Développement: nilpotents sur un corps fini

Arthur Maritch-Roy

Proposition 1. (lemme de Fitting)
Soient E un K-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Les suites $(\ker(u^k))$ et $\operatorname{Im}(u^k)$ sont respectivement croissante et décroissante à partir d'un certain rang n_0 et on a alors

$$E = \ker(u^{n_0}) \oplus \operatorname{Im}(u^{n_0}).$$

Démonstration. Les monotonies sont évidentes et elles stationnent au même rang par le théorème du rang, notons-le n_0. Soit $\ker(u^{n_0}) \cap \operatorname{Im}(u^{n_0})$ Pour $y = u^{n_0}(x)$, $u^{n_0}(y) = u^{2n_0}(x) = 0$ donc $x \in \ker(u^{n_0})$ ce qui donne exactement $y = 0$ donc la somme est directe. On conclut par égalité des dimensions. Dès lors, on voit que u restreint à $\ker(u^{n_0})$ est nilpotent et que son homologue sur $\operatorname{Im}(u^{n_0})$ est bijectif car $\operatorname{Im}(u^{n_0+1}) = \operatorname{Im}(u^{n_0})$. □

On obtient donc une décomposition dite de Fitting (F, G, v, w) où les F, G sont les espaces en question et les v, w sont les restrictions.

Proposition 2. La décomposition de Fitting d'un endomorphisme est unique.

Démonstration. Soit (F, G, v, w) une décomposition de Fitting de u avec w nilpotent. En écrivant la forme par blocs dans la décomposition adaptée, on montre que F et G sont bien les espaces que l'on a mis en évidence auparavant. Nécessairement, v et w sont les restrictions souhaitées. □

Théorème 3. Soit K fini de cardinal q. Le nombre n_d de matrices nilpotentes de $\mathcal{M}_d(K)$ est $q^{d(d-1)}$.

Démonstration. Soit X_k l'ensemble des couples (F, G) de sous-espaces de K^d tels que $\dim(F) = k$ et $F \oplus G = K^d$, soit m_k son cardinal. On a alors une action transitive de G sur X_k donnée par $g \cdot (F, G) = (g(F), g(G))$, et un stabilisateur est alors isomorphe à $\mathrm{GL}_k(K) \times \mathrm{GL}_{d-k}(K)$ d'où $m_k = \frac{g_d}{g_k g_{d-k}}$ où l'on a noté $g_i = |\mathrm{GL}_i(K)|$. La décomposition de Fitting donne alors une bijection entre $\mathcal{L}(E)$ et un couple de l'un des X_k, avec un nilpotent de $\mathcal{M}_k(K)$ et un automorphisme de $\mathrm{GL}_{n-k}(K)$, soit

$$|\mathcal{L}(E)| = \sum_{k=0}^{d} m_k \, n_k \, g_{d-k}.$$

Soit

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

d'où

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

□

Proposition 4. Le nombre de matrices diagonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$ est

$$\sum_{n_1 + \ldots + n_q = n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)| \cdots |\mathrm{GL}_{n_q}(\mathbb{F}_q)|}.$$

Démonstration. Soit $A \in \mathcal{M}_n(\mathbb{F}_q)$. Alors A est diagonalisable si et seulement si

$$A = \bigoplus_{i=1}^{q} \ker(A - \zeta_i I_n),$$

où $\{\zeta_i\}$ est une énumération de $\mathbb{F}_q$. Soit alors $(n_1, \ldots, n_q)$ fixé tel que $n_1 + \cdots + n_q = n$. On va chercher à compter le nombre de diagonalisables $u \in \mathcal{L}(\mathbb{F}_q)$ tels que $\ker(u - \zeta_i \mathrm{id}) = n_i$ pour tout i. Ce nombre correspond au nombre de décompositions en sous-espaces $E = \bigoplus_{i=1}^{q} F_i$ telles que $\dim(F_i) = n_i$. En effet, si on note $\mathcal{E}_{(n_i)}$ l'ensemble de telles décompositions, on construit une bijection par

$$u \mapsto (\ker(u - \zeta_i \mathrm{id}))_i, (F_i) \mapsto \sum_{i=1}^{q} \zeta_i \mathrm{id}_{F_i}.$$

Dénombrons-donc $\mathcal{E}_{(n_i)}$. Pour cela, on considère l'action de groupes :

$$(u, (F_i)) \mapsto (u(F_i)).$$

C'est bien une action de groupes, qui est transitive. On n'a donc qu'une seule orbite, égale à $\mathcal{E}_{(n_i)}$. Pour conclure, il nous faut le cardinal du stabilisateur, qui est isomorphe au produit $(\mathrm{GL}_{n_1}(\mathbb{F}_q) \times \cdots \times \mathrm{GL}_{n_q}(\mathbb{F}_q))$. □

Proposition 5. Le nombre de matrices trigonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$ est

$$\sum_{n_1 + \ldots + n_q = n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)| \cdots |\mathrm{GL}_{n_q}(\mathbb{F}_q)|} \prod_{i=1}^{q} q^{n_i(n_i - 1)}.$$

Démonstration. On considère toujours $\mathcal{E}_{(n_i)}$ l'ensemble des décompositions en somme directe, et la bijection est alors cette fois-ci :

$$u \mapsto (\ker(u - \zeta_i \mathrm{id})^{m_i})_i, (u - \zeta_1 \mathrm{id}_{n_1}, \ldots, u - \zeta_q \mathrm{id}_{n_q})_i \text{ ou } ((w_i), (F_i))_i \mapsto \sum_i (\zeta_i \mathrm{id}_{F_i} + w_i).$$

□