Développement : Dénombrement des matrices diagonalisables dans $\mathbb{F}_q$

Algèbre & Géométrie

Référence : [ROM] Rombaldi J., *Mathématiques pour l'agrégation - Algèbre et géométrie,* ***2ème édition***, deoboek supérieur, 2021, p203
(Aussi disponible dans la première édition, p148)
Pour les leçons :
- 101 : Groupes opérant sur un ensemble. Exemples et applications.
- 103 : Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications. (À voir, ça a l'air abusif mais ça utilise des résultats sur la diagonalisabilité, qui peuvent être mis en lien avec une action par conjugaison sur des matrices...)
- 106 : Groupe linéaire d'un espace vectoriel de dimension finie E. Sous-groupes de $\mathrm{GL}(E)$. Applications.
- 123 : Corps finis. Applications.
- 150 : Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.
- 152 : Endomorphismes diagonalisables en dimension finie.
- 190 : Méthodes combinatoires, problèmes de dénombrement.

Soient $n \in \mathbb{N}^*$ et $q = p^m$, avec p premier et $m \in \mathbb{N}^*$. Soit E un $\mathbb{F}_q$-espace vectoriel de dimension n. On note $\mathcal{D}_n(\mathbb{F}_q)$ l'ensemble des matrices diagonalisables sur $\mathbb{F}_q$.
L'objectif de ce développement est de montrer le théorème suivant :

Théorème 1. ***Cardinal des matrices diagonalisables dans*** $\mathbb{F}_q$***.***

On a :

$$|\mathcal{D}_n(\mathbb{F}_q)| = \sum_{\substack{(m_1,\dots,m_q) \in \mathbb{N}^q \\ m_1+\cdots+m_q = n}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|}.$$

Preuve : Procédons par étapes. Notons $\lambda_1, \dots, \lambda_q$ les éléments de $\mathbb{F}_q$.
⋆ Étape 1 : Montrons que $\mathcal{D}_n(\mathbb{F}_q) = \{M \in \mathcal{M}_n(\mathbb{F}_q) \mid M^q = M\}$.
Si $M \in \mathcal{M}_n(\mathbb{F}_q)$ tel que $M^q = M$, alors $X^q - X$ est un polynôme annulateur de M, scindé à racines simples, puisque :

$$X^q - X = \prod_{i=1}^{q}(X - \lambda_i).$$

Donc $M \in \mathcal{D}_n(\mathbb{F}_q)$.
Réciproquement, si $M \in \mathcal{D}_n(\mathbb{F}_q)$, alors il existe $P \in \mathbb{F}_q[X]$ tel que $P(M) = 0$ avec P scindé à racines simples. Ses racines étant dans $\mathbb{F}_q$, on a $P \mid \prod_{i=1}^{q}(X - \lambda_i) = X^q - X$, ce qui prouve que $M^q = M$.
D'où l'égalité.

⋆ Étape 2 : Soit $A \in \mathcal{D}_n(\mathbb{F}_q)$. Montrons que $E = \bigoplus_{i=1}^{q} \mathrm{Ker}(A - \lambda_i I_n)$.

Par l'Étape 1, $X^q - X$ est annulateur de A, avec $X^q - X = \prod_{i=1}^{q}(X - \lambda_i)$. Les polynômes $(X - \lambda_i)_{i \in [\![1;q]\!]}$ sont premiers entre eux deux à deux. D'après le lemme des noyaux, il vient :

$$E = \bigoplus_{i=1}^{q} \mathrm{Ker}(A - \lambda_i I_n).$$

⋆ Étape 3 : Montrons que $\mathcal{D}_n(\mathbb{F}_q)$ est en bijection avec $\mathcal{F} := \left\{ (E_1, \dots, E_q) \text{ sous-espaces vectoriels de } E \mid E = \bigoplus_{i=1}^{q} E_i \right\}$.
Soit $\phi : \mathcal{D}_n(\mathbb{F}_q) \longmapsto \mathcal{F}$ définie par :

$$\forall M \in \mathcal{D}_n(\mathbb{F}_q) \quad \phi(M) = (\mathrm{Ker}(M - \lambda_i I_n))_{i \in [\![1;q]\!]}.$$

L'Étape 2 assure que ϕ est bien définie.
$\longrightarrow$ ϕ est injective : En effet, si $(M, N) \in \mathcal{D}_n(\mathbb{F}_q)^2$ tel que $\phi(M) = \phi(N)$, alors pour tout $i \in [\![1; q]\!]$, on a :

$$\mathrm{Ker}(M - \lambda_i I_n) = \mathrm{Ker}(N - \lambda_i I_n).$$

Soit $(e_1, \dots, e_r)$ une base de vecteurs propres de M (existe bien car M est diagonalisable). Pour $i \in [\![1; r]\!]$, il existe $\lambda_i \in \mathbb{F}_q$ tel que $e_i \in \mathrm{Ker}(M - \lambda_i I_n)$, et donc :

