \leqslant n}$ est une famille libre de F, donc $\dim F \geqslant n$ et finalement $F = E$.

[21] L'hypothèse indique que $\mathrm{Sp}(u)$ n'est pas vide.

(2) ⇒ (1)

Les sous-espaces propres de u forment une famille $(E_i)_{1 \leqslant i \leqslant p}$ de sous-espaces supplémentaires dans E tels que chaque restriction u_{E_i} soit une homothétie. [22]

[22] Donc u est diagonalisable d'après le théorème 10.

(2) ⇒ (3)

Soit u_i l'endomorphisme de $E_u(\mu_i)$ induit par u, u_i est l'homothétie $x \mapsto \mu_i x$.

On a $\chi_{u_i} = (\mu_i - X)^{q_i}$ et χ_{u_i} divise χ_u (propriété 22).

Les χ_{u_i} étant premiers entre eux deux à deux, $\prod_{i=1}^{p} \chi_{u_i}$ divise χ_u.

D'autre part **(2)** donne $\sum_{i=1}^{p} q_i = n$ donc $\deg \prod_{i=1}^{p} \chi_{u_i} = n = \deg \chi_u$.

De plus, ces deux polynômes ont le même coefficient dominant $(-1)^n$, donc :

$$\chi_u = \prod_{i=1}^{p} \chi_{u_i} = \prod_{i=1}^{p} (\mu_i - X)^{q_i} \quad \text{ce qui montre (3).}$$

Copyrighted material

(3) ⇒ (2)

D'après **(3)**, on a $\chi_u = \prod_{i=1}^{p} (\mu_i - X)^{q_i}$ avec $q_i = \dim E_u(\mu_i)$.

Alors $n = \deg \chi_u = \sum_{i=1}^{p} q_i = \sum_{i=1}^{p} \dim E_u(\mu_i) = \dim F$, donc $E = F$.

Théorème 12

Soit $u \in \mathcal{L}(E)$, u est diagonalisable si et seulement si il existe un polynôme Q scindé dans $\mathbb{K}[X]$ n'admettant que des racines simples et tel que $Q(u) = 0$.

(23) On conserve les notations de la démonstration précédente.

(23)

- Si u est diagonalisable, il existe une base $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ de E formée de vecteurs propres de u et on a $\chi_u = \prod_{i=1}^{p} (\mu_i - X)^{q_i}$. Posons alors $Q = \prod_{i=1}^{p} (\mu_i - X)$. Il vient :

$$Q(u) = (\mu_1 \operatorname{Id}_E - u) \circ (\mu_2 \operatorname{Id}_E - u) \circ \cdots \circ (\mu_p \operatorname{Id}_E - u),$$

ces termes étant permutables. Soit x vecteur propre associé à la valeur propre μ_i. On a :

$$Q(u)(x) = \prod_{\substack{j=1 \\ j \neq i}}^{p} (\mu_j \operatorname{Id}_E - u) \circ (\mu_i \operatorname{Id}_E - u)(x) = 0.$$

Ainsi, pour tout $i \in [\![1, n]\!]$, $Q(u)(e_i) = 0$ et donc $Q(u) = 0$.

- S'il existe $Q = \prod_{i=1}^{p} (\mu_i - X)$ avec les μ_i deux à deux distincts, tel que $Q(u) = 0$, d'après le théorème 6 (décomposition des noyaux), on a $E = \bigoplus_{i=1}^{p} \operatorname{Ker}(\mu_i \operatorname{Id}_E - u)$ et u est diagonalisable d'après la proposition (2) du théorème 11.

Corollaire 1

Soit $u \in \mathcal{L}(E)$, u est diagonalisable si et seulement si son polynôme minimal est scindé dans $\mathbb{K}[X]$ et n'admet que des racines simples.

Théorème 13

Pour que $u \in \mathcal{L}(E)$ soit diagonalisable, il suffit que χ_u admette n racines simples dans $\mathbb{K}$.

χ_u est alors scindé et, d'après le théorème 9, on a, pour toute valeur propre λ, $1 \leqslant \dim E_u(\lambda) \leqslant 1$, donc $\dim E_u(\lambda) = 1$ et la conclusion résulte du théorème 11-(3).

Définition 11

$A \in \mathcal{M}_n(\mathbb{K})$ est dite **diagonalisable** si et seulement si l'endomorphisme de $\mathbb{K}^n$ qui lui est canoniquement associé est diagonalisable.

Propriété 23

Une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable si et seulement si il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}AP$ soit diagonale. (24)

Alors, $P^{-1}AP = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ où les λ_i sont les valeurs propres de A.

(24) Une matrice carrée est diagonalisable si et seulement si elle est semblable à une matrice diagonale.

P est la matrice de passage de la base canonique de $\mathbb{K}^n$ à une base de vecteurs propres.

Copyrighted material

4. Pratique de la diagonalisation

$$u \in \mathcal{L}(E). \quad A = \mathrm{mat}_{\mathcal{B}}\, u \in \mathcal{M}_n(\mathbb{K}).$$

1) Calculer $\chi_u = \chi_A$ et factoriser dans $\mathbb{K}[X]$.

2) ▪ **Si χ_A n'est pas scindé dans $\mathbb{K}[X]$**, A et donc u n'est pas diagonalisable.
▪ **Si χ_A est scindé dans $\mathbb{K}[X]$**, on détermine les sous-espaces propres.
Pour $\lambda \in \mathrm{Sp}\, u$, $E_u(\lambda)$ est défini par le système homogène $(A - \lambda I_n)X = 0$, donc :
$$\dim E_u(\lambda) = n - \mathrm{rg}\,(A - \lambda I_n).$$
Si λ est valeur propre simple, on sait que $\dim E_u(\lambda) = 1$, donc $\mathrm{rg}\,(A - \lambda I_n) = n - 1$.

3) Si, pour tout $\lambda \in \mathrm{Sp}\, u$, $\dim E_u(\lambda) = m$ (ordre de multiplicité de λ), [25] u et A sont diagonalisables et on obtient une base de E formée de vecteurs propres de u en «réunissant» des bases des $E_u(\lambda)$.

[25] Ce qui est réalisé si toutes les valeurs propres sont simples.

Remarques

1) Si λ est valeur propre d'ordre n, la matrice A n'est diagonalisable que si $A = \lambda I_n$.

2) Si λ est valeur propre d'ordre $n-1$ et A diagonalisable, alors $\mathrm{rg}\,(A - \lambda I_n) = 1$. [26]

[26] Dans ce cas, le sous-espace propre correspondant est un hyperplan.

3) Si λ est valeur propre simple, la matrice $A - \lambda I_n$ est de rang $n-1$. On en cherche le noyau ; celui-ci peut s'obtenir directement [27] en exhibant une combinaison linéaire nulle des vecteurs colonnes de $A - \lambda I_n$.

[27] Sans former le système homogène.

4) Le polynôme caractéristique d'une matrice carrée d'ordre 2 ou 3 peut s'écrire sans l'aide des déterminants.
$$n = 2 \ : \ \chi_A(X) = X^2 - (\mathrm{Tr}\, A)X + \det A$$
$$n = 3 \ : \ \chi_A(X) = -X^3 + (\mathrm{Tr}\, A)X^2 - \mathrm{Tr}(\mathrm{Com}\, A)X + \det A.$$ [28]

[28] On peut utiliser cette méthode à titre de vérification.

5) Pour $A \in \mathcal{M}_n(\mathbb{K})$ et $B = A + \alpha I_n$, $(\alpha \in \mathbb{K})$, on a $\chi_B(X) = \chi_A(X - \alpha)$ et :
$$\forall P \in \mathrm{GL}_n(\mathbb{K}),\ P^{-1}BP = P^{-1}AP + \alpha I_n$$
Les matrices A et B ont les mêmes vecteurs propres, elles sont simultanément diagonalisables ou non.

Exemple 7 Pour quelles valeurs des paramètres réels a, b, c, d, e, f les matrices suivantes sont-elles diagonalisables dans $\mathcal{M}_4(\mathbb{R})$?
$$A = \begin{pmatrix} 1 & a & b & c \\ 0 & 2 & d & e \\ 0 & 0 & 2 & f \\ 0 & 0 & 0 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 2 & f \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

▪ $\chi_A(X) = (1 - X)(2 - X)^3$.

1 est valeur propre simple donc $\dim E_A(1) = 1$.

2 est valeur propre triple, A sera donc diagonalisable dans $\mathcal{M}_4(\mathbb{R})$ si et seulement si :
$$\dim E_A(2) = 3 \text{ c'est-à-dire si et seulement si } \mathrm{rg}(A - 2I_4) = 1.$$
$$A - 2I_4 = \begin{pmatrix} -1 & a & b & c \\ 0 & 0 & d & e \\ 0 & 0 & 0 & f \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \mathrm{rg}(A - 2I_4) = 1 \iff d = e = f = 0.$$
Dans ce cas, $E_A(2)$ est l'hyperplan d'équation $x - ay - bz - ct = 0$.

▪ $\chi_B(X) = (1 - X)^2(2 - X)^2$.

1 et 2 sont valeurs propres doubles, B sera donc diagonalisable si et seulement si :
$$\dim E_B(1) = \dim E_B(2) = 2 \text{ c'est-à-dire si et seulement si } \mathrm{rg}(B - I_4) = \mathrm{rg}(B - 2I_4) = 2.$$
$$B - I_4 = \begin{pmatrix} 0 & a & b & c \\ 0 & 0 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathrm{rg}(B - I_4) = 2 \iff a = 0.$$

Copyrighted material

$$B - 2I_4 = \begin{pmatrix} -1 & a & b & c \\ 0 & -1 & d & e \\ 0 & 0 & 0 & f \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \operatorname{rg}(B - 2I_4) = 2 \iff f = 0.$$

Exemple 8 Soit E un $\mathbb{R}$-espace vectoriel de dimension finie. Alors $f \in \mathcal{L}(E)$ tel que :

(1) : $(f - \mathrm{Id}_E)^3 \circ (f + 2\,\mathrm{Id}_E) = 0$; **(2)** : $(f - \mathrm{Id}_E)^2 \circ (f + 2\,\mathrm{Id}_E) \neq 0$ n'est pas diagonalisable.

De **(1)**, on déduit que $\mathrm{Sp}(f) \subset \{1, -2\}$ (cf. propriété 13).

Si f était diagonalisable, on aurait $(f - \mathrm{Id}_E) \circ (f + 2\,\mathrm{Id}_E) = 0$ [29] donc on aurait aussi $(f - \mathrm{Id}_E)^2 \circ (f + 2\,\mathrm{Id}_E) = 0$. Ainsi f est non diagonalisable.

[29] Démonstration du théorème 12.

Exemple 9 $A \in \mathcal{M}_n(\mathbb{C})$ telle que $A^3 - A^2 - 4A + 4I = 0$ est diagonalisable.

La relation donnée s'écrit $P(A) = 0$ avec $P(X) = X^3 - X^2 - 4X + 4 = (X - 1)(X + 2)(X - 2)$.

La transcription matricielle du théorème 12 donne immédiatement que A est diagonalisable :

$$\mathrm{Sp}(A) \subset \{-2, 1, 2\}.$$

Restriction d'un endomorphisme diagonalisable à un sous-espace stable

Théorème 14

Soit $u \in \mathcal{L}(E)$, $F \neq \{0\}$ un sous-espace vectoriel de E stable par u et v l'endomorphisme de F induit par u. Si u est diagonalisable, $v = u_F$ est également diagonalisable.

D'après le théorème 12, u étant diagonalisable, il existe $Q \in \mathbb{K}[X]$ scindé et n'admettant que des racines simples tel que $Q(u) = 0$.

$Q(u) = 0$ donne $Q(v) = 0$ et, [30] v est diagonalisable.

[30] Toujours d'après le théorème 12.

Corollaire

Soit $u \in \mathcal{L}(E)$, diagonalisable, et F un sous-espace non nul de E. Alors, F est stable par u si et seulement si F admet une base formée de vecteurs propres de u.

Exemple 10 Détermination des sous-espaces de $\mathbb{R}^3$ stables par l'endomorphisme canoniquement associé à :

$$A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

$\chi_A(X) = X(X - 1)(2 - X)$: [31] donc A est diagonalisable dans $\mathcal{M}_3(\mathbb{R})$.

[31] A admet trois valeurs propres simples.

Sous-espaces propres :

$E_A(0)$ Équations : $\begin{cases} x + y - z = 0 \\ x + y + z = 0 \end{cases}$ Base : $c_1 = (1, -1, 0)$

$E_A(1)$ Équations : $\begin{cases} y - z = 0 \\ x + z = 0 \end{cases}$ Base : $c_2 = (-1, 1, 1)$

$E_A(2)$ Équations : $\begin{cases} -x + y - z = 0 \\ x + y - z = 0 \end{cases}$ Base : $c_3 = (0, 1, 1)$

D'après le corollaire du théorème 14 :

- les droites stables sont $D_i = \mathrm{Vect}(c_i)$, $i \in \{1, 2, 3\}$;
- les plans stables sont $P_1 = \mathrm{Vect}(c_2, c_3)$, $P_2 = \mathrm{Vect}(c_1, c_3)$, $P_3 = \mathrm{Vect}(c_1, c_2)$.

En adjoignant $\{0\}$ et $\mathbb{R}^3$, on a ainsi tous les sous-espaces stables.

5. Trigonalisation

Définition 12

$u \in \mathcal{L}(E)$ est dit **trigonalisable** si et seulement si il existe une base de E dans laquelle la matrice de u est triangulaire.

Copyrighted material

Remarque

Soit $\mathcal{B} = (e_1, e_2, \dots, e_n)$ une base de E et $\mathcal{B}' = (e_n, e_{n-1}, \dots, e_1)$.

Si $\mathrm{mat}_{\mathcal{B}} u$ est triangulaire supérieure, $\mathrm{mat}_{\mathcal{B}'} u$ est triangulaire inférieure. [32]

[32] Conséquence : $u \in \mathcal{L}(E)$ est trigonalisable si et seulement si il existe une base dans laquelle sa matrice est triangulaire supérieure.

Théorème 15

$u \in \mathcal{L}(E)$ est trigonalisable si et seulement si χ_u [33] est scindé dans $\mathbb{K}[X]$.

Lorsque $\mathbb{K} = \mathbb{C}$, tout endomorphisme de E est donc trigonalisable.

[33] Polynôme caractéristique de u.

☞ ▪ Condition nécessaire

S'il existe $\mathcal{B} = (e_1, \dots, e_n)$ telle que :

$$\mathrm{mat}_{\mathcal{B}} u = \begin{pmatrix} t_{11} & \cdots & t_{n1} \\ (0) & \ddots & \vdots \\ & & t_{nn} \end{pmatrix}, \quad \text{alors} \quad \chi_u(X) = \prod_{i=1}^{n} (t_{ii} - X).$$

▪ Condition suffisante

Soit $\mathcal{P}(n)$ la propriété : pour tout $\mathbb{K}$-espace vectoriel E de dimension n et tout endomorphisme u de E, si $\chi_u(X)$ est scindé, u est trigonalisable.

Supposons $\mathcal{P}(n-1)$ vraie. Soit alors E un $\mathbb{K}$-espace vectoriel de dimension n et $u \in \mathcal{L}(E)$ tel que $\chi_u(X)$ soit scindé. $\chi_u(X)$ admet au moins une racine $\lambda \in \mathbb{K}$. [34]

Soit c_1 un vecteur propre de u associé à λ et $\mathcal{B} = (c_1, c_2', c_3', \dots, c_n')$ une base de E.

$$\mathrm{mat}_{\mathcal{B}} u = \begin{pmatrix} \lambda & L \\ 0_{n-1,1} & A \end{pmatrix}, L \in \mathcal{M}_{1,n-1}(\mathbb{K}), A \in \mathcal{M}_{n-1}(\mathbb{K})$$

donc $\chi_u(X) = (\lambda - X) \det\left(A - XI_{n-1}\right)$.

Soit $F = \mathrm{Vect}\left(c_2', c_3', \dots, c_n'\right)$, $v = u_{|F}$, p la projection sur F parallèlement à $\mathrm{Vect}\left(c_1\right)$ et $w = p \circ v$. On a $w \in \mathcal{L}(F)$ et $A = \mathrm{mat}_{(c_i')_{2 \leqslant i \leqslant n}} w$.

D'après $\mathcal{P}(n-1)$, il existe $(c_2, c_3, \dots, c_n)$ base de F telle que :

$$\mathrm{mat}_{(c_i)_{2 \leqslant i \leqslant n}} w = T \in \mathcal{M}_{n-1}(K) \text{ avec } T \text{ triangulaire supérieure.}$$

Il est maintenant immédiat que $\mathcal{B}' = (c_1, c_2, \dots, c_n)$ est une base de E.

Pour tout $i \in [\![2, n]\!]$, on a $u(c_i) = v(c_i) = p \circ v(c_i) + \alpha_i c_1$, $(\alpha_i \in \mathbb{K})$, soit :

$$u(c_i) = w(c_i) + \alpha_i c_1, \text{ donc } \mathrm{mat}_{\mathcal{B}'} u = \begin{pmatrix} \lambda & L' \\ 0_{n-1,1} & T \end{pmatrix} \text{ avec } L' = (\alpha_2, \alpha_3, \dots, \alpha_n),$$

$\mathrm{mat}_{\mathcal{B}'} u$ est triangulaire supérieure, ce qui montre que $\mathcal{P}(n)$ est vraie.

Par récurrence, [35] $\mathcal{P}(n)$ est donc vraie pour tout $n \in \mathbb{N}^*$.

[34] Une seule lorsque $\chi_u(X) = (\lambda - X)^n$.

[35] $\mathcal{P}(1)$ est évidemment vraie.

Définition 13

$A \in \mathcal{M}_n(\mathbb{K})$ est dite **trigonalisable** si et seulement si l'endomorphisme de $\mathbb{K}^n$ qui lui est canoniquement associé est trigonalisable.

Donc A est trigonalisable si et seulement si il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}AP$ soit triangulaire supérieure. [36]

[36] A est semblable à une matrice triangulaire supérieure.

Remarque

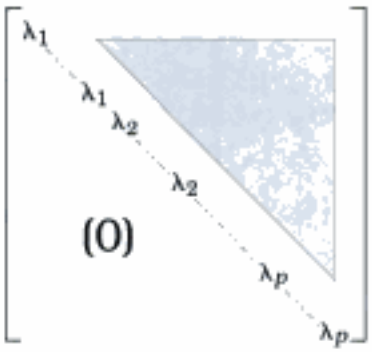
La démonstration du théorème 15 fournit une méthode pratique de trigonalisation :

1) on choisit une valeur propre λ et on détermine c_1 vecteur propre associé ;
2) on détermine $v = u_{|F}$ (notations de la démonstration) ;
3) on choisit μ valeur propre de v (donc de u) et on recommence l'opération.

Il en résulte que l'on peut construire T avec une diagonale ordonnée de façon arbitraire.

En particulier, si $\chi_u(X) = \prod_{i=1}^{p} \left(\lambda_i - X\right)^{m_i}$, $(\lambda_1, \dots, \lambda_p$ valeurs propres dinstinctes de u, d'ordres de multiplicité $m_1, m_2, \dots, m_p)$, on pourra toujours trouver T de la forme :

Copyrighted material



λ_1 figure m_1 fois
λ_2 figure m_2 fois
... ...
λ_p figure m_p fois

Exemple 11 Trigonalisation de $A = \begin{pmatrix} -2 & -1 & 2 \\ -15 & -6 & 11 \\ -14 & -6 & 11 \end{pmatrix}$.

On a $\chi_A(X) = (1-X)^3$: 1 est valeur propre triple, A n'est donc pas diagonalisable. [37]

[37] Sinon, on aurait $A = I_3$.

Soit $u \in \mathcal{L}(\mathbb{R}^3)$ tel que $A = \mathrm{mat}_{\mathcal{B}} u$ où $\mathcal{B} = (e_1, e_2, e_3)$ est la base canonique de $\mathbb{R}^3$.

$\mathrm{Ker}(u - \mathrm{Id}_E)$ est de dimension 1 : $\mathrm{Ker}(u - \mathrm{Id}_E) = \mathrm{Vect}(c_1)$ avec $c_1 = e_1 + e_2 + 2e_3$.

$\mathcal{B}' = (c_1, e_2, e_3)$ est une nouvelle base de $\mathbb{R}^3$.

$u(e_2) = -e_1 - 6e_2 - 6e_3 = -c_1 - 5e_2 - 4e_3$

$u(e_3) = 2e_1 + 11e_2 + 11e_3 = 2c_1 + 9e_2 + 7e_3$

$\mathrm{mat}_{\mathcal{B}'} u = \begin{pmatrix} 1 & -1 & 2 \\ 0 & -5 & 9 \\ 0 & -4 & 7 \end{pmatrix} = A'$.

Posons $F = \mathrm{Vect}(e_2, e_3)$, $v = u_{|F}$, $w = p \circ v$ où p est la projection sur F parallèlement à c_1.

On a $\mathrm{mat}_{(e_2,e_3)} w = \begin{pmatrix} -5 & 9 \\ -4 & 7 \end{pmatrix} = B$ puis $\chi_B(X) = (1-X)^2$. [38]

[38] Sans calcul car $\chi_A(X) = \chi_u(X) = (1-X)\,\chi_B(X)$.

On trouve $\mathrm{Ker}(w - \mathrm{Id}_F) = \mathrm{Vect}(c_2)$ avec $c_2 = 3e_2 + 2e_3$.

Dans la base (c_2, e_3) de F la matrice de w est triangulaire supérieure, de la forme $\begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$, donc dans la base $\mathcal{B}'' = (c_1, c_2, e_3)$ de $\mathbb{R}^3$ la matrice de u est triangulaire supérieure. [39]

[39] Démonstration du théorème 15.

On a alors :

$u(c_2) = 3u(e_2) + 2u(e_3) = c_1 + 3e_2 + 2e_3$ (d'après la matrice A')

$u(c_2) = c_1 + c_2$

$u(e_3) = 2c_1 + 9e_2 + 7e_3$ (d'après la matrice A')

$u(e_3) = 2c_1 + 3c_2 + e_3$

Finalement $\mathrm{mat}_{(c_1,c_2,c_3)} u = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} = T$ et $T = P^{-1}AP$ avec $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \\ 2 & 2 & 1 \end{pmatrix}$.

6. Le théorème de Cayley-Hamilton

Théorème 16

Soit E un $\mathbb{C}$-espace vectoriel de dimension $n \geqslant 1$. Pour tout $u \in \mathcal{L}(E)$, on a $\chi_u(u) = 0$.

☞ [40] χ_u est scindé dans $\mathbb{C}[X]$: $\chi_u = \prod_{i=1}^{n} (\lambda_i - X)$, donc :

$$\chi_u(u) = (\lambda_1 \mathrm{Id}_E - u) \circ (\lambda_2 \mathrm{Id}_E - u) \circ \ldots \circ (\lambda_n \mathrm{Id}_E - u).$$

[40] Il existe de nombreuses démonstrations de ce résultat. Aucune n'est exigible pour les concours.

u est trigonalisable : il existe une base $\mathcal{C} = (c_1, c_2, \ldots, c_n)$ telle que $\mathrm{mat}_{\mathcal{C}} u$ soit triangulaire supérieure :

$$\mathrm{mat}_{\mathcal{C}} u = [t_{ij}] \begin{cases} \forall i \in [\![1, n]\!], & t_{ii} = \lambda_i \\ \forall (i,j) \in [\![1, n]\!]^2, & i > j \Rightarrow t_{ij} = 0 \end{cases}$$

Pour tout $i \in [\![1, n]\!]$, posons $v_i = \lambda_i \mathrm{Id}_E - u$ et :

$$V_i = (\lambda_1 \mathrm{Id}_E - u) \circ (\lambda_2 \mathrm{Id}_E - u) \circ \ldots \circ (\lambda_i \mathrm{Id}_E - u) = v_1 \circ v_2 \circ \ldots \circ v_i.$$

Copyrighted material

Soit $\mathcal{P}(i)$ la propriété : $\forall j \in [\![1, i]\!],\ V_i(c_j) = 0$.

- $\mathcal{P}(1)$ est vraie : $V_1(c_1) = \lambda_1 c_1 - u(c_1) = 0$.
- Pour $i \in [\![2, n]\!]$, supposons $\mathcal{P}(i-1)$ vraie.

On a alors $V_i = V_{i-1} \circ v_i = v_i \circ V_{i-1}$ [41] donc :

pour $1 \leqslant j \leqslant i-1$, $V_i(c_j) = v_i\left(V_{i-1}(c_j)\right) = v_i(0) = 0$ d'après $\mathcal{P}(i-1)$;

pour $j = i$, avec $u(c_i) = \lambda_i c_i + \sum_{k=1}^{i-1} t_{k,i} c_k$, il vient $v_i(c_i) = -\sum_{k=1}^{i-1} t_{k,i} c_k$ puis :

$$V_i(c_i) = V_{i-1}\left(v_i(c_i)\right) = -\sum_{k=1}^{i-1} t_{k,i} V_{i-1}(c_k) = 0 \text{ d'après } \mathcal{P}(i-1).$$

Ainsi, on a montré que $\mathcal{P}(i)$ est vraie.

- Par récurrence, $\mathcal{P}(i)$ est donc vraie pour tout $i \in [\![1, n]\!]$.
- $\mathcal{P}(n)$ s'écrit $\forall i \in [\![1, n]\!],\ \chi_u(u)(c_i) = 0$, donc $\chi_u(u) = 0$.

[41] Calculs dans l'algèbre commutative $\mathbb{C}[u]$.

Corollaire

Pour tout $A \in \mathcal{M}_n(\mathbb{C})$, $\chi_A = \sum_{k=0}^{n} a_k X^k$ désignant le polynôme caractéristique de A, on a :

$$\chi_A(A) = \sum_{k=0}^{n} a_k A^k = 0.$$

Théorème 17

Pour tout endomorphisme u de E, $\mathbb{R}$-espace vectoriel [42] de dimension $n \geqslant 1$, on a :

$$\chi_u(u) = 0.$$

[42] Dans ce chapitre, on est limité, par le programme, à $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Corollaire

Pour toute matrice $A \in \mathcal{M}_n(\mathbb{R})$, on a $\chi_A(A) = 0$.

☞ $\mathcal{B} = (e_1, \ldots, e_n)$ étant une base de E, soit $A = \mathrm{mat}_{\mathcal{B}} u$ et soit $\overline{u}$ l'endomorphisme de $\mathbb{C}^n$ canoniquement associé à A. Le théorème 16 s'applique pour $\overline{u}$, d'après son corollaire on a donc $\chi_A(A) = 0$, ce qui donne aussi $\chi_u(u) = 0$.

Exemple 12 Soit E un $\mathbb{K}$-espace vectoriel de dimension $n \geqslant 1$ et $u \in \mathcal{L}(E)$. Alors, pour tout $p \in \mathbb{N}$, $u^p \in \mathrm{Vect}\left(\mathrm{Id}_E, u, u^2, \ldots, u^{n-1}\right)$. Application :

$$A = \begin{pmatrix} 2 & 0 & 4 \\ 3 & -4 & 12 \\ 1 & -2 & 5 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R}) \text{ et } p \in \mathbb{N}, \text{ écrire } A^p \text{ en combinaison linéaire de } I_3,\ A \text{ et } A^2.$$

- La division euclidienne de X^p par χ_u s'écrit : $X^p = \chi_u Q + R$, $\deg R < \deg \chi_u$. [43]

On en déduit $u^p = \chi_u(u) \circ Q(u) + R(u) = R(u)$ d'après le théorème de Cayley – Hamilton,

ou encore, en posant $R = \sum_{k=0}^{n-1} a_k X^k$: $u^p = \sum_{k=0}^{n-1} a_p u^k$.

- Dans l'exemple proposé : $\chi_A(X) = -X(X-1)(X-2)$.

La division euclidienne de X^p par $\chi_A(X)$ s'écrit $X^p = \chi_A(X)Q(X) + aX^2 + bX + c$.

On obtient : [44] $\begin{cases} 0 = c \\ 1 = a + b + c \\ 2^p = 4a + 2b + c \end{cases}$ d'où $\begin{cases} a = 2^{p-1} - 1 \\ b = 2 - 2^{p-1} \\ c = 0 \end{cases}$

et $A^p = \left(2^{p-1} - 1\right) A^2 + \left(2 - 2^{p-1}\right) A$.

[43] $\deg R \leqslant n-1$.

[44] En substituant successivement à X les valeurs 0, 1 et 2.

Copyrighted material

7. Une trigonalisation particulière

Théorème 18

Soit $u \in \mathscr{L}(E)$ dont le polynôme caractéristique χ_u est scindé dans $\mathbb{K}[X]$:

$$\chi_u = \prod_{i=1}^{p} (\lambda_i - X)^{m_i},$$

où $\lambda_1, \lambda_2, \ldots, \lambda_p$ sont les valeurs propres distinctes de u d'ordres de multiplicité respectifs $m_1, m_2, \ldots, m_p$. On pose $F_i = \operatorname{Ker}\left(u - \lambda_i \operatorname{Id}_E\right)^{m_i}$.

a) On a $E = \bigoplus_{i=1}^{p} F_i$ et chaque F_i est stable par u.

b) Pour tout $i \in [\![1, p]\!]$, l'endomorphisme u_i de F_i induit par u admet λ_i pour unique valeur propre. Il existe $\mathscr{B}_i$ base de F_i telle que $\operatorname{mat}_{\mathscr{B}_i} u_i = \lambda_i I_{n_i} + N_i$ où on a posé $n_i = \dim F_i$ et où $N_i \in \mathscr{M}_{n_i}(\mathbb{K})$ est triangulaire supérieure stricte.

c) Sur la base $\mathscr{B}$ de E, réunion des bases $\mathscr{B}_i$, $\operatorname{mat}_{\mathscr{B}} u$ à la forme suivante :

$$\begin{bmatrix} \lambda_1 & & & & \\ & \ddots & & (0) & \\ & & \lambda_1 & & \\ & & & \ddots & \\ & (0) & & & \lambda_p \\ & & & & \ddots \\ & & & & (0) \quad \lambda_p \end{bmatrix} = \begin{pmatrix} \lambda_1 I_{n_1} + N_1 & & (0) \\ & \ddots & \\ & & \lambda_p I_{n_p} + N_p \end{pmatrix}$$

☞ a) $\left(u - \lambda_i \operatorname{Id}_E\right)^{m_i}$ et u sont permutables car éléments de $\mathbb{K}[u]$, donc F_i est stable par u.

On a $E = \bigoplus_{i=1}^{p} F_i$ d'après les théorèmes de Cayley-Hamilton et de décomposition des noyaux.

b) En posant $u_i = u_{F_i}$, on a $\left(u_i - \lambda_i \operatorname{Id}_{F_i}\right)^{m_i} = 0$ donc $\left(X - \lambda_i\right)^{m_i}$ est annulateur de u_i ce qui impose $\operatorname{Sp}\left(u_i\right) \subset \left\{ \lambda_i \right\}$.

Or le polynôme caractéristique χ_{u_i} est scindé ✎(45) dans $\mathbb{K}[X]$ et ainsi $\operatorname{Sp}(u_i) = \lg\{\lambda_i\}$.

Sur une base $\mathscr{B}_i$ de F_i trigonalisant u_i, la matrice $\operatorname{mat}_{\mathscr{B}_i} u_i$ a donc la forme $\lambda_i I_{n_i} + N_i$.

c) Résulte évidemment de $E = \bigoplus_{i=1}^{p} F_i$ et b).

✎(45) Il divise χ_u.

Remarques

1) Les sous-espaces $\operatorname{Ker}\left(u - \lambda_i \operatorname{Id}_E\right)^{m_i}$ sont les **sous-espaces caractéristiques** de u.✎(46)

2) Les matrices N_i sont nilpotentes.

3) On peut montrer que pour tout i : $n_i = \dim \operatorname{Ker}\left(u - \lambda_i \operatorname{Id}_E\right)^{m_i} = m_i$.

✎(46) Leur étude est hors programme.

Exemple 13 Soit $A = \begin{pmatrix} 7 & 3 & -4 \\ -6 & -2 & 5 \\ 4 & 2 & -1 \end{pmatrix} \in \mathscr{M}_3(\mathbb{R})$. Montrons que A est semblable à : $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

On trouve $\chi_A(X) = (1 - X)^2(2 - X)$.

Copyrighted material

▪ **Sous-espaces propres**

Soit $f \in \mathcal{L}(\mathbb{R}^3)$ canoniquement associé à A :

$$\mathrm{mat}_{\mathcal{B}} f = A \quad , \quad \mathcal{B} = (e_1, e_2, e_3)$$

$$E_A(2) = \mathrm{Ker}\,(f - 2\,\mathrm{Id}_{\mathbb{R}^3}) = \mathrm{Vect}\,(c_1) \quad \text{avec} \quad c_1 = (1,1,2)$$
$$E_A(1) = \mathrm{Ker}\,(f - \mathrm{Id}_{\mathbb{R}^3}) = \mathrm{Vect}\,(c_2) \quad \text{avec} \quad c_2 = (-1,2,0)$$

On a ici $\dim E_A(1) < 2$, f et donc A n'est pas diagonalisable.

▪ **Trigonalisation**

Pour trouver une base de $\mathrm{Ker}\,(f - \mathrm{Id}_{\mathbb{R}^3})^2$, formons :

$$A - I_3 = \begin{pmatrix} 6 & 3 & -4 \\ -6 & -3 & 5 \\ 4 & 2 & -2 \end{pmatrix} \text{ et } (A - I_3)^2 = \begin{pmatrix} 2 & 1 & -1 \\ 2 & 1 & -1 \\ 4 & 2 & -2 \end{pmatrix}$$

On en déduit que $\mathrm{Ker}\,(f - \mathrm{Id}_{\mathbb{R}^3})^2$ est le plan d'équation $2x + y - z = 0$.

Une base de ce plan est (c_2, c_3) avec $c_3 = (0,1,1)$. Par construction, on a :

$$f(c_1) = 2c_1, \quad f(c_2) = c_2, \quad \text{et } f(c_3) = f(e_2 + e_3) = -e_1 + 3e_2 + e_3 = c_2 + c_3.$$

Ainsi, avec $P = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 1 \\ 2 & 0 & 1 \end{pmatrix}$, il vient $P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

E. Applications de la réduction

1. Puissance $p^{\text{ème}}$ d'une matrice ou d'un endomorphisme

1.1 – Utilisation du théorème de Cayley–Hamilton

Soit $A \in \mathcal{M}_n(\mathbb{K})$. Il existe $(Q, R) \in \mathbb{K}[X]^2$ tel que $X^p = \chi_A(X)Q(X) + R(X)$, $\deg R < n$. [47]

On a $\chi_A(A) = 0$. [48] D'où $A^p = R(A) = \sum_{k=0}^{n-1} a_k A^k$ où on a posé $R(X) = \sum_{k=0}^{n-1} a_k X^k$.

[47] Division euclidienne de X^p par $\chi_A(X)$. $n = \deg \chi_A$.

[48] Théorème de Cayley–Hamilton.

Exemple 14 Calcul de A^n pour $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R}), (n \in \mathbb{N}^*)$.

On a $\chi_A(X) = X(1+X)(2-X)$. Pour tout $n \in \mathbb{N}^*$, il existe $Q \in \mathbb{R}[X], (a,b,c) \in \mathbb{R}^3$, tels que :

$$X^n = Q(X)P_A(X) + aX^2 + bX + c,\ c = 0,\ a - b = (-1)^n,\ 4a + 2b = 2^n,$$ [49]

d'où $a = \frac{1}{3}\left(2^{n-1} + (-1)^n\right)$, $b = \frac{1}{3}\left(2^{n-1} + 2(-1)^{n-1}\right)$. On en déduit :

$$A^n = \frac{1}{3}\left(2^{n-1} + (-1)^n\right)A^2 + \frac{1}{3}\left(2^{n-1} + 2(-1)^{n-1}\right)A.$$

$A^2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & 1 \\ 2 & 2 & 2 \end{pmatrix}$ donne $A^n = \frac{1}{3}\begin{pmatrix} 2^{n-1} + (-1)^n & 2^{n-1} + 2(-1)^{n-1} & 2^{n-1} + (-1)^n \\ 2^n + (-1)^{n-1} & 2^n + 2(-1)^n & 2^n + (-1)^{n-1} \\ 3.2^{n-1} & 3.2^{n-1} & 3.2^{n-1} \end{pmatrix}$.

[49] En substituant successivement à X les valeurs 0, -1 et 2.

Copyrighted material

1.2 – Utilisation de la diagonalisation

On suppose que $A \in \mathcal{M}_n(\mathbb{K})$ est diagonalisable. Il existe alors $P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}AP = D$ soit diagonale : $P^{-1}AP = \mathrm{diag}\left(\lambda_1, \lambda_2, \ldots, \lambda_n\right)$.

Il en résulte $A = PDP^{-1}$ et $\forall p \in \mathbb{N}, A^p = PD^pP^{-1}$ avec $D^p = \mathrm{diag}\left(\lambda_1^p, \lambda_2^p, \ldots, \lambda_n^p\right)$.

▪ **Premier calcul de A^n**

Une première méthode possible consiste à opérer par diagonalisation effective de A, c'est-à-dire calculer P, P^{-1} puis $A^p = PD^pP^{-1}$.

Exemple 15 Soit $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$. ✎(50) Calculer A^n, $n \in \mathbb{N}^*$, par diagonalisation.

✎(50) Voir l'exemple 14.

On a $\chi_A(X) = X(1+X)(2-X)$.

Ayant trois valeurs propres distinctes, $0, -1$ et 2, A est diagonalisable.

Sous-espaces propres :

$$\begin{array}{lcll} E_A(0) & = & \mathrm{Vect}\left(c_1\right) & c_1 = (1,0,-1) \\ E_A(-1) & = & \mathrm{Vect}\left(c_2\right) & c_2 = (1,-1,0) \\ E_A(2) & = & \mathrm{Vect}\left(c_3\right) & c_3 = (1,2,3) \end{array}$$

donc $P^{-1}AP = \mathrm{diag}(0,-1,2)$ avec $P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & 2 \\ -1 & 0 & 3 \end{pmatrix}$. Le calcul donne :

$$P^{-1} = \frac{1}{6}\begin{pmatrix} 3 & 3 & -3 \\ 2 & -4 & 2 \\ 1 & 1 & 1 \end{pmatrix},$$

$$\begin{aligned} \text{donc } A^n &= \frac{1}{6}\begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & 2 \\ -1 & 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 \\ 0 & (-1)^n & 0 \\ 0 & 0 & 2^n \end{pmatrix}\begin{pmatrix} 3 & 3 & -3 \\ 2 & -4 & 2 \\ 1 & 1 & 1 \end{pmatrix} \\ &= \frac{1}{6}\begin{pmatrix} 0 & (-1)^n & 2^n \\ 0 & (-1)^{n-1} & 2^{n+1} \\ 0 & 0 & 3.2^n \end{pmatrix}\begin{pmatrix} 3 & 3 & -3 \\ 2 & -4 & 2 \\ 1 & 1 & 1 \end{pmatrix} \\ &= \frac{1}{3}\begin{pmatrix} (-1)^n + 2^{n-1} & 2(-1)^{n-1} + 2^{n-1} & (-1)^n + 2^{n-1} \\ (-1)^{n-1} + 2^n & 2(-1)^n + 2^n & (-1)^{n-1} + 2^n \\ 3.2^{n-1} & 3.2^{n-1} & 3.2^{n-1} \end{pmatrix} \end{aligned}$$

✎(51) L'exemple précédent met en évidence que la méthode «par diagonalisation effective» est bien plus laborieuse que celle qui utilise le théorème de Cayley-Hamilton.

▪ **Deuxième calcul** ✎(51)

Notons $u \in \mathcal{L}\left(\mathbb{K}^n\right)$ associé à A dans la base canonique $\mathcal{B}$: $A = \mathrm{mat}_{\mathcal{B}}\, u$.

Soit $\lambda_1, \ldots, \lambda_q$ les valeurs propres distinctes de A, d'après le théorème 10, on sait que u s'écrit :

$$u = \sum_{i=1}^{q} \lambda_i p_i$$

où pour tout $i \in [\![1, q]\!]$, p_i est la projection sur $E_u\left(\lambda_i\right) = \mathrm{Ker}\left(u - \lambda_i \mathrm{Id}_E\right)$ parallèlement à la somme $\bigoplus_{\substack{j=1 \\ j \neq i}}^{q} E_u(\lambda_j)$ des autres sous-espaces propres. Il en résulte :

$$\forall k \in \mathbb{N}, u^k = \sum_{i=1}^{q} \lambda_i^k p_i . \qquad (2)$$

Conséquence pratique : il existe q matrices de projection $\Pi_1, \ldots, \Pi_q$ telle que :

$$\forall k \in \mathbb{N}, A^k = \sum_{i=1}^{q} \lambda_i^k \Pi_i . \qquad (3)$$

On peut, par exemple, calculer les matrices Π_i en résolvant le système obtenu en écrivant la relation (3) pour $i = 1, 2, \ldots, q$.

Copyrighted material

Exemple 16 Calcul de $\lim_{n\to+\infty} A^n$ pour $A = \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$.

On a $\chi_A(X) = (1-X)\left(X^2+X+\frac{1}{2}\right)$. Donc A n'est pas diagonalisable dans $\mathcal{M}_3(\mathbb{R})$. (52)

(52) χ_A n'est pas scindé dans $\mathbb{R}[X]$.

En revanche, dans $\mathbb{C}[X]$: $\chi_A(X) = (1-X)\left(X+\frac{1+i}{2}\right)\left(X+\frac{1-i}{2}\right)$, donc A est diagonalisable dans $\mathcal{M}_3(\mathbb{C})$. Les trois valeurs propres distinctes sont : 1, $\frac{1}{\sqrt{2}}e^{3i\frac{\pi}{4}}$ et $\frac{1}{\sqrt{2}}e^{-3i\frac{\pi}{4}}$.

D'après l'étude précédente, il existe trois matrices de projection Π_1, Π_2, Π_3 telles que :

$$\forall n \in \mathbb{N},\ A^n = \Pi_1 + 2^{-\frac{n}{2}} e^{\frac{3ni\pi}{4}} \Pi_2 + 2^{-\frac{n}{2}} e^{-\frac{3ni\pi}{4}} \Pi_3.$$

(53) On obtient un système qui fournit Π_1, Π_2, Π_3.

(53) En écrivant cette relation pour $n=0$, $n=1$ et $n=2$.

$$\begin{cases} \Pi_1 + \Pi_2 + \Pi_3 = I_3 \\ \Pi_1 - \frac{1-i}{2}\Pi_2 - \frac{1+i}{2}\Pi_3 = A \\ \Pi_1 - \frac{i}{2}\Pi_2 + \frac{i}{2}\Pi_3 = A^2 \end{cases}$$

Remarquons que $\lim_{n\to+\infty} A^n = \Pi_1$, donc seul le calcul de Π_1 est utile, et on obtient :

$$\Pi_1 = \frac{1}{5}\left(I_3 + 2A + 2A^2\right).$$

Il reste à calculer $A^2 = \begin{pmatrix} 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & \frac{1}{2} \end{pmatrix}$ pour conclure à $\lim_{n\to+\infty} A^n = \Pi_1 = \frac{1}{5}\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}$.

1.3 – Utilisation d'une trigonalisation

On suppose que $A \in \mathcal{M}_n(\mathbb{K})$ est trigonalisable donc que χ_A est scindé dans $\mathbb{K}[X]$. (54)

(54) Ce qui est toujours vrai lorsque $\mathbb{K}=\mathbb{C}$.

- **Cas particulier**

A admet une seule valeur propre : $\lambda \in \mathbb{K}$. Il existe alors :

$P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}AP = \begin{pmatrix} \lambda & & \cdots \\ & \ddots & \ddots \\ (0) & & \lambda \end{pmatrix}$ donc $P^{-1}AP = \lambda I_n + N$ avec N nilpotente.

On en déduit $A = \lambda I_n + B$ avec $B = PNP^{-1}$ nilpotente. (55)

(55) $\forall p \in \mathbb{N},\ B^p = PN^pP^{-1}$.

I_n et B étant permutables, on obtient (56) : $\forall p \in \mathbb{N},\ A^p = \sum_{j=0}^{p} \mathcal{C}_p^j \lambda^{p-j} B^j$.

(56) Formule du binôme de Newton.

Soit alors r l'indice de nilpotence de B (on sait que $r \leqslant n$) : on a $B^j = 0$ pour tout $j \geqslant r$.

Il en résulte que, pour tout $p \geqslant r$, $A^p = \sum_{j=0}^{r} \mathcal{C}_p^j \lambda^{p-j} B^j$ avec $B = A - \lambda I_n$.

Exemple 17 Calcul de A^n, $n \in \mathbb{N}$, pour $A = \begin{pmatrix} -2 & -1 & 2 \\ -15 & -6 & 11 \\ -14 & -6 & 11 \end{pmatrix}$. (57)

(57) Voir l'exemple 11.

On a vu que $A = PTP^{-1}$ avec $T = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ et $P = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 3 & 0 \\ 2 & 2 & 1 \end{pmatrix}$.

$T = I_3 + N$ avec $N = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$ nilpotente d'indice 3 car $N^2 = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, donc :

$B = A - I_3$ est nilpotente d'indice 3.

Copyrighted material

On obtient alors $A^n = (I_3 + B)^n = I_3 + nB + \dfrac{n(n-1)}{2}B^2$ donc :

$$A^n = \frac{(n-1)(n-2)}{2}I_3 - n(n-2)A + \frac{n(n-1)}{2}A^2.$$

Compte tenu de $A^2 = \begin{pmatrix} -9 & -4 & 7 \\ -34 & -15 & 25 \\ -36 & -16 & 27 \end{pmatrix}$, il vient finalement :

$$A^n = \begin{pmatrix} -2n^2 - n + 1 & -n^2 & \dfrac{3n^2+n}{2} \\ -2n^2 - 13n & -n^2 - 6n + 1 & \dfrac{3n^2+19n}{2} \\ -4n^2 - 10n & -2n^2 - 4n & 3n^2 + 7n + 1 \end{pmatrix}.$$

▪ **Cas général**

A est alors semblable à une matrice du type détaillé au théorème 18. Il existe :

$P \in \mathrm{GL}_n(\mathbb{K})$ telle que $P^{-1}AP = \begin{pmatrix} T_1 & & (0) \\ & T_2 & \\ (0) & & \ddots \\ & & T_q \end{pmatrix} = T$, avec $T_i = \lambda_i I_{m_i} + N_i$ ✎(58)

✎(58) Notations du théorème 18.

On en déduit, pour tout $p \in \mathbb{N}^*$: $A^p = PT^pP^{-1}$ avec $T^p = \begin{pmatrix} T_1^p & & (0) \\ & T_2^p & \\ (0) & & \ddots \\ & & T_q^p \end{pmatrix}$

où, pour tout i, $(1 \leqslant i \leqslant q)$, si $p \geqslant r_i$, (r_i étant l'indice de nilpotence de N_i : $r_i \leqslant m_i$) :

$$T_i^p = \sum_{k=0}^{r_i} \mathrm{C}_p^k \lambda_i^{p-k} N_i^k.$$

– Premier calcul de A^n

Une méthode possible consiste donc à effectuer explicitement la réduction précédente.

Exemple 18 Calculer A^n, $n \in \mathbb{N}$, pour $A = \begin{pmatrix} 7 & 3 & -4 \\ -6 & -2 & 5 \\ 4 & 2 & -1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$.

Dans l'exemple 13, on a trouvé : $P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ avec $P = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 2 & 1 \\ 2 & 0 & 1 \end{pmatrix}$, d'où

$\forall n \in \mathbb{N}, A^n = P \begin{pmatrix} 2^n & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix} P^{-1}$. Le calcul fournit $P^{-1} = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 1 & -1 \\ -4 & -2 & 3 \end{pmatrix}$ d'où :

$$A^n = \begin{pmatrix} 2^{n+1} + 4n - 1 & 2^n + 2n - 1 & -2^n - 3n + 1 \\ 2^{n+1} - 8n - 2 & 2^n - 4n & -2^n + 6n + 1 \\ 2^{n+2} - 4 & 2^{n+1} - 2 & -2^{n+1} + 3 \end{pmatrix}.$$

– Deuxième calcul

Soit $u \in \mathcal{L}(\mathbb{K}^n)$ canoniquement associé à A : $A = \mathrm{mat}_{\mathcal{B}}\, u$, $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$.

On peut envisager, comme dans le cas des matrices diagonalisables, une décomposition de A utilisant les matrices Π_i des projections p_i sur $F_i = \mathrm{Ker}\left(u - \lambda_i \mathrm{Id}_E\right)^{m_i}$.

Considérons toujours les matrices $\Delta_i = \mathrm{diag}\left(0, \ldots, 0, I_{m_i}, 0, \ldots, 0\right)$ auxquelles nous adjoignons les matrices $\Omega_i = \mathrm{diag}\left(0, \ldots, 0, N_i, 0, \ldots, 0\right)$. ✎(59)

✎(59) Il s'agit ici de matrices diagonales par blocs.

La réduction précédente s'écrit alors $P^{-1}AP = \sum_{i=1}^{q} \lambda_i \Delta_i + \Omega_i$.

Copyrighted material

Hidden page

2. Étude des suites récurrentes linéaires d'ordre 2

Le but est de retrouver, grâce au calcul matriciel, l'expression du terme général d'une suite récurrente linéaire d'ordre 2. ✎(61)

✎(61) Ces suites ont été étudiées en première année (voir Analyse – MPSI).

2.1 – Généralités – Rappels

Étant donné des éléments a et b fixés de $\mathbb{K}$ avec $b \neq 0$, on note $\mathcal{S}$ l'ensemble des suites $(u_n)_{\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ telles que $\forall n \in \mathbb{N},\ u_{n+2} = au_{n+1} + bu_n$.

- $\mathcal{S}$ est un sous-espace vectoriel de $\mathbb{K}^{\mathbb{N}}$.
- L'application $\Phi : (u_n)_{\mathbb{N}} \mapsto (u_0, u_1)$ est un isomorphisme de $\mathcal{S}$ sur $\mathbb{K}^2$.
- $\mathcal{S}$ est de dimension 2.
- Deux suites $u = (u_n)_{\mathbb{N}}$ et $v = (v_n)_{\mathbb{N}}$ de $\mathcal{S}$ forment une base de $\mathcal{S}$ si et seulement si leurs images par Φ forment une base de $\mathbb{K}^2$ donc si et seulement si $\begin{vmatrix} u_0 & v_0 \\ u_1 & v_1 \end{vmatrix} \neq 0$.
- Une suite géométrique $(r^n)_{\mathbb{N}}$, $r \neq 0$, appartient à $\mathcal{S}$ si et seulement si r est solution de :

$$(\mathscr{C}) \quad r^2 - ar - b = 0. \text{ ✎(62)}$$

✎(62) $(\mathscr{C})$ est l'**équation caractéristique** de la récurrence.

- En observant que l'ensemble des suites réelles solutions de la récurrence est inclus dans l'ensemble des suites complexes solutions de la même récurrence, on peut limiter l'étude à $\mathbb{K} = \mathbb{C}$.

– **Premier cas** : $A = a^2 + 4b \neq 0$

$\mathcal{S}$ contient deux suites géométriques non nulles $(r_1^n)_{\mathbb{N}}$ et $(r_2^n)_{\mathbb{N}}$ où r_1 et r_2 sont les racines distinctes de $(\mathscr{C})$. Ces deux suites forment une base de $\mathcal{S}$, car $\begin{vmatrix} 1 & 1 \\ r_1 & r_2 \end{vmatrix} = r_1 - r_2 \neq 0$ et pour tout $(u_n)_{\mathbb{N}}$ de $\mathcal{S}$ il existe $(\lambda, \mu) \in \mathbb{K}^2$ tel que : $\forall n \in \mathbb{N},\ u_n = \lambda r_1^n + \mu r_2^n$. Le calcul de λ et μ se fait en résolvant le système :

$$\begin{cases} \lambda r_1 + \mu r_2 = u_1 \\ \lambda + \mu = u_0 \end{cases}$$

– **Deuxième cas** : $\Delta = a^2 + 4b = 0$ donc $a \neq 0$

$\mathcal{S}$ contient une seule suite géométrique non nulle $(r^n)_{\mathbb{N}}$ avec $r = \dfrac{a}{2}$ racine double de $(\mathscr{C})$. Une base de $\mathcal{S}$ est alors formée par les suites $(r^n)_{\mathbb{N}}$ et $(nr^n)_{\mathbb{N}}$ et pour tout $(u_n)_{\mathbb{N}}$ de $\mathcal{S}$, il existe $(\lambda, \mu) \in \mathbb{K}^2$ tel que : $\forall n \in \mathbb{N},\ u_n = \lambda r^n + \mu n r^n$. Pour obtenir λ et μ on résoud maintenant le système :

$$\begin{cases} \lambda r + \mu r = u_1 \\ \lambda = u_0 \end{cases}$$

2.2 – Calcul du terme général, $\mathbb{K} = \mathbb{C}$

Soit $u = (u_n)_{\mathbb{N}}$ un élément de $\mathcal{S}$ défini par la donnée de $(u_0, u_1) \in \mathbb{C}^2$.

À la suite u, on associe une suite vectorielle $(V_n)_{n \in \mathbb{N}^*}$ à valeurs dans $\mathbb{C}^2$, en posant :

$$\forall n \geqslant 1,\ V_n = \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix}$$

cette suite associée vérifie donc : $\forall n \geqslant 1,\ V_{n+1} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} V_n$.

On pose $A = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$ et on obtient : $\forall n \geqslant 1,\ V_n = A^{n-1} V_1$.

Le problème est ainsi ramené au calcul des puissances successives de la matrice A dont le polynôme caractéristique est $\chi_A = \det(A - XI_2) = X^2 - aX - b$.

- **Premier cas** : $\Delta = a^2 + 4b \neq 0$.

La matrice A a deux valeurs propres distinctes r_1 et r_2. On remarque qu'elles sont non nulles (car $b \neq 0$) et que ce sont les racines de l'équation $(\mathscr{C})$.

Dans ce cas, A est diagonalisable et on obtient : $P^{-1}AP = \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix}$ avec $P = \begin{pmatrix} r_1 & r_2 \\ 1 & 1 \end{pmatrix}$.

Copyrighted material

En conséquence :

$$A^n = P\begin{pmatrix} r_1^n & 0 \\ 0 & r_2^n \end{pmatrix} P^{-1} \quad , \quad P^{-1} = \frac{1}{r_1 - r_2}\begin{pmatrix} 1 & -r_2 \\ -1 & r_1 \end{pmatrix}$$

$$A^n = \frac{1}{r_1 - r_2}\begin{pmatrix} r_1^{n+1} - r_2^{n+1} & -r_1 r_2\left(r_1^n - r_2^n\right) \\ r_1^n - r_2^n & -r_1 r_2\left(r_1^{n-1} - r_2^{n-1}\right) \end{pmatrix}$$

et avec $\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A^{n-1}\begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$ on en déduit :

$$u_n = \frac{u_1 - r_2 u_0}{r_1 - r_2} r_1^n + \frac{r_1 u_0 - u_1}{r_1 - r_2} r_2^n .$$

▪ **Deuxième cas** : $\Delta = a^2 + 4b = 0$.

Posons alors $a = 2r$, on a donc $b = -r^2$. La matrice A s'écrit $A = \begin{pmatrix} 2r & -r^2 \\ 1 & 0 \end{pmatrix}$ et admet r pour valeur propre double. A n'est pas diagonalisable, mais on peut former une réduite triangulaire.

Compte tenu de $A\begin{pmatrix} r \\ 1 \end{pmatrix} = r\begin{pmatrix} r \\ 1 \end{pmatrix}$, $A\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2r \\ 1 \end{pmatrix} = \begin{pmatrix} r \\ 1 \end{pmatrix} + r\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, on pose $P = \begin{pmatrix} r & 1 \\ 1 & 0 \end{pmatrix}$;

alors $P \in \mathrm{GL}_2(\mathbb{K})$, $P^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -r \end{pmatrix}$ et $P^{-1}AP = \begin{pmatrix} r & 1 \\ 0 & r \end{pmatrix} = T$.

Avec $T^n = \left(rI_2 + \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\right)^n = \begin{pmatrix} r^n & nr^{n-1} \\ 0 & r^n \end{pmatrix}$, et $A^n = PT^nP^{-1}$, on a :

$$A^n = \begin{pmatrix} (n+1)r^n & -nr^{n+1} \\ nr^{n-1} & -(n-1)r^n \end{pmatrix}.$$

Finalement $\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = A^{n-1}\begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$ donne :

$$u_n = n\,r^{n-1}u_1 - (n-1)r^n u_0 \text{ ou encore } u_n = u_0 r^n + \left(\frac{u_1}{r} - u_0\right) n\,r^n.$$

3. Exponentielle de matrice

3.1 – Rappels et compléments

La notion d'exponentielle de matrice et les propriétés sont étudiées en Analyse. (63)

(63) Voir Analyse, MP, chapitre 5, Séries entières.

Étant donné $A \in \mathcal{M}_n(\mathbb{K})$, on forme $A_m = \sum_{k=0}^{m} \frac{1}{k!}A^k$. Alors $\exp A = \lim_{m \to +\infty} A_m$.

Soit A et B dans $\mathcal{M}_n(K)$. Si $AB = BA$, alors $\exp(A+B) = \exp A \exp B$.

Si A et B sont semblables : $B = P^{-1}AP$ avec $P \in \mathrm{GL}(\mathbb{K})$, alors $\exp(B) = P^{-1}\exp(A)P$ c'est-à-dire que $\exp A$ et $\exp B$ vérifient la même relation de similitude.

Méthode de base

Pour une matrice diagonale $D = \mathrm{diag}\left(d_1, \ldots, d_n\right)$, on a $\exp(D) = \mathrm{diag}\left(e^{d_1}, \ldots, e^{d_n}\right)$.

Si A est diagonalisable, $A = PDP^{-1}$ avec $P \in \mathrm{GL}_n(\mathbb{K})$ et $D = \mathrm{diag}\left(d_1, \ldots, d_n\right)$, on a :

$$\exp(A) = P\exp(D)P^{-1}.$$

Théorème 19

Étant donné $A \in \mathcal{M}_n(K)$, il existe $P \in \mathbb{K}[X]$, $\deg P < n$, tel que $\exp A = P(A)$.

☞ Soit χ_A le polynôme caractéristique de A. Dans la division de $P_m = \sum_{k=0}^{m} \frac{1}{k!}X^k$ par χ_A, on a :

$$P_m = \chi_A Q_m + R_m, \ \deg R_m < n.$$

Il vient alors $A_m = P_m(A) = R_m(A)$ puisque $\chi_A(A) = 0$. (64)

La suite $\left(R_m\right)_{m \in \mathbb{N}}$ est une suite de $K_{n-1}[X]$ telle que $\exp A = \lim_m R_m(A)$.

Comme $F = \mathrm{Vect}\left(I_n, A, \ldots, A^{n-1}\right)$ est de dimension finie, c'est un fermé de $\mathcal{M}_n(\mathbb{K})$.

Il s'ensuit que $\exp A$ appartient à F et il existe $P \in \mathbb{K}_{n-1}[X]$ tel que $\exp A = P(A)$.

(64) Théorème de Cayley-Hamilton.

Copyrighted material

3.2 – Exemples

Exemple 20 Calcul de $\exp A$, avec $(a,b)\in\mathbb{C}^2$, $A\in\mathcal{M}_n(\mathbb{C})$, $\forall (i,j)\in[\![1,n]\!]^2$, $a_{ii}=b$ et $a_{ij}=a$ pour $i\neq j$.

Avec $U\in\mathcal{M}_n(\mathbb{C})$ de termes tous égaux à 1, on a $A=aU+(b-a)I_n$ donc $e^A=e^{aU}e^{(b-a)I_n}$.

On a $e^{(b-a)I_n}=e^{b-a}I_n$. Pour e^{aU}, calculons $(aU)^k$, $k\in\mathbb{N}$.

(65) Par récurrence claire.

Avec $U^2=nU$, il vient (65) $(aU)^k=\dfrac{1}{n}(na)^kU$ pour $k\in\mathbb{N}$. De :

$$\sum_{k=0}^{m}\frac{1}{k!}(aU)^k=I_n+\sum_{k=1}^{m}\frac{1}{k!}(aU)^k=I_n+\frac{1}{n}\sum_{k=0}^{m}\frac{(na)^k}{k!}U-\frac{1}{n}U,$$

on déduit $e^{aU}=I_n-\dfrac{1}{n}U+\dfrac{e^{na}}{n}U$. Finalement, $e^A=e^{b-a}\left(I_n+\dfrac{1}{n}(e^{na}-1)\right)U$.

Si $a=0$, $e^A=e^bI_n$ et, pour $a\neq 0$, e^A est combinaison linéaire de I_n et A.

Exemple 21 Exponentielle d'une matrice carrée réelle d'ordre 2.

a) Premier cas, $A\in\mathcal{M}_2(\mathbb{R})$ admet des valeurs propres λ et μ distinctes.

Il existe $P\in\mathrm{GL}_2(\mathbb{R})$ telle que $A=PDP^{-1}$ avec $D=\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}$.

On a $e^D=\begin{pmatrix}e^\lambda & 0\\ 0 & e^\mu\end{pmatrix}=\alpha D+\beta I_2$ avec $\alpha=\dfrac{e^\lambda-e^\mu}{\lambda-\mu}$ et $\beta=\dfrac{\lambda e^\mu-\mu e^\lambda}{\lambda-\mu}$.

Alors $e^A=Pe^DP^{-1}=\alpha PDP^{-1}+\beta I_2=\alpha A+\beta I_2$.

b) Deuxième cas, A admet une valeur propre double λ.

Il existe alors $P\in\mathrm{GL}_n(\mathbb{R})$ et $\mu\in\mathbb{R}$ tels que $A=PTP^{-1}$ avec $T=\begin{pmatrix}\lambda & \mu\\ 0 & \lambda\end{pmatrix}$.

$A-\lambda I_2=P\left(T-\lambda I_2\right)P^{-1}$, où $N=T-\lambda I_2=\begin{pmatrix}0 & \mu\\ 0 & 0\end{pmatrix}$.

(66) N est nilpotente d'indice 2 en général.

Pour $k\in\mathbb{N}$, $k\geqslant 2$, on a $N^k=0$. (66)

Avec $\exp N=I_2+N$ donc $\exp\left(A-\lambda I_2\right)=P\exp\left(T-\lambda I_2\right)P^{-1}=I_2+\left(A-\lambda I_2\right)$,

(67) A et λI_2 commutent.

comme on a $\exp\left(A-\lambda I_2\right)=\exp(A)\exp\left(-\lambda I_2\right)$ (67) et $\exp\left(-\lambda I_2\right)=e^{-\lambda}I_2$, il vient $e^A=e^\lambda\left((1-\lambda)I_2+A\right)$.

1) Troisième cas, A n'a pas de valeur propre réelle.

(68) On a $\mu\neq 0$.

A admet des valeurs propres conjuguées non réelles. Soit $\lambda+i\mu$ l'une d'elles. (68)

Il existe alors $P\in\mathrm{GL}_n(\mathbb{R})$ telle que $P^{-1}AP=\begin{pmatrix}\lambda & -\mu\\ \mu & \lambda\end{pmatrix}$. Soit $J_2=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$.

On a $P^{-1}AP=\lambda I_2+\mu J_2$ et $J_2^2=-I_2$. Pour $k\in\mathbb{N}$, $J_2^{2k}=(-1)^kI_2$ et $J_2^{2k+1}=(-1)^kJ_2$

donne $\exp\left(\mu J_2\right)=\displaystyle\sum_{k=0}^{+\infty}(-1)^k\frac{\mu^{2k}}{(2k)!}I_2+\sum_{k=0}^{+\infty}(-1)^k\frac{\mu^{2k+1}}{(2k+1)!}J_2$, c'est-à-dire :

$$\exp\left(\mu J_2\right)=(\cos\mu)I_2+(\sin\mu)J_2.$$

(69) Voir le cas précédent.

Compte tenu de $P^{-1}\left(A-\lambda I_2\right)P=\mu J_2$ et $\exp\left(A-\lambda I_2\right)=e^{-\lambda}\exp A$, (69) il vient

$e^{-\lambda}\exp A=(\cos\mu)I_2+(\sin\mu)PJ_2P^{-1}$. Or $PJ_2P^{-1}=\dfrac{1}{\mu}\left(A-\lambda I_2\right)$. Finalement :

$$\exp A=e^\lambda\left((\cos\mu)I_2+\frac{\sin\mu}{\mu}\left(A-\lambda I_2\right)\right)=\frac{e^\lambda}{\mu}\left((\mu\cos\mu-\lambda\sin\mu)I_2+\sin\mu A\right).$$

Exemple 22 Si $A\in\mathcal{M}_n(\mathbb{R})$ est à termes non diagonaux positifs, alors tous les termes de $\exp A$ sont positifs.

Soit $\lambda=\sup\left\{|a_{ii}|,\ 1\leqslant i\leqslant n\right\}$. Alors tous les termes de $A+\lambda I_n$ sont positifs et il en résulte

(70) Par récurrence aisée.

que pour tout $k\in N$, les termes de $\left(A+\lambda I_n\right)^k$ sont tous positifs. (70)

Il en est donc de même pour ceux de $\exp\left(A+\lambda I_n\right)$. On conclut avec :

$$\exp A=e^{-\lambda}\exp\left(A+\lambda I_n\right).$$

Copyrighted material

Méthodes

L'essentiel

I. Éléments propres, diagonalisation

✔ **Si l'on veut** calculer les valeurs propres d'un endomorphisme u d'un espace E de dimension quelconque,

▪ **on peut** revenir à la définition : il s'agit de trouver les scalaires λ pour lesquels l'équation $f(x) = \lambda x$, $x \in E$, admet des solutions non nulles.

→ Voir *Mise en œuvre*, exercice 1

✔ **Si l'on veut** montrer que des vecteurs sont indépendants,

▪ **on peut** essayer de reconnaître une famille de vecteurs propres associés à des valeurs propres distinctes.

→ Voir *Mise en œuvre*, exercice 2

✔ **Si l'on veut** écrire une matrice admettant pour polynôme caractéristique un polynôme P donné,

▪ **on peut** penser à la matrice compagnon de P.

→ Voir *Mise en œuvre*, exercice 3

✔ **Si l'on veut** diagonaliser une matrice carrée qui s'écrit $A = \mu I_n + B$ où B est de rang 1,

▪ **on peut** observer que les sous-espaces propres de B sont $\operatorname{Ker} B$ et $\operatorname{Im} B$ et que ceux de A s'en déduisent très simplement.

✔ **Si l'on veut** diagonaliser une matrice B,

▪ **on peut** penser qu'il n'est pas toujours indispensable de former le polynôme caractéristique. Un polynôme annulateur peut fort bien faire l'affaire.

→ Voir *Mise en œuvre*, exercice 4

✔ **Si l'on veut** montrer qu'une matrice est diagonalisable,

▪ **on peut** montrer qu'elle a un polynôme annulateur scindé et à racines simples.

→ Voir *Mise en œuvre*, exercices 5, 6

II. Trigonalisation

✔ Une matrice est trigonalisable si et seulement si son polynôme caractéristique est scindé.

→ Voir *Mise en œuvre*, exercices 7, 8

✔ **Si l'on veut** trouver une matrice triangulaire semblable à une matrice A,

▪ **on peut** étudier $\operatorname{Ker}\left(A - \lambda I_n\right)^k$ où λ est valeur propre de multiplicité k.

→ Voir *Mise en œuvre*, exercices 8, 9

Copyrighted material

III. Théorème de Cayley-Hamilton

✔ Il s'agit d'un moyen particulièrement efficace pour obtenir un polynôme annulateur d'une matrice carrée.

