Cardinal du cône nilpotent sur $\mathbb{F}_q$.

Leçons : 190, (103, 150)

Réf : H2G2 Tome 2 p 213.

Théorème : Pour tout corps fini $\mathbb{F}_q$ à q éléments et $n \geq 1$, on note $\mathcal{N}_n(\mathbb{F}_q)$ le cône des matrices nilpotentes de taille $n \times n$ sur le corps $\mathbb{F}_q$. Alors $|\mathcal{N}_n(\mathbb{F}_q)| = q^{n(n-1)}$

Dém : On se donne E un espace vectoriel de dimension n pour pouvoir identifier $\mathcal{N}_n = \mathcal{N}_n(\mathbb{F}_q)$ aux endomorphismes nilpotents de E.

$E = \mathbb{F}_q^n$.

Prop : Soient $N \in \mathcal{N}_n$ et $x \in E \setminus \{0\}$. Soit r maximal tel que la famille $(x, Nx, \dots, N^{r-1}x)$ soit libre. Alors $N^r x = 0$.

Dém : Comme $x \neq 0$, on a $r \geq 1$. Soit u l'endomorphisme de E associé à N et notons F le sous-espace de E engendré par x et u i.e $F = \langle u^s(x),\ s \in \mathbb{N} \rangle$. Par hypothèse, $(x, u(x), \dots, u^{r-1}(x))$ est une base de F : il suffit de montrer qu'elle est génératrice : il n'y a qu'à voir que pour $s \geq r$, $u^s(x) \in F$. En effet par hypothèse, la famille $(x, \dots, u^{r-1}(x), u^r(x))$ est liée donc $u^r(x) \in F$ et donc cela se propage par récurrence. Posons $u^r(x) = \sum_{i=0}^{r-1} a_i u^i(x)$.
Ainsi F est stable par u et si on note u_F l'endomorphisme induit par u sur F, alors dans la base $(x, u(x), \dots, u^{r-1}(x))$ on a

$$\mathrm{Mat}(u_F) = \begin{pmatrix} 0 & & & a_0 \\ 1 & 0 & & \vdots \\ & \ddots & \ddots & \vdots \\ & & 1 \ 0 & \\ & & 1 & a_{r-1} \end{pmatrix}.$$

D'une part c'est la matrice compagnon de $P = X^r - \sum_{i=0}^{r-1} a_i X^i$ dont le polynôme caractéristique est P lui-même.
D'autre part u_F est encore nilpotent donc son polynôme caractéristique est X^r. Ainsi par identification des coeff., $a_0 = \dots = a_{r-1} = 0$ et donc $N^r x = 0$. $\blacksquare$

Soit désormais $L_{r,n}$ l'ensemble des familles libres de $\mathbb{F}_q^n$ à r éléments.
Posons $\nu_n = |\mathcal{N}_n(\mathbb{F}_q)|$ et déterminons une relation de récurrence vérifiée par ν_n. Pour cela, on calcule de deux manières différentes le cardinal de :

$$\widetilde{\mathcal{N}}_n = \left\{ (N, \underline{x}) : N \in \mathcal{N}_n,\ \exists r \in \{1, \dots, n\} \text{ tq } \underline{x} \in L_{r,n} \text{ et } \underbrace{N \text{ respecte } \underline{x}} \right\}$$

i.e $N x_s = x_{s+1}$ avec la convention $x_{r+1} = 0$.

$$\subset \mathcal{N}_n(\mathbb{F}_q) \times \bigcup_{r=1}^{n} L_{r,n}.$$

Notons π_i la projection sur la $i^{\text{ème}}$ composante

- Un élément de $\pi_1^{-1}(N)$ est entièrement déterminé par un vecteur non nul x_1 de $\mathbb{F}_q^n$ puisqu'il s'écrit alors $(N, (x_1, Nx_1, \dots, N^{r-1}x_1))$ pour un $r \geq 1$ convenable. D'après le lemme, cela donne $q^n - 1$ possibilités. Ainsi :

$$|\widetilde{\mathcal{N}}_n| = \sum_{N \in \mathcal{N}_n} |\pi_1^{-1}(N)| = \nu_n (q^n - 1).$$

- Par ailleurs, on a $|\widetilde{\mathcal{N}}_n| = \displaystyle\sum_{r=1}^{n} \sum_{\underline{x} \in L_{r,n}} |\pi_2^{-1}(\underline{x})|$.

Pour $1 \leq s \leq n$, on note $g_s = |GL_s(\mathbb{F}_q)|$.

action par image directe. $\Big\{$ L'action naturelle de $GL_n(\mathbb{F}_q)$ sur $L_{r,n}$ est transitive d'après le théorème de la base incomplète.

il suffit donc de regarder le stabilisateur !

