Dénombrement des endomorphismes diagonalisables sur un corps fini

1 Dénombrement des endomorphismes diagonalisables sur un corps fini

Recasages : 101, 104, 106, 123, 151, 152, 190

Théorème 1.1. *Le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ est*

$$\sum_{n_1+\cdots+n_q=n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|},$$

où les n_i sont des entiers positifs.

Proof. **Plan de la preuve :** On va montrer que l'ensemble des matrices diagonalisables sur $\mathcal{M}_n(\mathbb{F}_q)$ est en bijection avec l'union disjointe des décompositions de $\mathbb{F}_q^n$ en sommes directes de q sous espaces de tailles fixées. Pour calculer ce cardinal, il suffit donc de sommer les cardinaux des ensembles de décompositions de tailles fixées considérés. Pour dénombrer ces ensembles, on considère l'action naturelle de $GL_n(\mathbb{F}_q)$ sur ces décompositions et on utilise la relation orbites/stabilisateurs.

Fixons d'abord quelques notations. Notons $\mathcal{D}_{n,q}$ l'ensemble des matrices diagonalisables sur $\mathcal{M}_n(\mathbb{F}_q)$. On va être amené à travailler selon des décompositions de n en somme d'au plus q termes positifs, on notera donc $\mathcal{N}_i := (n_{i,1}, \ldots, n_{i,q})$ tout q-uplet d'entiers positifs de somme n. Enfin, pour un tel $\mathcal{N}_i$, $\mathcal{E}_{\mathcal{N}_i}$ désignera l'ensemble des q-uplets $(E_1, ..., E_q)$ de sous-espaces de $\mathbb{F}_q^n$ tels que $E_1 \oplus \cdots \oplus E_q = \mathbb{F}_q^n$ et $\dim(E_j) = n_{i,j}$, pour tout $1 \leq j \leq q$. La réunion des $\mathcal{E}_{\mathcal{N}_i}$, c'est-à-dire l'ensemble de toutes les décompositions de $\mathbb{F}_q^n$ en q sous-espaces de tailles arbitraires, sera notée $\mathcal{E}$.

Commençons par exhiber une bijection entre $\mathcal{D}_{n,q}$ et $\mathcal{E}$ la réunion disjointe des $\mathcal{E}_{\mathcal{N}_i}$ pour tous les $\mathcal{N}_i$ convenables.

Soient $\zeta_1, \ldots, \zeta_q$ les éléments ordonnés de $\mathbb{F}_q$ et $A \in \mathcal{D}_{n,q}$ une matrice diagonalisable. Considérons l'application

$$\varphi : \left| \begin{array}{ccc} \mathcal{D}_{n,q} & \longrightarrow & \mathcal{E} \\ A & \longmapsto & E_A \end{array} \right.$$

où E_A désigne la famille de sous-espaces $(E_1, \dots, E_q)$ où E_i est le sous-espaces propre de A associé à la valeur propre $\zeta_i \in \mathbb{F}_q$, ou l'espace trivial réduit à 0 si ζ_i n'est pas valeur propre de A. Comme A est diagonalisable, la somme des dimensions de ses sous-espaces propres vaut n (la dimension de l'espace ambiant) et l'application φ est donc bien définie.

Réciproquement, soit $\mathcal{N}_i := (n_{i,1}, \dots, n_{i,q})$ une partition de n (avec des termes éventuellement nuls) et $\mathcal{E}_{\mathcal{N}_i}$ l'ensemble de décompositions de $\mathbb{F}_q^n$ associé. Considérons maintenant l'application

$$\psi_{\mathcal{N}_i} : \left| \begin{array}{ccc} \mathcal{E}_{\mathcal{N}_i} & \longrightarrow & \mathcal{D}_{n,q} \\ (E_1, \dots, E_n) & \longmapsto & A_{(E_i)_i} \end{array} \right.$$

où $A_{(E_i)_i}$ est la matrice de l'endomorphisme u de $\mathbb{F}_q^n$ défini sur chaque E_i par $u(z_i) = \zeta_i z_i$ pour z_i dans E_i et $i \in \{1, \dots, q\}$. La matrice ainsi définie admet par construction pour sous-espaces propres les E_i non triviaux, qui sont en somme directe égale à l'espace tout entier, et est donc bien diagonalisable. Si on considère maintenant $\psi : \mathcal{E} \longrightarrow \mathcal{D}_{n,q}$ définie sur chaque $\mathcal{E}_{\mathcal{N}_i}$ comme $\psi_{\mathcal{N}_i}$, on a évidemment que φ et ψ sont bijectives puisque réciproques l'une de l'autre, d'où finalement la bijection ensembliste escomptée : $\mathcal{D}_{n,q} \simeq \mathcal{E}$.

