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

Théorème 0.1

Soient $n \in \mathbb{N}^*$ et q une puissance d'un nombre premier.
On note $D_n(q)$ l'ensemble des matrices diagonalisables de $M_n(q) := M_n(\mathbb{F}_q)$. Alors, avec la convention $|GL_0(q)| = 1$, on a :

$$|D_n(q)| = \sum_{\substack{m_1,\dots,m_q \in \mathbb{N} \\ m_1+\dots+m_q=n}} \frac{|GL_n(q)|}{\prod_{i=1}^{q} |GL_{m_i}(q)|}.$$

Démonstration. On a par définition :

$$D_n(q) = \{PDP^{-1} | D \in M_n(q) \text{ diagonale et } P \in GL_n(q)\}.$$

Donc $GL_n(q)$ agit par conjugaison sur $D_n(q)$. On a alors pour $M \in D_n(q)$:

$$\text{Orb}(M) = \{PMP^{-1} | P \in GL_n(q)\},$$
$$\text{et Stab}(M) = \{P \in GL_n(q) | PMP^{-1} = M\}.$$

On introduit alors des notations. Soit χ un polynôme scindé sur $\mathbb{F}_q$ unitaire : $\chi = \prod_{i=1}^{r} (X - \lambda_i)^{m_i}$ avec $(\lambda_i)_i$ une suite croissante d'éléments deux à deux distincts de $\mathbb{F}_q$ et $m_i \geq 0$. On définit alors la matrice $D_\chi := \text{diag}(\lambda_i I_{m_i})_{1 \leq i \leq r}$ par bloc. On pose :

$$\theta_n := \{D_\chi | \chi \text{ polynôme scindé sur } \mathbb{F}_q \text{ unitaire de degré } n\}.$$

On a alors que $D_n(q) = \bigsqcup_{D \in \theta_n} \text{Orb}(D)$.

Remarque 0.2

On montre ici que θ_n est un système de représentants des orbites de $D_n(q)$ sous l'action de $GL_n(q)$.

En effet, si $M \in D_n(q)$, alors D est semblable à une matrice diagonale, qui est dans θ_n quitte à permuter les vecteurs de la base pour ordonner les valeurs propres. Donc on a $D_n(q) = \bigcup_{D \in \theta_n} \text{Orb}(D)$. Soient χ, ψ deux polynômes scindes sur $\mathbb{F}_q$ unitaire de degré n tels que $D_\chi \in \text{Orb}(D_\psi)$. Alors D_χ est semblable à D_ψ et ont même polynôme caractéristique, donc $\chi = \psi$: l'union est disjointe.
En passant au cardinal, on a :

$$|D_n(q)| = \sum_{D \in \theta_n} |\text{Orb}(D)|.$$

On utilise ensuite la relation orbite-stabilisateur :

$$|D_n(q)| = \sum_{D \in \theta_n} \frac{|GL_n(q)|}{|\text{Stab}(M)|}.$$

On cherche alors le cardinal du stabilisateur d'un éléments de θ_n. Soit $D \in \theta_n$,

$$\begin{aligned} \big(P \in \text{Stab}(D)\big) &\iff \big(PDP^{-1} = D\big) \\ &\iff \big(PD = DP \text{ et } P \in GL_n(q)\big) \end{aligned}$$

En notant $C(D)$ le commutant de D, on en déduit $\text{Stab}(D) = C(D) \cup GL_n(q)$.
Si P commute avec D, alors les sous-espaces propres de D sont stables par P. Donc $P = \text{diag}(P_1, ..., P_r)$ avec $P_i \in M_{m_i}(q),\ 1 \leq i \leq r$. Pour que P soit inversible, il faut et il suffit que les P_i soient inversibles. Réciproquement, on peut vérifier par le calcul que P de cette forme commutent avec D. Il y'a donc une bijection entre $C(D) \cup GL_n(q)$ et l'ensembles des r-uplets de matrices de tailles $m_i \times m_i$ inversibles, et on en déduit donc que :

$$|D_n(q)| = \sum_{D \in \theta_n} \frac{|GL_n(q)|}{\prod_{i=1}^{r} |GL_{m_i}(q)|}.$$

Cette formule est indexée sur les valeurs propres des matrices D ce qui n'est pas très pratique, on va la réindexer et ainsi obtenir la formule annoncée. Par construction de l'ensemble θ_n, on a :

$$\theta_n \cong \{\text{polynômes scindes sur } \mathbb{F}_q \text{ unitaire de degrés } n\}.$$

En notant $\mathbb{F}_q = \{\alpha_1, ..., \alpha_q\}$, on a qu'un polynôme scindé sur $\mathbb{F}_q$ est de la forme $\prod_{i=1}^{q}(X - \alpha_i)^{m_i}$ avec $m_1, ..., m_q \in \mathbb{N}$.
Dire que le polynôme est de degré n, c'est ajouter la condition $m_1 + ... + m_q = n$, ce qui nous donne :

$$|D_n(q)| = \sum_{\substack{m_1,...,m_q \in \mathbb{N} \\ m_1+...+m_q=n}} \frac{|GL_n(q)|}{\prod_{i=1}^{q} |GL_{m_i}(q)|}.$$

□

Remarque 0.3

$|GL_n(q)| = (q^n - 1)(q^n - q)...(q^n - q^{n-1})$.
En effet, $M \in M_n(\mathbb{F}_q)$ est inversible ssi les vecteurs colonnes forment une base.
Il suffit donc que le premier vecteur soit non nul : $q^n - 1$ choix.
Le deuxième vecteur ne doit pas être colinéaire au premier : $q^n - q$ choix.
Le troisième ne doit pas appartenir au plan engendré par les deux premiers vecteurs : $q^n - q^2$ choix ect...