Matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$: 101, 104, 123, 150, 155, 190

On fixe $n \in \mathbb{N}^*$ et q une puissance d'un nombre premier, on note $\mathcal{D}_n(q) = \{A \in \mathcal{M}_n(\mathbb{F}_q),\ A \text{ diagonalisable}\}$. On note $\mathcal{M}_n(q) := \mathcal{M}_n(\mathbb{F}_q)$, $GL_n(q) := GL_n(\mathbb{F}_q)$

Théorème : Avec la convention $|GL_0(\mathbb{F}_q)| = 1$, on a

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

Notons qu'on a de façon quasi-immédiate le lemme suivant :

Lemme : $|GL_m(q)| = \prod_{i=0}^{m-1} (q^m - q^i) = q^{\frac{m(m-1)}{2}} \prod_{i=0}^{m-1} (q^{i+1} - 1)$

La preuve du lemme utilise en fait la caractérisation $\mathcal{D}_n(q) = \{PDP^{-1},\ P \in GL_n(q),\ D \in \mathcal{M}_n(q) \text{ diagonale}\}$

On considèrera dans la suite l'action de $GL_n(q) \circlearrowright \mathcal{D}_n(q)$ par conjugaison et on note $\mathrm{Orb}(M)$ et $\mathrm{Stab}(M)$ l'orbite et le stabilisateur de $M \in \mathcal{D}_n(q)$ sous cette action.

Définition : Si $\chi = \prod_{i=1}^{r} (X - \lambda_i)^{m_i} \in \mathbb{F}_q[X]$ est un polynôme unitaire scindé ($\lambda_i \neq \lambda_j$ par $i \neq j$, $\in \mathbb{F}_q$)

On définit
$$D_\chi = \begin{pmatrix} \lambda_1 I_{m_1} & & \\ & \ddots & \\ & & \lambda_r I_{m_r} \end{pmatrix} \in \mathcal{D}_n(q)$$
$$\mathrm{Scal}_n(q) = \{D_\chi,\ \chi \text{ unitaire, scindé sur } \mathbb{F}_q,\ d^\circ \chi = n\}$$

Remarque : D_χ dépend de l'ordre des λ_i mais on va en fait se servir que si $D_{\chi_1} \neq D_{\chi_2}$ dans $\mathrm{Scal}_n(q)$ alors $\chi_1 \neq \chi_2$. (en voyant D_χ comme une classe de matrices où on a juste échangé les blocs diagonaux).

Lemme 1 : $\mathrm{Scal}_n(q)$ est un système de représentants des orbites de $\mathcal{D}_n(q)$ sous $GL_n(q)$

en particulier $\mathcal{D}_n(q) = \bigsqcup_{D \in \mathrm{Scal}_n(q)} \mathrm{Orb}(D)$

Preuve : Tout d'abord, si $D' \in \mathcal{D}_n(q)$, alors $D_{\chi_{D'}}$ est un représentant de D' dans $\mathrm{Scal}_n(q)$ (en permutant les vecteurs de base de façon convenable).

Si de plus χ_1 et χ_2 sont 2 polynômes scindés unitaires sur $\mathbb{F}_q$, de degré n tq $D_{\chi_1} \in \mathrm{Orb}(D_{\chi_2})$ alors $D_{\chi_1} \sim D_{\chi_2}$ et par suite, elles ont même polynôme caractéristique : $\chi_1 = \chi_2$.

La formule des classes donne immédiatement : $|\mathcal{D}_n(q)| = \sum_{D \in \mathrm{Scal}_n(q)} |\mathrm{Orb}(D)|$. (*)

Lemme 2 : Pour $D \in \mathrm{Scal}_n(q)$, on a $\mathrm{Stab}(D) = \mathrm{Comm}(D) \cap GL_n(q)$

où $\mathrm{Comm}(D) = \{M \in \mathcal{M}_n(q),\ MD = DM\}$

preuve : Soit $P\in\mathcal{M}_n(q)$. $P\in Stab(D)$ ssi $[P\in GL_n(q)$ et $PDP^{-1}=D]$

ssi $[P\in GL_n(q)$ et $PD=DP]$

ssi $P\in GL_n(q)\cap Comm(D)$.

Notons que avec la relation orbite-stabilisateur transforme (*) en

$$|\mathcal{D}_n(q)| = \sum_{D\in Scal_n(q)} \frac{|GL_n(q)|}{|GL_n(q)\cap Comm(D)|}$$

: il reste à calculer $|GL_n(q)\cap Comm(D)|$.

