Nombres de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$

Réf: Carnet de Voyage en Algébrie, Caldero p. 20

Soit $n \in \mathbb{N}$ et $q = p^r$ ou p premier. On note $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$.

Théorème: On a:

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{m=1}^{n} \binom{q}{m} \sum_{\substack{v_1+\dots+v_m=m \\ v_t>0}} \frac{g_n}{\prod_{t=1}^{q} g_{v_t}} \quad \text{où } g_k = |GL_k(\mathbb{F}_q)|.$$

Preuve:

On note $\mathbb{F}_q = \{\lambda_1, \dots, \lambda_q\} =: \mathbb{K}$

On note $V = \{(n_1, \dots, n_q) \mid \sum_{i=1}^{q} n_i = n\}$ et pour $v \in V$ on note:

$$D_v = \mathrm{diag}(\underbrace{\lambda_1, \dots, \lambda_1}_{n_1}, \underbrace{\lambda_2, \dots, \lambda_2}_{n_2}, \dots, \underbrace{\lambda_q, \dots, \lambda_q}_{n_q})$$

On fait agir $GL_n(\mathbb{K})$ par conjugaison sur $\mathcal{D}_n(\mathbb{K})$ i.e:

$$\begin{aligned} GL_n(\mathbb{K}) \times \mathcal{D}_n(\mathbb{K}) &\longrightarrow \mathcal{D}_n(\mathbb{K}) \\ (g, d) &\longmapsto gdg^{-1} \end{aligned}$$

Soit $D \in \mathcal{D}_n(\mathbb{K})$ alors il existe un $v \in V$ tel que $D_v \in \mathcal{O}_D$ → orbite de D.
En effet D étant diagonalisable l'existence de v est clair. Montrons qu'il est unique.
Soit $v, v' \in V$ tel que D_v et $D_{v'}$ appartient à $\mathcal{O}_D$ alors D_v et $D_{v'}$ sont semblable, donc ils ont même polynômes caractéristique i.e:

$$\prod_{i=1}^{q} (X-\lambda_i)^{n_i} = \prod_{i=1}^{q} (X-\lambda_i)^{n_i'}$$

Par unicité $n_i = n_i'$ donc $v = v'$.
Ainsi les orbites sont indexés par V.

On fixe donc $v := (n_1, \dots, n_q) \in V$ et on cherche son stabilisateur.

Pour cela on pose $G_v = \{ \mathrm{diag}(A_1, .., A_q) \text{ avec } A_i \in GL_{m_i}(\mathbb{K}) \}$. Mq : $\mathrm{Stab}(D_v) = G_v$

Alors on a pour $g \in G_v$:

$$g D_v g^{-1} = \mathrm{diag}(\lambda_1 A_1 A_1^{-1}, .., \lambda_q A_q A_q^{-1}) = D_v .$$

Donc $G_v \subset \mathrm{Stab}(D_v)$.

Réciproquement soit $g \in \mathrm{Stab}(D_v)$ alors $g D_v g^{-1} = D_v$.

On écrit g par blocs par :

$$D_v = \begin{pmatrix} \lambda_1 I_{m_1} & & \\ & \ddots & \\ & & \lambda_q I_{m_q} \end{pmatrix} \quad \text{et} \quad g = \begin{pmatrix} M_{11} & \cdots & \\ \vdots & M_{22} & \\ & & M_{qq} \end{pmatrix} \text{ avec } M_{ij} \in \mathcal{M}_{m_i \times m_j}(\mathbb{K}).$$

Or on a $D_v g = g D_v$ ce qui donne :

$$\lambda_i M_{ij} = \lambda_j M_{ij} \text{ donc } (\lambda_i - \lambda_j) M_{ij} = 0$$

Si $i \neq j$ alors $\lambda_i \neq \lambda_j$ donc $M_{ij} = 0$.

Ainsi

$$g = \begin{pmatrix} M_{11} & & \\ & \ddots & \\ & & M_{qq} \end{pmatrix} \text{ et } g \in GL_n(\mathbb{K}) \text{ donc } \forall i, M_{ii} \in GL_{m_i}(\mathbb{K}) \text{ donc } g \in G_v .$$

On a donc $\mathrm{Stab}(D_v) = G_v$.

La formule des classes donnent :

$$|D_n(\mathbb{K})| = \sum_{v \in V} \frac{|GL_n(\mathbb{K})|}{|G_v|} = \sum_{\substack{(m_1, .., m_q) \\ m_1 + .. + m_q = n,\ i=1}} \frac{g_n}{\prod_{i=1}^{q} g_{m_i}} .$$

On va simplifier cette équation, pour cela on va dénombrer V.

Or choisir $v \in V$ revient à prendre les m, n_i non nuls ($1 \leq m \leq n$) et lui associé le m-uplet composé des m éléments non nuls.

Or pour tout m-uplets composé d'éléments non nuls on a $\binom{q}{m}$ éléments distincts de V d'où :

$$|D_n(\mathbb{K})| = \sum_{m=1}^{n} \binom{q}{m} \sum_{\substack{v_1 + .. + v_m = n \\ v_i > 0}} \frac{g_n}{\prod_{i=1}^{m} g_{v_i}}$$

Application: La probabilité de choisir une matrice diagonalisable dans $\mathcal{M}_n(\mathbb{K})$ tend vers $\frac{1}{n!}$ pour $q \longrightarrow +\infty$.

Preuve: On pose $\forall q = \frac{|\mathcal{D}_n(\mathbb{F}_q)|}{|\mathcal{GL}_n(\mathbb{F}_q)|}$ qui est donc une fraction rationnelle en q.

Il suffit donc d'étudier le monome de plus haut degré de $|\mathcal{D}_n(\mathbb{F}_q)|$ qui est une fraction rationnelle en q.

Or on sait que : $g_n = |\mathcal{GL}_n(\mathbb{K})| = (q^n - 1) \times \dots \times (q^n - q^{n-1})$ de degré n^2 en q.

et $\binom{q}{m} = \frac{q(q-1) \times \dots \times (q-m+1)}{m!}$ de degré m en q.

Ainsi chaque terme $\binom{q}{m} \frac{g_m}{\prod_{i=1}^{m} g_{v_i}}$ est de degré :

$$m + (n^2 - \sum_{t=1}^{m} v_t) \leq m + (n^2 - \sum_{t=1}^{m} v_t) \leq m + (n^2 - m) = n^2.$$

(m fois)

Or le seul monome de degré n^2 est pour $v = (1, \dots, 1)$.

En effet si on a degré le deuxième inégalité devient une égalité qui donne :

$$n = \sum_{t=1}^{m} v_t = m \quad \text{donc } v_t = 1.$$

Le terme correspond est donc :

$$\frac{q(q-1) \times \dots \times (q-n+1)}{n!} \times \frac{g_n}{(q-1)^n}.$$

Le monome dominant est $q^{n^2}/n!$ or $|\mathcal{D}_n(\mathbb{F}_q)| = q^{n^2}$ donc l'équivalent cherché est $\frac{q^{n^2}}{n!} \times \frac{1}{q^{n^2}} = \frac{1}{n!}$. ☒

Rmq: - En fait $|\mathcal{D}_n(\mathbb{F}_q)|$ est un pol en q

- Résultat découlant car dans $\mathbb{C}$ l'ensemble des mat diagonalisable est un ouvert dense de $\mathcal{M}_n(\mathbb{C})$.