Matrices diagonalisables dans $\mathbb{F}_q$

Référence : ~~ø~~ (NH2G2) (FGN Alg 1)

Leçons : Voyage en algèbre Caldero

Théorème : Soient q une puissance d'un nombre premier et $\mathbb{F}_q$ le corps fini à q éléments. Notons $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables dans $\mathbb{F}_q$.

Alors $$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1+\dots+n_q=n \\ n_i\geq 0}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)|\dots|GL_{n_q}(\mathbb{F}_q)|}$$

et $$\frac{|\mathcal{D}_n(\mathbb{F}_q)|}{|\mathcal{M}_n(\mathbb{F}_q)|} \underset{q\to+\infty}{\sim} \frac{1}{n!}$$

Preuve : Avant de commencer, prenons quelques notations : on pose $\mathbb{F}_q=\{x_1,\dots,x_q\}$, et on appelle q-partition de n la donnée d'un $(n_1,\dots,n_q)$ d'entiers positifs tq $n_1+\dots+n_q=n$.

Pour λ une q-partition, on pose $D_\lambda = \mathrm{Diag}(\underbrace{x_1,\dots,x_1}_{n_1},\underbrace{x_2,\dots,x_2}_{n_2},\dots,\underbrace{x_q,\dots,x_q}_{n_q})$

On peut attaquer la preuve.

Il s'agit de voir que $GL_n(\mathbb{F}_q)$ agit sur $\mathcal{D}_n(\mathbb{F}_q)$ via $P\cdot M = PMP^{-1}$ (par conjugaison).

L'équation aux classes assure que :
$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{D\in\mathcal{R}} |\mathcal{O}(D)| = \sum_{D\in\mathcal{R}} \frac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}(D)|}$$
où $\mathcal{R}$ désigne un système de représentants des orbites.

Prenons $\mathcal{R}=\{D_\lambda,\ \text{pour } \lambda\ q\text{-partition de } n\}$.

Alors $$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1+\dots+n_q=n \\ n_i\geq 0}} \frac{|GL_n(\mathbb{F}_q)|}{|\mathrm{Stab}(D_\lambda)|}$$

En fait il reste juste à savoir ce qu'est $\mathrm{Stab}(D_\lambda)=\left\{\begin{matrix}P\in GL_n(\mathbb{F}_q),\\ PDP^{-1}=D\end{matrix}\right\}$

$P\in \mathrm{Stab}(D_\lambda) \Leftrightarrow PD=DP \Leftrightarrow P\in \underbrace{\mathcal{C}(D_\lambda)}_{\text{commutant}}\cap GL_n(\mathbb{F}_q)$

Or si $P\in\mathcal{C}(D_\lambda)$, P commute avec D_λ donc chaque sous-espace propre de D_λ est stable par P. Au vu de la forme choisie pour D_λ, on a P est de la forme $P=\begin{pmatrix} P_{n_1} & (0) & (0) \\ (0) & \ddots & (0) \\ (0) & (0) & P_{n_q}\end{pmatrix}$ où $P_{n_i}\in GL_{n_i}(\mathbb{F}_q)$ vu que P est inversible.

Réciproquement, les P de cette forme commutent avec D_λ donc

$$\mathrm{Com}(D_\lambda) \cap GL_n(\mathbb{F}_q) \underset{\uparrow \atop \lambda = (m_1, \dots, m_q)}{=} \begin{pmatrix} GL_{m_1}(\mathbb{F}_q) & & (0) \\ & \ddots & \\ (0) & & GL_{m_q}(\mathbb{F}_q) \end{pmatrix} \quad \text{(notation abusive)}$$

et donc $|\mathrm{Stab}(D_\lambda)| = |GL_{m_1}(\mathbb{F}_q)| \dots |GL_{m_q}(\mathbb{F}_q)|$

D'où la formule annoncée !

Reste maintenant à traiter l'asymptotique. Ce qui est embêtant c'est que dans $m_1 + \dots + m_q$, q apparaît de manière incontrôlable.

Remarquons que comme les matrices sont de taille n, il y a au plus n éléments $m_i \neq 0$.

Disons que pour une q-partition $(m_1, \dots, m_q)$, il y a m m_i non nuls avec $1 \leq m \leq n$.

Combien de façons de former cette q-partition ? Il y a $\binom{q}{q-m} = \binom{q}{m}$ choix pour les m_i qui valent 0.

Disons qu'on conserve l'ordre de ceux non nuls : la q-partition $(m_1, \dots, m_q)$ devient $(m_{i_1}, \dots, m_{i_m})$ où $m_{i_j} > 0$ et $m_{i_1} + \dots + m_{i_m} = n$.

Alors on peut écrire
$$|D_n(\mathbb{F}_q)| = \sum_{m=1}^{n} \binom{q}{m} \sum_{\substack{m_{i_1} + \dots + m_{i_m} = n \\ m_{i_j} > 0}} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{m_{i_1}}(\mathbb{F}_q)| \dots |GL_{m_{i_m}}(\mathbb{F}_q)|}$$

Il y a beaucoup de termes, mais ils restent en nombre fini, c'est un cardinal qui est fraction rationnelle en q. En fait c'est même un polynôme en q : Écrivons $|D_n(\mathbb{F}_q)| = \frac{A(q)}{B(q)}$ avec $A, B \in \mathbb{Z}[X]$. On fait la division euclidienne de A par B unitaire dans $\mathbb{Z}[X]$ (B est unitaire, cf forme de $|D_n(\mathbb{F}_q)|$) pour écrire que
$\frac{A(q)}{B(q)} = Q(q) + \frac{R(q)}{B(q)}$ et $\frac{R(q)}{B(q)}$ ne prend que des valeurs entières (c'est un cardinal) et tend vers 0 en $q \to +\infty$ (cf degré en q). Il est donc stationnaire et s'annule une infinité de fois ce qui assure que $R = 0$.

Il s'agit donc de trouver le terme de degré dominant pour avoir l'équivalent. Or le degré en q de $\binom{q}{m} \frac{|GL_n(\mathbb{F}_q)|}{|GL_{m_{i_1}}(\mathbb{F}_q)| \dots |GL_{m_{i_m}}(\mathbb{F}_q)|}$ est $m + n^2 - \sum_{j=1}^{m} m_{i_j}^2 \leq n + n^2 - \sum m_{i_j}^2 \leq n + n^2 - \sum m_{i_j} \leq n^2$ et il y a égalité quand $m = n$ et chaque m_i vaut 1. Le terme correspond est $\binom{q}{n} \cdot \frac{|GL_n(\mathbb{F}_q)|}{|GL_1(\mathbb{F}_q)|^n} \underset{q \to +\infty}{\sim} \frac{q^{n^2}}{q^n} \cdot \frac{q^n}{n!} = \frac{q^{n^2}}{n!}$.