Nombre d'endomorphismes diagonalisables sur un corps fini

On note comme d'habitude $\mathbb{F}_q$ un corps à q éléments où q est une puissance d'un nombre premier p ; $\alpha_1, \ldots, \alpha_q$ désigneront les q éléments de $\mathbb{F}_q$.

Soit E un $\mathbb{F}_q$-espace vectoriel de dimension finie n. Le nombre d'endomorphismes diagonalisables de E est :

$$\sum_{\substack{(m_1,\ldots,m_q)\in\mathbb{N}^q \\ m_1+\cdots+m_q=n}} \frac{|\mathbf{GL_n}(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathbf{GL}_{m_i}(\mathbb{F}_q)|}$$

avec par convention $|\mathbf{GL_0}(\mathbb{F}_q)| = 1$.

Plan de la démonstration

1) Un endomorphisme f de E est diagonalisable si, et seulement si, $f^q = f$.

2) Puisque $X^q - X = \prod_{\alpha\in\mathbb{F}_q} (X - \alpha)$ (voir théorie des corps finis : $\mathbb{F}_q$ peut être vu comme un corps de décomposition sur $\mathbb{F}_p$ de $X^q - X$), f est diagonalisable si, et seulement si, $E = \bigoplus_{\alpha\in\mathbb{F}_q} \ker(f - \alpha\mathrm{Id}_E)$ (où certains des termes de cette somme directe peuvent être nuls). Notons $\mathcal{D}(E)$ l'ensemble des endomorphismes de E diagonalisables, $\mathcal{S}$ l'ensemble défini par

$$\mathcal{S} = \left\{(E_1, \ldots, E_q) \,/\, E_i \text{ s.e.v. de } E \text{ et } E = \bigoplus_{i=1}^{q} E_i\right\}$$

et $\Phi : \mathcal{D}(E) \to \mathcal{S}$ l'application qui, à f, associe $\big(\ker(f - \alpha_1\mathrm{Id}_E), \ldots, \ker(f - \alpha_q\mathrm{Id}_E)\big)$. Alors Φ est bijective.

3) Le groupe linéaire $\mathrm{GL}(E)$ agit sur $\mathcal{S}$ par $u \cdot (E_1, \ldots, E_q) = \big(u(E_1), \ldots, u(E_q)\big)$: le cardinal de $\mathcal{S}$ est égal à la somme du cardinal des différentes orbites pour cette action.

4) L'orbite d'un élément $\varepsilon = (E_1, \ldots, E_q)$ sous cette action est

$$\mathrm{orb}(\varepsilon) = \left\{(F_1, \ldots, F_q) \in \mathcal{S} \,/\, \dim F_i = \dim E_i\right\}.$$

5) Le cardinal du stabilisateur d'un élément $(E_1, \ldots, E_q)$ de $\mathcal{S}$ vaut $\prod_{i=1}^{q} \big|\mathrm{GL}_{m_i}(\mathbb{F}_q)\big|$ où $m_i = \dim E_i$.

6) Nous pouvons conclure comme suit. D'après le point 4, une orbite est caractérisée par un élément $(m_1, \ldots, m_q)$ de $\mathbb{N}^q$ vérifiant $m_1 + \cdots + m_q = n$. Puisque le cardinal de l'orbite d'un élément ε de $\mathcal{S}$ est égal à $\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{Stab}(\varepsilon)|}$, on déduit des points 2 et 5 :

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

Démonstration du point 1)

f est diagonalisable si, et seulement si, son polynôme minimal μ_f est scindé à racines simples sur $\mathbb{F}_q$ donc si, et seulement si, il existe $\lambda_1, \ldots, \lambda_s$ deux à deux distincts dans $\mathbb{F}_q$ tels que $\mu_f = \prod_{i=1}^{s} (X - \lambda_i)$.

Mais $X^q - X = \prod_{\alpha\in\mathbb{F}_q} (X - \alpha)$ donc f est diagonalisable si, et seulement si, μ_f divise $X^q - X$, c'est-à-dire $X^q - X$ annule f. Ce dernier point signifie que $f^q = f$.

Démonstration du point 2)

• Φ est injective car les sous-espaces propres d'un endomorphisme diagonalisable le caractérisent.

• Si $(E_1, \dots, E_q)$ est une famille de sous-espaces vectoriels de E vérifiant $E = \bigoplus_{i=1}^{q} E_i$, alors l'endomorphisme de E défini par $f(x) = \alpha_i x$ si $x \in E_i$ est diagonalisable avec $\ker(f - \alpha_i \mathrm{Id}_E) = E_i$. Ceci montre que Φ est surjectif.

Démonstration du point 4)

Bien sûr, pour $u \in GL(E)$, on a $\dim u(E_i) = \dim E_i$. Réciproquement, considérons un élément $(F_1, \dots, F_q)$ de $\mathcal{S}$ tel que $\dim F_i = \dim E_i$ pour chaque i. Si $e = (e_1, \dots, e_n)$ et $f = (f_1, \dots, f_n)$ sont deux bases de E compatibles respectivement avec les décompositions $E = \bigoplus_{i=1}^{q} E_i$ et $E = \bigoplus_{i=1}^{q} F_i$, (*ie* $(e_1, \dots, e_{m_1})$ est une base de E_1, $(e_{m_1+1}, \dots, e_{m_1+m_2})$ est une base de E_2, *etc*) alors $u \in \mathrm{GL}(E)$ défini par $u(e_i) = f_i$ envoie chaque E_i sur F_i.

Démonstration du point 5)

Fixons une base e de E compatible avec la décomposition $E = \bigoplus_{i=1}^{q} E_i$. Un automorphisme u de E est dans le stabilisateur de $(E_1, \dots, E_q)$ si, et seulement si, $u(E_i) = E_i$ pour tout i. Ainsi, la matrice d'un tel u dans la base e est de la forme $\mathrm{diag}(A_1, \dots, A_q)$ avec $A_i \in \mathrm{GL}_{m_i}(\mathbb{F}_q)$. Il est alors aisé de voir que l'application $\Psi : \mathrm{Stab}(E_1, \dots, E_q) \to \mathrm{GL}_{m_1}(\mathbb{F}_q) \times \cdots \times \mathrm{GL}_{m_q}(\mathbb{F}_q)$, qui à u associe le q-uplet $(A_1, \dots, A_q)$ ainsi défini, est bijective : elle est injective car l'ensemble des A_i déterminent entièrement u et surjective car, $(A_1, \dots, A_q)$ étant donné, on définit un automorphisme u de E en posant $[u]_b = \mathrm{diag}(A_1, \dots, A_q)$ et, par construction, cet automorphisme vérifie $u(E_i) = E_i$.

Bibliographie

[1] P. Caldero et J. Germoni – *Histoires hédonistes de groupes et de géométries - Tome premier*, Calvage & Mounet, 2013.

[2] S. Francinou, H. Gianella et S. Nicolas – *Exercices de mathématiques. Oraux-XENS, algèbre 1*, Cassini, 2001.

(pages 264-265 pour [1] et exercice 1.9 pour [2] : dans ce dernier cas, il ne s'agit pas de la même question, mais les idées les mêmes.)

Leçons

101 - Groupe opérant sur un ensemble. Exemples et applications.
123 - Corps finis. Applications.
154 - Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.
155 - Endomorphismes diagonalisables en dimension finie.
190 - Méthodes combinatoires, problèmes de dénombrement.