Compléments d'algèbre

25 mars 2019

Première partie

Décomposition de Dunford

Cette décomposition, qui ne figure pas au programme français, est pourtant très utile et permet de résoudre de nombreux exercices (d'oraux notamment).

1 Enoncé

Soit $A \in \mathcal{M}_n(\mathbb{K})$ une matrice trigonalisable. Alors,

$\exists (D, N) \in \mathcal{M}_n(\mathbb{K})^2 | DN = ND$, D soit diagonalisable et N nilpotente.

De plus cette décomposition est unique et D et N sont des polynômes en A. En pratique, c'est l'existence dont on se sert souvent.
Il existe une version équivalente pour les endomorphismes, et c'est celle que nous allons montrer. Soit $u \in \mathcal{L}(E)$ un endomorphisme trigonalisable :

$$\exists ! (d, n) \in \mathcal{L}(E) | dn = nd,\ d \text{ soit diagonalisable et } n \text{ nilpotent.}$$

2 Démonstration

2.1 Espaces caractéristiques

Pour la démonstration, commençons par introduire les sous-espaces caractéristiques d'un endomorphisme trigonalisable u.
Pour $\lambda \in \mathrm{Sp}(u)$ de multiplicité α_λ, on pose $F_\lambda = \mathrm{Ker}\,(u - \lambda Id)^{\alpha_\lambda}$.
Montrer que $E = \oplus_{\lambda \in \mathrm{Sp}(u)} F_\lambda$ et que ces sous-espaces sont stables par u.

2.2

Procédons par analyse-synthèse. Soit u un endomorphisme trigonalisable. Supposons qu'il existe d et n vérifiant les conditions voulues. On note $\mathrm{Sp}(d) = \{\lambda_1, ..., \lambda_p\}$ de multiplicités respectives $\alpha_1, ..., \alpha_p$ et, pour tout $i \in [|1, p|]$, on

pose $E_i = \mathrm{Ker}\,(d - \lambda_i Id)$.
Montrer que $E = \oplus_{i\in[|1,p|]} E_i$.

2.3

Montrer que les E_i sont stables par u, puis que l'endomorphisme $(u-\lambda_i Id)_{|E_i}$ est nilpotent. En déduire que les E_i associés à d sont les F_{λ_i} associés à u. L'endomorphisme d est donc défini de façon unique par :

$$\forall \lambda \in \mathrm{Sp}(u),\ d_{|\,\mathrm{Ker}\,(u-\lambda)^{\alpha_\lambda}} = \lambda Id.$$

2.4 Synthèse

En posant d défini tel que ci-dessus et $n = u - d$, vérifier que le couple (d, n) convient.

3 Applications

3.1 $\lim A^k$

Soit $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\forall \lambda \in \mathrm{Sp}(A)$, $|\lambda| < 1$. Montrer que $A^k \underset{k\to\infty}{\to} 0$.

Soit $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\forall \lambda \in \mathrm{Sp}(A)$, $|\lambda| \leq 1$. Montrer la convergence de :

$$\frac{\sum_{i=0}^{k-1} A^i}{k} \text{ lorsque } k \to \infty.$$

Donner une interprétation géométrique de cette limite.

3.2 $\exp A$

Soit $A, B \in \mathcal{M}_n(\mathbb{C})$ tel que $AB = BA$. Montrer que $\exp(A+B) = \exp A \exp B$. En déduire que l'exponentielle d'une matrice est toujours inversible (et donner l'expression de son inverse).

Trouver, à partir de la décomposition de Dunford, une méthode de calcul de l'exponentielle d'une matrice trigonalisable.

Deuxième partie
Réduction de Jordan

4 Enoncé

On commence par définir, $\forall n \in \mathbb{N}$, le bloc de Jordan J_n :
J_n est la matrice strictement triangulaire supérieure avec des 1 sur la sur-

diagonale et des 0 ailleurs.
On va montrer que tout endomorphisme nilpotent a pour matrice dans une certaine base une matrice diagonale par blocs de J_{k_i}, puis que tout endomorphisme trigonalisable a pour matrice dans une certaine base une matrice diagonale par blocs de $\lambda_i I_{k_i} + J_{k_i}$.

5 Réduction d'endomorphismes nilpotents

Montrer par récurrence sur la dimension de E qu'un endomorphisme nilpotent a pour matrice dans une certaine base une matrice diagonale par blocs de J_{k_i}.
Indication : en notant k l'indice de nilpotence de u, montrer qu'il existe $x \in E$ tel que $(x, u(x), ..., u^{k-1}(x))$ soit libre. En déduire l'existence de deux sous-espaces supplémentaires stables par u, puis procéder par récurrence.

6 Démonstration

Grâce au résultat sur les endomorphismes nilpotents, on va pouvoir prouver le théorème.
Démontrer le résultat dans le cas où il n'y a qu'une seule valeur propre, en utilisant la décomposition de Dunford.
En déduire le cas général par décomposition de E en somme directe des sous-espaces caractéristiques.