Il s'agit de dénombrer, alors dénombrons, passons à l'action ! Faisons donc agir $GL_n(\mathbb{F}_q)$ sur un $\mathcal{E}_{\mathcal{N}_i}$ naturellement, c'est-à-dire via l'action

$$g \cdot (E_1, \dots, E_q) = (g(E_1), \dots, g(E_q)).$$

Les éléments agissant étant des automorphismes de $\mathbb{F}_q^n$, ils préservent les dimensions des espaces E_i ainsi que leur propriété de somme directe, l'image d'un élément de $\mathcal{E}_{\mathcal{N}_i}$ par une application $g \in GL_n(\mathbb{F}_q)$ est donc bien dans $\mathcal{E}_{\mathcal{N}_i}$.

On dispose d'une bien belle action dont on cherche à compter les éléments de l'ensemble sur lequel on agit. Là, ça fait *tic* et tous les voyants s'allument, on utilise la formule des classes[1]! En l'occurrence sa mise en place est particulièrement aisée, puisque l'action que l'on considère est transitive : pour tout élément $E := (E_1, \dots, E_q)$ (resp. $E' := (E'_1, \dots, E'_q)$) de $\mathcal{E}_{\mathcal{N}_i}$, on peut construire une base $\mathcal{B}$ (resp. $\mathcal{B}'$) de $\mathbb{F}_q^n$ en concaténant des bases des E_i (resp. des E'_i) et considérer l'élément $g \in GL_n(\mathbb{F}_q)$ qui envoie la base $\mathcal{B}$ sur la base $\mathcal{B}'$ et vérifie donc $g \cdot E = E'$.

Il ne reste donc plus qu'à déterminer le stabilisateur de n'importe quel élément (disons, pour changer, $(E_1, \dots, E_q)$) de $\mathcal{E}_{\mathcal{N}_i}$. Un élément du stabilisateur stabilise alors en particulier tous les E_i et préserve leurs dimensions. Une écriture matricielle (les E_i sont en somme directe égale à l'espace tout entier donc un élément du stabilisateur s'écrit dans une base adaptée aux E_i comme

[1]Pour rappel, pour une action $G \curvearrowright X$ et (x_j) un système de représentants pour les orbites non triviales, on a $|X| = |Fix(G)| + \sum |Orb(x_j)| = |Fix(G)| + \sum [G : G_{x_j}]$, puisqu'on a une bijection **ensembliste** entre $G/Stab(x_j)$ et $Orb(x_j)$. Lorsque l'action est transitive (une seule orbite), on a en particulier pour n'importe quel élément x de X: $|X| = [G : Stab(x)]$ et donc, lorsque les groupes considérés sont finis, $|X| = |G|/|Stab(x)|$.

une matrice diagonale par blocs inversibles) permet de voir immédiatement:

$$Stab((E_1,\dots,E_q)) \simeq \prod_{i=1}^{q} GL(E_i) = \prod_{i=1}^{q} GL_{n_i}(\mathbb{F}_q).$$

La formule des classes donne alors

$$|\mathcal{E}_{\mathcal{N}_i}| = \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|},$$

et finalement puisque $\mathcal{E}$ est la réunion disjointe des $\mathcal{E}_{\mathcal{N}_i}$,

$$|\mathcal{D}_{n,q}| = |\mathcal{E}| = \sum_{n_1+\cdots+n_q=n} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|},$$

où les n_i sont des entiers positifs. □

1.1 Aller plus loin dans le développement ?

Calcul du cardinal de $GL_n(\mathbb{F}_q)$: c'est le nombre de bases de $\mathbb{F}_q^n$. On commence par choisir un premier vecteur non nul, puis un vecteur non colinéaire au premier, puis un vecteur qui ne soit pas dans le plan engendré par les deux premiers vecteurs... Au final on trouve:

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

Voir CVA pour en déduire une estimation de la probabilité de tirer aléatoirement une matrice diagonalisable sur $\mathcal{M}_n(\mathbb{F}_q)$ lorsque q tend vers l'infini ($1/n!$).