

Dénombrement des matrices diag. de $\text{dim}(\mathbb{F}_q)$:

Référence: [Rombaldi 148]

Énoncé:

$E = \mathbb{F}_q$ -ev de dim $n \geq 1$. $\mathcal{D}(E) = \{u \in \mathcal{L}(E) \mid u \text{ est diagonalisable}\}$

$$\#(\mathcal{D}(E)) = \sum_{\substack{m_1 + \dots + m_q = n \\ m_i \geq 0}} \frac{\#(GL(E))}{\prod_{i=1}^q \#(GL(E_i))}$$

Où E_i est un $\mathbb{F}_q$ -ev de dimension m_i

Étapes:

(E1) $\mathcal{D}(E) = \{u \in \mathcal{L}(E) \mid u^q = u\}$

(E2) $\forall u \in \mathcal{D}(E), E = \bigoplus_{i=1}^q \ker(u - \lambda_i \text{id}_E)$ ($\mathbb{F}_q = \{\lambda_1, \dots, \lambda_q\}$)

(E3) $\mathcal{F} = \{(E_1, \dots, E_q) \mid E = E_1 \oplus \dots \oplus E_q\}$

Ng $\varphi: \mathcal{D}(E) \rightarrow \mathcal{F}$ est surjective

(E4) $\psi: GL(E) \times \mathcal{F}_{(n_1, \dots, n_q)} \rightarrow \mathcal{F}_{(n_1, \dots, n_q)}$ est une
 $(u, (E_1, \dots, E_q)) \mapsto (u(E_1), \dots, u(E_q))$

action de groupes transitive

(E5) Dénombrement de $\mathcal{F}_{(n_1, \dots, n_q)}$ avec l'action de groupe + équation des classes

Étape 1: $\mathcal{D}(E) = \{u \in \mathcal{L}(E) \mid u^q = u\}$

$\subseteq$ Soit $u \in \mathcal{D}(E)$, comme u est diagonalisable alors son polynôme minimal est scindé à racines simples $\pi_u(X) = \prod_{\lambda \in \text{Sp}(u)} (X - \lambda)$.

$$\text{Mq } \prod_{\lambda \in \mathbb{F}_q} (X - \lambda) = X^q - X$$

$\prod_{\lambda \in \mathbb{F}_q} (X - \lambda)$ est unitaire, de degré q et a q racines

Comme $\mathbb{F}_q^*$ est cyclique d'ordre $q-1$, $\forall \lambda \in \mathbb{F}_q^*$, $\lambda^{q-1} = 1$ donc $\lambda^q - \lambda = 0$. De même si $\lambda = 0$, $\lambda^q - \lambda = 0$.

Bonc $X^q - X$ est un polynôme unitaire de degré q à q racines. $\prod_{\lambda \in \mathbb{F}_q} (X - \lambda) - X^q + X$ est donc de degré $< q$ et il

a q racines donc $\prod_{\lambda \in \mathbb{F}_q} (X - \lambda) - X^q + X = 0$.

d'où $\prod_{\lambda \in \mathbb{F}_q} (X - \lambda) = X^q - X$ (on peut aussi, par Bézout dans $\mathbb{F}_q[X]$ ppal, mq $\forall \lambda \in \mathbb{F}_q$, $(X - \lambda) \mid X^q - X$).

Bonc $\pi_u(X) = \prod_{\lambda \in \text{Sp}(u)} (X - \lambda) \mid X^q - X$ donc $X^q - X$ annule u donc $u^q = u$.

$\square$

Réciproquement si $u^q = u$ alors $X^q - X = \prod_{\lambda \in \mathbb{F}_q} (X - \lambda)$ est scindé et annule u . Donc u est diagonalisable.

Étape 2: $\forall u \in \mathcal{D}(E)$ $E = \bigoplus_{k=1}^q \ker(u - \lambda_k \text{id}_E)$.

Comme $u \in \mathcal{D}(E)$, u est annulé par $P(X) = X^q - X$.

On note $\mathbb{F}_q = \{\lambda_1, \dots, \lambda_q\}$.

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

De plus les $P_i(X) = X - \lambda_i \text{id}_E$ sont premiers entre eux deux-à-deux. Donc dans $\mathbb{F}_q[X]$ ppal, par le lemme des noyaux,

$$\ker(\underbrace{u^q - u}_{=0}) = \bigoplus_{i=1}^q \ker(u - \lambda_i \text{id}_E)$$

$$E = \bigoplus_{i=1}^q \ker(u - \lambda_i \text{id}_E)$$

Étape 3:

On va alors se ramener à dénombrer un ensemble plus simple $\mathcal{F}^q = \{(E_1, \dots, E_q), \forall i \in [1; q] E_i \subseteq E \text{ s.e.v.}, \text{ tels que } E = \bigoplus_{i=1}^q E_i\}$.

$$\forall \varphi: \mathcal{D}(E) \rightarrow \mathcal{F}^q$$

$$u \mapsto (\ker(u - \lambda_1 \text{id}), \dots, \ker(u - \lambda_q \text{id}))$$

est bijective.

