Lemme de Fitting
et
Cardinal du cône nilpotent

Cadre : Soient $\mathbb{K}$ un corps, E un $\mathbb{K}-e.v.$ de dimension finie d et $u \in \mathrm{End}(E)$.

Lemme 1 (**de Fitting**).
Les suites $\left(\mathrm{Ker}(u^k)\right)_{k\geqslant 0}$ et $\left(Im(u^k)\right)_{k\geqslant 0}$ sont respectivement croissante et décroissante stationnaires à partir d'un certain rang n_0 où l'on a :

$$E = \mathrm{Ker}(u^{n_0}) \oplus Im(u^{n_0})$$

Application 2 (**Cardinal du cône nilpotent**).
Le cardinal n_d de l'ensemble des matrices carrées nilpotentes de taille d sur un corps fini de cardinal q est :

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

Démonstration du lemme.

Il est clair que la suite des noyaux $\left(\mathrm{Ker}(u^k)\right)_{k\geqslant 0}$, resp. la suite des images $\left(\mathrm{Im}(u^k)\right)_{k\geqslant 0}$, est croissante, resp. décroissante, pour l'inclusion et donc stationnaire puisque nous sommes en dimension finie.

De plus, ces suites stationnent au même rang, car si $\dim \mathrm{Ker}(u^k) = \dim \mathrm{Ker}(u^{k+1})$ alors par la formule du rang on aura également que $\dim \mathrm{Im}(u^k) = \dim \mathrm{Im}(u^{k+1})$.
Notons n_0 le rang commun à partir duquel les suites sont stationnaires.
Montrons que $\mathrm{Ker}(u^{n_0})$ et $\mathrm{Im}(u^{n_0})$ sont supplémentaires. Par la formule du rang, on a déjà : $d = \dim \mathrm{Ker}(u^{n_0}) + \mathrm{rg}(u^{n_0})$ et comme $\mathrm{Ker}(u^{n_0}), \mathrm{Im}(u^{n_0}) \subset E$, on a : $E = \mathrm{Ker}(u^{n_0}) + \mathrm{Im}(u^{n_0})$. Il reste à montrer que $\mathrm{Ker}(u^{n_0}) \bigcap \mathrm{Im}(u^{n_0}) = \{0\}$. Soit donc $x \in \mathrm{Ker}(u^{n_0}) \bigcap \mathrm{Im}(u^{n_0})$. Alors $u^{n_0}(x) = 0$ et il existe $y \in E$ tel que $x = u^{n_0}(y)$. D'où :

$$u^{n_0}(x) = u^{n_0}(u^{n_0}(y)) = u^{2n_0}(y) = 0\,, i.e.,\ y \in \mathrm{Ker}(u^{2n_0})$$

Or, $\mathrm{Ker}(u^{2n_0}) = \mathrm{Ker}(u^{n_0})$ d'où $y \in \mathrm{Ker}(u^{n_0})$, *i.e.*, $u^{n_0}(y) = 0$. Donc $\mathrm{Ker}(u^{n_0}) \bigcap \mathrm{Im}(u^{n_0}) = \{0\}$. Ce qui montre la somme directe.
Notations : $F = \mathrm{Ker}(u^{n_0})$ et $G = \mathrm{Im}(u^{n_0})$.

Décomposition de Fitting

Il est facile de voir que F et G sont stables par u, ainsi u induit deux endomorphismes $u_F F \to F$ et $u_G : G \to G$ définis par $u_F(x) = u(x)$ pour $x \in F$ et $u_G(x) = u(x)$ pour $x \in G$. On a aussi que u_F est nilpotent d'indice n_0.
De plus, u_G est un automorphisme de G. En effet :

$$\mathrm{Im}(u_G) = u_G(G) = u_G(\mathrm{Im}(u^{n_0})) = u\left(\mathrm{Im}(u^{n_0})\right) = \mathrm{Im}(u^{n_0+1}) = \mathrm{Im}(u^{n_0})$$

Donc u_G est surjectif donc bijectif car nous sommes en dimension finie.
La donnée $((F, G), v, w)$ où :

$$F \oplus G = E\,, \quad F = \mathrm{Ker}(u^{n_0})\,, \quad G = \mathrm{Im}(u^{n_0})\,, \quad v = u_{_F} \text{ nilpotent d'indice } n_0\,, \quad w = u_{_G} \in \mathcal{A}\mathrm{ut}(G)$$

sera appelée la décomposition de Fitting de u.

□

Démonstration de l'application.

On note : $\mathfrak{m}_{k,\,d} = \#\big\{(F,G) \;:\; F \oplus G = \mathbb{K}^d \text{ et } \dim F = k\big\} = \dfrac{|\mathrm{GL}_d(\mathbb{K})|}{|\mathrm{GL}_k(\mathbb{K})| \times |\mathrm{GL}_{d-k}(\mathbb{K})|} = \dfrac{g_{_d}}{g_{_k} \times g_{_{d\,-\,k}}}$

Étape 1 :

On veut montrer que : $|\mathrm{End}(E)| = \displaystyle\sum_{k=0}^{d} \mathfrak{m}_{k,\,d} \times n_{_k} \times g_{_{d\,-\,k}}$ où $n_{_k}$ est le nombre de matrices nilpotentes de taille $k \times k$.

