

2 Développements d'algèbre

2.1 Dénombrement des matrices diagonalisables sur un corps fini

Références :

- Philippe Caldéro, Jérôme Germoni : *Nouvelles histoires hédonistes de groupes et de géométries*, Tome Second, pages 66-67
- Jean-Etienne Rombaldi : *Algèbre et Géométrie*, pages 148 à 151

Couplé avec les leçons : 101, 106, 123, 152, 190

Théorème :

Soient p un nombre premier et $n \in \mathbb{N}^*$, on pose $q = p^n$. Notons $\mathbb{F}_q$ le corps fini à q éléments et $D_n(\mathbb{F}_q)$ le nombre de matrices diagonalisables de $\mathcal{M}_n(\mathbb{F}_q)$. On a :

$$|D_n(\mathbb{F}_q)| = \sum_{\substack{n_1 + \dots + n_q = n \\ (n_1, \dots, n_q) \in \mathbb{N}^q}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^q |GL_{n_i}(\mathbb{F}_q)|}$$

Preuve :

Posons $\mathcal{F}$ l'ensemble des q -uplets $(E_1, \dots, E_k)$ de sous-espaces vectoriels de $\mathbb{F}_q^n$ tels que $\bigoplus_{i=1}^q E_i = \mathbb{F}_q^n$.

Et pour $(n_i)_{1 \leq i \leq q} \in \mathbb{N}^q$ tel que $\sum_{i=1}^q n_i = n$ on pose $\mathcal{F}_{(n_i)} := \{(E_i)_{1 \leq i \leq q} \in \mathcal{F} \mid \forall i \in \llbracket 1, q \rrbracket, \dim(E_i) = n_i\}$.

Posons $\mathbb{F}_q = \{\lambda_1, \dots, \lambda_q\}$. On montre d'abord qu'il y a une bijection entre $\mathcal{M}_n(\mathbb{F}_q)$ et $\mathcal{F}$.

On considère $\varphi : \begin{cases} D_n(\mathbb{F}_q) & \longrightarrow \mathcal{F} \\ A & \longmapsto E_A := (\text{Ker}(A - \lambda_i I_n))_{1 \leq i \leq q} \end{cases}$

D'une part, soit $A \in D_n(\mathbb{F}_q)$, pour $k \in \llbracket 1, q \rrbracket$, en posant $n_k := \dim(\text{Ker}(A - \lambda_k I_n))$, on a $E_A \in \mathcal{F}_{(n_i)} \subseteq \mathcal{F}$, car A est diagonalisable, .

D'autre part, soit $(E_i)_{1 \leq i \leq q} \in \mathcal{F}$, on définit l'endomorphisme $\Psi_{(E_i)} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ défini par :

$$\forall j \in \llbracket 1, q \rrbracket, \forall x_j \in E_j, \Psi_{(E_i)}(x_j) = \lambda_j x_j$$

Pour $\mathcal{B}$ une base de $\mathbb{F}_q^n$ adaptée à $(E_i)_{1 \leq i \leq q}$, la matrice $A_{(E_i)} = \text{Mat}_{\mathcal{B}}(\Psi_{(E_i)})$ est diagonale, par construction. Ainsi $\text{Mat}_{\mathcal{B}_{\text{can}}}(\Psi_{(E_i)})$ (avec $\mathcal{B}_{\text{can}}$ désignant la base canonique) est diagonalisable.

$\psi : \begin{cases} \mathcal{F} & \longrightarrow D_n(\mathbb{F}_q) \\ (E_i)_{1 \leq i \leq q} & \longmapsto \text{Mat}_{\mathcal{B}_{\text{can}}}(\Psi_{(E_i)}) \end{cases}$ est réciproque de φ . On a donc $|D_n(\mathbb{F}_q)| = |\mathcal{F}|$.

Les $\mathcal{F}_{(n_i)}$ forment une partition de $\mathcal{F}$, nous allons donc les dénombrer. Pour ce faire, on considère l'action de groupe suivante :

$$\begin{cases} GL_n(\mathbb{F}_q) \times \mathcal{F}_{(n_i)} & \longrightarrow \mathcal{F}_{(n_i)} \\ (g, (E_i)_{1 \leq i \leq q}) & \longmapsto g \cdot (E_i)_{1 \leq i \leq q} := (g((E_i)_{1 \leq i \leq q})) \end{cases}$$

Vérifions d'abord que cette action est bien définie.

Premièrement, nous avons pour tout $i \in \llbracket 1, q \rrbracket$, $\dim(g(E_i)) = \dim(E_i) = n_i$.

De plus, on a les $g(E_i)$ qui sont en somme directe. En effet, soient $(j, l) \in \llbracket 1, q \rrbracket^2$ avec $j \neq l$, soit $x \in g(E_j) \cap g(E_l)$, on a alors $g^{-1}1(x) \in E_j \cap E_l = \{0\}$ donc $x = 0$.

Finalement, les axiomes d'action de groupe se vérifient facilement :

$$\forall (g, g') \in GL_n(\mathbb{F}_q)^2, \forall (E_i) \in \mathcal{F}_{(n_i)}, \text{ on a } \begin{cases} g \cdot (g'(E_i)) = gg' \cdot (E_i) \\ \text{et } I_n \cdot (E_i) = (E_i) \end{cases}$$

Montrons maintenant que cette action est transitive.

Soient $((E_i)_{1 \leq i \leq q}, (E'_i)_{1 \leq i \leq q}) \in \mathcal{F}_{(n_i)}^2$. On prend $\mathcal{B}$ une base de $\mathbb{F}_q^n$ adaptée à $(E_i)_{1 \leq i \leq q}$ et respectivement $\mathcal{B}'$ adaptée à $(E'_i)_{1 \leq i \leq q}$ et on considère la matrice $g \in GL_n(\mathbb{F}_q)$ qui envoie $\mathcal{B}$ sur $\mathcal{B}'$. Nous avons bien $g(E_i)_{1 \leq i \leq q} = (E'_i)_{1 \leq i \leq q}$. Cette action n'admet alors qu'une seule orbite.

Quant aux stabilisateurs de cette action ; pour $(E_i)_{1 \leq i \leq q} \in \mathcal{F}_{(n_i)}$, son stabilisateur est le sous-groupe de $GL_n(\mathbb{F}_q)$ qui stabilise tous les E_i : c'est le sous-groupe de matrices diagonales par blocs :

$$\prod_{i \in \llbracket 1, q \rrbracket} GL(E_i) = \prod_{i \in \llbracket 1, q \rrbracket} GL_{n_i}(\mathbb{F}_q)$$

Pour $(n_i)_{1 \leq i \leq q} \in \mathbb{N}^q$ tel que $\sum_{i=1}^q n_i = n$, d'après la formule des classes, sachant qu'il n'y a qu'une orbite, nous avons :

$$|\mathcal{F}_{(n_i)}| = \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^q |GL_{n_i}(\mathbb{F}_q)|}$$

Finalement,

$$|\mathcal{F}| = \sum_{\substack{n_1 + \dots + n_q = n \\ (n_1, \dots, n_q) \in \mathbb{N}^q}} |\mathcal{F}_{(n_i)}| = \sum_{\substack{n_1 + \dots + n_q = n \\ (n_1, \dots, n_q) \in \mathbb{N}^q}} \frac{|GL_n(\mathbb{F}_q)|}{\prod_{i=1}^q |GL_{n_i}(\mathbb{F}_q)|}$$

□