Cardinal du cône nilpotent

Julie Parreaux

2018-2019

Référence du développement : H2G2 [1, p.213]

Leçons où on présente le développement : 101 (Action de groupe) ; 104 (Groupe fini) ; 106 (Groupe linéaire) ; 157 (Triangulaire et nilpotent).

1 Introduction

Le cône nilpotent des matrices $d \times d$ nilpotentes (c'est bien un cône par sa stabilité par la multiplication et son instabilité par addition), noté $\mathcal{N}_d = \mathcal{N}_d(K)$, sur un corps K est un objet convoité en géométrie algébrique, en théorie de Lie ou encore en théorie des représentations.

Par un calcul heuristique, via l'orbite du bloc de Jordan de $\mathcal{N}_d(q)$ construite par l'action de $GL_n(\mathbb{F}_q)$ sur $\mathcal{N}_d(\mathbb{F}_q)$ par conjugaison, on obtient que $\left|\mathcal{N}_d(\mathbb{F}_q)\right| = q^{d^2-d}$. Cette valeur est la valeur exacte du cardinal du cône et cette justesse d'estimation s'explique par le fait que $\mathcal{N}_d(\mathbb{F}_q)$ est une variété algébrique.

L'idée la plus naturelle pour calculer $\left|\mathcal{N}_d(\mathbb{F}_q)\right|$ est de partitionner $\mathcal{N}_d(\mathbb{F}_q)$ selon les orbites de l'action de $GL_n(\mathbb{F}_q)$ par conjugaison sur $\mathcal{N}_d(\mathbb{F}_q)$. On pourra ainsi sommer les classes de similitude. Cependant, ce calcul est fastidieux et la somme ne se simplifie pas facilement. La méthode que nous choisissons d'appliquer est inspirée de la désingularisation de Springer.

2 Calcul du cardinal du cône nilpotent sur $\mathbb{F}_q$

Schéma du développement (leçons 101 et 157)

1. Énoncer le théorème et la proposition que nous admettons.
2. Premier calcul via la première composante : $|X| = n_d(q^d - 1)$.
3. Deuxième calcul via la deuxième composante : $|X| = \sum_{r=1}^{d} \frac{g_d}{g_{d-r}} n_{d-r}$.
4. Comparaison des deux calculs.

Schéma du développement (leçons 104 et 106)

— Proposition : famille libre induite par N
   1. $\mathcal{E} = \left(e, Ne, \dots, N^{r-1}e\right)$ est une base de $F = \langle N^s e, s \in \mathbb{N} \rangle$.
   2. $N^r e = 0$ (prendre une restriction qui stabilise F).

— Théorème : cardinal du cône (à écrire au début, avant même l'énoncer de la proposition)
   1. Premier calcul via la première composante : $|X| = n_d(q^d - 1)$.
   2. Deuxième calcul via la deuxième composante : $|X| = \sum_{r=1}^{d} \frac{g_d}{g_{d-r}} n_{d-r}$ (calculs rapides).
   3. Comparaison des deux calculs (calculs rapides).

Proposition. *Soient E un K-espace vectoriel où K est un corps et $N \in \mathcal{N}_d(E)$ et e un vecteur non nul de E. On note r le nombre maximal tel que $\mathcal{E} = \left(e, Ne, \dots, N^{r-1}e\right)$ est une famille libre. On a alors, $N^r e = 0$.*

Démonstration. Soit $F = \langle N^s e, s \in \mathbb{N} \rangle$ le sous-espace vectoriel engendré par e et N.

Étape 1 : Montrons que $\mathcal{E}$ est une base F

— $\mathcal{E}$ est une famille libre dans F (par construction sinon problème avec la définition de r).