Lemme 3 : Pour $D=(\lambda_i I_{m_i})_{1\le i\le r}\in Scal_n(q)$ (avec $\lambda_i\neq\lambda_j$ pour $i\neq j$) on a

$$|GL_n(q)\cap Comm(D)| = \prod_{i=1}^{r} |GL_{m_i}(q)|$$

preuve : Soit $P\in Comm(D)$, comme D et P commutent, les sous-espaces propres de D sont stables par P et donc $P=(P_i)_{1\le i\le r}$ avec $P_i\in\mathcal{M}_{m_i}(q)$. Réciproquement, si P est de cette forme, on a bien $P\in Comm(D)$. Pour avoir P dans $GL_n(q)$, il faut et il suffit donc d'avoir $P_i\in GL_{m_i}(q)$.

démo du théorème : On a en injectant dans (*) : $|\mathcal{D}_n(q)| = \sum_{D\in Scal_n(q)} \frac{|GL_n(q)|}{\prod_{i=1}^{r}|GL_{m_i}(q)|}$

où on écrit $D\in Scal_n(q)$ sous une forme $D=(\lambda_i I_{m_i})_{1\le i\le r}$ avec $\lambda_i\neq\lambda_j$ pour $i\neq j$.

On veut réindexer la somme en une somme adaptée faisant intervenir les λ_i.

Par construction, $Scal_n(q) \overset{1:1}{\longleftrightarrow} \{P\in\mathbb{F}_q[X],\ \text{unitaire, scindé, } d°P=n\} \underset{(\Delta)}{\overset{1:1}{\longleftrightarrow}} \{(m_i)_{1\le i\le q}\in\mathbb{N}^q \text{ tq } \sum_{i=1}^{q} m_i=n\}$

(Δ) : en effet, en écrivant $\mathbb{F}_q=\{\mu_i\}_{1\le i\le q}$, $\varphi : \left|\begin{array}{ccc} \{(m_i)_{1\le i\le q}\in\mathbb{N}^q,\ \sum_{i=1}^{q} m_i=n\} & \longrightarrow & \{P\in\mathbb{F}_q[X],\ \text{unitaire, scindé, } d°P=n\} \\ (m_i)_{1\le i\le q} & \longmapsto & \prod_{i=1}^{q}(X-\mu_i)^{m_i} \end{array}\right.$

est une bijection (claire) donc le choix de $D\in Scal_n(q)$ équivaut à celui de $(m_i)_{1\le i\le n}$

d'où finalement : $$\boxed{|\mathcal{D}_n(q)| = \sum_{\substack{m_1,\dots,m_q\in\mathbb{N}^q\\ m_1+\dots+m_q=n}} \frac{|GL_n(q)|}{\prod_{i=1}^{q}|GL_{m_i}(q)|}}$$ (avec $|GL_0(q)|=1$).

Remarque : en posant $\nu_i(m)=|\{j\in[\![1;q]\!],\ m_j=i\}|$ et $\binom{a}{b_0,\dots,b_n}=\frac{a!}{b_0!\cdots b_n!}$, on peut réécrire la formule :

$$\boxed{|\mathcal{D}_n(q)| = \sum_{\substack{m_1\le\dots\le m_q\in\mathbb{N}^q\\ m_1+\dots+m_q=n}} \frac{|GL_n(q)|}{\prod_{i=1}^{q}|GL_{m_i}(q)|}\times\binom{q}{\nu_0(m),\dots,\nu_n(m)}}$$

En effet, étant donné un q-uplet $m=(m_i)_{1\le i\le q}$ fixé, on peut générer plusieurs polynômes (Ex : $q=3$, $m=(0,1,1)$ génère $X(X-1)$, $X(X-2)$ ou $(X-1)(X-2)$). Le nombre de tels polynômes est

$$\underbrace{\binom{q}{\nu_0(m)}}_{\text{blocs de taille 0 parmi}}\times\underbrace{\binom{q-\nu_0(m)}{\nu_1(m)}}_{\text{blocs de taille 1 parmi ceux restant}}\cdots\underbrace{\binom{q-\nu_0(m)-\dots-\nu_{n-1}(m)}{\nu_n(m)}}_{\text{blocs de taille n parmi ceux restants}} = \frac{q!(q-\nu_0(m))!\cdots(q-\nu_0(m)-\dots-\nu_{n-1}(m))!}{\nu_0(m)!(q-\nu_0(m))!\nu_1(m)!\cdots\nu_n(m)!\,0!} = \binom{q}{\nu_0(m),\dots,\nu_n(m)}$$

$\sum_{i=0}^{n}\nu_i(m)=q$