φ est bien définie et bien à valeurs dans $\mathcal{F}^q$ par l'E2.

Injective: soit $(u, v) \in \mathcal{D}(E)$ tq $\varphi(u) = \varphi(v)$.

Alors on note $\forall i \in [1, q]$ $E_i = \ker(u - \lambda_i \text{id}) = \ker(v - \lambda_i \text{id})$

On a $E \stackrel{(*)}{=} E_1 \oplus \dots \oplus E_q$. $\forall x \in E$ on note $x = x_1 + \dots + x_q$

l'écriture de x adaptée à la décomposition $(*)$

$$u(x) = u(x_1) + \dots + u(x_q) = \lambda_1 x_1 + \dots + \lambda_q x_q$$

$$v(x) = v(x_1) + \dots + v(x_q) = \lambda_1 x_1 + \dots + \lambda_q x_q = u(x)$$

Surjective : Soit $(E_1, \dots, E_q) \in \mathcal{F}$, on a $E = E_1 \oplus \dots \oplus E_q$.

On pose alors $u|_{E_i} = \lambda_i \text{id} \quad \forall i \in [1, q]$.

On a alors bien $u \in \mathcal{D}(E)$ et $\varphi(u) = (E_1, \dots, E_q)$.

Bonc $\#(\mathcal{D}(E)) = \#(\mathcal{F})$.

④ Pour $(n_k)_{1 \leq k \leq q}$ tel que $n = \sum_{k=1}^q n_k$, on note :

$$\mathcal{F}_{(n_1, \dots, n_q)} = \{(E_1, \dots, E_q) \mid \dim(E_i) = n_i\}$$

On mg l'application suivante définit une ac^e de $GL(E)$ sur $\mathcal{F}_{(n_1, \dots, n_q)}$
transitive à une seule orbite.

$$\psi: GL(E) \times \mathcal{F}_{(n_1, \dots, n_q)} \rightarrow \mathcal{F}_{(n_1, \dots, n_q)}$$

$$(u, (E_1, \dots, E_q)) \mapsto u \cdot (E_1, \dots, E_q) = (u(E_1), \dots, u(E_q))$$

▷ Soit $u \in GL(E)$, $(E_1, \dots, E_q) \in \mathcal{F}_{(n_1, \dots, n_q)}$

Comme $u \in GL(E)$, $\dim(E_i) = n_i = \dim(u(E_i))$, $\forall i$

$$\text{et } E = u(E) = u(E_1) + \dots + u(E_q)$$

$$\text{Bonc } E = u(E_1) \oplus \dots \oplus u(E_q)$$

Bonc ψ est bien définie et à valeurs dans $\mathcal{F}_{(n_1, \dots, n_q)}$.

▷ On a $\forall (E_1, \dots, E_q) \in \mathcal{F}_{(n_1, \dots, n_q)}^0$, $\text{id} \cdot (E_1, \dots, E_q) = (E_1, \dots, E_q)$.

et $\forall (u, v) \in \text{GL}(E)$, $\forall (E_1, \dots, E_q) \in \mathcal{F}_{(n_1, \dots, n_q)}^0$

$$(u \circ v) \cdot (E_1, \dots, E_q) = ((u \circ v)(E_1), \dots, (u \circ v)(E_q)) =$$

$$u \cdot (v \cdot (E_1, \dots, E_q)) = u \cdot (v(E_1), \dots, v(E_q))$$

$$= ((u \circ v)(E_1), \dots, (u \circ v)(E_q)) =$$

Donc Ψ est bien une action de groupes.

▷ Transitive :

Soit $((E_1, \dots, E_q), (F_1, \dots, F_q)) \in \mathcal{F}^2$, on cherche $u \in \text{GL}(E)$ tq

$$u \cdot (E_1, \dots, E_q) = (F_1, \dots, F_q).$$

Si on se donne $B = \bigcup_{i=1}^q \underline{B_i}$ et $C = \bigcup_{i=1}^q \underline{C_i}$ deux
base
de E_i
 $\dim(E_i) = n_i$ et base
de F_i
 $\dim(F_i) = n_i$

on définit alors $u \in \mathcal{L}(E)$ par $u(B_i) = C_i$.

On a alors $u(E_i) = F_i$ et $u \cdot (E_1, \dots, E_q) = (F_1, \dots, F_q)$.

