0.1 Dénombrément des automorphismes diagonalisables de F_q

Leçons concernées : 101, 104, 106, 123, 150, 152, 190

Soit E un $\mathbb{F}_q$ -espace vectoriel de dimension $n \geq 1$ (où q est la puissance d'un nombre premier), on désigne par $DL(E)$ l'ensemble des automorphismes de E qui sont diagonalisables et on note $\mathbb{F}_q^* = \{\lambda_1, \dots, \lambda_{q-1}\}$.

Lemme 0.1. On a $DL(E) = \{u \in GL(E) \mid u^{q-1} = id\}$.

Démonstration. Supposons que $u \in GL(E)$ est diagonalisable, alors son polynôme minimal noté μ_u est alors scindé à racines simples, soit $\mu_u(X) = \prod_{\lambda \in Sp(u)} (X - \lambda)$ avec $Sp(u) \subset \mathbb{F}_q^*$ et puisque μ_u divise $X^{q-1} - 1 = \prod_{\lambda \in \mathbb{F}_q^*} (X - \lambda)$, on a $u^{q-1} = id$.

Réciproquement, supposons que $u \in GL(E)$ est tel que $u^{q-1} = id$, le polynôme $X^{q-1} - 1$ est scindé à racines simples dans $\mathbb{F}_q[X]$ (d'après le théorème de Lagrange) annule u , donc u est diagonalisable. $\square$

Lemme 0.2. Pour tout $u \in DL(E)$, on a $E = \bigoplus_{k=1}^{q-1} Ker(u - \lambda_k id)$.

Démonstration. Pour tout $u \in DL(E)$ étant annulé par $P(X) = X^{q-1} - 1 = \prod_{k=1}^{q-1} (X - \lambda_k)$ le lemme des noyaux donne le résultat voulu. $\square$

On désigne par $\mathcal{F}$ l'ensemble des suites $(E_k)_{1 \leq k \leq q-1}$ de sous-espaces vectoriels de E tels que $E = \bigoplus_{k=1}^{q-1} E_k$.

Lemme 0.3. L'application :

$$\varphi : DL(E) \rightarrow \mathcal{F}, u \rightarrow (ker(u - \lambda_k id))_{1 \leq k \leq q-1}$$

est bijective.

Démonstration. Le lemme précédent nous assure que l'application φ est bien à valeurs dans $\mathcal{F}$. Soient $u, v \in DL(E)$ sont tels que $\varphi(u) = \varphi(v)$, on a alors $ker(u - \lambda_k id) = ker(v - \lambda_k id), \forall k$ compris entre 1 et $q-1$, donc pour tout $x \in ker(u - \lambda_k id), u(x) = v(x) = \lambda_k x$ ce qui entraîne que $u = v$ puisque $E = \bigoplus_{k=1}^{q-1} ker(u - \lambda_k id)$, donc φ est injective. Soit $(E_k) \in \mathcal{F}$, l'application linéaire u définie par $u|_{E_k} = \lambda_k id_{E_k}, \forall k$ est dans $DL(E)$ telle que $\varphi(u) = (E_1, \dots, E_{q-1})$, donc φ est surjective. $\square$

On a donc que $|DL(E)| = |\mathcal{F}|$ et il s'agit alors de dénombrer $\mathcal{F}$. Pour $(n_k) \in \mathbb{N}^{q-1}$ tel que $\sum_{k=1}^{q-1} n_k = n$, on note :

$$\mathcal{F}_{n_k} = \{(E_k) \in \mathcal{F} \mid dim(E_k) = n_k, 1 \leq k \leq q-1\}$$

ce qui nous donne une partition de $\mathcal{F}$.

Lemme 0.4. Soit $(n_k) \in \mathbb{N}^{q-1}$ fixé tel que $\sum_{k=1}^{q-1} n_k = n$, l'application :

$$GL(E) \times \mathcal{F}_{n_k} \rightarrow \mathcal{F}_{n_k}, (u, (E_1, \dots, E_{q-1})) \rightarrow (u(E_1), \dots, u(E_{q-1}))$$

définit une action transitive.

