Nombre d'automorphismes diagonalisables sur un corps fini

Dans le développement proposé ici, on dénombre les matrices inversibles à coefficients dans un corps fini $\mathbb{F}_q$ qui sont diagonalisables. Ce développement peut être utilisé dans les leçons suivantes :

Groupes opérant sur un ensemble. Exemples et applications.
Groupes finis. Exemples et applications.
Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $\mathrm{GL}(E)$.
Applications.
Nombres premiers. Applications.
Corps finis. Applications.
Endomorphismes diagonalisables.
Méthodes combinatoires, problèmes de dénombrement.

Théorème : *Soit $n \geq 1$ un entier. Alors le nombre de matrices diagonalisables dans le groupe linéaire $\mathrm{GL}_n(\mathbb{F}_q)$ sur le corps fini $\mathbb{F}_q$ est égal à*

$$\sum_{\substack{(n_1,\dots,n_{q-1}) \\ \text{t.q. } n_1+\cdots+n_{q-1}=n}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)|\dots|\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}\,.$$

La preuve utilise d'abord un exercice de [Gourdon] (page 176), puis adapte un argument que l'on trouve dans [FGN1] (*Nombre d'involutions*, page 17).

Preuve : On commence par observer qu'une matrice $A \in \mathrm{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^q - A = 0$. En effet si A est diagonalisable, on peut écrire $A = PDP^{-1}$ avec D diagonale. Comme les coefficients de D sont dans $\mathbb{F}_q$ on a $D^q = D$ dont on déduit $A^q = A$. Réciproquement, si $A^q = A$, alors A est annulé par le polynôme $X^q - X$, qui est à racines simples. Donc le polynôme minimal de A, diviseur de $X^q - X$, est à racines simples, donc A est diagonalisable.

Si $A \in \mathrm{GL}_n(\mathbb{F}_q)$, alors A est diagonalisable ssi $A^{q-1} = \mathrm{Id}$. Or on sait que le groupe multiplicatif $\mathbb{F}_q^\times$ est cyclique. Choisissons un générateur ζ : c'est donc une racine primitive $(q-1)$-ième de l'unité. Dès lors, on a la factorisation

$$X^{q-1} - 1 = (X-1)(X-\zeta)\dots(X-\zeta^{q-2})$$

On a donc $(A-\mathrm{Id})(A-\zeta\,\mathrm{Id})\dots(A-\zeta^{q-2}\,\mathrm{Id}) = 0$. Comme les polynômes $X-\zeta^i$ sont premiers entre eux, on en déduit que $E = \oplus E_i$ où $E_i = \ker(A-\zeta^i\,\mathrm{Id})$ pour $i = 0,\dots,q-2$. (On peut faire courrir i de 1 à $q-1$, ce qui ne change rien et donne une notation plus agréable.) Soit $n_i = \dim(E_i)$, on a $n_1 + \cdots + n_{q-1} = n$. Réciproquement, étant donné un $(q-1)$-uplet de sous-espaces vectoriels qui décomposent E en somme directe, l'automorphisme A est complètement déterminé puisque sa restriction à E_i est la multiplication par ζ^i. On a donc une bijection entre l'ensemble des matrices diagonalisables et l'ensemble des tels uplets, pour $(n_1,\dots,n_{q-1})$ variable.

Pour chaque $N = (n_1,\dots,n_{q-1})$ fixé, notons Z_N l'ensemble des $(q-1)$-uplets de sous-espaces vectoriels comme ci-dessus ; nous allons dénombrer Z_N. Il y a une action de $G = \mathrm{GL}_n(\mathbb{F}_q)$ sur

Z_N, qui à (E_i) associe $(g(E_i))$. Étant donnés des uplets (E_i) et (E'_i), on peut choisir des bases $(e_{i,j})$, $(e_{i,j})$ de E_i resp. E'_i (avec le même nombre d'éléments). On définit un automorphisme linéaire g qui envoie $e_{i,j}$ sur $e'_{i,j}$, de sorte que $g.(E_i)) = (E'_i)$. Il en résulte que l'action de G sur Z_N n'a qu'une orbite. Par ailleurs, le stabilisateur de (E_i) est constitué des automorphismes qui stabilisent chaque E_i, donc c'est le produit des $\mathrm{GL}_{n_i}(\mathbb{F}_q)$. Il s'ensuit que le cardinal de Z_N est égal à

$$\frac{|\,\mathrm{GL}_n(\mathbb{F}_q)|}{|\,\mathrm{GL}_{n_1}(\mathbb{F}_q)|\ldots|\,\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}$$

Le nombre de matrices diagonalisables dans $\mathrm{GL}_n(\mathbb{F}_q)$ est la somme des cardinaux des Z_N, ce qui donne le résultat. □

Bibliographie

[FGN1] Francinou, Gianella, Nicolas, Exercices de mathématiques des oraux de l'Ecole polytechnique et des Ecoles normales supérieures : Algèbre, Tome I, *Cassini*.
[Gourdon] Gourdon, Algèbre, *Ellipses*.