

Nombre d'endomorphismes nilpotents sur un corps fini

On dénombre les matrices carrées à coefficients dans un corps fini \mathbb{F}_q qui sont nilpotentes d'indice maximal. Ce développement présente un lien avec les leçons suivantes :

Groupes opérant sur un ensemble. Exemples et applications.

Groupes finis. Exemples et applications.

Groupe linéaire d'un espace vectoriel de dimension finie E , sous-groupes de $\text{GL}(E)$. Applications.

Corps finis. Applications.

Endomorphismes nilpotents.

Méthodes combinatoires, problèmes de dénombrement.

Voici deux références : Fresnel et Matignon, *Algèbre et géométrie - 81 thèmes pour l'agrégation de mathématiques*, Caldero et Germoni, *Histoires hédonistes de groupes et de géométries, tome 2* (chapitre IV). Dans ces livres se trouve le calcul du cardinal du cône nilpotent tout entier.

Théorème : Soit $n \geq 1$ un entier et \mathbb{F}_q un corps fini. Alors le nombre de matrices nilpotentes d'indice maximal n dans l'anneau $M_n(\mathbb{F}_q)$ est égal à $(q^n - 1)(q^n - q) \dots (q^n - q^{n-2})$.

La preuve utilise une propriété importante des endomorphismes *cycliques* (voir [Gourdon] p. 279 et suivantes, notamment p. 282). Une définition simple est que f est cyclique si et seulement si son polynôme minimal est de degré n . Une définition équivalente est qu'il existe un vecteur x tel que tout vecteur y est l'image de x par un polynôme en f . La propriété importante que nous utiliserons est qu'un endomorphisme f est cyclique si et seulement si son commutant ⁽¹⁾ se réduit à l'ensemble des polynômes en f .

On utilise ici un cas particulier puisqu'une matrice nilpotente d'indice n a pour polynôme minimal X^n . Sur cet exemple, on peut démontrer directement la propriété sur le commutant ; c'est ce que je fais dans la preuve qui suit. Ce cas particulier est aussi utile pour démontrer la non-surjectivité de l'exponentielle de $\text{SL}_n(\mathbb{C})$, ou pour étudier les endomorphismes cycliques.

Preuve : Considérons l'action par conjugaison de $\text{GL}_n(\mathbb{F}_q)$ sur $M_n(\mathbb{F}_q)$. Alors l'ensemble des endomorphismes nilpotents d'indice n est égal à l'orbite de la matrice nilpotente

$$N_0 = \begin{pmatrix} 0 & \dots & \dots & \dots & 0 \\ 1 & 0 & & & \vdots \\ 0 & 1 & 0 & & \vdots \\ \vdots & & \ddots & 0 & \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

En effet, si N est nilpotente d'indice n , c'est-à-dire $N^n = 0$ mais $N^{n-1} \neq 0$, alors on peut choisir un vecteur x qui ne soit pas dans $\ker N^{n-1}$. On vérifie que $\{1, x, N(x), \dots, N^{n-1}(x)\}$ est une

1. Le commutant de f est l'ensemble des endomorphismes qui commutent avec f .

famille libre, donc une base de $(\mathbb{F}_q)^n$. La matrice de N dans cette base est la matrice ci-dessus, ce qui démontre l'assertion.

Il reste à calculer le cardinal du stabilisateur de cette matrice, puis à utiliser la formule $|\mathcal{O}(x)| = |G|/|G_x|$. On va montrer que le stabilisateur en question, qui est le commutant de N_0 dans $\text{GL}_n(\mathbb{F}_q)$, est égal à l'ensemble des polynômes en N_0 . (En fait tout sera vrai pour une matrice nilpotente N d'indice n , je note donc N au lieu de N_0).

On choisit encore $x \notin \ker N^{n-1}$ et on observe que comme $\{1, x, N(x), \dots, N^{n-1}(x)\}$ est une base, tout vecteur y s'écrit $y = \sum a_i N^i(x)$ et est donc l'image de x par un polynôme en N , à savoir $P(N) = \sum a_i N^i$.

Soit C une matrice commutant avec N . Par ce qui précède pour $y = C(x)$, il existe un polynôme P tel que $C(x) = P(N)(x)$. Pour montrer que $C = P(N)$, il suffit de montrer que pour tout vecteur y on a $C(y) = P(N)(y)$. Or $y = Q(N)(x)$ pour un certain polynôme Q , donc

$$C(y) = (C \circ Q(N))(x) = (Q(N) \circ C)(x)$$

(puisque C commute avec N et donc avec tout polynôme en N)

$$\dots = Q(N)(C(x)) = Q(N)(P(N)(x)) = P(N)(Q(N)(x)) = P(N)(y) .$$

On a obtenu $C = P(N) = a_0 + a_1 N + \dots + a_d N^d$, un polynôme en N .

Pour finir considérons le morphisme $\mathbb{F}_q[X] \rightarrow \text{M}_n(\mathbb{F}_q)$ qui à l'indéterminée X associe N . Son noyau est l'idéal engendré par le polynôme minimal de N i.e. X^n . Donc le sous-espace $\mathbb{F}_q[N] \subset \text{M}_n(\mathbb{F}_q)$ des polynômes en N est isomorphe à $\mathbb{F}_q[X]/X^n$, de dimension n sur \mathbb{F}_q . Pour une matrice $C = a_0 + a_1 N + \dots + a_{n-1} N^{n-1}$, si $a_0 = 0$, alors C est nilpotente, donc non inversible. Si $a_0 \neq 0$, C est la somme de la matrice d'homothétie $a_0 \text{Id}$, inversible, et d'une matrice nilpotente, les deux commutant entre elles ; C est donc inversible. En conclusion l'ensemble des matrices inversibles commutant avec N est déterminé par la seule condition $a_0 \neq 0$, il possède $(q-1)q^{n-1}$ éléments. Donc le cardinal recherché est

$$\frac{|\text{GL}_n(\mathbb{F}_q)|}{(q-1)q^{n-1}} = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{(q-1)q^{n-1}} = (q^n - 1)(q^n - q) \dots (q^n - q^{n-2}) .$$

□

Bibliographie

[Gourdon] GOURDON, Algèbre, *Ellipses*.