Démonstration. Pour $u \in GL(E)$ et $E = \bigoplus_{k=1}^{q-1} E_k$ avec $\dim(E_k) = n_k$, on a $E = u(E)$ (car c'est un automorphisme et donc il envoie une base de E sur une base de E) $u(E) = \sum_{k=1}^{q-1} u(E_k)$ avec $\dim(u(E_k)) = \dim(E_k) = n_k$, donc $E = \bigoplus_{k=1}^{q-1} u(E_k)$, c'est-à-dire que $(u(E_k)) \in \mathcal{F}_{n_k}$.
Montrer la transitivité de cette action revient à montrer que pour tout $(E_k) \in \mathcal{F}_{n_k}$, on a que pour tout $(F_k) \in \mathcal{F}_{n_k}$, il existe $u \in GL(E)$ telle que $u(E_k) = F_k$ pour tout k compris entre 1 et $q-1$. En effet, on se donne deux bases $\mathcal{B} = \cup_{k=1}^{q-1} \mathcal{B}_k$ et $\mathcal{B}' = \cup_{k=1}^{q-1} \mathcal{B}'_k$ de E telles que pour tout k , $\mathcal{B}_k$ est une base de E_k et $\mathcal{B}'_k$ une base de F_k . Comme $\dim(E_k) = \dim(F_k) = n_k$, on peut définir $u \in GL(E)$ par $u(\mathcal{B}) = \mathcal{B}'$ et cet automorphisme est tel que $u(E_k) = F_k$ d'où le résultat. $\square$

Lemme 0.5. En notant, pour $(n_k) \in \mathbb{N}^{q-1}$ tel que $\sum_{k=1}^{q-1} n_k = n$ et $(E_k) \in \mathcal{F}_{n_k}$:

$$Stab(E_1, \dots, E_{q-1}) = \{u \in GL(E) \mid u(E_k) = E_k, 1 \leq k \leq q-1\}$$

le stabilisateur de (E_k) , on a $|Stab(E_k)| = \prod_{k=1}^{q-1} |GL(E_k)|$ et $|\mathcal{F}| = \frac{|GL(E)|}{\prod_{k=1}^{q-1} |GL(E_k)|}$.

Démonstration. Pour tout $u \in Stab(E_1, \dots, E_{q-1})$, on a $u(E_k) = E_k$, donc $u|_{E_k} \in GL(E_k)$. Réciproquement si $u \in GL(E)$ est tel que $u|_{E_k} \in GL(E_k)$, on a alors que $u(E_k) = E_k$. (car les automorphismes envoient une base sur une base) On a donc :

$$Stab(E_1, \dots, E_{q-1}) = \{u \in GL(E) \mid u|_{E_k} \in GL(E_k), 1 \leq k \leq q-1\}$$

et en conséquence $|Stab(E_k)| = \prod_{k=1}^{q-1} |GL(E_k)|$. Comme il y a une seule orbite, on a :

$$|\mathcal{F}_{n_k}| = \frac{|GL(E)|}{|Stab(E_1, \dots, E_{q-1})|} = \frac{|GL(E)|}{\prod_{k=1}^{q-1} |GL(E_k)|}.$$

$\square$

Théorème 0.6. On a :

$$|DL(E)| = \sum_{n_1 + \dots + n_{q-1} = n} \frac{|GL(E)|}{|GL(E_1)| \dots |GL(E_{q-1})|}.$$

Démonstration. Les $\mathcal{F}_{n_k}$ formant une partition de $\mathcal{F}$, on aboutit à :

$$\begin{aligned} |DL(E)| &= |\mathcal{F}| = \sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1 + \dots + n_{q-1} = n}} |\mathcal{F}_{(n_1, \dots, n_{q-1})}| \\ &= \sum_{\substack{(n_1, \dots, n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1 + \dots + n_{q-1} = n}} \frac{|GL(E)|}{\prod_{k=1}^{q-1} |GL(E_k)|} \end{aligned}$$