

CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$

[Rom17, §5.6, p148–151]

ÉNONCÉ

APPLICATION. [CARDINAL DE $\mathcal{D}_n(\mathbb{F}_q)$]

Soient $n \in \mathbb{N}$ et $q = p^r$ où p est premier et $r \in \mathbb{N}^*$. Soit $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de taille n sur $\mathbb{F}_q$. Alors en posant $|\mathcal{GL}_0(\mathbb{F}_q)| = 1$, on a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{(n_k)_{1 \leq k \leq q} \in \mathbb{N}^q \\ n_1 + \dots + n_q = n}} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}.$$

DÉVELOPPEMENT

Soit $E = (\mathbb{F}_q)^n$ muni de sa base canonique (ou tout autre $\mathbb{F}_q$ -espace vectoriel de dimension n). Dans tout ce qui suit, E_k désignera un sous-espace vectoriel de E . Notons :

$$\mathcal{F} = \left\{ (E_k)_{1 \leq k \leq q} : E = \bigoplus_{k=1}^q E_k \right\},$$

puis, pour $n_1, \dots, n_q$ entiers tels que $\sum_{k=1}^q n_k = n$:

$$\mathcal{F}_{(n_1, \dots, n_q)} = \left\{ (E_k)_{1 \leq k \leq q} \in \mathcal{F} : \forall k \in \llbracket 1, q \rrbracket, \dim(E_k) = n_k \right\}.$$

On remarque que les $(\mathcal{F}_{(n_1, \dots, n_q)})_{n_1 + \dots + n_q = n}$ forment une partition de $\mathcal{F}$. On va montrer que $|\mathcal{D}_n(\mathbb{F}_q)| = |\mathcal{F}|$ puis on calculera le cardinal de chaque $\mathcal{F}_{(n_1, \dots, n_q)}$.

LEMME. Soit $M \in \mathcal{M}_n(\mathbb{F}_q)$. Alors $M \in \mathcal{D}_n(\mathbb{F}_q) \iff M^q = M$.

Soit M diagonalisable. Son polynôme minimal est scindé à racines simples : écrivons

$$\pi_M(X) = \prod_{\lambda \in \text{Sp}(M)} X - \lambda.$$

Il est clair que $\pi_M(X) \mid X^q - X = \prod_{\lambda \in \mathbb{F}_q} X - \lambda$. Donc $M^q = M$.

Réciproquement, si $M^q = M$, alors M admet un polynôme annulateur scindé à racines simples, donc est diagonalisable.

LEMME. On a $|\mathcal{D}_n(\mathbb{F}_q)| = |\mathcal{F}|$.

Pour $M \in \mathcal{D}_n(\mathbb{F}_q)$, appliquons le lemme des noyaux à $X^q - X = \prod_{\lambda \in \mathbb{F}_q} X - \lambda$:

$$E = \bigoplus_{\lambda \in \mathbb{F}_q} \ker(M - \lambda \text{Id}) = \bigoplus_{k=1}^q \underbrace{\ker(M - \lambda_k \text{Id})}_{E_k}.$$

Il est alors clair que

$$\begin{aligned} \phi : \mathcal{D}_n(\mathbb{F}_q) &\longrightarrow \mathcal{F} \\ M &\longmapsto (E_k)_{1 \leq k \leq q} \end{aligned}$$

est une bijection (puisque $\phi(M) = \phi(M')$ implique que M et M' coïncident sur chaque E_k , donc par somme directe $M = M'$, et la surjectivité est immédiate).

Calculons désormais $|\mathcal{F}_N|$, où $N = (n_1, \dots, n_q) \in \mathbb{N}^q$ est fixé tel que $\sum_{k=1}^q n_k = n$.

Considérons l'application

$$\begin{aligned} \mathcal{GL}_n(\mathbb{F}_q) \times \mathcal{F}_N &\longrightarrow \mathcal{F}_N \\ (M, (E_k)_{1 \leq k \leq q}) &\longmapsto (ME_k)_{1 \leq k \leq q}. \end{aligned}$$

Elle est bien à valeurs dans $\mathcal{F}_N$ car pour $M \in \mathcal{GL}_n(\mathbb{F}_q)$ et $(E_k)_{1 \leq k \leq q} \in \mathcal{F}_N$, on a $E = ME = \sum_{k=1}^q ME_k$ avec $\dim(ME_k) = n_k$ donc $E = \bigoplus_{k=1}^q ME_k$ et ainsi $(ME_k)_{1 \leq k \leq q} \in \mathcal{F}_N$. C'est une action de groupe (les axiomes sont vérifiés grâce aux propriétés des matrices).

Notons de plus que l'action est transitive. En effet, si $(E_k^1)_{1 \leq k \leq q}, (E_k^2)_{1 \leq k \leq q} \in \mathcal{F}_N$, munissons chaque E_k^i d'une base $\mathcal{B}_k^i$ et considérons M qui envoie la base $\mathcal{B}_k^1$ sur la base $\mathcal{B}_k^2$ (ce qui est possible puisque les deux bases ont même cardinal). Alors M est entièrement déterminée et on a clairement $M(E_k^1)_{1 \leq k \leq q} = (E_k^2)_{1 \leq k \leq q}$.

Contemplant le stabilisateur de $(E_k)_{1 \leq k \leq q} \in \mathcal{F}_N$: on a que $M \in \text{Stab}((E_k)_{1 \leq k \leq q})$ si et seulement si $ME_k \subset E_k$ pour tout $1 \leq k \leq q$ (avec en fait égalité par bijectivité). Donc $\text{Stab}((E_k)_{1 \leq k \leq q})$ est en bijection avec les matrices diagonales par blocs avec des blocs de tailles $n_1, \dots, n_q$ pour lesquelles chaque bloc est une matrice inversible (en faisant un changement de base). On a donc $|\text{Stab}((E_k)_{1 \leq k \leq q})| = \prod_{k=1}^q |\mathcal{GL}_{n_k}(\mathbb{F}_q)|$.

L'action étant transitive, l'équation aux classes donne

$$|\mathcal{F}_N| = \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}.$$

Il ne reste plus qu'à utiliser le deuxième lemme et le partitionnement de $\mathcal{F}$ pour obtenir :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{(n_k)_{1 \leq k \leq q} \in \mathbb{N}^q \\ n_1 + \dots + n_q = n}} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^q |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}.$$

COMMENTAIRES

Pour éviter de s'embrouiller sur l'isomorphisme ϕ , une bonne manière de procéder est de voir M comme la matrice d'une application de $\text{GL}(E)$ **dans la base canonique** de E . Fixant la base, on associe une unique application à une matrice, et donc l'isomorphisme devient plus clair.