Matrices diagonalisables dans $\mathbb{F}_q$.

Leçon : 101, 104, 123, ~~[illegible]~~, 155, 190

Ref : Histoire Hédoniste de Groupes et de Géométrie, tome 2 / Rombaldi

Théorème Le nombre d'éléments de $M_n(\mathbb{F}_q)$ diagonalisable est

$$\sum_{\substack{n_1,\dots,n_q \geq 0 \\ n_1+\dots+n_q=n}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{n_i}(\mathbb{F}_q)|}, \text{ où } |GL_0(\mathbb{F}_q)|=1.$$

Lemme Une matrice $A\in M_n(\mathbb{F}_q)$ est diagonalisable ssi $A^q=A$.

Démonstration

$\boxed{\Rightarrow}$ Soit $M\in M_n(\mathbb{F}_q)$ une matrice diagonalisable.

Alors son polynôme minimal est scindé à racines simples, donc

$\Pi_M(X)=\prod_{\lambda\in Sp(M)}(X-\lambda)$. Or $X^q-X=\prod_{\mu\in\mathbb{F}_q}(X-\mu)$, donc $\Pi_M(X)\mid X^q-X$

et donc $\boxed{M^q=M}$

$\boxed{\Leftarrow}$ Si $M^q=M$. Alors le polynôme X^q-X est scindé à racines simples sur $\mathbb{F}_q$ et annule M, donc M est diagonalisable

□

On note : $D_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables sur $\mathbb{F}_q$.

- Pour $k\in\mathbb{N}^*$ et $n_1,\dots,n_k\in\mathbb{N}$ tq $\sum_{i=1}^{k} n_i=k$

$$\mathcal{F}_{k,n_1,\dots,n_k}=\left\{E_1,\dots,E_k \text{ sev de } \mathbb{F}_q^{\,n},\ \begin{cases}\dim E_i=n_i\\ E_1\oplus\dots\oplus E_k=\mathbb{F}_q^{\,n}\end{cases}\right\}.$$

Lemme Si $n_1+\dots+n_k=n$, alors $|\mathcal{F}_{k,n_1,\dots,n_k}|=\dfrac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^{k}|GL_{n_i}(\mathbb{F}_q)|}$

Démonstration (on confond $GL_n(\mathbb{F}_q)$ et $GL(\mathbb{F}_q^{\,n})$)

On fait agir $GL_n(\mathbb{F}_q)$ sur l'ensemble de ses k-uplets, donc

$GL_n(\mathbb{F}_q) \curvearrowright \underbrace{\mathcal{F}_{k,n_1,\dots,n_k}}_{\text{on note } \mathcal{F}}$ via $P.(E_1,\dots,E_k)=(P(E_1),\dots,P(E_k))$

* L'action est bien définie car si $P\in GL_n(\mathbb{F}_q)$, alors $\dim E_i=\dim P(E_i)$.
* Montrons que cette action est transitive.

Soit $(E_i)_{1\leq i\leq k}, (F_i)_{1\leq i\leq k}\in\mathcal{F}$. Montrons qu'il existe $P\in GL_n(\mathbb{F}_q)$ tq $\forall i\in[\![1,k]\!]$ $P(E_i)=F_i$.

On a : $\begin{cases} E = F_1 \oplus \cdots \oplus F_k \\ E = E_1 \oplus \cdots \oplus E_k \end{cases}$, on se donne deux bases adaptées à chaque décomposition : $\begin{cases} \mathcal{B}_1 = \bigcup_{i=1}^{k} \mathcal{B}_1^i, \text{ adaptée à } (E_i)_i \\ \mathcal{B}_2 = \bigcup_{i=1}^{k} \mathcal{B}_2^i \text{ ——— } (F_i)_i \end{cases}$

$\forall i \in [\![1, k]\!]$ $\dim(E_i) = \dim(F_i) = m_i$, on peut donc définir $P \in GL_m(\mathbb{F}_q)$ par $P(\mathcal{B}_1^i) = \mathcal{B}_2^i$ $\forall i \in [\![1, k]\!]$.

Alors $\forall i \in [\![1, k]\!]$ $P(E_i) = F_i$, et $P \in GL_m(\mathbb{F}_q)$, il envoie une base sur une autre base.

L'action est donc transitive.

Ainsi, si $(E_i)_{1 \leq i \leq k} \in \mathcal{F}$, alors $\mathrm{Orb}_{GL_m(\mathbb{F}_q)}((E_i)_{1 \leq i \leq k}) = \mathcal{F}$.

Déterminons, pour $(E_i)_{1 \leq i \leq k}$, le stabilisateur.

Soit $P \in \mathrm{Stab}_{GL_m(\mathbb{F}_q)}(E_1, \dots, E_k)$. Alors pour tout $i \in [\![1, k]\!]$, $P(E_i) = E_i$, donc $P|_{E_i} \in GL_{m_i}(\mathbb{F}_q)$ ($\dim E_i = m_i$).

Réciproque, si $P \in GL_m(\mathbb{F}_q)$ tq $\forall i \in [\![1, k]\!]$ $P|_{E_i} \in GL_{m_i}(\mathbb{F}_q)$. Alors $P \in \mathrm{Stab}_{GL_m(\mathbb{F}_q)}((E_i)_i)$.

Donc $\mathrm{Stab}_{GL_m(\mathbb{F}_q)}(E_1, \dots, E_k) = \{P \in GL_m(\mathbb{F}_q) : \forall i \in [\![1, k]\!]\ P|_{E_i} \in GL_{m_i}(\mathbb{F}_q)\}$.