→ Voir *Mise en œuvre*, exercices 8, 9, 10

✔ **Si l'on veut** écrire l'espace E en somme directe de sous-espaces stables,

▪ **on peut** utiliser le théorème de décomposition des noyaux à partir du polynôme caractéristique.

→ Voir *Mise en œuvre*, exercice 9

✔ **Si l'on veut** calculer les puissances d'une matice A,

▪ **on peut** diviser X^k par le polynôme caractéristique de A et utiliser le théorème de Cayley-Hamilton.

→ Voir *Mise en œuvre*, exercice 10

IV. Sous-espaces stables

✔ Les vecteurs propres donnent les droites stables.

→ Voir *Mise en œuvre*, exercice 12

✔ **Si l'on veut** déterminer, en dimension finie, les hyperplans stables par un endomorphisme de matrice A,

▪ **on peut** étudier les valeurs propres de la transposée de A.

→ Voir *Mise en œuvre*, exercices 11, 12

V. Exponentielle de matrice

✔ Des méthodes sont données dans les exemples du cours.

✔ On peut définir l'exponentielle d'un endomorphisme nilpotent, même en dehors d'un contexte de dimension finie.

→ Voir *Mise en œuvre*, exercice 13

✔ **Si l'on veut** calculer une exponentielle de matrice A,

▪ **on peut** décomposer A en $\mu I_n + B$ avec B nilpotente.

→ Voir *Mise en œuvre*, exercice 14

VI. Questions de densité

✔ On fait appel ici à la notion d'espace vectoriel normé. Certains résultats sont faciles à établir sur telle partie F de $\mathcal{M}_n(\mathbb{K})$ et peuvent ensuite être généralisés grâce à la densité de F dans $\mathcal{M}_n(\mathbb{K})$ et à un argument de continuité.

→ Voir *Mise en œuvre*, exercices 15, 16

Mise en œuvre

I. Éléments propres d'un endomorphisme, diagonalisation

Ex. 1

Soit E le $\mathbb{R}$-espace vectoriel des fonctions réelles continues sur $\mathbb{R}$ admettant une limite finie en $+\infty$ et T l'endomorphisme de E défini par :

$$\forall f \in E, \forall x \in \mathbb{R}, T(f)(x) = f(x+1).$$

1) Montrer que si λ est valeur propre de T alors $|\lambda| \leqslant 1$.

2) Examiner si λ est valeur propre de T et déterminer le sous-espace propre éventuellement associé dans les cas suivants : a) $\lambda \in \{0, 1, -1\}$; b) $\lambda \in]0, 1[$; c) $\lambda \in]-1, 0[$.

Indications

1) Étudier $\lim\limits_{n \to +\infty} f(x+n)$, $n \in \mathbb{N}^*$.

2) a) Étudier les noyaux : $\operatorname{Ker} T$, $\operatorname{Ker}(T - \mathrm{Id}_E)$ et $\operatorname{Ker}(T + \mathrm{Id}_E)$.

b) Pour $\lambda \in]0, 1[$, exhiber un vecteur propre «évident» associé à λ.

c) Même démarche.

Solution

1) Soit $\lambda \in \operatorname{Sp}(T)$. Il existe $f \in E \setminus \{0\}$ tel que :

$$\forall x \in \mathbb{R},\ f(x+1) = \lambda f(x).$$

On en déduit $\forall x \in \mathbb{R}, \forall n \in \mathbb{N}^*,\ f(x+n) = \lambda^n f(x)$.

Donc, en posant $L = \lim\limits_{+\infty} f$ on obtient pour tout $x \in \mathbb{R}$:

$$\lim_{n \to +\infty} f(x+n) = \lim_{n \to +\infty} \lambda^n f(x) = L.$$

f étant non nulle, il existe $a \in \mathbb{R}$ tel que $f(a) \neq 0$ et, avec $\lim\limits_{n \to +\infty} \lambda^n f(a) = L$, il vient $|\lambda| \leqslant 1$.

2) a) ▪ Étudions $\operatorname{Ker} T$.

$f \in \operatorname{Ker} T$ s'écrit $\forall x \in \mathbb{R}, f(x+1) = 0$ soit aussi :

$$\forall x \in \mathbb{R}, f(x) = 0 \text{ et donc } f = 0_E.$$

Ainsi $\operatorname{Ker} T = \{0_E\}$ et 0 n'est pas valeur propre de T.

▪ Étudions $\operatorname{Ker}(T - \mathrm{Id}_E)$.

$f \in \operatorname{Ker}(T - \mathrm{Id}_E)$ s'écrit $\forall x \in \mathbb{R}, f(x+1) = f(x)$ ce qui traduit que f est 1-périodique. On obtient alors :

$$\forall x \in \mathbb{R}, \forall n \in \mathbb{N}^*, f(x+n) = f(x)$$

donc $f(x) = \lim\limits_{n \to +\infty} f(x+n) = L$. En notant C le sous-espace de E constitué des fonctions constantes, on a donc $\operatorname{Ker}(T - \mathrm{Id}_E) \subset C$.

D'autre part, il est clair que toute fonction constante appartient à $\operatorname{Ker}(T - \mathrm{Id}_E)$, d'où finalement, $\operatorname{Ker}(T - \mathrm{Id}_E) = C$, ce qui prouve que $1 \in \operatorname{Sp}(T)$.

Commentaires

Retour à la définition : la condition $f \neq 0$ est essentielle.

Par hypothèse, tout élément de E admet une limite réelle en $+\infty$.

Car $C \neq \{0_E\}$.

Copyrighted material

Hidden page

Ex. 2

Pour $n \in \mathbb{N}$, soit f_n et g_n dans $\mathscr{C}^\infty(\mathbb{R}, \mathbb{R})$ définies par $\forall x \in \mathbb{R}, f_n(x) = \cos nx$ et $g_n(x) = \sin nx$.
Montrer que, pour tout $n \in \mathbb{N}$, la famille $(f_0, f_1, g_1, f_2, g_2, \ldots, f_n, g_n)$ est libre.

Indications

f_n et g_n sont vecteurs propres de l'opérateur dérivation à l'ordre 2.

Des sous-espaces propres de valeurs propres distinctes sont en somme directe.

Solution

Soit $E = \mathscr{C}^\infty(\mathbb{R}, \mathbb{R})$ et $d \in \mathscr{L}(E)$, $d : f \mapsto f''$, on a :

$$\forall k \in \mathbb{N},\ f_k'' = -k^2 f_k,\ g_k'' = -k^2 g_k.$$

Ainsi f_k et g_k sont vecteurs propres de d associés à la valeur propre $-k^2$.
D'autre part, $\forall k \in \mathbb{N}^*$, (f_k, g_k) est libre.
En effet, $\lambda f_k + \mu g_k = 0$ impose $\lambda = 0$, puis $\mu = 0$.
Les sous-espaces propres $E_d(0), E_d(-1), E_d(-4), \ldots, E_d(-n^2)$ étant en somme directe, il vient alors que $(f_0, f_1, g_1, g_2, \ldots, f_n, g_n)$ est libre.

Commentaires

Faire $x = 0$ dans $\lambda \cos kx + \mu \sin kx = 0$.

Ex. 3

Soit $n \in \mathbb{N}^*$, $n \geqslant 2$. À tout polynôme unitaire de $\mathbb{K}_n[X]$, $P = X^n - \sum_{i=1}^{n} a_i X^{n-i}$, on associe la matrice :

$$A = \begin{bmatrix} 0 & & & & a_n \\ 1 & 0 & (0) & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ & (0) & \ddots & 0 & a_2 \\ & & & 1 & a_1 \end{bmatrix} \in \mathcal{M}_n(\mathbb{K}).$$

A est appelée matrice compagnon du polynôme P.

1) Calculer le polynôme caractéristique de A : $\chi_A(X) = \det(A - XI_n)$.

2) Montrer que la famille $(A^k)_{0 \leqslant k \leqslant n-1}$ est libre. En déduire le polynôme minimal de A.

Indications

1) Établir une formule de récurrence liant Δ_n et Δ_{n-1}.

2) Observer que le degré du polynôme minimal est $\geqslant n$.

Solution

1) Posons $\Delta_n = \chi_A(X) = \begin{vmatrix} -X & 0 & & & a_n \\ 1 & -X & (0) & & \vdots \\ 0 & 1 & \ddots & & \vdots \\ & (0) & \ddots & -X & a_2 \\ & & & 1 & a_1 - X \end{vmatrix}$.

En développant suivant la première ligne, il vient :

$$\Delta_n = (-1)^{n+1} a_n - X\Delta_{n-1}.$$

Donc pour tout $k \in [\![3, n]\!]$:

$$(-1)^k \frac{\Delta_k}{X^k} - (-1)^{k-1} \frac{\Delta_{k-1}}{X^{k-1}} = -\frac{a_k}{X^k}$$

puis $\sum_{k=3}^{n} (-1)^k \frac{\Delta_k}{X^k} - (-1)^{k-1} \frac{\Delta_{k-1}}{X^{k-1}} = -\sum_{k=3}^{n} \frac{a_k}{X^k}$ c'est-à-dire :

Commentaires

On recherche une formule de récurrence.

Calcul dans le corps $\mathbb{K}(X)$ des fractions rationnelles à coefficient dans $\mathbb{K}$.

Copyrighted material

Hidden page

0 est valeur propre de B. Le sous-espace propre associé $E_B(0) = \operatorname{Ker} B$ a pour équation $x_1 + x_2 + x_3 + x_4 = 0$.
Une base de $E_B(0)$ est, par exemple, (c_1, c_2, c_3) :

$$c_1 = (1,-1,0,0)\ ,\ c_2 = (1,0,-1,0)\ ,\ c_3 = (1,0,0,-1).$$

Un vecteur propre de B associé à une valeur propre non nulle est à rechercher dans $\operatorname{Im} B$ et $\operatorname{Im} B$ est visiblement la droite engendrée par $c_4 = (1,1,1,1)$.
Avec $Bc_4 = 4c_4$, on a c_4 vecteur propre associé à la valeur propre 4.

B est diagonalisable : en posant $P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$, on a :

$$P^{-1}BP = \operatorname{diag}(0,0,0,4) \text{ donc } P^{-1}AP = \operatorname{diag}(15,15,15,19).$$

B est visiblement de rang 1.

Propriété 14.

Ex. 5

$A = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{R})$ est-elle diagonalisable dans $\mathcal{M}_{2n}(\mathbb{R})$? dans $\mathcal{M}_{2n}(\mathbb{C})$?
Effectuer la diagonalisation quand elle est possible.

Indications

Un polynôme scindé dans $\mathbb{C}$ annule A. Si λ est valeur propre de A, alors λ^2 est valeur propre de A^2.

Solution

- On a $A^2 = -I_{2n}$ donc, dans $\mathbb{R}$: $\operatorname{Sp}(A) = \varnothing$; dans $\mathbb{C}$: $\operatorname{Sp}(A) \subset \{i, -i\}$.
- A est non diagonalisable dans $\mathcal{M}_{2n}(\mathbb{R})$ mais est diagonalisable dans $\mathcal{M}_{2n}(\mathbb{C})$ avec $\operatorname{Sp}(A) \subset \{-i, i\}$.

$E_A(i)$ a pour équations : $\begin{cases} -ix_k + x_{n+k} = 0, & 1 \leqslant k \leqslant n \\ -x_k - ix_{n+k} = 0, & 1 \leqslant k \leqslant n \end{cases}$

Système équivalent à $-ix_k + x_{n+k} = 0,\ 1 \leqslant k \leqslant n$.

Une base de $E_A(i)$ est donc $(c_1, c_2, \ldots, c_n)$, $c_k = e_k + ie_{n+k}$.

De même, $E_A(-i)$ a pour base $(c'_1, \ldots, c'_n)$, $c'_k = e_k - ie_{n+k}$.

Ainsi, avec $P = \begin{pmatrix} I_n & I_n \\ iI_n & -iI_n \end{pmatrix} \in \mathrm{GL}_{2n}(\mathbb{C})$, on a $P^{-1}AP = \begin{pmatrix} iI_n & 0 \\ 0 & -iI_n \end{pmatrix}$.

Commentaires

Propriété 13.

Théorème 12.

$(e_j)_{1 \leqslant j \leqslant 2n}$ est la base canonique de $\mathbb{C}^{2n}$.

Il suffit de remplacer i par $-i$.

Ex. 6

Soit $M \in \mathrm{GL}_n(\mathbb{C})$ telle que M^2 soit diagonalisable. Montrer que M est diagonalisable.

Indications

$M \in \mathcal{M}_n(\mathbb{K})$, avec $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, est diagonalisable si et seulement si il existe un polynôme annulateur scindé et à racines simples.

Solution

M^2 est inversible, ses valeurs propres sont donc non nulles.

Soit $P = \prod_{k=1}^{p} (X - \lambda_k)$ annulateur de M^2 : $\prod_{k=1}^{p} (M^2 - \lambda_k I_n) = 0$.

Notons, pour $k \in [\![1, p]\!]$, μ_k et $-\mu_k$ les racines carrées complexes de λ_k.

Alors $Q(X) = \prod_{k=1}^{p} (X - \mu_k)(X + \mu_k)$ est annulateur de M.

Ce plynôme Q étant scindé, à racines simples, M est diagonalisable.

Commentaires

M est inversible.

$\lambda_1, \ldots, \lambda_p$ valeurs propres distinctes.

Avec $\lambda_k \neq 0$, on a $\mu_k \neq -\mu_k$.

$M^2 - \lambda_k I_n = (M - \mu_k I_n)(M + \mu_k I_n)$.

Résultat rappelé en indications.

Copyrighted material

II. Trigonalisation

Ex. 7

Les matrices $A = \begin{pmatrix} 0 & 1 & 2 \\ -2 & 3 & 6 \\ -3 & 3 & 15 \end{pmatrix}$ ou $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$ sont-elles trigonalisables dans $\mathcal{M}_3(\mathbb{R})$?

Indications

Toute matrice de $\mathcal{M}_n(\mathbb{R})$ ou $\mathcal{M}_n(\mathbb{C})$ est trigonalisable dans $\mathcal{M}_n(\mathbb{C})$ puisque son polynôme caractéristique est scindé dans $\mathbb{C}$. La question ici posée revient à examiner si ce polynôme caractéristique est scindé dans $\mathbb{R}$.

Solution

1) $\begin{vmatrix} -X & 1 & 2 \\ -2 & 3-X & 6 \\ -3 & 3 & 15-X \end{vmatrix} = \begin{vmatrix} 1-X & 1 & 2 \\ 1-X & 3-X & 6 \\ 0 & 3 & 15-X \end{vmatrix}$ conduit à :

$$\det\left(A - XI_3\right) = (1-X)\left(X^2 - 17X + 18\right).$$

Et $X^2 - 17X + 18$ est scindé dans $\mathbb{R}$.

Alors A est diagonalisable puisque son polynôme caractéristique est scindé à racines simples.

2) $\begin{vmatrix} 1-X & 0 & 0 \\ 0 & -X & 1 \\ 0 & -1 & -X \end{vmatrix} = (1-X)\left(X^2+1\right)$ n'est pas scindé dans $\mathbb{R}$, donc B n'est pas trigonalisable dans $\mathcal{M}_3(\mathbb{R})$.

Commentaires

Colonne 1 + colonne 2.

Discriminant positif.

Donc trigonalisable !

Ex. 8

1) Calculer le polynôme caractéristique χ_A de $A = \begin{pmatrix} -6 & 5 & -3 \\ -17 & 13 & -7 \\ -13 & 9 & -4 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$. A est-elle diagonalisable ?

1) Prouver qu'il existe $\lambda \in \mathbb{R}$ tel que $B = A - \lambda I_3$ soit nilpotente.

2) En déduire qu'il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que : $P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Indications

On peut utiliser le théorème de Cayley-Hamilton pour obtenir un polynôme annulateur de A.

Pour $f \in \mathcal{L}(\mathbb{R}^3)$ tel que $f^2 \neq 0$ et $f^3 = 0$, il existe une base $\left(a, f(a), f^2(a)\right)$.

Solution

1) On obtient $\chi_A(X) = (1-X)^3$: 1 est valeur propre triple, A n'est donc pas diagonalisable.

2) On a $\left(A - I_3\right)^3 = 0$ donc $B = A - I_3$ est nilpotente.

Le calcul donne $B^2 = \begin{pmatrix} 3 & -2 & 1 \\ 6 & -4 & 2 \\ 3 & -2 & 1 \end{pmatrix}$: B est nilpotente d'indice 3.

Commentaires

Sinon, on aurait $A = I_3$.

Théorème de Cayley-Hamilton.

3) Soit $f \in \mathcal{L}(\mathbb{R}^3)$ nilpotent d'indice 3 : $f^3 = 0, f^2 \neq 0$. Il existe $a \in \mathbb{R}^3$ tel que $f^2(a) \neq 0$, alors $\left(a, f(a), f^2(a)\right)$ est une base de $\mathbb{R}^3$.

Voir chapitre 3, propriété 26.

En posant $u_1 = f^2(a)$, $u_2 = f(a)$, $u_3 = a$, on a :

$$\mathrm{mat}_{(u_i)_{1\leqslant i\leqslant 3}} f = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Sur la base $(u_i)_{1 \leqslant i \leqslant 3}$.

Appliquons ce résultat avec $f \in \mathcal{L}(\mathbb{R}^3)$ tel que $B = \mathrm{mat}_{(e_i)_{1\leqslant i\leqslant 3}} f$.

$(e_i)_{1 \leqslant i \leqslant 3}$ base canonique de $\mathbb{R}^3$.

On peut donc choisir :

La lecture de B^2 montre que $f^2(e_3) \neq 0$.

$$\begin{array}{rcll} u_3 & = & e_3 & = (0,0,1) \\ u_2 & = & f(e_3) & = (-3,-7,-5) \\ u_1 & = & f^2(e_3) & = (1,2,1) \end{array}$$

d'où la matrice de passage de $(e_i)_{1\leqslant i\leqslant 3}$ à $(u_i)_{1\leqslant i\leqslant 3}$:

$$P = \begin{pmatrix} 1 & -3 & 0 \\ 2 & -7 & 0 \\ 1 & -5 & 1 \end{pmatrix}$$

On a $P^{-1}BP = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$ donc $P^{-1}AP = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Par construction de la base $(u_i)_{1\leqslant i\leqslant 3}$.

III. Théorème de Cayley-Hamilton

Ex. 9

Soit $A = \begin{pmatrix} 8 & -1 & -5 \\ -2 & 3 & 1 \\ 4 & -1 & -1 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$ et $f \in \mathcal{L}(\mathbb{R}^3)$ de matrice A dans la base canonique $\left(e_i\right)_{1\leqslant i\leqslant 3}$ de $\mathbb{R}^3$.

1) Calculer le polynôme caractéristique χ_A. La matrice A est-elle diagonalisable ?

2) Justifier que $\mathbb{R}^3 = \mathrm{Ker}\left(f - 2\,\mathrm{Id}_{\mathbb{R}^3}\right) \oplus \mathrm{Ker}\left(f - 4\,\mathrm{Id}_{\mathbb{R}^3}\right)^2$.

On pose $F_1 = \mathrm{Ker}\left(f - \mathrm{Id}_{\mathbb{R}^3}\right)$ et $F_2 = \mathrm{Ker}\left(f - 4\,\mathrm{Id}_{\mathbb{R}^3}\right)^2$ et soit $g \in \mathcal{L}\left(F_2\right)$ l'endomorphisme de F_2 induit par f, calculer $\left(g - 4\,\mathrm{Id}_{F_2}\right)^2$. En déduire qu'il existe $P \in \mathrm{GL}_3(\mathbb{R})$, que l'on explicitera, telle que :

$$P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{pmatrix}.$$

Indications

Si λ est une valeur propre d'ordre m, il faut que son sous-espace propre soit de dimension m pour que la matrice soit diagonalisable. Le théorème de décomposition des noyaux permet de mettre en évidence des sous-espaces stables.

Solution

1) On obtient $\chi_A = \det(A - XI_3) = (2 - X)(4 - X)^2$.

$A - 4I_3 = \begin{pmatrix} 4 & -1 & -5 \\ -2 & -1 & 1 \\ 4 & -1 & -5 \end{pmatrix}$ montre que :

$$\dim \mathrm{Ker}\left(f - 4\,\mathrm{Id}_{\mathbb{R}^3}\right) = 1.$$

Ainsi f (et donc A) n'est pas diagonalisable.

Commentaires

Calcul préliminaire.

$A - 4I_3$ n'est visiblement pas de rang 1.

Copyrighted material

2) χ_A est polynôme annulateur de f donc, d'après le théorème de décomposition des noyaux, on a :

$$\mathbb{R}^3 = \operatorname{Ker}\left(f - 2\operatorname{Id}_{\mathbb{R}^3}\right) \oplus \left(f - 4\operatorname{Id}_{\mathbb{R}^3}\right)^2.$$

Les polynômes $X-2$ et $(X-4)^2$ sont premiers entre eux.

$\mathbb{R}^3 = F_1 \oplus F_2$.

- $\operatorname{Ker}\left(f - 4\operatorname{Id}_{\mathbb{R}^3}\right)^2$ est stable par f, ce qui assure l'existence de g endomorphisme de F_2 induit par f.
Pour $x \in F_2$, on a $\left(f - 4\operatorname{Id}_{\mathbb{R}^3}\right)^2(x) = 0$ donc $\left(g - 4\operatorname{Id}_{F_2}\right)^2(x) = 0$ ce qui prouve $\left(g - 4\operatorname{Id}_{F_2}\right)^2 = 0$.

f et $(f-4\operatorname{Id}_{\mathbb{R}^3})^2$ commutent.

- On a $\dim F_2 = 2$ et $\dim \operatorname{Ker}\left(g - 4\operatorname{Id}_{F_2}\right) = 1$ donc $h = g - 4\operatorname{Id}_{F_2}$ est un endomorphisme de F_2 nilpotent d'indice 2 : $h^2 = 0$ et $h \neq 0$.
Il existe $b \in F_2$ tel que $h(b) \neq 0$, $\left(h(b), b\right)$ est une base de F_2 telle que :

$$\operatorname{mat}_{(h(b),b)} h = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{donc} \quad \operatorname{mat}_{(h(b),b)} g = \begin{pmatrix} 4 & 1 \\ 0 & 4 \end{pmatrix}.$$

Car $\mathbb{R}^3 = F_1 \oplus F_2$ et $\dim F_1 = 1$.

- Avec a vecteur propre de f associé à la valeur propre 2, $\left(a, f(b), b\right)$ est une base de $\mathbb{R}^3$ telle que : $\operatorname{mat}_{(a,f(b),b)} f = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{pmatrix}$.

$F_1 = \mathbb{R}a$.

- Le calcul donne : $(A - 4I_3)^2 = \begin{pmatrix} -2 & 2 & 4 \\ -2 & 2 & 4 \\ -2 & 2 & 4 \end{pmatrix}$.

Une base de F_2 est donc (u, v) avec $u = (1, 1, 0)$ et $v = (1, -1, 1)$. On obtient $\left(g - 4\operatorname{Id}_{F_2}\right)(u) = (3, -3, 3)$, on prendra donc :

$$b = (1, 1, 0) \ , \ h(b) = (3, -3, 3).$$

De plus $A - 2I_3 = \begin{pmatrix} 6 & -1 & -5 \\ -2 & 1 & 1 \\ 4 & -1 & -3 \end{pmatrix}$ d'où $F_1 = \mathbb{R}a$ avec $a = (1, 1, 1)$.

Finalement $P = \begin{pmatrix} 1 & 3 & 1 \\ 1 & -3 & 1 \\ 1 & 3 & 0 \end{pmatrix}$ donne $P^{-1}AP = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{pmatrix}$.

$P^{-1} = \frac{1}{6}\begin{pmatrix} -3 & 3 & 6 \\ 1 & -1 & 0 \\ 6 & 0 & -6 \end{pmatrix}$.

Ex. 10

Calculer A^n pour $A = \begin{pmatrix} 2 & -1 & 2 \\ 5 & -3 & 3 \\ -1 & 0 & -2 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$, $n \in \mathbb{N}^*$.

Indications

On divise X^n par le polynôme caractéristique de A et on utilise le théoème de Cayley-Hamilton.

Solution

On trouve $P_A(X) = -(X+1)^3$. La division euclidienne de X^n par $(X+1)^3$ s'écrit : $X^n = (X+1)^3 Q(X) + aX^2 + bX + c$. (1)

On en déduit $nX^{n-1} = 3(X+1)^2 Q(X) + (X+1)^3 Q'(X) + 2aX + b$ (2)

et $n(n-1)X^{n-2} = 6(X+1)Q(X) + 6(X+1)^2 Q'(X) + (X+1)^3 Q''(X) + 2a$ (3)

On obtient : $\begin{cases} (-1)^n = a - b + c \\ n(-1)^{n-1} = -2a + b \\ n(n-1)(-1)^{n-2} = 2a \end{cases}$

Commentaires

Par deux dérivations successives.

En substituant à X la valeur -1 dans (1), (2) et (3).

Hidden page

Hidden page

Solution

1) Le polynôme caractéristique de A est $P_A(X) = -(1+X)^3$.

$A + I_3 = \begin{pmatrix} 0 & a & a \\ -1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ est de rang 2. Le sous-espace propre associé à -1 est engendré par $V_1 = (0,-1,1)$. V_2 et V_3 doivent vérifier :

$$(A + I_3)V_2 = V_1 \text{ et } (A + I_3)V_3 = V_2.$$

$V_2 = (1,0,0)$ et $V_3 = \frac{1}{a}(0,1,0)$ conviennent.

A est ainsi semblable à $T = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$.

2) $B = A + I_3$ vérifie $B^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -a & -a \\ 0 & a & a \end{pmatrix}$ et $B^3 = 0$.

On en déduit $A^n = (-1)^n \left(I_3 - nB + \frac{n(n-1)}{2} B^2 \right)$, c'est-à-dire :

$$A^n = (-1)^n \begin{pmatrix} 1 & -na & -na \\ n & 1 - n(n-1)\frac{a}{2} & -n(n-1)\frac{a}{2} \\ -n & n(n-1)\frac{a}{2} & 1 + n(n-1)\frac{a}{2} \end{pmatrix}.$$

Avec $A = -I_3 + B$ et, pour tout $n \in \mathbb{N}$, $n \geqslant 2$:

$$\frac{1}{n!}(xA)^n = (-1)^n \frac{x^n}{n!} I_3 + x(-1)^{n-1} \frac{x^{n-1}}{(n-1)!} B + \frac{x^2}{2}(-1)^{n-2} \frac{x^{n-2}}{(n-2)!} B^2,$$

il vient finalement $\exp(xA) = e^{-x} \left(I_3 + xB + \frac{x^2}{2} B^2 \right)$, c'est-à-dire :

$$\exp(xA) = e^{-x} \begin{pmatrix} 1 & ax & ax \\ -x & 1 - \frac{1}{2}ax^2 & -\frac{1}{2}ax^2 \\ x & \frac{1}{2}ax^2 & 1 + \frac{1}{2}ax^2 \end{pmatrix}.$$

Commentaires

Règle de Sarrus par exemple. Noter que $P_A(X)$ ne dépend pas de a.

$a \neq 0$. Le sous-espace propre est de dimension 1. $AV_1 = -V_1$.

On cherche des antécédents simples.

V_1, V_2, V_3 sont indépendants.

Formule du binôme et B nilpotente.

VI. Questions de densité

Ex. 15

1) Montrer que $\mathrm{GL}_n(\mathbb{K})$ est dense dans $\mathcal{M}_n(\mathbb{K})$.

2) Montrer que pour tout couple (A, B) de $\mathcal{M}_n(\mathbb{K})$, AB et BA ont même polynôme caractéristique.

3) Soit A et M dans $\mathcal{M}_n(\mathbb{K})$ telles que A est nilpotente et $AM = MA$. Montrer que $\det(A + M) = \det M$.

Indications

$\mathcal{M}_n(\mathbb{K})$ est supposé muni d'une norme quelconque qu'il est inutile de préciser plus puisque l'on sait que, sur un espace de dimension finie, toutes les normes sont équivalentes.

1) Pour tout $A \in \mathcal{M}_n(\mathbb{K})$, considérer les matrices $A_p = A - \frac{1}{p} I_n$.

2) Envisager d'abord le cas où l'une des matrices est inversible.

3) Commercer par le cas où $M = I_n$.

Copyrighted material

Solution

1) Étant donné $A \in \mathcal{M}_n(\mathbb{K})$, pour tout $p \in \mathbb{N}^*$, posons $A_p = A - \frac{1}{p} I_n$.

Il est clair que $\lim\limits_{p \to +\infty} A_p = A$.

A_p est non inversible lorsque $\det\left(A - \frac{1}{p} I_n\right) = 0$, c'est-à-dire lorsque $\frac{1}{p}$ est valeur propre de A, donc, puisque A admet au plus n valeurs propres distinctes, l'ensemble $\left\{p \in \mathbb{N}^* \,/\, \frac{1}{p} \in \mathrm{Sp}(A)\right\}$ est fini et il existe $p_0 \in \mathbb{N}$ tel que, pour $p \geqslant p_0$, on ait $\frac{1}{p} \notin \mathrm{Sp}(A)$. En conséquence, $\left(A_p\right)_{p \geqslant p_0}$ est une suite de $\mathrm{GL}_n(\mathbb{K})$ convergeant vers A ce qui montre que $A \in \overline{\mathrm{GL}_n(\mathbb{K})}$. On a ainsi prouvé que $\mathcal{M}_n(\mathbb{K}) = \overline{\mathrm{GL}_n(\mathbb{K})}$.

2) Supposons dans un premier temps que $A \in \mathrm{GL}_n(\mathbb{K})$. On a alors pour tout $x \in \mathbb{K}$, $AB - xI_n = A\left(B - xA^{-1}\right)$ et $BA - xI_n = \left(B - xA^{-1}\right)A$ donc :

$$\begin{aligned} \chi_{AB}(x) &= \det\left(AB - xI_n\right) = \det A \det\left(B - xA^{-1}\right) \\ &= \det\left(BA - xI_n\right) \\ &= \chi_{BA}(x) \end{aligned}$$

Il en résulte : $\chi_{AB} = \chi_{BA}$.

Pour généraliser la propriété, remarquons d'abord que si, pour $M \in \mathcal{M}_n(\mathbb{K})$ on pose $\chi_M = \sum\limits_{k=0}^{n} a_k(M) X^k$, les a_k sont des fonctions continues sur $\mathcal{M}_n(\mathbb{K})$ puisqu'il s'agit de fonctions polynômes par rapport aux coefficients m_{ij} de M.

Étant donné $A \in \mathcal{M}_n(\mathbb{K})$, considérons une suite $\left(A_p\right)_{p \in \mathbb{N}}$ de matrices inversibles convergeant vers A. Le produit matriciel étant une application continue sur $\mathcal{M}_n(\mathbb{K})^2$ on obtient alors :

$$AB = \lim_{p \to +\infty} \left(A_p B\right) \text{ et } BA = \lim_{p \to +\infty} BA_p$$

donc, par continuité des a_k, il vient :

$$\forall k \in [\![0, n]\!],\ a_k(AB) = \lim_{p \to +\infty} a_k\left(A_p B\right)$$

$$\text{et } a_k(BA) = \lim_{p \to +\infty} a_k\left(BA_p\right)$$

Or l'étude du premier cas nous donne :

$$\forall k \in [\![0, n]\!], \forall p \in \mathbb{N},\ a_k\left(A_p B\right) = a_k\left(BA_p\right)$$

d'où finalement $\forall k \in [\![0, n]\!],\ a_k(AB) = a_k(BA)$ et donc $\chi_{AB} = \chi_{BA}$.

3) Envisageons d'abord le cas où $M = I_n$.

A étant nilpotente, il existe $P \in \mathrm{GL}_n(\mathbb{C})$ telle que $P^{-1}AP = T$ où T est triangulaire supérieure de diagonale nulle. Avec :

$$T = \begin{bmatrix} 0 & \times & \cdots & \times \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \times \\ 0 & \cdots & \cdots & 0 \end{bmatrix} \text{ il vient } P^{-1}\left(A + I_n\right)P = \begin{bmatrix} 1 & \times & \cdots & \times \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \times \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

donc $\det\left(A + I_n\right) = \det\left(P^{-1}\left(A + I_n\right)P\right) = 1 = \det M$.

Commentaires

Car $\| A_p - A \| = \frac{1}{p} \| I_n \|$.

Car $\deg \det(A - XI_n) = n$.

Pour les déterminants on sait que
$\det(MN) = \det(NM)$
$= \det N \det M$

Dans $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$, l'égalité des fonctions polynômes donne l'égalité des polynômes χ_{AB} et χ_{BA}.

$a_k : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$.

Utilisaton de la densité de $\mathrm{GL}_n(\mathbb{K})$ dans $\mathcal{M}_n(\mathbb{K})$.

$A_p \in \mathrm{GL}_n(\mathbb{K})$ donne $\chi_{A_p B} = \chi_{BA_p}$.

A étant nilpotente, on a $\mathrm{Sp}(A) = \{0\}$ et dans $\mathcal{M}_n(\mathbb{C})$ toute matrice est trigonalisable.

La propriété est démontrée dans ce premier cas

Supposons maintenant M inversible.
On a alors $A+M=\left(AM^{-1}+I_n\right)M$, donc :

$$\det(A+M)=\det M\det\left(AM^{-1}+I_n\right)$$
$$=\det M\det\left(B+I_n\right) \text{ où on a posé } B=AM^{-1}.$$

A et M^{-1} sont permutables donc $B^n=A^n\left(M^{-1}\right)^n=0$. Ainsi B est nilpotente et l'étude du premier cas donne $\det\left(B+I_n\right)=1$ d'où $\det(A+M)=\det M$.

$AM=MA$ donne $M^{-1}A=AM^{-1}$.

Dans le cas général, pour toute matrice M, on a $M=\lim\limits_{\lambda\to 0}M+\lambda I_n$ et les matrices $M+\lambda I_n$ sont inversibles pour $|\lambda|$ assez petit.

C'est encore la densité de $\mathrm{GL}_n(\mathbb{K})$ dans $\mathcal{M}_n(\mathbb{K})$ et, cela se prouve exactement comme dans le 1).

On obtient alors $\det(A+M)=\lim\limits_{\lambda\to 0}\det\left(A+M+\lambda I_n\right)$, puis d'après l'étude du deuxième cas : $\det\left(A+M+\lambda I_n\right)=\det\left(M+\lambda I_n\right)$ dès que $M+\lambda I_n$ est inversible, donc :

$$\det(A+M)=\lim_{\lambda\to 0}\det\left(M+\lambda I_n\right)$$

$\lambda\mapsto\det(A+M+\lambda I_n)$ est une fonction polynôme continue.

c'est-à-dire : $\det(A+M)=\det M$.

Par continuité de $\lambda\mapsto\det(M+\lambda I_n)$.

Ex. 16

1) Soit $\mathfrak{D}_n(\mathbb{C})$ l'ensemble des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{C})$, montrer que $\mathfrak{D}_n(\mathbb{C})$ est dense dans $\mathcal{M}_n(\mathbb{C})$.

2) Retrouver le théorème de Cayley-Hamilton en commençant par le cas des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{C})$.

Indications

1) Pour $A\in\mathcal{M}_n(\mathbb{C})$, construire une suite de matrices de valeurs propres deux à deux distinctes et convergeant vers A.

Solution

1) a) Toute matrice $A\in\mathcal{M}_n(\mathbb{C})$ est trigonalisable dans $\mathcal{M}_n(\mathbb{C})$. En posant $\chi_A(X)=\prod\limits_{k=1}^{n}\left(\lambda_k-X\right)$, il existe $P\in\mathrm{GL}_n(\mathbb{C})$ telle que $P^{-1}AP=T$ où T est triangulaire supérieure de diagonale $\left[\lambda_1,\ldots,\lambda_n\right]$.
Pour tout $p\in\mathbb{N}^*$, posons :

$$T_p=T+\mathrm{diag}\left(\frac{1}{p},\frac{2}{p},\ldots,\frac{n}{p}\right) \text{ et } A_p=PT_pP^{-1}.$$

On a clairement $\lim\limits_{p\to+\infty}T_p=T$ donc, par continuité du produit matriciel,

$$\lim_{p\to+\infty}A_p=A. \qquad (1)$$

Montrons maintenant que, pour p assez grand, les scalaires $\mu_k=\lambda_k+\frac{k}{p}$, $1\leqslant k\leqslant n$, sont deux à deux distincts.

- Premier cas : $\lambda_1=\lambda_2=\cdots=\lambda_n$. Les $\frac{k}{p}$ étant deux à deux distincts, il en est de même pour les μ_k quel que soit $p\in\mathbb{N}^*$.

Pour tout $(i,j)\in[\![1,n]\!]^2$, $\mu_i-\mu_j=\frac{i-j}{p}$.

- Deuxième cas : il existe $(i,j)\in[\![1,n]\!]^2$ tel que $\lambda_i\neq\lambda_j$. Posons alors

$$r=\frac{1}{2}\min\left\{\left|\lambda_i-\lambda_j\right| / (i,j)\in[\![1,n]\!]^2,\lambda_i\neq\lambda_j\right\}\text{ ; on a } r>0.$$

$2r$ est le plus petit élément d'un ensemble fini, non vide, de réels strictement positifs.

Pour tout $(i,j)\in[\![1,n]\!]^2$ tel que $\lambda_i\neq\lambda_j$, les boules ouvertes $\mathcal{B}_o\left(\lambda_i,r\right)$ et $\mathcal{B}_o\left(\lambda_j,r\right)$ sont disjointes car, s'il existait $z\in\mathcal{B}_o\left(\lambda_i,r\right)\cap\mathcal{B}_o\left(\lambda_j,r\right)$, on aurait $\left|\lambda_i-\lambda_j\right|\leqslant|\lambda_i-z|+\left|z-\lambda_j\right|<2r$ ce qui est contraire à la définition de r.

$\mathcal{B}_o(\lambda_i,r)=\{z\in\mathbb{C}/|\lambda_i-z|<r\}$.

Commentaires

Car $\chi_A(X)$ est scindé dans $\mathbb{C}[X]$. Avec cette convention, les λ_i ne sont pas supposés deux à deux distincts : chaque valeur propre apparaît dans la liste $[\lambda_1,\lambda_2,\ldots,\lambda_n]$ un nombre de fois égal à son ordre de multiplicité.

Copyrighted material

Hidden page

Exercices

Niveau 1

Ex. 1

Diagonaliser la matrice

$$A = \begin{pmatrix} a & & & b \\ & \ddots & \iddots & \\ & & a+b & \\ & \iddots & & \ddots \\ b & & & a \end{pmatrix} \in \mathcal{M}_{2n-1}(\mathbb{R}).$$

Ex. 2

Soit u, v, f trois endomorphismes de E, $\mathbb{K}$-espace vectoriel de dimension finie tels qu'il existe $(\lambda, \mu) \in \mathbb{K}^2$ avec :

$f = \lambda u + \mu v, f^2 = \lambda^2 u + \mu^2 v, f^3 = \lambda^3 u + \mu^3 v.$ (1)

Montrer que f est diagonalisable.

Ex. 3

Diagonaliser $A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ et montrer que l'on peut choisir la matrice de passage telle que $P^{-1} = P$.

Ex. 4

Trouver les sous-espaces de $\mathbb{R}^3$ stables par u canoniquement associé à : $A = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 2 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.

Ex. 5

Trouver les puissances de $M = \begin{pmatrix} 1 & 4 & 2 \\ 0 & -3 & -2 \\ 0 & 4 & 3 \end{pmatrix}$.

Niveau 2

Ex. 6

Diagonaliser la matrice :

$$A = \begin{pmatrix} 2 & 1 & & (0) \\ 1 & 2 & \ddots & \\ & \ddots & \ddots & 1 \\ (0) & & 1 & 2 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R}).$$

Ex. 7

Soit $A \in \mathcal{M}_n(\mathbb{C})$ et $B = {}^t\mathrm{com}\, A$. Montrer que tout vecteur propre de A est vecteur propre de B.

Ex. 8

Soit $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_2(\mathbb{R})$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$ deux matrices diagonalisables. Montrer que :

$C = \begin{pmatrix} b_1 A & b_2 A \\ b_3 A & b_4 A \end{pmatrix} \in \mathcal{M}_{2n}(\mathbb{R})$ est diagonalisable.

Ex. 9

1) Soit $A \in \mathcal{M}_n(\mathbb{K})$ admettant n valeurs propres deux à deux distinctes et $B \in \mathcal{M}_n(\mathbb{K})$ telle que $B^2 = A$.

Montrer que B est diagonalisable.

2) Trouver toutes les matrices $B \in \mathcal{M}_3(\mathbb{R})$ telles que :

$$B^2 = \begin{pmatrix} 11 & -5 & 5 \\ -5 & 3 & -3 \\ 5 & -3 & 3 \end{pmatrix}.$$

Ex. 10

Soit E un $\mathbb{C}$-espace vectoriel de dimension n et u, f, g des endomorphismes de E tels que $u \circ f = g \circ u$ et $\mathrm{rg}(u) = r \geqslant 1$.

Montrer que les polynômes caractéristiques χ_f et χ_g ont au moins une diviseur communs de degré $\geqslant r$.

Ex. 11

Soit $A = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 4 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$. Trouver les matrices $X \in \mathcal{M}_3(\mathbb{R})$ telles que $X^2 = A$. (1)

Ex. 12

Soit E un $\mathbb{R}$-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$ tel que $u^3 = u$.

Trouver les sous-espaces de E stables par u.

Copyrighted material

Ex. 13

Soit E un $\mathbb{R}$-espace vectoriel et $f \in \mathscr{L}(E)$ pour lequel il existe $P \in \mathbb{R}[X]$ tel que $P(0) = 0$, $P'(0) \neq 0$ et $P(f) = 0$.

Montrer que $E = \operatorname{Im} f \oplus \operatorname{Ker} f$.

Ex. 14

1) Soit $A \in \mathscr{M}_n(\mathbb{K})$:

$$A = \begin{bmatrix} 0 & & & 1 \\ 1 & \ddots & (0) & \\ (0) & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}.$$

Montrer que A est diagonalisable.

2) Soit $(a_1, \ldots, a_n) \in \mathbb{C}^n$, calculer $\det M$ avec :

$$M = \begin{bmatrix} a_n & a_{n-1} & \cdots & a_2 & a_1 \\ a_1 & \ddots & \ddots & & a_2 \\ a_2 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{n-1} \\ a_{n-1} & \cdots & a_2 & a_1 & a_n \end{bmatrix}.$$

Expliciter les cas $n = 3$ et $n = 4$.

Niveau 3

Ex. 15

Soit f et g deux endomorphismes permutables d'un $\mathbb{C}$-espace vectoriel E de dimension finie ($f \circ g = g \circ f$).

1) Montrer que f et g ont au moins un vecteur propre commun.

2) Montrer qu'il existe une base de E dans laquelle les matrices de f et g sont triangulaires supérieures.

3) Montrer que si f et g sont diagonalisables, il existe une base de E dans laquelle les matrices f et g sont diagonales.

Ex. 16

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie n et u un endomorphisme de E. On pose :

$$\mathscr{C}(u) = \{v \in \mathscr{L}(E) / u \circ v = v \circ u\}$$

(ensemble des commutants de u).

1) Vérifier que $\mathscr{C}(u)$ est une sous-algèbre de $\mathscr{L}(E)$ contenant $\mathbb{K}[u]$, algèbre des polynômes en u.

2) On suppose u diagonalisable :

$$E = \bigoplus_{i=1}^{p} E_u(\lambda_i)$$

où $E_u(\lambda_i) = \operatorname{Ker}(u - \lambda_i \operatorname{Id}_E)$ et $\lambda_1, \ldots, \lambda_p$ étant les valeurs propres distinctes de u.

Soit $\mathscr{B} = (e_i)_{1 \leqslant i \leqslant n}$ une base adaptée à la somme directe $E = \bigoplus_{i=1}^{p} E_u(\lambda_i)$.

Montrer que $v \in \mathscr{L}(E)$ est un commutant de u si et seulement si $\operatorname{mat}_{\mathscr{B}} v$ est de la forme :

$$A = \begin{pmatrix} A_1 & & & (0) \\ & A_2 & & \\ (0) & & \ddots & \\ & & & A_p \end{pmatrix}$$

avec $A_i \in \mathscr{M}_{m_i}(\mathbb{K})$ et $m_i = \dim E_u(\lambda_i)$.

En déduire $\dim \mathscr{C}(u)$.

3) Soit $A = \begin{pmatrix} 1 & 3 & -2 \\ -1 & -1 & 2 \\ 2 & 2 & -4 \end{pmatrix} \in \mathscr{M}_3(\mathbb{R})$ et $u \in \mathscr{L}(\mathbb{R}^3)$ canoniquement associé à A.

Déterminer $\mathscr{C}(u)$.

Montrer que $\mathscr{C}(u) = \operatorname{Vect}\{\operatorname{Id}_E, u, u^2\}$.

4) Dans le cas général, hypothèses du 2), montrer que $\mathscr{C}(u) = \mathbb{K}[u]$ si et seulement si u n' a que des valeurs propres simples.

Ex. 17

Soit $A = \begin{pmatrix} 1 & -3 & -3 \\ -3 & 1 & -3 \\ 3 & 3 & 7 \end{pmatrix} \in \mathscr{M}_3(\mathbb{R})$.

Résoudre l'équation $M^2 = A$ **(1)** avec $M \in \mathscr{M}_3(\mathbb{R})$.

Ex. 18

Soit $A = \begin{pmatrix} -2 & 1 & 1 \\ 8 & 1 & -5 \\ 4 & 3 & -3 \end{pmatrix} \in \mathscr{M}_3(\mathbb{R})$ et $f \in \mathscr{L}(\mathbb{R}^3)$ tel que $A = \operatorname{mat}_{\mathscr{B}} f$ où $\mathscr{B} = (e_1, e_2, e_3)$ est la base canonique de $\mathbb{R}^3$. On posera $\mathbb{R}^3 = E$.

1) Trouver les droites de E stables par f.

2) Soit P un plan de E stable par f, montrer que soit $P = \operatorname{Ker}(f^2 + 2f)$ soit $P = \operatorname{Ker}(f + 2\operatorname{Id}_E)^2$. En déduire les plans de E stables par f.

Copyrighted material

Indications

Ex. 6

Associer au système définissant un vecteur propre, une suite récurrente linéaire d'ordre 2.

On montrera que A admet n valeurs propres distinctes.

Ex. 7

Distinguer les cas :

$$\operatorname{rg} A = n\,,\ \operatorname{rg} A = n-1\,,\ \operatorname{rg} A \leqslant n-2.$$

Ex. 8

On travaille avec des matrices diagonales semblables à A et à B.

C est semblable à une matrice diagonale par blocs.

Ex. 9

A et B sont permutables.

Avec $P^{-1}AP$ diagonale, former $P^{-1}BP$.

Ex. 10

$\operatorname{rg} U = r$, il existe P et Q dans $\mathrm{GL}_n(\mathbb{C})$ telles que :

$$PUQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Commencer par le cas $U = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Ex. 11

Étudier les sous-espaces propres de A.

Noter que, si X est solution, alors A et X commutent. On en déduit des conditions nécessaires sur la forme des colonnes 2 et 3.

Ex. 12

Le polynôme annulateur de u permet de décomposer E en somme directe (décomposition des noyaux).

Faire apparaître des sous-espaces des trois noyaux mis en évidence.

Ex. 13

$P = XQ$, $Q(0) \neq 0$. Montrer que $E = \operatorname{Ker} f \oplus \operatorname{Ker} Q(f)$.

On peut donner une démonstration en dimension finie.

Ex. 14

1) $A^n = I_n$.

2) $M = \sum_{k=1}^{n} a_k A^k$.

Ex. 15

1) Si des endomorphismes commutent, le noyau de l'un est stable par l'autre.

2) Procéder par récurrence sur la dimension de E.

3) Décomposer E en somme directe des sous-espaces propres.

Ex. 16

1) et **2)** S'inspirer de l'exercice précédent.

3) Il y a trois valeurs propres réelles.

Utiliser alors **2)**.

4) Le théorème de Cayley-Hamilton montre que u^n est dans le sous-espace engendré par :

$$\mathrm{Id}_E\,,\ u,\ \dots\,,\ u^{n-1}.$$

D'où $\dim \mathbb{K}[u] \leqslant n$.

Ex. 17

Justifier que A est diagonalisable.

Observer que si M est solution, alors $AM = MA$.

Étudier ensuite les racines carrées d'une matrice diagonale.

Ex. 18

1) Noter que A n'est pas diagonalisable.

2) Démontrer d'abord l'inclusion :

$$P \subset \operatorname{Ker}\left(f^2 + 2f\right) \text{ ou } P \subset \operatorname{Ker}\left(f + 2\,\mathrm{Id}_E\right)^2.$$

Copyrighted material

Solutions des exercices

Quand il n'y a pas d'ambiguïté, on convient de nommer de la même façon une matrice et l'endomorphisme canoniquement associé. Cela permet de noter $\mathrm{Ker}(A-\lambda I)$ ou $\mathrm{Ker}\left(A-\lambda I_n\right)$ les sous-espaces propres de A.

Niveau 1

Ex. 1

Soit $\left(e_j\right)_{1\leqslant j\leqslant 2n-1}$ la base canonique de $\mathbb{R}^{2n-1}$ et $f\in\mathcal{L}\left(\mathbb{R}^{2n-1}\right)$ canoniquement associé à A.

On constate $\forall j\in[\![1,2n-1]\!], f\left(e_j\right)=ae_j+be_{2n-j}$ d'où :

$$f\left(e_j+e_{2n-j}\right)=(a+b)\left(e_j+e_{2n-j}\right)\ .\ f\left(e_j-e_{2n-j}\right)=(a-b)\left(e_j-e_{2n-j}\right).$$

Notons alors :

$$c_j=\begin{cases} e_j+e_{2n-j} & \text{pour } 1\leqslant j\leqslant n\\ e_j-e_{2n-j} & \text{pour } n+1\leqslant j\leqslant 2n-1\end{cases}$$

La matrice du système $\left(c_j\right)_{1\leqslant j\leqslant 2n-1}$ dans la base $\left(e_j\right)_{1\leqslant j\leqslant 2n-1}$ est :

$$P=\begin{pmatrix} 1 & & & 0 & & & -1\\ & \ddots & & & & \iddots & \\ & & 1 & & -1 & & \\ 0 & & & 2 & & & 0\\ & & 1 & & 1 & & \\ & \iddots & & & & \ddots & \\ 1 & & & 0 & & & 1\end{pmatrix}\in \mathrm{GL}_{2n-1}(\mathbb{R}).$$

Donc $\left(c_j\right)_{1\leqslant j\leqslant 2n-1}$ est une base de $\mathbb{R}^{2n-1}$ formée de vecteurs propres de f : f et A sont diagonalisables.

Si $b\neq 0$, f admet deux valeurs propres distinctes $(a+b)$ et $(a-b)$, les sous-espaces propres associés ayant pour bases respectives $\left(c_j\right)_{1\leqslant j\leqslant n}$ et $\left(c_k\right)_{n+1\leqslant k\leqslant 2n-1}$.

Ex. 2

Des relations **(1)**, on tire $(\lambda+\mu)f^2=\lambda^3u+\mu^3v+\lambda\,\mu\,(\lambda u+\mu v)$ c'est-à-dire :

$$f^3-(\lambda+\mu)f^2+\lambda\,\mu\,f=0.$$

Ainsi $P(X)=X^3-(\lambda+\mu)X^2+\lambda\,\mu\,X=X(X-\lambda)(X-\mu)$ est polynôme annulateur de f.

- Si $0,\lambda,\mu$ sont distincts, P n'a que des racines simples et f est diagonalisable (cf. théorème 12).
- Si $\lambda=\mu=0$, $f=0$ est diagonalisable.
- Si $\lambda=0,\mu\neq 0$: $f=\mu v, f^2=\mu^2 v$ donne $v^2=v$, v est un projecteur donc est diagonalisable : $f=\mu v$ est diagonalisable.
- Si $\lambda\neq 0,\mu=0$: $f=\lambda u$, le cas est identique au précédent (u est un projecteur).
- Si $\lambda=\mu\neq 0$: $f=\lambda(u+v), f^2=\lambda^2(u+v)$ donne $(u+v)^2=u+v$, ce cas est encore identique aux deux précédents, ($u+v$ est un projecteur).

Ex. 3

Polynôme caractéristique : $\chi_A(X)=(3-X)(3+X)(1-X)(1+X)$. Avec quatre valeurs propres distinctes, A est diagonalisable dans $\mathcal{M}_4(\mathbb{R})$. Chaque sous-espace propre est de dimension 1 : nous en donnons un système d'équations et un vecteur directeur.

$$\lambda=1 \qquad \mathrm{Ker}(A-I)\begin{cases} -x+y=0\\ 3x-y+2z=0\\ z-t=0\end{cases} \qquad \text{vecteur directeur } \begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}$$

Copyrighted material

$$\lambda = -1 \qquad \mathrm{Ker}(A+I)\begin{cases} x+y=0 \\ 3x+y+2z=0 \\ z+t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

$$\lambda = 3 \qquad \mathrm{Ker}(A-3I)\begin{cases} -3x+y=0 \\ 3x-3y+2z=0 \\ z-3t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 1 \\ 3 \\ 3 \\ 1 \end{pmatrix}$$

$$\lambda = -3 \qquad \mathrm{Ker}(A+3I)\begin{cases} 3x+y=0 \\ 3x+3y+2z=0 \\ z+3t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 1 \\ -3 \\ 3 \\ -1 \end{pmatrix}$$

Choix de P

- Si P diagonalise A : $P^{-1}AP = D$ (diagonale) alors ${}^tP\,{}^tA\,{}^tP^{-1} = D$ donc ${}^tP^{-1}$ diagonalise ${}^tA$. En conséquence, les lignes de P^{-1} sont vecteurs propres de ${}^tA$. Donc, si le choix proposé est possible, nécessairement les lignes de P sont les vecteurs propres de ${}^tA$. **(1)**
- Les valeurs propres de ${}^tA$ sont celles de A (car $\chi_{{}^tA} = \chi_A$). Sous-espaces propres de ${}^tA$:

$$\lambda = 1 \qquad \mathrm{Ker}({}^tA-I)\begin{cases} -x+3y=0 \\ x-y+2z=0 \\ 3z-t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 3 \\ 1 \\ -1 \\ -3 \end{pmatrix}$$

$$\lambda = -1 \qquad \mathrm{Ker}({}^tA+I)\begin{cases} x+3y=0 \\ x+y+2z=0 \\ 3z+t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 3 \\ -1 \\ -1 \\ 3 \end{pmatrix}$$

$$\lambda = 3 \qquad \mathrm{Ker}({}^tA-3I)\begin{cases} -3x+3y=0 \\ x-3y+2z=0 \\ 3z-3t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\lambda = -3 \qquad \mathrm{Ker}({}^tA+3I)\begin{cases} 3x+3y=0 \\ x+3y+2z=0 \\ 3z+3t=0 \end{cases} \qquad \text{vecteur directeur} \quad \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

Pour que la condition **(1)** soit réalisée, nous pouvons prendre : $P_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 1 & -1 & -3 \\ 3 & -1 & -1 & 3 \\ 1 & -1 & 1 & -1 \end{pmatrix}$.

On a alors $P_1^2 = 8I$, donc avec $P = \dfrac{1}{2\sqrt{2}}P_1$, il vient $P^2 = I$, c'est-à-dire :

$$P^{-1} = P \text{ et } P^{-1}AP = PAP = \mathrm{diag}(3,1,-1,-3).$$

Ex. 4

Qu'un endomorphisme soit ou ne soit pas diagonalisable, les droites stables sont toujours les droites dirigées par des vecteurs propres. Le calcul du polynôme caractéristique donne : $\chi_A(X) = (2-X)\big((1-X)^2+1\big)$.

u admet une seule valeur propre : 2 ; celle-ci est simple, on a donc une seule droite stable par u, c'est la droite vectorielle $E_u(2)$ engendrée par $(1,1,1)$.

u n'est pas diagonalisable. Pour les plans stables, on peut utiliser l'exercice 11 *Mise en œuvre* : le plan H d'équation $\alpha_1x_1+\alpha_2x_2+\alpha_3x_3 = 0$ est stable par u si et seulement si $(\alpha_1,\alpha_2,\alpha_3) \neq (0,0,0)$ est vecteur propre de ${}^tA$.

$\chi_{{}^tA} = \chi_A$: ${}^tA$ a une seule valeur propre : 2, le sous-espace propre associé est $\mathrm{Vect}(y)$ avec $y = (0,1,1)$, d'où l'unique plan stable H d'équation $x_2+x_3 = 0$.

Copyrighted material

Ex. 5

- **Première solution**

Le polynôme caractéristique de M est $\chi_M(X) = -(X+1)(X-1)^2$.

L'équation $MU = U$ a pour solutions indépendantes $U_1 = (1,0,0)$ et $U_2 = (0,1,-2)$.

M est alors diagonalisable et semblable à la matrice diagonale $D = \text{diag}(-1,1,1)$ (sans avoir à résoudre $MU = -U$).

Avec $D^{2n} = I_3$ et $D^{2n+1} = D$, il vient $M^{2n} = I_3$ et $M^{2n+1} = M$.

- **Deuxième solution**

On a $M^2 = I_3$ donc $X^2 - 1$ est polynôme annulateur de M. Alors $M^3 = M$. Il vient aisément $M^{2n} = I_3$ et $M^{2n+1} = M$.

Niveau 2

Ex. 6

Soit $\lambda \in \mathbb{R}$ une valeur propre de A et $X = \left[x_i\right] \in \mathcal{M}_{n,1}(\mathbb{R})$ un vecteur propre associé. Il existe alors une suite $\left(x_k\right)_{k\in\mathbb{N}}$ telle que $x_0 = x_{n+1} = 0$ et $\forall k \in \mathbb{N}^*,\ x_{k-1} + (2-\lambda)x_k + x_{k+1} = 0$.

L'équation caractéristique associée à cette suite récurrente est $x^2 + (2-\lambda)x + 1 = 0$.

Notons u et v ses racines complexes : $u + v = \lambda - 2$, $u \cdot v = 1$.

Dans le cas où elles sont distinctes, il existe $(\alpha,\beta) \in \mathbb{C}^2 \setminus \{(0,0)\}$ tel que $\forall k \in \mathbb{N},\ x_k = \alpha u^k + \beta v^k$.

$x_0 = 0$ et $x_{n+1} = 0$ donnent $\alpha + \beta = 0$, $\alpha u^{n+1} + \beta v^{n+1} = 0$ d'où $u^{n+1} = v^{n+1}$ puis $u^{2(n+1)} = 1$.

On en déduit $u = e^{\frac{p i\pi}{n+1}}$, $p \in [\![0, n]\!]$, donc $v = e^{\frac{-p i\pi}{n+1}}$ et, avec $\alpha = -\beta = \frac{x_1}{2i}$, il vient :

$$x_k = x_1 \sin\frac{kp\pi}{n+1},\quad \lambda = 2 + 2\cos\frac{p\pi}{n+1} = 4\cos^2\frac{p\pi}{2(n+1)}.$$

On vérifie alors que, pour tout $p \in [\![1, n]\!]$, le vecteur $X_p = \left[\sin\frac{kp\pi}{n+1}\right]_{1\leqslant k\leqslant n}$ est vecteur propre de A (il est non nul) associé à la valeur propre $\lambda_p = 4\cos^2\frac{p\pi}{2(n+1)}$ (utiliser $\sin(k-1)\theta + \sin(k+1)\theta = 2\cos\theta\sin k\theta$).

Admettant n valeurs propres distinctes $\left(\lambda_p \in]0,4[\right)$, A est diagonalisable et on peut écrire :

$$P^{-1} \cdot AP = \text{diag}\left[4\cos^2\frac{\pi}{2n+2}, \ldots, 4\cos^2\frac{j\pi}{2n+2}, \ldots, 4\cos^2\frac{n\pi}{2n+2}\right] \text{ avec } P = \left[\sin\frac{ij\pi}{n+1}\right].$$

Ex. 7

On suppose que $n \geqslant 2$. Il est utile ici de considérer la relation : $A \cdot B = B \cdot A = (\det A) I_n$.

Soit $X \in \mathcal{M}_{n,1}(\mathbb{C})$ un vecteur propre de A associé à la valeur propre λ : $AX = \lambda X$, $X \neq 0$.

- Si $\lambda \neq 0$, $BAX = (\det A)X$ donne $BX = \dfrac{\det A}{\lambda} X$: X est vecteur propre de B associé à la valeur propre $\dfrac{\det A}{\lambda}$.
- Si $\lambda = 0$, alors $\det A = 0$ (car 0 est valeur propre de A) donc $AB = BA = 0$:
  - pour $\text{rg}\, A \leqslant n-2$, on a $B = 0$ et X est vecteur propre de B,
  - pour $\text{rg}\, A = n-1$, de $AB = BA = 0$ on déduit $\text{rg}\, B = 1$ et $\text{Ker}\, A = \text{Im}\, B$ (droite vectorielle). Dans ce cas, on a $X \in \text{Ker}\, A$ donc $X \in \text{Im}\, B$ et puisque $BX \in \text{Im}\, B$, il existe $\mu \in K$ tel que $BX = \mu X$: X est vecteur propre de B.

Remarque

1) De cette étude, il résulte que si A est diagonalisable, B l'est aussi.

2) On peut aussi en déduire le polynôme caractéristique de B (ou de $\text{com}\, A$).

- Si $\text{rg}\, A = n$, alors $B = (\det A)A^{-1}$ et, avec :

$$\chi_A(X) = \prod_{i=1}^{n} (\lambda_i - X),$$

Copyrighted material

il vient :

$$\chi_B(X) = \prod_{i=1}^{n} \left(\frac{\det A}{\lambda_i} - X \right).$$

- Si $\operatorname{rg} A = n-1$:

$$\chi_B(X) = (-X)^{n-1}(\operatorname{Tr} B - X)$$

où $\operatorname{Tr} B$ est la somme des cofacteurs des éléments diagonaux de A.

- Si $\operatorname{rg} A \leqslant n-2$, $\chi_B(X) = (-X)^n$, $(B = 0)$.

Ex. 8

Il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que $P^{-1}AP = D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$.

De même, il existe $Q \in \mathrm{GL}_2(\mathbb{R})$ telle que $Q^{-1}BQ = \operatorname{diag}(\mu_1, \mu_2)$

$$Q = \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix}, \quad Q^{-1} = \begin{pmatrix} q'_1 & q'_2 \\ q'_3 & q'_4 \end{pmatrix}, \quad Q^{-1}BQ = \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix}.$$

On en déduit :

$$\begin{pmatrix} q'_1 I_n & q'_2 I_n \\ q'_3 I_n & q'_4 I_n \end{pmatrix} \begin{pmatrix} b_1 A & b_2 A \\ b_3 A & b_4 A \end{pmatrix} \begin{pmatrix} q_1 I_n & q_2 I_n \\ q_3 I_n & q_4 I_n \end{pmatrix} = \begin{pmatrix} \mu_1 A & 0 \\ 0 & \mu_2 A \end{pmatrix}$$

avec :

$$\begin{pmatrix} q'_1 I_n & q'_2 I_n \\ q'_3 I_n & q'_4 I_n \end{pmatrix} \begin{pmatrix} q_1 I_n & q_2 I_n \\ q_3 I_n & q_4 I_n \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix} = I_{2n}.$$

Donc C est semblable à $C' = \begin{pmatrix} \mu_1 A & 0 \\ 0 & \mu_2 A \end{pmatrix}$.

On a d'autre part :

$$\begin{pmatrix} P^{-1} & 0 \\ 0 & P^{-1} \end{pmatrix} \begin{pmatrix} \mu_1 A & 0 \\ 0 & \mu_2 A \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & p \end{pmatrix} = \begin{pmatrix} \mu_1 D & 0 \\ 0 & \mu_2 D \end{pmatrix}$$

avec :

$$\begin{pmatrix} P^{-1} & 0 \\ 0 & P^{-1} \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix} = I_{2n}.$$

Donc C' est semblable à $\Delta = \begin{pmatrix} \mu_1 D & 0 \\ 0 & \mu_2 D \end{pmatrix}$ qui est diagonale.

Finalement C est diagonalisable :

$$R^{-1}CR = \begin{pmatrix} \mu_1 D & 0 \\ 0 & \mu_2 D \end{pmatrix} \text{ avec } R = \begin{pmatrix} q_1 I_n & q_2 I_n \\ q_3 I_n & q_4 I_n \end{pmatrix} \begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix} = \begin{pmatrix} q_1 P & q_2 P \\ q_3 P & q_4 P \end{pmatrix} \in \mathrm{GL}_{2n}(\mathbb{R}).$$

Ex. 9

1) A ayant n valeurs propres distinctes, il existe $P \in \mathrm{GL}_n(\mathbb{K})$ telle que :

$$P^{-1}AP = D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$$

Posons $P^{-1}BP = C$ d'où $C^2 = P^{-1}B^2P = P^{-1}AP = D$. Montrons alors que C est diagonale.

On constate que C et $D = C^2$ commutent : $CD = DC$. L'égalité des termes (i,j) donne $\lambda_j C_{ij} = \lambda_i C_{ij}$, or pour $i \neq j$, $\lambda_i \neq \lambda_j$ donc $C_{ij} = 0$.

2) Le calcul donne $\chi_A(X) = -X(1-X)(16-X)$. Avec $\lambda_1 = 0, \lambda_2 = 1, \lambda_3 = 16$ et les notations du 1), on a :

$$P = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \quad D = \operatorname{diag}(0, 1, 16).$$

Les matrices diagonales C vérifiant $C^2 = D$ sont $\operatorname{diag}(0, \varepsilon_1, 4\varepsilon_2)$ où $\varepsilon_i \in \{-1, 1\}$.

Les matrices cherchées sont alors $B = PCP^{-1}$. Le calcul donne :

$$P^{-1} = \frac{1}{6} \begin{pmatrix} 0 & 3 & 3 \\ 2 & 2 & -2 \\ 2 & -1 & 1 \end{pmatrix} \text{ et } B \in \left\{ \pm \begin{pmatrix} 3 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \pm \frac{1}{3} \begin{pmatrix} -7 & 5 & -5 \\ 5 & -1 & 1 \\ -5 & 1 & -1 \end{pmatrix} \right\}.$$

Copyrighted material

Hidden page

La condition **(3)** donne $\alpha = 1$ ou -1 c'est-à-dire $\alpha = \varepsilon_1$ ou $\alpha = -\varepsilon_1$. Or d'après **(4)**, $\alpha + \varepsilon_1 \neq 0$, le système **(3) (4) (5)** est donc équivalent à :

$$\alpha = \varepsilon_1 \quad , \quad \beta = \frac{\varepsilon_1}{2} \quad , \quad \gamma = \frac{1}{\varepsilon_1 + 2\varepsilon_2} .$$

- Conclusion

L'équation **(1)** a quatre solutions : $X = \varepsilon \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ \frac{1}{3} & 0 & 2 \end{pmatrix}$, $X = \varepsilon \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ -1 & 0 & -2 \end{pmatrix}$, $\varepsilon \in \{-1, 1\}$.

Ex. 12

Le polynôme $X^3 - X = X(X-1)(X+1)$ est scindé dans $\mathbb{R}$, à racines simples, et annulateur de u. Donc u est diagonalisable et, en posant $E_0 = \operatorname{Ker} u$, $E_1 = \operatorname{Ker}\left(u - \mathrm{Id}_E\right)$, $E_{-1} = \operatorname{Ker}\left(u + \mathrm{Id}_E\right)$, on a $E = E_0 \oplus E_1 \oplus E_{-1}$.

