Nombre d'endomorphismes diagonalisables sur un corps fini

Théorème : Soit $n \in \mathbb{N}$ et q une puissance d'un nombre premier. Le nombre de matrices diagonalisables (dont on note $D(\mathbb{F}_q^n)$ l'ensemble de ces éléments) sur $\mathcal{M}_n(\mathbb{F}_q)$ est

$$\sum_{\substack{(n_1,...,n_q) \geq 0 \\ n_1+...+n_q=n}} \frac{|GL_n(\mathbb{F}_q|)}{|GL_{n_1}(\mathbb{F}_q)|...|GL_{n_q}(\mathbb{F}_q|)}$$

Preuve du théorème :

Étape 1 : Une matrice M est diagonalisable si et seulement si $M^q = M$

On sait que M est diagonalisable si et seulement si son polynôme minimal μ_M est scindé à racines simples sur $\mathbb{F}_q$. Or $X^q - X = \prod_{\alpha \in \mathbb{F}_q} X - \alpha$ donc μ_M est scindé à racines simples si et seulement si μ_M divise $X^q - X$ ce qui est équivalent à $M^q = M$.

Étape 2 : L'application ϕ est bijective où

$$\phi : \begin{array}{ccc} D(\mathbb{F}_q^n) & \to & S := \{(E_1,...,E_q) : E_i \text{ sous ev de } \mathbb{F}_q^n, \oplus E_i = \mathbb{F}_q^n\} \\ M & \mapsto & (\ker(M - \alpha_1 \mathrm{Id}),...,\ker(M - \alpha_q \mathrm{Id})) \end{array}$$

où les α_i décrivent $\mathbb{F}_q$.
D'après l'étape 1 on sait que si M est diagonalisable le lemme des noyaux nous dit que

$$\mathbb{F}_q^n = \bigoplus_{\alpha_i} \ker(M - \alpha_i \mathrm{Id}).$$

L'application ϕ est donc bien définie.

L'injectivité vient du fait qu'un endomorphisme diagonalisable est entièrement caractérisé par ses sous-espaces propres (ça se voit bien avec une base de vecteurs propres par exemple).

Soit $(E_1,...,E_q) \in S$. On peut alors définir $f : x \in \mathbb{F}_q^n \mapsto \alpha_i x$ si $x \in E_i$. C'est suffisant pour définir f car elle est linéaire et on l'a, en particulier, définie sur un base. Ainsi, la matrice M associée à f est diagonalisable et est d'image $(E_1,...,E_q)$ par ϕ.

Étape 3 : On s'intéresse aux orbites de l'action de $GL(\mathbb{F}_q^n)$ sur S

Il est clair que $GL(\mathbb{F}_q^n)$ agit sur S par $M((E_1,...,E_q)) = (M(E_1),...,M(E_q))$. Comme les orbites d'une action forment une partition, on sait que

$$|S| = \sum_{E \in S'} |\text{orb}(E)| \text{ où } S' \subset S \text{ est un système de représentant des orbites.}$$

On peut remarquer que $\text{orb}((E_1, ..., E_q)) = \{(F_1, ..., F_q) : \dim(F_i) = \dim(E_i) \, \forall \, 1 \leq i \leq q\}$. En effet si M est inversible il est clair que $\dim(M(E_i)) = \dim(E_i)$. Réciproquement, si on se donne $(E_1, ..., E_q)$ et $(F_1, ..., F_q)$ tels que $\dim(E_i) = \dim(F_i)$ pour tout i, on peut se donner des bases cohérentes $(e_1, ..., e_n)$ et $(f_1, ..., f_n)$ et il suffit de prendre M qui envoie e_i sur f_i (M est alors bien inversible et envoie E_i sur F_i).

Étape 4 : On s'intéresse aux stabilisateurs de l'action

Soit $E = (E_1, .., E_q) \in S$. On se donne $\mathcal{B} = (e_1, ..., e_n)$ une base cohérente à E. On sait alors que $M \in \text{stab}(E)$ ssi $M(E_i) = E_i$ pour tout $1 \leq i \leq q$. Cela implique qu'un élément $M \in \text{stab}(E)$ est diagonalisable par blocs et on peut donc écrire $M = \text{Diag}(A_1, ..., A_q)$ avec $A_i \in GL_{\dim E_i}(\mathbb{F}_q)$. On peut alors correctement définir l'application

$$\psi : \begin{array}{ccc} \text{Stab}(E_1, ..., E_q) & \to & GL_{\dim E_1}(\mathbb{F}_q) \times ... \times GL_{\dim E_q}(\mathbb{F}_q) \\ \text{Diag}(A_1, ..., A_q) & \mapsto & (A_1, ..., A_q) \end{array}.$$

Il se trouve que cette application est bijective. L'injectivité vient du fait qu'une matrice diagonale par blocs est entièrement déterminée par ses blocs diagonaux (on est pas loin de la tautologie là...) et la surjectivité vient du fait qu'une matrice de la forme $\text{Diag}(A_1, ..., A_q)$ avec les A_i dans $GL_{\dim E_i}(\mathbb{F}_q)$ est dans $\text{Stab}(E_1, ..., E_q)$ par définition. On vient ainsi de montrer que

$$|\text{Stab}((E_1, ..., E_q)) = \prod |GL_{\dim E_i}(\mathbb{F}_q)|.$$

Étape 5 : Conclusion

Par l'étape 2 on sait que $|D(\mathbb{F}_q^n)| = |S|$. Par l'étape 4 on sait que $|\text{orb}(E)| = \dfrac{|GL_n(\mathbb{F}_q)|}{|\text{Stab}(E)|}$ et par l'étape 3 il vient alors

$$|D(\mathbb{F}_q^n)| = |S| = \sum_{E \in S'} |\text{orb}(E)| = \sum_{E \in S'} \frac{|GL_n(\mathbb{F}_q)|}{\prod |GL_{\dim E_i}(\mathbb{F}_q)|}$$

où la dernière somme porte en fait que les n-uplets $(n_1, ..., n_q)$ vérifiant $n_1 + ... + n_q = n$ par l'étude des différentes orbites faite en étape 3.□

Remarques importantes :

- Je ne pense pas avoir été très malin à vouloir tout faire avec des matrices, c'est sans doute mieux de faire avec les endomorphismes (ou du moins, un meilleur mélange)
- Quand je parle de "base cohérente" c'est dans le sens "union de bases des E_i non réduit à $\{0\}$"
- Vérifiez que vous êtes au clair sur la raison de $X^q - X = \prod_{\alpha \in \mathbb{F}_q} X - \alpha$