Pour cela, montrons que l'application : $\begin{array}{rccl} \Phi : & \mathrm{End} & \longrightarrow & \mathcal{E} \\ & u & \longmapsto & \big(\mathrm{Ker}(u^{n_0})\,, \mathrm{Im}(u^{n_0})\,, u_{_{\mathrm{Ker}(u^{n_0})}}, v_{_{\mathrm{Im}(u^{n_0})}}\big) \end{array}$ est bijective avec : $\mathcal{E} = \big\{\big((F,G)\,, v\,, w\big) \;:\; F \oplus G = E\,, v \textit{ nilpotente}\,, w \in \mathcal{A}\mathrm{ut}(G)\big\}$.

Grâce à la décomposition de Fitting, Φ est bien définie et Φ est injective.

On pose $u = v \oplus w$ et par stabilité de v et w on a : $u^n = v^n \oplus w^n = 0_{_F} \oplus w^n$ et on obtient :

$$\mathrm{Mat}_{\underline{e}}(u^n) = \begin{pmatrix} 0 & 0 \\ 0 & \mathrm{Mat}_{\underline{e}}(w^n) \end{pmatrix}$$

Ainsi, on voit que F est le noyau de u^n et que $\mathrm{Im}(u^n) = \mathrm{Im}(w^n) = G$. Ce qui montre la surjectivité de Φ et donc Φ est bien bijective.

Or, $\dim F \in [\![0, d]\!]$, donc $\#\mathcal{E} = \displaystyle\sum_{k=0}^{d} \mathfrak{m}_{k,\,d} \times n_{_k} \times g_{_{d-}}$ avec :

- $\mathfrak{m}_{k,\,d}$: nombre de couple (F,G) où $\dim F = k$
- $n_{_k}$: nombre de matrices nilpotentes de taille k
- $g_{_{d\,-\,k}}$: nombre d'automorphismes de taille $d - k$

D'où, par bijectivité de Φ, on obtient :

$$\mathrm{End}(E) \;=\; \sum_{k=0}^{d} \mathfrak{m}_{k,\,d} \times n_{_k} \times g_{_{d-}}$$

Étape 2 :

On veut montrer que : $\quad n_{_d} = q^{d(d-1)}$. On a : $\mathfrak{m}_{k,\,d} \times n_{_k} \times g_{_{d\,-\,k}} = \dfrac{g_{_d}}{g_{_k} \times g_{_{d\,-\,k}}} \times n_{_k} \times g_{_{d\,-\,k}} = \dfrac{g_{_d} \times n_{_k}}{g_{_k}}$.

De plus : $\quad \dim\left(\mathrm{End}(E)\right) = d^2 \quad$ donc $\quad \#\mathrm{End}(E) = q^{d^2}$. $\quad$ D'où :

$$\#\mathrm{End}(E) = \sum_{k=0}^{d} \frac{g_d \times n_{_k}}{g_{_k}} = q^{d^2}\,, \quad \textit{i.e.,} \quad \frac{q^{d^2}}{g_{_d}} = \sum_{k=0}^{d} \frac{n_{_k}}{g_{_k}}$$

Si l'on remplace d par $d - 1$, on obtient :

$$\frac{q^{(d-1)^2}}{g_{_{d\,-\,1}}} = \sum_{k=0}^{d-1} \frac{n_{_k}}{g_{_k}}$$

Ainsi, en soustrayant les deux, on obtient :

$$\frac{q^{d^2}}{g_{_d}} - \frac{q^{(d-1)^2}}{g_{_{d\,-\,1}}} = \frac{n_{_d}}{g_{_d}}\,, \qquad \textit{i.e.,} \qquad n_{_d} = q^{d^2} - q^{(d-1)^2}\,\frac{g_{_d}}{g_{_{d\,-\,1}}}$$

Or,

$$\begin{aligned} g_m &= \big(q^m-1\big)\big(q^m-q\big)\cdots\big(q^m-q^{m-1}\big) = \big(q^m-1\big)\big(q^{m-1}-1\big)q^2\big(q^{m-2}-1\big)\cdots q^{m-1}\big(q-1\big) \\ &= q^{\sum_{i=0}^{m-1} i} \prod_{k=0}^{m-1} \big(q^{m-k}-1\big) = q^{\frac{m(m-1)}{2}} \prod_{k=0}^{m-1} \big(q^{m-k}-1\big) \end{aligned}$$

D'où :

$$\begin{aligned} \frac{g_d}{g_{d-1}} &= \frac{q^{d(d-1)/2}\big(q^d-1\big)\big(q^{d-1}-1\big)\cdots\big(q-1\big)}{q^{(d-1)(d-2)/2}\times\big(q^{d-1}-1\big)\big(q^{d-2}-1\big)\cdots\big(q-1\big)} = q^{(d-1)(d-d+2)/2}\big(q^d-1\big) \\ &= q^{d-1}\times\big(q^d-1\big) = q^{2d-1}-q^{d-1} \end{aligned}$$

Ainsi :

$$\begin{aligned} n_d &= q^{d^2} - q^{(d-1)^2}\frac{g_d}{g_{d-1}} = q^{d^2} - q^{(d-1)^2}\left(q^{2d-1}-q^{d-1}\right) \\ &= q^{d^2} - q^{d^2-2d+1+2d-1} + q^{d^2-2d+1+d-1} = q^{d^2} - q^{d^2} + q^{d^2-d} \end{aligned}$$

Finalement :

$$\boxed{q^{d(d-1)}}$$

$\square$