Soit F un sous-espace de E stable par u. Alors u induit un endomorphisme u_F de F dont $X^3 - X$ est polynôme annulateur ce qui montre que u_F est diagonalisable, donc que F est somme directe des sous-espaces propres de u_F.

Tout vecteur propre de u_F étant un vecteur propre de u, on en déduit :

$$F = F_0 \oplus F_1 \oplus F_{-1} \text{ avec } \begin{cases} F_0 = \operatorname{Ker} u_F = F \cap E_0 \\ F_1 = \operatorname{Ker}\left(u_F - \mathrm{Id}_F\right) = F \cap E_1 \\ F_{-1} = \operatorname{Ker}\left(u_F + \mathrm{Id}_F\right) = F \cap E_{-1} \end{cases}$$

Finalement, si F est stable par u, il existe F_0 sous-espace de E_0, F_1 sous-espace de E_1 et F_{-1} sous-espace de E_{-1} tels que $F = F_0 \oplus F_1 \oplus F_{-1}$.

La réciproque est évidente, l'ensemble des sous-espaces stables par u est donc constitué des sous-espaces de la forme $F_0 \oplus F_1 \oplus F_{-1}$ où F_0, F_1, F_{-1} sont des sous-espaces de E_0, E_1, E_{-1} respectivement. Ce sont aussi les sous-espaces de E admettant une base formée de vecteurs propres de u.

Ex. 13

Il existe $Q \in \mathbb{R}[X]$ tel que $P = XQ$ et $Q(0) \neq 0$. On a alors $X \wedge Q = 1$ donc, puisque $P = XQ$ est annulateur de f, le théorème de décomposition des noyaux donne $E = \operatorname{Ker} f \oplus Ker Q(f)$.

- En dimension finie

$\dim E = n$. $E = \operatorname{Ker} f \oplus \operatorname{Ker} Q(f)$ donne $\dim \operatorname{Ker} Q(f) = \operatorname{rg} f$. Or $0 = P(f) = Q(f) \circ f$ donne $\operatorname{Im} f \subset \operatorname{Ker} Q(f)$, d'où $\operatorname{Im} f = \operatorname{Ker} Q(f)$ avec l'égalité des dimensions. Finalement, $E = \operatorname{Im} f \oplus \operatorname{Ker} f$.

- Hors dimension

On a encore $\operatorname{Im} f \subset \operatorname{Ker} Q(f)$. Posons $a = Q(0) \neq 0$. Alors $Q(X) = a + XQ_1(X)$ donc $Q(f) = a\,\mathrm{Id}_E + f \circ Q_1(f)$.

Pour $x \in \operatorname{Ker} Q(f)$, on a alors $0 = ax + f\left(Q_1(f)(x)\right)$, d'où $x \in \operatorname{Im} f$. Il s'ensuit $\operatorname{Ker} Q(f) = \operatorname{Im} f$ et la conclusion.

Ex. 14

1) A est une matrice de permutation. On obtient aisément $A^n = I_n$ donc $X^n - 1$ est annulateur de A et, puisqu'il s'agit d'un polynôme scindé à racines simples dans $\mathbb{C}$, A est diagonalisable (théorème 12).

Pour préciser les valeurs propres, formons χ_A :

$$\chi_A = \begin{vmatrix} -X & & & 1 \\ 1 & \ddots & & \\ (0) & \ddots & \ddots & \\ & & 1 & -X \end{vmatrix}$$

En développant suivant la première ligne, il vient :

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

Ainsi A possède n valeurs propres simples : ce sont les n racines $n^{\text{èmes}}$ de l'unité c'est-à-dire ω^k, $0 \leqslant k \leqslant n-1$, où on a posé $\omega = e^{\frac{2i\pi}{n}}$.

Copyrighted material

Hidden page

Pour tout $i \in [\![1, p]\!]$, le sous-espace $E_f(\lambda_i)$ est stable par g. Notons g_i l'endomorphisme induit par la restriction de g à $E_f(\lambda_i)$; g étant diagonalisable, g_i l'est aussi (théorème 14).

Il existe donc une base $\mathcal{B}_i$ de $E_f(\lambda_i)$ formée de vecteurs propres de g_i (donc de g et f). Le système de vecteurs formé de la «réunion» $\mathcal{B}_1, \dots, \mathcal{B}_p$ est une base $\mathcal{B}$ de E formée de vecteurs propres communs à f et g. Les matrices $\mathrm{mat}_{\mathcal{B}} f$ et $\mathrm{mat}_{\mathcal{B}} g$ sont donc diagonales.

Ex. 16

1) Vérifications immédiates.

2) Si $v \in \mathcal{L}(E)$ commute avec u, on a $\forall i \in [\![1, p]\!], v(E_u(\lambda_i)) \subset E_u(\lambda_i)$.

La réciproque est évidente. Il en résulte que $v \in \mathcal{C}(u)$ si et seulement si $\mathrm{mat}_{\mathcal{B}} v$ a la forme annoncée. $\mathcal{C}(u)$ est donc isomorphe à l'ensemble des matrices de cette forme et :

$$\dim \mathcal{C}(u) = \sum_{i=1}^{p} m_i^2. \text{ Noter que } n \leqslant \dim \mathcal{C}(u) \leqslant n^2.$$

3) $\chi_A(X) = \det(A - XI_3) = -X(X^2 + 4X + 2)$.

A est diagonalisable puisqu'elle a trois valeurs propres réelles distinctes :

$$\lambda_1 = 0, \quad \lambda_2 = -2 - \sqrt{2}, \quad \lambda_3 = -2 + \sqrt{2}.$$

$\mathcal{B} = (e_1, e_2, e_3)$ étant la base canonique de $\mathbb{R}^3$, une base formée de vecteurs propres de u est $\mathcal{B}' = (e'_1, e'_2, e'_3)$ avec :

$$\begin{array}{lll} e'_1 = 2e_1 + e_3 & \text{associé à} & \lambda_1 = 0 \\ e'_2 = (2\sqrt{2}+1)e_1 - (\sqrt{2}+1)e_2 + (2\sqrt{2}+2)e_3 & \text{associé à} & \lambda_2 = -2 - \sqrt{2} \\ e'_3 = (-2\sqrt{2}+1)e_1 + (\sqrt{2}-1)e_2 - (2\sqrt{2}-2)e_3 & \text{associé à} & \lambda_3 = -2 + \sqrt{2} \end{array}$$

Alors $\mathrm{mat}_{\mathcal{B}} u = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2-\sqrt{2} & 0 \\ 0 & 0 & -2+\sqrt{2} \end{pmatrix} = P^{-1}AP = D$ avec $P = \begin{pmatrix} 2 & 2\sqrt{2}+1 & -2\sqrt{2}+1 \\ 0 & -\sqrt{2}-1 & \sqrt{2}-1 \\ 1 & 2\sqrt{2}+2 & -2\sqrt{2}+2 \end{pmatrix}$.

D'après le 2), $v \in \mathcal{L}(E)$ est élément de $\mathcal{C}(u)$ si et seulement si :

$$\mathrm{mat}_{\mathcal{B}'} v = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \quad (\alpha, \beta, \gamma) \in \mathbb{R}^3$$

On a ici $\dim \mathcal{C}(u) = 3$.

Il est facile de voir directement que (Id_E, u, u^2) est libre et donc que $\dim \mathbb{R}[u] \geqslant 3$.

En effet, $\lambda \mathrm{Id}_E + \mu u + \nu u^2 = 0$ avec $(\lambda, \mu, \nu) \in \mathbb{R}^3$ donne $\lambda I_3 + \mu D + \nu D^2 = 0$, c'est-à-dire :

$$\begin{cases} \lambda = 0 \\ \lambda - \mu(2+\sqrt{2}) + \nu(2+\sqrt{2})^2 = 0 \\ \lambda - \mu(2-\sqrt{2}) + \nu(2-\sqrt{2})^2 = 0 \end{cases} \quad \text{d'où } \lambda = \mu = \nu = 0.$$

L'inclusion $\mathbb{R}[u] \subset \mathcal{C}(u)$ donne alors, en tenant compte des dimensions, $\mathbb{R}[u] = \mathcal{C}(u)$.

4) D'après le théorème de Cayley-Hamilton, on a $u^n \in \mathrm{Vect}(\mathrm{Id}_E, u, \dots, u^{n-1})$ donc $\dim \mathbb{K}[u] \leqslant n$.

D'autre part $\dim \mathcal{C}(u) = \sum_{i=1}^{p} m_i^2 \geqslant \sum_{i=1}^{p} m_i = n$ ($\forall i \in [\![1, p]\!], m_i^2 \geqslant m_i \geqslant 1$)

et $\dim \mathcal{C}(u) = \sum_{i=1}^{p} m_i^2 > \sum_{i=1}^{p} m_i = n$ si l'un des m_i est strictement supérieur à 1 ; il en résulte que :

$$\mathbb{K}[u] = \mathcal{C}(u) \Rightarrow \forall i \in [\![1, p]\!], m_i = 1.$$

Réciproquement, en supposant $\forall i \in [\![1, p]\!], m_i = 1$ (ce qui exige $p = n$), on peut établir comme en 3) que $(\mathrm{Id}_E, u, \dots, u^{n-1})$ est libre, et en déduire $\mathbb{R}[u] = \mathcal{C}(u)$.

Copyrighted material

Ex. 17

Notons $E = \mathbb{R}^3$ et (e_1, e_2, e_3) la base canonique de $\mathbb{R}^3$.

Soit $f \in \mathscr{L}(E)$ tel que $A = \mathrm{mat}_{(e_i)} f$ et, pour tout $M \in \mathscr{M}_3(\mathbb{R})$, soit $g \in \mathscr{L}(E)$ tel que $M = \mathrm{mat}_{(e_i)} g$.

L'équation matricielle $M^2 = A$ est équivalente à $g^2 = f$.

- Commençons par réduire A.

On obtient $\chi_A = \det(A - XI_3) = (1-X)(4-X)^2$.

$\mathrm{Ker}(f - 4\,\mathrm{Id}_E)$ est le plan d'équation $x_1 + x_2 + x_3 = 0$ de base (u_1, u_2) avec :

$$u_1 = (-1, 1, 0) = -e_1 + e_2 \quad , \quad u_2 = (-1, 0, 1) = -e_1 + e_3 .$$

À ce niveau du calcul, on sait que f (et donc A) est diagonalisable.

$\mathrm{Ker}(f - \mathrm{Id}_E)$ est la droite d'équations $x_2 + x_3 = 0$. $x_1 + x_3 = 0$, d'où :

$$\mathrm{Ker}(f - \mathrm{Id}_E) = \mathbb{R}u_3 \text{ avec } u_3 = (-1, -1, 1) = -e_1 - e_2 + e_3.$$

En posant $P = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}$, on a donc :

$$P^{-1}AP = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ ou en écrivant par blocs } P^{-1}AP = \begin{pmatrix} 4I_2 & 0 \\ 0 & 1 \end{pmatrix}.$$

- Application à l'équation

Le changement d'inconnue défini par $N = P^{-1}MP$ transforme l'équation **(1)** proposée en :

$$N^2 = \begin{pmatrix} 4I_2 & 0 \\ 0 & 1 \end{pmatrix} \qquad \textbf{(2)}$$

On a maintenant $N = \mathrm{mat}_{(u_i)} g$. On observe que si g est solution du problème $f \circ g = g \circ f = f^3$, les sous-espaces propres de f sont donc stables par g et N est de la forme $\begin{pmatrix} N' & 0 \\ 0 & \lambda \end{pmatrix}$, $N' \in \mathscr{M}_2(\mathbb{R})$. Ainsi l'équation **(2)** équivaut à :

$$N'^2 = 4I_2, \quad \lambda^2 = 1.$$

La condition $N'^2 = 4I_2$ caractérise que $\frac{1}{2}N'$ est une matrice de symétrie donc $N' = 2I_2$ ou $N' = -2I_2$ ou N' est semblable à $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$.

Finalement, les solutions de **(1)** sont les matrices :

$$P\begin{pmatrix} 2I_2 & 0 \\ 0 & \pm 1 \end{pmatrix}P^{-1} \quad , \quad P\begin{pmatrix} -2I_2 & 0 \\ 0 & \pm 1 \end{pmatrix}P^{-1} \quad , \quad P\begin{pmatrix} 2Q^{-1}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}Q & 0 \\ 0 & \pm 1 \end{pmatrix}P^{-1}$$

où Q est quelconque dans $\mathrm{GL}_2(\mathbb{R})$.

En termes d'endomorphismes, les solutions de $g^2 = f$ sont les endomorphismes g de E tels que :

- $F_1 = \mathrm{Vect}(u_1, u_2)$ est stable par g et l'endomorphismes $g_{F_1} \in \mathscr{L}(F_1)$ induit par g est tel qu'il existe s symétrie de F_1 avec $g = 2s$,
- $F_2 = \mathrm{Vect}(u_3)$ est stable par g et $g_{F_2} \in \mathscr{L}(F_2)$ induit par g est tel que $g = \pm\,\mathrm{Id}_{F_2}$.

Ex. 18

1) Une droite $D = \mathbb{R}u$ est stable par f si et seulement si u est vecteur propre de f.

Le calcul donne $\chi_A = \det(A - XI_3) = -X(X+2)^2$;

$\mathrm{Ker}\, f = \mathbb{R}u_1$ avec $u_1 = (3, 1, 5) = 3e_1 + e_2 + 5e_3$;

$\mathrm{Ker}(f + 2\,\mathrm{Id}_E) = \mathbb{R}u_2$ avec $u_2 = (1, -1, 1) = e_1 - e_2 + e_3$.

On remarque que f n'est pas diagonalisable. Il existe exactement deux droites de E stables par f, ce sont $\mathbb{R}u_1$ et $\mathbb{R}u_2$.

2) Si P plan de E est stable par f, il existe $g \in \mathscr{L}(P)$ induit par f.

On sait alors que le polynôme caractéristique de g, χ_g divise $\chi_f = X(X+2)^2$ (propriété 22).

Copyrighted material

D'autre part, $\deg \chi_g = \dim P = 2$, il y a donc deux possibilités :

a) $\chi_g = X(X+2)$;

b) $\chi_g = (X+2)^2$.

Dans chaque cas le théorème de Cayley-Hamilton donne $\chi_g(g) = 0$ donc :

cas a) : $\forall x \in P,\ f \circ (f + 2\,\mathrm{Id}_E)(x) = 0$

cas b) : $\forall x \in P,\ (f + 2\,\mathrm{Id}_E)^2(x) = 0$

c'est-à-dire $P \subset \mathrm{Ker}\left(f \circ (f + 2\,\mathrm{Id}_E)\right)$ dans le cas a)

ou $P \subset \mathrm{Ker}\left((f + 2\,\mathrm{Id}_E)^2\right)$ dans le cas b)

D'après le théorème de décomposition des noyaux, on a :

$$\mathrm{Ker}\left(f \circ (f + 2\,\mathrm{Id}_E)\right) = \mathrm{Ker}\, f \oplus \mathrm{Ker}\,(f + 2\,\mathrm{Id}_E)$$

donc compte-tenu des dimensions, dans le cas a) :

$$P = \mathrm{Ker}\, f \oplus \mathrm{Ker}\,(f + 2\,\mathrm{Id}_E).$$

Le théorème de Cayley-Hamilton donne aussi :

$$E = \mathrm{Ker}\left(f \circ (f + 2\,\mathrm{Id}_E)^2\right)$$

donc avec le théorème de décomposition des noyaux :

$$E = \mathrm{Ker}\, f \oplus \mathrm{Ker}\left((f + 2\,\mathrm{Id}_E)^2\right)$$

et on en déduit $\dim \mathrm{Ker}\left((f + 2\,\mathrm{Id}_E)^2\right) = 2$ et dans le cas b) $P = \mathrm{Ker}\left((f + 2\,\mathrm{Id}_E)^2\right)$.

Les deux plans précédents $P_1 = \mathrm{Ker}\left(f \circ (f + 2\,\mathrm{Id}_E)\right)$ et $P_2 = \mathrm{Ker}\left((f + 2\,\mathrm{Id}_E)^2\right)$ sont les seules possibilités de plans stables par f.

D'autre part, puisque les polynômes en f : $f \circ (f + 2\,\mathrm{Id}_E)$ et $(f + 2\,\mathrm{Id}_E)^2$ sont permutables avec f, ces deux plans sont effectivement stables par f. Ainsi, il y a exactement deux plans de E : P_1 et P_2 stables par f.

Pour conclure, notons que $P_1 = \mathrm{Vect}\,(u_1, u_2)$ (on peut remarquer que f_{P_1} est diagonalisable) et le calcul de $(A + 2I)^2 = \begin{pmatrix} 12 & 6 & -6 \\ 4 & 2 & -2 \\ 20 & 10 & -10 \end{pmatrix}$ montre que P_2 a pour équation $2x_1 + x_2 - x_3 = 0$ donc que :

$$P_2 = \mathrm{Vect}\,(u_2, u_3) \text{ avec } u_3 = (0, 1, 1) = e_2 + e_3.$$

Copyrighted material

CHAPITRE 6

Espaces préhilbertiens

Copyrighted material

A. Formes bilinéaires symétriques Formes quadratiques

Dans cette section, E désigne un $\mathbb{R}$-espace vectoriel et E^* son espace dual.

1. Formes bilinéaires [1]

[1] La notion d'application p-linéaire a été introduite en Algèbre et Géométrie, MPSI, chapitre 14 et revue dans le chapitre 3 de cet ouvrage.

1.1 – Généralités

Définition 1

On appelle **transposée d'une forme bilinéaire** φ sur E, la forme bilinéaire sur E, notée ${}^t\varphi$, définie par :

$$\forall (x, y) \in E^2, \quad {}^t\varphi(x, y) = \varphi(y, x).$$

Propriété 1

Une forme bilinéaire φ sur E est :

- symétrique si et seulement si ${}^t\varphi = \varphi$,
- antisymétrique si et seulement si ${}^t\varphi = -\varphi$.

Propriété 2

Les espaces vectoriels $\mathscr{L}_2(E)$, $\mathscr{S}_2(E)$, $\mathscr{A}_2(E)$.

a) L'ensemble $\mathscr{L}_2(E)$ des formes bilinéaires sur E est un sous-espace de $\mathscr{F}(E^2, \mathbb{R})$ [2]

b) L'application de $\mathscr{L}_2(E)$ dans lui-même, $\varphi \mapsto {}^t\varphi$ est un automorphisme involutif.

c) Les ensembles $\mathscr{S}_2(E)$ [3] et $\mathscr{A}_2(E)$ [4] sont des sous-espaces supplémentaires de $\mathscr{L}_2(E)$. La décomposition de tout $\varphi \in \mathscr{L}_2(E)$ est donnée par :

$$\sigma = \frac{1}{2}\left(\varphi + {}^t\varphi\right) \in \mathscr{S}(E), \alpha = \frac{1}{2}\left(\varphi - {}^t\varphi\right) \in \mathscr{A}_2(E), \varphi = \sigma + \alpha$$

σ et α sont appelées partie symétrique et partie antisymétrique de φ.

[2] À ne pas confondre avec $\mathscr{L}(E^2, \mathbb{R})$.

[3] Formes bilinéaires symétriques.

[4] Formes bilinéaires antisymétriques.

Propriété 3

Restriction d'une forme bilinéaire à un sous-espace vectoriel

Soit F un sous-espace de E et $\varphi \in \mathscr{L}_2(E)$.

La restriction de φ à F^2 est une forme bilinéaire sur F ; elle est symétrique lorsque φ est symétrique, antisymétrique lorsque φ est antisymétrique.

Exemple 1 Avec $E = \mathcal{C}([a, b], \mathbb{R})$, $\varphi : E^2 \to \mathbb{R}, (f, g) \mapsto \displaystyle\int_a^b f(t)g(t)\mathrm{d}t$.

φ est une forme bilinéaire symétrique sur E.

Exemple 2 Avec $E = \mathcal{M}_n(\mathbb{R})$, $\varphi : E^2 \to \mathbb{R}, (A, B) \mapsto \mathrm{Tr}(AB)$.

φ est une forme bilinéaire symétrique sur E.

Exemple 3 Soit $\varphi \in \mathscr{L}_2(E)$, f et g deux endomorphismes de E.

L'application $E^2 \to \mathbb{R}, (x, y) \mapsto \varphi\big(f(x), g(x)\big)$ est une forme bilinéaire sur E.

Par exemple, $(x, y) \mapsto \varphi(x + y, x - y)$ est une forme bilinéaire antisymétrique.

Exemple 4 Soit θ_1 et θ_2 deux formes linéaires sur E. L'application $\varphi : E^2 \to \mathbb{R}, (x, y) \mapsto \theta_1(x) \cdot \theta_2(y)$ est une forme bilinéaire.

Avec les notations de la propriété 2 c), on a :

$$\sigma(x, y) = \frac{1}{2}\left[\theta_1(x)\ \theta_2(y) + \theta_2(x)\ \theta_1(y)\right] \qquad \alpha(x, y) = \frac{1}{2}\left[\theta_1(x)\ \theta_2(y) - \theta_2(x)\ \theta_1(y)\right].$$

Copyrighted material

Hidden page

Propriété 8

Deux matrices M et M' de $\mathcal{M}_n(\mathbb{R})$ sont congruentes si et seulement si étant donné $\varphi \in \mathcal{L}_2(\mathbb{R}^n)$ définie par $M = \mathrm{mat}_{\mathcal{B}} \varphi$ où $\mathcal{B}$ est une base quelconque de $\mathbb{R}^n$, il existe une base $\mathcal{B}'$ de $\mathbb{R}^n$ telle que : $M' = \mathrm{mat}_{\mathcal{B}'} \varphi$.

Propriété 9

Deux matrices congruentes ont le même rang.

Exemple 5 On dispose sur $\mathcal{M}_n(\mathbb{R})$ de trois relations d'équivalence distinctes avec les notions de matrices équivalentes, semblables et congruentes.

Voici dans $\mathcal{M}_2(\mathbb{R})$ des exemples qui distinguent ces relations.

a) Montrer que $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ sont équivalentes, non semblables, non congruentes.

b) Montrer que $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$ sont semblables, non congruentes.

c) Montrer que $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ sont non semblables, congruentes.

On sait que deux matrices sont équivalentes si et seulement si elles ont même rang (voir chapitre 4 de ce tome). D'autre part, si deux matrices sont semblables, elles ont même polynôme caractéristique. ✎(6)

✎(6) Voir le chapitre 5.

Remarquons enfin que, si deux matrices sont congruentes, l'une est symétrique (resp. antisymétrique) si et seulement si l'autre est symétrique (resp. antisymétrique).

a) $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

On a ici $\mathrm{rg}\, A = \mathrm{rg}\, B$ donc A et B sont équivalentes. Les polynômes caractéristiques sont $\chi_A = X(X-1)$ et $\chi_B = X^2$, A et B ne sont donc pas semblables.

A est symétrique et B ne l'est pas, A et B ne sont donc pas congruentes.

b) $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$

Les polynômes caractéristiques $\chi_A = X^2 - 1$ et $\chi_B = X^2 - 1$ sont scindés et n'admettent que des racines simples : A et B sont toutes deux semblables à $D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et, par transitivité, elles sont semblables.

A est symétrique et B ne l'est pas, A et B ne sont donc pas congruentes.

c) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Les polynômes caractéristiques sont $\chi_A = X^2 - 2X$ et $\chi_B = X(X-1)$, A et B ne sont donc pas semblables.

Soit φ la forme bilinéaire de $\mathbb{R}^2$ canoniquement associée à A, et $\mathcal{B} = (e_1, e_2)$ la base canonique de $\mathbb{R}^2$. Pour $x = x_1 e_1 + x_2 e_2$, $y = y_1 e_1 + y_2 e_2$ on a :

$$\varphi(x, y) = x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2 \text{ donc } \varphi(x, y) = (x_1 + x_2)(y_1 + y_2).$$

Considérons alors le changement de base défini par :

$$\begin{cases} x'_1 = x_1 + x_2 \\ x'_2 = x_2 \end{cases} \text{ c'est-à-dire aussi } \begin{cases} x_1 = x'_1 - x'_2 \\ x_2 = x'_2 \end{cases}$$

Dans la nouvelle base $\mathcal{B}'$ on a $\varphi(x, y) = x'_1 y'_1$ et $\mathrm{mat}_{\mathcal{B}'} \varphi = B$ donc A et B sont congruentes.

La matrice de changement de base est $P = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, donc la base $\mathcal{B}'$ est :

$$(e'_1, e'_2) \text{ avec } e'_1 = e_1,\ e'_2 = -e_1 + e_2.$$

Copyrighted material

2. Formes quadratiques

2.1 – Généralités

Théorème 1

L'application $\mathcal{Q} : \mathcal{L}_2(\mathbb{R}) \to \mathcal{F}(E, \mathbb{R}), \varphi \mapsto q$, où q est telle que $q(x) = \varphi(x, x)$, est linéaire. Son noyau est $\mathcal{A}l_2(E)$. Elle induit un isomorphisme de $\mathcal{S}_2(E)$ sur son image notée $\mathcal{Q}(E)$.

☞ La linéarité de $\mathcal{Q}$ est évidente. Pour tout $\varphi \in \mathcal{L}_2(E)$ avec $q = \mathcal{Q}(\varphi)$, on a :

$$\forall (x, y) \in E^2, q(x + y) = q(x) + q(y) + \varphi(x, y) + \varphi(y, x).$$

Si $q = 0$, il vient $\varphi(y, x) = -\varphi(x, y)$, donc $\varphi \in \mathcal{A}l_2(E)$ et la réciproque est immédiate. On conclut en rappelant que $\mathcal{S}_2(E)$ est un supplémentaire de $\mathcal{A}l_2(E)$. ✎(7)

✎(7) Une application linéaire induit un isomorphisme de tout supplémentaire du noyau sur l'image.

Définition 5

Tout élément de $\operatorname{Im} \mathcal{Q} = \mathcal{Q}(E)$ s'appelle **une forme quadratique sur** E.

Définition 6

On appelle **forme polaire d'une forme quadratique** q sur E, la forme bilinéaire symétrique $\varphi \in \mathcal{S}_2(E)$ caractérisée par : $\forall x \in E, q(x) = \varphi(x, x)$.

Définition 7

Si q est une forme quadratique sur E, on a $q(0_E) = 0$.

Lorsque l'ensemble $C(q) = \{x \in E / q(x) = 0\}$ est réduit à $\{0_E\}$, on dit que la forme quadratique q est **définie**.

Remarque

Pour $q \in \mathcal{Q}(E)$, l'ensemble $C(q) = \{x \in E / q(x) = 0\}$ est invariant par toute homothétie :

$$\lambda \in \mathbb{R}, \quad x \mapsto \lambda x.$$

Il est appelé **cône isotrope** de q.

Formulaire

Soit $q \in \mathcal{Q}(E)$ et $\varphi \in \mathcal{S}_2(E)$ sa forme polaire. Pour tout $(x, y) \in E^2$ et $(\alpha, \beta) \in \mathbb{R}^2$, on a :

Formulaire 1

(1) $q(\alpha x + \beta y) = \alpha^2 q(x) + 2\,\alpha\,\beta\,\varphi(x, y) + \beta^2 q(y)$.

(2) $q(x + y) = q(x) + 2\,\varphi(x, y) + q(y)$.

(3) $q(x - y) = q(x) - 2\,\varphi(x, y) + q(y)$.

Formulaire 2

Identités de polarisation ✎(8)

(4) $\varphi(x, y) = \frac{1}{2}\left[q(x + y) - q(x) - q(y)\right]$.

(5) $\varphi(x, y) = \frac{1}{4}\left[q(x + y) - q(x - y)\right]$.

✎(8) Ces relations caractérisent la forme polaire φ de la forme quadratique q.

Formulaire 3

Identité du parallélogramme

$$q(x + y) + q(x - y) = 2\left(q(x) + q(y)\right).$$

Copyrighted material

Propriété 10

Caractérisation d'une forme quadratique

Une application $q : E \to \mathbb{R}$ est une forme quadratique si et seulement si :

$$\begin{cases} \forall (\alpha, x) \in \mathbb{R} \times E, \quad q(\alpha x) = \alpha^2 q(x) \\ E^2 \to \mathbb{R}, \quad (x, y) \mapsto q(x+y) - q(x-y) \text{ est une forme bilinéaire symétrique} \end{cases}$$

Propriété 11

Restriction d'une forme quadratique

Soit F un sous-espace de E. La restriction à F d'une forme quadratique sur E est une forme quadratique sur F.

Propriété 12

Soit $f \in \mathcal{L}(E, F)$ et $q \in \mathcal{Q}(F)$. Alors la composée $q \circ f$ est une forme quadratique sur E.
Si φ est la forme polaire de q, celle que $q \circ f$ est :

$$E^2 \to \mathbb{R}, \quad (x, y) \mapsto \varphi\big(f(x), f(y)\big).$$

Exemple 6 Soit $\theta, \theta_1, \theta_2$ des formes linéaires sur E.

a) L'application $q_1 = \theta^2 : E \to \mathbb{R}, \quad x \mapsto \big(\theta(x)\big)^2$ est une forme quadratique de forme polaire :

$$\varphi_1 : E^2 \to \mathbb{R}, \quad (x, y) \mapsto \theta(x)\,\theta(y).$$

b) Soit l'application q_2 définie sur E par $q_2 : E \to \mathbb{R}, \quad x \mapsto \theta_1(x)\,\theta_2(x)$.

$\varphi_2 : E^2 \to \mathbb{R}, \quad (x, y) \mapsto \dfrac{1}{2}\big(\theta_1(x)\,\theta_2(y) + \theta_2(x)\,\theta_1(y)\big)$ est bilinéaire symétrique et telle que $\forall x \in E, \quad q_2(x) = \varphi_2(x, x)$, donc q_2 est une forme quadratique de forme polaire φ_2.

Exemple 7 Soit $E = \mathcal{C}([a, b], \mathbb{R}), \quad (a < b)$, et la forme quadratique $q : E \to \mathbb{R}, \ f \mapsto \displaystyle\int_a^b f^2(t)\mathrm{d}t$, de forme polaire $\varphi : E^2 \to \mathbb{R}, \ (f, g) \mapsto \displaystyle\int_a^b f(t)g(t)\mathrm{d}t$. (Voir Exemple 1.)

La fonction f^2 étant positive, continue sur $[a, b]$, on sait que $\displaystyle\int_a^b f^2(t)\mathrm{d}t = 0$ exige $f(t) = 0$ pour tout t de $[a, b]$, c'est-à-dire $f = 0_E$. La forme quadratique q est donc définie.

Exemple 8 Soit q une forme quadratique sur E de forme polaire φ. Le **noyau** de q (ou de φ), noté $N(q)$ ou $N(\varphi)$ est l'ensemble : $\big\{x \in E \ / \ \forall\, y \in E, \quad \varphi(x, y) = 0\big\}$.

a) Montrer que $N(q)$ est un sous-espace vectoriel de E contenu dans le cône isotrope $C(q)$.

b) Trouver le noyau et le cône isotrope pour les formes quadratiques de l'exemple 6.

a) Pour tout $y \in E$, l'application $\varphi_y : E \to \mathbb{R}, \quad x \mapsto \varphi(x, y)$, est une forme linéaire sur E.

Par définition on a $N(q) = \displaystyle\bigcap_{y \in E} \operatorname{Ker} \phi_y$ donc $N(q)$ est un sous-espace vectoriel de E. ✎(9)

Si $x \in N(q)$ on a en particulier $\varphi(x, x) = 0$ donc $q(x) = 0$. Ainsi $N(q) \subset C(q)$.

b) 1) Il est clair que $C\big(q_1\big) = \operatorname{Ker} \theta$.

Pour $\theta \neq 0$, il existe $y_0 \in E$, $\theta\big(y_0\big) \neq 0$, alors $\varphi_1\big(x, y_0\big) = 0$ équivaut à $x \in \operatorname{Ker} \theta$.

On en déduit $N\big(q_1\big) = \operatorname{Ker} \theta$.

Pour $\theta = 0$, on a $\varphi_1 = 0$ donc $N\big(q_1\big) = E$ soit encore $N\big(q_1\big) = \operatorname{Ker} \theta$.

2) Il est clair que $C\big(q_2\big) = \operatorname{Ker} \theta_1 \cup \operatorname{Ker} \theta_2$.

- Si l'une des deux formes linéaires θ_1 ou θ_2 est nulle, on a $q_2 = 0$ et $N\big(q_2\big) = E$.
- Si les deux formes sont non nulles et proportionnelles : $\theta_2 = \lambda\theta_1, \quad \lambda \in \mathbb{R} \setminus \{0\}$, on a $q_2 = \lambda\theta_1^2$ et ✎(10) $N\big(q_2\big) = \operatorname{Ker} \theta_1$ donc $N\big(q_2\big) = \operatorname{Ker} \theta_1 = \operatorname{Ker} \theta_2 = \operatorname{Ker} \theta_1 \cap \operatorname{Ker} \theta_2$.

✎(9) Intersection d'une famille de sous-espaces vectoriels.

✎(10) Comme dans le 1).

Copyrighted material

Hidden page

☞ a) Pour $(x, y) \in E^2$ fixé, considérons l'application :

$$T : \mathbb{R} \to \mathbb{R}, \quad t \mapsto q(tx + y) = t^2 q(x) + 2t\,\varphi(x, y) + q(y).$$

On constate que T est une fonction polynôme de degré 2 au plus, à valeurs dans $\mathbb{R}_+$.

Si $q(x) = 0$, T étant de signe constant, on a aussi : $\varphi(x, y) = 0$. ✎(13)

Si $q(x) \neq 0$, la fonction polynôme T est de degré 2 et de signe constant donc son discriminant est négatif ou nul : $\Delta' = \big(\varphi(x, y)\big)^2 - q(x)q(y) \leqslant 0$.

Dans les deux cas, l'inégalité annoncée est prouvée.

b) Si x est nul, (x, y) est lié.

Si x est non nul, on a $q(x) \neq 0$ (q définie) et :

$$\big[\varphi(x, y)\big]^2 = q(x) \cdot q(y) \;\Rightarrow\; q\left(y - \frac{\varphi(x, y)}{q(x)}x\right) = 0 \quad \text{d'où} \quad y = \frac{\varphi(x, y)}{q(x)}x.$$

✎(13) Sinon T s'annulerait en changeant désigne au point $t_0 = -\frac{q(y)}{2\varphi(x,y)}$.

Théorème 3

Inégalité de Minkowski

a) Soit q une forme quadratique positive sur E. Alors :

$$\forall (x, y) \in E^2,\ \sqrt{q(x + y)} \leqslant \sqrt{q(x)} + \sqrt{q(y)}.$$

b) Si q est définie-positive, on a :

$$\sqrt{q(x + y)} = \sqrt{q(x)} + \sqrt{q(y)} \iff \exists\, \lambda \in \mathbb{R}_+,\ y = \lambda x \text{ ou } x = \lambda y.$$

☞ a) D'après l'inégalité de Cauchy-Schwarz, on a pour tout (x, y) :

$$\varphi(x, y) \leqslant |\varphi(x, y)| \leqslant \sqrt{q(x)}\sqrt{q(y)} \qquad \textbf{(1)}$$

donc $q(x) + 2\varphi(x, y) + q(y) \leqslant q(x) + 2\sqrt{q(x)}\sqrt{q(y)} + q(y)$ c'est-à-dire :

$$q(x + y) \leqslant \left(\sqrt{q(x)} + \sqrt{q(y)}\right)^2 \qquad \textbf{(2)}$$

et on conclut avec la positivité de $q(x + y)$.

b) Le calcul précédent s'écrit :

$$q(x + y) = q(x) + 2\varphi(x, y) + q(y) \leqslant q(x) + 2\sqrt{q(x)}\sqrt{q(y)} + q(y) = \left(\sqrt{q(x)} + \sqrt{q(y)}\right)^2$$

donc l'égalité $q(x + y) = \left(\sqrt{q(x)} + \sqrt{q(y)}\right)^2$ donne $\varphi(x, y) = \sqrt{q(x)}\sqrt{q(y)}$ et compte tenu de **(1)** on a aussi :

$$\varphi(x, y) = |\varphi(x, y)| = \sqrt{q(x)}\sqrt{q(y)}.$$

D'après l'étude du cas d'égalité de Cauchy-Schwarz, $\varphi(x, y) = \sqrt{q(x)}\sqrt{q(y)}$ donne (x, y) lié. Alors,

- si $x = 0$, on a $x = \lambda y$ avec $\lambda = 0 \in \mathbb{R}_+$;
- si $x \neq 0$, on a $y = \lambda x$ avec $\lambda \in \mathbb{R}$ et $\varphi(x, y) = |\varphi(x, y)|$ s'écrit $\lambda q(x) = |\lambda|\, q(x)$ ce qui, avec $q(x) > 0$, donne $\lambda \in \mathbb{R}_+$.

La réciproque est évidente.

Exemple 9 Une forme quadratique est convexe si et seulement si elle est positive.

Pour tout $(x, y) \in E^2$, $t \in [0, 1]$, on a :

$$q\big[(1 - t)x + ty\big] = (1 - t)^2 q(x) + 2(1 - t)t\,\varphi(x, y) + t^2 q(y).$$

On en déduit $(1 - t)q(x) + tq(y) - q\big[(1 - t)x + ty\big] = t(1 - t)q(x - y)$ et la conclusion en résulte.

Exemple 10 Si q est une forme quadratique sur E, on a l'équivalence :

$$N(q) = C(q) \iff q \text{ est positive ou négative.}$$

Le noyau d'une forme quadratique a été défini dans l'exemple 8.

Copyrighted material

Hidden page

2) Étant donné $M \in \mathcal{S}_n(\mathbb{R})$ par définition des matrices symétriques réelles positives ou définies-positives, on obtient :

$$M \in \mathcal{S}_n^+(\mathbb{R}) \iff \forall X \in \mathcal{M}_{n,1}(\mathbb{R}),\ {}^tXMX \geqslant 0$$

$$M \in \mathcal{S}_n^{++}(\mathbb{R}) \iff \forall X \in \mathcal{M}_{n,1}(\mathbb{R}) \setminus \{0\},\ {}^tXMX > 0$$

3) Étant donné une famille de scalaires $\left(\alpha_{ij}\right)_{1 \leqslant i \leqslant j \leqslant n}$, l'application :

$$\Phi : \mathbb{R}^n \to \mathbb{R}, x = \left(x_1, \cdots, x_n\right) \mapsto \sum_{1 \leqslant i \leqslant j \leqslant n} \alpha_{ij} x_i x_j$$

est une forme quadratique sur $\mathbb{R}^n$, sa forme polaire est :

$$(x, y) \mapsto \sum_{i=1}^{n} \alpha_{ii} x_i y_i + \frac{1}{2} \sum_{1 \leqslant i \leqslant j \leqslant n} \alpha_{ij} \left(x_i y_j + x_j y_i\right).$$

Sa matrice dans la base canonique de $\mathbb{R}^n$ est donnée par :

$$m_{ii} = \alpha_{ii} \quad et \quad m_{ij} = \frac{1}{2}\alpha_{ij} \quad \text{pour } i \neq j.$$

On dit aussi que Φ est un **polynôme quadratique** sur $\mathbb{R}^n$.

La forme polaire associée s'obtient par la règle dite de **dédoublement des variables** :

$$x_i^2 \longrightarrow x_i y_i \quad (i \neq j), x_i x_j \longrightarrow \frac{1}{2}\left(x_i y_j + x_j y_i\right).$$

4) Soit $\mathcal{B}$ et $\mathcal{B}'$ deux bases de E, $P = \mathcal{P}_{\mathcal{B}\mathcal{B}'}$ la matrice de passage, et $q \in \mathcal{Q}(E)$.

Avec $M = \mathrm{mat}_{\mathcal{B}}\, q$ et $M' = \mathrm{mat}_{\mathcal{B}'}\, q$, on a :

$$M' = {}^tPMP \quad \text{et} \quad \det M' = (\det P)^2 \cdot \det M.$$

Les matrices symétriques M et M' sont congruentes, donc de même rang.

Définition 12

Rang d'une forme quadratique

Soit q une forme quadratique sur E et φ sa forme polaire.

On appelle rang de q (ou rang de φ) le rang de $\mathrm{mat}_{\mathcal{B}}\, q = \mathrm{mat}_{\mathcal{B}}\, \varphi$.

Il ne dépend pas du choix de la base $\mathcal{B}$, on le note $\mathrm{rg}\, q$ (ou $\mathrm{rg}\, \phi$).

Définition 13

On appelle **discriminant** de $q \in \mathcal{Q}(E)$ dans une base $\mathcal{B}$, le scalaire :

$$\Delta_{\mathcal{B}}(q) = \det(\mathrm{mat}_{\mathcal{B}}\, q)$$

Avec les notations de la remarque 3) précédente, on a : $\Delta_{\mathcal{B}'}(q) = (\det P)^2 \cdot \Delta_{\mathcal{B}}(q)$.

Définition 14

Une forme quadratique $q \in \mathcal{Q}(E)$ est dite **non dégénérée** lorsque $\mathrm{rg}\, q = \dim E$.

Sinon, c'est-à-dire lorsque $\mathrm{rg}\, q < \dim E$, elle est dite **dégénérée**.

Exemple 11 Matrice sur la base canonique $\mathcal{B}$ et rang des formes quadratiques définies sur $\mathbb{R}^4$ par :

$$q_1(x) = x_1^2 - x_2^2 + 2x_4^2 - 2x_1x_2 + 4x_1x_3 - 2x_2x_4\,.$$

$$q_2(x) = x_1x_2 - 2x_1x_4 + 2x_2x_3 - 4x_3x_4\,.$$

On applique la remarque 3) suivant la définition 11.

La diagonale est formée des coefficients des termes carrés x_1^2, x_2^2, ... et en dehors de la diagonale, on met les coefficients des x_ix_j $(i \neq j)$ divisés par 2.

$$A_1 = \mathrm{mat}_{\mathcal{B}}\, q_1 = \begin{pmatrix} 1 & -1 & 2 & 0 \\ -1 & -1 & 0 & -1 \\ 2 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2 \end{pmatrix}.$$

Le calcul donne facilement $\det A_1 = 12$ donc $\mathrm{rg}\, q_1 = 4$.

Copyrighted material

Hidden page

$$\left\langle \sum_{i=1}^{n} \lambda_i x_i \,\middle|\, \sum_{j=1}^{p} \mu_j y_j \right\rangle = \sum_{i=1}^{n} \sum_{j=1}^{p} \lambda_i \mu_j \langle x_i \mid y_j \rangle$$

$$\left\langle \sum_{i=1}^{n} \lambda_i x_i \,\middle|\, \sum_{j=1}^{n} \lambda_j x_j \right\rangle = \sum_{i=1}^{n} \lambda_i^2 \langle x_i \mid x_i \rangle + 2 \sum_{1 \leqslant i < j \leqslant n} \lambda_i \lambda_j \langle x_i \mid x_j \rangle$$

Exemples usuels

1) $E = \mathbb{R}^n, \varphi : E^2 \to \mathbb{R}, (x, y) \mapsto \sum_{i=1}^{n} x_i y_i$ où $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$.

φ est un produit scalaire euclidien sur E dit **produit scalaire euclidien canonique**. (17)

(17) C'est le produit scalaire de la géométrie usuelle.

2) $E = \mathcal{C}^k([a, b], \mathbb{R}), (a, b) \in \mathbb{R}^2, a < b, k \geqslant 0$.

$\varphi : E^2 \to \mathbb{R}, (f, g) \mapsto \int_a^b fg$: φ est un produit scalaire euclidien sur E.

La vérification des axiomes **(1)** et **(2)** est évidente. (18) Celle de l'axiome **(5)** résulte d'une propriété connue de l'intégrale d'une fonction continue positive sur un segment $[a, b]$ $(a < b)$.

(18) Linéarité de l'intégrale.

Définition 16

Un **espace préhilbertien réel** est un :

$\mathbb{R}$-espace vectoriel E muni d'un produit scalaire euclidien φ.

Un tel espace sera noté (E, φ) ou E s'il n'y a pas d'ambiguïté.

Théorème 4

Sous espaces-préhilbertiens réels

Soit (E, φ) un espace préhilbertien réel et F un sous-espace vectoriel de E.

La restriction $\varphi_{|F^2}$ de φ à F^2 est un produit scalaire euclidien sur F, il est encore noté φ.

Exemple 13 Soit E l'ensemble des suites réelles $u = (u_n)_{n \in \mathbb{N}}$ telles que la série $\sum_{n \geqslant 0} u_n^2$ soit convergente.

a) E est un $\mathbb{R}$-espace vectoriel.

Il s'agit de montrer que E est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$.

E est non vide car il contient la suite nulle et il est clair que, pour tout $u \in E$ et tout réel λ, $\lambda u \in E$. En remarquant que, pour tous réels a et b, on a $(a + b)^2 \leqslant 2(a^2 + b^2)$, on obtient :

$$\forall n \in \mathbb{N}, (u_n + v_n)^2 \leqslant 2(u_n^2 + v_n^2).$$

Si $u \in E$ et $v \in E$, alors les séries de termes généraux u_n^2 et v_n^2 sont convergentes et il en est de même pour la série de terme général $2(u_n^2 + v_n^2)$, donc le critère de domination des séries à termes positifs donne la convergence de $\sum_{n=0}^{+\infty} (u_n + v_n)^2$; ainsi $u + v \in E$.

b) $\varphi : E \to \mathbb{R}, (u, v) \mapsto \sum_{n=0}^{+\infty} u_n v_n$ est un produit scalaire euclidien.

Il faut d'abord prouver la convergence de $\sum_{n \geqslant 0} u_n v_n$ avec u et v dans E.

Pour tous réels a et b, on a $|ab| \leqslant a^2 + b^2$, donc $\forall n \in \mathbb{N}, |u_n v_n| \leqslant u_n^2 + v_n^2$.

Si $u \in E$ et $v \in E$, le critère de domination des séries à termes positifs donne la convergence de $\sum_{n \geqslant 0} |u_n v_n|$. La convergence de $\sum_{n \geqslant 0} u_n v_n$ en résulte.

On vérifie sans difficulté que φ satisfait aux axiomes de définition du produit scalaire :

φ est bilinéaire, symétrique et, si $u \in E \setminus \{0\}$, il existe $n_0 \in \mathbb{N}$ tel que $u_{n_0} \neq 0$ et alors :

$$\varphi(u, u) = \sum_{n=0}^{+\infty} u_n^2 \geqslant u_{n_0}^2 > 0.$$

Copyrighted material

2. Norme euclidienne

E est un espace préhilbertien réel, le produit scalaire de deux vecteurs x et y est noté $\langle x \mid y \rangle$.

Notation 3

Pour tout x de E, $\langle x \mid x \rangle$ est un réel positif, on note : $\|x\| = \sqrt{\langle x \mid x \rangle}$.

Conséquences

1) $\forall x \in E \setminus \{0\}, \|x\| > 0$. 2) $\forall x \in E, \|x\| \geqslant 0$. 3) $\forall x \in E, \|x\| = 0 \Rightarrow x = 0$.

Théorème 5

Inégalités de Cauchy-Schwarz et de Minkowski

a) $\forall (x, y) \in E^2, \left|\langle x \mid y \rangle\right| \leqslant \|x\| \|y\|$ (Inégalité de Cauchy-Schwarz).

b) $\forall (x, y) \in E^2, \|x + y\| \leqslant \|x\| + \|y\|$ (Inégalité triangulaire, ou de Minkowski).

☞ On applique les théorèmes 2 et 3 avec :

$$\varphi(x, y) = \langle x \mid y \rangle \text{ et } q(x) = \langle x \mid x \rangle = \|x\|^2.$$

Théorème 6

Cas d'égalité de Cauchy-Schwarz et Minkowski

a) $\left|\langle x \mid y \rangle\right| = \|x\| \|y\|$ équivaut à (x, y) est lié.

b) $\|x + y\| = \|x\| + \|y\|$ équivaut à (x, y) est positivement lié.

☞ On applique de même les théorèmes 2 et 3.

Théorème 7

Norme euclidienne

L'application $E \to \mathbb{R}^+, x \mapsto \|x\| = \sqrt{\langle x \mid x \rangle}$ est une norme sur E.

☞ On vérifie les axiomes de définition des normes.

$\|x\| = 0$ exige $x = 0$ par définition d'un produit scalaire.

$\|\lambda x\| = \sqrt{\lambda^2 \langle x \mid x \rangle} = |\lambda| \|x\|, (\lambda \in \mathbb{R})$.

$\|x + y\| \leqslant \|x\| + \|y\|$ (Inégalité de Minkowski).

Formulaire 4

Pour tout x de E, on a $\|x\| = \sup_{y \in \mathcal{B}} \left|\langle x \mid y \rangle\right|$ [19] où $\mathcal{B}$ désigne la boule unité fermée de E :

$$\mathcal{B} = \left\{y \in E \,/\, \|y\| \leqslant 1\right\}.$$

[19] On notera aussi $\|x\| = \sup_{\|y\| \leqslant 1} |\langle x \mid y \rangle|$.

☞ Pour tout $y \in \mathcal{B}$, l'inégalité de Cauchy-Schwarz donne $\left|\langle x \mid y \rangle\right| \leqslant \|x\| \|y\| \leqslant \|x\|$ donc :

$$\sup_{y \in \mathcal{B}} \left|\langle x \mid y \rangle\right| \leqslant \|x\|. \quad \text{(i)}$$

Si x est non nul, on a $\dfrac{x}{\|x\|} \in \mathcal{B}$ et $\left|\left\langle x \,\middle|\, \dfrac{x}{\|x\|} \right\rangle\right| = \|x\|$ donc $\|x\| \leqslant \sup_{y \in \mathcal{B}} \left|\langle x \mid y \rangle\right|$. (ii)

Avec (i) et (ii) on obtient alors $\|x\| = \sup_{y \in \mathcal{B}} \left|\langle x \mid y \rangle\right|$.

Cette égalité étant évidente lorsque $x = 0_E$, la preuve est complète.

Copyrighted material

Hidden page

Hidden page

Hidden page

☞ Soit x et y fixés dans E.

a) $\forall \lambda \in \mathbb{C},\ \|\lambda x + y\|^2 = \langle \lambda x + y \mid \lambda x + y \rangle = |\lambda|^2 \|x\|^2 + 2\,\mathrm{Re}\,\overline{\lambda}\langle x \mid y \rangle + \|y\|^2$ **(1)**

Posons $|\langle x \mid y \rangle| = r$ et $\langle x \mid y \rangle = re^{i\theta}$, on déduit de **(1)** que, pour tout t réel :

$$\|te^{i\theta}x + y\|^2 = t^2\|x\|^2 + 2rt + \|y\|^2.$$

- Si $x \neq 0_E$, $t \mapsto \|te^{i\theta}x + y\|^2$ est une fonction polynôme réelle du second degré à valeurs positives, d'où :

$$r^2 - \|x\|^2\|y\|^2 \leqslant 0 \text{ c'est-à-dire } |\langle x \mid y \rangle| \leqslant \|x\|\,\|y\|. \text{ (25)}$$

- Si $x = 0_E$, alors $\langle x \mid y \rangle = 0$ et l'inégalité a) est encore vraie.

b) En utilisant $\mathrm{Re}\,\langle x \mid y \rangle \leqslant |\langle x \mid y \rangle| \leqslant \|x\|\,\|y\|$, on obtient :

$$\|x+y\|^2 = \|x\|^2 + 2\,\mathrm{Re}\,\langle x \mid y \rangle + \|y\|^2 \leqslant \|x\|^2 + 2\|x\|\,\|y\| + \|y\|^2 = \left(\|x\| + \|y\|\right)^2$$

(25) Son discriminant est négatif ou nul.

Théorème 11

Cas d'égalité de Cauchy-Schwarz et de Minkowski

a) $|\langle x \mid y \rangle| = \|x\|\,\|y\|$ équivaut à (x, y) est lié.

b) $\|x + y\| = \|x\| + \|y\|$ équivaut à (x, y) est positivement lié.

☞ a) Supposons $|\langle x \mid y \rangle| = \|x\|\,\|y\|$.

- Si $\|x\| = 0$, on a $x = 0_E$ et (x, y) est lié.
- Si $\|x\| \neq 0$, il existe $t \in \mathbb{R}$ racine double de $t^2\|x\|^2 + 2rt + \|y\|^2 = 0$ (26)

donc tel que $\|te^{i\theta}x + y\|^2 = 0$, ce qui exige $te^{i\theta}x + y = 0_E$, donc (x, y) est lié. (27)

b) Supposons $\|x + y\| = \|x\| + \|y\|$.

- Si $x = 0_E$, (x, y) est positivement lié ($x = 0 \cdot y$).
- Si $x \neq 0_E$, $\|x + y\|^2 = \left(\|x\| + \|y\|\right)^2$ donne $\mathrm{Re}\,\langle x \mid y \rangle = \|x\|\,\|y\|$ et, puisque $\mathrm{Re}\,\langle x \mid y \rangle \leqslant |\langle x \mid y \rangle| \leqslant \|x\|\,\|y\|$, on en déduit :

$$\mathrm{Re}\,\langle x \mid y \rangle = |\langle x \mid y \rangle| = \|x\|\,\|y\|.$$

D'après a), $|\langle x \mid y \rangle| = \|x\|\,\|y\|$ donne l'existence de $\lambda \in \mathbb{C}$ tel que $y = \lambda x$ donc :

$$\langle x \mid y \rangle = \lambda\|x\|^2.$$

D'autre part, $\mathrm{Re}\,\langle x \mid y \rangle = |\langle x \mid y \rangle|$ donne que $\langle x \mid y \rangle$ est réel positif, donc λ est réel positif et (x, y) est positivement lié. La réciproque est évidente.

(26) Cette équation a un discriminant nul.

(27) La réciproque est évidente.

Théorème 12

Norme hermitienne

L'application $E \to \mathbb{R}_+, x \mapsto \|x\| = \sqrt{\langle x \mid x \rangle}$ est une norme sur E.

☞ On vérifie les axiomes de définition des normes.

$\|x\| = 0$ donne $x = 0_E$.

$\|\lambda x\| = \sqrt{\langle \lambda x \mid \lambda x \rangle} = \sqrt{|\lambda|^2 \langle x \mid x \rangle} = |\lambda|\,\|x\|,\ \lambda \in \mathbb{C}$.

$\|x + y\| \leqslant \|x\| + \|y\|$ (Inégalité de Minkowski).

Formulaire 6

Pour tout x de E, on a $\|x\| = \sup_{y \in \mathcal{B}} |\langle x \mid y \rangle|$ où $\mathcal{B}$ désigne la boule unité fermée de E :

$$\mathcal{B} = \{y \in E \,/\, \|y\| \leqslant 1\}.$$

☞ La démonstration est identique à celle du formulaire 4.

Copyrighted material

Formulaire

Pour tous vecteurs x et y de E :

(1) $\|x+y\|^2 = \|x\|^2 + \langle x \mid y\rangle + \langle y \mid x\rangle + \|y\|^2$.

(2) $\|x-y\|^2 = \|x\|^2 - \langle x \mid y\rangle - \langle y \mid x\rangle + \|y\|^2$.

(3) $\|x+iy\|^2 = \|x\|^2 + i\langle x \mid y\rangle - i\langle y \mid x\rangle + \|y\|^2$.

(4) $\|x-iy\|^2 = \|x\|^2 - i\langle x \mid y\rangle + i\langle y \mid x\rangle + \|y\|^2$.

(5) $\langle x \mid y\rangle = \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2 - i\|x+iy\|^2 + i\|x-iy\|^2\right)$.

La formule (5) est appelée **identité de polarisation**, elle permet de retrouver le produit scalaire en fonction de la norme.

D. Orthogonalité

[28] $\mathbb{K}$ désigne $\mathbb{R}$ ou $\mathbb{C}$.

$(E, \langle \cdot \mid \cdot \rangle)$ est un espace préhilbertien réel ou complexe. [28]

1. Définitions – Propriétés générales

Définition 22

Deux vecteurs x et y sont dits **orthogonaux** si $\langle x \mid y\rangle = 0$.

[29] Euclidien ou hermitien.

On remarquera que, quel que soit le cas, [29] $\langle x \mid y\rangle = 0$ équivaut à $\langle y \mid x\rangle = 0$.
La relation ainsi définie est donc symétrique.

Définition 23

Deux parties A et B de E sont dites orthogonales si $\forall (x,y) \in A \times B, \langle x \mid y\rangle = 0$.

Définition 24

L'orthogonal d'une partie $A \neq \emptyset$ de E est l'ensemble $A^\perp = \{x \in E \,/\, \forall y \in A, \langle x \mid y\rangle = 0\}$.
Si $A = \emptyset$, on pose $A^\perp = E$.
Le double orthogonal $(A^\perp)^\perp$ est noté $A^{\perp\perp}$.

En particulier, $E^\perp = \{0_E\}$ et $\{0_E\}^\perp = E$.

Définition 25

Une famille $(u_i)_{i\in I}$ de E est dite :

- **orthogonale** si $\forall (i,j) \in I^2, i \neq j \Rightarrow \langle u_i \mid u_j\rangle = 0$,
- **orthonormale** [30] si $\forall (i,j) \in I^2, \langle u_i \mid u_j\rangle = \delta_{ij}$.

[30] Ou orthonormée.

Si $(u_i)_{i\in I}$ est une base, on parle de base orthogonale ou orthonormale.

Propriété 15

Orthogonal d'une partie de E

A et B désignent des parties de E.

a) $A^\perp$ est un sous-espace vectoriel de E.

b) Si $A \subset B$ alors $B^\perp \subset A^\perp$.

c) $A^\perp = (\text{Vect } A)^\perp$.

d) $A \subset A^{\perp\perp}$.

Copyrighted material

Hidden page

$$\sum_{j=1}^{p} x_j = 0_E \text{ donne } 0 = \left\langle x_i \,\middle|\, \sum_{j=1}^{p} x_j \right\rangle = \|x_i\|^2 \text{ donc } x_i = 0_E.$$

Autre preuve

Pour tout $i \in [\![1, p]\!]$ on a $\sum_{\substack{1 \leqslant j \leqslant p \\ j \neq i}} F_j \subset F_i^{\perp}$ donc $F_i \cap \sum_{\substack{1 \leqslant j \leqslant p \\ j \neq i}} F_j = \{0_E\}$.

Définition 27

Soit $(F_i)_{1 \leqslant i \leqslant p}$ une famille finie de sous-espaces vectoriels de E deux à deux orthogonaux.

Si la somme directe $\bigoplus_{1 \leqslant i \leqslant p} F_i$ est égale à E, on dit que $(F_i)_{1 \leqslant i \leqslant p}$ est une famille de sous-espaces **supplémentaires orthogonaux**.

Exemple 15 On reprend $E = \left\{ (u_n)_{\mathbb{N}} \in \mathbb{R}^{\mathbb{N}} \,\middle|\, \sum_{n=0}^{+\infty} u_n^2 < +\infty \right\}$, [34] $\forall (u, v) \in E^2$, $u = (u_n)_{\mathbb{N}}$, $v = (v_n)_{\mathbb{N}}$, $\langle u \,|\, v \rangle = \sum_{n=0}^{+\infty} u_n v_n$. Alors, pour le sous-espace F de E formé des suites presque nulles, on a :

$$F \oplus F^{\perp} \neq E \text{ et } F^{\perp\perp} \neq F.$$

[34] Espace préhilbertien réel défini dans l'exemple 13.

L'ensemble F des suites presque nulles est un sous-espace vectoriel de $\mathbb{R}^{\mathbb{N}}$. [35] et si u est presque nulle, la série de terme général u_n^2 converge, donc F est un sous-espace vectoriel de E.

[35] $u \in \mathbb{R}^{\mathbb{N}}$ est dite presque nulle lorsqu'il existe $n_0 \in \mathbb{N}$ tel que : $n > n_0 \Rightarrow u_n = 0$.

Par ailleurs, une base de F est $(H_n)_{n \in \mathbb{N}}$ où les H_n sont les suites définies par $H_n = (\delta_{n,k})_{k \in \mathbb{N}}$ (avec $\delta_{n,k} = 0$ si $k \neq n$ et $\delta_{n,n} = 1$: symbole de Kronecker).

Soit $u \in E$, d'après la propriété 15 :

$$u \in F^{\perp} \iff \forall n \in \mathbb{N}, \langle u \,|\, H_n \rangle = 0$$

$$\text{donc } u \in F^{\perp} \iff \forall n \in \mathbb{N}, u_n = 0$$

Ainsi, on a $F^{\perp} = \{0_E\}$ et $F \oplus F^{\perp} = F$.

F est différent de E puisque, par exemple, la suite $\left(\frac{1}{n+1}\right)_{n \in \mathbb{N}}$ est élément de E mais n'appartient pas à F.

Enfin, $F^{\perp} = \{0_E\}$ donne $F^{\perp\perp} = E$ et donc $F \neq F^{\perp\perp}$.

Propriété 19

Sous-espaces supplémentaires orthogonaux

Si F et G sont deux sous-espaces supplémentaires : $E = F \oplus G$, les propriétés suivantes sont équivalentes :

(1) F et G sont orthogonaux, **(2)** $G = F^{\perp}$, **(3)** $F = G^{\perp}$.

- Les parties F et G sont orthogonales si et seulement si : [36]

$$\forall x \in F, \ \forall y \in G, \ \langle x \,|\, y \rangle = 0$$

et cette proposition est équivalente à [37] $G \subset F^{\perp}$ et à $F \subset G^{\perp}$.

[36] Définition 23.

[37] Propriété 16.

- Les implications **(2)** $\Rightarrow$ **(1)** et **(3)** $\Rightarrow$ **(1)** sont évidentes.
- Montrons que **(1)** $\Rightarrow$ **(2)**.

On suppose donc que F et G sont deux sous-espaces tels que $E = F \oplus G$ et $G \subset F^{\perp}$, il s'agit de montrer que $F^{\perp} \subset G$.

Étant donné $x \in F^{\perp}$, puisque $E = F \oplus G$, il existe $x' \in F$ et $x'' \in G$ tels que $x = x' + x''$, et on a alors $\langle x | x' \,|\, = \rangle 0$ et, puisque $G \subset F^{\perp}$, $\langle x' \,|\, x'' \rangle = 0$, donc $\| x' \|^2 = \langle x \,|\, x' \rangle - \langle x'' \,|\, x' \rangle = 0$, puis $x' = 0_E$; en conséquence, $x = x'' \in G$, ce qui montre $F^{\perp} \subset G$.

On a de même **(1)** $\Rightarrow$ **(3)**, (en fait F et G jouant des rôles symétriques dans **(1)**, les implications **(1)** $\Rightarrow$ **(2)** et **(1)** $\Rightarrow$ **(3)** sont identiques.

Copyrighted material

Propriété 20

Si F est un sous-espace de E tel que $E = F \oplus F^\perp$, on a alors $F = F^{\perp\perp}$.

☞ C'est un corollaire de la propriété 19. En effet, $G = F^\perp$ donne $F = G^\perp = F^{\perp\perp}$.

Propriété 21

Si $(F_i)_{1\leqslant i\leqslant p}$ est une famille finie de sous-espaces supplémentaires orthogonaux, on a :

$$\forall i \in [\![1, p]\!], \quad \sum_{\substack{1\leqslant j\leqslant p \\ j\neq i}} F_j = F_i^\perp.$$

☞ C'est un corollaire de la propriété 19.

En effet, avec $G = \sum_{\substack{1\leqslant j\leqslant p \\ j\neq i}} F_j$, on a $G \subset F_i^\perp$ et $E = G \oplus F_i$ donc $G = F_i^\perp$.

Propriété 22

Familles orthogonales

a) Toute famille orthogonale $(u_i)_{i\in I}$ de vecteurs non nuls est libre.

b) Si $(u_i)_{1\leqslant i\leqslant p}$ est une famille orthogonale, alors $\left\| \sum_{i=1}^{p} u_i \right\|^2 = \sum_{i=1}^{p} \| u_i \|^2$.

☞ a) Il suffit de prouver que toute famille finie $(u_{i_k})_{1\leqslant k\leqslant p}$ est libre. Soit donc $(\lambda_k)_{1\leqslant k\leqslant p}$ une famille de scalaires telle que $\sum_{i=1}^{p} \lambda_k u_{i_k} = 0_E$. En multipliant scalairement par $u_{i_{k_0}}$, on obtient [38] $0 = \left\langle u_{i_{k_0}} \middle| \sum_{i=1}^{p} \lambda_k u_{i_k} \right\rangle = \lambda_{k_0} \left\| u_{i_{k_0}} \right\|^2$ donc $\lambda_{k_0} = 0$ car $u_{i_{k_0}} \neq 0_E$.

On a ainsi prouvé que les λ_k sont tous nuls et donc que $(u_{i_k})_{1\leqslant k\leqslant p}$ est libre.

b) Il suffit de développer $\left\langle \sum_{i=1}^{p} u_i \middle| \sum_{j=1}^{p} u_j \right\rangle$: c'est le **théorème de Pythagore**.

[38] Quel que soit le cas de figure : $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Cas particulier

Théorème 13

Soit E un espace préhilbertien réel et $(x, y) \in E^2$.

x et y sont orthogonaux si et seulement si $\| x + y \|^2 = \| x \|^2 + \| y \|^2$.

☞ En effet, on a alors $\| x + y \|^2 - \| x \|^2 - \| y \|^2 = 2\langle x \mid y \rangle$.

Remarque

Ce résultat est faux dans un espace préhilbertien complexe car on a alors :

$$\| x + y \|^2 - \| x \|^2 - \| y \|^2 = 2 \operatorname{Re} \langle x \mid y \rangle.$$

Par exemple, dans $\mathbb{C}^2$ hermitien canonique, soit : $x = (i, 1)$, $y = (1, -i)$.

On a alors $\langle x \mid y \rangle = -i - i = -2i \neq 0$, x et y ne sont pas orthogonaux.

Cependant, $\| x \|^2 = 2$, $\| y \|^2 = 2$ et $x + y = (1 + i, 1 - i)$, donc :

$$\| x + y \|^2 = 4 = \| x \|^2 + \| y \|^2.$$

Copyrighted material

Hidden page

2.2 – Cas où F est de dimension finie

E est maintenant supposé de dimension quelconque.

Théorème 17

Orthogonal d'un vecteur non nul

Soit $a \in E \setminus \{0_E\}$, alors $(a)^\perp = (\mathbb{K}a)^\perp$ est un hyperplan supplémentaire orthognal de la droite vectorielle $\mathbb{K}a$: $E = \mathbb{K}a \oplus (\mathbb{K}a)^\perp$.

☞ $(\mathbb{K}a)^\perp$ est le noyau de la forme linéaire $f : E \to \mathbb{K}, x \mapsto \langle a \mid x \rangle$. Cette forme linéaire est non nulle car $f(a) = \| a \|^2 \neq 0$ donc $\operatorname{Ker} f$ est un hyperplan de E. Tout x de E s'écrit :

$$x = \frac{\langle a \mid x \rangle}{\| a \|^2} a + \left(x - \frac{\langle a \mid x \rangle}{\| a \|^2} a \right)$$

avec $\frac{\langle a \mid x \rangle}{\| a \|^2} a \in \mathbb{K}a$ et $x - \frac{\langle a \mid x \rangle}{\| a \|^2} a \in (\mathbb{K}a)^\perp$ d'où $E = \mathbb{K}a \oplus (\mathbb{K}a)^\perp$.

Théorème 18

Si F est un sous-espace de dimension finie de l'espace préhilbertien E, alors $E = F \oplus F^\perp$.

☞ La propriété est évidente si $F = \{0_E\}$. On se limite donc au cas où F est de dimension $n \geqslant 1$. F admet une base orthonormale $(e_i)_{1 \leqslant i \leqslant n}$. [40]

Étant donné $x \in E$ et $(\lambda_1, \ldots, \lambda_n) \in \mathbb{K}^n$, posons $y = x - \sum_{i=1}^{n} \lambda_i e_i$.

