Nombre de matrices diagonalisables dans $\mathcal{M}_n(\mathbb{F}_q)$

Leçons 101, 104, 123, 150, 155, 190
Salim Rostam

22 mai 2014

Référence : Oraux X-ENS, algèbre, tome 1, exercice 1.10 (donne l'idée de la démonstration).

Soit n un élément de $\mathbb{N}^*$ et soit q une puissance d'un nombre premier. On note $\mathcal{D}_n(q)$ l'ensemble des matrices de $\mathcal{M}_n(q) := \mathcal{M}_n(\mathbb{F}_q)$ diagonalisables sur $\mathbb{F}_q$; on s'intéresse au cardinal de $\mathcal{D}_n(q)$. On note $\chi_A(X) := \det(XI_n - A)$ le polynôme caractéristique d'une matrice A de taille n, et si X est un ensemble fini on note $|X|$ son cardinal.

Théorème 1. *Avec la convention* $|\mathrm{GL}_0(q)| = 1$ *on a la formule suivante :*

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1,\dots,m_q \in \mathbb{N} \\ m_1+\dots+m_q=n}} \frac{|\mathrm{GL}_n(q)|}{\prod_{i=1}^q |\mathrm{GL}_{m_i}(q)|}.$$

Remarquons tout de suite que l'on a une formule explicite pour le cardinal du groupe linéaire.

Lemme 2. *Pour* $m \in \mathbb{N}$ *on a* $|\mathrm{GL}_m(q)| = \prod_{i=0}^{m-1}(q^m - q^i) = q^{\frac{m(m-1)}{2}} \prod_{i=1}^m (q^i - 1)$.

Venons-en à la démonstration du théorème. On va se baser sur le fait suivant :

$$\mathcal{D}_n(q) = \{PDP^{-1} : D \in \mathcal{M}_n(q) \text{ diagonale et } P \in \mathrm{GL}_n(q)\}. \tag{1}$$

Remarquons que $\mathrm{GL}_n(q)$ agit par conjugaison sur $\mathcal{D}_n(q)$; pour $M \in \mathcal{D}_n(q)$, on note $\mathrm{Orb}(M)$ son orbite et $\mathrm{Stab}(M)$ son stabilisateur pour l'action de $\mathrm{GL}_n(q)$ sur $\mathcal{D}_n(q)$.

Définition 3. Soit χ un polynôme scindé unitaire sur $\mathbb{F}_q$ de degré n ; on écrit $\chi = \prod_{i=1}^r (X - \lambda_i)^{m_i}$ avec les $\lambda_i \in \mathbb{F}_q$ deux à deux distincts. On lui associe la matrice diagonale $D_\chi := \mathrm{diag}(\lambda_i I_{m_i})_{1 \leqslant i \leqslant r}$ et on note $\mathrm{Scal}_n^{\mathrm{b}}(q) := \{D_\chi : \chi \text{ polynôme scindé unitaire sur } \mathbb{F}_q \text{ de degré } n\}$.

Remarque 4. En réalité, D_χ dépend de l'ordre que l'on choisit pour les racines de χ mais cela n'est pas grave : la chose importante est que deux éléments distincts de $\mathrm{Scal}_n^{\mathrm{b}}(q)$ ont leur polynôme caractéristique distinct (le polynôme caractéristique de D_χ étant bien sûr χ).

Lemme 5. $\mathrm{Scal}_n^{\mathrm{b}}(q)$ *est un système de représentants des orbites de* $\mathcal{D}_n(q)$ *sous l'action de* $\mathrm{GL}_n(q)$*, en particulier :*

$$\mathcal{D}_n(q) = \bigsqcup_{D \in \mathrm{Scal}_n^{\mathrm{b}}(q)} \mathrm{Orb}(D).$$

Démonstration. Tout d'abord, chaque $D' \in \mathcal{D}_n(q)$ possède au moins un représentant de son orbite dans $\mathrm{Scal}_n^{\mathrm{b}}(q)$, à savoir $D_{\chi_{D'}}$. En effet, D' est semblable à une matrice diagonale et cette matrice diagonale est semblable à $D_{\chi_{D'}}$ (par une matrice de permutation par exemple : il suffit de permuter les vecteurs de la base). Finalement, si χ et ψ sont deux polynômes scindés unitaires sur $\mathbb{F}_q$ de degré n tels que $D_\chi \in \mathrm{Orb}(D_\psi)$ alors D_χ et D_ψ sont semblables ; elles ont donc le même polynôme caractéristique d'où $\chi = \psi$. □

Une conséquence immédiate de ce lemme est la chose suivante (formule des classes) :

$$|\mathcal{D}_n(q)| = \sum_{D \in \mathrm{Scal}_n^{\mathrm{b}}(q)} |\mathrm{Orb}(D)|. \tag{2}$$

Lemme 6. *Pour $D \in \mathrm{Scal}_n^{\mathrm{b}}(q)$ on a $\mathrm{Stab}(D) = \mathcal{C}(D) \cap \mathrm{GL}_n(q)$ où $\mathcal{C}(D) := \{M \in \mathcal{M}_n(q) : MD = DM\}$ est le commutant de D.*

Démonstration. Soit $P \in \mathcal{M}_n(q)$; on a $P \in \mathrm{Stab}(D)$ ssi $P \in \mathrm{GL}_n(q)$ et $PDP^{-1} = D$ ssi $P \in \mathrm{GL}_n(q)$ et $PD = DP$ ssi $P \in \mathrm{GL}_n(q) \cap \mathcal{C}(D)$. □

D'après l'équation (2) et la relation orbite–stabilisateur, il reste donc plus qu'à déterminer $|\mathcal{C}(D) \cap \mathrm{GL}_n(q)|$.

