Lemme de Fitting et cardinal du cône nilpotent

Geoffrey Deperle

Leçons associées :
- 123 : Corps finis. Applications.
- 151 : Dimension d'un espace vectoriel. Rang. Exemples et applications.
- 153 : Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie.
- 154 : Sous-espaces stables par un endomorphisme en dimension finie. Applications.
- 157 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

Le but de ce développement est de montrer le théorème suivant :

Théorème. *Soit E un espace vectoriel de dimension n et $u \in \mathcal{L}(E)$, il existe $p \in \mathbb{N}$ tel que*

$$E = \mathrm{Ker} u^p \oplus \mathrm{Im} u^p$$

Preuve : Soit P un polynôme annulateur de u et p la multiplicité de 0 comme racine de P. Notons Q le polynôme tel que $Q(0) \neq 0$ et $P(X) = X^p Q(X)$.
D'après le lemme des noyaux : $E = \mathrm{Ker} u^p \oplus \mathrm{Im} u^p$.

Montrons que $\mathrm{Ker} Q(u) = \mathrm{Im} u^p$,
Comme $\mathrm{Ker} Q(u)$ est stable par u^p et $\mathrm{Ker} u^p \cap \mathrm{Ker} Q(u) = \{0\}$, l'endomorphisme induit $u^p_{\mathrm{Ker} Q(u)}$ est injectif donc réalise un isomorphisme de $\mathrm{Ker} Q(u)$ dans $\mathrm{Ker} Q(u)$.
D'où $\mathrm{Ker} Q(u) = u^p(\mathrm{Ker} Q(u)) \subset \mathrm{Im} u^p$ et par théorème du rang, $\dim \mathrm{Im} u^p = \dim E - \dim \mathrm{Ker} u^p = \dim \mathrm{Ker} Q(u)$.
D'où $\mathrm{Ker} Q(u) = \mathrm{Im} u^p$. □

Corollaire 1. *Toute matrice M 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 nilpotente et C est une matrice carrée inversible.*

Preuve : Soit u l'endomorphisme canoniquement associé à $M \in \mathcal{M}_n(\mathbb{K})$, on a

$$\mathbb{K}^n = \mathrm{Ker} u^p \oplus \mathrm{Im} u^p$$

Comme les espaces $\mathrm{Ker} u^p$ et $\mathrm{Im} u^p$ sont stables par u (car pour $x \in \mathrm{Ker} u^p, u(x) \in \mathrm{Ker} u^{p+1} \subset \mathrm{Ker} u^p$ et si $y \in \mathrm{Im} u^p$, alors il existe $x \in \mathbb{K}^n$ tel que $y = u^p(x)$ donc $u(y) = u^p(u(x)) \in \mathrm{Im} u^p$).

La matrice de u dans la base obtenue par concaténation d'une base de $\mathrm{Ker} u^p$ et $\mathrm{Im} u^p$ est de la forme

$$\begin{pmatrix} N & 0 \\ 0 & C \end{pmatrix}$$

Avec

— $u_{\mathrm{Ker}u^p}$ est nilpotente d'indice p donc N est nilpotente.

— $u_{\mathrm{Im}u^p}(\mathrm{Im}u^p) = \mathrm{Im}u^p$ donc $u_{\mathrm{Im}u^p}$ est surjective donc bijective donc C est inversible.

$\square$

Application. *Soit n_d le cardinal de l'ensemble des matrices nilpotente de taille d sur $\mathbb{F}_q$ alors*

$$n_d = q^{d(d-1)}$$

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

— $(F,G) = (\mathrm{Ker}u^{n_0}, \mathrm{Im}u^{n_0})$ est un couple de sous-espaces vectoriels supplémentaires dans E.

— $v = u_{\mathrm{Ker}u^{n_0}}$ est un endomorphisme nilpotent de $\mathrm{Ker}u^{n_0}$

— $w = u_{\mathrm{Im}u^{n_0}}$ un automorphisme de $\mathrm{Im}u^{n_0}$.

Réciproquement, on peut montrer qu'une telle donnée détermine un élément de $\mathcal{L}(E)$.

Notons $m_{k,d}$ le nombre de couples de sous-espaces (F,G) de $\mathbb{K}^d$ tel que $\dim F = k$ et $\dim F \oplus G = \mathbb{K}^d$, notons n_k le nombre de matrices nilpotentes sur $\mathbb{F}_q$ et $g_k = |\mathrm{GL}_m(\mathbb{F}_q)|$. On a

$$\underbrace{|\mathcal{L}(E)|}_{=q^{d^2}} = \sum_{k=0}^{d} m_{k,d} n_k g_{d-k}$$

Or, comme $\mathrm{GL}_n(\mathbb{K})$ agit transitivement sur les (F,G) tel que $F \oplus G = \mathbb{F}_q^n$ avec

$$\mathrm{Stab}((F,G)) \simeq \mathrm{GL}_k(\mathbb{F}_q^n) \times \mathrm{GL}_{n-k}(\mathbb{F}_q^n)$$

Par transitivité, $m_{k,d} = \dfrac{|\mathrm{GL}_d(\mathbb{F}_q)|}{|\mathrm{GL}_k(\mathbb{F}_q) \times \mathrm{GL}_{d-k}(\mathbb{F}_q)|} = \dfrac{g_d}{g_k g_{d-k}}$.

D'où $q^{d^2} = \displaystyle\sum_{k=0}^{d} \frac{g_d}{g_k g_{d-k}} n_k g_{d-k}$ d'où $\dfrac{q^{d^2}}{g_d} = \displaystyle\sum_{k=0}^{d} \frac{n_k}{g_k}$.

Donc en soustrayant l'égalité entre d et $d-1$, $\frac{q^{d^2}}{g_d} - \frac{q^{(d-1)^2}}{g_{d-1}} = \frac{n_d}{g_d}$ d'où $n_d = q^{d^2} - \frac{g_d}{g_{d-1}} q^{(d-1)^2}$.

Or, comme $g_d = q^{\frac{d(d-1)}{2}} \displaystyle\prod_{i=1}^{d} (q^i - 1)$, on a $\frac{g_d}{g_{d-1}} = q^{d-1}(q^d - 1)$ d'où

$$\begin{aligned} n_d &= q^{d^2} - q^{d-1}(q^d-1)q^{(d-1)^2} \\ &= q^{d^2} - q^{d^2-2d+1+d-1}(q^d-1) \\ &= q^{d^2} - q^{d(d-1)}(q^d-1) \\ &= q^{d(d-1)} \end{aligned}$$

$\square$

Références

[1] Philippe Caldero et Marie Peronnier. *Carnet de voyage en Algébrie*. Calvage Mounet, 2019.

[2] Roger Mansuy et Rached Mneimné. *Algèbre linéaire : Réduction des endomorphismes*. Vuibert, 2012.