Dénombrement dans un espace vectoriel fini

Dans ce document, on considère un espace vectoriel E de dimension finie $n \in \mathbb{N}^*$ sur un corps fini $\mathbb{F}_q$. Comme E est isomorphe à $\mathbb{F}_q^n$, le cardinal de E est q^n.

1. Dénombrement des endomorphismes de E

On commence par dénombrer l'ensemble des endomorphismes de E.

Proposition : *Le cardinal de* $\mathscr{L}(E)$ *est* q^{n^2}.

Démonstration :
L'espace vectoriel $\mathscr{L}(E)$ est de dimension n^2 sur le corps $\mathbb{F}_q$, donc il est isomorphe à $\mathbb{F}_q^{n^2}$, d'où le résultat. □

On peut également dénombrer les endomorphismes bijectifs.

Proposition : *Le cardinal du groupe* $\mathrm{GL}(E)$ *est*

$$\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q)) = \prod_{k=0}^{n-1}(q^n - q^k).$$

Démonstration :
1) En fixant une base de E, on obtient une bijection de $\mathrm{GL}(E)$ sur $\mathrm{GL}_n(\mathbb{F}_q)$. Il suffit donc de calculer le cardinal de $\mathrm{GL}_n(\mathbb{F}_q)$.
2) Si $M \in \mathscr{M}_n(\mathbb{F}_q)$, notons $M_1, \dots, M_n \in \mathbb{F}_q^n$ les colonnes de M. Une matrice $M \in \mathscr{M}_n(\mathbb{F}_q)$ est inversible si et seulement si

$$M_1 \neq 0, \quad M_2 \in \mathbb{F}_q^n \setminus \mathrm{Vect}(M_1), \quad \dots, \quad M_n \in \mathbb{F}_q^n \setminus \mathrm{Vect}(M_1, \dots, M_{n-1}).$$

On dispose donc de $q^n - 1$ possibilités pour la colonne M_1, puis $q^n - q$ possibilités pour la colonne M_2,..., puis $q^n - q^{n-1}$ possibilités pour la colonne M_n, d'où le résultat. □

On en déduit le cardinal du groupe $\mathrm{SL}(E)$.

Proposition : *Le cardinal du groupe* $\mathrm{SL}(E)$ *est*

$$\mathrm{Card}(\mathrm{SL}_n(\mathbb{F}_q)) = \frac{1}{q-1} \cdot \prod_{k=0}^{n-1}(q^n - q^k).$$

Démonstration :
1) En fixant une base de E, on obtient une bijection de $\mathrm{SL}(E)$ sur $\mathrm{SL}_n(\mathbb{F}_q)$ qui ont donc le même cardinal.
2) Le morphisme de groupes $\det : \mathrm{GL}(E) \to \mathbb{F}_q^*$ est surjectif de noyau $\mathrm{SL}(E)$. On a donc la relation

$$\mathrm{Card}(\mathrm{GL}(E)) = \mathrm{Card}(\mathrm{SL}(E)) \cdot \mathrm{Card}(\mathbb{F}_q^*),$$

d'où le résultat. □

Finalement, rappelons que les centres respectifs de $\mathrm{GL}(E)$ et de $\mathrm{SL}(E)$ ne contiennent que des homothéties.

Proposition : *Le centre de* $\mathrm{GL}(E)$ *est de cardinal* $q-1$ *et le centre de* $\mathrm{SL}(E)$ *est de cardinal* $n \wedge (q-1)$.

Démonstration :
1) Les homothéties dans $\mathrm{GL}(E)$ sont les $\lambda \cdot \mathrm{Id}_E$ avec $\lambda \in \mathbb{F}_q^*$, d'où le résultat pour le cardinal du centre de $\mathrm{GL}(E)$.
2) Les homothéties dans $\mathrm{SL}(E)$ sont les $\lambda \cdot \mathrm{Id}_E$ avec $\lambda \in \mathbb{F}_q^*$ vérifiant $\lambda^n = 1$. Comme $\mathbb{F}_q^*$ est un groupe d'ordre $q-1$, on a $\lambda^{q-1} = 1$ pour tout $\lambda \in \mathbb{F}_q^*$. En notant $d = n \wedge (q-1)$, on en déduit que $\lambda^n = 1$ si et seulement si $\lambda^d = 1$ en utilisant l'identité de Bézout, donc

$$Z(\mathrm{SL}(E)) = \{\lambda \cdot \mathrm{Id}_E \in \mathrm{GL}(E) \mid \lambda \in \mathbb{F}_q^*, \quad \lambda^d = 1\}.$$

