Développement 10. Nombre d'endomorphismes diagonalisables sur un corps fini

Le lemme suivant, nécessaire à la preuve, est l'exercice 2 page 178 du livre [2]. La preuve théorème principal est une adaptation de l'exercice 1.9 page 17 du livre [1].

Lemme 1. Soit $A \in \mathscr{M}_n(\mathbf{F}_q)$. Alors la matrice A est diagonalisable si et seulement si elle est annulée par le polynôme $X^q - X \in \mathbf{F}_q[X]$. En particulier, lorsque A est inversible, elle est diagonalisable si et seulement si $A^{q-1} = I_n$.

Preuve Remarquons d'abord que

$$X^q - X = \prod_{\alpha \in \mathbf{F}_q} (X - \alpha). \tag{1}$$

En effet, le corps $\mathbf{F}_q$ étant de cardinal q, tout élément $\alpha \in \mathbf{F}_q$ est une racine du polynôme $X^q - X$. Pour des raisons de degré, on obtient l'égalité (1).

On sait que la matrice A est diagonalisable si et seulement s'il est annulé par un polynôme scindé simple sur $\mathbf{F}_q$, c'est-à-dire si et seulement s'il existe un polynôme annulateur $P \in \mathbf{F}_q[X]$ tel que $P \mid X^q - X$. Ceci conclut le lemme. ◁

Théorème 2. Le nombre de matrices diagonalisables de $\mathrm{GL}_n(\mathbf{F}_q)$ vaut

$$\sum_{\substack{(n_1,\dots,n_{q-1}) \in \mathbf{N}^{q-1} \\ n_1+\cdots+n_{q-1}=n}} \frac{|\mathrm{GL}_n(\mathbf{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbf{F}_q)| \cdots |\mathrm{GL}_{n_{q-1}}(\mathbf{F}_q)|}.$$

Preuve Notons $\mathrm{D}_n(q) \subset \mathrm{GL}_n(\mathbf{F}_q)$ l'ensemble des matrices diagonalisables. Avec le lemme 1, ce dernier s'écrit

$$\mathrm{D}_n(q) = \{A \in \mathscr{M}_n(\mathbf{F}_q) \mid A^{q-1} = I_n\}.$$

Soit $A \in \mathrm{D}_n(q)$. Comme pour montrer l'égalité (1), le polynôme $X^{q-1} - X$ s'écrit de la manière

$$X^{q-1} - 1 = \prod_{\alpha \in \mathbf{F}_q^\times} (X - \alpha)$$

et le lemme des noyaux donne alors

$$\mathbf{F}_q^n = \bigoplus_{\alpha \in \mathbf{F}_q^\times} \mathrm{Ker}(A - \alpha I_n). \tag{2}$$

On note $\mathscr{F}$ l'ensemble des $q-1$-uplets $(E_1, \dots, E_{q-1})$ de sous-espaces vectoriels de $\mathbf{F}_q^n$ qui vérifient $\mathbf{F}_q^n = E_1 \oplus \cdots \oplus E_{q-1}$. L'égalité (2) autorise la définition de l'application

$$f : \left| \begin{array}{l} \mathrm{D}_n(q) \longrightarrow \mathscr{F}, \\ \quad A \longmapsto (\mathrm{Ker}(A - \alpha I_n))_{\alpha \in \mathbf{F}_q^\times}. \end{array} \right.$$

Vérifions qu'il est bijectif. Une matrice diagonalisable $A \in \mathrm{D}_n(q)$ étant caractérisée par ses sous-espaces propres, l'application f est injective. Pour sa surjectivité, considérons une famille $(E_1, \dots, E_{q-1}) \in \mathscr{F}$. Pour tout indice $i \in [\![1, q-1]\!]$, on note $A_i \in \mathrm{D}_n(q)$ la matrice de la projection de $\mathbf{F}_q^n$ sur E_i. Alors $f(\mathrm{diag}(A_1, \dots, A_q)) = (E_1, \dots, E_{q-1})$.

