Développement. Cardinal du cône nilpotent sur un corps fini

Soit $n \in \mathbf{N}^*$ un entier. Pour un corps $\mathbf{K}$, on considère l'ensemble $\mathrm{Nil}_n(\mathbf{K})$ des matrices nilpotentes de taille n à coefficients dans $\mathbf{K}$.

Lemme 1. Soit E un $\mathbf{K}$-espace vectoriel de dimension n. Soient $N \in \mathscr{L}(E)$ un endomorphisme nilpotent et $e \in E \setminus \{0\}$ un vecteur non nul. Soit $r \in \mathbf{N}^*$ l'entier maximal tel que la famille $\mathscr{E} := (e, N(e), \dots, N^{r-1}(e))$ soit libre. Alors $N^r(e) = 0$.

Preuve On considère le sous-espace vectoriel $F := \mathrm{Vect}\{N^s e\}_{s\in\mathbf{N}}$. Montrons que la famille $\mathscr{E}$ en est une base. Sa liberté étant une définition, il suffit de montrer qu'elle le génère. Soit $s \in \mathbf{N}$. On veut montrer que $N^s(e) \in \mathrm{Vect}\,\mathscr{E}$. Si $s < r$, il n'y a rien à faire. En effectuant ensuite une récurrence, il suffit de montrer que $N^r(e) \in \mathrm{Vect}\,\mathscr{E}$. Par définition, la famille $(e, N(e), \dots, N^r(e))$ n'est pas libre, donc il existe des scalaires $\lambda_0, \dots, \lambda_r \in \mathbf{K}$ non tous nuls tels que

$$\lambda_0 e + \lambda_1 N(e) + \dots + \lambda_r N^r(e) = 0.$$

Comme la famille $\mathscr{E}$ est libre, le scalaire λ_r ne peut être nul et on en déduit

$$N^r(e) = -\frac{1}{\lambda_r}[\lambda_0 e + \lambda_1 N(e) + \dots + \lambda_{r-1} N^{r-1}(e)] \in \mathrm{Vect}\,\mathscr{E}. \tag{1}$$

Ceci conclut que la famille $\mathscr{E}$ est une base du sous-espace vectoriel F.

L'endomorphisme N stabilisant le sous-espace vectoriel F, notons N_F l'endomorphisme induit. Avec l'égalité (1), sa matrice dans $\mathscr{E}$ est la matrice compagnon du polynôme

$$P := X^n + \sum_{i=0}^{r-1} \frac{\lambda_i}{\lambda_r} X^i \in \mathbf{K}[X],$$

donc son polynôme caractéristique est ce polynôme P. L'endomorphisme N_F étant nilpotent, les scalaires λ_i/λ_r avec $i \in [\![0, r-1]\!]$ sont tous nuls ce qui donne $N^r(e) = 0$. ◁

Théorème 2. Soit $\mathbf{F}_q$ le corps fini à q éléments. Alors $|\mathrm{Nil}_n(\mathbf{F}_q)| = q^{n(n-1)}$.

Preuve Soit $r \in [\![1, n]\!]$. On note $\mathfrak{L}_{r,n}$ l'ensemble des familles libres de $\mathbf{F}_q^n$ à r éléments. On dit qu'une matrice $N \in \mathrm{Nil}_n(\mathbf{F}_q)$ *respecte* une famille $\mathscr{E} := (e_1, \dots, e_r) \in \mathfrak{L}_{r,n}$, noté $N \vdash \mathscr{E}$, si

$$Ne_s = e_{s+1} \quad \text{et} \quad Ne_r = 0, \quad s \in [\![1, r-1]\!].$$

On définit $k_n := |\mathrm{Nil}_n(\mathbf{F}_q)|$. Déterminons une formule de récurrence vérifiée par la suite $(k_n)_{n\in\mathbf{N}^*}$ en calculant, de deux manières différentes, le cardinal de l'ensemble

$$\widetilde{\mathrm{Nil}}_n(\mathbf{F}_q) := \{(N, \mathscr{E}) \in \mathrm{Nil}_n(\mathbf{F}_q) \times \bigsqcup_{r=1}^{n} \mathfrak{L}_{r,n} \mid N \vdash \mathscr{E}\}.$$

