Dénombrement des endomorphismes nilpotents sur un corps fini :

I Le développement

Le but de ce développement est de déterminer le nombre d'endomorphismes nilpotents définis sur un corps fini.

Théorème 1 : [Caldero, p.74]
Si $\mathbb{K}$ est un corps fini commutatif de cardinal q, alors il y a $n_d = q^{d(d-1)}$ matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{K}$.

Preuve :
On considère $\mathbb{K}$ est un corps fini commutatif de cardinal q et E un $\mathbb{K}$-espace vectoriel de dimension d.
$*$ Montrons que $\mathcal{L}(E)$ est en bijection avec l'ensemble des décompositions de Fitting :
- Si $u \in \mathcal{L}(E)$, alors on lui associe sa décomposition de Fitting.

- Soit $((F,G),v,w)$ avec $E = F \oplus G$, v nilpotent sur F et w un automorphisme sur G.
Pour tout $x \in E$, il existe un unique couple $(x_F, x_G) \in F \times G$ tel que $x = x_F + x_G$. On définit alors u sur E par $u(x) = v(x_F) + w(x_G) = (v \oplus w)(x)$ et pour tout $k \in \mathbb{N}^*$, $u^k = v^k \oplus w^k$. On a alors pour tout entier naturel k supérieur ou égal à l'indice de nilpotence de v, $u^k = 0_F \oplus w^k$ et donc $F = \mathrm{Ker}\left(u^k\right)$ et $G = \mathrm{Im}\left(u^k\right)$.
Ainsi, $((F,G),v,w)$ est la décomposition de Fitting de u.

$*$ Calcul intermédiaire :
Posons $X_k = \{(F,G) \text{ tq } E = F \oplus G \text{ et } \dim(F) = k\}$.
On a alors $\mathrm{Card}(\mathcal{L}(E)) = \sum_{k=0}^{d} m_{k,d} n_k \,\mathrm{Card}(\mathrm{GL}_{d-k}(\mathbb{K}))$, avec $m_{k,d} = \mathrm{Card}(X_k)$.
On considère également l'action :

$$* : \left| \begin{array}{ccc} \mathrm{GL}_d(\mathbb{K}) \times X_k & \longrightarrow & X_k \\ (g,(F,G)) & \longmapsto & (g(F),g(G)) \end{array} \right.$$

Cette action est bien définie car g est inversible et préserve les dimensions (l'image d'une base est une base).

Soient $(F,G) \in X_k$ et $(F',G') \in X_k$ avec $\mathcal{B}, \mathcal{B}'$ des bases respectivement adaptées aux décompositions $E = F \oplus G$ et $E' = F' \oplus G'$.
Il existe alors $g \in \mathrm{GL}_d(\mathbb{K})$ tel que $\mathcal{B}' = g(\mathcal{B})$, donc $g * (F,G) = (F',G')$ et on a alors $\mathrm{Orb}((F,G)) = X_k$. De plus, on a par la relation orbite-stabilisateur :

$$\begin{aligned} \mathrm{Card}(\mathrm{GL}_d(\mathbb{K})) &= \mathrm{Card}\left(\mathrm{Stab}_{\mathrm{GL}_d(\mathbb{K})}(F,G)\right) \mathrm{Card}(\mathrm{Orb}((F,G))) \\ &= \mathrm{Card}\left(\mathrm{Stab}_{\mathrm{GL}_d(\mathbb{K})}(F,G)\right) \mathrm{Card}(X_k) \end{aligned}$$

Puisque l'action est transitive, il nous suffit de calculer un seul stabilisateur :
Pour $(F_0,G_0) \in X_k$, en considérant une base de E adaptée à la décomposition $E = F_0 \oplus G_0$, on a :

$$\mathrm{Stab}_{\mathrm{GL}_d(\mathbb{K})}(F,G) = \left\{ \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},\ A \in \mathrm{GL}_k(\mathbb{K}) \text{ et } B \in \mathrm{GL}_{d-k}(\mathbb{K}) \right\}$$