On a alors $y \in F^\perp$ si et seulement si $\forall\, k \in [\![1, n]\!], \langle e_k \mid y \rangle = 0$

donc si et seulement si $\forall\, k \in [\![1, n]\!], \langle e_k \mid x \rangle - \sum_{i=1}^{n} \lambda_i \langle e_k \mid e_i \rangle = 0$

soit encore si et seulement si $\forall\, k \in [\![1, n]\!], \lambda_k = \langle e_k \mid x \rangle$.

En conséquence, pour tout x de E, on a $x = \sum_{i=1}^{n} \langle e_i \mid x \rangle e_i + \left(x - \sum_{i=1}^{n} \langle e_i \mid x \rangle e_i \right)$ avec $\sum_{i=1}^{n} \langle e_i \mid x \rangle e_i \in F$, et, d'après le calcul précédent $\left(x - \sum_{i=1}^{n} \langle e_i \mid x \rangle e_i \right) \in F^\perp$.

Ceci montre que $E = F \oplus F^\perp$. [41]

[40] D'après le théorème 15.

[41] On sait déjà que F et $F^\perp$ sont en somme directe.

2.3 – Projection orthogonale sur un sous-espace de dimension finie

Définition 28

Soit F un sous-espace de dimension finie d'un espace préhilbertien E.

On alors $E = F \oplus F^\perp$ et le projecteur de noyau $F^\perp$ et d'image F est appelé projection orthogonale sur F.

Théorème 19

Si $(e_i)_{1 \leqslant i \leqslant n}$ est une base orthonormale du sous-espace F de dimension finie, la projection orthogonale p_F sur F est définie par : [42]

$$\forall x \in E, \quad p_F(x) = \sum_{i=1}^{n} \langle e_i \mid x \rangle e_i .$$

[42] Voir la démonstration du théorème 18.

Copyrighted material

Hidden page

En conséquence, il y a une infinité de solutions pour y_{n+1}, il s'agit des vecteurs :

$$\lambda\left(x_{n+1} - p_n(x_{n+1})\right) \quad \text{avec} \quad \lambda \in \mathbb{K} \setminus \{0\}.$$

Ces solutions décrivent une droite vectorielle privée de 0_E.

La propriété est donc récurrente.

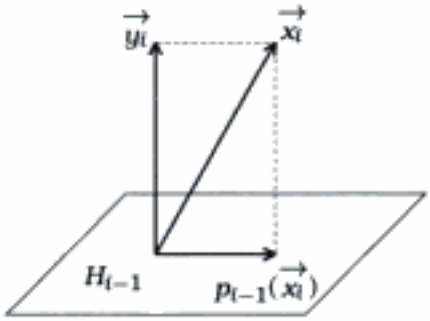
Remarque

Il résulte de cette démonstration que chaque vecteur y_i est défini à un coefficient de colinéarité près.

Dans la pratique, il suffit de construire une famille $(y_i)_{1\leqslant i\leqslant n}$ pour connaître toutes les solutions du problème.

On prendra, par exemple, la famille qui est définie par :

$$y_1 = x_1, \quad \forall i \in [\![2, n]\!],\ y_i = x_i - p_{i-1}(x_i)$$



Exemple 17 Sur $E = \mathbb{C}_2[X]$, $\langle P \,|\, Q\rangle = \overline{P(1)}Q(1) + \overline{P(i)}Q(i) + \overline{P(-i)}Q(-i)$ définit un produit scalaire hermitien. Détermination d'une base orthogonale (P_0, P_1, P_2) avec $\deg P_k = k$.

a) On vérifie aisément que $\varphi : (P, Q) \mapsto \overline{P(1)}Q(1) + \overline{P(i)}Q(i) + \overline{P(-i)}Q(-i)$ est une forme sesquilinéaire hermitienne sur E.

Elle est positive car $\varphi(P, P) = |P(1)|^2 + |P(i)|^2 + |P(-i)|^2 \geqslant 0$.

Elle est définie car $\varphi(P, P) = 0$ donne $P(1) = P(i) = P(-i) = 0$ et donc $P = 0$, car un polynôme non nul de degré $\leqslant 2$ a au plus deux racines distinctes.

b) On applique le procédé d'orthogonalisation de Schmidt à la base canonique $(1, X, X^2)$.

$$P_0 = 1,\ P_1 = X - \frac{\langle P_0 \,|\, X\rangle}{\langle P_0 \,|\, P_0\rangle} P_0,\ P_2 = X^2 - \frac{\langle P_0 \,|\, X^2\rangle}{\langle P_0 \,|\, P_0\rangle} P_0 - \frac{\langle P_1 \,|\, X^2\rangle}{\langle P_1 \,|\, P_1\rangle} P_1.$$

On trouve successivement :

$$\langle P_0 \,|\, X\rangle = 1 + i - i = 1,\ \langle P_0 \,|\, P_0\rangle = 3 \text{ donc } P_1 = X - \frac{1}{3};$$

$$\langle P_0 \,|\, X^2\rangle = 1 - 1 - 1 = -1,\ \langle P_1 | X^2 \,|=\rangle \frac{2}{3} + \left(-i - \frac{1}{3}\right) \times (-1) + \left(i - \frac{1}{3}\right) \times (-1) = \frac{4}{3};$$

$$\langle P_1 \,|\, P_1\rangle = \left(\frac{2}{3}\right)^2 + \left|i - \frac{1}{3}\right|^2 + \left|-i - \frac{1}{3}\right|^2 = \frac{8}{3} \text{ donc } P_2 = X^2 - \frac{X}{2} + \frac{1}{2}.$$

Théorème 21

Orthonormalisation

Pour toute famille libre $(x_i)_{1\leqslant i\leqslant n}$, il existe au moins une famille libre orthonormale telle que :

$$\forall i \in [\![1, n]\!],\ \text{Vect}\,(x_1, \ldots, x_i) = \text{Vect}\,(y_1, \ldots, y_i)$$

Il suffit de prendre la famille y_i définie par :

$$y_1 = \frac{x_1}{\|x_1\|} \quad \text{et} \quad \forall i \in [\![2, n]\!],\ y_i = \frac{x_i - p_{i-1}(x_i)}{\|x_i - p_{i-1}(x_i)\|}.$$

Remarque. Cas des espaces préhilbertiens réels

Théorème 22

Pour toute famille libre $(x_i)_{1\leqslant i\leqslant n}$, il existe une unique famille orthonormale telle que :

$$\forall i \in [\![1, n]\!],\ \text{Vect}\,(x_1, \ldots, x_i) = \text{Vect}\,(y_1, \ldots, y_i),\ \langle x_i \,|\, y_i\rangle > 0.$$

Copyrighted material

☞ En effet, il y a deux possibilités pour y_1 : $y_1 = \dfrac{x_1}{\|x_1\|}$ ou $y_1 = -\dfrac{x_1}{\|x_1\|}$.

La condition $\langle y_1 \mid x_1 \rangle \in \mathbb{R}_+^*$ impose alors $y_1 = \dfrac{x_1}{\|x_1\|}$.

Pour tout $i \in [\![2, n]\!]$, il y a aussi deux possibilités :

$$y_i = \frac{x_i - p_{i-1}(x_i)}{\|x_i - p_{i-1}(x_i)\|} \quad \text{ou} \quad y_i = -\frac{x_i - p_{i-1}(x_i)}{\|x_i - p_{i-1}(x_i)\|}.$$

Avec $\langle y_i \mid p_{i-1}(x_i) \rangle = 0$, le premier cas donne :

$$\langle y_i \mid x_i \rangle = \|x_i - p_{i-1}(x_i)\| \, \|y_i\|^2$$

et le second : $\langle y_i \mid x_i \rangle = -\|x_i - p_{i-1}(x_i)\| \, \|y_i\|^2$.

Donc la condition $\langle y_i \mid x_i \rangle \in \mathbb{R}_+^*$ impose $y_i = \dfrac{x_i - p_{i-1}(x_i)}{\|x_i - p_{i-1}(x_i)\|}$.

3. Projections et symétries orthogonales

Définition 29

Projecteur orthogonal

Étant donné un projecteur p de E, les propositions suivantes sont équivalentes :

(1) $\operatorname{Im} p$ et $\operatorname{Ker} p$ sont orthogonaux,

(2) $\operatorname{Ker} p = (\operatorname{Im} p)^\perp$,

(3) $\operatorname{Im} p = (\operatorname{Ker} p)^\perp$.

Lorsqu'il vérifie l'une de ces trois propositions, le projecteur p est dit **orthogonal**.

Remarque

p étant un projecteur, on sait que $E = \operatorname{Im} p \oplus \operatorname{Ker} p$ et l'équivalence entre **(1)**, **(2)** et **(3)** résulte de la propriété 19.

Définition 30

Symétrie orthogonale

Une symétrie s est **orthogonale** quand le projecteur ✎(45) $p = \dfrac{1}{2}(s + \mathrm{Id}_E)$ est orthogonal.

✎(45) Projecteur associé.

Conséquence

À une décomposition de E en somme directe orthogonale : $E = F \oplus F^\perp$, on peut associer deux projecteurs orthogonaux et donc deux symétries orthogonales.

p_F : projection d'image F et de noyau $F^\perp$;

$p_{F^\perp}$: projection d'image $F^\perp$ et de noyau F ;

s_F : symétrie orthogonale par rapport à F : $s_F = 2p_F - \mathrm{Id}_E$;

$s_{F^\perp}$: symétrie orthogonale par rapport à $F^\perp$: $s_{F^\perp} = 2p_{F^\perp} - \mathrm{Id}_E = \mathrm{Id}_E - 2p_F$.

Définition 31

Une **réflexion** est une symétrie orthogonale par rapport à un hyperplan H de E.

Propriété 23

Soit p un projecteur de E. Les propositions suivantes sont équivalentes :

(1) p est un projecteur orthogonal ;

(2) $\forall (x, y) \in E^2, \langle p(x) \mid y \rangle = \langle x \mid p(y) \rangle$;

(3) $\forall x \in E, \|p(x)\| \leqslant \|x\|$.

Copyrighted material

☞ **(1) ⇒ (2)**

p étant projecteur orthogonal, on a :

$$\langle x \mid p(y)\rangle = \langle x - p(x) \mid p(y)\rangle + \langle p(x) \mid p(y)\rangle = \langle p(x) \mid p(y)\rangle$$

car $x - p(x) \in \operatorname{Ker} p = (\operatorname{Im} p)^{\perp}$ et $p(y) \in \operatorname{Im} p$; de même $\langle p(x) \mid y\rangle = \langle p(x) \mid p(y)\rangle$.

(2) ⇒ (3)

On applique **(2)** avec $y = p(x)$, ce qui donne alors $p(y) = p^2(x) = p(x)$.

Il vient $\| p(x)\|^2 = \langle x \mid p(x)\rangle$, donc, d'après l'inégalité de Cauchy–Schwarz :

$$\| p(x)\|^2 \leqslant \| x\| \, \| p(x)\|,$$

et pour $p(x) \neq 0$, par simplification par $\| p(x)\|$, on obtient :

$$\| p(x)\| \leqslant \| x\|.$$

Pour $p(x) = 0$, cette inégalité est encore vérifiée.

(3) ⇒ (1)

Supposons que le projecteur p ne soit pas orthogonal, il existe alors $x \in \operatorname{Im} p$ et $y \in \operatorname{Ker} p$ tels que $\langle x \mid y\rangle \neq 0$, donc $x \neq 0$ et $y \neq 0$.

Avec $\lambda = -\dfrac{\langle y \mid x\rangle}{\| y\|^2}$, on obtient $\langle y \mid x + \lambda y\rangle = 0$ et $\lambda \neq 0$, puis, d'après le théorème de Pythagore : $\| x\|^2 = \| x + \lambda y\|^2 + |\lambda|^2 \| y\|^2$ donc $\| x\| > \| x + \lambda y\|$.

Cette dernière inégalité est en contradiction avec **(3)** car $p(x + \lambda y) = p(x) = x$.

Propriété 24

Soit s une symétrie de E. Les propositions suivantes sont équivalentes :

(1) s est une symétrie orthogonale ;

(2) $\forall (x, y) \in E^2, \langle x \mid s(y)\rangle = \langle s(x) \mid y\rangle$;

(3) $\forall x \in E, \| s(x)\| = \| x\|$.

☞ **(1) ⇒ (2)**

Le projecteur p associé à s [46] étant orthogonal, il vient :

$$\langle x \mid p(y)\rangle = \langle p(x) \mid y\rangle$$

donc $\langle x \mid s(y)\rangle = 2\langle x \mid p(y)\rangle - \langle x \mid y\rangle = 2\langle p(x) \mid y\rangle - \langle x \mid y\rangle = \langle s(x) \mid y\rangle$.

(2) ⇒ (3)

On applique **(2)** avec $y = s(x)$ [47] et il vient $\langle x \mid x\rangle = \langle s(x) \mid s(x)\rangle$.

(3) ⇒ (1)

On reprend la démonstration **(3) ⇒ (1)** de la propriété 23. Alors $s(x + \lambda y) = x - \lambda y$, puis [48] $\| x - \lambda y\|^2 = \| x + \lambda y\|^2 + 4\,|\lambda|^2 \| y\|^2$ donc $\| x - \lambda y\| \neq \| x + \lambda y\|$ ce qui est en contradiction avec **(3)**.

[46] $s = 2p - \mathrm{Id}_E$.

[47] Donc $s(y) = x$.

[48] Théorème de Pythagore.

Interprétation géométrique dans un espace préhilbertien réel

Tout se passe dans le plan $\operatorname{Vect}(x, y)$, on est ainsi ramené à un problème de géométrie plane.

Le choix de λ fait apparaître deux triangles rectangles.

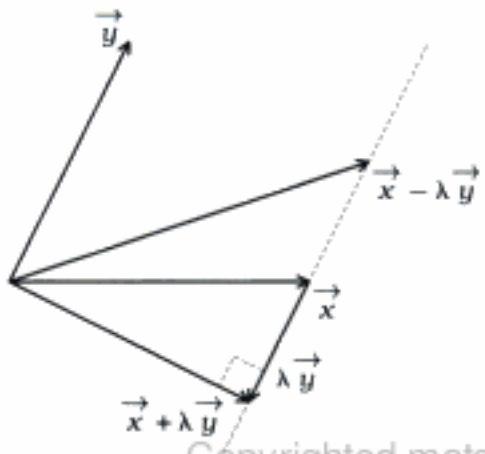
Dans chacun de ces triangles, la longueur de l'hypoténuse est strictement supérieure à la longueur d'un côté de l'angle droit.

Pour la propriété 23, cela donne :

$$\| x\| > \| x + \lambda y\|$$

et, pour la propriété 24 :

$$\| x - \lambda y\| > \| x + \lambda y\|.$$



Copyrighted material

Théorème 23

Distance d'un vecteur à un sous-espace

Soit $x \in E$ et F un sous-espace vectoriel de E :

a) l'ensemble $\{y \in F \,/\, d(x,F) = \|x-y\|\}$ a au plus un élément ;

b) soit $x_0 \in F$, on a $d(x,F) = \|x-x_0\|$ si et seulement si $x - x_0 \in F^\perp$;

c) si F admet un supplémentaire orthogonal, ce qui est le cas lorsque F est de dimension finie, on a $d(x,F) = \|x - p_F(x)\|$ où p_F est la projection orthogonale sur F.

Rappelons que E étant un espace vectoriel normé, pour tout x de E et toute partie non vide A de E, la distance de x à A est $d(x,A) = \inf\{\|x-y\| \,/\, y \in A\}$.

a) Soit y et z dans F tels que $\|x-y\| = \|x-z\| = d(x,F)$.
L'identité du parallélogramme appliquée aux vecteurs $x-y$ et $x-z$ donne :

$$\|2x-y-z\|^2 + \|y-z\|^2 = 2\|x-y\|^2 + 2\|x-z\|^2$$

d'où $\|y-z\|^2 = 4d(x,F)^2 - 4\left\|x - \frac{y+z}{2}\right\|^2$.

Puisque F est un sous-espace vectoriel de E, on a $\frac{y+z}{2} \in F$ donc $\left\|x - \frac{y+z}{2}\right\| \geqslant d(x,F)$ et avec l'égalité précédente il vient $\|y-z\|^2 \leqslant 0$, d'où enfin $y = z$. (49)

(49) On peut remarquer que cette démonstration reste valable dans le cas où F est seulement supposé être un convexe de E.

b) ▪ Supposons $x - x_0 \in F^\perp$.
Alors, pour tout y de F, $\|x-y\|^2 = \|x-x_0\|^2 + \|x_0-y\|^2$, (50) donc $\|x-y\| \geqslant \|x-x_0\|$.
Il en résulte $d(x,F) = \|x-x_0\|$.
▪ Supposons $d(x,F) = \|x-x_0\|$.

Si $x - x_0 \notin F^\perp$, il existe $y \in F$ tel que $\langle x-x_0 \,|\, y\rangle \neq 0$ et, en posant $\lambda = \frac{\langle y \,|\, x-x_0\rangle}{\|y\|^2}$, on obtient $\langle y \,|\, x - x_0 - \lambda y\rangle = 0$.

(50) Théorème de Pythagore.

Avec le théorème de Pythagore, il vient $\|x-(x_0+\lambda y)\|^2 = \|x-x_0\|^2 - |\lambda|^2\|y\|^2$ donc :

$$\|x-(x_0+\lambda y)\| < \|x-x_0\| \quad \text{car} \quad |\lambda| \neq 0.$$

Cette dernière inégalité est en contradiction avec :

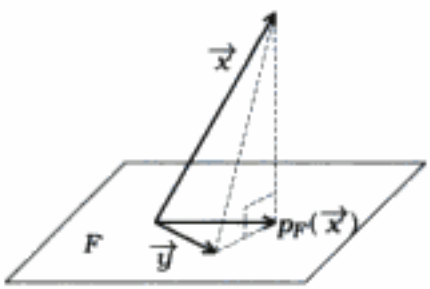
$$\|x-x_0\| = d(x,F) = \inf\{\|x-z\| / z \in F\} \quad \text{et} \quad x_0 + \lambda y \in F$$

en conséquence, on a $x - x_0 \in F^\perp$.

Interprétation géométrique

Si $\vec{y} \neq p_F(\vec{x})$, dans le triangle rectangle la longueur de l'hypothénuse est strictement supérieure à la longueur d'un côté de l'angle droit :

$$\|\vec{x} - \vec{y}\| > \|\vec{x} - p_F(\vec{x})\|.$$



Exemple 18 Distance d'un vecteur à un hyperplan

Soit $a \in E \setminus \{0_E\}$ dans E, D la droite $\mathbb{K}a$ et H l'hyperplan orthogonal de a.

Écrire les expressions de $d(x,D)$ et $d(x,H)$ en fonction de $\|x\|$ et $\langle a \,|\, x\rangle$.

On a ici $E = D \oplus H$, $H = D^\perp$, $p_D(x) = \frac{\langle a \,|\, x\rangle}{\|a\|^2} a$, $p_H(x) = x - \frac{\langle a \,|\, x\rangle}{\|a\|^2} a$

$d(x,H) = \|x - p_H(x)\| = \|p_D(x)\|$ donc $d(x,H) = \frac{|\langle a \,|\, x\rangle|}{\|a\|}$

$d(x,D) = \|x - p_D(x)\| = \|p_H(x)\|$, or d'après le théorème de Pythagore :

$\|x\|^2 = \|p_D(x)\|^2 + \|p_H(x)\|^2$ donc $d(x,D)^2 = \|x\|^2 - \frac{|\langle a \,|\, x\rangle|^2}{\|a\|^2}$.

Copyrighted material

Exemple 19 Expression analytique de la distance d'un vecteur x à un sous-espace F de dimension finie et à son orthogonal

Soit F un sous-espace de dimension finie $n \geqslant 1$, et $(u_i)_{1\leqslant i\leqslant n}$ une base orthonormale de F.

On exprime $d(x, F)$ et $d(x, F^\perp)$ en fonction de $\|x\|$ et des produits scalaires $\langle u_i \mid x\rangle$.

On a $p_F(x) = \sum_{i=1}^{n} \langle u_i \mid x\rangle u_i$, $p_{F^\perp}(x) = x - \sum_{i=1}^{n} \langle u_i \mid x\rangle u_i$.

$d(x, F^\perp) = \|x - p_{F^\perp}(x)\| = \|p_F(x)\|$ donc $d(x, F^\perp)^2 = \sum_{i=1}^{n} |\langle u_i \mid x\rangle|^2$

$d(x, F) = \|x - p_F(x)\| = \|p_{F^\perp}(x)\|$, or, d'après le théorème de Pythagore :

$\|x\|^2 = \|p_{F^\perp}(x)\|^2 + \|p_F(x)\|^2$ donc $d(x, F)^2 = \|x\|^2 - \sum_{i=1}^{n} |\langle u_i \mid x\rangle|^2$.

4. Matrice d'un produit scalaire (dimension finie)

L'espace préhilbertien $(E, \langle \cdot \mid \cdot \rangle)$ est maintenant supposé de dimension finie $n \geqslant 1$.

Définition 32

Soit $\mathcal{B} = (e_i)_{1\leqslant i\leqslant n}$ une base de E, la matrice [51] du produit scalaire $\varphi : (x, y) \mapsto \langle x \mid y\rangle$ est la matrice $A \in \mathcal{M}_n(\mathbb{K})$ de terme général $a_{ij} = \langle e_i \mid e_j\rangle$.

On note $\mathrm{mat}_{\mathcal{B}}\,\varphi = [\langle e_i \mid e_j\rangle]$. [52]

[51] Dans la base $\mathcal{B}$.

[52] Dans le cas euclidien : $\mathbb{K} = \mathbb{R}$, on retrouve la matrice d'une forme bilinéaire (voir définition 2).

Propriété 25

Soit $A = \mathrm{mat}_{\mathcal{B}}\,\varphi$.

- Si $\mathbb{K} = \mathbb{R}$, [53] alors $A = {}^tA$: A est **symétrique réelle**.
- Si $\mathbb{K} = \mathbb{C}$, [54] alors $A = {}^t\overline{A}$: la matrice A est égale à sa transconjuguée. On dit que c'est une **matrice hermitienne**.

[53] Produit scalaire euclidien.

[54] Produit scalaire hermitien.

Propriété 26

$\mathcal{B} = (e_i)_{1\leqslant i\leqslant n}$ est une base orthonormale si et seulement si $\mathrm{mat}_{\mathcal{B}}\,\varphi = I_n$.

Propriété 27

Écriture matricielle du produit scalaire

Aux vecteurs $x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{j=1}^{n} y_j e_j$, on associe leurs matrices :

$X = [x_i] \in \mathcal{M}_{n,1}(\mathbb{K})$ et $Y = [y_j] \in \mathcal{M}_{n,1}(\mathbb{K})$ dans la base $\mathcal{B}$.

a) Cas euclidien : $A = \mathrm{mat}_{\mathcal{B}}\,\varphi \iff \forall (x, y) \in E^2, \langle x \mid y\rangle = {}^tXAY$.

b) Cas hermitien : $A = \mathrm{mat}_{\mathcal{B}}\,\varphi \iff \forall (x, y) \in E^2, \langle x \mid y\rangle = {}^t\overline{X}AY$.

Démontrons b).

On pose $A = [a_{ij}]$.

$\langle x \mid y\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{x}_i y_j \langle e_i \mid e_j\rangle$ donc si $A = \mathrm{mat}_{\mathcal{B}}\,\varphi$, $\langle x \mid y\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} \overline{x}_i y_j a_{ij} = {}^t\overline{X}AY$.

Réciproquement, si $\forall (x, y) \in E^2, \langle x \mid y\rangle = {}^t\overline{X}AY$ alors, en appliquant cette égalité avec $x = e_i$ et $y = e_j$, on obtient $a_{ij} = \langle e_i \mid e_j\rangle$.

Copyrighted material

Propriété 28

Changement de base

Soit $\mathfrak{B} = (e_i)_{1 \leqslant i \leqslant n}$ et $\mathfrak{B}' = (e'_i)_{1 \leqslant i \leqslant n}$ deux bases de E, P la matrice de passage de $\mathfrak{B}$ à $\mathfrak{B}'$:

$$P = \mathrm{mat}_{\mathfrak{B}}(e'_1, \ldots, e'_n).$$

On pose $A = \mathrm{mat}_{\mathfrak{B}} \varphi$ et $A' = \mathrm{mat}_{\mathfrak{B}'} \varphi$.

a) Cas euclidien : $A' = {}^tPAP$.

b) Cas hermitien : $A' = {}^t\overline{P}AP$.

(55) Le cas a) est réglé par la propriété 6.

Démontrons b). (55)

Pour tout $(x, y) \in E^2$, soit $X = \mathrm{mat}_{\mathfrak{B}}(x)$, $X' = \mathrm{mat}_{\mathfrak{B}'}(x)$, $Y = \mathrm{mat}_{\mathfrak{B}}(y)$, $Y' = \mathrm{mat}_{\mathfrak{B}'}(y)$ on a alors $X = PX'$, $Y = PY'$, donc :

$$\forall (x, y) \in E^2, \langle x \mid y \rangle = {}^t\overline{X}AY = {}^t\left(\overline{PX'}\right)A\left(PY'\right) \quad . \quad \langle x \mid y \rangle = {}^t\overline{X'}\left({}^t\overline{P}AP\right)Y'$$

et, d'après la propriété 27 b), $A' = {}^t\overline{P}AP$

Propriété 29

Si $A \in \mathcal{M}_n(\mathbb{K})$ est la matrice d'un produit scalaire, on a :

$$A \in \mathrm{GL}_n(\mathbb{K}) \quad \text{et} \quad \det A > 0.$$

D'après le théorème 15, il existe au moins une base orthonormale, donc il existe $P \in \mathrm{GL}_n(\mathbb{K})$ tel que :

$${}^tPAP = I_n \text{ (cas euclidien) ou } {}^t\overline{P}AP = I_n \text{ (cas hermitien)}$$

d'où on déduit $\det A = \dfrac{1}{(\det P)^2}$ (cas euclidien).

ou $\det A = \dfrac{1}{|\det P|^2}$ (cas hermitien).

Exemple 20 La matrice $A \in \mathcal{M}_n(\mathbb{R})$ de terme général $a_{ij} = \dfrac{1}{i+j+1}$, $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant n-1$, est inversible et $\det A > 0$.

Il suffit d'interpréter A comme la matrice d'un produit scalaire euclidien.

On remarque que pour tout $(i, j) \in \mathbb{N}^2$:

$$\frac{1}{i+j+1} = \int_0^1 x^{i+j} \mathrm{d}x.$$

Introduisons donc l'espace vectoriel $E = \mathbb{R}_{n-1}[X]$ muni du produit scalaire défini par :

$$\forall (P, Q) \in E^2, \quad \langle P \mid Q \rangle = \int_0^1 P(x)\,Q(x) \mathrm{d}x.$$

A est la matrice de ce produit scalaire sur la base canonique, donc A est inversible avec $\det A > 0$.

Copyrighted material

L'essentiel

I. Formes quadratiques positives

E désigne un $\mathbb{R}$-espace vectoriel de dimension finie n.

✔ **Si l'on veut** montrer qu'une forme quadratique q sur E est positive,

- **on peut** si M est une matrice de q, prouver que :
$$\forall X \in \mathcal{M}_{n,1}(\mathbb{R}),\ {}^tXMX \geqslant 0.$$
→ Voir *Mise en œuvre*, exercice 1

✔ **Si l'on veut** sachant que la forme quadratique q est positive, montrer qu'elle est définie,

- **on peut** si M est une matrice de q, vérifier que M est inversible.
→ Voir *Mise en œuvre*, exercice 1

✔ **Si l'on veut** traduire qu'une forme quadratique est définie-positive,

- **on peut** écrire qu'il existe une base de E sur laquelle la matrice de q est I_n.
→ Voir *Mise en œuvre*, exercice 2

II. Espaces préhilbertiens réels

✔ **Si l'on veut** montrer qu'une famille finie est génératrice d'un espace préhilbertien réel,

- **on peut** vérifier que l'orthogonal du sous-espace qu'elle engendre est réduit au vecteur nul.
→ Voir *Mise en œuvre*, exercice 3

✔ **Si l'on veut** montrer qu'une famille finie est libre,

- **on peut** remarquer qu'il est suffisant qu'elle soit orthonormale.
→ Voir *Mise en œuvre*, exercice 3

✔ **Si l'on veut** travailler dans une base orthonormale plutôt que dans une base donnée,

- **on peut** introduire une base orthonormale donnée par la méthode de Gram-Schmidt. (Souvent son existence suffit, sans avoir besoin de la construire explicitement.)
→ Voir *Mise en œuvre*, exercice 4

✔ **Si l'on veut** déterminer le projeté orthogonal d'un vecteur x sur un sous-espace F de dimension finie rapporté à une base quelconque $(f_i)_{1 \leqslant i \leqslant p}$,

- **on peut** rechercher le vecteur y de F tel que $\forall i \in [\![1, p]\!],\ \langle x - y \,|\, f_i \rangle = 0$.
→ Voir *Mise en œuvre*, exercice 5

✔ **Si l'on veut** déterminer le minimum d'un polynôme quadratique de n variables réelles $a_1, \ldots, a_n$,

- **on peut** essayer d'interpréter ce minimum au moyen de la distance d'un vecteur x à un sous-espace F de dimension finie, dans un espace préhilbertien E bien choisi.
→ Voir *Mise en œuvre*, exercice 6

Méthodes

III. Espaces préhilbertiens complexes

✔ Les résultats plus familiers pour un produit scalaire euclidien restent vrais pour un produit scalaire hermitien.

Toutefois, les moyens utilisés diffèrent en intermédiaires de calcul, principalement :

$\langle v \mid u \rangle = \overline{\langle u \mid v \rangle}$, $\langle \alpha u \mid v \rangle = \overline{\alpha} \langle u \mid v \rangle$.

$\| (u+v) \|^2 = \| u \|^2 + 2 \operatorname{Re} \langle u \mid v \rangle + \| v \|^2$,

$\| \alpha u \|^2 = \alpha\overline{\alpha} \| u \|^2$,

$\| (u+iv) \|^2 = \| u \|^2 - 2 \operatorname{Im} \langle u \mid v \rangle + \| v \|^2$.

→ Voir *Mise en œuvre*, exercice 7

✔ **Si l'on veut** calculer la norme (hermitienne) d'un vecteur u,

▪ **on peut** utiliser ses coordonnées (a_k) dans une base orthonormale $(e_k)_{k \in \mathbb{N}}$.

✔ La norme de u a pour carré $\sum_{k \in \mathbb{N}} |a_k|^2$.

Attention à ne pas oublier le module des a_k !

→ Voir *Mise en œuvre*, exercice 8

Copyrighted material

Hidden page

Hidden page

Hidden page

Hidden page

on en déduit l'intégrabilité avec le critère de domination.
Il est clair que φ est bilinéaire symétrique.

Si $P \in E \setminus \{0\}$, la fonction $x \mapsto P^2(x)e^{-x}$ est continue, positive, donc $\int_0^1 P^2(x)e^{-x}\mathrm{d}x > 0$ et on obtient *a fortiori* $\varphi(P,P) > 0$.

et non identiquement nulle sur $[0,1]$.

$\varphi(P,P) \geqslant \int_0^1 P^2(x)e^{-x}\mathrm{d}x$.

2) $P = a + bX + cX^2$ est le projeté orthogonal de X^3 sur $F = \mathbb{R}_2[X]$ si et seulement si $X^3 - P \in F^\perp$.
Le triplet (a, b, c) est donc défini par le système :

C'est-à-dire si et seulement si $X^3 - P$ est orthogonal à 1, à X et à X^2.

$$\begin{array}{rcrcrcl} a\langle 1 \mid 1\rangle & + & b\langle X \mid 1\rangle & + & c\langle X^2 \mid 1\rangle & = & \langle X^3 \mid 1\rangle \\ a\langle 1 \mid X\rangle & + & b\langle X \mid X\rangle & + & c\langle X^2 \mid X\rangle & = & \langle X^3 \mid X\rangle \\ a\langle 1 \mid X^2\rangle & + & b\langle X \mid X^2\rangle & + & c\langle X^2 \mid X^2\rangle & = & \langle X^3 \mid X^2\rangle \end{array}$$

$\forall n \in \mathbb{N}$, $\int_0^{+\infty} x^n e^{-x}\mathrm{d}x = n!$ donne :

$$\forall (n,p) \in \mathbb{N}^2,\ \left\langle X^n \,\middle|\, X^p \right\rangle = (n+p)!.$$

Un calcul auxiliaire usuel.

Le système s'écrit alors :

$$\begin{cases} a + b + 2c = 6 \\ a + 2b + 6c = 24 \\ 2a + 6b + 24c = 120 \end{cases}$$

$$\begin{cases} a + b + 2c = 6 \\ b + 4c = 18 \\ 2b + 10c = 54 \end{cases} \quad \begin{cases} a + b + 2c = 6 \\ b + 4c = 18 \\ 2c = 18 \end{cases}$$

Systèmes équivalents obtenus par la méthode du pivot de Gauss.

On en déduit $c = 9$, $b = -18$, $a = 6$.
Le projeté orthogonal de X^3 sur $\mathbb{R}_2[X]$ est donc $P = 6 - 18X + 9X^2$.

Ex. 6

Calculer $\lambda = \inf_{(a,b,c)\in\mathbb{R}^3} \int_0^{+\infty} \left(x^3 + ax^2 + bx + c\right)^2 e^{-x}\mathrm{d}x$.

Indications

Dans l'exercice précédent, a vu que $(P,Q) \mapsto \int_0^{+\infty} P(x)Q(x)e^{-x}\mathrm{d}x$ est un produit scalaire sur $\mathbb{R}_3[X]$.

Le projeté orthogonal de X^3 sur $\mathbb{R}_2[X]$ est $P_0 = 9X^2 - 18X + 6$.

Il s'agit ici de calculer $\inf_{P\in\mathbb{R}_2[X]} \| X^3 - P \|^2$ $\left(P = -aX^2 - bX - c \text{ décrit } \mathbb{R}_2[X]\right)$.

Solution

$\lambda = d\left(X^3, \mathbb{R}_2[X]\right)^2 = \| X^3 - P_0 \|^2$.

D'après le théorème de Pythagore, on a aussi :

$$\| X^3 - P_0 \|^2 = \| X^3 \|^2 - \| P_0 \|^2.$$

Donc, avec $P_0^2 = 81X^4 - 324X^3 + 432X^2 - 216X + 36$, compte tenu de $\int_0^{+\infty} x^n e^{-x}\mathrm{d}x = n!$, on obtient :

$$\left\| X^3 - P_0 \right\|^2 = 6! - 81 \cdot 4! + 324 \cdot 3! - 432 \cdot 2! + 216 \cdot 1! - 36 \cdot 0!$$

On conclut alors $\lambda = 36$.

Commentaires

P_0 projeté orthogonal de X^3 sur $\mathbb{R}_2[X]$.

Car $P_0 \perp X^3 - P_0$.

Calcul désagréable mais facile.

III. Espaces préhilbertiens complexes

Ex. 7

Similitudes

Soit E un espace vectoriel hermitien. $f \in \mathscr{L}(E)$ est appelé une similitude quand il existe λ réel, $\lambda > 0$, tel que :

$$\forall x \in E,\ \|f(x)\| = \lambda \|x\|. \qquad (1)$$

1) Montrer que la condition **(1)** équivaut à :

$$\forall (x, y) \in E^2,\ \langle f(x) \,|\, f(y)\rangle = \lambda^2 \langle x \,|\, y\rangle. \qquad (2)$$

2) Montrer que, si E est de dimension finie, alors l'ensemble des similitudes est un sous-groupe de $\mathrm{GL}(E)$.

Donner un contre-exemple si E n'est pas de dimension finie.

Indications

Les similitudes d'un espace vectoriel réel sont plus familières.

Une importante différence de calcul est $\langle x \,|\, y\rangle = \overline{\langle y \,|\, x\rangle}$ au lieu de la symétrie dans le cas réel.

Solution

1) L'implication **(2)** $\Rightarrow$ **(1)** est banale en tenant compte de $\lambda > 0$.

Pour la réciproque, formons $\|f(x+y)\|^2$. Il vient :

$$\|f(x+y)\|^2 = \|f(x)\|^2 + 2\,\mathrm{Re}\,\langle f(x) \,|\, f(y)\rangle + \|f(y)\|^2.$$

Avec $\|f(x+y)\|^2 = \lambda^2 \|x+y\|^2$, il vient :

$$\|f(x+y)\|^2 = \lambda^2 \left(\|x\|^2 + 2\,\mathrm{Re}\,\langle x \,|\, y\rangle + \|y\|^2\right).$$

On en déduit $\mathrm{Re}\,\langle f(x) \,|\, f(y)\rangle = \lambda^2\,\mathrm{Re}\,\langle x \,|\, y\rangle$.

De même, en développant $\|f(x+iy)\|^2$ et $\lambda^2\|x+iy\|^2$, il vient :

$$\mathrm{Im}\,\langle f(x) \,|\, f(y)\rangle = \lambda^2\,\mathrm{Im}\,\langle x \,|\, y\rangle,\ \text{puis}\ \langle f(x) \,|\, f(y)\rangle = \lambda^2 \langle x \,|\, y\rangle.$$

2) Injectivité : $f(x) = 0 \Rightarrow \|f(x)\| = 0 \Rightarrow \lambda\|x\| = 0 \Rightarrow x = 0$.

En dimension finie, une similitude est alors bijective.

Si f, g sont des similitudes de rapports λ, μ dans $\mathbb{R}_+^*$, alors :

$$\forall x \in E,\ \|(f \circ g)(x)\| = \|f\big(g(x)\big)\| = \lambda\|g(x)\| = \lambda\,\mu\,\|x\|,$$

donc $f \circ g$ est une similitude de rapport $\lambda\mu$.

Pour tout $x \in E$,

$$\|f\big(f^{-1}(x)\big)\| = \lambda\|f^{-1}(x)\| \ \Rightarrow\ \|f^{-1}(x)\| = \frac{1}{\lambda}\|x\|,$$

donc f^{-1} est une similitude de rapport $\dfrac{1}{\lambda}$.

▪ **Contre-exemple** hors dimension finie.

En exemple 14 du cours, nous avons installé l'espace préhilbertien complexe E des suites de carré sommable.

À $(u_n)_{n\in\mathbb{N}}$, on associe $(v_n)_{n\in\mathbb{N}}$: $v_0 = 0$ et, $\forall n \in \mathbb{N}^*$, $v_n = u_{n-1}$.

$f : E \to E$ ainsi définie n'est évidemment pas surjective.

$\sum_{n\in\mathbb{N}} u_n^2 = \sum_{n\in\mathbb{N}} v_n^2$ donne $\|f(u)\| = \|u\|$.

f est alors une isométrie non surjective.

Commentaires

Il suffit de prendre $y = x$.

Avec $f(x+y) = f(x)+f(y)$.

$\|u+v\|^2 = \|u\|^2 + 2\,\mathrm{Re}\,(u \,|\, v) + \|v\|^2$.

$\|u+iv\|^2 = \|u\|^2 - 2\,\mathrm{Im}\,(u \,|\, v) + \|v\|^2$.

Égalité des parties réelles et imaginaires.

Tout le traitement de cette deuxième partie ne présente aucune différence formelle avec les similitudes en espace préhilbertien réel.

f est bijective.

À l'analogue des suites réelles de même type vu en exemple 13.

La suite $(\delta_{0,n})$ n'a pas d'antécédent.

$u = (u_n)_{n\in\mathbb{N}}$.

Similitude de rapport 1.

Copyrighted material

Ex. 8

Soit $n \in \mathbb{N}^*$ et Φ l'application de $\mathbb{C}_n[X]^2$ dans $\mathbb{C}$ définie par $\Phi(P, Q) = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \overline{P(e^{i\theta})}\,Q(e^{i\theta})\,d\theta$.

1) Montrer que Φ est un produit scalaire hermitien et que la base canonique de $\mathbb{C}_n[X]$ est orthonormale.

2) Étant donné $Q = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{C}_n[X]$, calculer $\|Q\|^2$.

Soit $M = \sup_{|z|=1} |Q(z)|$. Montrer que $M \geqslant 1$.

Déterminer les polynômes Q tels que $M = 1$.

Indications

La première partie est voisine de l'exemple 16 du cours.

La calcul d'une norme est aisé avec les coordonnées dans une base orthonormale.

Solution

1) $\displaystyle\int_0^{2\pi} f\bar{g}$ est conjugué de $\displaystyle\int_0^{2\pi} \bar{f}g$, donc $\Phi(Q, P) = \overline{\Phi(P, Q)}$.

La linéarité de l'intégrale montre facilement que Φ est semi-linéaire à gauche et linéaire à droite.

$\Phi(P, P) = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} \left|P(e^{i\theta})\right| d\theta$ est un réel positif.

$\Phi(P, P) = 0$ implique $|P(z)| = 0$, donc $P(z) = 0$ pour tout z de module 1, c'est-à-dire $P = 0$.

En conclusion, Φ est un produit scalaire hermitien.

Soit r, s dans $[\![0, n]\!]$. Alors :

$$\Phi(X^r, X^s) = \frac{1}{2\pi}\int_0^{2\pi} e^{i(-r+s)\theta}\,d\theta.$$

On a donc $\|X^r\|^2 = \dfrac{1}{2\pi}\displaystyle\int_0^{2\pi} d\theta = 1$, et, pour $r \neq s$,

$$\langle X^r \mid X^s \rangle = \frac{1}{2\pi}\frac{1}{i(-r+s)}\left[e^{i(-r+s)\theta}\right]_0^{2\pi} = 0.$$

La base canonique est donc orthonormale.

2) On a $\|Q\|^2 = 1 + \displaystyle\sum_{k=1}^{n} |a_k|^2$, donc $\|Q\| \geqslant 1$.

Pour avoir $M = 1$, il faut $\displaystyle\sum_{k=1}^{n} |a_k|^2 = 0$ donc $a_k = 0$ pour tout $k \in [\![1, n]\!]$, c'est-à-dire $Q = X^n$.

Commentaires

Symétrie hermitienne.

Φ est sesquilinéaire.

Positivité de l'intégrale.

Puisque P admet une infinité de racines.

$s = r$. Les vecteurs de la base canonique sont normés.

On a déjà vu que $\|X^n\| = 1$.

Copyrighted mat

Exercices

Niveau 1

Ex. 1

Soit φ une forme bilinéaire symétrique non dégénérée sur un $\mathbb{R}$-espace vectoriel E de dimension n. Soit f une application surjective de E sur E telle que :

$$\forall (x, y) \in E^2,\ \varphi\big(f(x), f(y)\big) = \varphi(x, y).$$

Montrer que f est un automorphisme de E.

Ex. 2

Dans $\mathbb{R}^n$ rapporté à sa base canonique, déterminer le rang de la forme quadratique :

$$q(x) = \sum_{1 \leqslant i \leqslant j \leqslant n} (x_i - x_j)^2.$$

Ex. 3

Soit n un entier naturel non nul.

Trouver les réels $x_1, x_2, \ldots, x_n$ tels que :

$$\begin{aligned} x_1 &+ x_2 &+ \cdots &+ x_n &= n \\ x_1^2 &+ x_2^2 &+ \cdots &+ x_n^2 &= n \end{aligned}$$

Ex. 4

Soit $A = [a_{k\ell}] \in \mathcal{M}_n(\mathbb{R})$ avec :

$$a_{k\ell} = \int_0^{\frac{\pi}{2}} \sin kx \sin \ell x \, dx.$$

Montrer que $\det A > 0$.

Ex. 5

Soit $A = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$ avec :

$$a^2 + b^2 + c^2 = 1.$$

1) Montrer que $|\det A| \leqslant 1$.

2) Étudier les cas d'égalité.

Ex. 6

Dans $\mathbb{R}^4$ euclidien canonique, former la matrice par rapport à la base canonique $\mathcal{B}$ de la symétrie orthogonale par rapport au plan H d'équations :

$$x_1 + x_2 - x_3 - x_4 = 0,\ x_1 + 3x_2 + x_3 - x_4 = 0.$$

Niveau 2

Ex. 7

Soit E un $\mathbb{R}$-espace vectoriel et f une forme bilinéaire sur E^2 telle que :

$$\forall (x, y) \in E^2,\ f(x, y) = 0 \ \Rightarrow\ f(y, x) = 0. \qquad (1)$$

Montrer que f est symétrique ou antisymétrique.

Ex. 8

Soit q une forme quadratique définie positive sur $\mathbb{R}^n$ dont la matrice dans la base canonique de $\mathbb{R}^n$ est $A = [a_{ij}]$ et soit q' la forme quadratique de $\mathbb{R}^{n-1}$ définie sur la base canonique de $\mathbb{R}^{n-1}$ par :

$$q'(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} x_i x_j \begin{vmatrix} a_{ni} & a_{nj} \\ a_{nj} & a_{ij} \end{vmatrix}$$

Montrer que q' est définie positive.

Ex. 9

Soit $E = \mathbb{R}_2[X]$ muni de sa structure euclidienne canonique, et $\mathcal{C}$ l'ensemble des polynômes $P \in E$ scindés dans $\mathbb{R}$.

1) Montrer que $\mathcal{C}$ est un cône fermé de E.

2) Calculer la distance de $A = X^2 + 1$ à $\mathcal{C}$.

Ex. 10

Soit E un espace préhilbertien et F un sous-ensemble non vide de E convexe et complet.

1) Montrer que, pour tout a de E, il existe $b \in F$, unique, tel que : $d(a, F) = \| b - a \|$.

2) En déduire que, si F est un sous-espace vectoriel complet de E, $E = F \oplus F^{\perp}$.

Copyrighted material

Ex. 11

Polynômes de Legendre

Soit E le $\mathbb{R}$-espace vectoriel $\mathcal{C}^0([-1,1],\mathbb{R})$ muni du produit scalaire $\langle \cdot \mid \cdot \rangle : E^2 \to \mathbb{R}, (f,g) \mapsto \displaystyle\int_{-1}^{1} fg$.

1) a) Montrer qu'il existe une suite $(P_n)_{n\in\mathbb{N}}$ de polynômes vérifiant :

(1) $\forall n \in \mathbb{N}, \deg P_n = n$

(2) $\forall (i,j) \in \mathbb{N}^2, i \neq j \Rightarrow \langle P_i \mid P_j \rangle = 0$.

b) Soit $n \in \mathbb{N}^*$, montrer que P_n a au moins une racine réelle sur $]-1,1[$.

On appelle $\alpha_1, \alpha_2, \cdots, \alpha_p$ les racines réelles distinctes de P_n appartenant à $]-1,1[$ et en lesquelles P_n change de signe. En considérant le produit scalaire de P_n et $(X-\alpha_1)\cdots(X-\alpha_p)$, montrer que $p = n$.

c) Montrer qu'il existe une suite unique $(L_n)_{n\in\mathbb{N}}$ de polynômes vérifiant :

(1) $\forall n \in \mathbb{N}, \deg L_n = n$

(2) $\forall (i,j) \in \mathbb{N}^2, i \neq j \Rightarrow \langle L_i \mid L_j \rangle = 0$

(3) $\forall n \in \mathbb{N}, L_n(1) = 1$.

2) Montrer que, pour $n \in \mathbb{N}$, fixé, il existe Q unique dans $\mathbb{R}[X]$ tel que :

$$\deg Q = 2n, \quad (X-1)^n \text{ divise } Q,$$
$$L_n = Q^{(n)} \text{ (dérivée } n^{\text{ème}}\text{)}.$$

3) En utilisant $\langle L_n \mid X^i \rangle = 0$ pour :

$$i \in \{0, 1, \cdots, n-1\}$$

montrer que $(X+1)^n$ divise Q.

En déduire qu'il existe $\mu \in \mathbb{R}$ tel que :

$$Q = \mu(X^2-1)^n.$$

Montrer que $\mu = \dfrac{2^{-n}}{n!}$.

Ex. 12

Soit E un espace préhilbertien.

Pour $(x_1, x_2, \cdots, x_n) \in E^n$, on note $G(x_1, \cdots, x_n)$ la matrice de terme général $a_{ij} = \langle x_i \mid x_j \rangle$. C'est la matrice de Gram du système $(x_1, x_2, \cdots, x_n)$.

$DG(x_1, \cdots, x_n) = \det G(x_1, \cdots, x_n)$ est le déterminant de Gram du système $(x_1, \cdots, x_n)$.

1) Montrer les équivalences :

a) $(x_1, \cdots, x_n)$ lié $\iff DG(x_1, \cdots, x_n) = 0$

b) $(x_1, \cdots, x_n)$ libre $\iff DG(x_1, \cdots, x_n) > 0$.

2) Montrer que :

a) $\forall \sigma \in \mathcal{S}_n$ (permutation de $[\![1, n]\!]$),

$DG(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = DG(x_1, \cdots, x_n)$.

b) Montrer que $DG(x_1, \cdots, x_n)$ est invariant lorsque l'on ajoute à l'un des x_i une combinaison linéaire des autres.

c) Calculer $DG(\lambda x_1, x_2, \cdots, x_n)$.

3) Soit $(x_1, x_2, \cdots, x_n)$ libre et p_H la projection orthogonale sur $H = \text{Vect}(x_1, x_2, \cdots, x_n)$. Montrer que $\forall x \in E$,

$$\| x - p_H(x) \|^2 = \frac{DG(x, x_1, x_2, \cdots, x_n)}{DG(x_1, x_2, \cdots, x_n)}.$$

Niveau 3

Ex. 13

Soit q une forme quadratique non dégénérée sur $\mathbb{R}^n$ et B sa forme polaire. On pose :

$$G = \{ f \in \mathcal{L}(\mathbb{R}^n) \mid \forall x \in \mathbb{R}^n, q(f(x)) = q(x) \}.$$

1) a) Montrer que pour $f \in \mathcal{L}(\mathbb{R}^n)$, f est élément de G si et seulement si :

$$\forall (x,y) \in \mathbb{R}^n \times \mathbb{R}^n, B(f(x), f(y)) = B(x,y).$$

b) Préciser la structure de $(G, \circ)$.

c) Quel est le déterminant d'un élément f de G ?

2) On prend $n = 4$, et sur la base canonique $(e_i)_{1\leqslant i\leqslant 4}$ de $\mathbb{R}^4$: $q(x) = x_1^2 + x_2^2 + x_3^2 - x_4^2$.

Soit $f \in G$ de matrice $A = [a_{ij}]$ sur la base (e_i).

a) Montrer que $a_{44}^2 \geqslant 1$.

Calculer f^{-1} en fonction des a_{ij}.

b) Soit f et $g \in G$, $A = \text{mat}_{(e_i)} f = [a_{ij}]$,

$B = \text{mat}_{(e_i)} g = [b_{ij}]$,

$C = \text{mat}_{(e_i)} f \circ g = [c_{ij}]$

Montrer que $a_{44} b_{44} \geqslant 0 \Rightarrow c_{44} \geqslant 0$.

Ex. 14

Soit $E = \mathcal{C}^2([0,1],\mathbb{R})$ l'espace vectoriel des applications de classe $\mathcal{C}^2$ de $[0,1]$ dans $\mathbb{R}$, et :

$$V = \{ f \in E \,/\, f(0) = -1, f(1) = 1 \}.$$

1) Montrer que V est un sous-espace affine non vide de E.

2) Montrer que $\varphi : (f,g) \mapsto f(0)\,g(0) + \displaystyle\int_0^1 f'$ est un produit scalaire sur E.

3) Pour tout $f \in E$, on pose :

$$I(f) = \int_0^1 f'^2(t)\,dt + 2\int_0^1 e^t f(t)\,dt.$$

Montrer qu'il existe $f_0 \in V$ tel que $I(f_0) = \inf\limits_{f\in V} I(f)$.

Calculer f_0 et $\min\limits_{f\in V} I(f)$.

Copyrighted material

Hidden page

Solutions des exercices

Niveau 1

Ex. 1

- Soit $(\lambda, x) \in \mathbb{R} \times E$. Montrons que $f(\lambda x) = \lambda f(x)$.

Par hypothèse, on a $\forall y \in E,\ \exists z \in E,\ y = f(z)$, donc :

$$\forall y \in E,\ \varphi\big(f(\lambda x), y\big) = \varphi\big(f(\lambda x), f(z)\big) = \varphi(\lambda x, z) = \lambda\, \varphi\,(x, z).$$

Or, on a aussi $\varphi\big(f(x), y\big) = \varphi\big(f(x), f(z)\big) = \varphi(x, z)$, d'où :

$$\forall y \in E,\ \varphi\big(f(\lambda x), y\big) = \lambda\, \varphi\,\big(f(x), y\big) \quad \text{soit} \quad \forall y \in E,\ \varphi\big(f(\lambda x) - \lambda f(x), y\big) = 0.$$

φ étant non dégénérée, son noyau est nul et on en conclut que : $f(\lambda x) = \lambda f(x)$.

- Soit $\left(x, x'\right) \in E^2$, on a, avec les mêmes notations que ci-dessus :

$$\begin{aligned}\forall y \in E,\ \varphi\big(f\left(x + x'\right), y\big) &= \varphi\big(f\left(x + x'\right), f(z)\big) = \varphi\left(x + x', z\right)\\ &= \varphi(x, z) + \varphi\left(x', z\right)\\ &= \varphi\big(f(x), y\big) + \varphi\big(f\left(x'\right), y\big)\end{aligned}$$

donc $\forall y \in E,\ \varphi\big(f\left(x + x'\right) - f(x) - f\left(x'\right), y\big) = 0$, et φ étant non dégénérée, il vient : $f\left(x + x'\right) = f(x) + f\left(x'\right)$.

f est donc un endomorphisme surjectif de E et puisque E est de dimension finie, c'est un automorphisme.

Remarque

L'injectivité peut se prouver directement très facilement. En effet, soit $x \in \operatorname{Ker} f$, on a :

$$\forall y \in E,\ \varphi(x, y) = \varphi\big(0_E, f(y)\big) = 0, \quad \text{donc } x = 0_E \text{ et } f \text{ est injective.}$$

Ex. 2

q se développe $q(x) = (n-1)\sum_{i=1}^{n} x_i^2 - 2\sum_{1 \leqslant i < j \leqslant n} x_i x_j$, on en déduit la matrice de q sur la base canonique :

$$A = \begin{pmatrix} n-1 & & & \\ & \ddots & (-1) & \\ & (-1) & \ddots & \\ & & & n-1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{R})$$

- De façon immédiate, la somme de toutes les lignes est nulle, d'où : $\operatorname{rg} q \leqslant n - 1$.
- Calculons alors le déterminant d'ordre $n - 1$ (par des manipulations immédiates sur les lignes) :

$$A = \begin{vmatrix} n-1 & & & \\ & \ddots & (-1) & \\ & (-1) & \ddots & \\ & & & n-1 \end{vmatrix} = \begin{vmatrix} 1 & \cdots & \cdots & \cdots & 1 \\ & n-1 & & & \\ & & \ddots & (-1) & \\ & (-1) & & \ddots & \\ & & & & n-1 \end{vmatrix} = \begin{vmatrix} 1 & \cdots & \cdots & \cdots & 1 \\ 0 & n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & n \end{vmatrix} = n^{n-2}$$

donc : $\operatorname{rg} A = \operatorname{rg} q = n - 1$.

Copyrighted material

Ex. 3

L'inégalité de Cauchy-Schwarz appliquée, dans $\mathbb{R}^n$ euclidien canonique, aux vecteurs $u = (1, 1, \dots, 1)$ et $v = (x_1, x_2, \dots, x_n)$ donne :

$$\left(\sum_{i=1}^{n} x_i\right)^2 \leqslant n \sum_{i=1}^{n} x_i^2. \qquad (1)$$

Si $(x_1, \dots, x_n)$ est solution de $\begin{cases} x_1 + x_2 + \dots + x_n = n \\ x_1^2 + x_2^2 + \dots + x_n^2 = n \end{cases}$

l'inégalité (1) devient une égalité et on sait que cela donne u et v liés. Il existe donc $\lambda \in \mathbb{R}$ tel que :

$$\forall i \in [\![1, n]\!], x_i = \lambda.$$

Réciproquement, $(x_1, \dots, x_n) = \lambda(1, 1, \dots, 1)$ est solution du système si et seulement si $\lambda = 1$.

Le système proposé a donc une solution et une seule : $(1, 1, \dots, 1)$.

Ex. 4

Soit $f_k : x \mapsto \sin kx$, $f_k \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ et $E = \text{Vect}(f_1, f_2, \dots, f_n)$.

On montre facilement que $(f_1, f_2, \dots, f_n)$ est libre : ce sont, par exemple, des vecteurs propres associés à n valeurs propres distinctes $(-1, -2^2, \dots, -n^2)$ de l'endomorphisme $d_2 : f \mapsto f''$ de $\mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$.

En conséquence, $(f_1, \dots, f_n)$ est une base de E et A n'est autre que la matrice sur cette base du produit scalaire sur E définit par $\varphi : (f, g) \mapsto \displaystyle\int_0^{\frac{\pi}{2}} fg$, donc $\det A > 0$.

Ex. 5

1) Développons le déterminant de A. En ajoutant les colonnes 2 et 3 à la colonne 1, il vient :

$$\det A = \begin{vmatrix} a+b+c & b & c \\ a+b+c & a & b \\ a+b+c & c & a \end{vmatrix} = (a+b+c) \begin{vmatrix} 1 & b & c \\ 1 & a & b \\ 1 & c & a \end{vmatrix}$$

d'où $\det A = (a+b+c)\left(a^2+b^2+c^2-bc-ca-ab\right)$;

puis avec $(a+b+c)^2 = a^2+b^2+c^2+2(ab+bc+ca)$:

$$\det A = (a+b+c)\left[\frac{3}{2}\left(a^2+b^2+c^2\right) - \frac{1}{2}(a+b+c)^2\right].$$

Soit $S = \left\{(a, b, c) \in \mathbb{R}^3 \;/\; a^2+b^2+c^2 = 1\right\}$: c'est la sphère unité de $\mathbb{R}^3$ euclidien canonique, pour tout $(a, b, c) \in S$, on a :

$$\det A = \frac{1}{2}(a+b+c)\left[3-(a+b+c)^2\right]$$

soit en posant $s = a+b+c$, $\det A = \frac{1}{2}s\left(3-s^2\right)$.

D'après l'inégalité de Cauchy-Schwarz appliquée dans $\mathbb{R}^3$ euclidien canonique aux vecteurs $(1, 1, 1)$ et (a, b, c) on a :

$$|a+b+c| \leqslant \sqrt{3}\sqrt{a^2+b^2+c^2}$$

donc pour $(a, b, c) \in S$, $|s| \leqslant \sqrt{3}$.

La fonction $\varphi : s \mapsto \frac{1}{2}s(3-s^2)$ est impaire et $\varphi'(s) = \frac{3}{2}\left(1-s^2\right)$, ses variations sur $[0, \sqrt{3}]$ sont résumées par le tableau :

s	0		1		$\sqrt{3}$
$\varphi'(s)$		+	0	−	
$\varphi(s)$	0	↗	1	↘	0

Copyrighted material

donc $\forall s \in \left[-\sqrt{3}, \sqrt{3}\right]$, $|\varphi(s)| \leqslant 1$ et $\forall (a,b,c) \in S$, $|\det A| \leqslant 1$.

2) L'étude des variations de φ montre que l'égalité est réalisée si et seulement si $s = 1$ ou $s = -1$ c'est-à-dire $(a,b,c) \in \mathscr{C}_1 \cup \mathscr{C}_2$ où $\mathscr{C}_1$ et $\mathscr{C}_2$ sont deux cercles symétriques par rapport à O.

$$\mathscr{C}_1 \begin{cases} a^2 + b^2 + c^2 = 1 \\ a + b + c = 1 \end{cases} \qquad \mathscr{C}_2 \begin{cases} a^2 + b^2 + c^2 = 1 \\ a + b + c = -1 \end{cases}$$

$\mathscr{C}_1$ est le cercle du plan $P(a+b+c=1)$ centré en $A\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$ et de rayon $R = \sqrt{\frac{2}{3}}$.

Ex. 6

Le système $\begin{cases} x_1 + x_2 - x_3 - x_4 = 0 \\ x_1 + 3x_2 + x_3 - x_4 = 0 \end{cases}$ est de rang 2 (H est bien un plan) et équivaut à :

$$\begin{cases} x_3 = -x_2 \\ x_4 = x_1 + 2x_2 \end{cases}$$

Une base de H est donc (u_1, u_2) avec $u_1 = (1,0,0,1)$, $u_2 = (0,1,-1,2)$.

La méthode de Schmidt fournit une base orthonormale de H : (v_1, v_2) avec

$$v_1 = \frac{u_1}{\|u_1\|} = \frac{1}{\sqrt{2}}(1,0,0,1), \quad v_2 = \frac{u_2 - \langle u_2 \mid v_1\rangle v_1}{\|u_2 - \langle u_2 \mid v_1\rangle v_1\|} = \frac{1}{2}(-1,1,-1,1).$$

Soit p la projection orthogonale sur H, pour tout $x = (x_1, x_2, x_3, x_4)$, on a :

$$p(x) = \langle v_1 \mid x\rangle v_1 + \langle v_2 \mid x\rangle v_2 = \frac{1}{\sqrt{2}}(x_1 + x_4)v_1 + \frac{1}{2}(-x_1 + x_2 - x_3 + x_4)v_2.$$

Avec $\mathscr{B} = (e_i)_{1 \leqslant i \leqslant 4}$, la formule précédente permet de calculer $p(e_i)$, $i \in [\![1,4]\!]$, ce qui donne les colonnes de $\mathrm{mat}_{\mathscr{B}} p$. On obtient :

$$\mathrm{mat}_{\mathscr{B}} p = \frac{1}{4}\begin{pmatrix} 3 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 3 \end{pmatrix}.$$

Si s désigne la symétrie orthogonale par rapport à H, on a $s = 2p - \mathrm{Id}$ donc :

$$\mathrm{mat}_{\mathscr{B}} s = \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & 1 \end{pmatrix}.$$

Niveau 2

Ex. 7

Soit $f \in \mathscr{L}_2(E)$ vérifiant **(1)** et non alternée. Il existe donc $a \in E$ tel que $q(a) \neq 0$ où q est la forme quadratique définie sur E par : $\forall x \in E$, $q(x) = f(x,x)$.

1) Montrons que $\forall x \in E$, $f(x,a) = f(a,x)$. **(2)**

Pour $\lambda \in \mathbb{R}$, on a $f(a, x + \lambda a) = f(a,x) + \lambda q(a)$, donc puisque $q(a) \neq 0$, avec $\lambda = -\frac{f(a,x)}{q(a)}$, on a :

$$f(a, x + \lambda a) = 0$$

d'où, d'après **(1)**, $f(a, x + \lambda a) = f(x + \lambda a, a) = 0$. Il en résulte :

$$f(a,x) + \lambda q(a) = f(x,a) + \lambda q(a) \text{ donc } f(a,x) = f(x,a).$$

2) Montrons que $\forall (x,y) \in E^2$, $f(x,y) = f(y,x)$ **(3)**

- Si $f(x,a) \neq 0$, en posant $\lambda = -\frac{f(x,y)}{f(x,a)}$, on a $f(x, y + \lambda a) = 0$ et alors :

$$f(x, y + \lambda a) = f(y + \lambda a, x) = 0 \text{ donc } f(x,y) + \lambda f(x,a) = f(y,x) + \lambda f(a,x)$$

et, d'après **(2)** : $f(x,y) = f(y,x)$.

Copyrighted material

Puisque x et y jouent des rôles symétriques dans **(3)**, le résultat reste valable si $f(y, a) \neq 0$.

- Si $f(x, a) = f(y, a) = 0$, on a pour tout λ réel, $f(x + a, y + \lambda a) = f(x, y) + \lambda q(a)$, donc avec $\lambda = -\dfrac{f(x, y)}{q(a)}$, il vient : $f(x + a, y + \lambda a) = 0$. Et d'après **(1)** :

$$f(x + a, y + \lambda a) = f(y + \lambda a, x + a).$$

Il en résulte $f(x, y) + \lambda q(a) = f(y, x) + \lambda q(a)$ et enfin $f(x, y) = f(y, x)$.

Ex. 8

Soit $x = (x_1, x_2, \cdots, x_n) \in \mathbb{R}^n$, $q(x) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j$.

Posons $x' = (x_1, \cdots, x_{n-1}) \in \mathbb{R}^{n-1}$: $q'(x') = a_{nn}\sum_{i=1}^{n-1}\sum_{j=1}^{n-1} a_{ij}x_ix_j - \sum_{i=1}^{n-1}\sum_{j=1}^{n-1} x_ix_ja_{ni}a_{nj}$ **(1)**

On a $\sum_{i=1}^{n-1}\sum_{j=1}^{n-1} a_{ij}x_ix_j = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j - 2x_n\sum_{j=1}^{n} a_{nj}x_j + a_{nn}x_n^2$ et :

$$\sum_{i=1}^{n-1}\sum_{j=1}^{n-1} x_ix_ja_{ni}a_{nj} = \left(\sum_{i=1}^{n-1} a_{ni}x_i\right)^2 = \left(\sum_{i=1}^{n} a_{ni}x_i - a_{nn}x_n\right)^2$$

$$= \left(\sum_{i=1}^{n} a_{ni}x_i\right)^2 - 2a_{nn}x_n\sum_{i=1}^{n} a_{ni}x_i + a_{nn}^2x_n^2$$

D'où, en reportant dans **(1)** : $q'(x') = a_{nn}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j - \left(\sum_{i=1}^{n} a_{ni}x_i\right)^2$ ou encore, en notant $(e_i)_{1\leqslant i\leqslant n}$ la base canonique de $\mathbb{R}^n$ et φ la forme polaire de q :

$$q'(x') = q(e_n)q(x) - \left[\varphi(x, e_n)\right]^2.$$

D'après l'inégalité de Cauchy-Schwarz appliquée à la forme quadratique q positive, on en conclut que q' est positive.

D'autre part, $q'(x') = 0$ s'écrit : $\varphi(x, e_n)^2 = q(e_n)q(x)$; or, q étant définie-positive, l'inégalité de Cauchy-Schwarz se réduit à une égalité si et seulement si les vecteurs sont liés, donc $x = \lambda e_n$ et $x' = 0$. Finalement q' est définie-positive.

Ex. 9

1) $\mathscr{C}$ est l'ensemble des polynômes $P = aX^2 + bX + c$ tels que $b^2 - 4ac \geqslant 0$, c'est donc un cône car il est stable par toute homothétie $P \mapsto \lambda P$, et on a $\mathscr{C} = \Phi^{-1}(\mathbb{R}_+)$ où Φ est l'application de E dans $\mathbb{R}$ définie par Φ :

$$aX^2 + bX + c \mapsto b^2 - 4ac.$$

La fonction $\varphi : \mathbb{R}^3 \to \mathbb{R}, (a, b, c) \mapsto b^2 - 4ac$ est continue (c'est une fonction polynôme) donc Φ est continue en tant que composée des fonctions continues :

$$\pi : E \to \mathbb{R}^3, aX^2 + bX + c \mapsto (a, b, c) \text{ et } \varphi.$$

En conséquence, $\mathscr{C}$ est un fermé de E puisqu'il s'agit de l'image réciproque, par la fonction continue Φ, de $\mathbb{R}_+$ qui est un fermé de $\mathbb{R}$. (Voir Analyse MP, chapitre 1.)

2) Le cône $\mathscr{C}$ est la réunion des droites vectorielles $D_P = \mathbb{R}P$ avec $P = aX^2 + bX + c$ tel que $b^2 - 4ac \geqslant 0$ (ce sont les génératrices). De plus, quitte à remplacer P par un polynôme proportionnel, on peut se limiter à :

$$\|P\|^2 = a^2 + b^2 + c^2 = 1 \quad \text{et} \quad a \geqslant 0.$$

En conséquence $d(A, \mathscr{C}) = \inf\{d(P) / P = aX^2 + bX + c, a^2 + b^2 + c^2 = 1, a \geqslant 0, b^2 - 4ac \geqslant 0\}$ où l'on a noté $d(P)$ la distance de A à la droite D_P.

