Cardinal du cône nilpotent

↪ Ref : Carnet de voyage en Algèbre, p74-76

Soit $\mathbb{K}$ un corps, E un $\mathbb{K}$-ev de dimension finie d et $u \in End(E)$.

Lemme (de Fitting) : les suites $(Ker(u^k))_{k\geq 0}$ et $(Im(u^k))_{k\geq 0}$ sont respectivement strictement croissante et strictement décroissante puis stationnent à partir d'un certain rang n_0 où l'on a $E = Ker(u^{n_0}) \oplus Im(u^{n_0})$.
De plus, l'endomorphisme induit $u_{Ker(u^{n_0})}$ est nilpotent et l'endomorphisme induit $u_{Im(u^{n_0})}$ est un automorphisme.

La donnée de $((F,G), v, w)$ où $E = F \oplus G$, $F = Ker(u^{n_0})$, $G = Im(u^{n_0})$, $v = u_{Ker(u^{n_0})}$ nilpotent d'indice n_0, $w = u_{Im(u^{n_0})} \in Aut(G)$ sera appelée la décomposition de Fitting de u.

Théorème : Le cardinal n_d de l'ensemble des matrices carrées nilpotentes de taille d sur un corps de cardinal q est $n_d = q^{d(d-1)}$.

Preuve du lemme de Fitting : Il est clair que la suite des noyaux $(Ker(u^k))_{k\geq 0}$ est croissante, et que la suite des images $(Im(u^k))_{k\geq 0}$ est décroissante pour l'inclusion, et chacune est donc stationnaire puisque l'on travaille en dimension finie.
Les noyaux sont en fait croissants strictement : Mq $Ker\, u^k = Ker\, u^{k+1} \Rightarrow Ker\, u^{k+1} = Ker\, u^{k+2}$
Si $x \in Ker\, u^{k+2}$ alors $u^{k+1}(u(x)) = 0$ donc $u(x) \in Ker\, u^{k+1} = Ker\, u^k$ donc $u^{k+1}(x) = 0$
De même, la suite des images est strictement décroissante ; grâce au théorème du rang, $\dim(Im(u^k)) = \dim E - \dim(Ker(u^k))$.
Ce théorème du rang nous indique également que la suite des images stationne au même rang que la suite des noyaux : si $\dim(Ker(u^k)) = \dim(Ker(u^{k+1}))$, alors $\dim(Im(u^k)) = \dim(Im(u^{k+1}))$.
Notons n_0 le rang commun à partir duquel les suites sont stationnaires.
Montrons que $E = Ker(u^{n_0}) \oplus Im(u^{n_0})$. Par la formule du rang, on a déjà $\dim E = \dim(Ker(u^{n_0})) + \dim(Im(u^{n_0}))$. Il suffit donc de montrer que $Ker(u^{n_0}) \cap Im(u^{n_0}) = \{0\}$.
Soit $x \in Ker(u^{n_0}) \cap Im(u^{n_0})$. Il existe $y \in E$ tel que $x = u^{n_0}(y)$ et $0 = u^{n_0}(x) = u^{2n_0}(y)$. Donc $y \in Ker(u^{2n_0}) = Ker(u^{n_0})$ et donc $x = u^{n_0}(y) = 0$.

Les deux sous espaces $Ker(u^{n_0})$ et $Im(u^{n_0})$ sont bien stables par u (u commute avec u^{n_0}), les endo induits sont bien définis.
De plus, par définition de $Ker(u^{n_0})$, $u_{Ker(u^{n_0})}$ est nilpotent d'indice n_0.
Enfin, $u_{Im(u^{n_0})}$ est un automorphisme car il est surjectif*:
$Im(u_{Im(u^{n_0})}) = Im(u^{n_0+1}) = Im(u^{n_0})$ par définition de n_0.
(* suffit car dimension finie)
On pose $\mathbb{K} = \mathbb{F}_q$ et $E = \mathbb{K}^d$.