7 Applications

7.1 ${}^tA$

Grâce à la réduction de Jordan, montrer qu'une matrice trigonalisable est semblable à sa transposée.
Par existence d'une clôture algébrique, ce résultat est vrai pour toute matrice.

7.2 $\exp A$

Calculer l'exponentielle d'une matrice réduite sous forme de Jordan.

7.3 Equations différentielles

Vous verrez dans le cours sur les équations différentielles que toute équation différentielle peut se réduire en une équation différentielle matricielle d'ordre 1 : $\forall t$, $y'(t) = A(t)y(t)$ et $y(0) = y_0$, où $y \in \mathcal{C}^1(\mathbb{R}, \mathbb{C}^n)$ et $A \in \mathcal{C}^0(\mathbb{R}, \mathcal{M}_n(\mathbb{C}))$.

Dans le cas où A est constante, l'unique solution de ce problème de Cauchy est $t \mapsto \exp(tA)y_0$.
On peut donc calculer explicitement les solutions.

Existence d'une clôture algébrique Dans plusieurs démonstrations et exercices sur les matrices réelles, on scinde le polynôme minimal ou caractéristique dans le corps des complexes. C'est en fait un cas particulier d'une méthode qui consiste à utiliser l'existence d'une clôture algébrique.

Un corps est dit algébriquement clos lorsque tout polynôme à coefficients dans ce corps est scindé. C'est le cas du corps des complexes, mais pas de celui des réels. Or, $\mathbb{R}$ est un sous-corps de $\mathbb{C}$: on dit alors que $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.
Il s'agit aussi d'une clôture algébrique de $\mathbb{Q}$, dont une autre clôture algébrique plus petite (et même dénombrable) est l'ensemble :

$$\{\alpha \in \mathbb{R} | \exists P \in \mathbb{Q}[X] | P(\alpha) = 0\}$$

La démonstration se fait en utilisant le lemme de Zorn, équivalent à l'axiome du choix.

Des applications en algèbre linéaire sont la similitude entre une matrice et sa transposée, mais aussi la caractérisation de la nilpotence de f par $\forall k \in \mathbb{N}^*$, $\operatorname{tr} f^k = 0$, ou en fait tout résultat qui se démontre facilement si l'on suppose la matrice trigonalisable.

Troisième partie

Racine carrée d'une matrice symétrique positive

Soit $S \in \mathcal{S}_n(\mathbb{R})$. Montrer qu'il existe une unique matrice symétrique définie positive dont le carré est égal à S.
Pour l'unicité, on peut procéder en supposant A et B vérifiant de telles conditions et en montrant que :

$$\forall \lambda \in \operatorname{Sp}(S),\ E_{\sqrt{\lambda}}(A) = E_\lambda(S) = E_{\sqrt{\lambda}}(B)$$

On peut aussi montrer que A est un polynôme en S, d'où B commute avec A.
On conclut alors par diagonalisation simultanée.

Quatrième partie

Décomposition polaire

On va montrer que toute matrice réelle M s'écrit comme le produit d'une matrice orthogonale et d'une matrice symétrique.

Cette factorisation, appelée décomposition polaire, est un bon exemple d'utilisation des racines carrées de matrices symétriques positives. Elle est utile pour étudier les propriétés topologiques des groupes linéaires.

8 Matrices inversibles

Soit $M \in GL_n(\mathbb{R})$. Montrer que ${}^tMM$ est symétrique définie positive. En notant S sa racine carrée symétrique positive, montrer que S est inversible, puis que MS^{-1} est orthogonale.

Soit O orthogonale et S symétrique positive tel que $M = OS$. Montrer que $S^2 = {}^tMM$. En déduire l'unicité de S, puis de O.

9 Matrices réelles

Montrer l'existence de la décomposition polaire pour $M \in \mathcal{M}_n(\mathbb{R})$ en utilisant le résultat précédent.
L'unicité n'est pas assurée pour les matrices non inversibles.

10 Matrices complexes

Les résultats ci-dessus se retrouvent pour les matrices complexes par les analogies suivantes (en fait une seule analogie) :
On parle d'adjoint et non de transposée.
On parle de matrices unitaires et non orthogonales.
On parle de matrices hermitiennes et non symétriques.

Pour le cas $n = 1$, on retrouve le fait qu'un complexe z s'écrit $\rho e^{i\theta}$ avec $\rho \in \mathbb{R}_+$ et $\theta \in \mathbb{R}$, d'où le nom de décomposition polaire.

11 Topologie

Montrer que l'application suivante est un homéomorphisme (continu bijectif de réciproque continue) :

$$\left(\begin{array}{lcl} \mathcal{O}_n(\mathbb{R}) \times \mathcal{S}_n^{++}(\mathbb{R}) & \to & GL_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array} \right)$$

On peut en déduire des propriétés topologiques du groupe linéaire réel.

Cinquième partie

Décomposition LU et Cholesky

Soit $A = (a_{i,j})_{1 \leq i,j \leq n}$. Pour k entre 1 et n, on note $A_k = (a_{i,j})_{1 \leq i,j \leq k}$.
Supposons que les A_k soient toutes inversibles. Montrer par récurrence l'existence de L triangulaire inférieure (lower) à diagonale unité et U triangulaire supérieure (upper).
Montrer l'unicité de cette décomposition.