Finalement, comme d divise $q-1$ et que $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$, il est classique que $\{\lambda \in \mathbb{F}_q^* \mid \lambda^d = 1\}$ est l'unique sous-groupe d'ordre d de $\mathbb{F}_q^*$, d'où le résultat. □

2. Nombres de sous-espaces vectoriels

Dans cette partie, on va compter le nombre de sous-espaces vectoriels de E d'une dimension donnée.

Proposition : *Soit $d \in [\![0, n]\!]$. Le nombre de sous-espace vectoriels de E de dimension d est*

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \prod_{k=0}^{d-1} \frac{(q^n - q^k)}{(q^d - q^k)}.$$

Démonstration :
Si F est sous-espace vectoriel de E de dimension d, alors chaque base de F est une famille libre de cardinal d dans l'espace vectoriel E. Par le même argument utilisé pour $\mathrm{Card}(\mathrm{GL}(E))$, le nombre de telle famille libre est

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

De plus, l'espace vectoriel F admet $\mathrm{Card}(\mathrm{GL}_d(\mathbb{F}_q))$ bases distinctes. On conclut que le nombre cherché est $\alpha_d / \mathrm{Card}(\mathrm{GL}_d(\mathbb{F}_q))$, d'où le résultat. □

Remarques :

a) En particulier, le nombre de droites vectorielles dans E est $(q^n - 1)/(q - 1)$.

b) Le nombre $\begin{bmatrix} n \\ d \end{bmatrix}_q$ est appelé un coefficient q-binomial.

c) Comme un sous-espace vectoriel de E de dimension d correspond de manière unique à un sous-espace vectoriel de dimension $n - d$ de E^* par dualité, on en déduit la relation

$$\forall d \in [\![0, n]\!], \quad \begin{bmatrix} n \\ d \end{bmatrix}_q = \begin{bmatrix} n \\ n-d \end{bmatrix}_q.$$

Proposition : *Soit $(n_1, \dots, n_r) \in (\mathbb{N})^r$ avec $n_1 + \cdots + n_r = n$ et $r \in \mathbb{N}^*$. Le nombre de décompositions en somme directe $E = F_1 \oplus \cdots \oplus F_r$ où F_i est un sous-espace vectoriel de E vérifiant $\dim(F_i) = n_i$ pour tout $i \in [\![1, r]\!]$ est*

$$\frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{\mathrm{Card}(\mathrm{GL}_{n_1}(\mathbb{F}_q)) \cdots \mathrm{Card}(\mathrm{GL}_{n_r}(\mathbb{F}_q))}.$$

Démonstration :
Notons $\mathscr{D}$ l'ensemble des $(F_1, \dots, F_r)$ vérifiant les conditions ci-dessus. Le groupe $\mathrm{GL}(E)$ agit transitivement sur $\mathscr{D}$ par

$$u \cdot (F_1, \dots, F_r) = (u(F_1), \dots, u(F_r)).$$

De plus, le stabilisateur d'un élément $(F_1, \dots, F_r) \in \mathscr{D}$ est isomorphe à

$$\mathrm{GL}(F_1) \times \cdots \times \mathrm{GL}(F_r) \simeq \mathrm{GL}_{n_1}(\mathbb{F}_q) \times \cdots \times \mathrm{GL}_{n_r}(\mathbb{F}_q).$$

On obtient donc le résultat avec la formule usuelle

$$\mathrm{Card}(\mathrm{Orb}(F_1, \dots, F_r)) = \frac{\mathrm{Card}(\mathrm{GL}(E))}{\mathrm{Card}(\mathrm{Stab}(F_1, \dots, F_r))}.$$

□

3. Les endomorphismes diagonalisables

Dans la suite, si $n > q$, on considèrera que $\binom{q}{n} = 0$. Nous allons déterminer le nombre d'endomorphismes de E dont le polynôme caractéristique est scindé à racines simples.

