

Denombrement de $DL(\mathbb{F}_q^m)$

Lemme 1: Soit E $\mathbb{F}_q$ -Ev de dimension m , $DL(E) := \{u \in GL(E) \mid u \text{ diagonalisable}\}$

Alors $|DL(E)| = |\mathcal{F}|$ où $\mathcal{F} := \{F = (F_k)_{k=1}^{q-1} \mid F_k \in E \text{ et } E = \bigoplus_{k=1}^{q-1} F_k\}$

① $DL(E) = \{u \in GL(E) \mid u^{q-1} = \text{Id}_E\}$ ② $\varphi: u \in DL(E) \mapsto (\text{Ker}(u - \lambda_k \text{Id}))_{k=1}^{q-1} \in \mathcal{F}$ bijective

① Si $u \in DL(E)$, alors $\mu_u = \prod_{\lambda \in \text{Sp}(u)} (X - \lambda)$ est scindé à racines simples. Or $P = X^{q-1} - 1 = \prod_{k=1}^{q-1} (X - \lambda_k)$ où $\mathbb{F}_q^* = \{\lambda_1, \dots, \lambda_{q-1}\}$, donc $\mu_u \mid P$ et $P(u) = 0$. Réciproquement, si P scindé à racines simples annule u , alors $u \in DL(E)$.

② Bien def * Par le lemme des noyaux, on a $\forall u \in DL(E)$ $E = \bigoplus_{k=1}^{q-1} \text{Ker}(u - \lambda_k \text{Id})$. Donc $\varphi(u) \in \mathcal{F}$, φ bien défini.

inj * Soit $u, v \in DL(E)$ tels que $\varphi(u) = \varphi(v)$. On a $\forall x = \sum_{k=1}^{q-1} x_k \in E = \bigoplus_{k=1}^{q-1} \text{Ker}(u - \lambda_k \text{Id}) = \bigoplus_{k=1}^{q-1} \text{Ker}(v - \lambda_k \text{Id})$
 $u(x) = \sum_{k=1}^{q-1} u(x_k) = \sum_{k=1}^{q-1} \lambda_k x_k = \sum_{k=1}^{q-1} v(x_k) = v(x)$. Donc $u = v$ et φ injective

surj * Soit $F = (F_k)_{k=1}^{q-1} \in \mathcal{F}$. On pose $u \in DL(E)$ tel que $u|_{F_k} = \lambda_k \text{Id}_{F_k}$. Alors u est diagonalisable dans une base adaptée à $E = \bigoplus_{k=1}^{q-1} F_k$, de valeurs propres non nulles. Donc $u \in DL(E)$ et $\varphi(u) = F$.

Lemme 2: Pour $n = (n_i)_{i=1}^{q-1} \in \mathbb{N}^{q-1}$, $\sum_{k=1}^{q-1} n_k = m$, $GL(E)$ agit transitivement sur $\mathcal{F}_n := \{F \in \mathcal{F} \mid \dim F_k = n_k\}$ par $GL(E) \times \mathcal{F}_n \rightarrow \mathcal{F}_n$, $u \cdot F := (u(F_k))_{k=1}^{q-1}$

bien def * On a $\forall u \in GL(E)$, $\forall F \in \mathcal{F}_n$, $E = u(E) = u(\bigoplus_{k=1}^{q-1} F_k) = \bigoplus_{k=1}^{q-1} u(F_k)$ et $\dim u(F_k) = \dim F_k = n_k$

action Donc $E = \bigoplus_{k=1}^{q-1} u(F_k)$ et $u \cdot F = (u(F_k))_{k=1}^{q-1} \in \mathcal{F}_n$. De plus, $\forall u, v \in GL(E)$ et $\forall F \in \mathcal{F}_n$ on a

$u \cdot (v \cdot F) = u \cdot (v(F_k))_{k=1}^{q-1} = (u(v(F_k)))_{k=1}^{q-1} = (u \circ v)(F_k)_{k=1}^{q-1} = (u \circ v) \cdot F$, et $\text{Id}_E \cdot F = F$. Donc $GL(E)$ agit sur $\mathcal{F}_n$

transitive * Par ailleurs, $\forall F, F' \in \mathcal{F}_n$, on considère $e = \bigcup_{k=1}^{q-1} e_k$ et $e' = \bigcup_{k=1}^{q-1} e'_k$ bases adaptées à $E = \bigoplus_{k=1}^{q-1} F_k$ et $E = \bigoplus_{k=1}^{q-1} F'_k$. Puisque $\forall k \in [1, q-1]$ $\dim F_k = \dim F'_k = n_k$, on peut définir $u \in GL(E)$ tel que $u(e_k) = e'_k$. Alors $u \cdot F = F'$ et l'action est transitive