Ceci conclut la bijectivité. Comme les ensembles

$$\mathscr{F}(n_1, \dots, n_{q-1}) \coloneqq \{(E_1, \dots, E_{q-1}) \in \mathscr{F} \mid \forall i \in [\![1, q]\!],\ \dim E_i = n_i\}$$

avec des entiers $n_1, \dots, n_{q-1} \in \mathbf{N}$ vérifiant $n_1 + \cdots + n_{q-1} = n$ forment une partition de l'ensemble $\mathscr{F}$, il suffit de calculer leurs cardinaux.

Soient $n_1, \dots, n_{q-1} \in \mathbf{N}$ des entiers vérifiant $n_1 + \cdots + n_{q-1} = n$. Dénombrons l'ensemble $\mathscr{F}' \coloneqq \mathscr{F}(n_1, \dots, n_{q-1})$. Le groupe $G \coloneqq \mathrm{GL}(\mathbf{F}_q^n)$ agit sur l'ensemble $\mathscr{F}'$ par l'action définie par l'égalité

$$g \cdot (E_1, \dots, E_{q-1}) = (g(E_1), \dots, g(E_{q-1})), \qquad g \in G,\ (E_1, \dots, E_{q-1}) \in \mathscr{F}'.$$

Montrons que cette action est transitive. Soient $(E_1, \dots, E_{q-1}), (F_1, \dots, F_{q-1}) \in \mathscr{F}'$. Pour tout indice $i \in [\![1, q-1]\!]$, on prend une base $\mathscr{B}_i$ de E_i et une base $\mathscr{C}_i$ de F_i. On sait qu'il existe un isomorphisme $g \in G$ envoyant toute base $\mathscr{B}_i$ avec $i \in [\![1, q-1]\!]$ sur la base $\mathscr{C}_i$. Alors $g \cdot (E_1, \dots, E_{q-1}) = (F_1, \dots, F_{q-1})$. L'action est donc transitive. En particulier, elle ne contient qu'une seule orbite. Il s'agit alors de calculer le stabilisateur d'un élément quelconque $(E_1, \dots, E_{q-1}) \in \mathscr{F}'$. On reprend les bases $\mathscr{B}_i$ et on note $\mathscr{B}$ leur concaténation. Alors un isomorphisme $g \in G$ stabilise la famille $(E_1, \dots, E_{q-1})$ si et seulement si sa matrice dans la base $\mathscr{B}$ est de la forme

$$\mathrm{diag}(M_1, \dots, M_{q-1}) \quad \text{avec} \quad M_i \in \mathrm{GL}_{n_i}(\mathbf{F}_q).$$

Ainsi le cardinal du stabilisateur de la famille $\{E_1, \dots, E_{q-1}\}$ vaut

$$|\mathrm{Stab}_G(E_1, \dots, E_{q-1})| = |\mathrm{GL}_{n_1}(\mathbf{F}_q)| \times \cdots \times \left|\mathrm{GL}_{n_{q-1}}(\mathbf{F}_q)\right|.$$

L'action étant transitive, on en déduit

$$|\mathscr{F}'| = |\mathrm{Orb}_G(E_1, \dots, E_{q-1})| = \frac{|G|}{|\mathrm{Stab}_G(E_1, \dots, E_{q-1})|}.$$

Grâce à la partition, on obtient

$$|\mathscr{F}| = \sum_{\substack{(n_1,\dots,n_{q-1}) \in \mathbf{N}^{q-1} \\ n_1+\cdots+n_{q-1}=n}} |\mathscr{F}(n_1, \dots, n_{q-1})|$$

et la bijection f permet de conclure. ◁

Remarque. Pour calculer le cardinal du groupe $\mathrm{GL}_n(\mathbf{F}_q)$, on peut dénombrer les bases du $\mathbf{F}_q$-espace vectoriel $\mathbf{F}_q^n$ pour obtenir la formule

$$|\mathrm{GL}_n(\mathbf{F}_q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

[1] Serge Francinou, Hervé Gianella et Serge Nicolas. *Exercices de mathématiques. Oraux X-ENS. Algèbre 1*. Cassini, 2001.

[2] Xavier Gourdon. *Algèbre*. 2e édition. Ellipses, 2009.