Copyrighted material

On sait que $d(P)^2 = \| A - p_P(A) \|^2 = \| A \|^2 - \dfrac{\langle A \mid P \rangle^2}{\| P \|^2}$ ($p_P(A)$ est le projeté orthogonal de A sur la droite D_P : $p_P(A) = \dfrac{\langle A \mid P \rangle}{\| P \|^2} P$), donc $d(P)^2 = 2 - (a+c)^2$ et :

$$d(A, \mathscr{C})^2 = \inf \left\{ 2 - (a+c)^2 \,/\, a^2 + b^2 + c^2 = 1, a \geqslant 0, b^2 - 4ac \geqslant 0 \right\}.$$

De $b^2 - 4ac \geqslant 0$ et $a^2 + b^2 + c^2 = 1$, on déduit :

$$2ac \leqslant \frac{1 - (a^2 + c^2)}{2} \text{ d'où } (a+c)^2 \leqslant \frac{1 + a^2 + c^2}{2}.$$

Avec $a^2 + c^2 = 1 - b^2 \leqslant 1$, il vient alors $(a+c)^2 \leqslant 1$ et enfin $2 - (a+c)^2 \geqslant 1$, donc $d(A, \mathscr{C}) \geqslant 1$.

Il suffit de constater que pour $P = 1$, on a $P \in \mathscr{C}$ et $d(P) = 1$, pour conclure à $d(A, \mathscr{C}) = 1$.

On peut vérifier que, pour $P \in \mathscr{C}$ tel que $\| P \| = 1$ et $a \geqslant 0$, on a $d(P) = 1$ c'est-à-dire $2 - (a+c)^2 = 1$ si et seulement si $P = X^2$ ou $P = 1$ ou -1, ce qui définit deux génératrices du cône $\mathscr{C}$.

En effet, les conditions $\| P \| = 1$ et $d(P) = 1$ s'écrivent $a^2 + b^2 + c^2 = 1$, $a^2 + 2ac + c^2 = 1$, ce qui donne $b^2 = 2ac$ donc $ac \geqslant 0$ et, avec $b^2 - 4ac \geqslant 0$, on en déduit $ac \leqslant 0$ d'où finalement $ac = 0$.

Pour $a = 0$, on obtient $b = 0$ donc $c = \pm 1$, c'est-à-dire $P = 1$ ou $P = -1$.

Pour $c = 0$, on obtient $b = 0$ donc $a = 1$, c'est-à-dire $P = X^2$.

Les projections de A sur ces deux génératrices sont :

$$P_1 = \frac{\langle A \mid X^2 \rangle}{\| X^2 \|^2} X^2 = X^2 \quad \text{et} \quad P_2 = \frac{\langle A \mid 1 \rangle}{\| 1 \|^2} 1 = 1$$

ce sont les «points» de $\mathscr{C}$ en lesquels la distance $d(A, \mathscr{C})$ est atteinte.

Ex. 10

1) a) L'ensemble $\left\{ x \in F \,/\, d(a, F) = \| x - a \| \right\}$ a au plus un élément : voir démonstration du théorème 23, proposition a).

b) Il reste donc à prouver l'existence de $b \in F$ tel que $d(a, F) = \| b - a \|$.

$d^2(a, F)$ est le plus grand minorant de $\left\{ \| x - a \|^2 \,/\, x \in F \right\}$ donc, pour tout $n \in \mathbb{N}^*$, il existe $x_n \in F$ tel que :

$$d^2(a, F) \leqslant \| x_n - a \|^2 < \frac{1}{n^2} + d^2(a, F). \qquad (1)$$

Le théorème de la médiane donne :

$$\| x_n - a \|^2 + \| x_p - a \|^2 = 2 \left\| a - \frac{x_n + x_p}{2} \right\|^2 + 2 \left\| \frac{x_n - x_p}{2} \right\|^2.$$

Puisque $\dfrac{x_n + x_p}{2} \in F$ (convexité), on a $\left\| a - \dfrac{x_n + x_p}{2} \right\|^2 \geqslant d^2(a, F)$ et il vient :

$$\left\| \frac{x_n - x_p}{2} \right\|^2 \leqslant \frac{1}{2} \left[\| x_n - a \|^2 + \| x_p - a \|^2 \right] - d^2(a, F)$$

donc $\dfrac{1}{4} \| x_n - x_p \|^2 \leqslant \dfrac{1}{2} \left[d^2(a, F) + \dfrac{1}{n^2} + d^2(a, F) + \dfrac{1}{p^2} \right] - d^2(a, F)$ et enfin :

$$\| x_n - x_p \|^2 \leqslant 2 \left(\frac{1}{n^2} + \frac{1}{p^2} \right).$$

En conséquence, $\sup\limits_{p \in [\![n, +\infty [\![} \| x_n - x_p \| \leqslant \dfrac{2}{n}$ et la suite $(x_n)_{\mathbb{N}^*}$ est de Cauchy (voir Analyse MP, chapitre 1).

F étant complet, cette suite converge vers $b \in F$ et par continuité de la norme, on a : $\| b - a \| = \lim\limits_{n \to +\infty} \| x_n - a \|$ donc, d'après l'inégalité **(1)** : $\| b - a \| = d(a, F)$.

2) D'après le théorème 23, $\| b - a \| = d(a, F)$ donne $b - a \in F^\perp$.

En écrivant, pour tout a de E, $a = a - b + b$ avec $a - b \in F^\perp$ et $b \in F$, on prouve ainsi que $E = F + F^\perp$ donc $E = F \oplus F^\perp$ (car on sait que $F \cap F^\perp = \{0\}$ est toujours vrai).

Copyrighted material

Ex. 11

1) a) Les conditions **(1)** et **(2)** sont équivalentes à :

$$\forall n \in \mathbb{N}, (P_0, P_1, \cdots, P_n) \text{ est un système orthogonal}$$

$$\forall n \in \mathbb{N}, \text{Vect}\left(1, X, X^2, \cdots, X^n\right) = \text{Vect}\left(P_0, P_1, \cdots, P_n\right)$$

donc $\left(P_N\right)_{n\in\mathbb{N}}$ se déduit de $\left(X^n\right)_{n\in\mathbb{N}}$ par le procédé d'orthogonalisation de Schmidt.

On sait que chaque polynôme P_n est défini à un coefficient de proportionnalité près. Une solution est fournie par :

$$P_0 = 1 \ , \ \forall n \in \mathbb{N} \ , \ P_n = X^n - \sum_{k=0}^{n-1} \frac{\langle X^n \mid P_k \rangle}{\langle P_k \mid P_k \rangle} P_k.$$

b) Pour $n \geqslant 1$, on a $\langle P_n \mid P_0 \rangle = 0$ c'est-à-dire $\displaystyle\int_{-1}^{1} P_n(x)\mathrm{d}x = 0$.

La fonction P_n est continue sur $[-1, 1]$, si elle ne s'annulait pas en changeant de signe sur $]-1, 1[$, elle resterait de signe constant sur $[-1, 1]$.

Dans ces conditions, $\displaystyle\int_{-1}^{1} P_n(x)\mathrm{d}x = 0$ exige $\forall x \in [-1, 1], P_n(x) = 0$, ce qui est impossible puisqu'un polynôme de degré n a au plus n racines réelles.

En conséquence, P_n s'annule au moins une fois en changeant de signe sur $]-1, 1[$.

Soit alors $\alpha_1, \cdots, \alpha_p$ les racines réelles distinctes de P_n, appartenant à $]-1, 1[$, en lesquelles P_n change de signe.

Puisque $\deg P_n = n$, on a $p \leqslant n$. Avec $p < n$, le polynôme $Q = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_p)$ appartiendrait à $\text{Vect}\left(P_0, P_1, \cdots, P_{n-1}\right)$ et serait donc orthogonal à P_n.

On aurait ainsi $\displaystyle\int_{-1}^{1} P_n(x)Q(x)\mathrm{d}x = 0$ avec une fonction P_nQ continue et de signe constant (les changements de signe de P_n et Q étant simultanés, le produit ne change pas de signe), ce qui exige $\forall x \in [-1, 1]$, $P_n(x)Q(x) = 0$ donc $\forall x \in [-1, 1]$, $P_n(x) = 0$. C'est encore une impossibilité.

En conséquence, on a $p = n$, c'est-à-dire que P_n a exactement n racines réelles simples et situées sur l'intervalle $]-1, 1[$.

c) Une suite $\left(L_n\right)_{n\in\mathbb{N}}$ vérifiant **(1)** et **(2)** est de la forme :

$$\left(\lambda_n P_n\right)_{n\in\mathbb{N}} \text{ où } \forall n \in \mathbb{N}, \ \lambda_n \in \mathbb{R}^*.$$

D'après le b), on a $P_n(1) \neq 0$ donc la condition **(3)** est réalisée si et seulement si $\forall n \in \mathbb{N}, \lambda_n = \dfrac{1}{P_n(1)}$ d'où l'existence et l'unicité de $\left(L_n\right)_{n\in\mathbb{N}}$ vérifiant **(1)**, **(2)** et **(3)**.

2) $\left((X-1)^k\right)_{0\leqslant k\leqslant 2n}$ est une base de $\mathbb{R}_{2n}[X]$, tout polynôme Q de degré $2n$ et tel que $(X-1)^n$ divise Q s'écrit de manière unique :

$$Q = \sum_{k=n}^{2n} q_k (X-1)^k \text{ avec } q_{2n} \neq 0$$

et on a alors :

$$Q^{(n)} = \sum_{k=n}^{2n} k(k-1)\cdots(k-n+1)\, q_k (X-1)^{k-n}$$

$$= \sum_{k=0}^{n} \frac{(k+n)!}{k!} q_{k+n} (X-1)^k$$

De même L_n s'écrit de manière unique : $\displaystyle L_n = \sum_{k=0}^{n} \ell_{n,k} (X-1)^k$

donc $Q^{(n)} = L_n$ équivaut à $\forall k \in [\![0, n]\!]$, $\dfrac{(k+n)!}{k!} q_{k+n} = \ell_{n,k}$.

Copyrighted material

On en déduit l'existence et l'unicité d'un polynôme Q vérifiant les conditions données :

$$Q = \sum_{k=n}^{2n} \frac{(k-n)!}{k!}\, \ell_{n,k-n}\, (X-1)^k$$

(on a bien $q_{2n} = \dfrac{n!}{(2n)!}\, \ell_{n,n} \neq 0$ car $\deg L_n = n$).

3) 1 est racine d'ordre n de Q donc :

$$\forall k \in [\![0, n-1]\!],\ Q^{(k)}(1) = 0$$

Avec $\langle L_n \mid 1 \rangle = 0$ on obtient $\displaystyle\int_{-1}^{1} Q^{(n)}(x)\mathrm{d}x = 0$ donc $Q^{(n-1)}(1) - Q^{(n-1)}(-1) = 0$ puis $Q^{(n-1)}(-1) = 0$.

Si $n \geqslant 2$, avec $\langle L_n \mid X \rangle = 0$, on obtient $\displaystyle\int_{-1}^{1} x\, Q^{(n)}(x)\mathrm{d}x = 0$ puis en intégrant par parties :

$$\left[x\, Q^{(n-1)}(x)\right]_{-1}^{1} - \int_{-1}^{1} Q^{(n-1)}(x)\mathrm{d}x = 0$$

donc $-Q^{(n-2)}(1) + Q^{(n-2)}(-1) = 0$ et enfin $Q^{(n-2)}(-1) = 0$.

Supposons que pour $k < n$, $Q^{(n-1)}(-1) = Q^{(n-2)}(-1) = \cdots = Q^{(n-k+1)}(-1) = 0$. Avec $\langle L_n \mid X^{k-1} \rangle = 0$, on obtient $\displaystyle\int_{-1}^{1} x^{k-1} Q^{(n)}(x)\mathrm{d}x = 0$ et en intégrant $k-1$ fois par parties :

$$(-1)^{k-1}(k-1)! \int_{-1}^{1} Q^{(n-k+1)}(x)\mathrm{d}x = 0$$

donc $Q^{(n-k)}(1) - Q^{(n-k)}(-1) = 0$ puis $Q^{(n-k)}(-1) = 0$.

On a ainsi par récurrence $Q^{(k)}(-1) = 0$ pour tout $k \in [\![0, n-1]\!]$, c'est-à-dire que -1 est racine d'ordre n de Q ou encore que $(x+1)^n$ divise Q.

En conséquence, Q est divisible par $\left(X^2-1\right)^n = (X+1)^n(X-1)^n$ et compte tenu de $\deg Q = 2n$, il existe un réel μ tel que : $\qquad Q = \mu(X^2-1)^n$.

La formule de Leibniz donne :

$$\frac{\mathrm{d}^n}{\mathrm{d}x^n}(x^2-1)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \frac{\mathrm{d}^k}{\mathrm{d}x^k}(x+1)^n \frac{\mathrm{d}^{n-k}}{\mathrm{d}x^{n-k}}(x-1)^n$$

donc $L_n = \mu \displaystyle\sum_{k=0}^{n} n! \left(\mathrm{C}_n^k\right)^2 (x+1)^{n-k}(x-1)^k$ et la condition $L_n(1) = 1$ fournit $\mu = \dfrac{1}{2^n n!}$.

Finalement, on obtient la formule, dite de Rodrigues : $L_n = \dfrac{1}{2^n n!} \dfrac{\mathrm{d}^n}{\mathrm{d}x^n}(x^2-1)^n$.

Ex. 12

1) Notons $C_1, \ldots, C_n$ les colonnes de $G(x_1, \ldots, x_n)$.

a) ▪ Si $(x_1, \ldots, x_n)$ est lié, l'un des vecteurs x_j est combinaison linéaire des autres :

$$x_j = \sum_{\substack{k=1 \\ k \neq j}}^{n} \lambda_k x_k .$$

Alors $\forall i \in [\![1, n]\!]$, $\langle x_i \mid x_j \rangle = \displaystyle\sum_{\substack{k=1 \\ k \neq j}}^{n} \lambda_k \langle x_i \mid x_k \rangle$ donc $C_j = \displaystyle\sum_{\substack{k=1 \\ k \neq j}}^{n} \lambda_k C_k$ et $DG(x_1, \ldots, x_n) = 0$.

▪ Si $(x_1, \ldots, x_n)$ est libre, $G(x_1, \ldots, x_n)$ est la matrice sur la base $(x_i)_{1 \leqslant i \leqslant n}$ de $F = \mathrm{Vect}(x_1, \ldots, x_n)$ du produit scalaire, donc G est inversible d'après la propriété 29.

b) La matrice d'un produit scalaire sur une base $\mathcal{B}$ a un déterminant strictement positif, donc :

$$(x_1, \ldots, x_n) \text{ libre } \Rightarrow\ DG(x_1, \ldots, x_n) > 0.$$

L'implication réciproque résulte de a).

Copyrighted material

Hidden page

Hidden page

La fonction f'^2 étant continue et positive sur $[0,1]$, la condition $\int_0^1 f'(t)^2 \mathrm{d}t = 0$ donne $\forall t \in [0,1], f'(t) = 0$ donc f est constante sur $[0,1]$ et, avec $f(0) = 0$, il vient $f = 0$ (fonction nulle sur $[0,1]$). On a ainsi prouvé que φ est définie-positive. C'est donc un produit scalaire sur E. On notera :

$$\varphi(f,g) = \langle f \mid g \rangle \quad \text{et} \quad \varphi(f,f) = \|f\|^2.$$

3) Pour tout f de V, une intégration par parties donne :

$$\int_0^1 e^t f(t)\mathrm{d}t = \left[e^t f(t)\right]_0^1 - \int_0^1 e^t f'(t)\mathrm{d}t = e + 1 - \int_0^1 e^t f'(t)\mathrm{d}t$$

d'où :

$$\begin{aligned} I(f) &= \int_0^1 \left(f'^2(t) - 2e^t f'(t)\right)\mathrm{d}t + 2e + 2 \\ &= \int_0^1 \left(f'(t) - e^t\right)^2 \mathrm{d}t - \frac{e^2}{2} + 2e + \frac{5}{2} \end{aligned}$$

En posant $g(t) = f(t) - e^t$ on a $g \in E$ avec $g(0) = -2$, donc :

$$\int_0^1 \left(f'(t) - e^t\right)^2 \mathrm{d}t = \int_0^1 g'(t)^2 \mathrm{d}t = \|g\|^2 - 4$$

et :

$$I(f) = \|g\|^2 - \frac{1}{2}e^2 + 2e - \frac{3}{2}.$$

Il est alors clair que l'ensemble $\left\{I(f) \,/\, f \in V\right\}$ est borné inférieurement et que cette borne est atteinte quand $\|g\|$ est minimum.

En posant $f = P + h$, d'après le 1), f décrit V si et seulement si h décrit le sous-espace vectoriel W, et on a $g = h - (\exp - P)$. Donc la borne inférieure de $\|g\|$ est atteinte en au plus un point h_0 de W et c'est le cas si et seulement si $h_0 - (\exp - P) \in W^\perp$ c'est-à-dire $f_0 - \exp \in W^\perp$ en posant $f_0 = h_0 + P$, (voir le théorème 23).

Remarque

W n'étant évidemment pas de dimension finie, le cours ne nous permet pas d'affirmer l'existence du projeté orthogonal de $\exp - P$ sur W.

Nous sommes ainsi ramenés à la recherche de $f_0 \in V$ tel que $\langle f_0 - \exp \mid u \rangle = 0$ pour tout $u \in W$.

Pour $u \in W$, on a :

$$\begin{aligned} \langle f_0 - \exp \mid u \rangle &= u(0)\left(f_0(0) - 1\right) + \int_0^1 u'(t)\left(f_0'(t) - e^t\right)\mathrm{d}t \\ &= \int_0^1 u'(t)\left(f_0'(t) - e^t\right)\mathrm{d}t \quad (\text{car } u(0) = 0) \end{aligned}$$

et en intégrant par parties :

$$\langle f_0 - \exp \mid u \rangle = -\int_0^1 u(t)\left(f_0''(t) - e^t\right)\mathrm{d}t \quad (\text{car } u(0) = u(1) = 0).$$

En conséquence pour avoir $f_0 - \exp \in W^\perp$, il suffit que :

$$\forall t \in [0,1], \quad f_0''(t) = e^t$$

c'est-à-dire , compte tenu de $f_0(0) = -1$ et $f_0(1) = 1$:

$$\forall t \in [0,1], \quad f_0(t) = e^t + (3 - e)t - 2.$$

Comme on sait que ce problème a au plus une solution, cette fonction f_0 est l'unique élément de V en lequel $\|g\|$ et donc $I(f)$ atteint sa borne inférieure. On a alors :

$$\begin{aligned} \min_{f \in V} I(f) &= \|f_0 - \exp\|^2 - \frac{1}{2}e^2 + 2e - \frac{3}{2} \\ &= \int_0^1 \left(f_0'(t) - e^t\right)^2 \mathrm{d}t - \frac{1}{2}e^2 + 2e + \frac{5}{2} \\ &= \frac{1}{2}e^2 - 4e + \frac{23}{2}. \end{aligned}$$

Copyrighted material

Ex. 15

Une norme vérifie : $\forall x \in E, \| -x \| = \| x \|$, donc f est symétrique.

1) $4\big(f(x+y,z)+f(x-y,z)\big) = \| x+y+z \|^2 - \| x+y-z \|^2 + \| x-y+z \|^2 - \| x-y-z \|^2$.

Or $\| x+y+z \|^2 + \| x-y+z \|^2 = 2\big(\| x+z \|^2 + \| y \|^2\big)$ et $\| x+y-z \|^2 + \| x-y-z \|^2 = 2\big(\| x-z \|^2 + \| y \|^2\big)$ et il s'ensuit $4\big(f(x+y,z)+f(x-y,z)\big) = 2\big(\| x+z \|^2 - \| x-z \|^2\big) = 8f(x,z)$, c'est-à-dire :

$$f(x+y,z)+f(x-y,z) = 2f(x,z).$$

En particulier, on a $f(2x,z)+f(0,z) = 2f(x,z)$. Or $4f(0,z) = \| z \|^2 - \| -z \|^2 = 0$, d'où $f(2x,z) = 2f(x,z)$.

Notons aussi que $\forall (u,z) \in E^2$, $4f(-u,z) = \| -u+z \|^2 - \| -u-z \|^2 = \| u-z \|^2 - \| u+z \|^2 = -4f(u,z)$.

On applique $f(x+y,z)+f(x-y,z) = 2f(x,z)$ à $x = \dfrac{1}{2}(u+v)$ et $y = \dfrac{1}{2}(u-v)$ et il vient :

$$f(u,z)+f(v,z) = 2f\Big(\frac{1}{2}(u+v),z\Big).$$

Il reste à utiliser $2f(x,z) = f(2x,z)$ pour obtenir $f(u,z)+f(v,z) = f(u+v,z)$.

On a ainsi établi que la première application partielle de f c'est-à-dire $f(\cdot\,,y) \ : \ x \mapsto f(x,y)$ est, quel que soit $y \in E$, un morphisme additif.

2) Avec $f(u,z)+f(v,z) = f(u+v,z)$, on obtient par récurrence $\forall n \in \mathbb{N}^*$, $f(nx,z) = nf(x,z)$.

Avec $f(-u,z) = -f(u,z)$ et $f(0,z) = 0$, on a $\forall n \in \mathbb{Z}$, $f(nx,z) = nf(x,z)$.

Ensuite, pour tout $p \in \mathbb{N}^*$, $f\Big(p\dfrac{x}{p},z\Big) = pf\Big(\dfrac{x}{p},z\Big)$ donne $f\Big(\dfrac{x}{p},z\Big) = \dfrac{1}{p}f(x,z)$.

Enfin, pour tout $r \in Q$, en écrivant $r = \dfrac{n}{p}$, $n \in \mathbb{Z}$, $p \in \mathbb{N}^*$, on obtient :

$$\forall (x,z) \in E^2, \ \ f(rx,z) = nf\Big(\frac{x}{p},z\Big) = \frac{n}{p}f(x,z) = rf(x,z).$$

Tout réel λ est limite d'une suite (r_n) de rationnels. À partir de $\lim f(r_n x,z) = \lim r_n f(x,z) = \lambda f(x,z)$, la continuité de f par rapport au premier argument permet de conclure que $f(\lambda x,z) = \lambda f(x,z)$ et établir le second volet de la linéarité de la première application partielle de f.

- Continuité

E étant un espace vectoriel normé, l'application $x \mapsto \| x \|$ est continue sur E, tandis que $(x,y) \mapsto x+y$ et $(x,y) \mapsto x-y$ sont continues sur E^2. Il en résulte que f est continue sur E^2 (par composition d'applications continues) ce qui assure la continuité sur E de $x \mapsto f(x,z)$.

Avec la symétrie déjà citée, f est une forme bilinéaire symétrique sur E.

Pour conclure, on forme $4f(x,x) = \| 2x \|^2 + \| 0_E \|^2$, ce qui montre que f est positive.

Avec $\| 0_E \| = 0$, on a $4f(x,x) = \| 2x \|^2$, donc $f(x,x) = 0 \iff 2x = 0_E$, c'est-à-dire $x = 0_E$ et la forme f est définie-positive : c'est un produit scalaire sur E.

Remarque

$\forall (\lambda,x) \in \mathbb{R} \times E$, $\| \lambda x \| = |\lambda| \| x \|$, donc $f(x,x) = \| x \|^2$. On a ainsi prouvé que si une norme sur un $\mathbb{R}$-espace vectoriel vérifie l'identité du parallélogramme, alors il s'agit d'une norme euclidienne.

Ex. 16

1) La bilinéarité de φ résulte clairement de la linéarité de l'application «trace».

D'autre part $\mathrm{Tr}(M) = \mathrm{Tr}({}^tM)$ donne $\mathrm{Tr}({}^tAB) = \mathrm{Tr}({}^tBA)$: φ est symétrique.

Avec $A = \big[a_{ij}\big]$ on a ${}^tAA = \big[m_{ij}\big]$, $m_{ij} = \displaystyle\sum_{k=1}^{n} a_{ki}a_{kj}$ donc : $\varphi(A,A) = \mathrm{Tr}({}^tAA) = \displaystyle\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2$.

Le calcul montre que $\forall A \in E$, $\varphi(A,A) \geqslant 0$, et si $\varphi(A,A) = 0$ on a : $\forall (i,j) \in [\![1,n]\!]^2$, $a_{ij} = 0$ donc $A = 0$.

Ainsi φ est bien un produit scalaire, la norme euclidienne associée étant définie par :

$$\forall A \in E, \ \ \| A \|^2 = \sum_{i=1}^{n}\sum_{i=1}^{n} a_{ij}^2.$$

Copyrighted material

Les a_{ij} étant les coordonnées de A sur la base canonique $\left(E_{ij}\right)_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}$ de $\mathcal{M}_n(\mathbb{R})$ (les E_{ij} sont les matrices élémentaires), on constate que la norme définie par $\|A\|^2 = \operatorname{Tr}\left({}^tAA\right)$ n'est autre que la norme euclidienne canonique sur $\mathcal{M}_n(\mathbb{R})$ (voir *Mise en œuvre*, Exercice 2).

2) a) L'inégalité de Cauchy-Schwarz donne :

$$\begin{aligned} &&\left|\langle I_n \mid A\rangle\right| &\leqslant \|I_n\|\|A\| \\ \text{donc} &&|\operatorname{Tr} A| &\leqslant \sqrt{n}\sqrt{\operatorname{Tr}({}^tAA)} \\ \text{et } a\ fortiori &&\operatorname{Tr} A &\leqslant \sqrt{n\operatorname{Tr}({}^tAA)}\end{aligned}$$

b) Si A est telle que $\operatorname{Tr} A = \sqrt{n\operatorname{Tr}({}^tAA)}$ compte tenu de :

$$\begin{aligned} \operatorname{Tr} A \leqslant |\operatorname{Tr} A| &\leqslant \sqrt{n\operatorname{Tr}({}^tAA)} \\ \text{on a aussi} \qquad |\operatorname{Tr} A| &= \sqrt{n\operatorname{Tr}({}^tAA)} \\ \text{c'est-à-dire} \qquad \left|\langle I_n \mid A\rangle\right| &= \|I_n\|\|A\|\end{aligned}$$

Il existe donc $\lambda \in \mathbb{R}$ tel que $A = \lambda I_n$. (C'est le cas d'égalité de Cauchy-Schwarz.)
Réciproquement, pour $A = \lambda I_n$ on obtient :

$$\operatorname{Tr} A = n\lambda \text{ et } \operatorname{Tr}({}^tAA) = n\lambda^2 \text{ donc } \sqrt{n\operatorname{Tr}({}^tAA)} = n|\lambda|.$$

Il y a donc égalité si et seulement si λ est positif ou nul.
En conclusion, $\operatorname{Tr} A = \sqrt{n\operatorname{Tr}({}^tAA)}$ équivaut à $A = \lambda I_n$ avec $\lambda \in \mathbb{R}_+$.

3) a) Posons $A = \left[a_{ij}\right]$, $B = \left[b_{ij}\right]$, $AB = C = \left[c_{ij}\right]$ on a alors : $\forall (i,j) \in [\![1,n]\!]^2$, $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.

En notant $LA_i = \left(a_{i1}, a_{i2}, \ldots, a_{in}\right) \in \mathbb{R}^n$ le $i^{\text{ème}}$ vecteur ligne de A,
et $CB_j = \left(b_{1j}, b_{2j}, \ldots, b_{nj}\right) \in \mathbb{R}^n$ le $j^{\text{ème}}$ vecteur colonne de B,
dans $\mathbb{R}^n$ euclidien canonique, on a : $c_{ij} = \langle LA_i \mid CB_j\rangle$ donc, d'après l'inégalité de Cauchy-Schwarz, $c_{ij}^2 \leqslant \|LA_i\|^2\|CB_j\|^2$. Il en résulte :

$$\|AB\|^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} c_{ij}^2 \leqslant \sum_{i=1}^{n}\sum_{j=1}^{n} \|LA_i\|^2\|CB_j\|^2 \text{ donc aussi } \|AB\|^2 \leqslant \sum_{i=1}^{n}\|LA_i\|^2 \sum_{j=1}^{n}\|CB_j\|^2.$$

D'autre part $\sum_{i=1}^{n}\|LA_i\|^2 = \sum_{i=1}^{n}\sum_{k=1}^{n} a_{ik}^2 = \|A\|^2$ et de même $\sum_{j=1}^{n}\|CB_j\|^2 = \|B\|^2$, d'où finalement :

$$\|AB\|^2 \leqslant \|A\|^2\|B\|^2.$$

b) D'après le calcul précédent, on aura $\|AB\|^2 = \|A\|^2\|B\|^2$ si et seulement si :

$$\forall (i,j) \in [\![1,n]\!], \quad c_{ij}^2 = \|LA_i\|^2\|CB_j\|^2$$

c'est-à-dire, d'après l'étude des cas d'égalité de Cauchy-Schwarz, si et seulement si :

$$\forall (i,j) \in [\![1,n]\!], \quad LA_i \text{ et } CB_j \text{ sont liés.}$$

Lorsque $A = 0$ ou $B = 0$, ces conditions sont évidemment réalisées. Lorsque $A \neq 0$ et $B \neq 0$, si LA_{i_0} est une ligne non nulle de A, chaque colonne CB_j est colinéaire à LA_{i_0} et si CB_{j_0} est une colonne non nulle de B, chaque ligne LA_i est colinéaire à CB_{j_0}.
Dans tous les cas, il existe donc une colonne $U \in \mathcal{M}_{n,1}(\mathbb{R})$ ($\mathcal{M}_{n,1}(\mathbb{R})$ peut être identifié à $\mathbb{R}^n$) $U \neq 0$ et des réels $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ tels que :

$$A = \begin{pmatrix} \alpha_1\,{}^tU \\ \alpha_2\,{}^tU \\ \vdots \\ \alpha_n\,{}^tU \end{pmatrix} \quad , \quad B = \left[\beta_1 U, \beta_2 U, \ldots, \beta_n U\right].$$

Réciproquement pour des couples (A, B) de ce type, on a évidemment $\left(LA_i, CB_j\right)$ lié pour tout $(i,j) \in [\![1,n]\!]^2$ donc $\|AB\| = \|A\|\|B\|$.

Remarques

- Pour $\alpha_1 = \alpha_2 = \ldots = \alpha_n = 0$ on retrouve $A = 0$,
- si $(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq (0, 0, \ldots, 0)$ et $(\beta_1, \beta_2, \ldots \beta_n) \neq (0, 0, \ldots, 0)$ les matrices A et B sont de rang 1 avec $\operatorname{Im}{}^tA = \operatorname{Im} B = \operatorname{Vect} U$.

Copyrighted material

CHAPITRE

7 Espaces euclidiens

Copyrighted material

A. Structure d'espace euclidien

Définition 1

Un **espace euclidien** est un espace préhilbertien réel de dimension finie non nulle.

Dans cette section, E désigne un espace euclidien de dimension $n \geqslant 1$.

1. Bases orthonormales

L'étude des espaces préhilbertiens réels, dans le cas de la dimension finie, effectuée dans le chapitre 6, nous donne les propriétés suivantes.

Propriété 1

Pour tout sous-espace F d'un espace euclidien E, on a :

$$E = F \oplus F^{\perp} \quad , \quad F^{\perp\perp} = F.$$

Propriété 2

Un espace euclidien E admet au moins une base orthonormale. ✎(1)

Toute famille orthonormale peut être complétée en une base orthonormale.

✎(1) Ou orthonormée.

Pour toute base $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ de E, nous notons :

$$x = \sum_{i=1}^{n} x_i e_i \quad , \quad X = \mathrm{mat}_{\mathcal{B}}(x) = \begin{pmatrix} x_1 \\ \\ x_n \end{pmatrix}$$

et $G_{\mathcal{B}} = \left[\langle e_i \mid e_j \rangle\right]$ la matrice du produit scalaire dans la base $\mathcal{B}$.

Propriété 3

Soit $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ une base de E. Les propriétés suivantes sont équivalentes :

(1) $\mathcal{B}$ est orthonormale ;

(2) $G_{\mathcal{B}} = I_n$;

(3) $\forall (x, y) \in E^2, \langle x \mid y \rangle = \sum_{i=1}^{n} x_i y_i = {}^t XY$;

(4) $\forall x \in E, \|x\|^2 = \sum_{i=1}^{n} x_i^2 = {}^t XX$.

Propriété 4

Si $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ est une base orthonormale de E : ✎(2)

$$\forall x \in E, \quad x = \sum_{i=1}^{n} \langle x \mid e_i \rangle e_i .$$

✎(2) Les coordonnées d'un vecteur sur une base orthonormale sont les produits scalaires de ce vecteur avec les vecteurs de base.

Propriété 5

On munit un $\mathbb{R}$-espace vectoriel E de dimension $n \geqslant 1$ d'une structure d'espace euclidien en déclarant une base $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ de E comme base orthonormale ; le produit scalaire associé est alors donné par :

$$(x, y) \mapsto \langle x \mid y \rangle = \sum_{i=1}^{n} x_i y_i .$$

La situation précédente appliquée à $E = \mathbb{R}^n$ et $\mathcal{B}$ base canonique de $\mathbb{R}^n$, confère à $\mathbb{R}^n$ une **structure euclidienne** dite **canonique**.

Copyrighted material

Exemple 1 La base canonique de $\mathcal{M}_n(\mathbb{R})$ est formée des matrices élémentaires E_{ij}, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$,

$$E_{ij} = \left[\delta_{k,i}\,\delta_{\ell,j}\right]_{\substack{1\leqslant k\leqslant n\\ 1\leqslant \ell\leqslant n}},$$

le produit scalaire et la norme euclidienne canonique sont donc définis respectivement par :
pour toutes matrices $A = [a_{ij}]$ et $B = [b_{ij}]$ de $\mathcal{M}_n(\mathbb{R})$,

$$\langle A \mid B\rangle = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}b_{ij}, \quad \|A\|^2 = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^2$$

c'est-à-dire aussi :

$$\langle A \mid B\rangle = \operatorname{Tr}\left({}^tAB\right), \quad \|A\|^2 = \operatorname{Tr}\left({}^tAA\right).$$

(Voir chapitre 6, *Mise en œuvre*, Exercice 2.)

Théorème 1

Procédé d'orthogonalisation de Schmidt

Soit $(u_i)_{1\leqslant i\leqslant n}$ une base d'un espace euclidien E.

Il existe une unique base orthonormale $(e_i)_{1\leqslant i\leqslant n}$ de E telle que : ✎(3)

$$\forall j \in [\![1, n]\!],\ \operatorname{Vect}(e_1, \dots, e_j) = \operatorname{Vect}(u_1, \dots, u_j) \quad \text{et} \quad \langle e_j \mid u_j\rangle \in \mathbb{R}_+^*$$

✎(3) Ce théorème est un cas particulier des théorèmes vus au chapitre 6.

Remarques

1) La construction se fait de manière récurrente :

$$v_1 = u_1, \quad e_1 = \frac{u_1}{\|u_1\|}$$

et, pour $j \geqslant 2$: $v_j = u_j - \sum_{k=1}^{j-1} \langle e_k \mid u_j\rangle e_k$, $\quad e_j = \dfrac{v_j}{\|v_j\|}$.

2) Pour que les deux bases $(u_i)_{1\leqslant i\leqslant n}$ et $(e_i)_{1\leqslant i\leqslant n}$ vérifient :

$$\forall j \in [\![1, n]\!], \quad \operatorname{Vect}(e_1, \dots, e_j) = \operatorname{Vect}(u_1, \dots, u_j)$$

il faut et il suffit que la matrice P de passage de la base $(u_i)_{1\leqslant i\leqslant n}$ à la base $(e_i)_{1\leqslant i\leqslant n}$ soit triangulaire supérieure, donc aussi que la matrice P^{-1} de passage de la base $(e_i)_{1\leqslant i\leqslant n}$ à la base $(u_i)_{1\leqslant i\leqslant n}$ soit triangulaire supérieure.

3) Les coefficients diagonaux de P^{-1} sont les nombres $\langle e_i \mid u_i\rangle$, $\quad i = 1, 2, \dots, n$.

Exemple

Voir *Mise en œuvre*, Exercice 2.

2. Isomorphisme canonique d'un espace euclidien sur son dual

Théorème 2

L'application $I : E \to E^*,\ x \mapsto \langle \cdot \mid x\rangle$ est un isomorphisme de E sur E^*

☞ Pour tout x de E, $I(x)$ est l'application $y \mapsto \langle y \mid x\rangle$, donc $I(x) \in E^*$.

- I est linéaire.
- I est injective car $\langle y \mid x\rangle = 0$, pour tout y, exige $x = 0$.
- La conclusion résulte donc de $\dim E = \dim E^*$.

Remarque

Cet isomorphisme I transforme une base orthonormale en sa base duale.

Copyrighted material

En effet, si $(e_i)_{1\leqslant i\leqslant n}$ est une base orthonormale, les formes coordonnées de cette base (c'est-à-dire les éléments de la base duale) sont les applications :

$$e_i^* : x \mapsto \langle x \mid e_i \rangle \quad \text{donc} \quad e_i^* = I(e_i).$$

Corollaire 1

Pour toute forme linéaire θ de E, il existe un unique vecteur a de E tel que :

$$\forall x \in E,\ \theta(x) = \langle x \mid a \rangle.$$

Ce vecteur est $a = I^{-1}(\theta)$.

Corollaire 2

Un vecteur x de E est entièrement déterminé par ses produits scalaires avec les vecteurs d'une base $(e_i)_{1\leqslant i\leqslant n}$ quelconque.

☞ Cela revient à montrer que pour toute base $\mathcal{B} = (e_i)_{1\leqslant i\leqslant n}$ de E et tout $(\alpha_1, \cdots, \alpha_n) \in \mathbb{R}^n$, il existe un unique vecteur x de E vérifiant :

$$\forall i \in [\![1, n]\!], \langle x \mid e_i \rangle = \alpha_i.$$

Notons $(e_i^*)_{1\leqslant i\leqslant n}$ la base duale de $(e_i)_{1\leqslant i\leqslant n}$.

La condition $\forall i \in [\![1, n]\!],\ \langle x \mid e_i \rangle = \alpha_i$ se lit $\forall i \in [\![1, n]\!],\ I(x)(e_i) = \alpha_i$ et elle équivaut donc à : $I(x) = \sum_{i=1}^{n} \alpha_i e_i^*$. ✎(4)

✎(4) Les coordonnées sur $(e_i^*)_{1\leqslant i\leqslant n}$ d'une forme linéaire f sont les $f(e_i)$, $1 \leqslant i \leqslant n$.

D'où l'existence et l'unicité de x avec $x = I^{-1}(\theta)$ où l'on a posé $\theta = \sum_{i=1}^{n} \alpha_i e_i^*$.

3. Orthogonalité, perpendicularité, écart angulaire

Définition 2

On dit que des sous-espaces F et G de E euclidien sont **perpendiculaires** si les trois propriétés équivalentes sont vérifiées :

(1) $F^\perp \subset G$ (2) $G^\perp \subset F$ (3) $F^\perp$ et $G^\perp$ sont orthogonaux.

Définition 3

L'**écart angulaire** de deux vecteurs non nuls u et v de E est le réel :

$$\theta(u, v) = \operatorname{Arccos} \frac{\langle u \mid v \rangle}{\|u\| \cdot \|v\|} \in [0, \pi].$$

L'écart angulaire de deux droites $\mathcal{D} = \mathbb{R}u$ et $\mathcal{D}' = \mathbb{R}u'$ de E est le réel ✎(5)

$$\theta(\mathcal{D}, \mathcal{D}') = \operatorname{Arccos} \frac{|\langle u \mid u' \rangle|}{\|u\| \cdot \|u'\|} \in \left[0, \frac{\pi}{2}\right].$$

✎(5) $\theta(\mathcal{D}, \mathcal{D}') = \theta(u, u')$ si $\theta(u, u') \in \left[0, \frac{\pi}{2}\right]$.
$\theta(\mathcal{D}, \mathcal{D}') = \pi - \theta(u, u')$ si $\theta(u, u') \in \left[\frac{\pi}{2}, \pi\right]$.

Définition 4

L'écart angulaire de deux hyperplans $\mathcal{H} = (\mathbb{R}u)^\perp$ et $\mathcal{H}' = (\mathbb{R}u')^\perp$ de E est le réel :

$$\theta(\mathcal{H}, \mathcal{H}') = \operatorname{Arccos} \frac{|\langle u \mid u' \rangle|}{\|u\| \cdot \|u'\|} \in \left[0, \frac{\pi}{2}\right].$$

L'écart angulaire d'une droite $\mathcal{D} = \mathbb{R}u$ et d'un hyperplan $\mathcal{H} = (\mathbb{R}v)^\perp$ de E est le réel :

$$\theta(\mathcal{D}, \mathcal{H}) = \operatorname{Arcsin} \frac{|\langle u \mid v \rangle|}{\|u\| \cdot \|v\|} \in \left[0, \frac{\pi}{2}\right].$$

Copyrighted material

Remarques

1) L'inégalité de Schwarz donne $\dfrac{\langle u \mid v \rangle}{\|u\| \cdot \|v\|} \in [-1, 1]$, ce qui justifie ces définitions.

2) Dans le cas de droites ou hyperplans, l'écart angulaire ne dépend pas du vecteur choisi pour diriger une droite ou l'orthogonal d'un hyperplan.

Exemple 2 Il n'existe pas trois vecteurs d'un espace euclidien E dont les écarts angulaires deux à deux dépassent $\dfrac{2\pi}{3}$.

Soit trois vecteurs u_1, u_2, u_3, supposés normés, tels que $\langle u_i \mid u_j \rangle < -\dfrac{1}{2}$, pour $(1 \leqslant i < j \leqslant 3)$.

On a alors $\| u_1 + u_2 + u_3 \|^2 = \sum_{i=1}^{3} \| u_i \|^2 + 2 \sum_{1 \leqslant i < j \leqslant 3} \langle u_i \mid u_j \rangle < 3 + 2 \times 3 \times \left(-\dfrac{1}{2} \right) = 0.$

Ce qui est absurde.

B. Adjoint d'un endomorphisme Endomorphismes remarquables

E est un espace euclidien de dimension $n \geqslant 1$ et $\mathcal{B} = (e_j)_{1 \leqslant j \leqslant n}$ est une base orthonormale de E.

1. Adjoint d'un endomorphisme

Théorème 3

Pour tout endomorphisme $f \in \mathcal{L}(E)$, il existe une unique application f^* de E dans E telle que :

$$\forall (x, y) \in E^2, \quad \langle f(x) \mid y \rangle = \langle x \mid f^*(y) \rangle.$$

☞ Avec les notations du théorème 2, I désigne l'isomorphisme canonique de E sur E^*.

▪ Analyse

Supposons qu'il existe $g \in \mathcal{L}(E)$ tel que :

$$\forall (x, y) \in E^2, \langle f(x) \mid y \rangle = \langle x \mid g(y) \rangle.$$

Pour tout y fixé dans E, notons F_y l'application $x \mapsto \langle f(x) \mid y \rangle$; F_y est linéaire en tant que composée d'applications linéaires, donc $F_y \in E^*$. On a alors :

$$\forall (x, y) \in E^2, \quad F_y(x) = \langle x \mid g(y) \rangle = I\big(g(y)\big)(x)$$

donc $\forall y \in E, F(y) = I\big(g(y)\big)$ soit aussi :

$$\forall y \in E, g(y) = I^{-1}\big(F_y\big).$$

En conséquence, la seule solution possible du problème est l'application :

$$g : y \mapsto I^{-1}\big(F_y\big).$$ ✎(6)

✎(6) On a prouvé l'unicité sous réserve d'existence.

▪ Synthèse

La bilinéarité du produit scalaire montre que $y \mapsto F_y$ est linéaire et donc $g : y \mapsto I^{-1}\big(F_y\big)$ est linéaire comme composée d'applications linéaires : $g \in \mathcal{L}(E)$.

On a de plus :

$$\forall y \in E, I\big(g(y)\big) = F(y),$$

donc $\forall (x, y) \in E^2, \langle x \mid g(y) \rangle = F_y(x) = \langle f(x) \mid y \rangle$. ✎(7)

✎(7) Ce qui montre l'existence d'une solution.

L'application g est bien (l'unique) solution du problème et, au passage, on a montré que g est linéaire.

Copyrighted material

Définition 5

L'endomorphisme f^* associé à f par le théorème 3 s'appelle l'**adjoint** de f.

Définition 6

Un automorphisme $f \in \mathrm{GL}(E)$ est dit **orthogonal** lorsque $f^* = f^{-1}$, c'est-à-dire

$$\forall (x, y) \in E^2,\ \langle f(x) \,|\, y \rangle = \langle x \,|\, f^{-1}(y) \rangle.$$

Définition 7

Un endomorphisme $f \in \mathscr{L}(E)$ est dit :

- **symétrique** si $f^* = f$, c'est-à-dire $\forall (x, y) \in E^2,\ \langle f(x) \,|\, y \rangle = \langle x \,|\, f(y) \rangle$;
- **antisymétrique** si $f^* = -f$, c'est-à-dire $\forall (x, y) \in E^2,\ \langle f(x) \,|\, y \rangle = -\langle x \,|\, f(y) \rangle$.

Propriété 6

L'application $f \mapsto f^*$ (adjonction) est un endomorphisme involutif de $\mathscr{L}(E)$:

$$\forall (\alpha, \beta) \in \mathbb{R}^2,\ \forall (f, g) \in \mathscr{L}(E)^2,\ \begin{cases} (\alpha f + \beta g)^* = \alpha f^* + \beta g^* & \textbf{(1)} \\ (f^*)^* = f & \textbf{(2)} \end{cases}$$

☞ **(1)** Il suffit de vérifier que $\forall (x, y) \in E^2$:

$$\langle \alpha f(x) + \beta g(x) \,|\, y \rangle = \langle x \,|\, \alpha f^*(y) + \beta g^*(y) \rangle$$

et en effet
$$\begin{aligned} \langle \alpha f(x) + \beta g(x) \,|\, y \rangle &= \alpha \langle f(x) \,|\, y \rangle + \beta \langle g(x) \,|\, y \rangle \\ &= \alpha \langle x \,|\, f^*(y) \rangle + \beta \langle x \,|\, g^*(y) \rangle \\ &= \langle x \,|\, \alpha f^*(y) + \beta g^*(y) \rangle \end{aligned}$$

(2) La relation $\forall (x, y) \in E^2,\ \langle f^*(y) \,|\, x \rangle = \langle y \,|\, f(x) \rangle$ donne $f = (f^*)^*$.

Propriété 7

Image et noyau de l'adjoint

Pour tout $f \in \mathscr{L}(E)$, on a :

$$\mathrm{Ker}\, f^* = (\mathrm{Im}\, f)^\perp. \qquad \textbf{(1)}$$

et
$$\mathrm{Im}\, f^* = (\mathrm{Ker}\, f)^\perp. \qquad \textbf{(2)}$$

☞ **(1)** Utilisons que $u = 0_E \iff \forall v \in E,\ \langle u \,|\, v \rangle = 0$, il vient :

$$\begin{aligned} f^*(x) = 0_E &\iff \forall y \in E,\ \langle f^*(x) \,|\, y \rangle = 0 \\ &\iff \forall y \in E,\ \langle x \,|\, f(y) \rangle = 0 \end{aligned}$$

Donc $x \in \mathrm{Ker}\, f^* \iff x \in (\mathrm{Im}\, f)^\perp$.

(2) En appliquant **(1)** à f^* il vient :

$$\mathrm{Ker}\,(f^*)^* = (\mathrm{Im}\, f^*)^\perp \quad \text{c'est-à-dire} \quad \mathrm{Ker}\, f = (\mathrm{Im}\, f^*)^\perp$$

d'où $(\mathrm{Ker}\, f)^\perp = (\mathrm{Im}\, f^*)^{\perp\perp} = \mathrm{Im}\, f^*$.

Propriété 8

Adjoint d'un composé, d'un inverse

a) Pour tout $(f, g) \in \mathscr{L}(E)^2$: $(g \circ f)^* = f^* \circ g^*$.

b) $(\mathrm{Id}_E)^* = \mathrm{Id}_E$.

c) Pour tout $f \in \mathrm{GL}(E)$: $f^* \in \mathrm{GL}(E)$ et $(f^{-1})^* = (f^*)^{-1}$.

Copyrighted material

a) Pour tout $(x, y) \in E^2$, on a : $\langle g \circ f(x) \,|\, y \rangle = \langle f(x) \,|\, g^*(y) \rangle = \langle x \,|\, f^* \circ g^*(y) \rangle$, donc :

$$(g \circ f)^* = f^* \circ g^*.$$

b) C'est évident.

c) D'après b), $(f^{-1} \circ f)^* = \mathrm{Id}_E$ donc avec a), $f^* \circ (f^{-1})^* = \mathrm{Id}_E$ et il en résulte que f^* est inversible avec :

$$(f^*)^{-1} = (f^{-1})^*.$$

Propriété 9

Matrice de l'adjoint dans une base orthonormale

Soit $f \in \mathcal{L}(E)$, $g \in \mathcal{L}(E)$ et $\mathcal{B} = (e_j)_{1 \leqslant j \leqslant n}$ une base orthonormale [8] de E.

On a alors $g = f^*$ si et seulement si $\mathrm{mat}_{\mathcal{B}} g = {}^t \mathrm{mat}_{\mathcal{B}} f$. [9]

[8] Hypothèse indispensable.

[9] Ce résultat aurait pu être démontré immédiatement après la définition 5, ce qui permet de déduire les propriétés 6 et 8 des propriétés connues de la transposition matricielle.

Par définition, $g = f^*$ équivaut à : $\forall (x, y) \in E^2, \langle f(x) \,|\, y \rangle = \langle x \,|\, g(y) \rangle$. Donc $g = f^*$ donne :

$$\forall (i, j) \in [\![1, n]\!]^2, \langle f(e_i) \,|\, e_j \rangle = \langle e_i \,|\, g(e_j) \rangle$$

et il en résulte $\mathrm{mat}_{\mathcal{B}} g = {}^t \mathrm{mat}_{\mathcal{B}} f$ car $e_i^* (f(e_j))$ (resp. $e_i^* (g(e_j))$) est le terme général de $\mathrm{mat}_{\mathcal{B}} f$ (resp. $\mathrm{mat}_{\mathcal{B}} g$) et, la base $\mathcal{B}$ étant orthonormale, on a :

$$e_i^* (f(e_j)) \quad (\text{resp. } e_i^* (g(e_j)) = \langle e_i \,|\, g(e_j) \rangle.$$

Réciproquement, supposons $\mathrm{mat}_{\mathcal{B}} f = A$, $\mathrm{mat}_{\mathcal{B}} g = {}^t A$. En posant pour tout $(x, y) \in E^2$, $X = \mathrm{mat}_{\mathcal{B}}(x)$ et $Y = \mathrm{mat}_{\mathcal{B}}(y)$, on a :

$$\mathrm{mat}_{\mathcal{B}} (f(x)) = AX \text{ et } \mathrm{mat}_{\mathcal{B}} (g(y)) = {}^t AY$$

donc, la base $\mathcal{B}$ étant orthonormale, il vient :

$$\langle x \,|\, g(y) \rangle = {}^t ({}^t AY) X = {}^t YAX = \langle f(x) \,|\, y \rangle$$

ce qui prouve que $g = f^*$.

Propriété 10

Polynôme caractéristique – Diagonalisation

Un endomorphisme et son adjoint ont le même polynôme caractéristique ; si l'un est diagonalisable, l'autre l'est aussi.

C'est un corollaire de la propriété précédente.

Propriété 11

Si F est un sous-espace de E stable par $f \in \mathcal{L}(E)$, alors son orthogonal $F^\perp$ est stable par f^*.

Soit $y \in F^\perp$. Pour tout $x \in F$, on a $f(x) \in F$ et donc $\langle y \,|\, f(x) \rangle = 0$, d'où $\langle f^*(y) \,|\, x \rangle = 0$, ce qui montre que $f^*(y)$ appartient à $F^\perp$.

Exemple 3 Étant donné $f \in \mathcal{L}(E)$, E espace euclidien, $\mathrm{Ker}\,(f^* \circ f) = \mathrm{Ker}\, f$ et $\mathrm{Im}\,(f^* \circ f) = \mathrm{Im}\,(f^*)$.

a) $\mathrm{Ker}\,(f^* \circ f) \supset \mathrm{Ker}\, f$ est une relation connue.

Soit $x \in \mathrm{Ker}\,(f^* \circ f)$.

De $(f^* \circ f)(x) = 0_E$, on déduit $\langle (f^* \circ f)(x) \,|\, x \rangle = 0$, c'est-à-dire $\langle f(x) \,|\, f(x) \rangle = 0$, soit $\|f(x)\|^2 = 0$ puis $f(x) = 0_E$.

On a donc $\mathrm{Ker}\,(f^* \circ f) \subset \mathrm{Ker}\, f$ et enfin $\mathrm{Ker}\,(f^* \circ f) = \mathrm{Ker}\, f$.

b) On a $\mathrm{Im}\,(f^* \circ f) = \left[\mathrm{Ker}\,(f^* \circ f)^*\right]^\perp = \left[\mathrm{Ker}\,(f^* \circ f)\right]^\perp = \left[\mathrm{Ker}\, f\right]^\perp = \mathrm{Im}\, f^*$.

Compléments

En échangeant les rôles de f et f^*, avec $(f^*)^* = f$, il vient :

$$\mathrm{Ker}\,(f \circ f^*) = \mathrm{Ker}\,(f^*) \text{ et } \mathrm{Im}\,(f \circ f^*) = \mathrm{Im}\, f.$$

Copyrighted material

The Final Days of Tony Blair

For a battler like Mr Blair, who has a strong and often admirable conviction that he is right and his opponents wrong, it will always be hard to stand down. That may be especially true just when he has won a parliamentary vote, on school reforms that, even in their watered-down form, he holds dear.

His reluctance will be reinforced by his own doubts about whether his all-but-inevitable successor, Gordon Brown, will really carry on his reforms in health and education, and by his natural resentment at Mr Brown's often disruptive and petulant behaviour during their nine years in office together.

And there is Iraq, the invasion of which has its third anniversary on March 19th: Mr Blair's decision to take part in that venture is the single biggest reason why he is loathed by many Labour MPs but also the main reason why he is so admired across the Atlantic. Little by little, British troops are being withdrawn from the relatively peaceful areas of southern Iraq in which they have been based. No doubt Mr Blair would prefer to stay on until he can say that the British job has been done and the withdrawal has been a success.

(206 mots)

The Economist – 16th March 2006.

Copyrighted material

$$\langle f(x) \,|\, f(y)\rangle = \frac{1}{4}\left(\|f(x+y)\|^2 - \|f(x-y)\|^2\right) \quad (f \text{ est linéaire})$$
$$= \frac{1}{4}\left(\|x+y\|^2 - \|x-y\|^2\right) \quad (\text{d'après } (2))$$
$$= \langle x \,|\, y\rangle.$$

(12) $f(x) = 0_E$ donne $x = 0_E$ car E est de dimension finie.

(1) ⇒ (3) : si l'endomorphisme f vérifie **(1)** (donc **(2)**), il est injectif (12) donc bijectif. (13) On a alors :

$$\forall (x, y) \in E^2,\ \langle f(x) \,|\, f(f^{-1}(y))\rangle = \langle x \,|\, f^{-1}(y)\rangle$$

c'est-à-dire $\forall (x, y) \in E^2,\ \langle f(x) \,|\, y\rangle = \langle x \,|\, f^{-1}(y)\rangle$ donc $f^{-1} = f^*$ et $f \in \mathcal{O}(E)$.

(3) ⇒ (1) : si $f \in \mathcal{O}(E)$, on a $\forall (x, y) \in E^2,\ \langle f(x) \,|\, f(y)\rangle = \langle x \,|\, f^{-1}(f(y))\rangle = \langle x \,|\, y\rangle$.

Exemple 5 Une application qui conserve le produit scalaire est linéaire.

Pour tout $(x, y) \in E^2$ et tout $\alpha \in \mathbb{R}$:

$$\begin{aligned}\|f(\alpha x + y) - \alpha f(x) - f(y)\|^2 &= \|f(\alpha x + y)\|^2 + \alpha^2\|f(x)\|^2 + \|f(y)\|^2 \\ &\quad - 2\alpha\langle f(\alpha x + y) \,|\, f(x)\rangle - 2\langle f(\alpha x + y) \,|\, f(y)\rangle \\ &\quad + 2\alpha\langle f(x) \,|\, f(y)\rangle \\ &= \|\alpha x + y\|^2 + \alpha^2\|x\|^2 + \|y\|^2 \\ &\quad - 2\alpha\langle \alpha x + y \,|\, x\rangle - 2\langle \alpha x + y \,|\, y\rangle + 2\alpha\langle x \,|\, y\rangle \\ &= 0\end{aligned}$$

Ce qui montre que $\forall \alpha \in \mathbb{R},\ \forall (x, y) \in E^2,\ f(\alpha x + y) = \alpha f(x) + f(y)$.

Propriété 13

Un endomorphisme f de E est orthogonal si et seulement si l'image par f d'une base orthonormale est une base orthonormale.

a) Supposons f orthogonal. Étant donné $\mathcal{B} = (e_1, \ldots, e_n)$ une base orthonormale de E, (14) $\langle f(e_i) \,|\, f(e_j)\rangle = \langle e_i \,|\, e_j\rangle = \delta_{ij}$ montre que $f(\mathcal{B})$ est une base orthonormale de E.

(14) Conservation du produit scalaire.

b) Supposons que $f \in \mathcal{L}(E)$ transforme une base orthonormale $(e_i)_{1 \leqslant i \leqslant n}$ en une base orthonormale $(f(e_i))_{1 \leqslant i \leqslant n}$, f est donc un automorphisme de E.

Pour $x = \sum_{k=1}^{n} x_k e_k$, on a $f(x) = \sum_{k=1}^{n} x_k f(e_k)$.

Les bases $(e_1, \ldots, e_n)$ et $(f(e_1), \ldots, f(e_n))$ étant orthonormales, il vient :

$$\|x\|^2 = \sum_{k=1}^{n} x_k^2 \quad \text{et} \quad \|f(x)\|^2 = \sum_{k=1}^{n} x_k^2.$$

Ainsi f est linéaire et conserve la norme, c'est donc un automorphisme orthogonal.

Propriété 14

Un endomorphisme f de E est orthogonal si et seulement si sa matrice M dans une base orthonormale $\mathcal{B}$ vérifie ${}^tMM = I_n$.

La proposition $\forall x \in E,\ \|f(x)\|^2 = \|x\|^2$ équivaut à :

$$\forall X \in \mathcal{M}_{n,1}(\mathbb{R}),\ {}^t(MX)MX = {}^tXX$$

c'est-à-dire $\forall X \in \mathcal{M}_{n,1}(\mathbb{R}),\ {}^tX\,{}^tMMX = {}^tXX$ ou encore à ${}^tMM = I_n$.

Copyrighted material

Propriété 15

Symétries orthogonales et réflexions

a) Toute symétrie orthogonale, en particulier toute réflexion, est un automorphisme orthogonal de E.

b) Étant donné deux vecteurs a et b unitaires et distincts, il existe une réflexion et une seule les échangeant.

Il s'agit de la réflexion d'hyperplan $H = (b-a)^\perp$, on la note $s_{a,b}$.

En posant $u = \dfrac{b-a}{\|b-a\|}$, on a : $\forall x \in E,\ \ s_{a,b}(x) = x - 2\langle u \,|\, x\rangle u$.

c) Étant donné deux droites distinctes $\mathbb{R}a$ et $\mathbb{R}b$ où a et b sont des vecteurs unitaires, il existe deux réflexions les échangeant, il s'agit de $s_{a,b}$ et $s_{a,-b}$.

☞ a) Voir chapitre 6, Projections et symétries.

b) Si s est une réflexion d'hyperplan H échangeant a et b, on a :

$$s(b-a) = s(b) - s(a) = a - b$$

donc $b - a \in \mathrm{Ker}\left(s + \mathrm{Id}_E\right)$ c'est-à-dire $b - a \in H^\perp$.

Comme $H^\perp$ est une droite et, $b-a$ étant non nul, il vient $H^\perp = \mathbb{R}(b-a)$ donc $H = (b-a)^\perp$.

Réciproquement, considérons la réflexion s d'hyperplan $H = (b-a)^\perp$. ✎(15)

Avec $\langle b-a \,|\, b+a\rangle = \|b\|^2 - \|a\|^2 = 0$, il vient que $b + a \in H$.

Sachant que $H = \mathrm{Ker}\left(s - \mathrm{Id}_E\right)$ et $H^\perp = \mathrm{Ker}\left(s + \mathrm{Id}_E\right)$, on a maintenant :

$$s(b+a) = b + a \ \text{ et } \ s(b-a) = a - b$$

c'est-à-dire $s(b) + s(a) = b + a$ et $s(b) - s(a) = a - b$ d'où l'on tire :

$$s(a) = b \ \text{ et } \ s(b) = a.$$

Enfin, p désignant la projection orthogonale sur $H^\perp$, on sait que $s = \mathrm{Id}_E - 2p$.

Donc, en posant $u = \dfrac{b-a}{\|b-a\|}$, il vient : $\forall x \in E,\ \ s(x) = x - 2\langle u \,|\, x\rangle u$.

c) Il suffit de noter que a et b étant unitaires, l'image de a doit être b ou $-b$.

✎(15) C'est la seule solution possible.

Remarques

- Une symétrie orthogonale est un automorphisme orthogonal.
- En dehors du cas particulier de l'identité, une projection orthogonale n'est pas un automorphisme orthogonal.

Propriété 16

On rappelle qu'une isométrie de E est une application $g : E \to E$ telle que :

$$\forall (x, y) \in E^2,\ \ \|g(x) - g(y)\| = \|x - y\|.$$

Une application $g : E \to E$ est une isométrie si et seulement si il existe un couple (t, f) où t est une translation et $f \in \mathcal{O}(E)$ tel que $g = t \circ f$.

☞ ✎(16) Soit g une isométrie et t la translation de vecteur $g(0)$.

Alors, $f = t^{-1} \circ g$ est une isométrie telle que $f(0) = 0$.

Le choix de $y = 0$ dans $\|f(x) - f(y)\| = \|x - y\|$ montre que f conserve la norme.

On en déduit que f conserve le produit scalaire. En effet,

$$\text{pour tout } (x, y) \in E^2, \text{ on a } \ \|f(x) - f(y)\|^2 = \|x - y\|^2$$

c'est-à-dire $\|f(x)\|^2 - 2\langle f(x) \,|\, f(y)\rangle + \|f(y)\|^2 = \|x\|^2 - 2\langle x \,|\, y\rangle + \|y\|^2$ et donc :

$$\langle f(x) \,|\, f(y)\rangle = \langle x \,|\, y\rangle.$$

Il en résulte enfin que f est linéaire. ✎(17)

✎(16) Une translation et un automorphisme orthogonal sont des isométries. Il en est donc de même pour leur composé. Seule la réciproque est à prouver.

✎(17) Voir l'exemple 4.

Copyrighted material

Propriété 17

Propriétés des automorphismes orthogonaux

Soit $f \in \mathcal{O}(E)$.

a) Le spectre de f est inclus dans $\{-1, 1\}$.

Les sous-espaces propres de f, $\mathrm{Ker}\,(f - \mathrm{Id}_E)$ et $\mathrm{Ker}\,(f + \mathrm{Id}_E)$, sont orthogonaux.

b) Le déterminant de f est $+1$ ou -1.

c) Si f est diagonalisable, f est une symétrie orthogonale.

d) Si F est un sous-espace de E stable par f, alors $F^\perp$ est stable par f.

☞ a) Soit $\lambda \in \mathrm{Sp}(f)$: il existe $x \in E \setminus \{0\}$, $f(x) = \lambda x$ donc $\|x\| = |\lambda| \|x\|$ puis $|\lambda| = 1$.
Si $x \in \mathrm{Ker}\,(f - \mathrm{Id}_E)$ et $y \in \mathrm{Ker}\,(f + \mathrm{Id}_E)$, on a $f(x) = x$ et $f(y) = -y$ donc :

$$\langle x \,|\, y \rangle = -\langle f(x) \,|\, f(y) \rangle.$$

Or $\langle f(x) \,|\, f(y) \rangle = \langle x \,|\, y \rangle$ d'où finalement $\langle x \,|\, y \rangle = 0$.

b) $(\det f)^2 = 1$ découle du théorème (4).

c) est un corollaire de a).

d) Si F est stable par f alors $F^\perp$ est stable par f^* (propriété 11).
Or $f^* = f^{-1}$ donc $F^\perp$ est stable par f^{-1} et donc aussi par f.

Notation 1

$\mathcal{SO}(E)$ [18] est aussi noté $\mathcal{O}^+(E)$. Ses éléments sont les **rotations** de E.
L'ensemble $\mathcal{O}(E) \setminus \mathcal{SO}(E)$ est aussi noté $\mathcal{O}^-(E)$. Ses éléments sont les automorphismes orthogonaux de E, de déterminant -1, encore appelés **antirotation**.

[18] Groupe spécial orthogonal.

3. Matrices orthogonales

Théorème 5

a) L'ensemble des matrices $M \in \mathcal{M}_n(\mathbb{R})$ vérifiant ${}^tM \cdot M = I_n$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$, appelé **groupe orthogonal réel d'ordre** n, il est noté $\mathcal{O}_n(\mathbb{R})$.

b) L'ensemble $\{M \in \mathcal{O}_n(\mathbb{R}) / \det M = 1\}$ est un sous-groupe de $\mathcal{O}_n(\mathbb{R})$, appelé **groupe spécial orthogonal réel d'ordre** n, il est noté $\mathcal{SO}_n(\mathbb{R})$.

[19] La démonstration matricielle directe est facile.

[19] On peut déduire ces résultats du théorème 4 et de la propriété 14, en observant qu'une base orthonormale $\mathcal{B}$ étant fixée, l'application :

$$\mathrm{mat}_{\mathcal{B}} : \mathcal{L}(E) \to \mathcal{M}_n(\mathbb{R}), \quad f \mapsto \mathrm{mat}_{\mathcal{B}} f$$

induit un isomorphisme de $\mathcal{O}(E)$ sur $\mathcal{O}_n(\mathbb{R})$ (resp. de $\mathcal{SO}(E)$ sur $\mathcal{SO}_n(\mathbb{R})$).

Propriété 18

Caractérisation des matrices orthogonales

Les propositions suivantes sont équivalentes :

(1) $M \in \mathcal{O}_n(\mathbb{R})$, **(2)** ${}^tM \in \mathcal{O}_n(\mathbb{R})$, **(3)** ${}^tM \cdot M = I_n$, **(4)** $M \cdot {}^tM = I_n$,

(5) Le système des vecteurs colonnes (resp. lignes) de M est une base orthonormale de $\mathbb{R}^n$ muni de sa structure euclidienne canonique.

(6) Étant donné E espace euclidien de dimension n muni d'une base orthonormale $\mathcal{B}_0$, il existe une base orthonormale $\mathcal{B}_1$ telle que M soit la matrice de passage de $\mathcal{B}_0$ à $\mathcal{B}_1$. [20]

[20] On résume usuellement cet énoncé en disant que M est une matrice de changement de base orthonormale.

Copyrighted material

Propriété 19

Propriétés des matrices orthogonales

Soit $M \in \mathcal{O}_n(\mathbb{R})$.

a) Le spectre de M est inclus dans $\{-1, 1\}$.

b) Le déterminant de M est 1 ou -1.

