I.E Automorphismes diagonalisables (101) (104) (106) (123) (151) (152) (190)

Théorème 6: Dénombrement de $DL(E)$

Soient $n \in \mathbb{N}$ et $q = p^r$ où p est premier et $r \in \mathbb{N}^*$. Soit $DL_n(\mathbb{F}_q)$ l'ensemble des matrices inversibles diagonalisables de taille n sur $\mathbb{F}_q$. Ou soit E un $\mathbb{F}_q$-espace vectoriel de dimension n. La cardinal de $DL(E)$ est :

$$|DL_n(E)| = \sum_{\substack{(n_k)_{1\leqslant k\leqslant q-1}\in\mathbb{N}^{q-1} \\ n_1+\cdots+n_{q-1}=n}} \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q-1} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}$$

Démonstration. Soit E un $\mathbb{F}_q$-e.v. de dimension n. On va commencer par décrire les éléments de $DL(E)$, puis en faisant agir $\mathrm{GL}(E)$ sur un ensemble en bijection avec $DL(E)$, on déterminera le cardinal cherché.

1. Montrons que $DL(E) = \{u \in \mathrm{GL}(E) \quad / \quad u^{q-1} = u\}$.
   On pense raisonnablement à cela car on sait que le groupe multiplicatif d'un corps fini est cyclique.

   • Soit $u \in DL(E)$. Comme u est diagonalisable, son polynôme minimal est scindé simple sur $\mathbb{F}_q$:

   $$\mu_u = \prod_{\lambda\in\mathrm{Sp}(u)} (X-\lambda).$$

   Comme $\mathrm{Sp}(u) \subset \mathbb{F}_q^\times$, puisqu'il est scindé simple : $\mu_u \mid \prod_{\lambda\in\mathbb{F}_q^\times} (X-\lambda) = X^{q-1} - X$. Donc $u^{q-1} = u$.

   • Réciproquement, si $u^{q-1} = u$, alors u admet un polynôme annulateur scindé simple $(X^{q-1} - 1)$, donc est diagonalisable.

Par le lemme des noyaux, on a donc :

$$E = \bigoplus_{\lambda\in\mathbb{F}_q^\times} \ker(u - \lambda\mathrm{id}).$$

2. Dans tout ce qui suit, E_k désignera un sous-espace vectoriel de E.
   On note :

   $$\mathcal{F} = \left\{ (E_k)_{1\leqslant k\leqslant q-1} : E = \bigoplus_{k=1}^{q-1} E_k \right\}.$$

   Montrons que E est $\mathcal{F}$ ont même cardinal. Pour cela on définit l'application suivante :

   $$\varphi : \begin{array}{ccc} DL_n(E) & \longrightarrow & \mathcal{F} \\ u & \longmapsto & (\ker(u-\lambda_k\mathrm{id}))_{1\leqslant k\leqslant q-1} \end{array}.$$

   • Cette application est bien définie par le lemme des noyaux.
   • Elle est injective car si $\varphi(u) = \varphi(v)$ alors $\forall\lambda \in \mathbb{F}_q^\times \quad \forall x \in \ker(u - \lambda\mathrm{id}) = \ker(v - \lambda\mathrm{id}$, on a $u(x) = \lambda x = v(x)$. Mais comme $E = \bigoplus E_k$, on a donc $u = v$.
   • Elle est surjective car si $(E_k) \in \mathcal{F}$ alors on considère u tel que $u_{|E_k} = \lambda_k\mathrm{id}_{E_k}$. Alors $u \in DL(E)$ et $\varphi(u) = (E_k)$

Il en résulte que :

$$|DL(E)| = |\mathcal{F}|.$$

Et c'est ce dernier cardinal que l'on va chercher à expliciter grâce à une action bien choisie.