— $\mathcal{E}$ est une famille génératrice dans F. Montrons par récurrence sur $k \in \mathbb{N}$ que $N^{r+k}e \in \text{Vect}(\mathcal{E})$. (On a besoin de la récurrence car la définition nous assure de la suite des itérés jusqu'à $N^r e$ est liée (et libre juste avant) mais ne dit rien sur la famille des itérés jusqu' $N^{r-1}e$ à laquelle on ajoute une itérée quelconque.)

Cas $k = 0$ Comme la famille $\left(e, Ne, \dots, N^{r-1}e, N^r e\right)$ est liée (sinon contradiction avec la définition de r), on peut écrire $N^r e = -\sum_{i=0}^{r-1} a_i N^i e$ pour $a_0, \dots, a_{r-1}$ non tous nuls (le caractère liant de la famille impose $a_r \neq 0$ (on peut donc le supposer égal à 1) car sinon on contredirait la liberté de la famille $\mathcal{E}$).

Cas $k \in \mathbb{N}$ Soit $k \in \mathbb{N}$ tel que pour tout $j < k$, $N^{r+j} \in \text{Vect}(\mathcal{E})$, montrons que $N^{r+k} \in \text{Vect}(\mathcal{E})$. Notons $s = r + k$, on a alors

$$\begin{array}{rcll} N^s e & = & N^{k+r}e & (s = k + r) \\ & = & N^k N^r e & \text{(par manipulation des puissances)} \\ & = & N^k \left(-\sum_{i=0}^{r-1} a_i N^i e\right) & \text{(par le cas } k = 0) \\ & = & -\sum_{i=0}^{r-1} a_i N^k N^i e & \text{(par linéairité de } N) \\ & = & -\sum_{i=0}^{r-1} a_i N^{k+i} e & \text{(par manipulation des puissances)} \\ & \in & \text{Vect}(\mathcal{E}) & \text{(par hypothèse de récurrence forte)} \end{array}$$

Étape 2 : Montrons que $N^r e = 0$

— N stabilise F : soit $x \in F$, alors $Nx = NN^s e = N^{s+1}e \in F$ pour un certain s. On note $\tilde{N} = N_F$ l'endomorphisme induit par la restriction de N à F.

— Expression de la matrice de $\tilde{N}$ dans la base $\mathcal{E}$:

$$\text{Mat}_{\mathcal{E}}\left(\tilde{N}\right) = \begin{pmatrix} 0 & \cdots & \cdots & 0 & a_0 \\ 1 & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & a_{r-1} \end{pmatrix}$$

— $\tilde{N}(e) = Ne$

— $\forall s \in [\![0, r-2]\!]$, $\tilde{N}\left(N^s e\right) = N^s Ne = N^{s+1}e$

— $\tilde{N}\left(N^{r-1}e\right) = N^r e = -\sum_{i=0}^{r-1} a_i N^i e$

On reconnaît une matrice compagnon du polynôme $P = X^r + \sum_{i=0}^{r-1} a_i X^i$ de polynôme caractéristique (qui est également minimal) P.

— Comme $\tilde{N}^r e = N^r e$ (car restriction sur F de N) et $\tilde{N}^r = 0$ (car $\tilde{N}$ est nilpotente d'indice r, donné par son polynôme caractéristique), $N^r = 0$.

□

Théorème. *Pour tout corps fini $\mathbb{F}_q$ de cardinal q et tout entier d, on a $\left|\mathcal{N}_d(\mathbb{F}_q)\right| = q^{d(d-1)}$.*

Démonstration. Soit E un $\mathbb{F}_q$-espace vectoriel de dimension d, on pose $\mathcal{N}_d = \mathcal{N}_d(\mathbb{F}_q)$ l'ensemble des matrices nilpotentes de E. Soit $L_{r,d}$ l'ensemble des parties libres de E à r éléments. On dit que N respecte une famille $\mathcal{E} = (e_1, \dots, e_r)$ de $L_{r,d}$ si $\forall s \in [\![1, r]\!]$, $Ne_s = e_{s+1}$ et $N_{r+1} = 0$.