Par conséquent, $|\mathrm{Stab}_{GL_m(\mathbb{F}_q)}(E_1, \dots, E_k)| = \prod_{i=1}^{k} |GL_{m_i}(\mathbb{F}_q)|$.

Par la relation orbite-stabilisateur, on a

$$|\mathcal{F}| = \frac{|GL_m(\mathbb{F}_q)|}{\prod_{i=1}^{k} |GL_{m_i}(\mathbb{F}_q)|}.$$

□

Lemme Si $M \in \mathcal{D}_m(\mathbb{F}_q)$, alors $E = \bigoplus_{k=1}^{q} \mathrm{Ker}(M - \lambda_k I_m)$, où $\mathbb{F}_q = \{\lambda_1, \dots, \lambda_q\}$ | à mettre en 1ème

Démonstration

Les polynômes $X - \lambda_1, \dots, X - \lambda_q$ sont 2 à 2 premiers entre eux. Donc par le lemme des noyaux

$\mathrm{Ker}\,(M^q - M) = \bigoplus_{i=1}^{q} \mathrm{Ker}(M - \lambda_i I_m)$.

Or $M \in \mathcal{D}_m(\mathbb{F}_q) \iff M^q - M = 0$, donc $\mathrm{Ker}\,(M^q - M) = \mathbb{F}_q^{\,m}$. $\square$

<u>Démonstration</u> (du théorème)

On pose $\mathcal{H} = \{ E_1, \dots, E_q \text{ sev de } \mathbb{F}_q^{\,m} \text{ tq } \mathbb{F}_q^{\,m} = E_1 \oplus \dots \oplus E_q \}$.

Alors $\Phi : \mathcal{D}_m(\mathbb{F}_q) \to \mathcal{H}$ est une bijection.

$$D \mapsto (\mathrm{Ker}\,(D - \lambda_k I_m))_{1 \le k \le q}$$

→ injectivité : immédiat, $\Phi(D) = \Phi(D') \Rightarrow Dx = D'x \ \forall x \in \mathrm{Ker}\,(D - \lambda_k \mathrm{Id})$ $\forall k$

et $\mathbb{F}_q^{\,m} = \bigoplus_{i=1}^{k} \mathrm{Ker}\,(D - \lambda_k \mathrm{Id})$.

→ surjectivité : on définit D par $D|_{E_i} = \lambda_i I_m|_{E_i}$, on a bien $D \in \mathcal{D}_m(\mathbb{F}_q)$.

Donc
$$|\mathcal{D}_m(\mathbb{F}_q)| = |\mathcal{H}| = \sum_{\substack{m_1 + \dots + m_q = m \\ \forall i\ m_i \in \mathbb{N}}} |\mathcal{F}_{q, m_1, \dots, m_q}|$$

$$= \sum_{\substack{m_1 + \dots + m_q = m \\ \forall i\ m_i \in \mathbb{N}}} \frac{|GL_m(\mathbb{F}_q)|}{\prod_{i=1}^{q} |GL_{m_i}(\mathbb{F}_q)|} \quad \square$$

<u>Rmq</u> : - plutôt des "drapeaux" que des lemmes

- on peut juste prendre $k = q$ dans le 2ème lemme.
- commencer par le dénombrement de $|\mathcal{F}|$, c'est plus intéressant (surtout si c'est une leçon sur les actions de groupe).

Pour aller plus loin :

$g_n = |GL_n(\mathbb{F}_q)|$.

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{n_1+\dots+n_q=n \\ n_i \geq 0}} \frac{g_n}{\prod_{i=1}^{q} g_{n_i}}.$$

Si $(n_1,\dots,n_q) \vdash n$, soit m le nbr de $n_i \neq 0$.

Donc $1 \leq m \leq n$.

On peut réindexer et associer à $(n_1,\dots,n_q)$ le m-uplet $(n_{i_1},\dots,n_{i_m})$. On a $\sum_{k=1}^{m} n_{i_k} = n$.

Donc, comme par convention $g_0 = 1$, on a

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{m=1}^{n} \underbrace{\binom{q}{m}}_{\substack{\text{on choisit} \\ \text{les } q\text{-uplets avec } m \text{ termes} \\ \neq 0}} \sum_{\substack{\nu_1,\dots,\nu_m > 0 \\ \nu_1+\dots+\nu_m=n}} \frac{g_n}{\prod_{i=1}^{m} g_{\nu_i}}$$

Si $\pi(q) = \dfrac{|\mathcal{D}_n(\mathbb{F}_q)|}{|\mathcal{M}_n(\mathbb{F}_q)|} = q^{-n^2} |\mathcal{D}_n(\mathbb{F}_q)|$.

$\pi(q)$ est une fraction rationnelle en q.

$g_n = (q^n-1)\cdots(q^n-q^{n-1}) = q^{\frac{n}{2}(n-1)} (q^n-1)\cdots(q-1)$

↳ pol. de degré n^2 en q, et $\binom{q}{m} = \frac{1}{m!} q(q-1)\cdots(q-m+1)$

donc $\binom{q}{m} \frac{g_n}{\prod_{i=1}^{m} g_{\nu_i}}$ est de degré $m + (n^2 - \sum_{i=1}^{m} \nu_i^2) \leq m + n^2 - \sum_{i=1}^{m} \nu_i$
$\leq n^2$.

... $\pi(q) \to 1/n!$ (CVA)