Soit $\underline{x} \in L_{r,n}$ qu'on complète en une base $\tilde{\underline{x}}$ de $\mathbb{F}_q^n$. Dans cette base, le stabilisateur n'est autre que

$$\left\{ \begin{pmatrix} I_r & M \\ 0 & B \end{pmatrix} : M \in \mathcal{M}_{r,n-r}(\mathbb{F}_q),\ \underbrace{B \in GL_{n-r}(\mathbb{F}_q)}_{\text{pour rester inversible.}} \right\}$$

qui est de cardinal $|GL_{n-r}(\mathbb{F}_q)| \cdot |\mathcal{M}_{r,n-r}(\mathbb{F}_q)| = g_{n-r}\, q^{r(n-r)}$.
Ainsi $|L_{r,n}| = \dfrac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}|} = \dfrac{g_n}{g_{n-r}\, q^{r(n-r)}}.$

Par ailleurs, un endomorphisme nilpotent u respecte $\underline{x}$ si et seulement si dans une base $\tilde{\underline{x}}$ on a :

$$\mathrm{Mat}_{\tilde{\underline{x}}}(u) = \begin{pmatrix} \begin{matrix} 0 & & 0 \\ 1 & \ddots & \vdots \\ & 1 & 0 \end{matrix} & \tilde{M} \\ 0 & \tilde{B} \end{pmatrix} = \begin{pmatrix} J_r & \tilde{M} \\ 0 & \tilde{B} \end{pmatrix}$$

où J_r est le bloc de Jordan de taille r (car u respecte $\underline{x}$), $\tilde{M}$ vit dans $\mathcal{M}_{r,n-r}(\mathbb{F}_q)$ et $\tilde{B}$ est nilpotente de taille $n-r$ (car u est nilpotent)

Donc $|\pi_2^{-1}(\underline{x})| = q^{r(n-r)} \nu_{n-r}$.

$$\text{Donc } |\tilde{\mathcal{N}}_n| = \sum_{r=1}^{n} \frac{g_n}{g_{n-r}\, q^{r(n-r)}}\, q^{r(n-r)}\, \nu_{n-r}$$

· On a donc $\dfrac{\nu_n}{g_n}(q^n-1) = \displaystyle\sum_{r=1}^{n} \frac{\nu_{n-r}}{g_{n-r}}$ donc avec $m_s = \dfrac{\nu_s}{g_s}$:

$$m_n(q^n-1) = \sum_{r=0}^{n-1} m_r = m_{n-1} + \underbrace{\sum_{r=0}^{n-2} m_r}_{m_{n-1}(q^{n-1}-1)}$$

$$= q^{n-1} m_{n-1}$$

Par récurrence, on obtient :

$$\frac{\nu_n}{g_n} = m_n = \frac{q^{n-1}\cdots q^1}{\prod_{r=1}^{n}(q^r-1)} \underbrace{m_1}_{=1} = \frac{q^{n(n-1)/2}}{\prod_{r=1}^{n}(q^r-1)} = \frac{q^{n(n-1)}}{g_n}$$

d'où $\nu_n = |\mathcal{N}_n(\mathbb{F}_q)| = q^{n(n-1)}$. $\square$

Rappel : $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$
$= (q^n-1)(q^{n-1}-1)\cdots(q-1)\, q^{n(n-1)/2}$.

C'est le nombre de bases de $\mathbb{F}_q^n$: voir NH2G2 Tome 2 p 41.

Bonus

Heuristique...

$N_n(\mathbb{F}_q)$ = matrices nilpotentes maximales sur $\mathbb{F}_q$

$= \{ M \in \mathcal{N}_n(\mathbb{F}_q) : M^{n-1} \neq 0 \}$. ouvert dense de $\mathcal{N}_n(\mathbb{F}_q)$

$$J_n = \begin{pmatrix} 0 & & & \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix} \in N_n(\mathbb{F}_q)$$ et en fait, soit par Jordan nilpotent, soit en le faisant à la main, $N_n(\mathbb{F}_q) = \omega(J_n)$.

Donc $$|N_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}(J_n)|}$$

avec $\mathrm{Stab}(J_n) = \{ P \in GL_n(\mathbb{F}_q) : PJ_n = J_n P \}$

$= C(J_n)$

$= \mathbb{F}_q[J_n]^*$

$$= \left\{ \begin{pmatrix} a_0 & & & 0 \\ a_1 & \ddots & & \\ \vdots & \ddots & \ddots & \\ a_{n-1} & \cdots & a_1 & a_0 \end{pmatrix} : a_i \in \mathbb{F}_q,\ \underbrace{a_0 \neq 0}_{\text{pour être inversible}} \right\}$$

Donc $|\mathrm{Stab}(J_n)| = (q-1)q^{n-1}$

Donc $$|N_n(\mathbb{F}_q)| \underset{q \to \infty}{\sim} \frac{q^{n^2}}{q^n} = q^{n(n-1)}.$$

Donc ? : Quand q est grand, la proba de tomber dans l'orbite du bloc de Jordan indécomposable J_n lorsqu'on tire une matrice nilpotente de $\mathcal{M}_n(\mathbb{F}_q)$ tend vers 1.

Est-ce étonnant ? Tomber exactement sur une puissance de q laisse penser que le cône serait un (sous-)espace vectoriel, ce qui n'est clairement pas le cas. Donc oui c'est un peu étonnant mais bref... (lissité rationnelle....)