Posons $n_d = |\mathcal{N}_d|$ et donnons une formule de récurrence pour exprimer n_d. On calcul alors de deux manières différentes le cardinal de l'ensemble $\{(N, e) \mid N \in \mathcal{N}_d, \exists r \in \{1, \dots, d\}$ tel que r respecte $\mathcal{E}\}$. On note π_1 (respectivement π_2) la projection sur la première (respectivement la seconde) composante.

Premier calcul :

— $|X| = \sum_{N \in \mathcal{N}_d} \left|\pi_1^{-1}(N)\right|$ (en partitionnant $\mathcal{N}_d$ en fonction des valeurs de e dans X : $|X = \{r, b\}| = \sum_{N \in \mathcal{N}_d} \left|\pi_1^{-1}(a, b)\right|$).

— $|X| = n_d(q^d - 1)$ (la proposition nous assure l'existence d'une bijection entre $E \setminus \{0\}$ et les familles libres respectée par N).

Deuxième calcul : Par construction de l'ensemble X, on a :

$$|X| = \underbrace{\sum_{r=1}^{d}}_{\text{test l'ensemble des } r} \quad \underbrace{\sum_{e \in L_{r,d}}}_{\text{condition : } e \in X} \left|\pi_2^{-1}(e)\right|$$

On cherche à simplifier cette somme.

— Soit $1 \leq r \leq d$, notons g_r l'ordre de $GL_r(\mathbb{F}_q)$. L'action de $GL(E)$ sur $L_{r,d}$ est transitive par le théorème de la base incomplète.

  — $\mathcal{E}$ peut être complété en une base de E.

  — $\forall \mathcal{E}, \mathcal{E}' \in L_{r,d}, \exists g \in GL(E)\ g.\mathcal{E} = \mathcal{E}'$ (on complète $\mathcal{E}$ en une base, un changement de base nous donne $\mathcal{E}'$ complété en une base).

  Donc $|\text{Orb}(\mathcal{E})| = \left|L_{r,d}\right|$.

— Soit $\mathcal{E} \in L_{r,d}$ et $\tilde{\mathcal{E}}$ sa base complété de $\mathcal{E}$. On raisonne maintenant sur cette base. On a $\text{Stab}(\mathcal{E}) = \{\begin{pmatrix} I_r & M \\ 0 & B \end{pmatrix} \mid M \in \mathcal{M}_{r,d-r}(\mathbb{F}_q), B \in GL_{d-r}(\mathbb{F}_q)\}$ par définition du stabilisateur. Par la relation d'orbite stabilisateur, $\left|L_{r,d}\right| = \frac{|GL(E)|}{|\text{Stab}(\mathcal{E})|} = \frac{g_d}{g_{d-r} q^{r(d-r)}}$ car g_d est l'ordre de $GL(E)$, g_{d-r} celui de $GL_{d-r}(\mathbb{F}_q)$ et $q^{r(d-r)}$ celui de $\mathcal{M}_{r,d-r}(\mathbb{F}_q)$.

— Une matrice nilpotente N respecte $\mathcal{E}$ si et seulement si la matrice de l'application linéaire associée à N dans une base $\tilde{\mathcal{E}}$ est de la forme $\text{Mat}_{\tilde{\mathcal{E}}} = \begin{pmatrix} J_r & M \\ 0 & N_{d-r} \end{pmatrix}$ où J_r est le bloc de Jordan de taille $n \times r$, $M \in \mathcal{M}_{r,d-r}(\mathbb{F}_q)$ et $N_{d-r} \in \mathcal{N}_{d-r}(\mathbb{F}_q)$ (la préservation provient du bloc de Jordan de taille r).

On a alors $|X| = \sum_{r=1}^{d} \left|L_{r,d}\right| q^{r(d-r)} n_{d-r}$ (car $|\pi - 1_2(\mathcal{E})| = \underbrace{q^{r(d-r)}}_{|\mathcal{M}_{r,d-r}|} \underbrace{n_{d-r}}_{|\mathcal{N}_{r,d-r}|}$). D'où en remplaçant par la valeur de $\left|L_{r,d}\right|$, $|X| = \sum_{r=1}^{d} \frac{g_d}{g_{d-r}} n_{d-r}$.