L'action étant transitive il n'y a alors qu'une seule orbite.

(E5) Calcul du cardinal de $\mathcal{F}_{(n_1, \dots, n_q)}^0$ avec l'équa^e des classes.

$$|\mathcal{F}_{(n_1, \dots, n_q)}^0| = \frac{|\text{GL}(E)|}{|\text{Stab}(E_1, \dots, E_q)|} \quad \text{où } (E_1, \dots, E_q) \in \mathcal{F}_{(n_1, \dots, n_q)}^0$$

car il n'y a qu'une orbite

$$\begin{aligned} \text{Stab}((E_1, \dots, E_q)) &= \{u \in \text{GL}(E) \mid u \cdot (E_1, \dots, E_q) = (E_1, \dots, E_q)\} \\ &= \{u \in \text{GL}(E) \mid \forall k \in [1; q] \ u(E_k) = E_k\} \end{aligned}$$

$$\text{Mq } \text{Stab}((E_1, \dots, E_q)) = \{u \in \text{GL}(E) \mid \forall k, u|_{E_k} \in \text{GL}(E_k)\}$$

$$\boxed{\subseteq} \text{ si } u \in \text{Stab}((E_1, \dots, E_q)) \quad u(E_k) = E_k \quad \forall k \in [1; q]$$

$$\text{donc } u|_{E_k} \in \text{GL}(E_k) \quad \forall k \in [1; q]$$

$$\boxed{\supseteq} \text{ Réciproquement si } u \in \text{GL}(E) \text{ tq } \forall k \in [1; q] \ u|_{E_k} \in \text{GL}(E_k)$$

$$\text{alors } u(E_k) = E_k \quad \forall k \in [1; q] \text{ et } u \in \text{Stab}((E_1, \dots, E_q))$$

$$\text{Donc } \text{Stab}((E_1, \dots, E_q)) = \{u \in \text{GL}(E) \mid \forall k \ u|_{E_k} \in \text{GL}(E_k)\}$$

$$\text{donc } \#(\text{Stab}((E_1, \dots, E_q))) = \prod_{k=1}^q \#(\text{GL}(E_k))$$

$$\text{Donc } \#(\mathcal{F}_{(n_1, \dots, n_q)}) = \frac{\#(\text{GL}(E))}{\prod_{k=1}^q \#(\text{GL}(E_k))}$$

$$\{\mathcal{F}_{(n_1, \dots, n_q)} \mid n_1 + \dots + n_q = n\} = \mathcal{F}$$

$$\text{Donc } \#(\mathcal{F}) = \sum_{\substack{n_1 + \dots + n_q = n \\ n_i \geq 0}} \frac{\#(\text{GL}(E))}{\prod_{k=1}^q \#(\text{GL}(E_k))}$$

(E6) Calcul de $\#(\text{GL}_n(\mathbb{F}_q))$:

$$\#(\mathbb{F}_q) = q, \quad \dim(\text{GL}_n(\mathbb{F}_q)) = n$$

Nombre de bases de $\mathbb{K}^n$

▷ premier vecteur : $q^n - 1$ options

▷ deuxième vecteur : $q^n - 1$ vecteurs non-nuls

moins $(q-1)$ vecteurs colinéaires au premier

vecteur: $q^n - 1 - (q-1) = q^n - q$

▷ 3^{ème} $q^n - 1 - (q-1)(q-1) - (q-1) - (q-1)$

$$= q^n - 1 - q^2 + 2q - 1 - q + 1 - q + 1$$

$$= q^n - q^2$$

↑
hors les
vecteurs

↑
hors les vecteurs de $\text{vect}(e_1, e_2)$,
ce qui inclue 0 et qui on retire
donc

▷ k-ième vecteur $q - q^{k-1}$

▷ n-ième $q^n - q^{n-1}$

Total: il y a $\prod_{k=0}^{n-1} (q^n - q^k)$ bases de K^n

$$\prod_{k=0}^{n-1} (q^n - q^k) = \prod_{k=0}^{n-1} q^k (q^{n-k} - 1)$$

$$= q^1 \cdots q^{n-1} \prod_{k=0}^{n-1} (q^{n-k} - 1)$$

$$1 + \cdots + (n-1) = \sum_{k=1}^{n-1} k = \frac{n(n-1)}{2} (q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$$

Soit B_0 une base de K^n , $\Phi_0: GL_n(K) \rightarrow B = \{\text{em. base de } K^n\}$
est une bijection.

(réciproque: matrice de passage) donc

$$\# GL_n(K) = \frac{n(n-1)}{2} (q^n - 1) \cdots (q - 1)$$