Proposition : *Le nombre d'endomorphismes de E admettant un polynôme caractéristique scindé à racines simples est*

$$\binom{q}{n} \cdot \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{(q-1)^n}.$$

Démonstration :
1) Dans le cas où $q < n$, le cardinal cherché est nul, donc le résultat énoncé est valable. Dans la suite, on suppose que $q \geqslant n$.
2) En fixant une base, on se ramène à raisonner sur les matrices. On note $\mathscr{C}$ l'ensemble des matrices de $\mathscr{M}_n(\mathbb{F}_q)$ dont le polynôme caractéristique est scindé à racines simples. Le groupe $\mathrm{GL}_n(\mathbb{F}_q)$ agit par conjugaison sur $\mathscr{C}$. Deux matrices de $\mathscr{C}$ sont dans la même orbite pour cette action si et seulement si elles ont le même spectre. On en déduit qu'il y a $\binom{q}{n}$ orbites. De plus, tous les éléments de l'ensemble $\mathscr{C}$ sont diagonalisables et si $D \in \mathscr{C}$ est une matrice diagonale, on a par un calcul direct que

$$\mathrm{Stab}(D) = \{\mathrm{Diag}(\lambda_1, \dots, \lambda_n) \in \mathrm{GL}_n(\mathbb{F}_q) \mid (\lambda_1, \dots, \lambda_n) \in (\mathbb{F}_q^*)^n\}.$$

On obtient donc le résultat avec la formule usuelle

$$\mathrm{Card}(\mathrm{Orb}(D)) = \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{\mathrm{Card}(\mathrm{Stab}(D))} = \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{(q-1)^n}.$$

□

Exemple : En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a 6 matrices dans $\mathscr{M}_2(\mathbb{F}_2)$ admettant deux valeurs propres distinctes. Par un calcul direct, on trouve que ce sont les matrices

$$\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\0&1\end{pmatrix}.$$

On dispose aussi d'une formule pour le nombre de tous les endomorphismes diagonalisables de E.

Proposition : *Le nombre d'endomorphisme diagonalisable de E est*

$$\sum_{(n_1,\dots,n_q)\in\Omega_q} \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{\mathrm{Card}(\mathrm{GL}_{n_1}(\mathbb{F}_q)) \cdots \mathrm{Card}(\mathrm{GL}_{n_q}(\mathbb{F}_q))}$$

avec $\Omega_q = \{(n_1, \dots, n_q) \in \mathbb{N}^q \mid n_1 + \cdots + n_q = n\}$.

Démonstration :
Un endomorphisme diagonalisable $u \in \mathscr{L}(E)$ est caractérisé par la décomposition en somme directe

$$E = \bigoplus_{\lambda\in\mathbb{F}_q} F_\lambda \quad \text{avec} \quad F_\lambda = \mathrm{Ker}(u - \lambda \cdot \mathrm{Id}_E)$$

En distinguant selon le q-uplet des dimensions $(\dim(F_\lambda))_{\lambda\in\mathbb{F}_q}$, on obtient le résultat avec la dernière proposition de la partie précédente. □

Exemple : En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a $8 = 1+6+1$ matrices diagonalisables dans $\mathscr{M}_2(\mathbb{F}_2)$. Par un calcul direct, on trouve que ce sont les matrices

$$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\0&1\end{pmatrix}.$$

4. Dénombrement des endomorphismes nilpotents

En utilisant des méthodes analogues, nous allons montrer le résultat suivant.