$$Me_i = \lambda_i e_i = Ne_i.$$

Ainsi, $M = N$.
$\longrightarrow$ ϕ est surjective : Soit $E_0 = (E_1, \dots, E_q) \in \mathcal{F}$. Soit $u \in \mathcal{L}(E)$ l'endomorphisme défini par :

$$\forall i \in [\![1; q]\!] \quad u_{|E_i} : x \longmapsto \lambda_i x.$$

Notons M sa matrice dans une base adaptée à la décomposition E_0 de E. On a bien que M est diagonalisable avec $\phi(M) = E_0$.
D'où le résultat.
$\star$ Étape 4 : Calculons $|\mathcal{F}|$. Pour cela, faisons agir $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\mathcal{F}$ par :

$$\forall (M, (E_1, \dots, E_q)) \in \mathrm{GL}_n(\mathbb{F}_q) \times \mathcal{F} \quad M \cdot (E_1, \dots, E_q) = (M(E_1), \dots, M(E_q)).$$

Si $M \in \mathrm{GL}_n(\mathbb{F}_q)$, l'action est bien définie. Soit $E_0 = (E_1, \dots, E_q) \in \mathcal{F}$.
$\longrightarrow$ Étude de l'orbite de E_0, $\mathcal{O}_{E_0}$: On a $\mathcal{O}_{E_0} = \{(F_1, \dots, F_q) \in \mathcal{F} \mid \forall i \in [\![1; q]\!] \quad \dim(E_i) = \dim(F_i)\}$.
En effet, l'inclusion directe est claire.
Réciproquement, si $F_0 := (F_1, \dots, F_q) \in \mathcal{F}$ tel que pour $i \in [\![1; q]\!]$, $\dim(E_i) = \dim(F_i)$, alors soit $\mathcal{B} = (\mathcal{B}_1, \dots, \mathcal{B}_q)$ une base adaptée à la décomposition E_0 de E, ainsi qu'une autre base $\mathcal{B}' = (\mathcal{B}'_1, \dots, \mathcal{B}'_q)$ adaptée à la décomposition F_0 de E.
Soit $u \in \mathcal{L}(E)$ l'endomorphisme défini par :

$$\forall i \in [\![1; q]\!] \quad u(\mathcal{B}_i) = \mathcal{B}'_i.$$

Autrement dit, la matrice M de u dans la base $\mathcal{B}$ est la matrice de passage de la base $\mathcal{B}$ à la base $\mathcal{B}'$.
On a donc $M \in \mathrm{GL}_n(\mathbb{F}_q)$, et $(M(E_1), \dots, M(E_q)) \in \mathcal{O}_{E_0}$.
D'où l'égalité de l'orbite.
$\longrightarrow$ Étude du stabilisateur de $E_0 := (E_1, \dots, E_q) \in \mathcal{F}$: Si $M \in \mathrm{GL}_n(\mathbb{F}_q)$, on a :

$$(\forall i \in [\![1; q]\!] \quad M(E_i) = E_i) \iff \left(\forall i \in [\![1; q]\!] \quad \exists M_i \in \mathrm{GL}_{\dim(E_i)}(\mathbb{F}_q) \quad M = \begin{pmatrix} M_1 & & (0) \\ & \ddots & \\ (0) & & M_q \end{pmatrix} \right).$$

Donc :

$$\begin{aligned} \mathrm{Stab}(E_0) &= \{M \in \mathrm{GL}_n(\mathbb{F}_q) \mid \forall i \in [\![1; q]\!] \quad M(E_i) = E_i\} \\ &= \left\{M \in \mathrm{GL}_n(\mathbb{F}_q) \mid \forall i \in [\![1; q]\!] \quad M_i \in \mathrm{GL}_{\dim(E_i)}(\mathbb{F}_q)\right\} \\ &\simeq \prod_{i=1}^{q} \mathrm{GL}_{\dim(E_i)}(\mathbb{F}_q). \end{aligned}$$

$\star$ Étape 5 : Concluons.
Notons Ω l'ensemble des représentants des orbites. D'après l'Étape 4, cet ensemble est en bijection avec :

$$\left\{(m_1, \dots, m_q) \in \mathbb{N}^q \mid \sum_{i=1}^{q} m_i = n\right\}.$$

L'équation aux classes et les résultats précédents fournissent enfin :

$$\begin{aligned} |\mathcal{D}_n(\mathbb{F}_q)| &= |\mathcal{F}| \\ &= \sum_{E_0 \in \Omega} |\mathcal{O}_{E_0}| \\ &= \sum_{E_0 \in \Omega} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Stab}(E_0)|} \\ &= \sum_{\substack{(m_1, \dots, m_q) \in \mathbb{N}^q \\ m_1 + \cdots + m_q = n}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(\mathbb{F}_q)|}, \end{aligned}$$

puisque, si $E_0 \in \Omega$, $\sum_{i=1}^{q} \dim(E_i) = n$.
Cela achève la preuve. □