Preuve du théorème : Etape 1 : Montrons $\boxed{|End(E)| = \sum_{k=0}^{d} m_{k,d} \times n_k \times g_{d-k}}$
où $m_{k,d} = |\{(F,G),\ F \oplus G = \mathbb{K}^d \text{ et } \dim F = k\}|$, n_k le nombre de matrices nilpotentes de taille $k \times k$ et $g_i = |GL_i(\mathbb{K})|$.
Pour cela, montrons que l'application $\Phi : End(E) \longrightarrow \mathcal{E}$
$u \longmapsto (Ker(u^{n_0}), Im(u^{n_0}), u_{Ker(u^{n_0})}, u_{Im(u^{n_0})})$
est bijective, où $\mathcal{E} = \{((F,G), v, w),\ E = F \oplus G,\ v \text{ nilp sur } F,\ w \in Aut(G)\}$
Grâce à la décomposition de Fitting prouvée précédemment, Φ est bien définie et injective. Montrons que Φ est surjective
Si l'on se donne $((F,G), v, w)$ tel que $E = F \oplus G$, v nilp sur F et $w \in Aut(G)$, alors on définit u de la façon suivante : pour $x = \underset{\in F}{x_F} + \underset{\in G}{x_G}$ (décomposition de x sur $F \oplus G$), $u(x) = v(x_F) + w(x_G)$.
On note $u = v \oplus w$ ainsi construit. Alors $((F,G), v, w)$ est bien la décomposition de Fitting de u : soit n_0 l'indice de nilpotence de v, alors $u^{n_0} = v^{n_0} \oplus w^{n_0} = 0 \oplus w^{n_0}$, donc $F = Ker(u^{n_0})$ et $Im(u^{n_0}) = Im(w^{n_0}) = G$
Ainsi Φ est surjective.
Donc $|End(E)| = |\mathcal{E}| = \sum_{k=0}^{d} m_{k,d} \times n_k \times g_{d-k}$ (en fixant $k = \dim(F)$)

Etape 2 : Montrons que $\boxed{m_{k,d} = \frac{g_d}{g_k \times g_{d-k}}}$, où, on le rappelle,
$g_n = |GL_n(\mathbb{K})|$, et $g_n = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\cdots(q-1)$
Pour cela, on fait agir le groupe $GL_d(\mathbb{K})$ sur l'ensemble X_k :
$X_k = \{(F,G) \text{ sous espaces de } \mathbb{K}^d,\ \dim F = k \text{ et } F \oplus G = \mathbb{K}^d\}$ par l'action
$g \cdot (F,G) = (g(F), g(G))$ où $g \in GL_d(\mathbb{K})$ et $(F,G) \in X_k$.
L'action est transitive : on peut toujours envoyer une base adaptée à la décomposition $F \oplus G$ sur une base adaptée à la décomposition $F' \oplus G'$. (donc une seule orbite). Soit $F_0 = Vect(e_1, \dots, e_k)$ le sous espace engendré par les k premiers vecteurs de la base canonique de $\mathbb{K}^d$, et $G_0 = Vect(e_{k+1}, \dots, e_d)$ engendré par les $d-k$ suivants, de sorte que $(F_0, G_0) \in X_k$. Alors le stabilisateur de (F_0, G_0) dans $GL_d(\mathbb{K})$ est le sous groupe des matrices diagonales par blocs de la forme $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ avec $A \in GL_k(\mathbb{K})$ et $B \in GL_{d-k}(\mathbb{K})$
Le cardinal du stabilisateur est donc $g_k \times g_{d-k}$.

Ainsi, la relation orbite / stabilisateur nous donne le résultat attendu ie $|X_k| = m_{k,d} = \dfrac{g_d}{g_k \times g_{d-k}}$.

Etape 3 : Montrons que $\boxed{n_d = q^{d(d-1)}}$.

On a obtenu en combinant les deux étapes précédentes :

$$|End(E)| = \sum_{k=0}^{d} m_{k,d} \times n_k \times g_{d-k} = \sum_{k=0}^{d} \frac{g_d}{g_k \times g_{d-k}} \times n_k \times g_{d-k} = g_d \sum_{k=0}^{d} \frac{n_k}{g_k}.$$

Or $\dim(End(E)) = d^2$ donc $|End(E)| = q^{d^2}$.

Ainsi $\dfrac{q^{d^2}}{g_d} = \displaystyle\sum_{k=0}^{d} \frac{n_k}{g_k}$. En remplaçant d par $d-1$, on obtient

$$\frac{q^{(d-1)^2}}{g_{d-1}} = \sum_{k=0}^{d-1} \frac{n_k}{g_k}.$$

En soustrayant les deux équations, on déduit :

$$\frac{q^{d^2}}{g_d} - \frac{q^{(d-1)^2}}{g_{d-1}} = \frac{n_d}{g_d} \quad \text{ie} \quad n_d = q^{d^2} - q^{(d-1)^2} \frac{g_d}{g_{d-1}} \quad ⊛$$

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

Ainsi, $$n_d = q^{d^2} - q^{(d-1)^2}(q^{2d-1} - q^{d-1}) = q^{d^2} - q^{d^2-2d+1+2d-1} + q^{d^2-2d+1+d-1}$$
$$= q^{d^2} - q^{d^2} + q^{d^2-d} = q^{d^2-d}$$

Et ainsi $\underline{n_d = q^{d(d-1)}}$.