Proposition : *On suppose que $n = \dim(E) \geqslant 2$. Le nombre d'endomorphismes nilpotents de E d'indice n est*

$$\frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{q^{n-1}(q^n-1)} = \prod_{k=0}^{n-2}(q^n - q^k).$$

Démonstration :
1) On travaille matriciellement. Avec la réduction de Jordan, on a qu'une matrice $M \in \mathscr{M}_n(\mathbb{F}_q)$ est nilpotente d'indice n si et seulement si elle est conjuguée à la matrice

$$J = \begin{pmatrix} 0 & & & (0) \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ (0) & & 1 & 0 \end{pmatrix}.$$

2) La matrice J est la matrice compagnon de X^n, donc J est matrice d'un endomorphisme cyclique. On en déduit que son commutant est $\mathbb{F}_q[J]$. De plus, si $P \in \mathbb{F}_q[X]$ avec $\deg(P) \leqslant n$, on a par un calcul direct de $P(J)$ que $P(J)$ est inversible si et seulement si $P(0) \neq 0$. On en déduit que

$$\mathrm{Card}(\mathrm{Com}(J) \cap \mathrm{GL}_n(\mathbb{F}_q)) = q^{n-1}(q-1).$$

3) Le groupe $\mathrm{GL}_n(K)$ agit transitivement sur la classe de conjugaison de J par conjugaison. On en déduit avec le point 2 que

$$\mathrm{Card}(\mathrm{Orb}(J)) = \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{\mathrm{Card}(\mathrm{Stab}(J))} = \frac{\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q))}{q^{n-1}(q-1)}.$$

□

Exemple : En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a 3 matrices nilpotentes d'indice 2 dans $\mathscr{M}_2(\mathbb{F}_2)$. Par un calcul direct, on trouve que ce sont les matrices

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Pour terminer, nous allons déterminer le nombre d'endomorphismes nilpotents de E. Nous commençons par rappeler un résultat général d'algèbre linéaire.

Décomposition de Fitting : *Si $u \in \mathscr{L}(E)$ est un endomorphisme, alors il existe un unique couple (F, G) de sous-espaces vectoriels stables par u tel que*

(i) On a la somme directe $E = F \oplus G$.

(ii) La restriction de u à F est nilpotente.

(iii) La restriction de u à G est inversible.

Démonstration :

On commence par remarquer que les conditions énoncées imposent nécessairement que F est la réunion des $\mathrm{Ker}(u^k)$ pour $k \in \mathbb{N}$ et G est l'intersection des $\mathrm{Im}(u^k)$ pour $k \in \mathbb{N}$. Réciproquement, c'est un exercice classique de montrer que ces deux sous-espaces vectoriels conviennent. □

Proposition : *Le nombre d'endomorphismes nilpotents de E est q^{n^2-n}.*

Démonstration :

Pour tout $k \in \mathbb{N}$, on note N_k le nombre d'endomorphismes nilpotents de $\mathbb{F}_q^k$ et G_k le nombre d'automorphismes de $\mathbb{F}_q^k$. D'après la décomposition de Fitting, on en déduit une bijection de $\mathscr{L}(E)$ sur l'ensemble des quadruplets (F, G, f, g) vérifiant $E = F \oplus G$ et $(f, g) \in \mathscr{L}(F) \times \mathrm{GL}(G)$ avec f nilpotent. On utilisant la formule déterminée précédemment pour le nombre de décomposition en somme directe de E avec deux sous-espaces vectoriels, on obtient donc la relation

$$q^{n^2} = \sum_{k=0}^{n} N_k \cdot G_{n-k} \cdot \frac{G_n}{G_k \cdot G_{n-k}} = \sum_{k=0}^{n} N_k \cdot \frac{G_n}{G_k}.$$

En utilisant la même relation pour l'indice $n-1$, on obtient

$$q^{n^2} = N_n + \frac{G_n}{G_{n-1}} \sum_{k=0}^{n-1} N_k \cdot \frac{G_{n-1}}{G_k} = N_n + \frac{G_n}{G_{n-1}} \cdot q^{(n-1)^2}.$$

En remplaçant G_n et G_{n-1} par leur valeur et en simplifiant, on a

$$q^{n^2} = N_n + q^{n-1}(q^n - 1)q^{(n-1)^2},$$

d'où le résultat en isolant N_n. □

Exemple : En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a 4 matrices nilpotentes dans $\mathscr{M}_2(\mathbb{F}_2)$. Par un calcul direct, on trouve que ce sont les matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$