# Nombre de matrices diagonalisables sur un corps fini

## 1 Nombre de matrices diagonalisables sur un corps fini

*Référence(s) :*

— Philippe Caldéro & Jérôme Germoni ; *Nouvelles histoires hédonistes de groupes et de géométries, Tome Second*

**Leçons associées :** 101, 190

### Théorème :

Soient $n \in \mathbb{N}$ et $q$ une puissance d'un nombre premier. On note $\mathbb{F}_q$ le corps à $q$ éléments. Alors le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$ est :

$$\sum_{\substack{n_1+...+n_q=n \\ n_i \geqslant 0}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$$

### Démonstration :

Soit $k \in \mathbb{N}$, et soit $(n_i)_{1 \leqslant i \leqslant k} \in \mathbb{N}^k$ tel que : $n_1 + ... + n_k = n$. On note $\mathcal{E}_{k,(n_i)}$ l'ensemble des $k$-uplets $(E_1, ..., E_k)$ de sous-espaces de $\mathbb{F}_q^n$ tels que pour tout $i \in [\![1, k]\!]$ :

$$\begin{aligned} E_1 \oplus ... \oplus E_k &= \mathbb{F}_q^n \\ dim(E_i) &= n_i \end{aligned}$$

On étudie l'action du groupe $GL_n(\mathbb{F}_{||})$ sur $\mathcal{E}_{k,(n_i)}$ :

$$\forall g \in GL_n(\mathbb{F}_q),\ g \cdot (E_1, ..., E_k) = (g(E_1), ..., g(E_k))$$

C'est une action de groupe :

Soit $g \in GL_n(\mathbb{F}_{||})$. On a bien :

$$\forall i \in \{1, ..., k\},\ \dim(g(E_i)) = \dim(E_i)$$

Il reste à montrer que les $g(E_i)$ sont en somme directe.

Soient $l, j \in \{1, ..., k\},\ l \neq j$. Soit $x \in g(E_l) \cap g(E_j)$. On a : $g^{-1}(x) \in E_l \cap E_j$. Or comme la famille $(E_i)_{1 \leqslant i \leqslant k}$ est en somme directe, on a : $E_l \cap E_j = \{0\}$. Donc on trouve : $x = 0$.

La famille $(g(E_i))_{1 \leqslant i \leqslant k}$ est donc en somme directe.

On vérifie directement les axiomes de définition d'une action de groupe :

— $\forall g, g' \in GL_n(\mathbb{F}_{||}), \forall (E_i) \in \mathcal{E}_{k,(n_i)},\ g \cdot (g' \cdot (E_i)) = (gg') \cdot (E_i)$

— $\forall (E_i) \in \mathcal{E}_{k,(n_i)},\ \mathrm{Id}_n \cdot (E_i) = (E_i)$

<u>Orbite(s) de l'action :</u>
On montre que cette action est transitive :
Soient $(E_i), (E'_i) \in \mathcal{E}_{k,(n_i)}$. On note $B$ une base adaptée à $(E_i)$ (respectivement $B'$ une base adaptée à $(E'_i)$). Alors en considérant $g \in GL_n(\mathbb{F}_{\shortparallel})$ qui envoie $B$ sur $B'$, on a : $g \cdot (E_i) = (E'_i)$.
Donc $\mathcal{E}_{k,(n_i)}$ est composée d'une seule orbite pour l'action de $GL_n(\mathbb{F}_{\shortparallel})$.

<u>Stabilisateurs :</u>
Soit $(E_i) \in \mathcal{E}_{k,(n_i)}$. Le stabilisateur de $(E_i)$ est le sous-groupe de $GL_n(\mathbb{F}_q)$ qui stabilise tous les $E_i$ : c'est le sous-groupe diagonal par blocs :

$$\prod_{i \in \{1,\dots,k\}} GL(E_i) \quad = \prod_{i \in \{1,\dots,k\}} GL_{n_i}(\mathbb{F}_q)$$

On a donc, pour $(n_i)_{1 \leqslant i \leqslant k}$ de somme $n$ : $|\mathcal{E}_{k,(n_i)}| = \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{k} |GL_{n_i}(\mathbb{F}_q)|}$

<u>Calcul du nombre de matrices diagonalisables :</u>
On construit une bijection entre l'ensemble des matrices diagonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$ et l'ensemble noté $E$ des $\mathcal{E}_{q,(n_i)}$ pour tous les $(n_i)_{1 \leqslant i \leqslant q}$ dont la somme vaut $n$.
Dans la suite on note $\zeta_1, \dots, \zeta_q$ les éléments de $\mathbb{F}_q$.

Soit $A \in \mathcal{M}_n(\mathbb{F}_q)$ diagonalisable. On considère $E_A = (\mathrm{Ker}(A - \zeta_i \mathrm{I}_n))_{1 \leqslant i \leqslant q}$. On note $n_i = \dim(\mathrm{Ker}(A - \zeta_i \mathrm{I}_n))$. Comme $A$ est diagonalisable, on a $E_A \in \mathcal{E}_{q,(n_i)}$.

Réciproquement, soit $(n_i)_{1 \leqslant i \leqslant q}$ de somme $n$. Soit $(E_i) \in \mathcal{E}_{k,(n_i)}$. On considère l'endomorphisme $\phi$ défini par :

$$\forall i \in \{1, \dots, q\}, \forall z_i \in E_i,\ \phi(z_i) = \zeta_i z_i$$

On note $A_{(E_i)}$ la matrice de $\phi$ dans une base adaptée à $(E_i)$. On a par construction une matrice diagonale.

On a donc une bijection $A \mapsto E_A$ de réciproque $(E_i) \mapsto A_{(E_i)}$.

Or par les étapes précédentes, on a, pour $(n_i)_{1 \leqslant i \leqslant q}$ de somme $n$ : $|\mathcal{E}_{q,(n_i)}| = \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$

Donc :

$$|E| = \sum_{\substack{n_1 + \dots + n_q = n \\ n_i \geqslant 0}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}$$