Comparaison des deux calculs On a alors $n_d(q^d - 1) = \sum_{r=1}^{d} \frac{g_d}{g_{d-r}} n_{d-r}$. Donc en divisant par $g_d > 0$, on obtient

$$\begin{aligned}
\frac{n_d}{g_d}(q^d - 1) &= \sum_{r=1}^{d} \frac{n_{d-r}}{d_{d-r}} && \text{(divsion)} \\
&= \sum_{r=0}^{d-1} \frac{n_r}{d_r} && \text{(changement d'indice dans la somme)} \\
&= \frac{n_{d-1}}{d_{d-1}} + \sum_{r=0}^{d-2} \frac{n_r}{d_r} && \text{(on sort le dernier terme)} \\
&= \frac{n_{d-1}}{d_{d-1}} + \frac{n_{d-1}}{d_{d-1}}(q^{d-1} - 1) && \text{(récurrence sur la formule)} \\
&= \frac{n_{d-1}}{d_{d-1}}(q^{d-1}) && \text{(factorisation)}
\end{aligned}$$

On en déduit que $\frac{n_d}{g_d} = \frac{q^{d(d-1)/2}}{\prod_{r=1}^{d}(q^r - 1)}$ (par résolution de la récurrence). Puis, $\frac{n_d}{g_d} = \frac{q^{d(d-1)}}{g_d}$ (car $g_d = \prod_{r=1}^{d}(q^r - 1) q^{d(d-1)/2}$, on compte le nombre de possibles). Finalement, $n_d = q^{d(d-1)}$. □

3 Compléments autours de ce développement

Cardinal des ensembles de matrices dans des espaces vectoriels sur corps finis

Nous donnons ici une batterie de cardinaux [2, p.57] liés au groupe linéaire $GL_n(\mathbb{F}_q)$. On note l'entier n quantique $[n]_q = 1 + \cdots + q^{n-1}$ que l'on peut considérer comme une q-déformation du nombre n : si $q = 1$, on retrouve n.

On définit de même le factoriel et le coefficient binomial quantique. Pour $m_1, \ldots, m_k$ dans $\mathbb{N}$ tels que $m_1 + \cdots + m_k = n$, on définit le nombre multinomial quantique :

$$[n]_q! = [n]_q[n-1]_q \ldots [1]_q \qquad [0]_q! = 1 \qquad \begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{[n_q]!}{[m]_q![n-m]_q!} \qquad \begin{bmatrix} n \\ m_1 \ldots m_k \end{bmatrix}_q = \frac{[n]_q!}{\prod_{i=1}^k [m_i]_q!}$$

Lemme (Espace et sous-espace). *Soit $n, q \in \mathbb{N}$.*

1. *L'espace vectoriel :* $|E| = |\mathbb{F}_q^n| = q^n$
2. *L'espace projectif :* $|\mathbb{P}(E)| = [n]_q$
3. *Grassmannienne :* $|Gr_{m,n}(\mathbb{F}_q)| = \begin{bmatrix} n \\ m \end{bmatrix}_q$

Démonstration.
1. Existence d'une base.
2. On fait agir le groupe multiplicatif $\mathbb{K}^*$ sur $\mathbb{K}^{n+1} \setminus \{0\}$ par homothéties ($\lambda \in \mathbb{K}^*$ agit sur v par $\lambda.v = \lambda v$). L'action est libre : $\forall v \neq 0, Stab_{\mathbb{K}^*}(v) = \{1\}$. On en déduit que : $|\mathbb{P}^n(\mathbb{F}_q)| = \frac{|\mathbb{F}_{n+1_q} \setminus \{0\}|}{|\mathbb{F}_q^*|} = \frac{q^{n+1}-1}{q-1} = 1 + q + \cdots + q^n$.
3. $GL_n(\mathbb{K})$ agit transitivement sur la grassmannienne $Gr_{m,n}(\mathbb{K})$. Le stabilisateur d'un sous-espace F est donné par $Stab(F) = (GL_m(\mathbb{K}) \times GL_{n-m}(\mathbb{K}) \ltimes \mathcal{M}_{m,n-m}(\mathbb{K})$.

