Décomposition de Fitting
-
Cardinal du cône nilpotent

Leçon: 123, 153, 154, 157, 190

Ref: Carnet de voyage en algèbre

Théorème

Soient $\mathbb{K}$ un corps, E un $\mathbb{K}$-ev de dimension $d \in \mathbb{N}^*$, et $u \in \mathcal{L}(E)$. Alors il existe un entier $p \in \mathbb{N}$ tel que

$$E = \operatorname{Ker}(u^p) \oplus \operatorname{Im}(u^p)$$

<u>Démonstration</u>

Résultats préliminaires : $\star$ la suite $(\operatorname{Ker} u^k)_{k \geq 0}$ est $\nearrow$ et stationnaire.

$\star$ ——— $(\operatorname{Im} u^k)$ — $\searrow$ " "

$\star$ Soit $x \in \operatorname{Ker} u^k$, $k \geq 0$. Alors $u^{k+1}(x) = u(u^k(x)) = u(0) = 0$.

Donc $\operatorname{Ker} u^k \subset \operatorname{Ker} u^{k+1}$. La suite $(\operatorname{Ker} u^k)_{k\geq 0}$ est $\nearrow$.

La suite $(\dim(\operatorname{Ker} u^k))_{k \geq 0}$ est donc $\nearrow$, à valeurs dans $\mathbb{N}$, et majorée par d, elle est donc stationnaire.

$\star$ Soit $x \in \operatorname{Im} u^{k+1}$, $k \geq 0$. $(\operatorname{Im} u^0 = E)$.

Alors il existe $y \in E$ tq $x = u^{k+1}(y) \Rightarrow x = u^k(\underbrace{u(y)}_{\in E})$

donc $x \in \operatorname{Im} u^k$, $(\operatorname{Im} u^k)_{k\geq 0}$ est $\searrow$.

Pour les mêmes raisons, elle est stationnaire

Soit $p \in \mathbb{N}$ le plus petit entier tel que $\forall k \geq p$ $\operatorname{Ker} u^k = \operatorname{Ker} u^p$.

Alors par le thm du rang, $(\operatorname{Im} u^k)_{k\geq 0}$ stationne aussi à partir de p.

Mq $E = \operatorname{Ker} u^p \oplus \operatorname{Im} u^p$ pour ce p.

. Par le théorème du rang, $[\dim E = \dim \operatorname{Ker} u^p + \dim \operatorname{Im} u^p]$

. Soit $x \in \operatorname{Ker} u^p \cap \operatorname{Im} u^p$. Donc il existe $y \in E$ tq $u^p(y) = x$.

Donc $u^p(x) = u^{2p}(y) = 0$. Ainsi $y \in \operatorname{Ker} u^{2p}$.

Or $2p \geq p$, donc $\operatorname{Ker} u^{2p} = \operatorname{Ker} u^p$, donc $y \in \operatorname{Ker} u^p$ et $u^p(y) = x = 0$.

Ainsi $\boxed{E = \operatorname{Ker} u^p \oplus \operatorname{Im} u^p}$.

$\square$

Corollaire Toute matrice de $\mathcal{M}_n(\mathbb{K})$ est semblable à une matrice de la forme $\begin{pmatrix} N & 0 \\ 0 & C \end{pmatrix}$, où N est une matrice carrée nilpotente
C ______ inversible.

Démonstration

Soit $M \in \mathcal{M}_n(\mathbb{K})$. Soit u l'endo. canoniquement associé à M. On a par le théorème $\mathbb{K}^n = \operatorname{Ker} u^p \oplus \operatorname{Im} u^p$.

Les espaces sont stables par u :

. $x \in \operatorname{Ker} u^p \Rightarrow u^p(x) = 0 \Rightarrow u^p(u(x)) = u^{p+1}(x) = u(u^p(x)) = 0$
$\Rightarrow u(x) \in \operatorname{Ker} u^p$.

. $x \in \operatorname{Im} u^p \Rightarrow \exists y \in \mathbb{K}^n \; u^p(y) = x \Rightarrow \exists y \in \mathbb{K}^n \; u(x) = u^p(u(y))$
$\Rightarrow u(x) \in \operatorname{Im} u^p$.

On considère donc les endomorphismes induits. $u_{\operatorname{Ker} u^p}$ et $u_{\operatorname{Im} u^p}$.

$\rightarrow u_{\operatorname{Ker} u^p}$ est nilpotent d'indice p

$\rightarrow u_{\operatorname{Im} u^p}(\operatorname{Im} u^p) = \operatorname{Im} u^p$, surjectivité $\Leftrightarrow$ bijectivité (dimension finie).

En effet, $u_{\operatorname{Im} u^p} : \operatorname{Im} u^p \rightarrow \operatorname{Im} u^p$

$\rightarrow$ si $x \in u_{\operatorname{Im} u^p}(\operatorname{Im} u^p)$, donc il existe $y \in \operatorname{Im} u^p$ tq
$x = u_{\operatorname{Im} u^p}(y) = u(y) = u^{p+1}(z)$.
$\hookrightarrow$ où $y = u^p(z)$, $z \in E$.

Donc $x \in \operatorname{Im} u^{p+1} = \operatorname{Im} u^p$ par déf de p.