Remarques : * On peut obtenir ⊛ grâce aux séries formelles en remarquant que l'égalité $\dfrac{q^{d^2}}{g_d} = \displaystyle\sum_{k=0}^{d} \frac{n_k}{g_k} \times 1_{n-k}$ est un produit de Cauchy : $\displaystyle\sum_k \frac{q^{k^2}}{g_k} x^k = \sum_k \frac{n_k}{g_k} x^k \times \underbrace{\sum x^k}_{\frac{1}{1-x}}$, on multiplie par $(1-x)$ et le tour est joué !

* Une fois ce calcul effectué, on peut en déduire le nombre de matrices trigonalisables sur $\mathbb{F}_q$: $E = \bigoplus_{i=1}^{q} \mathrm{Ker}(M - \xi_i Id)^{n_i}$ pour M trig par le lemme des noyaux (éventuellement $\mathrm{Ker}(M - \xi_i Id) = \{0\}$) et sur cette espace, $M - \xi_i Id$ nilp donc $M = N + \xi_i Id$, ainsi

$$\{\text{matrices trig}\} \xrightarrow{\sim} \coprod_{\substack{n_1 + \cdots + n_q = d \\ n_i \geq 0}} \ \coprod_{\substack{E_1 \oplus \cdots \oplus E_q = E \\ \dim E_i = n_i}} Nil(E_1) \times \cdots \times Nil(E_q)$$

D'où $$|T_d(\mathbb{F}_q)| = \sum_{\substack{n_1 + \cdots + n_q = d \\ n_i \geq 0}} q^{\sum_i n_i(n_i-1)} \times \frac{g_d}{\prod_i g_{n_i}}$$

← bloc de Jordan nilp de taille max

* Heuristique : Pour $\mathbb{K}=\mathbb{C}$, l'orbite de J_d par l'action de $GL_d(\mathbb{K})$ est dense dans $\mathcal{N}_d$. Donc en extrapolant, on a envie de dire que sur $\mathbb{F}_q$, $|O_{J_d}|=|\mathcal{N}_d|$ (idée : """ $\mathbb{C}=\lim_{q\to+\infty}\mathbb{F}_q$ """)

Or sur $\mathbb{F}_q$, (relat° orbite stabilisateur), $|O_{J_d}|=\dfrac{|GL_d(\mathbb{F}_q)|}{|Stab_{J_d}|}$

et $Stab_{J_d}$ représente le commutant de J_d dans $GL_d(\mathbb{F}_q)$. Or J_d est une matrice cyclique donc $C(J_d)=\mathbb{F}_q[J_d]$ (*)

donc $Stab_{J_d}=\mathbb{F}_q[J_d]\cap GL_d(\mathbb{F}_q)$. Mais les polynômes en J_d sont de la forme $\begin{pmatrix} a_0 & a_1 & \cdots & a_d \\ & \ddots & \ddots & a_1 \\ (0) & & & a_0\end{pmatrix}$, inversible ssi $a_0\in\mathbb{F}_q^\times$: donc $(q-1)\times q^{d-1}$ choix de matrices.

D'où $|O_{J_d}|=\dfrac{(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})}{q^{d-1}(q-1)}\underset{q\to+\infty}{\sim}\dfrac{q^{d^2}}{q^d}=q^{d(d-1)}$ Surprise !

(*) <u>Rappels</u> : $\varphi_x : \mathbb{K}[X]\to E$, $P\mapsto P(u)(x)$, $\operatorname{Im}\varphi_x=:E_x$ ▷ u est cyclique s'il existe $x\in E$ tq $E_x=E$

▷ Il existe $x\in E$ tq $\mu_x=\mu$ ⟹ u est cyclique ssi $\chi=\mu$

▷ Soit $x\in E$ tq $\mu_x=\mu$. Alors E_x est un sous espace stable pour u pour lequel il existe un supplémentaire u-stable.

▷ [u est cyclique ssi $C(u)=\mathbb{K}[u]$]

"⟹" Soit $v\in C(u)$. Par hyp, $\exists x$, $E_x=E$ donc $v(x)=P(u)(x)$ pour $P\in\mathbb{K}[X]$
Mq $v=P(u)$. Soit $y\in E=E_x$, $y=Q(u)(x)$, or $v\in C(u)$ donc
$v(y)=v(Q(u)(x))=Q(u)(v(x))=Q(u)(P(u)(x))=P(u)(Q(u)(x))=P(u)(y)$

"⟸" On se donne $x\in E$ tel que $\mu_x=\mu$, et G supp. de E_x, alors $E=E_x\oplus G$ décomposition en sous espaces stables
π proj sur G, comme E_x et G sont u-stables, π et u commutent, donc par hyp, $\pi=P(u)$ pour $P\in\mathbb{K}[X]$.
Donc $P(u_{|E_x})=\pi_{|E_x}=0$ donc $\mu_{u_{|E_x}}=\mu_u$ divise P donc $\pi=P(u)=0$
▷ $G=\{0\}$ et $E_x=E$ ▷ u est cyclique.