• *Premier dénombrement.* Par définition du respect, d'après le lemme, pour une matrice $N \in \mathrm{Nil}_n(\mathbf{F}_q)$, un élément $(N, \mathscr{E}) \in \widetilde{\mathrm{Nil}}_n(\mathbf{F}_q)$ est uniquement déterminé par un élément non nul $e \in E \setminus \{0\}$. On en déduit

$$|\widetilde{\mathrm{Nil}}_n(\mathbf{F}_q)| = k_n \times |E \setminus \{0\}| = k_n(q^n - 1). \tag{2}$$

• *Second dénombrement.* Fixons un entier $r \in [\![1, n]\!]$ et posons

$$g_r := \mathrm{GL}_r(\mathbf{F}_q) = (q^r - 1)(q^r - q) \cdots (q^r - q^{r-1}) = q^{r(r-1)/2}(q^r - 1) \cdots (q - 1).$$

Soit $\mathscr{E} \in \mathfrak{L}_{r,n}$. On complète la famille libre $\mathscr{E}$ est une base $\tilde{\mathscr{E}}$ de E. De plus, le stabilisateur de $\mathscr{E}$ dans cette base est constitué des matrices de la forme

$$\begin{pmatrix} I_r & M \\ 0 & B \end{pmatrix} \quad \text{avec} \quad M \in \mathscr{M}_{r,n-r}(\mathbf{F}_q) \quad \text{et} \quad B \in \mathrm{GL}_{n-r}(\mathbf{F}_q).$$

Avec la transitivité de l'action du groupe $G := \mathrm{GL}_n(\mathbf{F}_q)$ sur $\mathfrak{L}_{r,n}$, on en déduit que

$$|\mathfrak{L}_{r,n}| = |\mathrm{Orb}_G(\mathscr{E})| = \frac{|G|}{|\mathrm{Stab}_G(\mathscr{E})|} = \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathrm{GL}_{n-r}(\mathbf{F}_q)| \times |\mathscr{M}_{r,n-r}(\mathbf{F}_q)|} = \frac{g_n}{g_{n-r} q^{r(n-r)}}.$$

Par ailleurs, une matrice $N \in \mathrm{Nil}_n(\mathbf{F}_q)$ respecte la famille $\mathscr{E}$ si et seulement si sa matrice est de la forme

$$\mathrm{Mat}_{\tilde{\mathscr{E}}}(N) = \begin{pmatrix} J_r & M \\ 0 & N \end{pmatrix} \quad \text{avec} \quad M \in \mathscr{M}_{r,n-r}(\mathbf{F}_q) \quad \text{et} \quad N \in \mathrm{Nil}_{n-r}(\mathbf{F}_q).$$

où la matrice $J_r \in \mathscr{M}_r(\mathbf{F}_q)$ est celle contenant des 1 sur sa sous-diagonale. D'où

$$|\widetilde{\mathrm{Nil}}_n(\mathbf{F}_q)| = \sum_{r=1}^{n} |\mathfrak{L}_{r,n}| \times q^{r(n-r)} k_{n-r} = \sum_{r=1}^{n} \frac{g_n}{g_{n-r}} k_{n-r}. \tag{3}$$

• *Conclusion.* En combinant les calculs (2) et (3), en posant $m_n := k_n/g_n$ pour tout entier $n \geqslant 1$, on trouve

$$(q^n - 1)m_n = m_0 + \dots + m_{n-1}, \quad n \geqslant 1.$$

On obtient alors la relation

$$(q^n - 1)m_n = m_{n-1} + (q^{n-1} - 1)m_{n-1} = q^{n-1} m_{n-1}, \quad n \geqslant 2.$$

Une récurrence immédiate donne alors

$$m_n = \frac{q^{n(n-1)/2}}{(q^n - 1) \cdots (q - 1)} = \frac{q^{n(n-1)}}{g_n}, \quad n \geqslant 1.$$

D'où $k_n = q^{n(n-1)}$ pour tout entier $n \in \mathbf{N}$. ◁

[1] Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries*. T. Tome second. Calvage & Mounet, 2015.