Lemme 7. *Pour $D = \mathrm{diag}\,(\lambda_i I_{m_i})_{1 \leqslant i \leqslant r} \in \mathrm{Scal}_n^{\mathrm{b}}(q)$ (avec les λ_i deux à deux distincts) on a la formule suivante :*

$$|\mathcal{C}(D) \cap \mathrm{GL}_n(q)| = \prod_{i=1}^{r} |\mathrm{GL}_{m_i}(q)|.$$

Démonstration. Soit D comme dans l'énoncé et soit $P \in \mathcal{C}(D)$. Comme D et P commutent, les sous-espaces propres de D sont stables par P, autrement dit P est de la forme $P = \mathrm{diag}(P_i)_{1 \leqslant i \leqslant r}$ avec $P_i \in \mathcal{M}_{m_i}(q)$. Réciproquement, on vérifie que si P est de cette forme alors $P \in \mathcal{C}(D)$. Finalement, pour avoir $P \in \mathrm{GL}_n(q)$ il faut et il suffit de choisir chaque P_i dans $\mathrm{GL}_{m_i}(q)$, ce qui conclut la preuve. □

Démonstration du théorème. Par les lemmes précédents et la relation orbite–stabilisateur on obtient :

$$|\mathcal{D}_n(q)| = \sum_{D \in \mathrm{Scal}_n^{\mathrm{b}}(q)} \frac{|\mathrm{GL}_n(q)|}{\prod_{i=1}^{r} |\mathrm{GL}_{m_i}(q)|}$$

où l'on écrit les matrices $D \in \mathrm{Scal}_n^{\mathrm{b}}(q)$ sous une forme $D = \mathrm{diag}(\lambda_i I_{m_i})$ avec les $\lambda_i \in \mathbb{F}_q$ deux à deux distincts. Le but est maintenant de réindexer la somme ; en particulier, la description actuelle n'est pas la plus adaptée car les valeurs propres des matrices D n'interviennent pas. On se souvient que, par construction, $\mathrm{Scal}_n^{\mathrm{b}}(q)$ est en bijection avec l'ensemble des polynômes unitaires scindés sur $\mathbb{F}_q$ de degré n ; or, ce dernier ensemble est lui-même en bijection avec l'ensemble des q-uplets $(m_1, \ldots, m_q) \in \mathbb{N}^q$ de somme n. En effet, en écrivant $\mathbb{F}_q =: \{\mu_1, \ldots, \mu_q\}$ l'application qui à un q-uplet $(m_1, \ldots, m_q)$ de somme n associe le polynôme $\prod_{i=1}^{q} (X - \mu_i)^{m_i}$ est une bijection sur les polynômes unitaires scindés sur $\mathbb{F}_q$ de degré n. On obtient alors la forme énoncée dans le théorème. □

Remarque 8. On peut réécrire le résultat sous la forme :

$$|\mathcal{D}_n(q)| = \sum_{\substack{m_1 \leqslant \cdots \leqslant m_q \in \mathbb{N} \\ m_1 + \cdots + m_q = n}} \binom{q}{\nu_0(m), \ldots, \nu_n(m)} \frac{|\mathrm{GL}_n(q)|}{\prod_{i=1}^{q} |\mathrm{GL}_{m_i}(q)|}$$

où :

- $\nu_i(m) := |\{j \in \{1,\ldots,q\} : m_j = i\}|$;
- $\binom{a}{b_0,\ldots,b_n} := \frac{a!}{b_0!\cdots b_n!}$ est le coefficient multinomial.

En effet, une fois qu'un q-uplet $m = (m_1,\ldots,m_q)$ est fixé alors on peut générer directement plusieurs polynômes scindés de degré n (*i.e.* pas seulement $\prod(X-\mu_i)^{m_i}$) ; par exemple avec $q = 3$, le couple $(0,1,1)$ peut aussi bien représenter $X(X-1)$ que $X(X-2)$ ou encore $(X-1)(X-2)$. Le nombre de polynômes que l'on peut générer à partir d'un q-uplet m est alors $\binom{q}{\nu_0}\binom{q-\nu_0}{\nu_1}\cdots\binom{q-\nu_0-\cdots-\nu_{i-1}}{\nu_n} = \frac{q!}{\nu_0!(q-\nu_0)!}\frac{(q-\nu_0)!}{\nu_1!(q-\nu_0-\nu_1)!}\cdots\frac{(q-\nu_0-\cdots-\nu_{i-1})!}{\nu_n!0!} = \frac{q!}{\nu_0!\nu_1!\cdots\nu_n!}$ qui est bien le coefficient multinomial qui apparaît.