□

Lemme (Groupes et sous-groupes). *Soit $n, q \in \mathbb{N}$.*

1. *Groupe linéaire :* $|GL_n(\mathbb{F}_q)| = g_n = q^{\frac{n(n-1)}{2}}(q-1)^n[n]_q!$
2. *Groupe spécial linéaire :* $|SL_n(\mathbb{F}_q)| = \frac{g_n}{q-1} = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$
3. *Groupe projectif :* $|PGL_n(\mathbb{F}_q)| = \frac{g_n}{q-1} = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$
4. *Groupe spécial projectif :* $|PSL_n(\mathbb{F}_q)| = \frac{g_n}{(q-1)d} = \frac{1}{d}q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$ *avec* $d = \gcd(q-1, n)$
5. *Groupe orthogonal impair : si ch* $\neq 2$, $|O_{2n+1}(\mathbb{F}_q)| = 2q^n \prod_{k=0}^{n-1}\left(q^{2n} - q^{2k}\right) = 2q^{n^2}(q^2-1)^n[n]_{q^2}!$
6. *Groupe orthogonal pair :*
$|O_{2n}(\mathbb{F}_q)| = 2\left(q^n - (-1)^{\frac{n(q-1)}{2}}\right)\prod_{k=0}^{n-1}\left(q^{2n} - q^{2k}\right) = 2q^{n(n-1)}\left(q^n - (-1)^{\frac{n(q-1)}{2}}\right)(q^2-1)^{n-1}[n]_{q^2}!$
7. *Groupe symplectique :* $|Sp_{2n}(\mathbb{F}_q)| = q^{n^2}\prod_{k=1}^{n}(q^{2k}-1) = q^{n^2}(q^2-1)^n[n]_{q^2}!$

Démonstration.
1. Deux démonstrations.
   — On fait agir transitivement $GL_n(\mathbb{K})$ sur $\mathbb{K}^n \setminus \{0\}$. On a $Stab(e_1) \simeq GL_{n-1}(\mathbb{K}) \ltimes \mathbb{K}^{n-1}$. On en déduit que $|GL_n(\mathbb{F}_q)| = |GL_{n-1}(\mathbb{F}_q)|q^{n-1}(q^n-1)$. On conclut par récurrence.
   — On compte le nombre de bases de l'espace $\mathbb{F}_q^n$. Pour cela, on fait agir simplement transitivement $Gl_n(\mathbb{F}_q)$ sur l'ensemble des bases. On raisonne ensuite par récurrence.
2. $|SL_n(\mathbb{F}_q)| = |GL_n(\mathbb{F}_q)| \setminus |\mathbb{F}_q^*|$ par la suite exacte suivante : $1 \longrightarrow SL_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^* \longrightarrow 1$.
3. $PGL_n(\mathbb{K}) \simeq GL_n(\mathbb{K}) \setminus \mathbb{K}^*$ ou on compte le nombre de repère projectif (de la même manière que le précédent).
4. Le groupe spécial projectif est le quotient du groupe spécial par son sous groupe distingué des homothéties. On cherche donc à montrer que le nombre de racine $n^{\text{ième}}$ de l'unité dans $\mathbb{F}_q$ vaut $d = \gcd(n, q-1)$ (on applique Lagrange et Bézout).