3. Pour $n_1, \ldots, n_{q-1}$ entiers tels que $\displaystyle\sum_{k=1}^{q-1} n_k = n$, on note :

$$\mathcal{F}_{(n_1,\ldots,n_{q-1})} = \left\{(E_k)_{1\leqslant k\leqslant q-1} \in \mathcal{F} : \forall k \in [\![1, q-1]\!], \dim(E_k) = n_k\right\}$$

Et on a alors que ces ensembles partitionnent $\mathcal{F}$.

Soit $n_1, \ldots, n_{q-1}$ entiers tels que $\displaystyle\sum_{k=1}^{q-1} n_k = n$. On considère l'action suivante :

$$\psi : \begin{array}{ccccc} \mathrm{GL}(E) & \times & \mathcal{F}_{(n_1,\ldots,n_{q-1})} & \to & \mathcal{F}_{(n_1,\ldots,n_{q-1})} \\ u & , & (E_k)_k & \mapsto & (u(E_k))_k \end{array}.$$

• ψ est bien définie car si $u \in \mathrm{GL}(E)$ et $(E_k) \in \mathcal{F}_{(n_1,\ldots,n_{q-1})}$ alors $E = u(E)$ et $\dim(u(E_k)) = \dim(E_k)$.

• Elle définit bien une action car :

  * $\mathrm{id} \cdot (E_k) = (E_k)$;
  * $(u \circ v) \cdot (E_k) = (u \circ v(E_k)) = u \circ (v(E_k)) = u \cdot (v \cdot E_k))$.

• Elle est transitive car si $(E_k) \in \mathcal{F}_{(n_1,\ldots,n_{q-1})}$ et $(F_k) \in \mathcal{F}_{(n_1,\ldots,n_{q-1})}$, alors en considérant des bases $\mathcal{B} = (\mathcal{B}_1, \ldots, \mathcal{B}_{q-1})$, où $\mathcal{B}_k$ est une base de E_k, et $\mathcal{C} = (\mathcal{C}_1, \ldots, \mathcal{C}_{q-1})$, où $\mathcal{C}_k$ est une base de F_k ; et $u : \mathcal{B} \mapsto \mathcal{C}$ (qui est alors entièrement déterminé et bien défini car les bases ont même cardinal) on a clairement $(F_k) = u((E_k))$.

4. Il ne nous reste plus qu'à étudier cette action pour conclure.

Montrons que le stabilisateur de $(E_k)_{1\leqslant k\leqslant q}$ a pour cardinal $\displaystyle\prod_{k=1}^{q-1} |GL_{n_k}(\mathbb{F}_q)|$. En effet :

• on a que $u \in \mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)$ si et seulement si par définition $u(E_k) \subseteq E_k$ pour tout $1 \leqslant k \leqslant q-1$. Mais pour des raisons de dimensions on a même $u \in \mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)$ si et seulement si $u(E_k) = E_k$ pour tout $1 \leqslant k \leqslant q-1$, soit si et seulement si $u_{|E_k} \in \mathrm{GL}(E_k)$ pour tout $1 \leqslant k \leqslant q-1$. Donc $\mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q}\right)$ est en bijection avec les matrices diagonales par blocs dont les blocs ont pour tailles $n_1, \ldots, n_{q-1}$ sont des matrices inversibles. On a donc

$$\left|\mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)\right| = \prod_{k=1}^{q-1} |\mathcal{GL}_{n_k}(\mathbb{F}_q)|$$

L'action étant transitive, l'équation aux classes (ou la relation orbite/stabilisateur) donne :

$$\#\left(\mathcal{F}_{(n_1,\ldots,n_{q-1})}\right) \times \left|\mathrm{Stab}\left((E_k)_{1\leqslant k\leqslant q-1}\right)\right| = |\mathrm{GL}(E)|$$

c'est-à-dire

$$\#\left(\mathcal{F}_{(n_1,\ldots,n_{q-1})}\right) = \frac{|\mathcal{GL}_n(\mathbb{F}_q)|}{\prod_{i=1}^{q} |\mathcal{GL}_{n_i}(\mathbb{F}_q)|}.$$

Et on conclut en utilisant la partition de $\mathcal{F}$.

■