Ce qui donne $\mathrm{Card}\left(\mathrm{Stab}_{\mathrm{GL}_d(\mathbb{K})}(F,G)\right) = g_k g_{d-k}$, et ainsi $m_{k,d} = \dfrac{g_d}{g_k g_{d-k}}$ et finalement :

$$q^{d^2} = \sum_{k=0}^{d} \frac{g_d}{g_k} n_k$$

$*$ Calculons n_d :
On a :

$$q^{d^2} = \sum_{k=0}^{d} \frac{g_d}{g_k} n_k = n_d + \sum_{k=0}^{d-1} \frac{g_d}{g_k} n_k = n_d + \frac{g_d}{g_{d-1}} \sum_{k=0}^{d-1} \frac{g_{d-1}}{g_k} n_k = n_d + \frac{g_d}{g_{d-1}} q^{(d-1)^2}$$

On a donc $n_d = q^{d^2} - \dfrac{g_d}{g_{d-1}} q^{(d-1)^2}$ et puisque $\dfrac{g_d}{g_{d-1}} = q^{d-1}\left(q^d - 1\right)$, on a alors :

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

Finalement, on a dénombré le nombre d'endomorphismes nilpotents sur E.

■

II Remarques sur le développement

II.1 Résultat(s) utilisé(s)

Dans ce développement, on a surtout utilisé le lemme ainsi que la décomposition de Fitting. On rappelle ci-dessous de quoi il s'agit en considérant u un endomorphisme de E de dimension d :

Lemme 2 : [Caldero, p.74]
Les suites $\left(\operatorname{Ker}\left(u^k\right)\right)_{k\in\mathbb{N}}$ et $\left(\operatorname{Im}\left(u^k\right)\right)_{k\in\mathbb{N}}$ sont respectivement croissante et décroissante au sens de l'inclusion.
De plus, ces deux suites sont stationnaires à partir d'un certain rang $n_0 \in \mathbb{N}$.

Preuve :
Il est clair que la suite $\left(\operatorname{Ker}\left(u^k\right)\right)_{k\in\mathbb{N}}$ est croissante et que la suite $\left(\operatorname{Im}\left(u^k\right)\right)_{k\in\mathbb{N}}$ est décroissante au sens de l'inclusion. De plus, comme E est de dimension finie, elles sont toutes les deux stationnaires à partir d'un certain rang (distinct a priori).

De plus, ces deux suites stationnent à partir du même rang. En effet, si l'on a $\dim\left(\operatorname{Ker}\left(u^k\right)\right) = \dim\left(\operatorname{Ker}\left(u^{k+1}\right)\right)$, alors par la formule du rang on a $\dim\left(\operatorname{Im}\left(u^k\right)\right) = \dim\left(\operatorname{Im}\left(u^{k+1}\right)\right)$ (et réciproquement) et on note alors n_0 ce rang à partir duquel les deux suites sont stationnaires.

■

Lemme 3 : Lemme de Fitting [Caldero, p.74] :
Avec les notations du lemme précédent, on a $E = \operatorname{Ker}(u^{n_0}) \oplus \operatorname{Im}(u^{n_0})$.
De plus, u induit un endomorphisme nilpotent sur $\operatorname{Ker}(u^{n_0})$ et un automorphisme sur $\operatorname{Im}(u^{n_0})$.

Preuve :
On reprend les notations du lemme précédent.
$*$ Pour montrer que $E = \operatorname{Ker}(u^{n_0}) \oplus \operatorname{Im}(u^{n_0})$ on peut se contenter de montrer (grâce la formule du rang) que $\operatorname{Ker}(u^{n_0}) \cap \operatorname{Im}(u^{n_0}) = \emptyset$.

Soit $x \in \operatorname{Ker}(u^{n_0}) \cap \operatorname{Im}(u^{n_0})$.
Il existe alors $y \in E$ tel que $x = u^{n_0}(y)$ et de plus, $u^{n_0}(x) = u^{2n_0}(y) = 0_E$. On a donc $y \in \operatorname{Ker}\left(u^{2n_0}\right) = \operatorname{Ker}(u^{n_0})$ et donc $x = u^{n_0}(y) = 0_E$.

Finalement on a bien $E = \operatorname{Ker}(u^{n_0}) \oplus \operatorname{Im}(u^{n_0})$.

$*$ Tout d'abord, u stabilise $\operatorname{Ker}(u^{n_0})$ et $\operatorname{Im}(u^{n_0})$ (car u commute avec u^{n_0}), donc on peut bien parler d'endomorphisme induit.