☞ Soit $f_M \in \mathcal{L}(\mathbb{R}^n)$ canoniquement associé à M.

$\mathbb{R}^n$ étant muni de sa structure euclidienne canonique, f_M est orthogoanl : $f_M \in \mathcal{O}(\mathbb{R}^n)$. La propriété découle donc de $\mathrm{Sp}(f_M) \subset \{-1, 1\}$ et $(\det f_M)^2 = 1$. ✎(21)

✎(21) Propriété 17.

Notation 2

$\mathcal{SO}_n(\mathbb{R})$ ✎(22) est aussi noté $\mathcal{O}_n^+(\mathbb{R})$. Ses éléments sont les matrices de rotation.

L'ensemble $\mathcal{O}_n(\mathbb{R}) \setminus \mathcal{SO}_n(\mathbb{R})$ est aussi noté $\mathcal{O}_n^-(\mathbb{R})$. Ses éléments sont les matrices orthogonales, de déterminant -1, encore appelées matrices d'antirotation.

✎(22) Groupe spécial orthogonal d'ordre n.

Exemple 6 Déterminant d'une matrice orthogonale à l'aide de la comatrice.

Pour toute matrice carrée M, on a ${}^t(\mathrm{com}\, M)M = (\det M)I_n$.

Avec $M \in \mathcal{O}_n(\mathbb{R})$, on a $M^{-1} = {}^t M$, d'où ${}^t(\mathrm{com}\, M) = (\det M)\,{}^t M$ puis $\mathrm{com}\, M = (\det M)M$.

Il suffit donc de comparer les signes d'un terme non nul de M et de son cofacteur pour voir si $\det M = 1$ ou $\det M = -1$.

Exemple 7 Étant donné $A \in \mathcal{O}_n(\mathbb{R})$ de terme général a_{ij}, $\left|\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\right| \leqslant n$. Étude des cas d'égalité.

$(e_i)_{1 \leqslant i \leqslant n}$ désignant la base canonique de $\mathbb{R}^n$, posons $u = \sum_{i=1}^{n} e_i$.

Notons $c_1, c_2, \ldots, c_n$ les vecteurs colonnes de A : $c_j = \sum_{i=1}^{n} a_{ij} e_i$.

On a alors ✎(23) $\sum_{i=1}^{n} a_{ij} = \langle c_j \mid u \rangle$ donc $\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij} = \sum_{j=1}^{n} \langle c_j \mid u \rangle = \left\langle \sum_{j=1}^{n} c_j \,\middle|\, u \right\rangle$.

Il vient alors ✎(24) $\left|\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\right|^2 \leqslant \left\|\sum_{j=1}^{n} c_j\right\|^2 \|u\|^2$ puis : ✎(25)

$$\left\|\sum_{j=1}^{n} c_j\right\|^2 = \sum_{j=1}^{n} \|c_j^2\| = n \quad \text{d'où} \quad \left|\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\right|^2 \leqslant n^2.$$

L'égalité a lieu si et seulement si $\left(\sum_{j=1}^{n} c_j,\ u\right)$ est lié.

Or, f désignant l'endomorphisme de $\mathbb{R}^n$ associé à A dans la base canonique, on a $\sum_{j=1}^{n} c_j = f(u)$, donc l'égalité a lieu si et seulement si u est vecteur propre de f, c'est-à-dire si et seulement si $f(u) = u$ ou $f(u) = -u$ ou encore :

$$\forall i \in [\![1, n]\!],\ \sum_{j=1}^{n} a_{ij} = 1 \quad \text{ou} \quad \forall i \in [\![1, n]\!],\ \sum_{j=1}^{n} a_{ij} = -1.$$

✎(23) Dans $\mathbb{R}^n$ euclidien canonique.

✎(24) Inégalité de Cauchy-Schwarz.

✎(25) Le système $(c_j)_{1 \leqslant j \leqslant n}$ est orthonormal.

Copyrighted material

Exemple 4 Soit $E = \mathcal{M}_{n,p}(\mathbb{R})$ muni du produit scalaire $\forall (X, Y) \in E^2,\ \langle X \mid Y \rangle = \mathrm{Tr}\left({}^tXY\right)$.

Pour A fixée dans E, $\Phi_A : E \to E,\ X \mapsto AXA$ est un endomorphisme symétrique de E.

Observer que ${}^tX \in \mathcal{M}_{p,n}(\mathbb{R})$, donc le produit ${}^tXY$ existe et appartient à $\mathcal{M}_p(\mathbb{R})$, ce qui assure que $\mathrm{Tr}\left({}^tXY\right)$ a un sens.

On peut vérifier, comme on l'a fait précédemment dans le cas de $\mathcal{M}_n(\mathbb{R})$, que $(X, Y) \mapsto \mathrm{Tr}\left({}^tXY\right)$ est le produit scalaire euclidien canonique sur $\mathcal{M}_{n,p}(\mathbb{R})$.

$A \in \mathcal{M}_{n,p}(\mathbb{R})$, ${}^tX \in \mathcal{M}_{p,n}(\mathbb{R})$ donne $A{}^tX \in \mathcal{M}_{n,n}(\mathbb{R})$ puis $A{}^tXA \in \mathcal{M}_{n,p}(\mathbb{R})$: Φ_A est à valeurs dans E.

La linéarité de Φ_A est claire, donc $\Phi_A \in \mathcal{L}(E)$.

Il faut vérifier $\forall (X, Y) \in E^2,\ \langle \Phi_A(X) \mid Y \rangle = \langle X \mid \Phi_A(Y) \rangle$.

Formons donc $\langle \Phi_A(X) \mid Y \rangle = \mathrm{Tr}\left({}^tAX\,{}^tAY\right)$.

Les propriétés de l'application «trace» donnent alors :

$$\langle \Phi_A(X) \mid Y \rangle = \mathrm{Tr}\left({}^tYA\,{}^tXA\right) \quad \left(\mathrm{Tr}(M) = \mathrm{Tr}({}^tM)\right)$$

$$\langle \Phi_A(X) \mid Y \rangle = \mathrm{Tr}\left({}^tXA\,{}^tYA\right) \quad \mathrm{Tr}(MN) = \mathrm{Tr}(NM)$$

$$\langle \Phi_A(X) \mid Y \rangle = \langle X \mid \Phi_A(Y) \rangle.$$

d'où la conclusion.

2. Le groupe orthogonal d'un espace euclidien

Théorème 4

a) L'ensemble des automorphismes orthogonaux d'un espace euclidien E est un sous-groupe de $\mathrm{GL}(E)$, appelé **groupe orthogonal de E**, et noté $\mathcal{O}(E)$.

b) L'ensemble $\{f \in \mathcal{O}(E) / \det f = 1\}$ est un sous-groupe de $\mathcal{O}(E)$, appelé **groupe spécial orthogonal de E**, et noté $\mathcal{SO}(E)$.

☞ a) Utiliser $\left(\mathrm{Id}_E\right)^* = \mathrm{Id}_E$ et la propriété 8.

b) Sachant que $\det f^* = \det f$ (cf. propriété 9) si $f \in \mathcal{O}(E)$, on a $f^* = f^{-1}$ et $(\det f)^2 = 1$.
On constate alors que l'application $f \mapsto \det f$ induit un morphisme de groupes de $\mathcal{O}(E)$ dans $\{-1, 1\}$ dont $\mathcal{SO}(E)$ est le noyau.

Remarque

Les éléments de $\mathcal{SO}(E)$ s'appellent les **rotations** de E.

Propriété 12

Caractérisation des automorphismes orthogonaux

Soit $f \in \mathcal{L}(E)$. Les propositions suivantes sont équivalentes :

(1) $\forall (x, y) \in E^2,\ \langle f(x) | f(y) \mid = \rangle \langle x \mid y \rangle$; [10]

(2) $\forall x \in E,\ \|f(x)\| = \|x\|$; [11]

(3) $f \in \mathcal{O}(E)$.

[10] On dit que f conserve le produit scalaire.

[11] On dit que f conserve la norme.

☞ **(1)** $\Rightarrow$ **(2)** : évident (faire $y = x$ dans **(1)**).

(2) $\Rightarrow$ **(1)** : $\langle f(x) \mid f(y) \rangle = \frac{1}{4}\left(\|f(x) + f(y)\|^2 - \|f(x) - f(y)\|^2\right)$.

Copyrighted material

Propriété 23

Caractérisation matricielle

L'endomorphisme f est symétrique (resp. antisymétrique) si et seulement si sa matrice dans une base orthonormale est symétrique (resp. antisymétrique). ✎(27)

✎(27) Dans une base orthonormale $\mathcal{B}$, $\mathrm{mat}_{\mathcal{B}} f^* = {}^t\mathrm{mat}_{\mathcal{B}} f$.

Propriété 24

Les sous-espaces $\mathcal{S}(E)$ et $\mathcal{A}(E)$

a) Les ensembles $\mathcal{S}(E)$ des endomorphismes symétriques et $\mathcal{A}(E)$ des endomorphismes antisymétriques sont des sous-espaces supplémentaires de $\mathcal{L}(E)$.

La décomposition de $f \in \mathcal{L}(E)$ sur la somme directe $\mathcal{S}(E) \oplus \mathcal{A}(E)$ est donnée par :

$$f = s + a \ , \ s = \frac{1}{2}(f + f^*) \in \mathcal{S}(E) \ , \ a = \frac{1}{2}(f - f^*) \in \mathcal{A}(E).$$

On dit que s est la partie symétrique de f et a la partie antisymétrique.

b) Une base orthonormale $\mathcal{B}$ étant donnée, l'application $f \mapsto \mathrm{mat}_{\mathcal{B}} f$ induit un isomorphisme de $\mathcal{S}(E)$ sur $\mathcal{S}_n(\mathbb{R})$ d'une part et de $\mathcal{A}(E)$ sur $\mathcal{A}_n(\mathbb{R})$ d'autre part.

c) $\dim \mathcal{S}(E) = \frac{1}{2}n(n+1)$, $\dim \mathcal{A}(E) = \frac{1}{2}n(n-1)$.

☞ a) ✎(28) $f^* = f$ et $f^* = -f$ donnent $f = 0$ donc $\mathcal{S}(E) \cap \mathcal{A}(E) = \{0\}$.

Tout $f \in \mathcal{L}(E)$ s'écrit $f = s + a$, $s = \frac{1}{2}(f + f^*)$, $a = \frac{1}{2}(f - f^*)$ et on a $s = s^*$, $a = -a^*$ donc $\mathcal{L}(E) = \mathcal{S}(E) \oplus \mathcal{A}(E)$.

b) ✎(29) L'image de $\mathcal{S}(E)$ (resp. $\mathcal{A}(E)$) par l'application $\mathrm{mat}_{\mathcal{B}}$ est $\mathcal{S}_n(\mathbb{R})$ (resp. $\mathcal{A}_n(\mathbb{R})$).

c) On sait que $\dim \mathcal{S}_n(\mathbb{R}) = \frac{1}{2}n(n+1)$, $\dim \mathcal{A}_n(\mathbb{R}) = \frac{1}{2}n(n-1)$.

✎(28) On vérifie facilement que $\mathcal{S}(E)$ et $\mathcal{A}(E)$ sont des sous-espaces vectoriels de $\mathcal{L}(E)$.

✎(29) Propriété 23.

Propriété 25

Projections et symétries

Un projecteur p (resp. une symétrie s) de E est orthogonal si et seulement si il est symétrique.

☞ Voir chapitre 6, propriétés 23 et 24.

Propriété 26

Propriétés des endomorphismes antisymétriques

a) Pour tout $f \in \mathcal{L}(E)$, on a : $f \in \mathcal{A}(E) \iff \forall x \in E, \langle f(x) \,|\, x \rangle = 0$.

b) Pour $f \in \mathcal{A}(E)$, 0 est la seule valeur propre éventuelle de f.

c) L'image et le noyau de $f \in \mathcal{A}(E)$ sont supplémentaires orthogonaux.

d) Si F est un sous-espace de E stable par $f \in \mathcal{A}(E)$, alors $F^\perp$ est stable par f.

e) Le rang de $f \in \mathcal{A}(E)$ est pair.

f) Si f est antisymétrique, alors $f \circ f$ est symétrique.

☞ a) Si $f \in \mathcal{A}(E)$, $\langle f(x) \,|\, x \rangle = -\langle f(x) \,|\, x \rangle$ donc $\langle f(x) \,|\, x \rangle = 0$.

Si $\forall x \in E$, $\langle f(x) \,|\, x \rangle = 0$ alors $\forall (x, y) \in E^2$, $\langle f(x+y) \,|\, x+y \rangle = 0$.

En développant, on obtient :

$$\langle f(x) \,|\, x \rangle + \langle f(x) \,|\, y \rangle + \langle f(y) \,|\, x \rangle + \langle f(y) \,|\, y \rangle = 0$$

d'où $\langle f(x) \,|\, y \rangle + \langle f(y) \,|\, x \rangle = 0$.

b) Si $\lambda \in \mathrm{Sp}(f)$, il existe $x \in E \setminus \{0\}$ tel que $f(x) = \lambda x$ et $\langle f(x) \,|\, x \rangle = 0$ donne :

$$\lambda \| x \|^2 = 0 \quad \text{d'où} \quad \lambda = 0.$$

Copyrighted material

Hidden page

Hidden page

Hidden page

2. Réduction dans le groupe orthogonal

Propriété 29

Soit E un $\mathbb{R}$-espace vectoriel de dimension $n \geqslant 1$, $\mathcal{B} = (e_i)_{1 \leqslant i \leqslant n}$ une base de E et q une forme quadratique sur E. Les propositions suivantes sont équivalentes.

(1) $\mathrm{mat}_{\mathcal{B}} q$ est diagonale.

(2) Pour tout $x \in E$, $x = \sum_{i=1}^{n} x_i e_i$, l'expression de $q(x)$ en fonction des x_i ne contient que des termes carrés. (41)

(41) Il n'apparaît aucun terme de la forme $x_i x_j$, $i \neq j$.

☞ Posons $A = [a_{ij}] = \mathrm{mat}_{\mathcal{B}} q$, on sait que $A \in \mathcal{S}_n(\mathbb{R})$ avec $\forall (i,j) \in [\![1, n]\!]^2$, $a_{ij} = \varphi(e_i, e_j)$ où φ est la forme polaire de q, et que pour tout $x = \sum_{i=1}^{n} x_i e_i$:

$$q(x) = \sum_{i=1}^{n} a_{i\,i} x_i^2 + 2 \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j .$$

En conséquence, l'expression de $q(x)$ ne contient que des termes carrés (quel que soit x) si et seulement si $\forall (i,j) \in [\![1, n]\!]^2$, $i \neq j \Rightarrow a_{ij} = 0$, donc si et seulement si A est diagonale.

Définition 9

Avec les notations de la propriété 29, une base $\mathcal{B}$ telle que $\mathrm{mat}_{\mathcal{B}} q$ soit diagonale est appelée une **base de réduction** de q. On dit aussi que q est **réduite** dans la base $\mathcal{B}$.

Théorème 10

Réduction d'une forme quadratique dans le groupe orthogonal

Soit q une forme quadratique sur un espace euclidien E ; il existe alors une base orthonormale de E dans laquelle q est réduite.

La détermination d'une telle base est appelée **réduction de q dans le groupe orthogonal** (de E).

☞ Soit f l'endomorphisme symétrique associé à q et $\mathcal{B} = (e_j)_{1 \leqslant j \leqslant n}$ une base orthonormale de E formée de vecteurs propres de f. (42)

On a alors $\mathrm{mat}_{\mathcal{B}} q = \mathrm{mat}_{\mathcal{B}} f = \mathrm{diag}(\lambda_1, \ldots, \lambda_n) = D$ où les réels $\lambda_1, \ldots, \lambda_n$ sont les valeurs propres de f.

En posant pour tout $x \in E$, $x = \sum_{j=1}^{n} x_j e_j$ on obtient alors $q(x) = \sum_{i=1}^{n} \lambda_i x_i^2$.

(42) L'existence d'une telle base résulte du théorème 6.

Corollaire 1

Endomorphismes symétriques positifs

Un endomorphisme symétrique sur E est **positif** (resp. **défini-positif**) c'est-à-dire que la forme quadratique associée est positive (resp. définie-positive) si et seulement si toutes ses valeurs propres sont positives (resp. strictement positives). (43)

(43) L'ensemble des endomorphismes symétriques positifs (resp. définis-positifs) de E sera noté $\mathcal{S}^+(E)$ (resp. $\mathcal{S}^{++}(E)$).

☞ On conserve les notations de la démonstration du théorème 10.

- Si q est positive (resp. définie-positive), on a :
$$\forall i \in [\![1, n]\!],\ \lambda_i = q(e_i) \geqslant 0 \quad (\text{resp. } \lambda_i = q(e_i) > 0).$$
- Si $\forall i \in [\![1, n]\!]$, $\lambda_i \geqslant 0$ (resp. $\lambda_i > 0$), il est clair que :
$$\forall x \in E \setminus \{0_E\},\ q(x) = \sum_{i=1}^{n} \lambda_i x_i^2 \geqslant 0 \quad (\text{resp. } q(x) = \sum_{i=1}^{n} \lambda_i x_i^2 > 0).$$

Copyrighted material

Hidden page

Théorème 12

Réduction simultanée de deux matrices symétriques réelles

Soit A et B deux matrices symétriques réelles d'ordre $n \geqslant 1$, l'une d'elles, par exemple A, étant définie-positive.

Alors il existe $P \in \mathrm{GL}_n(\mathbb{R})$ [45] telle que :

$$ {}^tPAP = I_n \quad \text{et} \quad {}^tPBP = D \quad \text{(diagonale)}. $$

[45] On remarquera que P n'est, en général, pas orthogonale, ceci ne pouvant se produire que si $A = I_n$.

☞ C'est la transcription matricielle du corollaire 2 du théorème 10.

Exemple 13 Réduction dans le groupe orthogonal de $\mathbb{R}^3$ euclidien canonique des formes quadratiques définies par : $q_1(u) = 2x^2 + 2y^2 + z^2 - 2yz + 2zx$.
$q_2(u) = 151x^2 - 119y^2 + 137z^2 - 192yz + 48zx + 144xy \quad u = (x, y, z)$.

La base canonique (e_1, e_2, e_3) est orthonormale. Pour chaque forme quadratique q_i, on note φ_i l'endomorphisme symétrique associé.

a) Avec $A = \mathrm{mat}_{(e_1,e_2,e_3)} \varphi_1 = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & -1 \\ 1 & -1 & 1 \end{pmatrix}$, on obtient :

$$ \chi_{\varphi_1}(X) = \chi_A(X) = -X(X-2)(X-3). $$

On trouve pour vecteurs propres :

$u_1 = (-1, 1, 2)$ associé à 0, $u_2 = (1, 1, 0)$ associé à 2 et $u_3 = (1, -1, 1)$ associé à 3.

Une base orthonormale de vecteurs propres est donc (v_1, v_2, v_3) avec :

$$ v_1 = \frac{1}{\sqrt{6}}(-1, 1, 2) \ , \quad v_2 = \frac{1}{\sqrt{2}}(1, 1, 0) \ , \quad v_3 = \frac{1}{\sqrt{3}}(1, -1, 1). $$

La réduction de A s'écrit :

$$ P^{-1}AP = {}^tPAP = \mathrm{diag}(0, 2, 3) \text{ avec } P = \begin{pmatrix} -\frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{3}} \\ \frac{2}{\sqrt{6}} & 0 & \frac{1}{\sqrt{3}} \end{pmatrix} \in \mathcal{O}_3(\mathbb{R}). $$

Dans la base (v_1, v_2, v_3) avec $u = Xv_1 + Yv_2 + Zv_3$ on a $q_1(u) = 2Y^2 + 3Z^2$.

Remarque

On a ici $v_3 = -v_1 \wedge v_2$, ceci permet un calcul de v_3 sans résolution du système :

$$ (A - 3I_3)X = 0. $$

b) Avec $B = \mathrm{mat}_{(e_1,e_2,e_3)} \varphi_2 = \begin{pmatrix} 151 & 72 & 24 \\ 72 & -119 & -96 \\ 24 & -96 & 137 \end{pmatrix}$, on obtient :

$$ \chi_{\varphi_2}(X) = \chi_B(X) = (X - 169)^2(X + 169). $$

Sachant que φ_2 est diagonalisable, $F = \mathrm{Ker}(\varphi_2 - 169\,\mathrm{Id})$ est un plan, on vérifie qu'il a pour équation $-3x + 12y + 4z = 0$.

$G = \mathrm{Ker}\,(\varphi_2 + 169\,\mathrm{Id})$ est l'orthogonal de ce plan, il est donc dirigé par le vecteur unitaire :

$$ v_3 = \frac{1}{13}(-3, 12, 4). $$

Un vecteur unitaire de F est $v_1 = \frac{1}{13}(12, 4, -3)$ donc $v_2 = v_3 \wedge v_1 = \frac{1}{13}(-4, 3, -12)$ est tel que (v_1, v_2) soit une base orthonormale de F et (v_1, v_2, v_3) une base orthonormale de $\mathbb{R}^3$. La réduction de B s'écrit :

$$ P^{-1}BP = {}^tPBP = \mathrm{diag}(169, 169, -169) \text{ avec } P = \frac{1}{13}\begin{pmatrix} 12 & -4 & -3 \\ 4 & 3 & 12 \\ -3 & -12 & 4 \end{pmatrix}. $$

Dans la base (v_1, v_2, v_3) avec $u = Xv_1 + Yv_2 + Zv_3$, on a $q_2(u) = 169(X^2 + Y^2 - Z^2)$.

Copyrighted material

Exemple 14 Si A et B sont des matrices symétriques positives (resp. définies-positives) de $\mathcal{M}_n(\mathbb{R})$, on a :
$$\mathrm{Tr}(AB) \geqslant 0 \quad (\text{resp. } \mathrm{Tr}(AB) > 0).$$

Il existe une matrice orthogonale $P \in \mathcal{O}_n(\mathbb{R})$ telle que $A' = P^{-1}AP = \mathrm{diag}\left(\alpha_1, \cdots, \alpha_n\right)$.

Avec $B' = P^{-1}BP = \left[\beta_{ij}\right]$, on a $\mathrm{Tr}(A'B') = \mathrm{Tr}\left(P^{-1}ABP\right) = \mathrm{Tr}(AB) = \sum_{i=1}^{n} \alpha_i \beta_{ii}$.

Notons q_A et q_B les formes quadratiques de $\mathbb{R}^n$ canoniquement associées aux matrices A et B.
- Si q_A et q_B sont positives, on a $\forall i \in [\![1, n]\!],\ \alpha_i \geqslant 0, \beta_{ii} \geqslant 0$ d'où $\mathrm{Tr}\, AB \geqslant 0$.
- Si q_A et q_B sont définies positives, on a $\forall i \in [\![1, n]\!],\ \alpha_i > 0, \beta_{ii} > 0$ d'où $\mathrm{Tr}\, AB > 0$.

On a utilisé $P^{-1} = {}^t P$ pour signifier que $B' = {}^t PBP$ est matrice de q_B dans la base $\left(u_i\right)_{1 \leqslant i \leqslant n}$ et, de ce fait, $\beta_{ii} = q_B\left(u_i\right)$. De même $\alpha_i = q_A\left(u_i\right)$.

D. Norme d'un endomorphisme d'un espace euclidien

E est un espace euclidien de dimension $n \geqslant 1$ et $\mathcal{B}$ désigne la boule unité de E :
$$\mathcal{B} = \left\{x \in E \,/\, \|x\| \leqslant 1\right\}.$$

Théorème 13

a) Pour tout endomorphisme f de E, on a :
$$|||f||| = \sup_{(x,y)\in\mathcal{B}^2} \left|\langle f(x) \,|\, y\rangle\right| = \sup_{(x,y)\in\mathcal{B}^2} \langle f(x) \,|\, y\rangle.$$ (46)

b) Si f est un endomorphisme symétrique positif, on a :
$$|||f||| = \sup_{x\in\mathcal{B}} \langle f(x) \,|\, x\rangle = \rho(f)$$
où $\rho(f)$ est la plus grande valeur propre de f.

(46) E étant de dimension finie, tout endomorphisme de E est continu, ce qui assure l'existence de $|||f|||$.

a) Remarquons d'abord que l'ensemble $\left\{\langle f(x) \,|\, y\rangle \,/\, (x, y) \in \mathcal{B}^2\right\}$ est symétrique par rapport à 0, il est donc borné si et seulement si il est majoré et, dans ce cas, on a :
$$\sup_{(x,y)\in\mathcal{B}^2} \left|\langle f(x) \,|\, y\rangle\right| = \sup_{(x,y)\in\mathcal{B}^2} \langle f(x) \,|\, y\rangle.$$

Par définition de $|||f|||$ on a pour tout $x \in E$, $\|f(x)\| \leqslant |||f|||\, \|x\|$ et l'inégalité de Cauchy-Schwarz donne $\left|\langle f(x) \,|\, y\rangle\right| \leqslant \|f(x)\|\, \|y\|$. Donc pour tout $(x, y) \in \mathcal{B}^2$, il vient :
$$\left|\langle f(x) \,|\, y\rangle\right| \leqslant |||f|||\, \|x\|\, \|y\| \leqslant |||f|||.$$

Il en résulte que $\left\{\left|\langle f(x) \,|\, y\rangle\right| \,/\, (x, y) \in \mathcal{B}^2\right\}$ est une partie majorée de $\mathbb{R}^+$ puis que :
$$\sup_{(x,y)\in\mathcal{B}^2} \left|\langle f(x) \,|\, y\rangle\right| \leqslant |||f|||. \qquad \text{(i)}$$

Soit $x \in \mathcal{B}$, si $f(x) \neq 0_E$ on a $\|f(x)\| = \left\langle f(x) \,\middle|\, \frac{f(x)}{\|f(x)\|} \right\rangle$ et en remarquant que $\frac{f(x)}{\|f(x)\|} \in \mathcal{B}$ on en déduit :
$$\|f(x)\| \leqslant \sup_{(x,y)\in\mathcal{B}^2} \left|\langle f(x) \,|\, y\rangle\right|.$$

Il est clair que cette inégalité reste vraie lorsque $f(x) = 0_E$. On a donc :
$$\forall x \in \mathcal{B},\ \|f(x)\| \leqslant \sup_{(x,y)\in\mathcal{B}^2} \left|\langle f(x) \,|\, y\rangle\right|$$
puis
$$|||f||| = \sup_{x\in\mathcal{B}} \|f(x)\| \leqslant \sup_{(x,y)\in\mathcal{B}^2} \left|\langle f(x) \,|\, y\rangle\right|. \qquad \text{(ii)}$$

Les inégalités (i) et (ii) donnent la proposition a).

Copyrighted material

Hidden page

Hidden page

Hidden page

Mise en œuvre

I. Produit scalaire, orthogonalité

Ex. 1

Soit $E = \mathbb{R}^3$ et sa base canonique (e_1, e_2, e_3).

Pour $(x, y) \in E^2$, on note $x = (x_1, x_2, x_3) = \sum_{i=1}^{3} x_i e_i$, $y = (y_1, y_2, y_3) = \sum_{i=1}^{3} y_i e_i$.

On considère l'application $\varphi : E^2 \to \mathbb{R}$, $(x, y) \mapsto x_1y_1 + 3x_2y_2 + 6x_3y_3 + x_1y_2 + x_2y_1 + x_1y_3 + x_3y_1$.

1) Vérifier que : $\forall x \in E$, $\varphi(x, x) = (x_1 + x_2 + x_3)^2 + (x_2 + x_3)^2 + (x_2 - 2x_3)^2$. **(1)**

En déduire que φ est un produit scalaire euclidien sur E. On note encore E l'espace euclidien ainsi défini.

2) Déduire de la formule **(1)** une base orthonormale de E.

3) Trouver des réels a, b tels que : $\forall x \in E$, $\varphi(x, x) = (x_1 + x_2 + x_3)^2 + (ax_2 + bx_3)^2 + dx_3^2$. **(2)**

En déduire une nouvelle base orthonormale de E.

Indications

Pour **2)** et **3)**, utiliser que, dans un espace euclidien E de dimension n, une base $(e_i)_{1 \leqslant i \leqslant n}$ est orthonormale si et seulement si pour tout $x = \sum_{i=1}^{n} x_i e_i$, on a $\|x\|^2 = \sum_{i=1}^{n} x_i^2$.

Solution

1) Pour $x \in E$, on a : $\varphi(x, x) = x_1^2 + 3x_2^2 + 6x_3^2 + 2x_1x_2 + 2x_1x_3$ et la vérification demandée est sans difficulté. En particulier, $\varphi(x, x) = 0$ implique $x_1 + x_2 + x_3 = 0$, $x_2 + x_3 = 0$, $x_2 - 2x_3 = 0$, d'où $x = 0$.

2) Une base $(e'_i)_{1 \leqslant i \leqslant 3}$ est orthonormale si et seulement si on a :

$$\text{pour tout } x = \sum_{i=1}^{3} x'_i e'_i, \quad \|x\|^2 = x_1'^2 + x_2'^2 + x_2'^3.$$

Donc, en posant $x'_1 = x_1 + x_2 + x_3$, $x'_2 = x_2 + x_3$, $x'_3 = x_2 - 2x_3$, x'_1, x'_2, x'_3 seront les coordonnées de x dans une base orthonormale.

$\|x\|^2 = \varphi(x, x)$.

Ces formules s'écrivent $\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = M \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ avec $M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & -2 \end{pmatrix}$.

Comme M est inversible et on a aussi : $\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = M^{-1} \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix}$.

$\det M = -3$.

Pour le calcul de M^{-1}, il vient successivement :

Méthode du pivot.

$$\begin{cases} x_1 + x_2 + x_3 = x'_1 \\ x_2 + x_3 = x'_2 \\ 3x_3 = x'_2 - x'_3 \end{cases} \qquad \begin{cases} x_1 = x'_1 - x'_2 \\ x_2 = \frac{2}{3}x'_2 + \frac{1}{3}x'_3 \\ x_3 = \frac{1}{3}x'_2 - \frac{1}{3}x'_3 \end{cases}$$

donc : $M^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & \frac{2}{3} & \frac{1}{3} \\ 0 & \frac{1}{3} & -\frac{1}{3} \end{pmatrix}$.

Commentaires

En développant la forme attendue.

$P = M^{-1}$ est la matrice de passage de la base $(e_i)_{1\leq i\leq 3}$ à la base orthonormale $(e'_1)_{1\leq i\leq 3}$ et on a donc :

$$e'_1 = e_1,\quad e'_2 = -e_1 + \frac{2}{3}e_2 + \frac{1}{3}e_3,\quad e'_3 = \frac{1}{3}e_2 - \frac{1}{3}e_3.$$

3) Écrivons $\varphi(x,x)$ en ordonnant par rapport à x_1 :

$$\varphi(x,x) = x_1^2 + 2x_1(x_2+x_3) + 3x_2^2 + 6x_3^2.$$

Remarquons que x_1 ne figure que dans le premier carré de la formule (2).

Avec $(x_1+x_2+x_3)^2 = x_1^2 + 2x_1(x_2+x_3) + (x_2+x_3)^2$, on en déduit :

$$\varphi(x,x) = (x_1+x_2+x_3)^2 + 2x_2^2 + 5x_3^2 - 2x_2x_3.$$

En notant que : $2\left(x_2^2 - x_2x_3\right) = 2\left(\left(x_2 - \frac{1}{2}x_3\right)^2 - \frac{1}{4}x_3^2\right)$, il vient finalement $\varphi(x,x) = (x_1+x_2+x_3)^2 + 2\left(x_2 - \frac{1}{2}x_3\right)^2 + \frac{9}{2}x_3^2$ ou :

$$\varphi(x,x) = (x_1+x_2+x_3)^2 + \left(x_2\sqrt{2} - x_3\frac{\sqrt{2}}{2}\right)^2 + \left(\frac{3x_3}{\sqrt{2}}\right)^2.$$

On pose : $\begin{cases} x''_1 = x_1 + x_2 + x_3 \\ x''_2 = x_2\sqrt{2} - x_3\frac{\sqrt{2}}{2} \\ x''_3 = \frac{3}{\sqrt{2}}x_3 \end{cases}$

On opère comme en 2).

c'est-à-dire $\begin{cases} x_1 = x''_1 - \frac{\sqrt{2}}{2}x''_2 - \frac{\sqrt{2}}{2}x''_3 \\ x_2 = \frac{\sqrt{2}}{2}x''_2 + \frac{\sqrt{2}}{6}x''_3 \\ x_3 = \frac{\sqrt{2}}{3}x''_3 \end{cases}$ soit :

L'inversion est facile. Ce sont là les formules de changement de base faisant passer de la base $(e_i)_{1\leq i\leq 3}$ à $(e''_i)_{1\leq i\leq 3}$.

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = Q\begin{pmatrix} x''_1 \\ x''_2 \\ x''_3 \end{pmatrix} \quad \text{avec} \quad Q = \begin{pmatrix} 1 & -\frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2} \\ 0 & \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{6} \\ 0 & 0 & \frac{\sqrt{2}}{3} \end{pmatrix}$$

$$e''_1 = e_1,\quad e''_2 = -\frac{\sqrt{2}}{2}e_1 + \frac{\sqrt{2}}{2}e_2,\quad e''_3 = -\frac{\sqrt{2}}{2}e_1 + \frac{\sqrt{2}}{6}e_2 + \frac{\sqrt{2}}{3}e_3.$$

À la lecture de la matrice Q.

La base $(e''_i)_{1\leq i\leq 3}$ est orthonormale car, dans celle-ci, $\|x\|^2 = \sum_{i=1}^{3} x''^2_i$.

Ex. 2

On considère encore l'espace $E = \mathbb{R}^3$ muni du produit scalaire défini dans l'exemple 1.

Trouver une base orthonormale de E en appliquant le procédé de Schmidt à la base canonique $(e_i)_{1\leq i\leq 3}$.

Indications

On applique méthodiquement la démarche vue dans le chapitre 6.

Solution

On obtient successivement :

- $\|e_1\| = 1$ donc $u = \frac{e_1}{\|e_1\|} = e_1$;
- $v' = e_2 - (u\,|\,e_2)u = e_2 - e_1$, donc $v = \frac{v'}{\|v'\|} = -\frac{\sqrt{2}}{2}e_1 + \frac{\sqrt{2}}{2}e_2$.

Commentaires

(u,v,w) est la base cherchée.

$\|v'\|^2 = 2$.

Copyrighted material

$$w = \frac{w'}{\| w' \|} \quad \text{avec} \quad w' = e_3 - \langle u \mid e_3 \rangle u - \langle v \mid e_3 \rangle v$$

$$= e_3 - u + \frac{\sqrt{2}}{2} v$$

$$= -\frac{3}{2} e_1 + \frac{1}{2} e_2 + e_3$$

$\| w' \|^2 = \frac{9}{2}$ donc $w = -\frac{\sqrt{2}}{2} e_1 + \frac{\sqrt{2}}{6} e_2 + \frac{\sqrt{2}}{3} e_3$.

Cette base n'est autre que (e_1'', e_2'', e_3'') obtenue au 3) de l'exemple 1.
C'est l'unique base orthonormale vérifiant :

$$\text{Vect}\,(e_1'') = \text{Vect}\,(e_1), \ \text{Vect}\,(e_1'', e_2'') = \text{Vect}\,(e_1, e_2),$$

c'est-à-dire déduite de $(e_i)_{1 \leqslant i \leqslant 3}$ par le procédé de Schmidt et vérifiant les conditions $\langle e_i \mid e_i'' \rangle > 0$ pour $i = 1, 2, 3$.

Ceci pouvait se prévoir car la matrice de passage Q était triangulaire.

II. Adjoint d'un endomorphisme

Ex. 3

Soit f un endomorphisme nilpotent d'un espace euclidien E, tel que $\text{Ker}\, f = \text{Ker}\, f^*$. Montrer que $f = 0$.

Indications

On établit que $E = \text{Im}\, f \oplus \text{Ker}\, f$ et que $\text{Im}\, f \subset \text{Im}\, f^n$.
La structure d'espace euclidien sert pour définir f^* et avoir $\text{Ker}\, f^* = (\text{Im}\, f)^\perp$.

Solution

Avec $\text{Ker}\, f^* = (\text{Im}\, f)^\perp$, il vient $E = \text{Im}\, f \oplus \text{Ker}\, f$.
Tout x de E s'écrit donc $x = x' + x''$ avec $x \in \text{Ker}\, f$ et $x'' \in \text{Im}\, f$ donc $x'' = f(x_1)$, $x_1 \in E$ et on obtient $f(x) = f^2(x_1)$.
De même, il existe x_2 tel que $f(x_1) = f^2(x_2)$ donc $f(x) = f^3(x_2)$.
On itère le procédé : il existe $x_{n-1} \in E$ tel que $f(x) = f^n(x_{n-1})$.
Or $f^n = 0$ donc $\forall x \in E,\ f(x) = 0$ c'est-à-dire $f = 0$.

Commentaires

$\text{Ker}\, f = (\text{Im}\, f)^\perp$. $\text{Ker}\, f$ et $\text{Im}\, f$ sont donc supplémentaires orthogonaux.

n dimension de E.

Ex. 4

Soit $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que $\text{rg}\, A = \text{rg}\, {}^tAA$.

Indications

On identifie A et l'endomorphisme $u \in \mathcal{L}(\mathbb{R}^n)$ canoniquement associé.
Grâce au théorème du rang, il revient au même de prouver que $\text{Ker}\,(u^* \circ u) = \text{Ker}\, u$.

Solution

Comme on a $\text{Ker}\,(u^* \circ u) \subset \text{Ker}\, u$, il suffit de prouver :

$$\text{Ker}\,(u^* \circ u) \supset \text{Ker}\, u.$$

Soit $x \in \text{Ker}\,(u^* \circ u)$. Alors $(u^* \circ u)(x) = 0$, ce qui donne :

$$\langle (u^* \circ u)(x) \mid x \rangle = 0, \text{ donc } \langle u(x) \mid u(x) \rangle.$$

Alors $\| u(x) \| = 0$ donne $u(x) = 0$, c'est-à-dire $x \in \text{Ker}\, u$.

Commentaires

$u(x)=0 \Rightarrow u^* \circ u(x)=0$.

Par définition de l'adjoint.

Copyrighted material

Hidden page

On trouve pour sous-espaces propres :

$$\operatorname{Ker} A = \operatorname{Vect}\big((-1,1,1)\big)$$
$$\operatorname{Ker}\big(A + I_3\big) = \operatorname{Vect}\big((1,0,1)\big)$$
$$\operatorname{Ker}\big(A - 3I_3\big) = \operatorname{Vect}\big((1,2,-1)\big)$$

En identifiant A et l'endomorphisme de $\mathbb{R}^3$ canoniquement associé.

Une base orthonormale de $\mathbb{R}^3$ est donc (u, v, w) avec :

$$u = \frac{1}{\sqrt{3}}(-1,1,1)\ ,\quad v = \frac{1}{\sqrt{2}}(1,0,1)\ ,\quad w = \frac{1}{\sqrt{6}}(1,2,-1).$$

$\mathbb{R}^3$ est muni de sa structure euclidienne canonique.

En conséquence, on a :

$$P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 3 \end{pmatrix} \text{ avec } P = \frac{1}{\sqrt{6}}\begin{pmatrix} -\sqrt{2} & \sqrt{3} & 1 \\ \sqrt{2} & 0 & 2 \\ \sqrt{2} & \sqrt{3} & -1 \end{pmatrix} \in \mathbb{O}_3(\mathbb{R}).$$

Ex. 7

1) Soit $A \in \mathcal{M}_n(\mathbb{R})$, symétrique, positive. Montrer que $\operatorname{Tr} A \geqslant n\sqrt[n]{\det A}$.

2) Montrer ce même résultat avec $A = A_1A_2$ où A_1 et A_2 sont symétriques réelles positives.

Indications

1) Si $\lambda_1, \ldots, \lambda_n$ sont n réels positifs ou nul, on a $\dfrac{1}{n}\displaystyle\sum_{i=1}^{n}\lambda_i \geqslant \sqrt[n]{\prod_{i=1}^{n}\lambda_i}$.

2) On pourra commencer par le cas où l'une des deux matrices A_1, A_2 est inversible.

Solution

1) A est diagonalisable dans le groupe orthogonal : il existe $P \in \mathbb{O}_n(\mathbb{R})$ telle que $P^{-1}AP = \operatorname{diag}\big(\lambda_1, \ldots, \lambda_n\big)$, et la positivité de A se traduit par $\lambda_i \geqslant 0$ pour tout i.

On a alors $\operatorname{Tr} A = \displaystyle\sum_{i=1}^{n}\lambda_i$, $\det A = \prod_{i=1}^{n}\lambda_i$ et la propriété annoncée résulte donc de l'inégalité bien connue :

$$\forall\big(\lambda_1, \lambda_2, \ldots, \lambda_n\big) \in \mathbb{R}_+^n,\ \left(\prod_{i=1}^{n}\lambda_i\right)^{\frac{1}{n}} \leqslant \frac{1}{n}\sum_{i=1}^{n}\lambda_i \qquad \text{(i)}$$

reliant les moyennes géométriques et arithmétiques des réels positifs $\lambda_1, \ldots, \lambda_n$.

2) Envisageons d'abord le cas où l'une des matrices A_1, A_2, par exemple A_1, est inversible.

Étant positive et inversible, A_1 est définie-positive, donc il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que $A_1 = P\,{}^tP$ et on obtient :

$$\operatorname{Tr}\big(A_1A_2\big) = \operatorname{Tr}\big(P\,{}^tPA_2\big) = \operatorname{Tr}\big({}^tPA_2P\big).$$

Puisqu'elle est congruente à A_2, la matrice $B = {}^tPA_2P$ est, elle aussi, symétrique positive.

Donc en appliquant le résultat du 1), il vient :

$$\operatorname{Tr}\big(A_1A_2\big) = \operatorname{Tr}(B) \geqslant n\sqrt[n]{\det B}$$

puis, avec $\det B = \det A_2(\det P)^2 = \det A_2 \det A_1 = \det\big(A_1A_2\big)$, on conclut : $\operatorname{Tr} A \geqslant n\sqrt[n]{\det A}$.

Commentaires

$P^{-1} = {}^tP$.

Si l'un des λ_i est nul l'inégalité (i) est évidente et, si tous les λ_i sont strictement positifs, elle équivaut à :

$$\frac{1}{n}\sum_{i=1}^{n}\ln\lambda_i \leqslant \ln\left(\frac{1}{n}\sum_{i=1}^{n}\lambda_i\right) \qquad \text{(ii)}$$

et (ii) est vraie par concavité de la fonction $\ln$.

Puisque $\operatorname{Tr}(A_1A_2) = \operatorname{Tr}(A_2A_1)$ et $\det(A_1A_2) = \det(A_2A_1)$

A_1 et A_2 jouent des rôles symétriques.

A_1 est la matrice d'un produit scalaire, donc elle est congruente à I_n.

$\operatorname{Tr}(MN) = \operatorname{Tr}(NM)$.

B et A_2 représentent la même forme quadratique dans des bases différentes. On peut aussi dire que l'hypothèse $\forall X \in \mathbb{R}^n,\ {}^tXA_2X \geqslant 0$ donne : $\forall x \in \mathbb{R}^n,\ {}^tXBX = {}^t(PX)A_2(PX) \geqslant 0$.

$A = A_1A_2$.

Il reste à traiter le cas où A_1 et A_2 sont toutes deux non inversibles. Alors $\det A = 0$ et le problème revient à montrer que $\operatorname{Tr} A \geqslant 0$.
Diagonalisons A_1 dans le groupe orthogonal : il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tPA_1P = D = \operatorname{diag}(\lambda_1, \cdots, \lambda_n)$. Il vient alors $A_1 = PD\,{}^tP$ et :

$$\operatorname{Tr}(A_1A_2) = \operatorname{Tr}(PD\,{}^tPA_2) = \operatorname{Tr}(D\,{}^tPA_2P).$$

Avec $\lambda_i \geqslant 0$ pour tout i, car A_1 est positive.
On a maintenant ${}^tP = P^{-1}$.

$\operatorname{Tr}(MN) = \operatorname{Tr}(NM)$.

La matrice $B = {}^tPA_2P$ est encore symétrique positive donc, en posant $B = [b_{ij}]$, si on appelle q_B la forme quadratique sur $\mathbb{R}^n$ de matrice B dans la base canonique $(e_i)_{1 \leqslant i \leqslant n}$, on a :

$$b_{ii} = q_B(e_i) \geqslant 0 \text{ pour tout } i \in [\![1, n]\!].$$

Il en résulte $\operatorname{Tr}(A_1A_2) = \operatorname{Tr}(DB) = \sum_{i=1}^{n} \lambda_i b_{ii} \geqslant 0$. Ainsi, dans tous les cas, si $A = A_1A_2$ avec A_1 et A_2 symétriques réelles positives, on a :

$$\operatorname{Tr} A \geqslant n\sqrt[n]{\det A}.$$

Ce qui achève la démonstration dans ce second cas.

Ex. 8

Soit $A \in \mathcal{M}_n(\mathbb{R})$ nilpotente et telle que ${}^tAA = A\,{}^tA$. Montrer que $A = 0$.

Indications

${}^tA$ et A étant permutables, on a $\forall k \in \mathbb{N}$, $({}^tAA)^k = {}^tA^kA^k$.

Solution

Remarquons d'abord que $B = {}^tAA$ est nilpotente.
En effet, ${}^tAA = A\,{}^tA$ donne $B^n = {}^tA^nA^n$ donc $B^n = 0$.
Par ailleurs, B est symétrique donc diagonalisable : il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que : ${}^tPBP = \operatorname{diag}(\lambda_1, \cdots, \lambda_n)$,

et, puisqu'elle est nilpotente, sa seule valeur propre est 0, donc ${}^tPBP = 0$ puis $B = 0$.
Enfin ${}^tAA = 0$ donne $\operatorname{Tr}({}^tAA) = 0$ c'est-à-dire $\|A\|^2 = 0$ puis $A = 0$.

Commentaires

car $A^n = 0$.

$\lambda_1, \cdots, \lambda_n$: valeurs propres de B.

Les valeurs propres de B sont racines du polynôme annulateur X^n.
L'application $M \mapsto \operatorname{Tr}({}^tMM)^{1/2}$ est la norme euclidienne canonique sur $\mathcal{M}_n(\mathbb{R})$.

IV. Formes quadratiques, réduction

Ex. 9

Soit $E = \mathbb{R}^3$ euclidien canonique. On considère la forme quadratique q définie par :

$$u = (x, y, z) \mapsto 4x^2 + 7y^2 + 4z^2 + 4xy - 2xz - 4yz.$$

1) Préciser la forme polaire de q ainsi que l'endomorphisme symétrique f qui lui est associé.

2) Déterminer une base de réduction de q.

Indications

1) On procède par la règle dite de «dédoublement des termes» :

$$x^2 \mapsto xx', \quad 2xy \mapsto xy' + x'y \text{ et les analogues.}$$

2) Une telle base est formée de vecteurs propres de f.

Copyrighted material

Solution

1) Avec $u = (x, y, z)$, $u' = (x', y', z')$, la forme polaire φ est définie par :

$\varphi(u, u')$

$= 4xx' + 7yy' + 4zz' + 2(xy' + x'y) - (xz' + x'z) - 2(yz' + y'z).$

Dans la base canonique $\mathcal{B}$ de $\mathbb{R}^3$, on a :

$$\mathrm{mat}_{\mathcal{B}}\, q = \mathrm{mat}_{\mathcal{B}}\, \varphi = A \text{ avec } A = \begin{pmatrix} 4 & 2 & -1 \\ 2 & 7 & -2 \\ -1 & -2 & 4 \end{pmatrix}.$$

f est l'endomorphisme de matrice A dans la base $\mathcal{B}$.

2) Le polynôme caractéristique de A est :

$$\chi_A(X) = \begin{vmatrix} 4-X & 2 & -1 \\ 2 & 7-X & -2 \\ -1 & -2 & 4-X \end{vmatrix} \text{ factorisable par } 3 - X.$$

On obtient $\chi_A(X) = (3 - X)^2(9 - X)$.

Le sous-espace propre V_3 associé à 3 est le plan d'équation :

$$x + 2y - z = 0.$$

Celui associé à 9 est la droite V_9 dirigée par $d = (1, 2, -1)$.

Une base orthonormale $\mathcal{B}'$ formée de vecteurs propres est par exemple :

$$e'_1 = \frac{1}{\sqrt{6}}(1, 2, -1),\ e'_2 = \frac{1}{\sqrt{2}}(1, 0, 1),\ e'_3 = \frac{1}{\sqrt{3}}(1, -1, -1).$$

La matrice de passage est $P = \dfrac{1}{\sqrt{6}} \begin{pmatrix} 1 & \sqrt{3} & \sqrt{2} \\ 2 & 0 & -\sqrt{2} \\ -1 & \sqrt{3} & -\sqrt{2} \end{pmatrix} \in \mathbb{O}_n(\mathbb{R})$.

Dans la base $\mathcal{B}'$, la matrice de f est $D = \mathrm{diag}(9, 3, 3)$.

Dans cette base, on a $\varphi(u, u') = 9XX' + 3YY' + 3ZZ'$, et, en particulier :

$$q(u) = 9X^2 + 3Y^2 + 3Z^2.$$

Commentaires

La règle de « dédoublement des termes » consiste à remarquer que les formes polaires des formes quadratiques $q_x : u \mapsto x^2$ et $q_{xy} : u \mapsto xy$ (et analogues) sont $\varphi_x : (u, u') \mapsto xx'$ et $\varphi_{xy} : (u, u') \mapsto \frac{1}{2}(xy' + x'y)$ (et analogues).

$\mathcal{B} = (e_1, e_2, e_3)$ est orthonormale.

Pour les valeurs propres.

Addition des colonnes 1 et 3.

On sait que A est diagonalisable.

Il est orthogonal à V_3.

Choix d'une base de V_3.

Les deux bases sont orthonormales.

$u = (X, Y, Z)$ et $u' = (X', Y', Z')$ dans $\mathcal{B}'$.

Ex. 10

Soit $k \in \mathbb{R}_+$. Trouver les matrices $A \in \mathcal{M}_n(\mathbb{R})$ telles que : ${}^tAA = A\,{}^tA$ et $A^2 + k^2 I_n = 0$.

Indications

Procéder par analyse-synthèse en remarquant que $({}^tAA)^2 = {}^tA^2A^2$.

$\mathbb{O}_n(\mathbb{R})$ ne contient des matrices antisymétriques que si n est pair.

Solution

Soit A une solution du problème, s'il en existe.

Posons $S = {}^tAA$, S est symétrique positive, donc diagonalisable dans le groupe orthogonal et de valeurs propres positives.

D'autre part, ${}^tAA = A\,{}^tA$ et $A^2 = -k^2 I_n$ donnent :

$$S^2 = {}^tA^2A^2 = k^4 I_n,$$

donc le polynôme $X^2 - k^4$ est annulateur de S ce qui prouve que :

$$\mathrm{Sp}(S) \subset \{-k^2, k^2\}.$$

Sachant que $\mathrm{Sp}(S) \subset \mathbb{R}^+$, il en résulte $\mathrm{Sp}(S) = \{k^2\}$.

Commentaires

$\forall X \in \mathbb{R}^n$, ${}^tXSX = \|AX\|^2 \geqslant 0$ où $\|AX\|$ désigne la norme euclidienne canonique de AX dans $\mathbb{R}^n$.

Les valeurs propres sont racines de tout polynôme annulateur.

Puisqu'elle admet une seule valeur propre : k^2, la matrice diagonalisable S est égale à $k^2 I_n$. On a donc ${}^tAA = k^2 I_n$. **(1)**
Envisageons alors deux cas : $k = 0$ et $k > 0$.

- Pour $k = 0$, on a ${}^tAA = 0$ donc $\mathrm{Tr}\left({}^tAA\right) = 0$ et $A = 0$.
- Pour $k > 0$, en posant $B = \frac{1}{k}A$, la relation **(1)** s'écrit ${}^tBB = I_n$ ce qui traduit que B est orthogonale.

Avec $A^2 + k^2 I_n = 0$, on obtient aussi $B^2 + I_n = 0$, donc $B + {}^tB = 0$, ce qui donne que B est antisymétrique.
Remarquons alors que l'existence de B orthogonale, antisymétrique, impose que n est pair. En effet, ${}^tB = -B$ donne $\det B = (-1)^n \det B$ donc, sachant que $\det B \neq 0$, il vient $(-1)^n = 1$ donc $n = 2p$.

Finalement, si A est solution du problème, avec $k > 0$, n est pair et il existe B orthogonale, antisymétrique telle que $A = kB$.

Synthèse

- Pour $k = 0$, il est clair que la matrice nulle est solution.
- Pour $k > 0$,

– si $n = 2p + 1$, le problème n'a pas de solution ;
– si $n = 2p$, soit $A = kB$ avec $B \in \mathcal{O}_n(\mathbb{R})$, ${}^tB = -B$. On a alors ${}^tAA = A\,{}^tA = k^2 I_n$ et $A^2 = k^2 B^2 = -k^2\,{}^tBB = -k^2 I_n$, donc A est solution.

Remarque

$\mathcal{O}_{2p}(\mathbb{R})$ contient bien des matrices antisymétriques, par exemple, toute matrice de la forme ${}^tPUP$ avec $P \in \mathcal{O}_{2p}(\mathbb{R})$ et :

$$U = \begin{bmatrix} S & & (0) \\ & S & \\ (0) & & \ddots \\ & & & S \end{bmatrix} \text{ où } S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tPSP = k^2 I_n$ donc $S = k^2 P\,{}^tP = k^2 I_n$.

$\mathrm{Tr}({}^tAA)^{1/2}$ est la norme euclidienne canonique de A dans $\mathcal{M}_n(\mathbb{R})$.

$B^2 + I_n = 0$ donne ${}^tBB^2 + {}^tB = 0$ et ${}^tBB = I_n$.

$\det B = -1$.

L'analyse nous a fourni les solutions possibles.

C'est alors l'unique solution.

On pourrait montrer que toute matrice orthogonale antisymétrique d'ordre $2p$ est de cette forme, ce qui est assez facile en utilisant la réduction des endomorphismes autoadjoints dans un espace hermitien. Mais cette notion est maintenant hors programme.

Ex. 11

1) Soit $P \in \mathrm{GL}(\mathbb{R})$. Montrer que ${}^tPP$ est une matrice symétrique définie-positive.

2) Montrer que toute matrice symétrique réelle, définie-positive, s'écrit sous la forme :

$$S = {}^tPP \text{ avec } P \in \mathrm{GL}_n(\mathbb{R}).$$

3) Soit $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que A est diagonalisable si et seulement si il existe une matrice S symétrique, définie-positive, telle que ${}^tA = S^{-1}AS$.

Indications

1) C'est du cours, ou presque.

2) Si S est symétrique réelle, définie-positive, c'est la matrice d'un produit scalaire.

3) Si ${}^tA = S^{-1}AS$ avec $S \in \mathcal{S}_n^{++}(\mathbb{R})$ il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que $P\,{}^tAP^{-1}$ soit symétrique, réelle.

Solution

1) Pour tout $X \in \mathbb{R}^n$, on a ${}^tX\,{}^tPPX = \| PX \|^2 \geqslant 0$ et la même expression montre que :

$${}^tX\,{}^tPPX = 0 \iff PX = 0.$$

Donc, P étant inversible :

$${}^tX\,{}^tPPX = 0 \iff X = 0.$$

Ceci prouve que ${}^tPP$ est symétrique réelle, définie-positive.

Commentaires

On identifie $\mathcal{M}_{n,1}(\mathbb{R})$ et $\mathbb{R}^n$ et pour tout X de $\mathbb{R}^n$, $\| X \|$ désigne la norme euclidienne canonique du vecteur X.

La symétrie de ${}^tPP$ est évidente.

Copyrighted material

Hidden page

Exercices

Niveau 1

Ex. 1

Soit $A = \begin{pmatrix} 13 & -2 & -3 \\ -2 & 10 & -6 \\ -3 & -6 & 5 \end{pmatrix}$. Trouver $P \in \mathcal{O}_3(\mathbb{R})$ telle que $P^{-1}AP$ soit diagonale.

Ex. 2

Dans $\mathbb{R}^4$ euclidien, on considère l'ensemble F des vecteurs $x = (x_1, x_2, x_3, x_4)$ tels que :

$$\sum_{k=1}^{4} x_k = 0 \quad \text{et} \quad \sum_{k=1}^{4} k x_k = 0.$$

Former la matrice, dans la base canonique de $\mathbb{R}^4$, de la réflexion de plan F.

Ex. 3

Étudier l'endomorphisme de $\mathbb{R}^3$ euclidien dont la matrice est $M = \frac{1}{7}\begin{pmatrix} -2 & 6 & -3 \\ 6 & 3 & 2 \\ -3 & 2 & 6 \end{pmatrix}$.

Ex. 4

Soit E un espace euclidien orienté de dimension 3. On considère des rotations f et g qui ne sont ni Id_E ni des demi-tours.

Que peut-on dire de f et g si elles commutent ?

Ex. 5

Soit q la forme quadratique sur $E = \mathbb{R}^4$, de forme polaire φ définie par :

$\forall (x, y) \in E^2$,

$$\begin{aligned}\varphi(x, y) = {} & 2x_1y_1 + 2x_2y_2 + 2x_3y_3 + 2x_4y_4 \\ & - \frac{1}{2}(x_1y_2 + x_2y_1) + \frac{1}{2}(x_1y_3 + x_3y_1) \\ & - (x_1y_4 + x_4y_1) - (x_2y_3 + x_3y_1) \\ & + \frac{1}{2}(x_2y_4 + x_4y_2) - \frac{1}{2}(x_3y_4 + x_4y_3).\end{aligned}$$

Donner une base dans laquelle q est réduite et justifier que φ est un produit scalaire sur $\mathbb{R}^4$.

Niveau 2

Ex. 6

Formes quadratiques sur $\mathbb{R}^2$. Ensemble de deux droites

Soit (i, j) une base orthonormale de $\mathbb{R}^2$ euclidien et q la forme quadratique sur $\mathbb{R}^2$ donnée par :

$$q(u) = ax^2 + 2bxy + cy^2 \quad \text{avec} \quad u = xi + yj.$$

On note f l'endomorphisme symétrique associé à q et χ_f son polynôme caractéristique.

1) Discuter, en fonction de f, la nature géométrique du cône isotrope C_q de q.

2) Lorsque $ac - b^2 < 0$, C_q est formé de deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$, à quelle condition ces droites sont-elles orthogonales ?

Ex. 7

Soit $(e_i)_{1 \leqslant i \leqslant n}$ et $(f_i)_{1 \leqslant i \leqslant n}$ deux bases orthonormales de E espace vectoriel euclidien et soit $u \in \mathcal{L}(E)$.

On pose $A = \sum_{i=1}^{n}\sum_{j=1}^{n} \langle u(e_i) \,|\, f_j \rangle^2$, montrer que A ne dépend ni de la base $(e_i)_{1 \leqslant i \leqslant n}$, ni de la base $(f_i)_{1 \leqslant i \leqslant n}$. Exprimer A en fonction de u.

Ex. 8

On pose $E = \mathcal{M}_n(\mathbb{R})$.

1) Montrer que $\varphi : E^2 \to \mathbb{R}, (X, Y) \mapsto \mathrm{Tr}({}^tXY)$ est un produit scalaire.

2) Pour $A \in E$, on note $C(A) = \{X \in E \,/\, AX = XA\}$.

Étant donné $B \in E$, montrer l'équivalence des deux propositions :

(i) $\exists X_0 \in E, B = AX_0 - X_0A$

(ii) $\forall X \in C(A), \mathrm{Tr}(BX) = 0$

Ex. 9

Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que ${}^tAA = A\,{}^tA$ et $A^3 = A^2$.

Montrer que $A^2 = A$.

Copyrighted material

Ex. 10

Trouver les matrices $A \in \mathcal{O}_n(\mathbb{R})$ pour lesquelles il existe $\lambda \in \mathbb{R}$ tel que $(A - \lambda I_n)^2 = 0$.

Ex. 11

Soit $A = \frac{1}{9}\begin{pmatrix} -7 & -4 & 4 \\ 4 & -8 & -1 \\ -4 & -1 & -8 \end{pmatrix} \in \mathcal{M}_3(\mathbb{R})$.

1) Quel endomorphisme de $\mathbb{R}^3$ euclidien la matrice A représente-t-elle ?

2) Trouver toutes les matrices qui commutent avec A.

Ex. 12

Dans un espace euclidien orienté E de dimension 3, on considère des rotations r et R.

Étudier $f = r^{-1} \circ R \circ r$.

Ex. 13

Soit E un espace euclidien orienté de dimension 3 et $f \in \mathcal{L}(E), f \neq 0$.

Montrer que f est une rotation si et seulement si :

$$\forall (x, y) \in E^2, f(x \wedge y) = f(x) \wedge f(y).$$

Ex. 14

Soit (i, j, k) une base orthonormale directe de E espace euclidien orienté de dimension 3, montrer qu'il existe une unique rotation f telle que :

$$f(i + j + k) = i + j - k \text{ et } f(3i + j) = 3j - k.$$

Ex. 15

Étant donné $n \in \mathbb{N}$, $n \geqslant 3$, déterminer le polynôme caractéristique de $A \in \mathcal{M}_n(\mathbb{R})$

$$A = \begin{pmatrix} & & & 1 \\ & & & 2 \\ & (0) & & \vdots \\ & & & n-1 \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Ex. 16

Soit E un espace euclidien de dimension $n \geqslant 2$ et u un endomorphisme symétrique à valeurs propres strictement positives.

1) S étant la sphère unité de E :

$$S = \{x \in E / \|x\| = 1\}$$

déterminer le minimum sur S de l'application :

$$f : x \mapsto \langle u(x) \,|\, x \rangle \langle u^{-1}(x) \,|\, x \rangle.$$

2) En quels points de S ce minimum est-il atteint ?

Ex. 17

Soit E un espace euclidien et u un endomorphisme symétrique de E : $u \in \mathcal{S}(E)$.

1) Montrer que $\|u\| = \max\{|\lambda|, \lambda \in \mathrm{Sp}(u)\}$.

2) Soit $v \in \mathcal{S}^+(E)$ et $\phi : \mathcal{S}(E) \to \mathbb{R}, u \mapsto \mathrm{Tr}(u \circ v)$. Calculer $\|\phi\|$.

Ex. 18

Soit (i, j) la base canonique de $E = \mathbb{R}^2$. Pour tout u de E, on pose : $u = (x, y) = xi + yj$.

1) Montrer que $\varphi : E^2 \to \mathbb{R}$,

$$(u_1, u_2) \mapsto x_1x_2 + x_1y_2 + x_2y_1 + 3y_1y_2$$

est un produit scalaire sur E.

2) Trouver une base (I, J) de E orthonormale pour ce produit scalaire.

3) On considère la fonction f définie sur $\mathbb{R}^2 \setminus \{0, 0\}$ par :

$$f(u) = \frac{x^2 + 3xy + 5y^2}{x^2 + 2xy + 3y^2}.$$

a) Écrire l'expression de $f(u)$ en fonction de (X, Y) coordonnées de u dans la base (I, J).

b) Prouver qu'il existe une base (I', J') de E dans laquelle, en posant $u = X'I + Y'J$, on a :

$$f(u) = \frac{\lambda X'^2 + \mu Y'^2}{X'^2 + Y'^2}.$$

c) En déduire les bornes de f sur $\mathbb{R}^2 \setminus \{(0, 0)\}$.

Ex. 19

L'espace euclidien orienté E, de dimension 3, est rapporté à une base orthonormale directe (i, j, k).

Trouver les similitudes f de E telles que :

$$f(j + 2k) = 15i - 30k$$

$$f(i + 2j - k) = 30i - 15j + 15k.$$

Ex. 20

Soit A et B dans $\mathcal{M}_n(\mathbb{R})$, symétriques et positives.

Montrer que $\det(A + B) \geqslant \det A + \det B$.

Ex. 21

Soit $\mathcal{T}$ l'ensemble des matrices réelles, triangulaires supérieures et à éléments diagonaux strictement positifs.

1) Vérifier que $\mathcal{T}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

2) Étant donné $A \in \mathcal{M}_n(\mathbb{R})$, matrice d'une forme quadratique q définie positive, montrer l'existence et l'unicité de $T \in \mathcal{T}$ telle que $A = {}^tTT$.

Copyrighted material

Hidden page

Ex. 10

- Commencer par calculer les valeurs possibles de λ.
- Pour qu'une matrice $M \in \mathcal{M}_n(\mathbb{R})$ soit nulle, il faut et il suffit que $\operatorname{Tr} {}^tMM = 0$.

Ex. 11

1) $-A$ est une matrice de rotation.

2) Montrer que la dimension du commutant de A est 3.

Ex. 12

f est une rotation. Étudier son axe.

Pour l'angle, commencer par étudier $\operatorname{Tr} f$.

Ex. 13

Si $f \in \mathcal{SO}(E)$, $f(x \wedge y) = f(x) \wedge f(y)$ équivaut à :

$\forall z \in E,\ \langle f(x \wedge y) \,|\, f(z)\rangle = \langle f(x) \wedge f(y) \,|\, f(z)\rangle$.

Ex. 14

Trouver un système de trois équations vérifié par :

$$\big(f(i), f(j), f(k)\big).$$

Ex. 15

A est symétrique réelle. Examiner son rang.

Exprimer qu'un vecteur non nul est propre pour $\lambda \in \mathbb{R}^*$.

Ex. 16

1) Diagonaliser u dans une base orthonormale.

2) Utiliser l'inégalité de Cauchy-Schwarz.

Ex. 17

1) C'est (presque) du cours.

2) Diagonaliser u dans le groupe orthogonal pour en déduire une majoration de $|\phi(u)|$ de la forme $k\|u\|$.

Ex. 18

1) $\varphi(u,u) = x^2 + 2xy + 3y^2 = (x+y)^2 + 2y^2$.

(I, J) est une base orthonormale si et seulement si pour tout $u = XI + YJ$ de E, $\varphi(u,u) = X^2 + Y^2$.

2) En posant $U = \begin{pmatrix} X \\ Y \end{pmatrix}$ on a :

$$X^2 + XY\frac{\sqrt{2}}{2} + \frac{3}{2}Y^2 = {}^tU \begin{pmatrix} 1 & \frac{\sqrt{2}}{4} \\ \frac{\sqrt{2}}{4} & \frac{3}{2} \end{pmatrix} U.$$

Diagonaliser A dans le groupe orthogonal.

Ex. 19

Calculer le rapport λ de la similitude et poser $g = \frac{1}{\lambda} f$.

$\big(g(i), g(j), g(k)\big)$ est une base orthonormale directe ou rétrograde selon les cas.

Ex. 20

Dans le cas $\det A > 0$, A et I_n sont congruentes.

Dans le cas $\det A = 0$, se ramener au cas précédent avec $A_t = A + tI_n$ et t réel, $t > 0$.

Ex. 21

Caractériser $T \in \mathcal{T}$ par l'endomorphisme u associé dans la base canonique $(e_i)_{1 \leqslant i \leqslant n}$ de $\mathbb{R}^n$ et les sous-espaces $E_p = \operatorname{Vect}(e_1, \cdots, e_p)$, $p \in [\![1, n]\!]$. Ensuite, utiliser le procédé de Schmidt.

Ex. 22

1) Pour l'égalité des images, comparer les rangs de f^* et de $f^* \circ f$.

3) Si $p = f^* \circ f$ est un projecteur orthogonal, on a $\operatorname{Im} p = (\operatorname{Ker} p)^\perp$ et utiliser $\operatorname{Ker} f = \operatorname{Ker} p$.

4) Pour x tel que $\|f(x)\| = \|x\|$, décomposer en $x = x_1 + x_2$ avec $x_1 \in \operatorname{Ker} f$ et $x_2 \in (\operatorname{Ker} f)^\perp$.