$\rightarrow$ Si $x \in \operatorname{Im} u^p$, $x \in \operatorname{Im} u^{p+1}$, donc $x = u^{p+1}(y) = u(\underbrace{u^p(y)}_{\in \operatorname{Im} u^p})$
donc $x \in u_{\operatorname{Im} u^p}(\operatorname{Im} u^p)$.

$\square$

Application Soit m_d le cardinal de l'ensemble des matrices nilpotentes de taille d sur $\mathbb{F}_q$. Alors
$$m_d = q^{d(d-1)}$$

Démonstration

D'après le théorème de décomposition de Fitting, à chaque $u \in \mathcal{L}(E)$ on peut associer $((F,G), v, w)$ où :

. $(F,G) = (\operatorname{Ker} u^p, \operatorname{Im} u^p)$ un couple de sev supplémentaires

. $v := u|_{\operatorname{Ker} u^p}$ un endo. nilpotent sur $\operatorname{Ker} u^p$

. $w = u|_{\operatorname{Im} u^p}$ un automorphisme de $\operatorname{Im} u^p$.

Réciproquement, si on se donne $((F,G), v, w)$, l'endo.

$u : x \mapsto v(x_F) + w(x_G)$, où $x = x_F + x_G$ est la décomposition de $x \in E$ sur $F \oplus G$, u est bien défini.

De plus pour $n \in \mathbb{N}$ assez grand, $u^n = \underbrace{v^n}_{\text{nilpotent}} + w^n = w^n$

donc, $F = \mathrm{Ker}\, u^n$ et $G = \mathrm{Im}\, u^n$.

On a alors une bijection :

$$\mathrm{End}(E) \longleftrightarrow ((F,G), v, w), \text{ où } \left|\begin{array}{l} .\ F \oplus G = E \\ .\ v \text{ nilpotent sur } F \\ .\ w \in \mathrm{Aut}(G) \end{array}\right.$$

On note : . $m_{k,d}$ le nombre de couple de sous-espaces (F,G) de $\mathbb{K}^d$ tel que $\dim F = k$ et $F \oplus G = \mathbb{K}^d$.

. m_k le nombre de matrice nilpotente sur $\mathbb{F}_q$.

. $g_d = |GL_d(\mathbb{F}_q)|$.

Alors : $|\mathrm{End}(E)| = q^{d^2}$ car $\dim \mathcal{L}(E) = (\dim E)^2 = d^2$ $\quad (\mathcal{L}(E) \leftrightarrow \mathrm{End}(E))$

et on a aussi $|\mathcal{L}(E)| = \sum_{k=0}^{d} m_{k,d}\, m_k\, g_{d-k}$

Or $GL_n(\mathbb{F}_q) \underset{\text{transitivement}}{\curvearrowright} \left\{ (F,G), \text{ t.q. } \left| \begin{array}{l} (F \oplus G = \mathbb{F}_q^n) \\ \dim F = k \end{array}\right. \right\}$

et $\mathrm{Stab}(F,G) \simeq GL_k(\mathbb{F}_q) \times GL_{d-k}(\mathbb{F}_q)$.

mais $|\mathrm{Orb}(F,G)| = \dfrac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}(F,G)|}$ et par transitivité

$\left[m_{k,d} = \dfrac{g_d}{g_k\, g_{d-k}} \right]$. Ainsi : $q^{d^2} = \sum_{k=0}^{d} \dfrac{g_d}{g_k \cancel{g_{d-k}}} m_k \cancel{g_{d-k}} = g_d \sum_{k=0}^{d} \dfrac{m_k}{g_k}$

Par soustraction de l'égalité en d et $d-1$:

$\dfrac{q^{d^2}}{g_d} - \dfrac{q^{(d-1)^2}}{g_{d-1}} = \dfrac{m_d}{g_d}$ soit $m_d = q^{d^2} - \dfrac{g_d}{g_{d-1}}\, q^{(d-1)^2}$.

Déterminons $g_d = |GL_d(\mathbb{F}_q)|$. Cela revient à dénombrer le nbr de base de $\mathbb{F}_q$, i.e d vecteurs de $\mathbb{F}_q$ indépendants.

1^{er} vecteur : tous les vecteurs sauf 0 : $q^d - 1$ choix.

$2^{ème}$ " ——— sauf ceux dans le vect. de la $1^{ère}$ colonne : $q^d - q$

...

Ainsi : $$\boxed{\begin{aligned} g_d &= (q^d-1)(q^d-q)(q^d-q^2)\cdots(q^d-q^{d-1}) \\ &= \prod_{i=0}^{d-1}(q^d - q^i). \end{aligned}}$$

Alors $$\frac{g_d}{g_{d-1}} = \frac{(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})}{(q^{d-1}-1)(q^{d-1}-q)\cdots(q^{d-1}-q^{d-2})} = q^{d-1}(q^d-1).$$

Ainsi on a finalement : $$\begin{aligned} m_d &= q^{d^2} - q^{d-1}(q^d-1)q^{(d-1)^2} \\ &= \cancel{q^{d^2}} - (\cancel{q^{2d-1}} - q^{d-1})q^{d^2-2d+1} \\ &= q^{d^2-d} \Rightarrow \boxed{m_d = q^{d(d-1)}}. \end{aligned}$$

□