Soit $S \in \mathcal{S}_n^{++}(\mathbb{R})$. Utiliser la décomposition LU pour montrer qu'il existe une unique matrice T réelle triangulaire supérieure à coefficients diagonaux strictement positifs telle que $S = {}^tTT$.
Cette factorisation est appelée décomposition de Cholesky.
Son utilité est surtout calculatoire, l'algorithme de cette décomposition est en effet simple à implémenter, et on accède alors au déterminant de la matrice, à son inverse...

Sixième partie

Théorème de Cauchy

Soit G un groupe fini (d'élément neutre noté e). Le théorème de Lagrange affirme que l'ordre de tout élément de G divise $|G|$. (La démonstration est à connaître). On peut alors se demander si, étant donné un diviseur de $|G|$, il existe un élément de G dont l'ordre est précisément ce diviseur.
Le théorème de Cauchy (et les théorèmes de Sylow, qui en sont une généralisation) apportent des réponses partielles.

12 Enoncé

Soit p un diviseur premier de $|G|$. Alors, il existe $x \in G$ d'ordre p.

13 Démonstration

On considère l'ensemble suivant :

$$X = \{(x_1, ..., x_p) \in G^p | x_1 x_2 ... x_p = e\}$$

Calculer $|X|$.

Dans $\mathbb{Z}/p\mathbb{Z}$, on identifie la classe d'équivalence $\overline{i} = i + p\mathbb{Z}$ à son unique représentant entre 1 et p.

Pour $x = (x_1, .., x_p)$, montrer qu'en notant $\bar{i}x = (x_{\overline{1+i}}, ..., x_{\overline{p+i}})$, on a défini une action de groupe, c'est-à-dire que :

$$\left(\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z}) & \to & S(G) \\ \bar{i} & \mapsto & \left(x \in X \mapsto \bar{i}x\right) \end{array} \right) \text{ est un morphisme de groupes.}$$

Montrer que l'orbite de tout $x \in X$ (c'est-à-dire l'ensemble $\{\bar{i}x, \bar{i} \in \mathbb{Z}/p\mathbb{Z}\}$) est de cardinal 1 ou p. On remarque en particulier que $(e, ..., e)$ a une orbite réduite à lui-même. Si ce n'est pas le seul, montrer que le théorème est vérifié.
On suppose par l'absurde que c'est le seul. Montrer que :

$$|X| \equiv 1[p]$$

Conclure.

14 Généralisation

A titre culturel, voici le premier théorème de Sylow, qui généralise ce résultat :
Soit p un diviseur de $|G|$ et m la valuation de p dans $|G|$. Alors, il existe un sous-groupe de G d'ordre p^m.

D'autres théorèmes permettent de décrire plus précisément de tels sous-groupes, appelés p-groupes de Sylow.

Septième partie
Groupes quotients

15 Définition

On dit qu'un sous-groupe H de G est distingué lorsque :

$$\forall g \in G,\ gHg^{-1} = H.$$

Soit H un sous-groupe distingué de G. Montrer que la relation suivante $\mathcal{R}$ est une relation d'équivalence :

$$x\mathcal{R}y \Leftrightarrow xy^{-1} \in H$$

On note G/H l'ensemble des classes d'équivalence de $\mathcal{R}$ sur G.
Montrer que ces classes d'équivalence s'écrivent xH avec $x \in G$. Montrer que, pour xH et yH dans G/H, l'opération $xH \times yH = (xy)H$ ne dépend pas du représentant choisi et définit bien une structure de groupe sur G/H. C'est ce qu'on appelle un groupe quotient.

16 Théorème de Lagrange

Utiliser la notion de groupes quotients pour démontrer rapidement le théorème de Lagrange.

17 Clôture algébrique

Les groupes quotients permettent notamment de montrer l'existence d'une clôture algébrique (et, plus généralement, de manipuler des extensions algébriques). En effet, en considérant un polynôme P irréductible sur $\mathbb{K}[X]$, et en notant I l'idéal principal $P\mathbb{K}[X]$, $\mathbb{K}[X]/I$ constitue une extension algébrique de $\mathbb{K}$.

18 Ensembles de nombres

Une fois qu'on a construit l'ensemble $\mathbb{N}$, la notion d'ensemble quotient s'avère très utile pour construire les autres ensembles de nombres usuels.
En notant $H = \{(a, b) \in \mathbb{N}^2 | a = b\}$, on peut voir $\mathbb{Z}$ comme $\mathbb{N}^2/H$.
En notant $H = \{(a, b) \in \mathbb{Z} \times \mathbb{N}^* | ab = 1\}$, on peut voir $\mathbb{Q}$ comme $\mathbb{Z} \times \mathbb{N}^*/H$.
En notant E les suites de Cauchy de $\mathbb{Q}^{\mathbb{N}}$, $H = \{U \in E | U_n \to 0\}$, on peut voir $\mathbb{R}$ comme E/H.