Ex. 23

Pour toute matrice A, on a :

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

Envisager les cas $\det A = 0$ et $\det A \neq 0$.

Ex. 24

Commencer par prouver la convergence de la série. Calculer $u^n(x)$ en fonction de $u(x)$ et de $u^2(x)$. Utiliser l'expression vectorielle d'une rotation.

Ex. 25

1) θ est trilinéaire alternée.

2) Former $\langle g(x \wedge y) \,|\, z\rangle$.

Ex. 26

1) Exploiter la symétrie en (x, y, z) en se plaçant dans une base orthonormale (I, J, K) avec :

$$K = \frac{1}{\sqrt{3}}(i + j + k).$$

2) Utiliser les résultats de l'exercice 6, en considérant la restriction q' de q à un plan vectoriel $\mathcal{P}$ de base (u, v).

Ex. 27

Il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que :

$${}^tPAP = \operatorname{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n).$$

En posant $Y = PX$ on a :

$${}^tXAX = \sum_{i=1}^{n} \lambda_i Y_i^2 \text{ et } {}^tXX = {}^tYY.$$

Ex. 28

1) $AT^{-1} = S$, T^{-1} est la matrice de passage de $\mathcal{B}'$ base de $\mathbb{R}^n$ formée des vecteurs colonnes de A à $\mathcal{B}''$ base orthonormale déduite de $\mathcal{B}'$ par le procédé de Schmidt.

Copyrighted material

Solutions des exercices

Niveau 1

Ex. 1

On obtient $\chi_A = \det(A - XI_3) = -X(X-14)^2$.

En notant encore A l'endomorphisme de $\mathbb{R}^3$ canoniquement associé à la matrice A, on a ici deux sous-espaces propres :

une droite : $\operatorname{Ker} A$ et un plan : $\operatorname{Ker}(A - 14I_3)$ avec $\operatorname{Ker}(A-14I_3) = (\operatorname{Ker} A)^\perp$.

On trouve $\operatorname{Ker} A = \operatorname{Vect}((1,2,3))$ donc $\operatorname{Ker}(A-14I_3)$ est le plan d'équation :

$$x_1 + 2x_2 + 3x_3 = 0 \quad \text{(dans la base canonique)}.$$

Un vecteur de $\operatorname{Ker}(A-14I_3)$ est $(2,-1,0)$ et on obtient un second vecteur de ce plan, orthogonal au précédent, avec le produit vectoriel $(1,2,3) \wedge (2,-1,0) = (3,6,-5)$.

Il reste à normer ces trois vecteurs pour obtenir une base orthonormale formée de vecteurs propres de A, et il vient :

$$P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 14 & 0 \\ 0 & 0 & 14 \end{pmatrix} \text{ avec } P = \frac{1}{\sqrt{70}} \begin{pmatrix} \sqrt{5} & 2\sqrt{14} & 3 \\ 2\sqrt{5} & -\sqrt{14} & 6 \\ 3\sqrt{5} & 0 & -5 \end{pmatrix} \in \mathcal{O}_3(\mathbb{R}).$$

Ex. 2

F est l'intersection de deux hyperplans distincts de $\mathbb{R}^4$, c'est donc un sous-espace de dimension 2.

Notons (e_1, e_2, e_3, e_4) la base canonique de $\mathbb{R}^4$.

Un autre système d'équations de F est $\begin{cases} x_1 + x_2 + x_3 + x_4 = 0 \\ x_2 + 2x_3 + 3x_4 = 0 \end{cases}$

Une base de F est (u, v), où $u = (1,-2,1,0)$ et $v = (2,-3,0,1)$.

Un vecteur $w' = v + \lambda u$ est orthogonal à u si et seulement si $\langle v \mid u \rangle + \lambda \| u \|^2 = 0$ c'est-à-dire $\lambda = -\frac{4}{3}$.

Posons $w = 3v - 4u = (2,-1,-4,3)$. Ainsi, (u, w) est une base orthogonale de F.

Soit p la projection orthogonale sur F : $\forall x \in \mathbb{R}^4, p(x) = \langle x \mid u \rangle \frac{u}{\| u \|^2} + \langle x \mid w \rangle \frac{w}{\| w \|^2}$.

Il vient donc $p(e_1) = \frac{1}{6}u + \frac{1}{15}w$, $p(e_2) = -\frac{1}{3}u - \frac{1}{30}w$, $p(e_3) = \frac{1}{6}u - \frac{2}{15}w$, $p(e_4) = \frac{1}{10}w$.

La matrice de p est $\frac{1}{10}\begin{pmatrix} 3 & -4 & -1 & 2 \\ -4 & 7 & -2 & -1 \\ -1 & -2 & 7 & -4 \\ 2 & -1 & -4 & 3 \end{pmatrix}$.

Celle de la réflexion $s = 2p - \mathrm{Id}$ est $\frac{1}{5}\begin{pmatrix} -2 & -4 & -1 & 2 \\ -4 & 2 & -2 & -1 \\ -1 & -2 & 2 & -4 \\ 2 & -1 & -4 & -2 \end{pmatrix}$.

Ex. 3

En formant les produits scalaires des vecteurs-colonnes deux à deux, on voit que M est orthogonale.

Elle est en outre symétrique. Il suffit alors d'étudier ses vecteurs invariants.

Avec $M - I = \frac{1}{7}\begin{pmatrix} -9 & 6 & -3 \\ 6 & -4 & 2 \\ -3 & 2 & -1 \end{pmatrix}$, il vient $MX = X$ si et seulement si $3x - 2y + z = 0$ et M représente la réflexion de plan $P = (\mathbb{R}u)^\perp$ avec $u = (3,-2,1)$.

Copyrighted material

Ex. 4

Puisque $f \neq \mathrm{Id}_E$, $\mathrm{Ker}\,(f - \mathrm{Id}_E)$ est une droite vectorielle.

Soit u un vecteur normé, base de $\mathrm{Ker}\,(f - \mathrm{Id}_E)$. On a donc $f \circ g(u) = g \circ f(u) = g(u)$.

Ainsi $g(u)$ est un vecteur invariant par f, il existe donc $\lambda \in \mathbb{R}$ tel que $g(u) = \lambda u$.

Or g, qui est une rotation autre qu'un demi-tour ou Id_E, admet 1 pour unique valeur propre.

Par suite, $g(u) = u$ et u est un vecteur directeur de l'axe de la rotation g.

Ainsi les rotations f, g ont nécessairement le même axe (droite des vecteurs invariants).

Réciproquement, soit f et g des rotations de même axe dirigé par u supposé normé.

Dans une base orthonormale $\mathcal{B} = (i, j, u)$, les rotations f et g ont des matrices de la forme :

$$\begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \cos\theta' & -\sin\theta' & 0 \\ \sin\theta' & \cos\theta' & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

On vérifie aisément que $f \circ g$ et $g \circ f$ ont la même matrice $\begin{pmatrix} \cos(\theta+\theta') & -\sin(\theta+\theta') & 0 \\ \sin(\theta+\theta') & \cos(\theta+\theta') & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Ex. 5

- Matrice A de φ dans la base $\mathcal{B}$.

$A = [a_{ij}]$: a_{ij} est le coefficient de $x_i y_j$ dans le développement de $\varphi(x, y)$ donc :

$$A = \begin{pmatrix} 2 & -\frac{1}{2} & \frac{1}{2} & -1 \\ -\frac{1}{2} & 2 & -1 & \frac{1}{2} \\ \frac{1}{2} & -1 & 2 & -\frac{1}{2} \\ -1 & \frac{1}{2} & -\frac{1}{2} & 2 \end{pmatrix}.$$

- Pour une base orthonormale de $\mathbb{R}^4$ euclidien canonique dans laquelle φ est réduite, on diagonalise la matrice A.

Pour cela, calculons son polynôme caractéristique :

$$\begin{aligned} \chi_A = \det\left(A - XI_4\right) &= X^4 - 8X^3 + 21X^2 - 22X + 8 \\ &= (X-1)^2(X-2)(X-4). \end{aligned}$$

On détermine une base orthonormale de chaque sous-espace propre :

$$\begin{aligned} \mathrm{Ker}\,(A - I_3) = \mathrm{Vect}\,(u_1, u_2) \quad &. \quad u_1 = \frac{1}{2}(e_1 + e_2 + e_3 + e_4) \\ &\quad\ u_2 = \frac{1}{2}(e_1 - e_2 - e_3 + e_4) \\ \mathrm{Ker}\,(A - 2I_3) = \mathrm{Vect}\,(u_3) \quad &. \quad u_3 = \frac{1}{2}(-e_1 - e_2 + e_3 + e_4) \\ \mathrm{Ker}\,(A - 4I_3) = \mathrm{Vect}\,(u_4) \quad &. \quad u_4 = \frac{1}{2}(-e_1 + e_2 - e_3 + e_4) \end{aligned}$$

$$P = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{O}_4(\mathbb{R}) \text{ et } P^{-1}AP = {}^tPAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}.$$

Sur la base $(u_i)_{1 \leqslant i \leqslant 4}$, pour $x = \sum_{i=1}^{4} x'_i u_i$, $y = \sum_{i=1}^{4} y'_i e_i$ on a :

$$\varphi(x, y) = x'_1 y'_1 + x'_2 y'_2 + 2x'_3 y'_3 + 4x'_4 y'_4.$$

- Pour justifier que φ est un produit scalaire sur $\mathbb{R}^4$, il suffit de noter que φ est définie-positive, puisque $\mathrm{Sp}(A) \subset \mathbb{R}_+^*$, ou de considérer l'expression réduite : $\varphi(x, x) = x_1'^2 + x_2'^2 + 2x_3'^2 + 4x_4'^2$.

Copyrighted material

Niveau 2

Ex. 6

1) On a $\underset{(i,j)}{\text{mat}} f = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ et $\chi_f(X) = X^2 - (a+c)X + (ac - b^2)$.

Les valeurs propres de λ et μ de f sont les racines de χ_f :

$$\chi_f(X) = (X-\lambda)(X-\mu) \text{ avec } \begin{cases} \lambda + \mu = a + c & = \text{Tr} f \\ \lambda\mu = ac - b^2 & = \det f \end{cases}$$

Il existe une base orthonormale (i', j') de $\mathbb{R}^2$ dans laquelle :

$$q(u) = \lambda x'^2 + \mu y'^2 \text{ avec } u = x'i' + y'j'$$

donc, dans (i', j'), C_q a pour équation $\lambda x'^2 + \mu y'^2 = 0$.

On en déduit les résultats suivants :

- si $\det f > 0$ alors $\lambda\mu > 0$ et $C_q = \{0\}$;
- si $\det f < 0$ alors $\lambda\mu < 0$ et en posant $\alpha = \sqrt{-\dfrac{\mu}{\lambda}}$: $q(u) = \lambda\left(x' + \alpha y'\right)\left(x' - \alpha y'\right)$;

C_q est formé des deux droites vectorielles $\mathcal{D}_1$ et $\mathcal{D}_2$ d'équations :

$$x' + \alpha y' = 0 \text{ et } x' - \alpha y' = 0 ;$$

- si $\det f = 0$ alors $\lambda\mu = 0$. En supposant $q \neq 0$, on a $(\lambda, \mu) \neq (0,0)$, donc, par exemple, $\lambda \neq 0$ et $\mu = 0$, et $q(u) = \lambda x'^2$ et C_q est la droite $\mathcal{D}_1$ d'équation $x' = 0$.

2) D'après le 1), $\mathcal{D}_1$ et $\mathcal{D}_2$ sont orthogonales si et seulement si $\alpha^2 = 1$, ce qui équivaut à $\lambda + \mu = 0$ soit encore $a + c = 0$.

Remarque

Compte tenu de $(a, b, c) \neq (0, 0, 0)$, la condition $a+c = 0$ donne $ac - b^2 < 0$, donc l'équation $ax^2 + 2bxy + cy^2 = 0$ représente un ensemble de deux droites orthogonales si et seulement si $a + c = 0$.

Ex. 7

Sur la base orthonormale $(f_j)_{1 \leqslant j \leqslant n}$ on a pour tout $i \in [\![1, n]\!]$:

$$u(e_i) = \sum_{j=1}^{n} \langle f_j \mid u(e_i) \rangle f_j \text{ donc } \| u(e_i) \|^2 = \sum_{j=1}^{n} \langle f_j \mid u(e_i) \rangle^2.$$

Ainsi $A = \displaystyle\sum_{i=1}^{n} \| u(e_i) \|^2 = \sum_{i=1}^{n} \langle u(e_i) \mid u(e_i) \rangle$ et, en introduisant l'adjoint de u :

$$A = \sum_{i=1}^{n} \langle e_i \mid u^* \circ u(e_i) \rangle.$$

Sous cette dernière forme, on reconnaît la trace de $u^* \circ u$: $A = \text{Tr}\left(u^* \circ u\right)$.

Ex. 8

1) φ est le produit scalaire euclidien canonique sur $\mathcal{M}_n(\mathbb{R})$.

2) Soit $f : E \to E, X \mapsto AX - XA$. Il est clair que $f \in \mathcal{L}(E)$, que $C(A) = \text{Ker} f$, et que la proposition (i) est alors équivalente à $B \in \text{Im} f$.

D'autre part, puisque $AX = XA$ équivaut à ${}^tX\,{}^tA = {}^tA\,{}^tX$, on a $X \in C(A) \iff {}^tX \in C({}^tA)$ et donc :

$$(ii) \iff \forall X \in C({}^tA), \text{Tr}\left(B\,{}^tX\right) = 0$$

$$(ii) \iff \forall X \in C({}^tA), \langle B \mid X \rangle = 0$$

$$\text{ou encore } (ii) \iff B \in C({}^tA)^{\perp}.$$

Copyrighted material

Pour conclure, il suffit donc de comparer $\mathrm{Im}\, f$ et $C({}^tA)^\perp$. Or on sait que $\mathrm{Im}\, f = \left(\mathrm{Ker}\, f^*\right)^\perp$, déterminons donc f^*.

Pour tout $(X, Y) \in E^2$, on a :

$$\begin{aligned}\langle f(X) \mid Y\rangle &= \langle AX \mid Y\rangle - \langle XA \mid Y\rangle \\ &= \mathrm{Tr}\left({}^tYAX\right) - \mathrm{Tr}\left(XA\,{}^tY\right)\end{aligned}$$

donc, sachant que $\mathrm{Tr}(MN) = \mathrm{Tr}(NM)$ pour tout $(M, N) \in E^2$, il vient :

$$\begin{aligned}\langle f(X) \mid Y\rangle &= \mathrm{Tr}\left(X\,{}^tYA\right) - \mathrm{Tr}\left(XA\,{}^tY\right) \\ &= \langle X \mid {}^tAY - Y\,{}^tA\rangle\end{aligned}$$

Il en résulte que f^* est l'application $Y \mapsto {}^tAY - Y\,{}^tA$, et donc que $\mathrm{Im}\, f = \left(\mathrm{Ker}\, f^*\right)^\perp = C({}^tA)^\perp$.

Finalement, on a : $(i) \iff B \in \mathrm{Im}\, f \iff B \in C({}^tA)^\perp \iff (ii)$.

Ex. 9

$S = {}^tAA$ est symétrique réelle donc il existe $U \in \mathcal{O}_n(\mathbb{R})$ telle que :

$${}^tUSU = \mathrm{diag}\left(\lambda_1, \cdots, \lambda_n\right) = D.$$

A et ${}^tA$ étant permutables, on a $S^2 = {}^tA^2A^2$ et $S^3 = {}^tA^3A^3$ donc $A^3 = A^2$ donne $S^3 = S^2$ c'est-à-dire $D^3 = D^2$.

Avec $D^3 = D^2$, on obtient $\forall i \in [\![1, n]\!]$, $\lambda_i^3 = \lambda_i^2$ donc $\lambda_i \in \{0, 1\}$.

Enfin $\lambda_i \in [\![0, 1]\!]$, pour tout i, donnne $\lambda_i^2 = \lambda_i$ et donc $D^2 = D$ puis $S^2 = S$.

Calculons alors $\|A^2 - A\|^2 = \mathrm{Tr}\left({}^t\left(A^2 - A\right)\left(A^2 - A\right)\right)$. On développe :

$$\begin{aligned}M &= {}^t\left(A^2 - A\right)\left(A^2 - A\right) \\ &= {}^tA^2A^2 + {}^tAA - {}^tA^2A - {}^tAA^2 \\ &= S^2 + S - {}^tAS - SA \\ &= 2S - {}^tAS - SA \ \text{ car } \ S^2 = S.\end{aligned}$$

Avec $S = S^2 = {}^tA^2A^2$, on obtient aussi :

$${}^tAS = {}^tAS^2 = {}^tA^3A^2 = {}^tA^2A^2 \ \text{ car } \ A^3 = A^2$$

donc $${}^tAS = S^2 = S.$$

De même $SA = S^2A = {}^tA^2A^3 = {}^tA^2A^2$ donc :

$$SA = S^2 = S.$$

Finalement, $M = 0$ et a fortiori $\|A^2 - A\|^2 = \mathrm{Tr}(M) = 0$ donc $A^2 = A$.

Ex. 10

- Si $A \in \mathcal{O}_n(\mathbb{R})$ est solution du problème associée au réel λ, on a $\det\left(A - \lambda I_n\right) = 0$, donc λ est valeur propre de A et puisque A est orthogonale, on a nécessairement $\lambda = 1$ ou -1.
- Supposons $\lambda = 1$ et $\left(A - I_n\right)^2 = 0$ avec $A \in \mathcal{O}_n(\mathbb{R})$.

On sait que $M \mapsto \left(\mathrm{Tr}\,{}^tMM\right)^{\frac{1}{2}}$ est la norme euclidienne canonique sur $\mathcal{M}_n(\mathbb{R})$. Formons donc :

$$\begin{aligned}\|A - I_n\|^2 &= \mathrm{Tr}\left({}^t\left(A - I_n\right)\left(A - I_n\right)\right) \\ &= \mathrm{Tr}\left(2I_n - A - {}^tA\right)\end{aligned}$$

Or $\quad 2I_n - A - {}^tA = -{}^tA\left(A^2 + I_n - 2A\right) \quad (\text{car } {}^tAA = I_n)$

$$= -{}^tA\left(A - I_n\right)^2 = 0$$

donc $\|A - I_n\|^2 = 0$ et $A = I_n$.

- De même, pour $\lambda = -1$, en supposant $(A + I_n)^2 = 0$, on obtient :

$$\|A + I_n\|^2 = \mathrm{Tr}\left({}^tA\left(A + I_n\right)^2\right) = 0 \ \text{ donc } \ A = -I_n.$$

Les seules solutions du problème sont I_n $(\lambda = 1)$ et $-I_n$ $(\lambda = -1)$.

Copyrighted material

Ex. 11

1) En notant c_1, c_2 et c_3 les vecteurs-colonnes de A dans la base canonique (i, j, k) de $\mathbb{R}^3$, on vérifie :

$$\begin{cases} \|c_1\| = \|c_2\| = \|c_3\| = 1 \\ \langle c_1 \,|\, c_2 \rangle = \langle c_2 \,|\, c_1 \rangle = \langle c_3 \,|\, c_1 \rangle = 0 \end{cases}$$

et A est une matrice orthogonale. Notons qu'elle n'est pas symétrique.

Le terme $-\frac{7}{9}$ est l'opposé de son cofacteur, on a donc $\det A = -1$.

A est orthogonalement semblable à une matrice $B = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

De $\operatorname{Tr} A = \operatorname{Tr} B$, on déduit $-\frac{23}{9} = 2\cos\theta - 1$ et $\cos\theta = -\frac{7}{9}$.

$A + I_3 = \frac{1}{9}\begin{pmatrix} 2 & -4 & 4 \\ 4 & 1 & -1 \\ -4 & -1 & 1 \end{pmatrix}$ permet de voir que $w = (0, 1, 1)$ est vecteur propre de A.

Le signe de $\sin\theta$ est celui de $\det(i, Ai, w) = \frac{1}{9}\begin{vmatrix} 1 & -7 & 0 \\ 0 & 4 & 1 \\ 0 & -4 & 1 \end{vmatrix} = \frac{8}{9}$. Par suite, $\theta = \operatorname{Arccos}\left(-\frac{7}{9}\right)$.

A représente la composée (commutative) de la réflexion de plan $w^\perp$ et de la rotation d'angle θ autour de w.

2) Posons $V = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$, $X = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $Y = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}$ et $U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

Alors $C = \begin{pmatrix} x & z & \alpha' \\ y & t & \beta' \\ \alpha & \beta & \gamma \end{pmatrix} = \begin{pmatrix} V & Y \\ {}^tX & \gamma \end{pmatrix}$ commute avec $B = \begin{pmatrix} U & 0 \\ 0 & -1 \end{pmatrix}$ si et seulement si :

$$UV = VU \;,\; {}^tXU = -{}^tX \;,\; UY = -Y.$$

Les deux dernières conditions donnent $X = 0$ et $Y = 0$.

On vérifie que $V = \begin{pmatrix} x & z \\ y & t \end{pmatrix}$ commute avec $U = (\cos\theta)I_3 + \sin\theta\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ si et seulement si V commute avec $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ donc si et seulement si $t = x$ et $z = -y$.

Finalement, les matrices qui commutent avec B sont $M = \begin{pmatrix} x & -y & 0 \\ y & x & 0 \\ 0 & 0 & \gamma \end{pmatrix}$.

Elles forment un sous-espace de dimension 3 de $\mathcal{M}_3(\mathbb{R})$. Le commutant de A est donc de dimension 3 lui aussi.

Comme (I_3, A, A^2) est une famille libre, il vient que le commutant de A est $\operatorname{Vect}(I_3, A, A^2)$.

Ex. 12

Puisque $\mathcal{SO}(E)$ est un groupe, comme produit de trois rotations, $f = r^{-1} \circ R \circ r$ est une rotation.

- Soit v un vecteur normé, directeur de l'axe de f. $r^{-1} \circ R \circ r(v) = v$ équivaut à $R \circ r(v) = r(v)$, ce qui montre que $r(v)$ est un vecteur directeur (normé) u de R : $v = r^{-1}(u)$.
- Soit α l'angle de f mesuré autour de v. Avec $\operatorname{Tr} f = 2\cos\alpha + 1$, $\operatorname{Tr} f = \operatorname{Tr}\left(r^{-1} \circ R \circ r\right) = \operatorname{Tr} R$ et $\operatorname{Tr} R = 2\cos\theta + 1$ où θ désigne l'angle de R mesuré autour de u, il vient $\cos\alpha = \cos\theta$.
- Il reste à examiner si $\sin\alpha$ et $\sin\theta$ ont le même signe ou non.

Soit x non colinéaire à $v = r^{-1}(u)$. Alors $\sin\alpha$ est du signe du produit mixte :

$$\left[v, x, f(x)\right] = \left[r^{-1}(u), r^{-1} \circ r(x), r^{-1} \circ R \circ r(x)\right] = \left(\det r^{-1}\right)\left[u, r(x), R(r(x))\right].$$

Or $\det r^{-1} = 1$ et $\left[u, r(x), R(r(x))\right]$ a le même signe que $\sin\theta$.

Il s'ensuit que $\sin\alpha$ et $\sin\theta$ ont le même signe et, en conclusion : $\alpha = \theta$, à 2π près.

Finalement, si R est une rotation d'angle θ autour de u, alors, pour toute rotation r, $r^{-1} \circ R \circ r$ est la rotation d'angle θ autour de $r^{-1}(u)$.

Copyrighted material

Hidden page

Ex. 15

La matrice A est symétrique réelle. Son polynôme caractéristique est donc scindé dans $\mathbb{R}[X]$.

Il est immédiat que A est de rang 2 et donc que 0 est valeur propre d'ordre $n-2$.

$\lambda \in \mathbb{R}^*$ est valeur propre si et seulement si il existe $x = (x_1, \dots, x_n)$ non nul tel que :

$$\begin{cases} \lambda x_1 = x_n \\ \lambda x_2 = 2x_n \\ \vdots \\ \lambda x_{n-1} = (n-1)x_n \\ \lambda x_n = x_1 + 2x_2 + \dots + (n-1)x_{n-1} + nx_n \end{cases}$$

Les $n-1$ premières équations donnent : $x_1 = \dfrac{1}{\lambda}x_n,\ x_2 = \dfrac{2}{\lambda}x_n, \dots, x_{n-1} = \dfrac{n-1}{\lambda}x_n$.

$x \neq (0, \dots, 0)$ équivaut donc à $x_n \neq 0$.

La dernière équation donne alors :

$$\lambda = n + \sum_{k=1}^{n-1} \frac{k^2}{\lambda} \text{ c'est-à-dire } \lambda^2 - n\lambda - \frac{n(n-1)(2n-1)}{6} = 0$$

et le polynôme caractéristique de A est :

$$(-1)^n X^{n-2}\left(X^2 - nX - \frac{n(n-1)(2n-1)}{6}\right).$$

Ex. 16

1) Par hypothèse, 0 n'est pas valeur propre de u ce qui assure l'existence de u^{-1}. Il existe une base orthonormale $(e_i)_{1 \leqslant i \leqslant n}$ de E formée de vecteurs propres de u, donc aussi de u^{-1} car $u(x) = \lambda x$ donne $u^{-1}(x) = \dfrac{1}{\lambda}x$.

Sur cette base, en posant $x = \sum_{i=1}^{n} x_i e_i$ et $\forall i \in [\![1, n]\!],\ u(e_i) = \lambda_i e_i$, on a :

$$\langle u(x) \,|\, x \rangle = \sum_{i=1}^{n} \lambda_i x_i^2 \quad , \quad \langle u^{-1}(x) \,|\, x \rangle = \sum_{i=1}^{n} \frac{x_i^2}{\lambda_i}.$$

Donc en introduisant les vecteurs $a = \sum_{i=1}^{n} x_i \sqrt{\lambda_i} e_i$ et $b = \sum_{i=1}^{n} \dfrac{x_i}{\sqrt{\lambda_i}} e_i$ il vient : $f(x) = \|a\|^2 \|b\|^2$, et d'après l'inégalité de Cauchy-Schwarz : $f(x) \geqslant \langle a \,|\, b \rangle^2$.

D'autre part, $\langle a \,|\, b \rangle = \sum_{i=1}^{n} x_i^2 = 1$ lorsque $x \in S$ donc $\inf_{x \in S} f(x) \geqslant 1$.

Il suffit de remarquer que pour $x = e_i \in S$, $f(e_i) = 1$ pour conclure à $\inf_{x \in S} f(x) = 1$.

2) Étant donné $x \in S$, on a $f(x) = 1$ si et seulement si en ce point x :

$$|\langle a \,|\, b \rangle| = \|a\| \, \|b\|.$$

On sait que cette égalité est réalisée si et seulement si le couple (a, b) est lié, c'est-à-dire, puisque a et b sont non nuls, si et seulement si il existe $\rho \in \mathbb{R}^*$ tel que $a = \rho b$, soit aussi :

$$\forall i \in [\![1, n]\!], \quad (\lambda_i - \rho) x_i = 0.$$

L'un au moins des x_i est non nul, on a donc nécessairement $\rho = \lambda_{i_0}$. Alors le système :

$$(\lambda_i - \lambda_{i_0}) x_i = 0, \quad 1 \leqslant i \leqslant n,$$

donne $x_i = 0$ pour $\lambda_i \neq \lambda_{i_0}$ soit aussi $x \in \operatorname{Ker}(u - \lambda_{i_0} \operatorname{Id}_E)$.

En conclusion, les points de S en lesquels f atteint son minimum sont les vecteurs propres de u de norme 1.

Copyrighted material

Hidden page

P orthogonale est matrice de passage de la base orthonormale (I, J) à une base (I', J') également orthonormale.
Les formules de passage s'écrivent :

$$U = PU' \quad \text{ou} \quad \begin{pmatrix} X \\ Y \end{pmatrix} = P \begin{pmatrix} X' \\ Y' \end{pmatrix}.$$

On a ${}^tUAU = {}^tU' \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} U' = \lambda X'^2 + \mu Y'^2$. Et avec $X^2 + Y^2 = X'^2 + Y'^2$, il vient :

$$f(u) = \frac{\lambda X'^2 + \mu Y'^2}{X'^2 + Y'^2}.$$

c) En posant $X' = r\cos\theta$, $Y' = r\sin\theta$, il vient $f(u) = \lambda\cos^2\theta + \mu\sin^2\theta$.
Supposons $\lambda \leqslant \mu$, alors $f(u) = \lambda + (\mu - \lambda)\sin^2\theta = (\lambda - \mu)\cos^2\theta + \mu$ donne :

$$\text{pour tout } u \neq 0, \quad \lambda \leqslant f(u) \leqslant \mu.$$

De plus, pour $\theta = 0$, $f(u) = \lambda$ et pour $\theta = \frac{\pi}{2}$, $f(u) = \mu$, d'où finalement :

$$\max_{\mathbb{R}^2 \setminus \{(0,0)\}} f = \mu \quad \text{et} \quad \min_{\mathbb{R}^2 \setminus \{(0,0)\}} f = \lambda.$$

Pour conclure, on calcule donc les valeurs propres λ et μ de A, ce sont les racines de l'équation $x^2 - \frac{5}{2}x + \frac{11}{8} = 0$.

On trouve $\lambda = \frac{5 - \sqrt{3}}{4}$, $\mu = \frac{5 + \sqrt{3}}{4}$.

Ex. 19

▪ Analyse

Soit $f \in \mathcal{L}(E)$ une solution du problème. On a alors :

$$\begin{array}{rcccl} \|f(j + 2k)\| & = & 15\|i - 2k\| & = & 15\|j + 2k\| \\ \|f(i + 2j - k\| & = & 15\|2i - j + k\| & = & 15\|i + 2j - k\| \end{array}$$

donc $g = \frac{1}{15}f$ est un automorphisme orthogonal vérifiant :

$$g(j + 2k) = i - 2k \qquad \textbf{(1)}$$

$$g(i + 2j - k) = 2i - j + k \qquad \textbf{(2)}$$

Si g est une rotation, $\big(g(i), g(j), g(k)\big)$ est une base orthonormale directe. Donc, en posant $I = g(i)$, $J = g(j)$, $K = g(k)$ et en effectuant le produit vectoriel membre à membre de **(1)** et **(2)**, on obtient :

$$(J + 2K) \wedge (I + 2J - K) = (i - 2k) \wedge (2i - j + k) \text{ c'est-à-dire } -5I + 2J - K = -2i - 5j - k \qquad \textbf{(3)}$$

Ainsi (I, J, K) vérifie le système :

$$\begin{cases} J + 2K = i - 2k & \textbf{(1)} \\ I + 2J - K = 2i - j + k & \textbf{(2)} \\ -5I + 2J - K = -2i - 5j - k & \textbf{(3)} \end{cases}$$

On en déduit :

$$I = \frac{2}{3}i + \frac{2}{3}j + \frac{1}{3}k$$

$$J = \frac{11}{15}i - \frac{2}{3}j - \frac{2}{15}k$$

$$K = \frac{2}{15}i + \frac{1}{3}j - \frac{14}{15}k$$

Si g est une antirotation, $\big(g(i), g(j), g(k)\big)$ est une base orthonormale rétrograde et avec les mêmes notations, on obtient :

$$5I - 2J + K = -2i - 5j - k \qquad \textbf{(4)}$$

Ainsi (I, J, K) est maintenant solution du système :

$$\begin{cases} J + 2K = i - 2k & \textbf{(1)} \\ I + 2J - K = 2i - j + k & \textbf{(2)} \\ 5I - 2J + K = -2i - 5j - k & \textbf{(4)} \end{cases} \quad \text{d'où on tire } I = -j,\ J = i,\ K = -k.$$

Copyrighted material

Hidden page

La condition portant sur les termes diagonaux de T s'exprime par $\forall p \in [\![1, n]\!]$, $\det u_p > 0$.

Ainsi, $T \in \mathcal{T}$ équivaut à $\forall p \in [\![1, n]\!]$, $u(E_p) = E_p$ et $\det u_p > 0$.

Avec cette caractérisation, il vient aisément que $\forall (T_1 . T_2) \in \mathcal{T}^2$, $T_1 T_2 \in \mathcal{T}$ et $\forall T \in \mathcal{T}$, $T \in \mathrm{GL}_n(\mathbb{R})$ et $T^{-1} \in \mathcal{T}$.

D'autre part, $\mathcal{T}$ est non vide puisqu'il contient I_n. C'est donc un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

2) La forme polaire de q est un produit scalaire sur $\mathbb{R}^n$.

Le procédé d'orthonormalisation de Schmidt donne l'existence d'une base q-orthonormale $\mathcal{B}' = (e'_1, \ldots, e'_n)$ telle que la matrice de passage P de $\mathcal{B}$ à $\mathcal{B}'$ soit dans $\mathcal{T}$.

Matriciellement, ce changement de base se traduit par ${}^tPAP = I_n$. Alors $T = P^{-1} \in \mathcal{T}$ donne $A = {}^tTT$ ce qui prouve l'existence souhaitée.

Reste à prouver l'unicité.

Soit $T_1 \in \mathcal{T}$ telle que $A = {}^tT_1 T_1$. De ${}^tTT = {}^tT_1 T_1$, on déduit ${}^tT_1^{-1}\,{}^tT = T_1 T^{-1}$ **(1)**.

Nous savons que $S = T_1 T^{-1}$ est dans $\mathcal{T}$ et que $S^{-1} = TT_1^{-1}$ est aussi dans $\mathcal{T}$. Comme **(1)** se lit alors ${}^tS^{-1} = S$, la matrice S est orthogonale.

Étant en outre triangulaire à éléments diagonaux strictement positifs, S est nécessairement égale à I_n, d'où il vient $T_1 = T$.

Ex. 22

1) Les inclusions $\mathrm{Ker}\, f \subset \mathrm{Ker}\,(f^* \circ f)$ et $\mathrm{Im}\,(f^* \circ f) \subset f^*$ sont usuelles.

Soit $x \in \mathrm{Ker}\,(f^* \circ f)$. On a $\|f(x)\|^2 = \langle f^* \circ f(x) \,|\, x \rangle = 0$ d'où $x \in \mathrm{Ker}\, f$. Il vient alors $\mathrm{Ker}\, f = \mathrm{Ker}\,(f^* \circ f)$.

On sait que $\mathrm{rg}\, f^* = \mathrm{rg}\, f$. Le théorème du rang et l'égalité des noyaux donne $\mathrm{rg}\, f = \mathrm{rg}\, f^* \circ f$.

Alors $\mathrm{Im}\,(f^* \circ f) \subset f^*$ et $\mathrm{rg}\, f^* = \mathrm{rg}\,(f^* \circ f)$ donne $\mathrm{Im}\,(f^* \circ f) = f^*$.

2) Pour $f \in A$, posons $p = f^* \circ f$. On a $p^* = p$ et $p^2 = f^* \circ (f \circ f^* \circ f) = f^* \circ f = p$.

Ainsi, p est un projecteur orthogonal.

Réciproquement, supposons que $p = f^* \circ f$ est un projecteur orthogonal.

Pour tout x de E, on a $f^* \circ f(x) = p(x) = p^2(x) = (f^* \circ f)(f^* \circ f(x))$, donc $f^* \circ f(x) - x$ est dans le noyau de $f^* \circ f$.

Il est donc dans le noyau de f, d'où $f \circ f^* \circ f(x) = f(x)$ puis $f \circ f^* \circ f = f$.

3) Si f est dans A, alors $p = f^* \circ f$ est un projecteur orthogonal, donc $(\mathrm{Ker}\, p)^\perp = \mathrm{Im}\, p$.

Avec $\mathrm{Ker}\, f = \mathrm{Ker}\,(f^* \circ f)$, il vient alors $(\mathrm{Ker}\, f)^\perp = \mathrm{Im}\, p$.

Il s'ensuit, pour tout $x \in (\mathrm{Ker}\, f)^\perp$, $\|f(x)\|^2 = \langle f^* \circ f(x) \,|\, x \rangle = \langle p(x) \,|\, x \rangle = \|x\|^2$.

Réciproquement, supposons que $\forall x \in (\mathrm{Ker}\, f)^\perp$, $\|f(x)\|^2 = \|x\|^2$.

Notons que, pour tout x et y dans $(\mathrm{Ker}\, f)^\perp$, on a :

$$\langle f^* \circ f(x) \,|\, y \rangle = \langle f(x) \,|\, f(y) \rangle = \frac{1}{2}\left(\|f(x+y)\|^2 - \|f(x)\|^2 - \|f(y)\|^2\right),$$

donc $\langle f^* \circ f(x) \,|\, y \rangle = \frac{1}{2}\left(\|x+y\|^2 + \|x\|^2 - \|y\|^2\right) = \langle x \,|\, y \rangle$.

Il s'ensuit que $f^* \circ f(x) - x$ est dans $\left((\mathrm{Ker}\, f)^\perp\right)^\perp = \mathrm{Ker}\, f$, donc $f \circ f^* \circ f(x) = f(x)$.

Il reste à remarquer que cette égalité est banale pour tout $x \in \mathrm{Ker}\, f$ pour en déduire $f \circ f^* \circ f = f$.

4) On vient de voir que $(\mathrm{Ker}\, f)^\perp \subset \{x \in E \,/\, \|f(x)\| = \|x\|\}$.

Réciproquement, soit $x \in E$ tel que $\|f(x)\| = \|x\|$.

Décomposons x en $x = x_1 + x_2$ avec $x_1 \in \mathrm{Ker}\, f$ et $x_2 \in (\mathrm{Ker}\, f)^\perp$.

On a alors $\|x\|^2 = \|x_1\|^2 + \|x_2\|^2$ avec le théorème de Pythagore.

On a aussi $f(x) = f(x_2)$ donc $\|f(x)\|^2 = \|f(x_2)\|^2$. En outre, $\|f(x_2)\|^2 = \|x_2\|^2$ puisque f conserve la norme de tout vecteur de $(\mathrm{Ker}\, f)^\perp$.

On en déduit $\|x_1\|^2 + \|x_2\|^2 = \|x_2\|^2$, d'où $x_1 = 0$ et $x = x_2$ ce qui montre que $x \in (\mathrm{Ker}\, f)^\perp$.

Copyrighted material

Niveau 3

Ex. 23

Rappelons que $M \mapsto \sqrt{\mathrm{Tr}({}^tMM)}$ est la norme euclidienne canonique sur $\mathcal{M}_n(\mathbb{R})$. On notera $\mathrm{Tr}\left({}^tMM\right) = \| M \|^2$.

▪ Recherche de conditions nécessaires

On suppose que $A \in \mathcal{M}_n(\mathbb{R})$ est solution de l'équation. Sachant que $\left({}^t\mathrm{Com}\, A\right)A = (\det A)I_n$, on obtient :

$$ {}^tAA = \lambda(\det A)I_n \qquad (2)$$

Cette égalité impose $\det A \geqslant 0$, en effet ${}^tAA$ est une matrice symétrique réelle positive dont les éléments diagonaux sont les carrés scalaires (dans $\mathbb{R}^n$ euclidien canonique) des vecteurs colonnes de A.

Envisageons alors deux cas :

a) $\det A = 0$: l'égalité **(2)** devient ${}^tAA = 0$ donc $\| A \|^2 = 0$ et $A = 0$.

b) $\det A > 0$:

En prenant le déterminant des deux membres, l'égalité **(2)** donne :

$$(\det A)^2 = \lambda^n(\det A)^n \quad \text{donc} \quad (\det A)^{2-n} = \lambda^n ;$$

• si $n = 2$, il reste $\lambda^2 = 1$ donc $\lambda = 1$ et d'après **(1)** $A = \mathrm{Com}\, A$.

Dans ce cas on a $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\mathrm{Com}\, A = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$ donc $a = d$, $c = -b$ et $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ soit encore, en posant $k = \sqrt{a^2 + b^2}$, $A = kR$ où R est une matrice de rotation : $R \in \mathcal{SO}_2(\mathbb{R})$;

• si $n \geqslant 3$, il vient $\det A = \lambda^{\frac{n}{2-n}}$ et en reportant dans **(2)** : ${}^tAA = \lambda^{\frac{2}{2-n}} I_n$ soit en encore, en posant $R = \lambda^{\frac{1}{n-2}} A$

$$ {}^tRR = I_n \qquad (3)$$

Avec $\det R = \lambda^{\frac{n}{n-2}} \det A = 1$, la relation **(3)** donne que R est une matrice de rotation, donc :

$$A = \lambda^{\frac{1}{2-n}} R \quad \text{avec} \quad R \in \mathcal{SO}_n(\mathbb{R}).$$

En conclusion, si A est solution de **(1)**, nécessairement :

$$A = 0 \quad \text{ou} \quad A = kR \quad \text{avec} \quad R \in \mathcal{SO}_n(\mathbb{R})$$

et $k = \lambda^{\frac{1}{2-n}}$ si $n \geqslant 3$, k quelconque dans $\mathbb{R}_+^*$ et $\lambda = 1$ si $n = 2$.

▪ Conditions suffisantes

On examine si les matrices précédentes conviennent. Il est clair que la matrice nulle est solution.

Pour $n = 2$,

si $\lambda \neq 1$ le problème n'a pas de solution ;

si $\lambda = 1$ toute matrice $A = k\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, $k \in \mathbb{R}_+^*$, $\theta \in \mathbb{R}$ est solution.

Pour $n \geqslant 3$, soit $A = \lambda^{\frac{1}{2-n}} R$ avec $R \in \mathcal{SO}_n(\mathbb{R})$.

On a alors $\det A = \lambda^{\frac{n}{2-n}} \det R = \lambda^{\frac{n}{2-n}}$ et $A^{-1} = \lambda^{\frac{-1}{2-n}}\, {}^tR$.

Avec $A^{-1} = \dfrac{1}{\det A}\, {}^t\mathrm{Com}\, A$ on en déduit $\mathrm{Com}\, A = \lambda^{\frac{n-1}{2-n}} R$ donc $\lambda\, \mathrm{Com}\, A = \lambda^{\frac{1}{2-n}} R = A$: A est solution.

▪ Conclusion

Soit S l'ensemble des solutions de **(1)**.

Si $n = 2$:

$$\begin{aligned} &\lambda \neq 1 \quad \text{alors} \quad S = \{0\} \\ &\lambda = 1 \quad \text{alors} \quad S = \left\{ kR \,/\, k \in \mathbb{R}^*,\ R \in \mathcal{SO}_2(\mathbb{R}) \right\} \end{aligned}$$

(pour $k = 0$, on retrouve la matrice nulle).

Si $n \geqslant 3$, $S = \{0\} \cup \{\lambda^{\frac{1}{2-n}} R \,/\, R \in \mathcal{SO}_n(\mathbb{R})\}$.

Copyrighted material

Ex. 24

Pour tout $x \in E$, $\| u(x) \| \leqslant \| a \| \| x \|$ et par récurrence $\| u^n(x) \| \leqslant \| a \|^n \| x \|$, $(n \in \mathbb{N})$.

La convergence de la série numérique $\sum_{n=0}^{+\infty} \frac{\| a \|^n}{n!}$ donne l'absolue convergence de la série de terme général $\frac{u^n(x)}{n!}$.

Avec la formule du double produit vectoriel, on obtient :

$$u^2(x) = \langle a \,|\, x \rangle a - \| a \|^2 x \text{ d'où } u^3(x) = -\| a \|^2 u(x).$$

Par récurrence, il vient alors :

$$\forall n \in \mathbb{N},\ u^{2n+1}(x) = (-1)^n \| a \|^{2n} u(x) \ .\ u^{2n+2}(x) = (-1)^n \| a \|^{2n} u^2(x).$$

En conséquence :

$$r(x) = x + \sum_{n=0}^{+\infty} (-1)^n \frac{\| a \|^{2n}}{(2n+2)!} u^2(x) + \sum_{n=0}^{+\infty} (-1)^n \frac{\| a \|^{2n}}{(2n+1)!} u(x)$$

et, d'après les développements en série entière des fonctions cosinus et sinus :

$$r(x) = x + \frac{1 - \cos \| a \|}{\| a \|^2} u^2(x) + \frac{\sin \| a \|}{\| a \|} u(x).$$

Avec $u(x) = a \wedge x$ et $u^2(x) = \langle a \,|\, x \rangle a - \| a \|^2 x$, en posant $\theta = \| a \|$ et $\omega = \frac{a}{\| a \|}$, on retrouve :

$$r(x) = x \cos \theta + (1 - \cos \theta) \langle \omega \,|\, x \rangle \, \omega + (\omega \wedge x) \sin \theta.$$

Donc r est la rotation d'axe $\mathbb{R}a$ et d'angle $\| a \|$.

Ex. 25

1) Si $x = y$, $\theta(x, x, z) = [f(x), x, z] + [x, f(x), z] + [x, x, f(z)] = 0$ car le produit mixte est alterné et antisymétrique.
De même, $\theta(x, y, z) = 0$ si $x = z$ ou si $y = z$ et θ est une forme alternée.
La linéarité de f et la trilinéarité du produit mixte entraînent la trilinéarité de θ.
L'espace des formes trilinéaires alternées sur E est de dimension 1, engendré par l'application produit mixte.
Il existe donc $\lambda \in \mathbb{R}$ tel que :

$$\forall (x, y, z) \in E^3,\ \theta(x, y, z) = \lambda [x, y, z].$$

En particulier, pour une base orthonormale directe (e_1, e_2, e_3) de E, $\theta(e_1, e_2, e_3) = \lambda$. Or :

$$\begin{aligned} \theta(e_1, e_2, e_3) &= [f(e_1), e_2, e_3] + [e_3, e_1, f(e_2)] + [e_1, e_2, f(e_3)] \\ &= \langle e_1 \,|\, f(e_1) \rangle + \langle e_2 \,|\, f(e_2) \rangle + \langle e_3 \,|\, f(e_3) \rangle. \end{aligned}$$

Il s'ensuit $\lambda = \operatorname{Tr} f$ et $\theta(x, y, z) = (\operatorname{Tr} f)[x, y, z]$ pour tout $(x, y, z) \in E^3$.

2) S'il existe $g \in \mathcal{L}(E)$ tel que, pour tout $(x, y) \in E^2$, $g(x \wedge y) = f(x) \wedge y + x \wedge f(y)$, on a, pour tout $z \in E$:

$$\langle g(x \wedge y) \,|\, z \rangle = \langle f(x) \wedge y + x \wedge f(y) \,|\, z \rangle,$$

d'où :

$$\langle g(x \wedge y) \,|\, z \rangle = [f(x), y, z] + [x, f(y), z].$$

Avec le résultat précédent, il vient $\langle g(x \wedge y) \,|\, z \rangle = (\operatorname{Tr} f)[x, y, z] - [x, y, f(z)]$.

Puis, avec $[x, y, f(z)] = \langle x \wedge y \,|\, f(z) \rangle = \langle f^*(x \wedge y) \,|\, z \rangle$ et $[x, y, z] = \langle x \wedge y \,|\, z \rangle$, on obtient :

$$\langle g(x \wedge y) \,|\, z \rangle = \langle (\operatorname{Tr} f) x \wedge y - f^*(x \wedge y) \,|\, z \rangle$$

d'où $g(x \wedge y) = (\operatorname{Tr} f) x \wedge y - f^*(x \wedge y)$ et, puisque $x \wedge y$ décrit E quand (x, y) décrit E^2, $g = (\operatorname{Tr} f) \operatorname{Id}_E - f^*$ est le seul endomorphisme possible.
On vérifie sans peine, en remontant les calculs, que $g = (\operatorname{Tr} f) \operatorname{Id}_E - f^*$ convient.

Ex. 26

1) Soit (I, J, K) une base orthonormale de E où $K = \frac{1}{\sqrt{3}}(i + j + k)$ (sans préciser davantage le choix de I et J).

En posant $u = xi + yk + zk = XI + YJ + ZK$, il vient (changement de coordonnées) :

$$Z = \langle u \,|\, K \rangle = \frac{1}{\sqrt{3}}(x + y + z) \text{ et } x^2 + y^2 + z^2 = X^2 + Y^2 + Z^2 = \| u \|^2.$$

Copyrighted material

On a alors : $2q(u) = (x+y+z)^2 - (x^2+y^2+z^2) = 2Z^2 - X^2 - Y^2$. Donc C est le cône de révolution d'axe $\mathbb{R}K$, de demi-angle au sommet $\alpha = \text{Arctan}\sqrt{2}$.

2) Soit le plan $\mathcal{P}$ d'équation $\alpha x + \beta y + \gamma z = 0$ $(\alpha, \beta, \gamma) \neq (0,0,0)$ et q' la restriction de q à $\mathcal{P}$.

La matrice de q' dans une base (u, v) de $\mathcal{P}$ est $\begin{pmatrix} q(u) & \varphi(u,v) \\ \varphi(u,v) & q(v) \end{pmatrix}$ où φ est la forme polaire de q.

Dans la base (u, v) de $\mathcal{P}$, $C' = C \cap \mathcal{P}$ a pour équation $q\left(x'u + y'v\right) = 0$ c'est-à-dire :

$$x'^2 q(u) + 2x'y'\,\varphi(u,v) + y'^2 q(v) = 0.$$

Si (u, v) est une base orthonormale de $\mathcal{P}$, C' est réunion de deux droites orthogonales si et seulement si $q(u) + q(v) = 0$ (voir l'exercice 6).

- Cas $(\alpha, \beta) \neq (0,0)$

Choisissons d'abord une base orthogonale $\left(u', v'\right)$ du plan $\mathcal{P}$: $u' = \beta i - \alpha j$, $v' = \gamma(\alpha i + \beta j) - \left(\alpha^2 + \beta^2\right) k$.

Avec $u = \dfrac{u'}{\|u'\|}$, $v = \dfrac{v'}{\|v'\|}$, (u, v) est une base orthonormale de $\mathcal{P}$. $q(u) + q(v) = 0$ s'écrit aussi :

$$\|v'\|^2 q(u') + \|u'\|^2 q(v') = 0 \qquad \textbf{(1)}$$

On calcule

$$q(u') = -\alpha\beta \qquad q(v') = \alpha\beta\gamma^2 - \left(\alpha^2+\beta^2\right)(\alpha\gamma + \beta\gamma)$$

$$\|u'\|^2 = \alpha^2 + \beta^2 \qquad \|v'\|^2 = \left(\alpha^2+\beta^2\right)\left(\alpha^2+\beta^2+\gamma^2\right)$$

L'équation **(1)** est équivalente à :

$$\alpha\beta + \beta\gamma + \gamma\alpha = 0 \qquad \textbf{(2)}$$

- Cas $(\alpha, \beta) = (0,0)$

L'équation de $\mathcal{P}$ est $z = 0$. Celles de $C' = C \cap \mathcal{P}$ sont $z = 0$, $xy = 0$. Dans ce cas, C' est la réunion des deux droites orthogonales $\mathbb{R}i$ et $\mathbb{R}j$. On constate que $(\alpha, \beta, \gamma) = (0,0,1)$ satisfait aussi à l'équation **(2)**.

Conclusion

Les plans vectoriels qui coupent le cône C suivant deux droites orthogonales sont les plans orthogonaux aux génératrices (ou droites) du cône C lui-même.

Ex. 27

1) Il existe $P \in \mathcal{O}_n(\mathbb{R})$ telle que ${}^tPAP = \text{diag}\left(\lambda_1, \cdots, \lambda_n\right) = D$.

On pose $X = PY$ (ce qui correspond à un changement de base orthonormale dans E muni de sa structure euclidienne canonique), avec $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ il vient alors :

$${}^tXAX = {}^tYDY = \sum_{i=1}^{n} \lambda_i y_i^2 \qquad {}^tXX = {}^tYY = \sum_{i=1}^{n} y_i^2.$$

Avec $\lambda_1\,{}^tYY - {}^tYDY = \sum_{i=1}^{n} \left(\lambda_1 - \lambda_i\right) y_i^2$, il est clair que :

$$\lambda_1\,{}^tYY - {}^tYDY \geqslant 0 \quad \text{c'est-à-dire} \quad \lambda_1\,{}^tXX \geqslant {}^tXAX$$

2) a) Développons le produit ${}^tXAX$: ${}^tXAX = \sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{1\leqslant i<j\leqslant n} a_{ij}x_ix_j = \sum_{i=1}^{n} a_{ii}|x_i|^2 + 2\sum_{1\leqslant i<j\leqslant n} a_{ij}x_ix_j$

$i \neq j \;\Rightarrow\; a_{ij} \geqslant 0$ donc $\sum_{1\leqslant i<j\leqslant n} a_{ij}x_ix_j \leqslant \sum_{1\leqslant i<j\leqslant n} a_{ij}|x_i|\,|x_j|$ et ${}^tXAX \leqslant {}^t\overline{X}A\overline{X}$.

b) Soit $X \in E$ un vecteur propre de A associé à λ_1 : $AX = \lambda_1 X$ ou $u(X) = \lambda_1 X$ où u est l'endomorphisme symétrique de E associé à A dans la base canonique.

On a alors : ${}^tXAX = \lambda_1\,{}^tXX$ et ${}^tXAX \leqslant {}^t\overline{X}A\overline{X} \leqslant \lambda_1\,{}^t\overline{X}\,\overline{X}$.

Copyrighted material

Or $ {}^t XX = {}^t\overline{X}\,\overline{X} = \sum_{i=1}^{n} x_i^2 $ d'où $ \lambda_1 {}^t\overline{X}\,\overline{X} \leqslant {}^t\overline{X}A\overline{X} \leqslant \lambda_1 {}^t\overline{X}\,\overline{X} $ et enfin $ {}^t\overline{X}A\overline{X} = \lambda_1 {}^t\overline{X}\,\overline{X}. $

Comme en 1), posons $ \overline{X} = PY' $, l'égalité précédente donne :

$$\sum_{i=1}^{n} (\lambda_1 - \lambda_i) y_i'^2 = 0$$

et puisque pour tout $ i \in [\![1, n]\!] $, $ \lambda_1 - \lambda_i $ est positif, il en résulte :

$$\forall i \in [\![1, n]\!], \quad (\lambda_1 - \lambda_i) y_i'^2 = 0$$

ce qui équivaut à $ y_i' = 0 $ pour tout $ i $ tel que $ \lambda_i \neq \lambda_1 $ donc encore à $ \overline{X} \in \operatorname{Ker}(u - \lambda_1 \operatorname{Id}_E) $.

Ex. 28

1) • **Analyse**

Supposons $ A = ST $ avec $ S \in \mathcal{O}_n(\mathbb{R}) $ et $ T $ triangulaire supérieure à éléments diagonaux $ t_{ii} $ dans $ \mathbb{R}_+^* $.

Alors $ T $ est inversible et $ U = T^{-1} $ est triangulaire supérieure à éléments diagonaux dans $ \mathbb{R}_+^* $: $ u_{ii} = \dfrac{1}{t_{ii}} $.

La relation $ A = ST $ s'écrit aussi $ AU = S $.

Interprétons dans $ \mathbb{R}^n $ euclidien canonique.

La matrice $ A $ est inversible, donc c'est la matrice de passage de $ \mathcal{B} = (e_i)_{1 \leqslant i \leqslant n} $ base canonique à une base $ \mathcal{B}' = (e_i')_{1 \leqslant i \leqslant n} $ (constituée des vecteurs colonnes de $ A $) : $ A = P_{\mathcal{B}\mathcal{B}'} $.

De même, $ U $ est inversible Il existe donc une base $ \mathcal{B}'' = (e_i'')_{1 \leqslant i \leqslant n} $ telle que $ U $ soit la matrice de passage de $ \mathcal{B}' $ à $ \mathcal{B}'' $: $ U = P_{\mathcal{B}'\mathcal{B}''} $.

On a alors $ S = AU = P_{\mathcal{B}\mathcal{B}'} P_{\mathcal{B}'\mathcal{B}''} = P_{\mathcal{B}\mathcal{B}''} $: $ S $ est la matrice de passage de $ \mathcal{B} $ à $ \mathcal{B}'' $. Puisque $ \mathcal{B} $ est une base orthonormale et que $ S $ est orthogonale, on en déduit que $ \mathcal{B}'' $ est une base orthonormale.

Ainsi $ U $ est la matrice de passage de $ \mathcal{B}' $ base des vecteurs colonnes de $ A $ à une base $ \mathcal{B}'' $ orthonormale. Le fait que $ U $ soit triangulaire supérieure équivaut à :

$$\forall i \in [\![1, n]\!], \ \operatorname{Vect}(e_1', \ldots, e_i') = \operatorname{Vect}(e_1'', \ldots, e_i'') \tag{1}$$

et les conditions $ u_{ii} > 0 $ donnent :

$$\forall i \in [\![1, n]\!], \ \langle e_i' \mid e_i'' \rangle > 0 \tag{2}$$

On en déduit que $ \mathcal{B}'' $ est l'unique base orthonormale de $ \mathbb{R}^n $ déduite de $ \mathcal{B}' $ par le procédé de Schmidt en observant les conditions **(2)**. Ceci prouve qu'il y a au plus un couple $ (S, T) $ solution du problème.

• **Synthèse**

Par le procédé de Schmidt en respectant les conditions **(2)**, on transforme la base $ \mathcal{B}' $ formée des vecteurs colonnes de $ A $ en une base $ \mathcal{B}'' $ orthonormale.

On a $ A = P_{\mathcal{B}\mathcal{B}'} $ et en posant $ U = P_{\mathcal{B}'\mathcal{B}''} $, on obtient $ AU = P_{\mathcal{B}\mathcal{B}''} $ avec $ U $ triangulaire supérieure et $ \forall i \in [\![1, n]\!], \ u_{ii} > 0 $. Les bases $ \mathcal{B} $ et $ \mathcal{B}'' $ étant orthonormales, $ S = AU $ est orthogonale. Il suffit alors de poser $ T = U^{-1} $ pour obtenir $ A = ST $ avec $ S \in \mathcal{O}_n(\mathbb{R}) $ et $ T $ triangulaire supérieure à éléments diagonaux dans $ \mathbb{R}_+^* $.

2) Sachant que $ S $ est orthogonale, on a $ \det S = \pm 1 $, donc :

$$(\det A)^2 = (\det T)^2 = \prod_{j=1}^{n} t_{jj}^2.$$

Or $ T = P_{\mathcal{B}''\mathcal{B}'} $ donc $ t_{jj} $ est la $ j^{\text{ème}} $ coordonnée de $ e_j' $ sur la base orthonormale $ \mathcal{B}'' $:

$$t_{jj} = \langle e_j'' \mid e_j' \rangle.$$

Il est donc clair que $ |t_{jj}| \leqslant \| e_j' \| $ d'où : $ (\det A)^2 \leqslant \prod_{j=1}^{n} \| e_j' \|^2 $.

On conclut en remarquant que : $ \| e_j' \|^2 = \sum_{i=1}^{n} a_{ij}^2 $.

Copyrighted material

CHAPITRE 8

Coniques Quadriques

Copyrighted material

Remarque : en géométrie, l'auteur s'obstine à noter les vecteurs avec une flèche !

A. Réduction de l'équation d'une conique

1. Courbes du second degré [1]

[1] $\mathscr{E}$ est le plan affine euclidien orienté $\mathbb{R}^2$.

Définition 1

Si, dans un repère $(O, \vec{i}, \vec{j})$ du plan, une courbe $\mathscr{C}$ admet une équation de la forme $f(x, y) = 0$ où f est un polynôme de degré 2, il en est de même dans tout autre repère. On dit que $\mathscr{C}$ est une courbe du second degré ou par abus de langage que $\mathscr{C}$ est une conique.

On pose $f(x, y) = ax^2 + 2bxy + cy^2 + dx + ey + k$. [2]

[2] f étant de degré 2, on a $(a,b,c) \neq (0,0,0)$.

Avec $\overrightarrow{OM} = x\vec{i} + y\vec{j}$, on écrit aussi $f(x, y) = f(\overrightarrow{OM})$ d'où l'équivalence :

$$M \in \mathscr{C} \iff f(\overrightarrow{OM}) = 0.$$

On note :

- $ax^2 + 2bxy + cy^2 = q(\overrightarrow{OM})$, q est une forme quadratique sur $\mathbb{R}^2$, on dit que c'est la **partie quadratique** de l'équation.
- $dx + ey = \ell(\overrightarrow{OM})$, ℓ est une forme linéaire sur $\mathbb{R}^2$, on dit que c'est la **partie linéaire** de l'équation.

Écriture matricielle de l'équation

Posons $V = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathcal{M}_{2,1}(\mathbb{R})$, $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$, $L = \begin{pmatrix} d \\ c \end{pmatrix} \in \mathcal{M}_{2,1}(\mathbb{R})$.

On a alors $q(\overrightarrow{OM}) = {}^tVAV$, $\ell(\overrightarrow{OM}) = {}^tLV$ et l'équation de $\mathscr{C}$ s'écrit :

$${}^tVAV + {}^tLV + k = 0.$$

2. Équation au centre

Soit dans un repère $\mathscr{R} = (O, \vec{i}, \vec{j})$ de $\mathscr{E}$, la courbe d'équation $f(x, y) = 0$ **(1)**

$$f(x, y) = ax^2 + 2bxy + cy^2 + 2dx + 2ey + k.$$

Effet d'une translation des axes

Soit $\Omega(x_0, y_0)$, dans le repère $\mathscr{R}' = (\Omega, \vec{i}, \vec{j})$, $\mathscr{C}$ a pour équation :

$$f(x_0 + x', y_0 + y') = 0.$$

On vérifie que :

$$f(x_0 + x', y_0 + y') = ax'^2 + 2bx'y' + cy'^2 + x'\frac{\partial f}{\partial x}(x_0, y_0) + y'\frac{\partial f}{\partial y}(x_0, y_0) + f(x_0, y_0).$$

La partie quadratique de l'équation est donc invariante par translation des axes.

Copyrighted material

Recherche d'un centre de $\mathscr{C}$

Principe : Ω est centre de symétrie de $\mathscr{C}$ si et seulement si la partie linéaire de l'équation de $\mathscr{C}$ dans le repère $\mathscr{R}'$ est nulle.

Cette condition équivaut à :

$$\forall (x', y') \in \mathbb{R}^2,\ f(x_0 + x', y_0 + y') = f(x_0 - x', y_0 - y').$$

Conséquence

$\Omega(x_0, y_0)$ est centre de symétrie de $\mathscr{C}$ si et seulement si :

$$\begin{cases} \dfrac{1}{2}\dfrac{\partial f}{\partial x}(x_0, y_0) = ax_0 + by_0 + d = 0 \\ \dfrac{1}{2}\dfrac{\partial f}{\partial y}(x_0, y_0) = bx_0 + cy_0 + e = 0 \end{cases}$$

c'est-à-dire, en posant $V_0 = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$: si et seulement si $AV_0 + L = 0$.

Théorème 1

Si $\operatorname{rg} A = 2$, la courbe $\mathscr{C}$ a un centre de symétrie $\Omega(x_0, y_0)$ et un seul. (3)

Dans le repère $(\Omega, \vec{i}, \vec{j})$, $\mathscr{C}$ a pour équation :

$$ax'^2 + 2bx'y' + cy'^2 + f(x_0, y_0) = 0. \qquad (2)$$

(3) Si $\operatorname{rg} A = 1$, $\mathscr{C}$ peut ne pas avoir de centre de symétrie, ou en avoir une infinité.

Théorème 2

On suppose que $(O, \vec{i}, \vec{j})$ est un repère orthonormal de $\mathbb{R}^2$, alors $\Omega(x_0, y_0)$ est centre de symétrie de $\mathscr{C}$ si et seulement si :

$$\overrightarrow{\operatorname{grad} f}(x_0, y_0) = 0.$$

Définition 2

Lorsque le centre existe, l'équation (2) est appelée **équation au centre** de $\mathscr{C}$.

3. Réduction de la partie quadratique

Le repère initial $(O, \vec{i}, \vec{j})$ est maintenant supposé orthonormal.

On sait qu'il existe $P \in \mathcal{SO}_2(\mathbb{R})$ (4) telle que :

$$^tPAP = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} = D.$$

(4) Matrice de rotation.

P est matrice de passage de $(\vec{i}, \vec{j})$ à une base orthonormale $(\vec{I}, \vec{J})$ de $\mathbb{R}^2$ formée de vecteurs propres de l'endomorphisme symétrique de la forme quadratique q.

Les formules de changement de repère de $(O, \vec{i}, \vec{j})$ à $(O, \vec{I}, \vec{J})$ s'écrivent :

$$V = PV'' \quad \text{avec} \quad V'' = \begin{pmatrix} x'' \\ y'' \end{pmatrix}.$$

Dans le repère $(O, \vec{I}, \vec{J})$, $\mathscr{C}$ a pour équation :

$$^tV''DV'' + {}^tLPV'' + k = 0$$

c'est-à-dire

$$\lambda x''^2 + \mu y''^2 + d_1 x'' + e_1 y'' + k = 0. \qquad (3)$$

(5) Par rotation des axes, on fait disparaître le «terme rectangle» de la partie quadratique.

Remarques

1) Le terme constant de l'équation est invariant par rotation des axes.

2) Si $\operatorname{rg} A = 2$, λ et μ sont non nuls, de même signe lorsque $\det A = ac - b^2 > 0$, de signes contraires lorsque $\det A = ac - b^2 < 0$.

Si $\operatorname{rg} A = 1$, l'une des valeurs propres λ, μ est nulle, l'autre est non nulle. (6)

(6) Sinon on aurait $A = 0$.

Copyrighted material

4. Pratique de la réduction

1) Calculer $\operatorname{rg} A$.

2) Dans le cas où $\operatorname{rg} A = 2$,

a) déterminer le centre Ω et former l'équation dans le repère $(\Omega, \vec{i}, \vec{j})$: [7]

$$ {}^tV'AV' + f(x_0, y_0) = 0 ;. $$

b) diagonaliser A dans le groupe orthogonal pour trouver un repère $(\Omega, \vec{I}, \vec{J})$ dans lequel $\mathscr{C}$ a pour équation :

$$ \lambda x''^2 + \mu y''^2 + f(x_0, y_0) = 0. $$

3) Dans le cas où $\operatorname{rg} A = 1$,

a) diagonaliser A dans le groupe orthogonal pour trouver un repère $(O, \vec{I}, \vec{J})$ dans lequel $\mathscr{C}$ a pour équation :

$$ \lambda x'^2 + d_1 x'' + e_1 y'' + k = 0 ; $$

Remarque

[8] La partie quadratique de l'équation **(1)** est alors un carré parfait :

$$ q(\overrightarrow{OM}) = \varepsilon(\alpha x + \beta y)^2 $$

donc $q(\overrightarrow{OM}) = \lambda \left(\dfrac{\alpha}{\sqrt{\alpha^2 + \beta^2}} x + \dfrac{\beta}{\sqrt{\alpha^2 + \beta^2}} y \right)^2$ avec $\lambda = \varepsilon \left(\alpha^2 + \beta^2 \right)$.

On peut donc pour obtenir l'équation souhaitée effectuer la rotation des axes définie par :

$$ \begin{pmatrix} x'' \\ y'' \end{pmatrix} = \frac{1}{\sqrt{\alpha^2 + \beta^2}} \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. $$

b) opérer une translation des axes pour simplifier la partie linéaire, l'équation précédente s'écrivant :

$$ \lambda \left(x'' + \frac{d_1}{2\lambda} \right)^2 + e_1 y'' + k - \frac{d_1^2}{4\lambda} = 0. $$

La translation des axes définie par $x' = x'' + \dfrac{d_1}{2\lambda}$, $y' = y''$ donne pour équation de $\mathscr{C}$ dans le nouveau repère :

$$ \lambda x'^2 + e_1 y' + k_1 = 0 \qquad \left(k_1 = k - \frac{d_1^2}{4\lambda} \right). $$

Type d'une courbe $\mathscr{C}$ du second degré

Soit $\mathscr{C}$ la conique d'équation :

$$ ax^2 + 2bxy + cy^2 + 2dx + 2d'y + e = 0. $$ [9]

- Si $ac - b^2 > 0$, on dit que $\mathscr{C}$ est du **type ellipse**.
- Si $ac - b^2 < 0$, on dit que $\mathscr{C}$ est du **type hyperbole**.
- Si $ac - b^2 = 0$, on dit que $\mathscr{C}$ est du **type parabole**.