On en ensuite $u|_{\operatorname{Ker}(u^{n_0})}$ nilpotent car il s'annule à la puissance n_0. Pour montrer que l'endomorphisme $u|_{\operatorname{Im}(u^{n_0})}$ est un automorphisme, il suffit de montrer qu'il est surjectif (car E est de dimension finie). Or, $\operatorname{Im}\left(u|_{\operatorname{Im}(u^{n_0})}\right) = \operatorname{Im}\left(u^{n_0+1}\right) = \operatorname{Im}(u^{n_0})$ (par construction de n_0).

Finalement, u induit bien un endomorphisme nilpotent sur $\operatorname{Ker}(u^{n_0})$ et un automorphisme sur $\operatorname{Im}(u^{n_0})$.

■

On peut alors donner la définition suivante :

Définition 4 : Décomposition de Fitting [Caldero, p.74] :
La donnée de $((F,G),v,w)$ où $F = \operatorname{Ker}(u^{n_0})$, $G = \operatorname{Im}(u^{n_0})$, $v = u|_F$ et $w = u|_G$ avec $E = F \oplus G$, v nilpotent et w un automorphisme est appelée **décomposition de Fitting**.

II.2 Pour aller plus loin...

Exemple 5 :
En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a 4 matrices nilpotentes dans $\mathcal{M}_2(\mathbb{F}_2)$. Par un calcul direct, on trouve que ce sont les matrices :

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Il est également possible de ne s'intéresser qu'aux endomorphismes nilpotents ayant un indice de nilpotence égal à d :

Proposition 6 :
Si $\dim(E) = d \geq 2$, alors le nombre d'endomorphismes nilpotents de E d'indice d est :

$$\frac{\mathrm{GL}_d(\mathbb{F}_q)}{q^{n-1}(q^n-1)} = \prod_{k=0}^{n-2}\left(q^n - q^k\right)$$

Preuve :
Travaillons matriciellement :
$*$ Avec la réduction de Jordan, on a qu'une matrice $M \in \mathcal{M}_d(\mathbb{F}_q)$ est nilpotente d'indice d si, et seulement si, elle est conjuguée à la matrice :

$$J = \begin{pmatrix} 0 & & & (0) \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ (0) & & 1 & 0 \end{pmatrix}$$

$*$ La matrice J est la matrice compagnon de X^d, donc J est la matrice d'un endomorphisme cyclique. On en déduit que son commutant est $\mathbb{F}_q[J]$. De plus, si $P \in \mathbb{F}_q[X]$ avec $\deg(P) \leq d$, on a par un calcul direct de $P(J)$ que $P(J)$ est inversible si, et seulement si, $P(0) \neq 0$. On en déduit que :

$$\text{Card}\left(\text{Com}(J) \cap \text{GL}_d\left(\mathbb{F}_q\right)\right) = q^{n-1}\left(q^n - 1\right)$$

$*$ Enfin, le groupe $\text{GL}_d\left(\mathbb{F}_q\right)$ agit transitivement sur la classe de conjugaison de J par conjugaison. On en déduit avec le point précédent que :

$$\text{Card}(\text{Orb}(J)) = \frac{\text{Card}\left(\text{GL}_d\left(\mathbb{F}_q\right)\right)}{\text{Card}\left(\text{Stab}_{\text{GL}_d\left(\mathbb{F}_q\right)}(J)\right)} = \frac{\text{GL}_d(\mathbb{F}_q)}{q^{n-1}(q^n-1)} = \prod_{k=0}^{n-2}\left(q^n - q^k\right)$$

■

Exemple 7 :

En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a 3 matrices nilpotentes d'indice 2 dans $\mathcal{M}_2\left(\mathbb{F}_2\right)$. Par un calcul direct, on trouve que ce sont les matrices :

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Remarque 8 :

Il est possible de chercher à dénombrer d'autres types d'endomorphismes dans un espace vectoriel fini. Par exemple on peut dénombrer les endomorphismes diagonalisables via le nombre d'endomorphismes admettant un polynôme caractéristique scindé à racines simple.

II.3 Recasages

Recasages : 101 - 104 - 106 - 123 - 148 - 151 - 156 - 190.

III Bibliographie

— Philippe Caldero, *Carnet de voyage en Algébrie*.