Dénombrement des matrices diagonalisables sur un corps fini

LACOSTE Cyril – PIERRON Théo

11 avril 2014

Soit n un entier et q une puissance d'un nombre premier.

Définition On note $D_n(q) = \{M \in \mathfrak{M}_n(\mathbb{F}_q), M \text{ diagonalisable}\}$.

THÉORÈME *Le cardinal de $D_n(q)$ vaut*

$$\sum_{m_1+\ldots+m_q=n} \frac{|\operatorname{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\operatorname{GL}_{m_i}(\mathbb{F}_q)|}$$

avec par convention $|\operatorname{GL}_0(\mathbb{F}_q)| = 1$.

On commence par fixer un ordre sur $\mathbb{F}_q$.

Définition Si $\chi = \prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ avec λ_i une suite croissante d'éléments de $\mathbb{F}_q$, on définit la matrice $D_\chi = \operatorname{diag}(\lambda_i I_{m_i})$.

On note aussi $S_n(q) = \{D_\chi, \chi \in \mathbb{F}_q[X] \text{ unitaire scindé de degré } n\}$.

Lemme 1
$S_n(q)$ est un système de représentants des orbites de $D_n(q)$ sous l'action de $\operatorname{GL}_n(\mathbb{F}_q)$.

Démonstration. Si $D \in D_n(q)$, D est semblable à une matrice diagonale. Quitte à permuter les vecteurs de base, on peut trouver une matrice diagonale à valeurs propres croissantes semblable à D, i.e. $D \sim D_{\chi_D}$.

De plus, si $\chi, \psi \in S_n(q)$, et si $D_\chi \sim D_\phi$, on a $\chi_{D_\chi} = \chi_{D_\psi}$ donc $\chi = \psi$. ■

Lemme 2
$\operatorname{Stab}(D_\chi) = \operatorname{GL}_n(\mathbb{F}_q) \cap C(D_\chi)$ où $C(D_\chi)$ est le commutant de D_χ.

Démonstration. Soit $P \in \mathfrak{M}_n(\mathbb{F}_q)$. On a alors

$$\begin{aligned} P \in \operatorname{Stab}(D_\chi) \quad & \text{ssi} \quad P \in \operatorname{GL}_n(\mathbb{F}_q) \text{ et } PD_\chi P^{-1} = D_\chi \\ & \text{ssi} \quad P \in \operatorname{GL}_n(\mathbb{F}_q) \text{ et } PD_\chi = D_\chi P \\ & \text{ssi} \quad P \in \operatorname{GL}_n(\mathbb{F}_q) \cap C(D_\chi) \end{aligned}$$

■

Lemme 3
Si $\chi = \prod_{i=1}^{r}(X-\lambda_i)^{m_i}$, on a

$$|C(D_\chi) \cap \operatorname{GL}_n(\mathbb{F}_q)| = \prod_{i=1}^{r} |\operatorname{GL}_{m_i}(\mathbb{F}_q)|$$

Démonstration. Si $P \in C(D_\chi)$, P commute avec D_χ donc les espaces propres de D_χ sont stables pour P. P est donc diagonale par blocs et ses blocs sont de taille $m_i \times m_i$.

Si on veut de plus P inversible, il faut et il suffit que chaque bloc soit inversible. On a donc une bijection entre $C(D_\chi) \cap \operatorname{GL}_n(\mathbb{F}_q)$ et les r-uplets de matrices $m_i \times m_i$ inversibles. D'où le résultat. ■

Démonstration du théorème. En utilisant successivement tous les lemmes et la formule des classes, on a

$$\begin{aligned}
|D_n(q)| &= \sum_{\chi \in S_n(q)} |\operatorname{Orb}(D_\chi)| = \sum_{\chi \in S_n(q)} \frac{|\operatorname{GL}_n(\mathbb{F}_q)|}{|\operatorname{Stab}(D_\chi)|} \\
&= \sum_{\chi \in S_n(q)} \frac{|\operatorname{GL}_n(\mathbb{F}_q)|}{|C(D_\chi) \cap \operatorname{GL}_n(\mathbb{F}_q)|} = \sum_{\chi \in S_n(q)} \frac{|\operatorname{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{r} |\operatorname{GL}_{m_i}(\mathbb{F}_q)|}
\end{aligned}$$

De plus, en notant $\mathbb{F}_q = \{\mu_1, \ldots, \mu_q\}$, l'application

$$\begin{cases} \{(x_1, \ldots, x_q), x_1 + \ldots + x_q = n\} & \to \quad S_q(n) \\ (m_1, \ldots, m_q) & \mapsto \quad \prod_{i=1}^{q} (X - \mu_i)^{m_i} \end{cases}$$

est bijective. Ainsi, on peut réindicer la somme :

$$|D_n(q)| = \sum_{m_1 + \ldots + m_q = n} \frac{|\operatorname{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\operatorname{GL}_{m_i}(\mathbb{F}_q)|} \qquad \blacksquare$$