

Pour  $n \geq \text{nil}(w)$ ,  
 $u^n = 0 \oplus w^n$   
 $x \in E, u^n(x) = w^n(x_2)$   
 Soit  $x \in F, u^n(x) = 0$   
 Soit  $x \in \ker(u^n), w^n(x_2) = 0$   
 donc  $x_2 = 0$  car  $w^n \in GL(F)$   
 donc  $x \in F$ .

Soit  $y \in \text{Im}(u^n), y = u^n(x) = w^n(x_2) \in G$   
 Soit  $y \in G, y = w^n(x_2)$   
 Soit  $x_2 \in G$  car  $w^n \in GL(F)$   
 Soit  $y = u^n(x)$ .

## nombrement des matrices nilpotentes sur $\mathbb{F}_q$

Caldère  
 CIAL.  
 p. 74

156, 190, 123, 101, 106, 104

Fitting: Soit  $u \in \mathcal{L}(E)$ ,  $\dim(E) = d$ . Alors les suites  
 $\dim \ker(u^k)$  et  $(\dim \text{Im}(u^k))_{k \in \mathbb{N}}$  sont respectivement croissante et  
 stationnaire et elles stationnent à partir d'un certain rang  $n_0$ .

En plus, on a  $E = \ker(u^{n_0}) \oplus \text{Im}(u^{n_0})$ .

Preuve: La monotonie des suites est claire, elles sont stationnaires car  $E$  est de dimension finie. De plus, elles stationnent au même rang car par la formule du rang:

$$\dim(\ker(u^k)) = \dim(\ker(u^{k+1})) \iff \dim(\text{Im}(u^k)) = \dim(\text{Im}(u^{k+1}))$$

Soit  $n_0$  le rang commun à partir duquel elles stationnent.

Par le théorème du rang:  $\dim(E) = \dim(\ker(u^{n_0})) + \dim(\text{Im}(u^{n_0}))$ .

Soit  $x \in \ker(u^{n_0}) \cap \text{Im}(u^{n_0})$ .  $\exists y \in E, x = u^{n_0}(y)$ .

$0 = u^{n_0}(x) = u^{2n_0}(y)$ . Donc  $y \in \ker(u^{2n_0}) = \ker(u^{n_0})$  donc  $x = 0$ .

Ainsi  $\ker(u^{n_0}) \cap \text{Im}(u^{n_0}) = \{0\}$  donc  $E = \ker(u^{n_0}) \oplus \text{Im}(u^{n_0})$ .

Théorème: Soit  $E$  un  $\mathbb{F}_q$ -espace vectoriel de dimension  $d$ . Il y a  $n_d = q^{d(d-1)/2}$  matrices nilpotentes de taille  $d \times d$  à coefficients dans  $\mathbb{F}_q$ .

Preuve: (i) Montrons que  $\mathcal{L}(E)$  est en bijection avec l'ensemble des décompositions de Fitting.

Soit  $u \in \mathcal{L}(E)$ . On lui associe sa décomposition de Fitting.

Soit  $((F, G), v, w)$  tel que  $E = F \oplus G$ ,  $v$  nilpotent sur  $F$ ,  $w \in GL(G)$ .

Soit  $x \in E$ ,  $\exists! (x_F, x_G) \in F \times G, x = x_F + x_G$ . Soit  $u \in \mathcal{L}(E)$  défini par:

$$u(x) = v(x_F) + w(x_G) = (v \oplus w)(x)$$

Par récurrence, on montre que:  $\forall k \in \mathbb{N}^*, u^k = v^k \oplus w^k$

Pour  $n \geq \text{nil}(v)$ ,  $u^n = 0 \oplus w^n$ . On tire de cette égalité que  $F = \ker(u^n)$  et  $G = \text{Im}(u^n)$ . Ainsi,  $((F, G), v, w)$  est la décomposition de Fitting de  $u$ .

(ii) On a  $\#X(E) = q^{d^2}$ . On pose:  $\forall k \in [0, d]$ ,  $X_k = \{(F, G) \in K^d / F \oplus G = E, \dim(F) = k\}$

$$(*) \#X(E) = \sum_{k=0}^d \#X_k m_{k,d} \quad \text{où } g_{d-k} = \#GL_{d-k}(K)$$

On note  $m_{k,d} = \#X_k$ . Montrons que  $m_{k,d} = \frac{g_d}{g_k g_{d-k}}$ .

Pour cela, introduisons l'action :

$$GL_d(K) \times X_k \rightarrow X_k \quad (\text{bien définie}).$$

$$(g, (F, G)) \mapsto (g(F), g(G))$$

Soit  $(F, G) \in X_k$  et  $(F', G') \in X_k$ . Soient  $B, B'$  des bases adaptées respectivement

$$\text{à } E = F \oplus G, \quad E = F' \oplus G'.$$

$\exists g \in GL_d(K), g(B) = B'$  donc  $g \cdot (F, G) = (F', G')$  donc l'action est transitive:  $\forall (F, G) \in X_k, \text{Orb}((F, G)) = X_k$ .

Par la relation orbite-stabilisateur,

$$\underbrace{\#GL_d(K)}_{=g_d} = \#Stab(F, G) \underbrace{\#Orb(F, G)}_{=\#X_k = m_{k,d}}$$

$(e_1, \dots, e_d)$  base canonique de  $K^d$ . On pose  $F_0 = \text{Vect}(e_1, \dots, e_k)$  et  $G_0 = \text{Vect}(e_{k+1}, \dots, e_d)$

$$(F_0, G_0) \in X_k \text{ et } Stab(F_0, G_0) = \{g \in GL_d(K) / g(F_0) = F_0, g(G_0) = G_0\}$$

$$= \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} / A \in GL_k(K), B \in GL_{d-k}(K) \right\}$$

D'où  $\#Stab(F_0, G_0) = g_k g_{d-k}$ . Ainsi,  $m_{k,d} = \frac{g_d}{g_k g_{d-k}}$

Or,  $g_d = \prod_{k=0}^{d-1} (q^d - q^k) = q^{\frac{d(d-1)}{2}} \prod_{k=0}^{d-1} (q^{d-k} - 1) \rightarrow$  factoriser par  $q^k \rightarrow q^{\sum}$

$$(iii) \quad q^{d^2} = \sum_{k=0}^d \frac{g_d}{g_k} m_{k,d} = m_{d,d} + \sum_{k=0}^{d-1} \frac{g_d}{g_k} m_{k,d} = m_{d,d} + \frac{g_d}{g_{d-1}} \underbrace{\sum_{k=0}^{d-1} \frac{g_{d-1}}{g_k} m_{k,d}}_{=q^{(d-1)^2}}$$

Donc  $m_d = q^{d^2} - \frac{g_d}{g_{d-1}} q^{(d-1)^2}$

Ainsi,  $\frac{g_d}{g_{d-1}} = q^{d-1} (q^d - 1)$  d'où  $m_d = q^{d^2} - q^{d-1} (q^d - 1) q^{(d-1)^2}$

$$m_d = q^{d^2} - q^{d^2-d} (q^d - 1)$$

$$m_d = q^{d^2-d} = q^{d(d-1)}$$

$$= q^{d-1} \frac{\prod_{k=0}^{d-1} q^{d-k-1}}{\prod_{k=0}^{d-2} q^{d-1-k-1}} = q^{d-1} \frac{\prod_{k=0}^{d-1} q^{d-k-1}}{\prod_{k=1}^{d-1} q^{d-k-1}}$$

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