(Les autres voir le tome 1) □

Lemme (Famille). *Soient $q, n, m \in \mathbb{N}$.*

1. *Famille libre à m éléments ($m \leq n$) :* $q^{\frac{m(m-1)}{2}}(q-1)^m\frac{[n]_q!}{[n-m]_q!}$
2. *Famille génératrice à m éléments ($m \geq n$) :* $q^{\frac{n(n-1)}{2}}(q-1)^n\frac{[m]_q!}{[m-n]_q!}$
3. *Bases :* $q^{\frac{n(n-1)}{2}}(q-1)^n[n]_q! = g_n$

Démonstration.
1. On fait agir transitivement $GL_n(\mathbb{F}_q)$ sur l'ensemble des systèmes libres de cardinal m (théorème de la base incomplète). On trouve un premier cardinal que l'on simplifie avec les résultats précédents.
2. Dualité
3. Lorsqu'on compte le nombre de base de $\mathbb{F}_q^n$ pour trouver $|GL_n(\mathbb{F}_q)|$.

□

Lemme (Application linéaire)**.** *Soient* $q, n, m \in \mathbb{N}$.

1. *Générale :* $\left|\mathcal{L}\left(\mathbb{F}_q^m, \mathbb{F}_q^n\right)\right| = q^{mn}$
2. *Injective de* $\mathbb{F}_q^m$ *vers* $\mathbb{F}_q^n$ $(m \leq n)$ *:* $q^{\frac{m(m-1)}{2}}(q-1)^m \frac{[n]_q!}{[n-m]_q!}$
3. *Surjective de* $\mathbb{F}_q^m$ *vers* $\mathbb{F}_q^n$ $(n \leq m)$ *:* $q^{\frac{n(n-1)}{2}}(q-1)^n \frac{[m]_q!}{[m-n]_q!}$
4. *De rang* r *de* $\mathbb{F}_q^m$ *vers* $\mathbb{F}_q^n$ $(r \leq m$ *et* $r \leq n)$ *:* $g_r \begin{bmatrix} m \\ r \end{bmatrix}_q \begin{bmatrix} n \\ r \end{bmatrix}_q = q^{\frac{r(r-1)}{2}}(q-1)^r [r]_q! \begin{bmatrix} m \\ r \end{bmatrix}_q \begin{bmatrix} n \\ r \end{bmatrix}_q$

Démonstration. 1. Argument de dimension

2. Application linéaire entièrement caractérisé par l'image d'une base. Le nombre d'application injective est donc le nombre de système libre.
3. Dualité via la transposition
4. On fait agir par multiplication à droite $GL_n(\mathbb{F}_q)$ sur $\mathcal{M}_{m,n}(\mathbb{F}_q)$. L'ensemble des matrices dont l'image est F un sous-espace de dimension r est une orbite qui ne dépend ni de r ni de F. On conclut via le stabilisateur.

□

Lemme (Endomorphisme)**.** *Soient* $q, n, m \in \mathbb{N}$.

1. *Généraux :* $|End(E)| = q^{n^2}$
2. *Diagonalisable :* $|\mathcal{D}_n| = \sum_{\substack{n_1+\cdots+n_q=n \\ n_i \geq 0}} \frac{g_n}{\prod_{i=1}^q g_{n_i}}$
3. *Niloptents :* $|\mathcal{N}_n| = q^{n(n-1)}$
4. *Trigonalisable :* $|\mathcal{T}_n| = \sum_{\substack{n_1+\cdots+n_q=n \\ n_i \geq 0}} \frac{g_n}{q^{-n}\prod_{i=1}^q g_{n_i}}$

Démonstration. 1. Par dimension

2. On fait agir $GL_n(\mathbb{F}_q)$ sur l'ensemble des sous-espaces propres.
3.
4. Mêmes arguments que pour la diagonalisation mais le lemme des noyaux est différents donc on n'utilise pas les sous-espaces propres.

□

Références

[1] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries, tome 2.* Calvage et Mounet, 2015.

[2] P. Caldero and J. Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, tome 2.* Calvage et Mounet, 2018.