Nature de $\mathscr{C}$ suivant son équation réduite

On dénombre neuf cas possibles présentés dans le tableau ci-après.

[7] Équation au centre.

[8] Éventuellement à un changement de signe près.

[9] La discussion se fait sur les équations réduites précédentes.

Copyrighted material

Il existe un repère orthonormal dans lequel $\mathscr{C}$ a pour équation :	Alors $\mathscr{C}$ est :
$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$	une ellipse
$\frac{x^2}{a^2}+\frac{y^2}{b^2}=0$	un point
$\frac{x^2}{a^2}+\frac{y^2}{b^2}=-1$	l'ensemble vide
$\frac{x^2}{a^2}-\frac{y^2}{b^2}=1$	une hyperbole
$\frac{x^2}{a^2}-\frac{y^2}{b^2}=0$	deux droites concourantes
$\frac{x^2}{a^2}=\frac{y}{b}$	une parabole
$\frac{x^2}{a^2}=1$	deux droites parallèles
$\frac{x^2}{a^2}=0$	une droite
$\frac{x^2}{a^2}=-1$	l'ensemble vide

Remarque

Dans le cas d'une ellipse ou d'une hyperbole, l'origine du repère est le centre ; dans le cas d'une parabole, c'est le sommet.

Exemple 1 Nature, éléments et dessin de la conique $\mathscr{C}$: $x^2+4xy+4y^2-5y=0$.

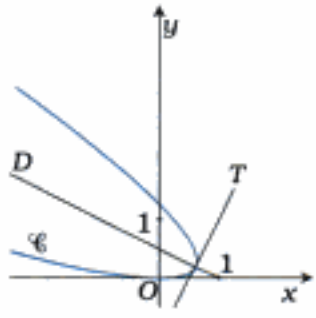
L'équation de $\mathscr{C}$ s'écrit $(x+2y)^2-5y=0$, $\mathscr{C}$ est une parabole.

Soit $(O,\vec{I},\vec{J})$ le repère orthonormal correspondant aux formules de changement de coordonnées :

$$\begin{cases} x+2y=X\sqrt{5} \\ -2x+y=Y\sqrt{5} \end{cases} \iff \begin{cases} x\sqrt{5}=X-2Y \\ y\sqrt{5}=2X+Y \end{cases}$$

L'équation de $\mathscr{C}$ devient :

$$5X^2-(2X+Y)\sqrt{5}=0 \iff (X\sqrt{5}-1)^2-(Y\sqrt{5}+1)=0.$$



Le sommet de la parabole est Ω : $X\sqrt{5}=1, Y\sqrt{5}=-1$ d'où $x=\frac{3}{5}, y=\frac{1}{5}$.

En écrivant l'équation de $\mathscr{C}$:

$$(x+2y-1)^2+(2x-y-1)=0,$$

on dispose de l'axe :

$$D : x+2y-1=0$$

et de la tangente au sommet

$$T : 2x-y-1=0.$$

Ici la parabole est tangente en O à Ox. (10)

(10) Pour dessiner la courbe il est utile de placer les points d'intersection avec les axes Ox et Oy.

Copyrighted material

Exemple 2 Mêmes questions pour $\mathscr{C}$: $x^2 + 6xy + y^2 + 4x = 0$.

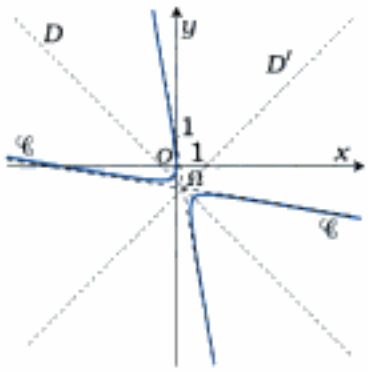
On a ici $A = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$, $\det A = -8$, donc $\mathscr{C}$ est du type hyperbole.

Le polynôme caractéristique de A est :

$$t^2 - 2t - 8 = (t-4)(t+2).$$

Une base orthonormale formée de vecteurs propres de A est $(\vec{I}, \vec{J})$:

$$\vec{I} = \frac{\vec{i} + \vec{j}}{\sqrt{2}}, \quad \vec{J} = \frac{-\vec{i} + \vec{j}}{\sqrt{2}}.$$



Avec $\begin{cases} x + y = X\sqrt{2} \\ -x + y = Y\sqrt{2} \end{cases} \iff \begin{cases} x\sqrt{2} = X - Y \\ y\sqrt{2} = X + Y \end{cases}$

l'équation de $\mathscr{C}$ dans $(O, \vec{I}, \vec{J})$ est $4X^2 - 2Y^2 + 2\sqrt{2}(X - Y) = 0$, soit :

$$4\left(X + \frac{\sqrt{2}}{4}\right)^2 - 2\left(Y + \frac{\sqrt{2}}{2}\right)^2 + \frac{1}{2} = 0.$$

Il s'agit d'une hyperbole.

Le centre Ω est défini par $X = -\frac{\sqrt{2}}{4}$, $Y = -\frac{\sqrt{2}}{2} \iff x = \frac{1}{4}$, $y = -\frac{3}{4}$.

L'axe focal est D : $x + y + \frac{1}{2} = 0$, l'axe non focal D' : $-x + y + 1 = 0$.

B. Quadriques

1. Surfaces du second degré [11]

[11] $\mathscr{E}$ est maintenant l'espace usuel affine euclidien orienté $\mathbb{R}^3$.

Définition 3

Si dans un repère $(O, \vec{i}, \vec{j}, \vec{k})$ de l'espace, une surface $\mathscr{S}$ admet une équation de la forme $f(x, y, z) = 0$ où f est un polynôme de degré 2, il en est de même dans tout autre repère. On dit que $\mathscr{S}$ est une **surface du second degré** ou par abus de langage que $\mathscr{S}$ est une **quadrique**.

On pose $f(x, y, z) = ax^2 + a'y^2 + a''z^2 + 2bxy + 2b'yz + 2b''zx + cx + c'y + c''z + k$.

Avec $\overrightarrow{OM} = x\vec{i} + y\vec{j} + z\vec{k}$, on écrit aussi $f(x, y, z) = f(\overrightarrow{OM})$ d'où l'équivalence :

$$M \in \mathscr{S} \iff f(\overrightarrow{OM}) = 0$$

On note :

- $ax^2 + a'y^2 + a''z^2 + 2bxy + 2b'yz + 2b''zx = q(\overrightarrow{OM})$: q est une forme quadratique sur $\mathbb{R}^3$, on dit que c'est la **partie quadratique** de l'équation.
- $cx + c'y + c''z = \ell(\overrightarrow{OM})$: ℓ est une forme linéaire sur $\mathbb{R}^3$, on dit que c'est la **partie linéaire** de l'équation.

Copyrighted material

Écriture matricielle de l'équation

$$V = \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathcal{M}_{3,1}(\mathbb{R}),\ A = \begin{pmatrix} a & b & b'' \\ b & a' & b' \\ b'' & b' & a'' \end{pmatrix} \in \mathcal{M}_3(\mathbb{R}),\ L = \begin{pmatrix} c \\ c' \\ c'' \end{pmatrix} \in \mathcal{M}_{3,1}(\mathbb{R}).$$

On a alors $q\left(\overrightarrow{OM}\right) = {}^tVAV$, $\ell\left(\overrightarrow{OM}\right) = {}^tLV$ et l'équation de $\mathcal{S}$ s'écrit :

$${}^tVAV + {}^tLV + k = 0.$$

Réduction de la partie quadratique par rotation des axes

Il existe une base orthonormale $\left(\vec{I}, \vec{J}, \vec{K}\right)$ formée de vecteurs propres de l'endomorphisme symétrique associé à q.

Avec $\overrightarrow{OM} = X\vec{I} + Y\vec{J} + Z\vec{K}$ on a alors :

$$q\left(\overrightarrow{OM}\right) = \lambda X^2 + \mu Y^2 + \nu Z^2.$$

Dans le repère $(O, \vec{I}, \vec{J}, \vec{K})$, $\mathcal{S}$ a pour équation :

$$\lambda X^2 + \mu Y^2 + \nu Z^2 + \alpha X + \alpha' Y + \alpha'' Z + k = 0.$$

2. Équation au centre

Le point Ω est centre de symétrie de la surface $\mathcal{S}$: $f(x, y, z) = 0$ si : [12]

$$f\left(\Omega + \overrightarrow{\Omega M}\right) = 0 \iff f\left(\Omega - \overrightarrow{\Omega M}\right) = 0 \quad (M \text{ désigne un point de } \mathcal{S}).$$

[12] On dit que Ω est un **centre de la quadrique**.

Équation au centre $\Omega(x_0, y_0, z_0)$ de la surface $\mathcal{S}$

- Dans $\left(\Omega, \vec{i}, \vec{j}, \vec{k}\right)$, $\mathcal{S}$: $q\left(x'\vec{i} + y'\vec{j} + z'\vec{k}\right) + f\left(x_0, y_0, z_0\right) = 0$.
- Dans $\left(\Omega, \vec{I}, \vec{J}, \vec{K}\right)$, $\mathcal{S}$: $\lambda X^2 + \mu Y^2 + \nu Z^2 + \delta = 0$.

Si $\Omega \in \mathcal{S}$, alors $\mathcal{S}$ est un cône de sommet Ω.

Détermination du centre

Les coordonnées (x, y, z) d'un centre vérifient le système :

$$\begin{cases} \dfrac{1}{2}\dfrac{\partial f}{\partial x} = ax + by + b''z + \dfrac{1}{2}c = 0 \\ \dfrac{1}{2}\dfrac{\partial f}{\partial y} = bx + a'y + b'z + \dfrac{1}{2}c' = 0 \\ \dfrac{1}{2}\dfrac{\partial f}{\partial z} = b''x + b'y + a''z + \dfrac{1}{2}c'' = 0 \end{cases}$$

c'est-à-dire :

$$A\begin{pmatrix} x \\ y \\ z \end{pmatrix} + \frac{1}{2}\begin{pmatrix} c \\ c' \\ c'' \end{pmatrix} = 0.$$ [13]

[13] Ou encore $\overrightarrow{\text{grad}} f(x,y,z) = 0$.

Discussion du système

- $\text{rg}\, A = 3$, $\mathcal{S}$ a un centre unique ;
- $\text{rg}\, A = 2$, l'ensemble des centres est une droite ou l'ensemble vide ;
- $\text{rg}\, A = 1$, l'ensemble des centres est un plan ou l'ensemble vide.

Copyrighted material

3. Les quadriques

3.1 – Nomenclature

Soit $\mathcal{S}$ une quadrique ; il existe un repère affine de $\mathcal{E}$ [14] dans lequel $\mathcal{S}$ a une **équation réduite**.

[14] Ou un repère orthonormal.

Les neuf surfaces intéressantes, avec leurs équations réduites, sont :

Ellipsoïde	$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}-1=0$
Hyperboloïde à une nappe	$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}-1=0$
Hyperboloïde à deux nappes	$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}+1=0$
Cône du second degré	$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}=0$
Paraboloïde elliptique	$\frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z}{c}=0$
Paraboloïde hyperbolique	$\frac{x^2}{a^2}-\frac{y^2}{b^2}-\frac{z}{c}=0$
Cylindre elliptique	$\frac{x^2}{a^2}+\frac{y^2}{b^2}-1=0$
Cylindre hyperbolique	$\frac{x^2}{a^2}-\frac{y^2}{b^2}-1=0$
Cylindre parabolique	$x^2-2py=0$

- Les coefficients a, b, c, p, q sont des réels strictement positifs.
- Dans les autres cas, on dit que $\mathcal{S}$ est dégénérée : [15]

[15] Dans les neuf cas précédents, on dit qu'il s'agit de **quadriques propres** ou **non dégénérées**.

$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}+1=0$, $\frac{x^2}{a^2}+\frac{y^2}{b^2}+1=0$, $\frac{x^2}{a^2}+1=0$ ($\mathcal{S}$ est vide).

$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=0$, $\frac{x^2}{a^2}+\frac{y^2}{b^2}=0$, $\frac{x^2}{a^2}=0$ ($\mathcal{S}$ est un point, une droite, un plan).

$\frac{x^2}{a^2}-\frac{y^2}{b^2}=0$, $\frac{x^2}{a^2}-1=0$ ($\mathcal{S}$ est réunion de deux plans sécants, parallèles).

- **Quadriques à centre**

L'ellipsoïde, l'hyperboloïde à une ou deux nappes, le cône admettent un centre unique : on dit que ce sont les quadriques à centre. Elles correspondent au cas où la forme quadratique associée est de rang 3.

- Les cylindres elliptiques et hyperboliques ont une droite de centres. [16]

[16] C'est un axe de symétrie ; la forme quadratique est de rang 2.

Copyrighted material

Exemple 3 Nature de la surface $\mathcal{S}_a$ d'équation :

$$x^2 + 5y^2 + 4z^2 + 4xy - 2xz - 2y - 6z = a. \qquad (1)$$

dans un repère orthonormal $(O, \vec{i}, \vec{j}, \vec{k})$.

Formons la matrice A de la partie quadratique.

Avec $q(\overrightarrow{OM}) = x^2 + 5y^2 + 4z^2 - 2zx + 4xy$, il vient :

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 5 & 0 \\ -1 & 0 & 4 \end{pmatrix}.$$

S'il s'agit d'une quadrique à centre, le problème revient à la détermination du signe des valeurs propres de A.

Le calcul donne $\det A = -1$ donc A est inversible et $\mathcal{S}_a$ admet un unique centre de symétrie Ω défini par le système :

$$\begin{cases} x + 2y - z = 0 \\ 2x + 5y = 1 \\ -x + 4z = 3 \end{cases} \quad \text{c'est-à-dire} \quad A\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix},$$

ce qui donne $x = -7,\ y = 3,\ z = -1$.

L'équation au centre de $\mathcal{S}_a$ s'obtient en effectuant la translation des axes définie par $x = -7+X$, $y = 3 + Y$, $z = -1 + Z$ ce qui donne :

$$X^2 + 5Y^2 + 4Z^2 - 2ZX + 4XY = a \text{ ✎(17)} \qquad (2)$$

✎(17) Équation de $\mathcal{S}_a$ dans le repère $(\Omega, \vec{i}, \vec{j}, \vec{k})$.

Formons maintenant le polynôme caractéristique de A :

$$\chi_A(\lambda) = -\lambda^3 + 10\lambda^2 - 24\lambda - 1.$$

On sait que χ_A est scindé dans $\mathbb{R}$ mais il n'y a pas de factorisation simple apparente.

Avec $\chi'_A(\lambda) = -3\lambda^2 + 20\lambda - 24$, on vérifie que χ_A n'a pas de racine double. En effet, si λ était racine double de χ_A on aurait successivement :

$$\begin{cases} 3\lambda^2 - 20\lambda + 24 = 0 & (E_1) \\ -3\lambda^3 + 10\lambda^2 - 24\lambda - 1 = 0 & (E_2) \end{cases}$$

$$\begin{cases} 3\lambda^2 - 20\lambda + 24 = 0 & (E_1) \\ 10\lambda^2 - 48\lambda - 3 = 0 & (E_3) \text{ ✎(18)} \end{cases}$$

$$\begin{cases} 3\lambda^2 - 20\lambda + 24 = 0 & (E_1) \\ 56\lambda = 249 & (E_4) \text{ ✎(19)} \end{cases}$$

✎(18) $(E_3) = \lambda(E_1) + 3(E_2)$

✎(19) $(E_4) = -10(E_1) + 3(E_3)$

et il est facile de voir que ce dernier système n'a pas de solution puisque les racines de χ'_A sont :

$$\frac{10 - 2\sqrt{7}}{3} \quad \text{et} \quad \frac{10 + 2\sqrt{7}}{3}.$$

En conséquence, χ_A a trois racines réelles simples $\lambda_1, \lambda_2, \lambda_3$ et on les indexe de façon que :

$$\lambda_1 < \lambda_2 < \lambda_3. \text{ ✎(20)}$$

✎(20) Le calcul numérique donne :
$\lambda_1 \simeq -0{,}04$
$\lambda_2 \simeq 4{,}13$
$\lambda_3 \simeq 5{,}91$.

Avec $\det A = \lambda_1\lambda_2\lambda_3 < 0$, les possibilités sont $\lambda_1 < 0 < \lambda_2 < \lambda_3$ et $\lambda_1 < \lambda_2 < \lambda_3 < 0$ et, compte tenu de $\operatorname{Tr} A = 10 = \lambda_1 + \lambda_2 + \lambda_3$, seule la première est à retenir.

Posons donc $\lambda_1 = -\frac{1}{\alpha^2}$, $\lambda_2 = \frac{1}{\beta^2}$, $\lambda_3 = \frac{1}{\gamma^2}$. Si $(\vec{I}, \vec{J}, \vec{K})$ est une base orthonormale formée de vecteurs propres de u_A, endomorphisme symétrique associé à A dans $(\vec{i}, \vec{j}, \vec{k})$ avec :

$$u_A(\vec{I}) = \lambda_1\vec{I},\ u_A(\vec{J}) = \lambda_2\vec{J},\ u_A(\vec{K}) = \lambda_3\vec{K},$$

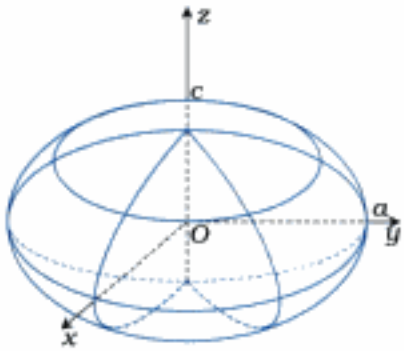
Copyrighted material

Hidden page

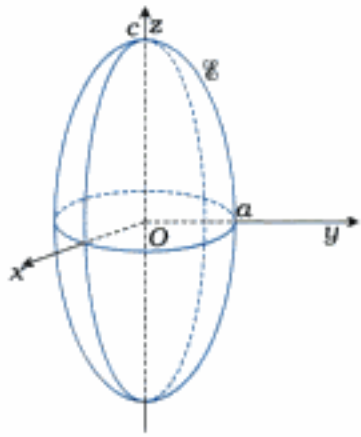
3.2 – Les quadriques de révolution

Ellipsoïde de révolution $\dfrac{x^2+y^2}{a^2}+\dfrac{z^2}{c^2}-1=0$ [21]

[21] L'ellipsoïde de révolution est engendré par une ellipse $\mathscr{E}$: $\frac{y^2}{a^2}+\frac{z^2}{c^2}-1=0$, $x=0$ tournant autour d'un de ses axes (ici Oz).



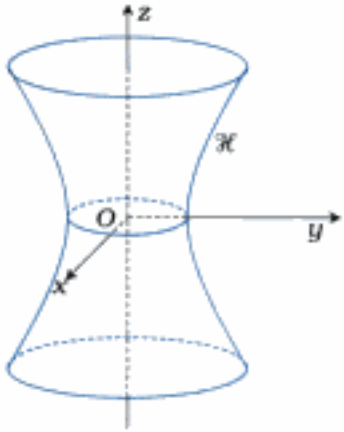
Ellipsoïde plat si $a > c$



Ellipsoïde long si $a < c$

Hyperboloïde de révolution [22]

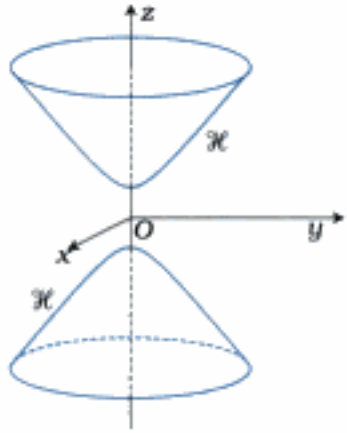
[22] La section d'un hyperboloïde de révolution par un plan orthogonal à l'axe et passant par le centre est vide si l'hyperboloïde a deux nappes.



à une nappe $\dfrac{x^2+y^2}{a^2}-\dfrac{z^2}{c^2}-1=0$

engendré par l'hyperbole $\mathscr{H}$:

$$\frac{y^2}{a^2}-\frac{z^2}{c^2}-1=0\ ,\quad x=0$$



à deux nappes $\dfrac{x^2+y^2}{a^2}-\dfrac{z^2}{c^2}+1=0$

engendré par l'hyperbole $\mathscr{H}$:

$$\frac{y^2}{a^2}-\frac{z^2}{c^2}+1=0\ ,\quad x=0$$

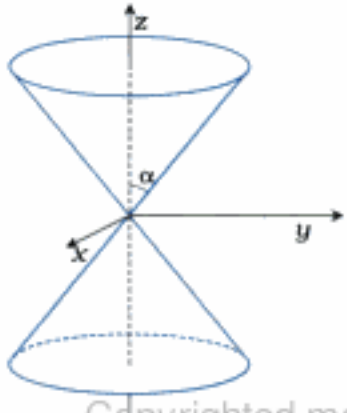
Cône de révolution $\dfrac{x^2+y^2}{a^2}-\dfrac{z^2}{c^2}=0$

ou $x^2+y^2-z^2\tan^2\alpha=0$

engendré par la droite $\mathscr{D}$:

$$z=\frac{c}{a}y\ ,\quad x=0$$

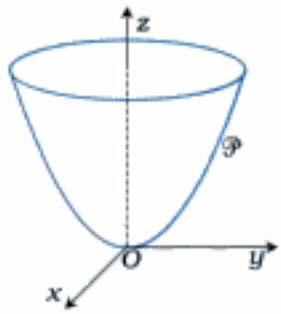
$\mathscr{C}$ est le cône de révolution d'axe Oz de demi-angle au sommet α.



Copyrighted material

Paraboloïde de révolution $x^2 + y^2 - 2pz = 0$

engendré par la parabole $\mathscr{P}$:
$y^2 - 2pz = 0$, $x = 0$



Cylindre de révolution $x^2 + y^2 - a^2 = 0$ d'axe Oz et de rayon a.

Les quadriques propres ne pouvant pas être de révolution sont :
le paraboloïde hyperbolique, le cylindre hyperbolique ou parabolique.

Théorème 3

Caractérisation d'une quadrique de révolution

Soit $\mathscr{S}$ une quadrique propre dont la forme quadratique associée a pour matrice A dans une base orthonormale.

Alors $\mathscr{S}$ est de révolution si et seulement si A a une valeur propre double non nulle. (23)

(23) Le cas d'une valeur propre triple est celui de la sphère exclusivement.

Théorème 4

$A \in \mathcal{M}_3(\mathbb{R})$ a une valeur propre double si et seulement si il existe un réel λ tel que :
$$\operatorname{rg}\left(A - \lambda I_3\right) = 1.$$

☞ L'image de $A - \lambda I_3$ donne la direction de l'axe de la quadrique de révolution éventuelle.

Exemple 5 Éléments de la surface de révolution $\mathscr{S}$ d'équation : $3x^2 + 8yz + 4zx - 4xy + y + z = 0$ **(1)** dans un repère orthonormal $(O, \vec{i}, \vec{j}, \vec{k})$.

Introduisons la matrice A de la forme quadratique associée à $\mathscr{S}$: $A = \begin{pmatrix} 3 & -2 & 2 \\ -2 & 0 & 4 \\ 2 & 4 & 0 \end{pmatrix}$.

On a $A - \lambda I_3 = \begin{pmatrix} 3-\lambda & -2 & 2 \\ -2 & -\lambda & 4 \\ 2 & 4 & -\lambda \end{pmatrix}$ et $\det\left(A - \lambda I_3\right) = -(\lambda + 5)(\lambda - 4)^2$.

Pour $\lambda = 4$, on a $\operatorname{rg}\left(A - \lambda I_3\right) = 1$ (24) et, avec $A - 4I_3 = \begin{pmatrix} -1 & -2 & 2 \\ -2 & -4 & 4 \\ 2 & 4 & -4 \end{pmatrix} = B$,

on obtient $(x\ y\ z)\, B \begin{pmatrix} x \\ y \\ z \end{pmatrix} = -(x + 2y - 2z)^2$.

(24) A étant diagonalisable et 4 valeur propre double,
$2 = 3 - \operatorname{rg}\left(A - 4I_3\right)$.

Comme $A = 4I_3 + B$, l'équation de **(1)** s'écrit : $4(x^2 + y^2 + z^2) - (x + 2y - 2z)^2 + y + z = 0$.

Choisissons un repère orthonormal $(O, \vec{I}, \vec{J}, \vec{K})$ avec $\vec{K} = \dfrac{\vec{i} + 2\vec{j} - 2\vec{k}}{3}$, en prenant pour nouvelles coordonnées :

$$\begin{cases} X = \frac{1}{3}(-2x + 2y + z) \\ Y = \frac{1}{3}(2x + y + 2z) \\ Z = \frac{1}{3}(x + 2y - 2z) \end{cases} \quad \text{d'où} \quad \begin{cases} x = \frac{1}{3}(-2X + 2Y + Z) \\ y = \frac{1}{3}(2X + Y + 2Z) \\ z = \frac{1}{3}(X + 2Y - 2Z) \end{cases}$$

Les formules inverses sont identiques car la matrice est orthogonale et symétrique.

Copyrighted material

Calculons $y+z=X+Y$ pour obtenir l'équation de $\mathscr{S}$ dans $(O,\vec{I},\vec{J},\vec{K})$:

$$4\left(X^2+Y^2+Z^2\right)-9Z^2+X+Y=0,\quad 4\left(X+\frac{1}{8}\right)^2+4\left(Y+\frac{1}{8}\right)^2-5Z^2-\frac{1}{8}=0 \quad (2)$$

$\mathscr{S}$ est un hyperboloïde de révolution à une nappe, de centre $\Omega = O-\frac{1}{8}(\vec{I}+\vec{J}) = O-\frac{1}{8}(\vec{j}+\vec{k})$ et d'axe $\Delta = \Omega + \mathbb{R}\vec{K}$.

3.3 – Description des quadriques usuelles

(25) Le tableau ci-après donne un définition géométrique de l'ellipsoïde, des hyperboloïdes et du paraboloïde elliptique en fonction des quadriques de révolution.

Dans le repère $(O,\vec{i},\vec{j},\vec{k})$ fixé, on considère l'affinité (ou dilatation) $\mathscr{A}$ définie par : (25)

$$A\ :\ M(x,y,z)\mapsto M'\left(x,\frac{b}{a}y,z\right).$$

La quadrique	est image par $\mathscr{A}$	de la quadrique de révolution
l'ellipsoïde $\mathscr{E}\ :\ \frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}=1$	...	l'ellipsoïde $\mathscr{E}_r\ :\ \frac{x^2+y^2}{a^2}+\frac{z^2}{c^2}=1$
l'hyperboloïde à une nappe $\mathscr{H}_1\ :\ \frac{x^2}{a^2}+\frac{y^2}{b^2}-\frac{z^2}{c^2}=1$	...	l'hyperboloïde de révolution à une nappe $\mathscr{H}_{1,r}\ :\ \frac{x^2+y^2}{a^2}-\frac{z^2}{c^2}=1$
l'hyperboloïde à deux nappes $\mathscr{H}_2\ :\ \frac{x^2+y^2}{a^2}-\frac{z^2}{c^2}=1$	...	l'hyperboloïde de révolution à deux nappes $\mathscr{H}_{2,r}\ :\ \frac{x^2+y^2}{a^2}-\frac{z^2}{c^2}=-1$
le paraboloïde elliptique $\mathscr{PE}\ :\ \frac{x^2}{a^2}+\frac{y^2}{b^2}=\frac{z}{c}$	...	le paraboloïde de révolution $\mathscr{PE}_r\ :\ \frac{x^2+y^2}{a^2}=\frac{z}{c}$

Étude particulière du paraboloïde hyperbolique $\mathscr{PH}\ :\ \frac{x^2}{a^2}-\frac{y^2}{b^2}=\frac{z}{c}$.

- Le $\mathscr{PH}$ est une surface réglée.

On peut mettre en évidence deux systèmes de génératrices $(\mathscr{D}_\lambda)_{\lambda\in\mathbb{R}}$ et $(\mathscr{D}'_\mu)_{\mu\in\mathbb{R}}$:

$$\mathscr{D}_\lambda\begin{cases}\dfrac{x}{a}-\dfrac{y}{b}=\lambda\\ \lambda\left(\dfrac{x}{a}+\dfrac{y}{b}\right)=\dfrac{z}{c}\end{cases}\qquad \mathscr{D}'_\mu\begin{cases}\dfrac{x}{a}+\dfrac{y}{b}=\mu\\ \mu\left(\dfrac{x}{a}-\dfrac{y}{b}\right)=\dfrac{z}{c}\end{cases}$$

- Le $\mathscr{PH}$ coupe tout plan $\mathscr{P}_\lambda(z=\lambda)$ suivant une hyperbole $\mathscr{H}_\lambda$:

$$\mathscr{H}_\lambda\ :\ z=\lambda\quad,\quad \frac{x^2}{a^2}-\frac{y^2}{b^2}=\frac{\lambda}{c}.$$

Si $\lambda=0$ cette hyperbole se décompose en deux droites.

Le $\mathscr{PH}$ est la réunion de la famille $(\mathscr{H}_\lambda)_{\lambda\in\mathbb{R}}$ d'où le qualificatif hyperbolique.

Copyrighted material

Hidden page

Hidden page

Hidden page

Exercices

Coniques

Ex. 1

Dans le plan euclidien rapporté à un repère orthonormal $(O, \vec{i}, \vec{j})$, on considère la droite $\mathcal{D}$ d'équation :

$$\frac{x}{a} + \frac{y}{b} = 1.$$

À tout point M du plan, on associe ses images M_0, M_1, M_2 dans les réflexions d'axes $\mathcal{D}$, Ox et Oy respectivement.

Trouver l'ensemble des points M tels que M_0, M_1, M_2 soient alignés.

Ex. 2

Dans le plan euclidien rapporté à un repère orthonormal $(O, \vec{i}, \vec{j})$, on donne deux cercles :

$$\mathcal{C}_1 : (x-2)^2 + y^2 = 4$$

$$\mathcal{C}_2 : x^2 + (y-1)^2 = 1$$

Former une équation cartésienne de l'ensemble des centres des cercles qui sont tangents extérieurement à $\mathcal{C}_1$ et à $\mathcal{C}_2$.

Ex. 3

Soit $ABCD$ un rectangle du plan euclidien.

Déterminer l'ensemble $\mathcal{L}$ des points M du plan tels que les cercles circonscrits aux triangles MAB et MBC aient même rayon.

Ex. 4

Trouver l'ensemble des centres des hyperboles équilatères de foyer F fixé et passant par un point A distinct de F.

Ex. 5

Trouver l'ensemble $\mathcal{L}$ des centres des hyperboles équilatères tangentes en un point A à une droite $\mathcal{D}$ fixée et passant par un point B fixé n'appartenant pas à $\mathcal{D}$.

Ex. 6

Montrer que, dans l'espace affine euclidien $\mathcal{E}_2$ rapporté à un repère orthonormal $(O, \vec{i}, \vec{j})$, les courbes Γ et Γ' d'équations respectives :

$$(ax+by)^2 + (a'x+b'y)^2 = 1$$

$$\text{et } (ax+a'y)^2 + (bx+b'y)^2 = 1$$

sont isométriques.

Quadriques

Ex. 7

Soit $\mathcal{D}_1$ et $\mathcal{D}_2$ deux droites non coplanaires.

Étudier l'ensemble des points M tels que :

$$d^2(M, \mathcal{D}_1) + d^2(M, \mathcal{D}_2) = k.$$

Ex. 8

Dans l'espace euclidien de dimension 3 rapporté à un repère orthonormal $(O, \vec{i}, \vec{j}, \vec{k})$, déterminer l'ensemble des sommets des cônes du second ordre, de révolution, et contenant la parabole d'équation :

$$z = 0 \ , \ y^2 = 2px \ , \ p > 0.$$

Ex. 9

Dans $\mathbb{R}^3$ rapporté à un repère orthonormal, soit la quadrique $\mathcal{Q}$ d'équation :

$$3x^2 - z^2 + 2xy + 2yz + 2zx - 2x - 8y + 6z = 0.$$

1) Former une équation réduite de $\mathcal{Q}$ et préciser sa nature.

2) Montrer que la forme quadratique :

$$q : x\vec{i} + y\vec{j} + z\vec{k} \mapsto 3x^2 - z^2 + 2xy + 2yz + 2zx$$

se décompose en le produit de deux formes linéaires indépendantes. En déduire deux systèmes de génératrices de $\mathcal{Q}$. Calculer l'angle des génératrices passant par O.

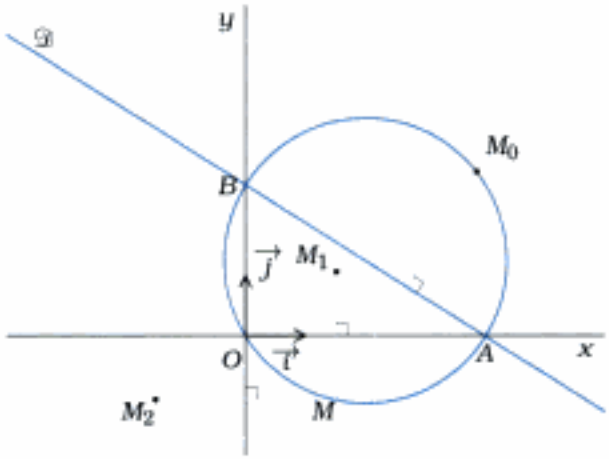
Copyrighted material

Hidden page

Solutions des exercices

Coniques

Ex. 1



$\mathcal{D}$ est définie par les points $A(a, 0)$ et $B(0, b)$, donc est dirigée par $\overrightarrow{AB} = -a\,\vec{i} + b\,\vec{j}$.

Étant donné un point $M(x, y)$, on a :

$$M = O + x\,\vec{i} + y\,\vec{j} \quad . \quad M_1 = O + x\,\vec{i} - y\,\vec{j} \quad . \quad M_2 = O - x\,\vec{i} + y\,\vec{j}$$

puis $\overrightarrow{AM_0} = 2\dfrac{\overrightarrow{AB}\cdot\overrightarrow{AM}}{\|\overrightarrow{AB}\|^2}\overrightarrow{AB} - \overrightarrow{AM}$ donc, avec $\overrightarrow{AB}\cdot\overrightarrow{AM} = -a(x-a) + by$ et $\|\overrightarrow{AB}\|^2 = a^2 + b^2$, il vient :

$$x_0 = \frac{x\left(a^2 - b^2\right) - 2aby + 2ab^2}{a^2 + b^2} \quad . \quad y_0 = \frac{-2abx + \left(b^2 - a^2\right)y + 2a^2b}{a^2 + b^2}.$$

En conséquence les trois points M_0, M_1, M_2 sont alignés si et seulement si :

$$\begin{vmatrix} \dfrac{x\left(a^2 - b^2\right) - 2aby + 2ab^2}{a^2 + b^2} & x & -x \\ \dfrac{-2abx + \left(b^2 - a^2\right)y + 2a^2b}{a^2 + b^2} & -y & y \\ 1 & 1 & 1 \end{vmatrix} = 0$$

donc si et seulement si $\begin{vmatrix} x\left(a^2 - b^2\right) - 2aby + 2ab^2 & x & -x \\ -2abx + \left(b^2 - a^2\right)y + 2a^2b & -y & y \\ a^2 + b^2 & 1 & 1 \end{vmatrix} = 0$ soit encore :

$$\begin{vmatrix} x\left(a^2 - b^2\right) - 2aby + 2ab^2 & 0 & -x \\ -2abx + \left(b^2 - a^2\right)y + 2a^2b & 0 & y \\ a^2 + b^2 & 2 & 1 \end{vmatrix} = 0$$

d'où enfin $x^2 + y^2 - ax - by = 0$.

Ainsi $\mathcal{Y}$ est le cercle de diamètre $[AB]$.

Copyrighted material

Ex. 2

$\mathscr{C}_1$ est le cercle de centre $A(2,0)$ et de rayon $R_1 = 2$,

$\mathscr{C}_2$ est le cercle de centre $B(0,1)$ et de rayon $R_2 = 1$.

Le cercle $\mathscr{C}$ de centre $M(x,y)$ et de rayon R est tangent extérieurement à $\mathscr{C}_1$ et à $\mathscr{C}_2$ si et seulement si :

$$AM = R + R_1 \quad \text{et} \quad BM = R + R_2 .$$

Pour qu'un tel cercle existe il faut et il suffit que :

$$AM - BM = R_1 - R_2 = 1 \quad \text{et} \quad BM \geqslant R_2 .$$

Il en résulte que M décrit la branche $\mathscr{H}$ d'hyperbole de foyer A et B d'équation :

$$\sqrt{(x-2)^2 + y^2} - \sqrt{x^2 + (y-1)^2} = 1 \quad \text{et} \quad x^2 + (y-1)^2 \geqslant 1.$$

Il est clair que les points de $\mathscr{C}_1 \cap \mathscr{C}_2$ font partie du lieu et l'ensemble cherché a aussi pour équations :

$$-2x + y + 1 = \sqrt{x^2 + (y-1)^2}, \ y \geqslant 2x$$

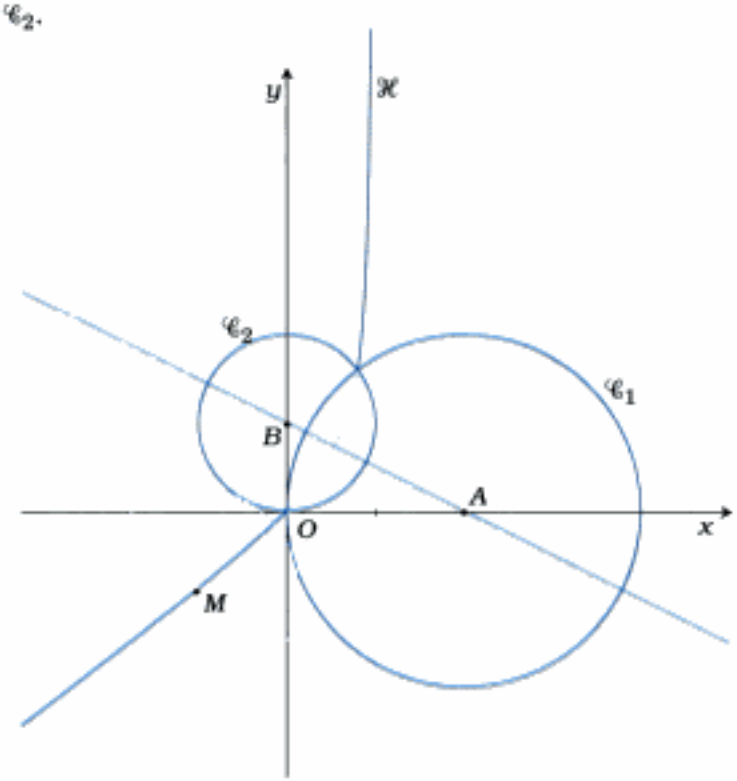
soit aussi :

$$4y(x-1) = 3x^2 - 4x \quad , \quad x \in]-\infty, 0] \cup \left[\frac{4}{5}, 1\right[.$$

Dans un repère orthonormal d'origine $\dfrac{A+B}{2}$, d'axe $OX = (AB)$, l'hyperbole a pour équation :

$$4X^2 - Y^2 - 1 = 0.$$

D'après la condition $x^2 + (y-1)^2 \geqslant 1$, le lieu cherché est formé des deux arcs de $\mathscr{H}$ extérieurs aux cercles $\mathscr{C}_1$ et $\mathscr{C}_2$. La partie de la branche d'hyperbole intérieure aux cercles $\mathscr{C}_1$ et $\mathscr{C}_2$ est l'ensemble des centres des cercles tangents intérieurement à $\mathscr{C}_1$ et $\mathscr{C}_2$.



Ex. 3

- Remarquons d'abord que tout point M du cercle Γ, circonscrit au triangle ABC, convient, les deux cercles MAB et MBC étant alors identiques.

- Choisissons un repère orthonormal $(O, \vec{i}, \vec{j})$ du plan tel que les coordonnées des points B, A, C soient respectivement : (a,b), $(a,-b)$, $(-a,b)$.

Soit $P(\alpha, 0)$ et $Q(0,\beta)$ les centres de deux cercles, l'un contenant $\{A,B\}$, l'autre contenant $\{B,C\}$; ils ont même rayon si et seulement si :

$$\| \overrightarrow{BP} \|^2 = \| \overrightarrow{BQ} \|^2 \iff (\alpha - a)^2 + b^2 = a^2 + (\beta - b)^2.$$

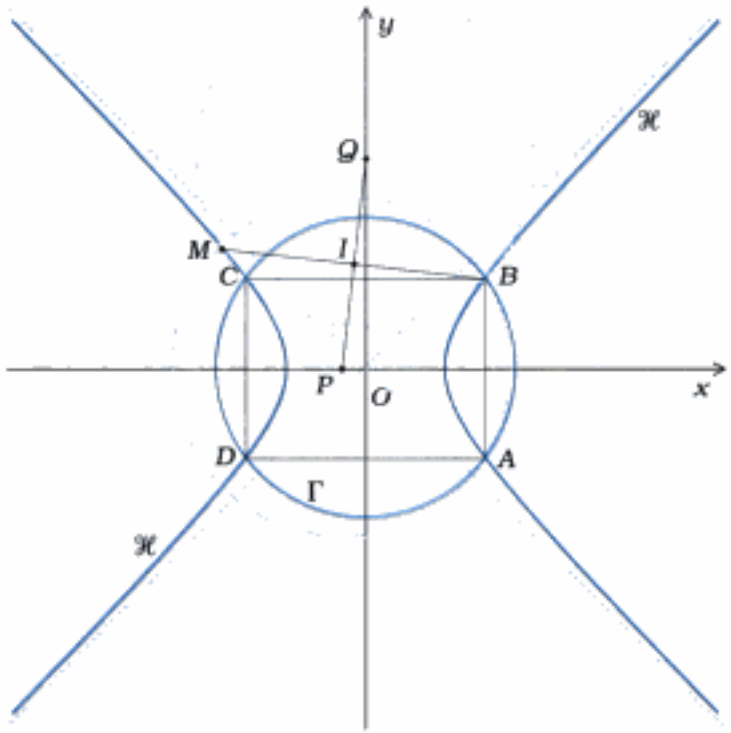
Copyrighted material

S'ils ne sont pas confondus $\big((\alpha,\beta)\neq(0,0)\big)$ ces cercles se recoupent en un point $M(x,y)$ symétrique de B par rapport au milieu I de PQ et on a alors : $x+a=\alpha$, $y+b=\beta$.

En conséquence, les deux cercles ont même rayon si et seulement si $x^2+b^2=a^2+y^2$.

C'est l'équation d'une hyperbole équilatère $\mathcal{H}$ de centre O, d'axes Ox et Oy circonscrite au rectangle $ABCD$.

Le lieu cherché est la réunion $L=\Gamma\cup\mathcal{H}$.



Ex. 4

Soit $(F,\vec{i},\vec{j})$ le repère orthonormal tel que $A=F+a\vec{i}$.

Une hyperbole équilatère $\mathcal{H}$ de foyer F a pour équation polaire :

$$r=\frac{p}{1+\sqrt{2}\cos\left(\theta-\theta_0\right)}.$$

$\mathcal{H}$ contient A si et seulement si $a=\dfrac{p}{1+\sqrt{2}\cos\theta_0}$ ou $-a=\dfrac{p}{1-\sqrt{2}\cos\theta_0}$ c'est-à-dire :

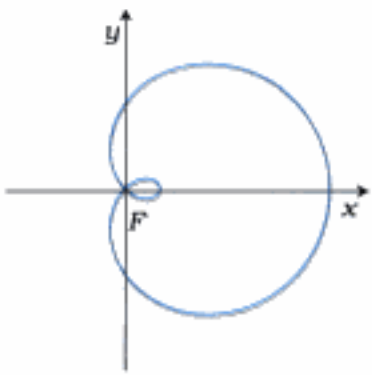
$$p=a\left(1+\sqrt{2}\cos\theta_0\right)\ \text{ou}\ p=-a\left(1-\sqrt{2}\cos\theta_0\right).$$

Les sommets S et S' de $\mathcal{H}$ ont donc pour coordonnées polaires :

- pour S :
$$\theta=\theta_0\quad,\quad r=\frac{p}{1+\sqrt{2}}$$
- pour S' :
$$\theta=\theta_0+\pi\quad,\quad r=\frac{p}{1-\sqrt{2}}$$
$$\text{ou}\quad\theta=\theta_0\quad,\quad r=\frac{p}{\sqrt{2}-1}$$

et, pour le centre Ω :

$$\theta=\theta_0\quad,\quad r=\frac{p}{2}\Big(\frac{1}{\sqrt{2}+1}+\frac{1}{\sqrt{2}-1}\Big)=p\sqrt{2}.$$



L'ensemble $\mathcal{L}$ cherché a donc pour équation polaire : $r=2a\left(\dfrac{1}{\sqrt{2}}+\cos\theta\right)$ ou $r=-2a\left(\dfrac{1}{\sqrt{2}}-\cos\theta\right)$.

Copyrighted material

Or, en posant $f(\theta) = 2a\left(\frac{1}{\sqrt{2}} + \cos\theta\right)$ et $g(\theta) = -2a\left(\frac{1}{\sqrt{2}} - \cos\theta\right)$, on a pour tout θ, $g(\theta + \pi) = -f(\theta)$, donc les deux équations $r = f(\theta)$ et $r = g(\theta)$ représentent la même courbe.

Finalement, l'ensemble $\mathcal{L}$ cherché est le limaçon de Pascal d'équation polaire $r = 2a\left(\frac{1}{\sqrt{2}} + \cos\theta\right)$.

Ex. 5

On choisit le repère orthonormal tel que A soit l'origine et l'axe des abscisses soit porté par $\mathcal{D}$. Le point B a alors pour coordonnées (a, b) avec $b \neq 0$.

La conique $\mathcal{C}$ d'équation : $\alpha x^2 + 2\beta xy + \gamma y^2 + \delta x + \varepsilon y + \lambda = 0$ **(1)**

est une hyperbole équilatère ou un ensemble de deux droites orthogonales si et seulement si les valeurs propres de la matrice de la partie quadratique sont opposées donc si et seulement si la trace de cette matrice est nulle, c'est-à-dire $\alpha + \gamma = 0$.

On a alors $(\alpha, \beta) \neq (0, 0)$, donc il existe $\theta \in \mathbb{R}$ tel que :

$$\cos\theta = \frac{\alpha}{\sqrt{\alpha^2 + \beta^2}} \quad , \quad \sin\theta = \frac{\beta}{\sqrt{\alpha^2 - \beta^2}}$$

et l'équation **(1)** s'écrit : $\left(x^2 - y^2\right)\cos\theta - 2xy\sin\theta + ux + vy + w = 0$ où on a posé :

$$\frac{\delta}{\sqrt{\alpha^2 + \beta^2}} = u, \quad \frac{\varepsilon}{\sqrt{\alpha^2 + \beta^2}} = v, \quad \frac{\lambda}{\sqrt{\alpha^2 + \beta^2}} = w.$$

$\mathcal{C}$ est tangente en A à $\mathcal{D}$ si et seulement si $w = u = 0$.

On a ainsi l'équation générale des hyperboles équilatères tangentes en A à $\mathcal{D}$:

$$\left(x^2 - y^2\right)\cos\theta - 2xy\sin\theta + vy = 0.$$

On écrit que $\mathcal{C}$ passe par $B(a, b)$ et il vient : $v = \dfrac{\left(b^2 - a^2\right)\cos\theta + 2ab\sin\theta}{b}$.

Le centre $\Omega\left(x_0, y_0\right)$ est défini par :

$$\begin{cases} x_0\cos\theta - y_0\sin\theta = 0 \\ x_0\sin\theta + y_0\cos\theta = \dfrac{v}{2} \end{cases} \quad \text{d'où} \quad \begin{cases} x_0 = \dfrac{v}{2}\sin\theta \\ y_0 = \dfrac{v}{2}\cos\theta \end{cases}$$

puis :

$$x_0 = \frac{1}{2b}\left[\left(b^2 - a^2\right)\cos\theta\sin\theta + 2ab\sin^2\theta\right]$$

$$y_0 = \frac{1}{2b}\left[\left(b^2 - a^2\right)\cos^2\theta + 2ab\sin\theta\cos\theta\right]$$

soit encore :

$$x_0 = \frac{1}{4b}\left[\left(b^2 - a^2\right)\sin 2\theta + 2ab(1 - \cos 2\theta)\right]$$

$$y_0 = \frac{1}{4b}\left[\left(b^2 - a^2\right)(1 + \cos 2\theta) + 2ab\sin 2\theta\right]$$

En résolvant ce système en $\cos 2\theta, \sin 2\theta$, on en déduit que $M(x, y)$ appartient à l'ensemble $\mathcal{L}$ si et seulement si il existe $\theta \in \mathbb{R}$ tel que :

$$\cos 2\theta = \frac{4b}{\left(a^2 + b^2\right)^2}\left[-2ab\left(x - \frac{a}{2}\right) + \left(b^2 - a^2\right)\left(y - \frac{b^2 - a^2}{4b}\right)\right]$$

$$\sin 2\theta = \frac{4b}{\left(a^2 + b^2\right)^2}\left[\left(b^2 - a^2\right)\left(x - \frac{a}{2}\right) + 2ab\left(y - \frac{b^2 - a^2}{4b}\right)\right]$$

Copyrighted material

Hidden page

Quadriques

Ex. 7

Désignons par (H_1H_2) la perpendiculaire commune aux deux droites $\mathcal{D}_1$, $\mathcal{D}_2$ et par O le milieu du segment H_1H_2.

O est centre de symétrie de $\mathcal{D}_1 \cup \mathcal{D}_2$, on choisit ce point pour origine du repère.

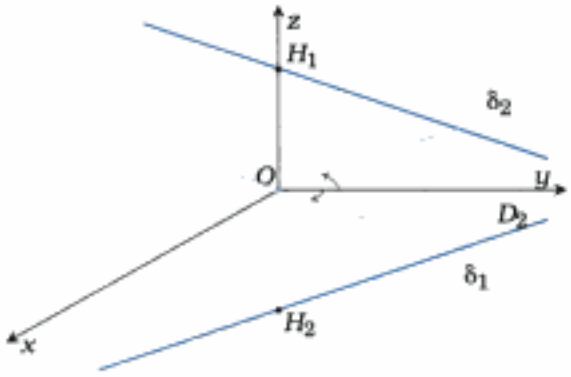
Dans le plan Π passant par O et perpendiculaire à la droite (H_1H_2), on prend pour axes $(x'Ox)$ et $(y'Oy)$, dirigés par les vecteurs unitaires $\vec{i}$ et $\vec{j}$, des deux bissectrices des droites δ_1 et δ_2, projections orthogonales sur Π des droites $\mathcal{D}_1$ et $\mathcal{D}_2$.

Il reste à compléter par $\vec{k}$, vecteur unitaire dirigeant (H_1H_2), pour obtenir $(O, \vec{i}, \vec{j}, \vec{k})$, repère orthonormal dont les trois axes sont axes de symétries de $\mathcal{D}_1 \cup \mathcal{D}_2$.

Dans ce repère, les droites $\mathcal{D}_1$ et $\mathcal{D}_2$ ont pour équations :

$$\mathcal{D}_1 \ : \ y = ax \ , \ z = \alpha$$

$$\mathcal{D}_2 \ : \ y = -ax \ , \ z = -\alpha \quad (a \neq 0, \alpha \neq 0)$$



Pour $M(x, y, z)$, on a :

$$d^2(M, \mathcal{D}_1) = \frac{(y - ax)^2}{1 + a^2} + (z - \alpha)^2$$

$$d^2(M, \mathcal{D}_2) = \frac{(y + ax)^2}{1 + a^2} + (z + \alpha)^2$$

et donc $\quad d^2(M, \mathcal{D}_1) + d^2(M, \mathcal{D}_2) = \dfrac{2}{1 + a^2}\left[a^2x^2 + y^2 + (1 + a^2)z^2 + (1 + a^2)\alpha^2\right].$

Le sous ensemble $\mathcal{E}$ des points $M(x, y, z)$ vérifiant $d^2(M, \mathcal{D}_1) + d^2(M, \mathcal{D}_2) = k$ est donc défini par l'équation

$$a^2x^2 + y^2 + (1 + a^2)z^2 = (1 + a^2)\left(\frac{k}{2} - \alpha^2\right).$$

- $k < 2\alpha^2$: $\mathcal{E} = \varnothing$,
- $k = 2\alpha^2$: $\mathcal{E} = \{O\}$,
- $k > 2\alpha^2$: $\mathcal{E}$ est un ellipsoïde de centre O et dont les directions principales sont définies par les axes de coordonnées.

Ex. 8

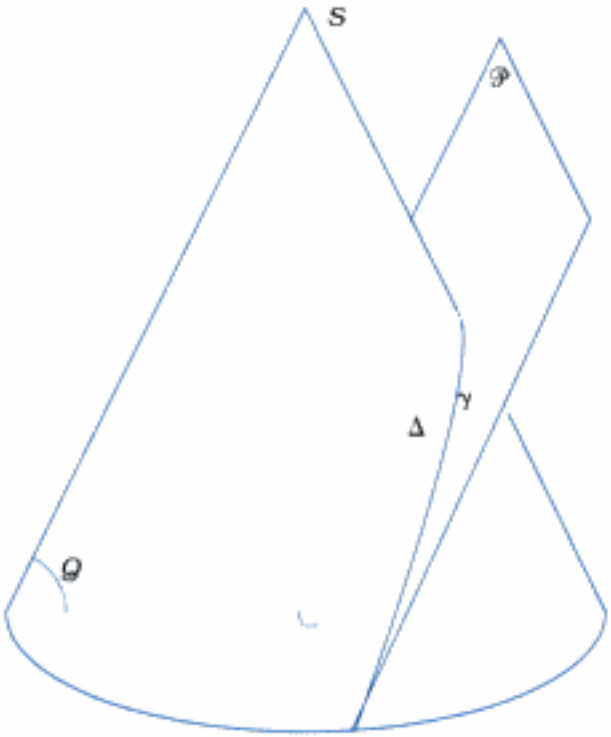
Si on exclut le cas où le cône est un plan, son sommet n'est pas dans le plan de la parabole.

Soit $\mathcal{C}$ un cône de révolution et $\mathcal{P}$ un plan coupant $\mathcal{C}$ suivant une parabole γ.

L'ensemble $\mathcal{C} \cup \mathcal{P}$ admet un plan de symétrie, à savoir le plan $\mathcal{Q}$ contenant l'axe de $\mathcal{C}$ ($\mathcal{Q}$ est donc un plan méridien) et perpendiculaire à $\mathcal{P}$.

Ce plan $\mathcal{Q}$ coupe $\mathcal{P}$ suivant l'axe de γ (par raison de symétrie), en conséquence on peut aussi dire que $\mathcal{S}$ se trouve dans le plan perpendiculaire à $\mathcal{P}$ suivant l'axe Δ de γ.

Copyrighted material



Dans l'exercice proposé, l'ensemble $\mathcal{L}$ cherché est donc inclus dans le plan perpendiculaire à xOy suivant l'axe de γ ($z = 0$, $y^2 = 2px$), c'est-à-dire dans xOz, privé de l'axe Ox.

Étant donné $S(x_0, 0, z_0)$, avec $z_0 \neq 0$, un point de ce plan xOz, formons une équation du cône $\mathcal{C}$ de sommet S et de directrice γ.

Pour tout $M(x, y, z)$ une représentation paramétrique de la droite (SM) est :

$$\lambda \mapsto \begin{pmatrix} x_0 + \lambda(x - x_0) \\ \lambda y \\ z_0 + \lambda(z - z_0) \end{pmatrix}.$$

donc $M \in \mathcal{C} \setminus \{S\} \iff \left(\dfrac{z_0 y}{z - z_0}\right)^2 = 2p\left(x_0 - \dfrac{z_0(x - x_0)}{z - z_0}\right) \quad z \neq z_0.$

Dans le repère $(S, \vec{i}, \vec{j}, \vec{k})$, $\mathcal{C}$ a donc pour équation :

$$z_0^2 Y^2 - 2pZ(x_0 Z - z_0 X) = 0 \quad Z \neq 0.$$

L'équation précédente représente un cône de révolution si et seulement si la matrice :

$$A = \begin{pmatrix} 0 & 0 & pz_0 \\ 0 & z_0^2 & 0 \\ pz_0 & 0 & -2px_0 \end{pmatrix}$$ admet une valeur propre double.

Remarque

Il existe alors une base orthonormale $(\vec{I}, \vec{J}, \vec{K})$ telle que dans le repère $(S, \vec{I}, \vec{J}, \vec{K})$, $\mathcal{C}$ ait pour équation : $\lambda(X_1^2 + Y_1^2) - \mu Z_1^2 = 0 \quad (\lambda > 0, \mu > 0)$.

Le polynôme caractéristique de A s'écrit :

$$\chi_A(\lambda) = (z_0^2 - \lambda)\left[\lambda(2px_0 + \lambda) - p^2 z_0^2\right] = (z_0^2 - \lambda)(\lambda^2 + 2px_0\lambda - p^2 z_0^2).$$

Le trinôme $\lambda^2 + 2px_0\lambda - z_0^2 p^2$ ne peut pas avoir de racine double (le produit de ses racines est $-z_0^2 p^2 < 0$).

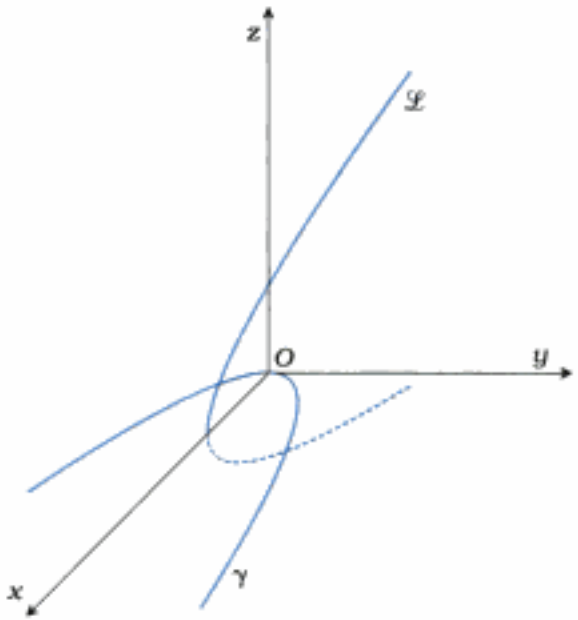
En conséquence, $\chi_A(\lambda)$ admet une racine double si et seulement si z_0^2 est racine du trinôme précédent avec $z_0 \neq 0$, c'est-à-dire :

$$z_0^4 + 2px_0 z_0^2 - p^2 z_0^2 = 0 \quad z_0 \neq 0 \quad \text{ou encore} \quad z_0^2 + 2px_0 - p^2 = 0 \quad z_0 \neq 0.$$

Le lieu cherché est donc la parabole $\mathcal{L}$ d'équations : $y = 0 \quad z^2 = 2p\left(\dfrac{p}{2} - x\right)$ privée de son sommet.

Copyrighted material

Les paraboles γ et $\mathscr{L}$ sont isométriques, situées dans des plans perpendiculaires, le sommet de l'une est le foyer de l'autre.



Ex. 9

1) Soit $A = \begin{bmatrix} 3 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & -1 \end{bmatrix}$ la matrice, dans la base $(\vec{i}, \vec{j}, \vec{k})$, de la forme quadratique q.

Le calcul donne $\det(A - \lambda I_3) = -\lambda\left(\lambda^2 - 2\lambda - 6\right)$ d'où les valeurs propres :

$$1+\sqrt{7} \quad , \quad 1-\sqrt{7} \quad \text{et} \quad 0.$$

Soit $(\vec{I}, \vec{J}, \vec{K})$ est une base orthonormale de $\mathbb{R}^3$, formée de vecteurs propres de l'endomorphisme symétrique f_q associé à q avec :

$$\mathbb{R}\vec{I} = \operatorname{Ker}\left(f_q - \left(1+\sqrt{7}\right)\operatorname{Id}\right) \ , \ \mathbb{R}\vec{J} = \operatorname{Ker}\left(f_q - \left(1-\sqrt{7}\right)\operatorname{Id}\right) \text{ et } \mathbb{R}\vec{K} = \operatorname{Ker} f_q.$$

Dans cette base, on a :

$$q(\vec{u}) = \left(1+\sqrt{7}\right)X^2 - \left(\sqrt{7}-1\right)Y^2 \quad \text{avec} \quad \vec{u} = x\vec{i} + y\vec{j} + z\vec{k} = X\vec{I} + Y\vec{J} + Z\vec{K}.$$

Donc, dans le repère $(O, \vec{I}, \vec{J}, \vec{K})$, $\mathcal{Q}$ a une équation de la forme :

$$\left(\sqrt{7}+1\right)X^2 - \left(\sqrt{7}-1\right)Y^2 + \alpha X + \beta Y + \gamma Z = 0.$$

Avec $\overrightarrow{OM} = x\vec{i} + y\vec{y} + z\vec{k} = X\vec{I} + Y\vec{J} + Z\vec{K}$, la partie quadratique de l'équation est :

$$q(\overrightarrow{OM}) = 3x^2 - z^2 + 2xy + 2yz + 2zx = \left(\sqrt{7}+1\right)X^2 - \left(\sqrt{7}-1\right)Y^2$$

et la partie linéaire est : $\ell(\overrightarrow{OM}) = -2x - 8y + 6z = \alpha X + \beta Y + \gamma Z$.

La discussion de la nature de $\mathcal{Q}$ repose essentiellement sur la nullité ou non nullité de γ.

En observant que $\gamma = \ell(\vec{K})$, on calcule $\vec{K}$. La résolution du système :

$$\begin{pmatrix} 3 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

donne : $$\operatorname{Ker} f_q = \operatorname{Vect}\left(\vec{i} - 2\vec{j} - \vec{k}\right).$$

On peut donc prendre $\vec{K} = \frac{1}{\sqrt{6}}\left(\vec{i} - 2\vec{j} - \vec{k}\right)$ et il vient alors :

$$\gamma = -\frac{2}{\sqrt{6}} + \frac{16}{\sqrt{6}} - \frac{6}{\sqrt{6}} = \frac{8}{\sqrt{6}}$$

Copyrighted material

Hidden page

Hidden page

Index

Copyrighted material

Copyrighted material

R

S

T

V

W

Copyrighted material

Notations usuelles

$\mathbb{K}$	Indifféremment $\mathbb{R}$ ou $\mathbb{C}$.
$[\![1, n]\!]$	Ensemble des entiers compris entre 1 et n au sens large, $n \in \mathbb{N}^*$.
$\mathbb{K}[X]$	Ensemble des polynômes sur $\mathbb{K}$.
$\mathbb{K}_n[K]$	$\subset \mathbb{K}[X]$, ensemble des polynômes de degré au plus égal à $n \in \mathbb{N}$.
$A \wedge B$	PGCD des éléments A et B, entiers ou polynômes.
$A \vee B$	PPCM des éléments A et B, entiers ou polynômes.
$\mathrm{Card}\, E$ ou $\#E$	Cardinal de l'ensemble E.
$\mathbb{Z}[i]$	Aneau des entiers de Gauss.
$\mathbb{Z}/n\mathbb{Z}$	Ensemble des classes d'équivalence modulo n.
$\varphi(n)$	Indicateur d'Euler de l'entier n.
$\mathscr{L}(E, F)$	Ensemble des applications linéaires de E dans F.
$\mathscr{L}(E)$	Ensemble des endomorphismes de E.
$\mathrm{GL}(E)$	Ensemble des automorphismes de E (groupe linéaire de E).
δ_{ij}	Symbole de Kronecker pour les éléments i et j.
$\mathrm{Im}\, f$	Image de l'application f.
$\mathrm{Ker}\, f$	Noyau de l'application linéaire f.
$\mathrm{rg}\, f$	Rang de l'applicaion linéaire f.
$A \oplus B$	Somme directe des sous-espaces vectoriels A et B.
$\mathrm{Vect}\, A$	Sous-espace vectoriel engendré par le sous-ensemble A.
$\det_{\mathscr{B}}$	Déterminant dans la base $\mathscr{B}$.
$\det f$	Déterminant de l'endomorphisme f.
$\mathfrak{S}(E)$	Ensemble des permutations de E.
$\mathfrak{S}_n$	Groupe symétrique d'ordre n, ensemble des permutations de $[\![1, n]\!]$.
$\varepsilon(\sigma)$	Signature de la permutation σ.

$\mathcal{M}_{n,p}(\mathbb{K})$	Ensemble des matrices de type (n, p) sur le corps $\mathbb{K}$.
$\mathcal{M}_n(\mathbb{K})$	Ensemble des matrices carrées d'ordre n sur le corps $\mathbb{K}$.
$\mathcal{S}_n(\mathbb{K})$	$\subset \mathcal{M}_n(\mathbb{K})$. Ensemble des matrices symétriques.
$\mathcal{A}_n(\mathbb{K})$	$\subset \mathcal{M}_n(\mathbb{K})$. Ensemble des matrices antisymétriques.
$\det A$	Déterminant de la matrice A.
$\mathrm{Tr}\, A$	Trace de la matrice A.
$\mathrm{Com}\, A$	Comatrice de la matrice A.
$\mathrm{GL}_n(\mathbb{K})$	$\subset \mathcal{M}_n(\mathbb{K})$. Ensemble des matrices carrées inversibles. Groupe linéaire d'ordre n.
$\langle u \mid v \rangle$	Produit scalaire des vecteurs u et v.
$[u, v, w]$	Produit mixte des vecteurs u, v, w.
$u \wedge v$	Produit vectoriel des vecteurs u et v.
$A^{\perp}$	Orthogonal d'un sous-ensemble A.
$\mathcal{O}n(\mathbb{R})$	$\subset \mathcal{M}_n(\mathbb{R})$. Ensemble des matrices réelles orthogonales. Groupe orthogonal.
$\mathcal{SO}_n(\mathbb{R})$	$\subset \mathcal{O}n(\mathbb{R})$, formé des matrices de déterminant +1. Groupe spécial orthogonal

Copyrighted material

Hidden page

Achevé d'imprimer en France par I.M.E. - 25110 Baume-les-Dames
N° d'impression : 17613 - Dépôt légal : août 2004
2080330/01

Copyrighted material

Copyrighted material

Titres disponibles en deuxième année dans la filière MP...

En Mathématiques
Analyse MP
Algèbre et géométrie MP

En Physique
Optique MP-PC-PSI-PT
Mécanique MP-PC
Électromagnétisme MP
Électronique MP
Thermodynamique MP

En Chimie
Chimie MP-PT

Livres d'exercices
Mathématiques MP
Physique MP

LES NOUVEAUX

Précis

BRÉAL

Une collection tenant compte de vos besoins et de vos contraintes, conçue pour vous aider tout au long de l'année à préparer efficacement les concours.

- **Un cours complet et très clair**, illustré de nombreux exemples, pour comprendre et assimiler.
- **Des pages de méthode**, facilement mémorisables, pour acquérir les savoir-faire et les réflexes nécessaires.
- **De nombreux exercices corrigés**, variés et progressifs, pour s'entraîner régulièrement.

Les Nouveaux Précis Bréal sont **la collection de référence** pour réussir sa prépa et intégrer une grande école d'ingénieurs.

BRÉAL, L'ÉDITEUR DES PRÉPAS

Réf. : 208.0330
ISBN : 2 7495 0388 4
www.editions-breal.fr