Théorème: On a $|DL(E)| = \sum_{n_1 + \dots + n_{q-1} = m} \prod_{k=1}^{q-1} |GL_n(\mathbb{F}_q)|$

$|Stab(F)|$ * Soit $u \in GL(E)$, $F \in \mathcal{F}_n$. On a $u \in Stab(F) \Leftrightarrow u \cdot F = F$ ou $u(F_k) = F_k \forall k \in [1, q-1]$ ou $u|_{F_k} \in GL(F_k)$
Donc $Stab(F) = \{u \in GL(E) \mid u|_{F_k} \in GL(F_k)\}$ et $|Stab(F)| = \prod_{k=1}^{q-1} |GL(F_k)|$.

Eq classe * Puisque l'action est transitive, il n'y a qu'une orbite et $|\mathcal{F}_n| = |Orb(F)| = \frac{|GL(E)|}{|Stab(F)|}$

Finalement, puisque $\mathcal{F} = \bigsqcup_{n_1 + \dots + n_{q-1} = m} \mathcal{F}_n$, on a $|DL(E)| = |\mathcal{F}| = \sum_{n_1 + \dots + n_{q-1} = m} \prod_{k=1}^{q-1} |GL_n(\mathbb{F}_q)|$

Lemme: $X^{q^1-1} - 1 = \prod_{\lambda \in \mathbb{F}_q^*} (X - \lambda) \in \mathbb{F}_q[X]$

Par Lagrange, $\forall x \in \mathbb{F}_q^* x^{q^1-1} = 1$. Donc les éléments de $\mathbb{F}_q^*$ sont racines de $X^{q^1-1} - 1$.

Or $|\mathbb{F}_q^*| = q-1$ et $X^{q^1-1} - 1$ a au plus $q-1$ racines. D'où $X^{q^1-1} - 1 = \prod_{\lambda \in \mathbb{F}_q^*} (X - \lambda)$.

Remarque: Pour $D(E) = \{v \in L(E) \text{ diagonalisable}\}$, on rajoute la valeur propre 0

donc $D(E) = \{v \in L(E) \mid v^q = v\}$ et $|D(E)| = \sum_{n_1 + \dots + n_q = m} \frac{|GL_m(\mathbb{F}_q)|}{\prod_{i=1}^q |GL_{n_i}(\mathbb{F}_q)|}$

Exemple: $q=2, m=2$

$E = \mathbb{F}_2^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$, $GL_2(\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$

Donc $|GL_2(\mathbb{F}_2)| = 6$, $DL(\mathbb{F}_2^2) = \frac{6}{6} = 1$, $D(\mathbb{F}_2^2) = 6 \left(\frac{1}{6} + \frac{1}{6} + \frac{1}{2} \right) = 8$

car $\begin{cases} n_2=2 \\ n_2=0 \end{cases} \begin{cases} n_1=1 \\ n_1=1 \end{cases} \begin{cases} n_1=0 \\ n_2=2 \end{cases}$ et $|GL_2(\mathbb{F}_2)| = 6$, $|GL_1(\mathbb{F}_2)| = 1$

Théorème: $E = \mathbb{F}_q$ Ev, de dimension m . On a $|GL(E)| = \prod_{k=1}^m (q^m - q^{k-1}) = q^{\frac{m(m-1)}{2}} \prod_{k=1}^m (q^k - 1)$

On a $|GL(E)| = |GL_m(\mathbb{F}_q)|$, et compter combien de $A \in GL_m(\mathbb{F}_q)$ revient à compter toutes les bases de $\mathbb{F}_q^m$ (les colonnes de A doivent former une base).

Pour choisir e_1 , on a $|E \setminus \{0\}| = q^m - 1$ choix. Pour choisir e_k , $\forall k \in \{2, m\}$, on

le choisit dans $E \setminus \bigoplus_{i=1}^{k-1} \mathbb{F}_q e_i$ donc $q^m - |\bigoplus_{i=1}^{k-1} \mathbb{F}_q e_i| = q^m - q^{k-1}$. Soit au total

$$\prod_{k=1}^m q^m - q^{k-1} = \prod_{k=1}^m q^{m-k+1} (q^{m-k+1} - 1) = q^{\sum_{k=1}^m (m-k+1)} \prod_{k=1}^m (q^{m-k+1} - 1) = q^{\frac{m(m+1)}{2}} \prod_{k=1}^m (q^k - 1) \text{ choix.}$$