Dénombrement des matrices diagonalisables de $\mathbb{F}_q$

Leçons : 101 ; 104 ; 106 ; 190

Références : CALDERO–GERMONI, *Nouvelles Histoires Hédonistes de Groupes et Géométries Tome 2* (p.66) [?]

Prérequis :

- les orbites d'une action sont disjointes [1]
- la relation orbite/stabilisateur
- même polynôme caractéristique pour des matrices semblables [2]

On notera $\mathcal{D}_n(q)$ l'ensemble des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$ où q est une puissance d'un nombre premier.

Introduction :

L'avantage des corps finis et notamment des espaces vectoriels de dimension finie sur les corps finis, c'est qu'ils sont justement finis. On peut alors se demander la proportion de matrices inversibles parmi toutes les matrices, ou la proportion de matrices diagonalisables parmi toutes les matrices. Pour cela, on va dénombrer $\mathrm{GL}_n(\mathbb{F}_q)$ et $\mathcal{D}_n(q)$.

Théorème 1. Soient q une puissance d'un nombre premier et $n \in \mathbb{N}$. On a alors

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|}$$

où, par convention, $|\mathrm{GL}_0(\mathbb{F}_q)| = 1$.

Démonstration. On va étudier l'action par conjugaison de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\mathcal{D}_n(q)$.

$$\varphi : \left\{ \begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_q) \times \mathcal{D}_n(q) & \to & \mathcal{D}_n(q) \\ (P, A) & \mapsto & PAP^{-1} \end{array} \right.$$

Étape 1 : *Etudions les orbites de cette action*

Soit $A \in \mathcal{D}_n(q)$, il existe donc une matrice $P \in \mathrm{GL}_n(\mathbb{F}_q)$ telle que

$$P^{-1}AP = \begin{pmatrix} \alpha_1 I_{m_1} & 0 & \dots & 0 \\ 0 & \alpha_2 I_{m_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \alpha_q I_{m_q} \end{pmatrix}$$

où $m = (m_1, \dots, m_q) \in \mathbb{N}^q$ tel que $m_1 + \cdots + m_q = n$ et où l'on écrit $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$.

1. cela s'écrit bien
2. cela vient de $\det(AB) = \det A \det B$

Pour chaque $m = (m_1, \dots, m_q) \in \mathbb{N}^q$ tel que $m_1 + \cdots + m_q = n$, on notera D_m cette matrice. Ainsi $D_m \in \mathcal{O}rb(A)$.

Soit m' tel que $D_{m'}$ est dans $\mathcal{O}rb(A)$. Regardons le polynôme caractéristique de $D_{m'}$.

$$\prod_{i=1}^{q}(X-\alpha_i)^{m'_i} = \chi_{D_{m'}} = \chi_A = \chi_{D_m} = \prod_{i=1}^{q}(X-\alpha_i)^{m_i}$$

D'où $m_i = m'_i$ pour tout $i \in \{1, \dots, q\}$, ce qui donne $D_m = D_{m'}$.

On vient de démontrer que, pour D_m et $D_{m'}$ différents, on a $\mathcal{O}rb(D_m) \cap \mathcal{O}rb(D_{m'}) = \emptyset$, autrement dit

$$\mathcal{D}_n(q) = \bigsqcup_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \mathcal{O}rb(D_m)$$

puisque dans chaque orbite, il y a au moins une matrice de la forme D_m.

Ainsi

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} |\mathcal{O}rb(D_m)|$$

On utilise la relation orbite/stabilisateur [3]

$$|\mathrm{GL}_n(\mathbb{F}_q)| = |\mathcal{O}rb(D_m)||\mathcal{S}tab(D_m)|$$

Étape 2 : *Etudions le stabilisateur de D_m*

Soit $P \in \mathcal{S}tab(D_m)$, on a donc $PD_m = D_mP$. Ainsi, pour toute valeur propre λ de D_m, pour tout $X \in E_\lambda$ [4],

$$D_mPX = PD_mX = \lambda PX$$

Donc $PX \in E_\lambda$, P stabilise donc tous les sous espaces propres, donc P est de la forme

$$P = \begin{pmatrix} P_1 & 0 & \dots & 0 \\ 0 & P_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & P_q \end{pmatrix}$$

où $P_i \in \mathrm{GL}_{m_i}(\mathbb{F}_q)$. Inversement, toute matrice de cette forme est dans le stabilisateur de D_m. De ce fait,

$$|\mathcal{S}tab(D_m)| = \prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|$$

On peut donc conclure

$$\begin{aligned} |\mathcal{D}_n(q)| &= \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathcal{S}tab(D_m)|} \\ &= \sum_{\substack{m_1+\cdots+m_q=n \\ m_i \geqslant 0}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|} \end{aligned}$$

□

3. car l'application $\begin{cases} G/\mathcal{S}tab(x) & \to & \mathcal{O}rb(x) \\ g & \mapsto & g.x \end{cases}$ est une bijection

4. E_λ est l'espace propre de D_m associé à la valeur propre λ

Pour compléter le résultat, il faut connaître le cardinal des matrices inversibles de taille n dans F_q.

Théorème 2. Soient q une puissance d'un nombre premier et $n \in \mathbb{N}$. On a alors

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

Démonstration. On a une bijection entre les bases de $\mathbb{F}_q^n$ et les matrices de $\mathrm{GL}_n(\mathbb{F}_q)$.

$$\varphi : \begin{cases} \{\text{bases de } \mathbb{F}_q^n\} & \to & \mathrm{GL}_n(\mathbb{F}_q) \\ (x_1, \dots, x_n) & \mapsto & \begin{pmatrix} & & \\ x_1 & \dots & x_n \\ & & \end{pmatrix} \end{cases}$$

Il suffit donc de compter les bases de $\mathbb{F}_q^n$. On a $(q^n - 1)$ choix pour le premier vecteur car il ne faut pas prendre le vecteur nul, ensuite pour le deuxième vecteur on a $(q^n - q)$ choix car il ne faut pas prendre un vecteur colinéaire au premier. Puis on a $(q^n - q^2)$ choix pour le troisième car il faut prendre un vecteur de $\mathbb{F}_q^n \backslash \mathrm{Vect}(x_1, x_2)$. etc... jusqu'au $n^{\text{ième}}$ vecteur où l'on a $(q^n - q^{n-1})$ choix. Ce qui fait que l'on trouve

$$|\{\text{bases de } \mathbb{F}_q^n\}| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

Ce qui conclut la preuve. □

Remarques :
Grâce au deuxième théorème, on peut aussi étudier les isomorphismes exceptionnels [**?**, p.49]

Astuces de l'agrégatif :
Le développement est assez court, il permet de bien prendre son temps pour expliquer tout ce qu'il faut comprendre, notamment la structure de la preuve dans l'étude de l'action.