Nombre d'automorphismes diagonalisables sur un corps fini

Julie Parreaux

2018-2019

Références du développement : H2G2 [4, p.66] ; Gourdon [5, p.176] ; X-ENS algèbre 1 [8, p.17].

Leçons où on présente le développement : 101 (Action de groupe) ; 104 (Groupe fini) ; 106 (Groupe linéaire) ; 190 (Dénombrement).
Leçons où on peut en parler : 121 (Nombre premier) ; 123 (Corps fini).

1 Introduction

Le nombre de matrice sur un corps fini est dénombrable (et même fini). On peut alors compter le nombre de matrice vérifiant certaines propriétés comme le fait qu'elle soit ou non diagonalisable. Les actions de groupes sont un bon moyen de dénombrer des ensembles finis. Ici, on utilise la formule des classes pour une action naturelle du groupe linéaire d'un corps fini.

2 Matrice diagonalisable sur $\mathbb{F}_q$

Schéma du développement

1. Énumération d'espaces vectoriels via une action de groupe.
   (a) Définition de l'action.
   (b) Cette action est transitive.
   (c) Calcul du cardinal.
2. Caractérisation des automorphismes diagonalisables.
3. Preuve du théorème.

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

$$\sum_{\substack{n_1,\dots,n_{q-1} \\ n_1+\cdots+n_{q-1}=n}} \frac{\left|GL_n(\mathbb{F}_q)\right|}{\left|GL_{n_1}(\mathbb{F}_q)\right| \cdots \left|GL_{n_{q-1}}(\mathbb{F}_q)\right|}$$

Démonstration. Soit $n \geq 1$ un entier. Calculons le nombre de matrices diagonalisables dans le groupe linéaire $GL_n(\mathbb{F}_q)$ sur le corps fini $\mathbb{F}_q$.

Étape 1 : énumération d'espaces vectoriels via une action de groupe.

Lemme 1. *Soit $\mathcal{E}_k$ l'ensemble des k-uplets $(E_1, \dots E_k)$ de sous-espaces de $\mathbb{F}_q^n$ tels que $E_1 \oplus \cdots \oplus E_k = \mathbb{F}_q^n$ avec $\dim E_i = n_i$ pour $1 \leq i \leq k$. Alors*

$$|\mathcal{E}_k| = \frac{\left|GL_n(\mathbb{F}_q)\right|}{\left|GL_{n_1}(\mathbb{F}_q)\right| \cdots \left|GL_{n_{q-1}}(\mathbb{F}_q)\right|}$$

Démonstration. On fait agir $GL_n(\mathbb{F}_q)$ sur $\mathcal{E}_k$ par l'action naturelle $g.(E_1,\dots,E_k) = (g(E_1),\dots,g(E_k))$.

Étape a : l'action est bien définie.

— $\dim(g(E_i)) = \dim(E_i)$ ($g \in GL_n(\mathbb{F}_q)$ donc g est un isomorphisme) $= n_i$ (hypothèse)

— Comme les E_i sont en somme directe montrons que les $g(E_i)$ le sont également.

- Soit $y \in \sum_{i=1}^k g(E_i)$. Supposons que $y = \sum_{i=1}^k g(x_i) = \sum_{i=1}^k g(\tilde{x}_i)$.
- Par linéarité de g $(\in GL_n(\mathbb{F}_q))$, $y = g\left(\sum_{i=1}^k x_i\right) = g\left(\sum_{i=1}^k \tilde{x}_i\right)$.
- Par application de g^{-1} $(\in GL_n(\mathbb{F}_q))$, $\sum_{i=1}^k x_i = \sum_{i=1}^k \tilde{x}_i$.
- Comme les E_i sont en somme directe, $\forall i, x_i = \tilde{x}_i$. Donc les $g(E_i)$ sont en somme directe.

Étape b : l'action est transitive : $\forall x, y \in \mathcal{E}_k, \exists! g \in GL_n(\mathbb{F}_q)$ tel que $g.x = y$.

— Pour tout k-uplet $(E_1,\dots,E_k) \in \mathcal{E}_k$, on construit une base de $\mathbb{F}_q^n$ en compilant les bases de E_i, $1 \leq i \leq k$ (caractérisation d'une somme directe).

— Pour deux k-uplets $(E_i)_i$ et $(E_i')_i$ de $\mathcal{E}_k$, on construit deux bases e et e'.

— $g \in GL_n(\mathbb{F}_q)$ qui envoie e sur e' (existe par changement de bases), envoie E_i sur E_i' (construction des bases).

Étape c : étude du cardinal Montrons que $|\mathcal{E}_k| = \dfrac{|GL_n(\mathbb{F}_q)|}{|GL_{n_1}(\mathbb{F}_q)|\cdots|GL_{n_{q-1}}(\mathbb{F}_q)|}$.

— $Stab_{(E_i)}$ est le sous-groupe de $GL_n(\mathbb{F}_q)$ qui stabilise tous les E_i (par définition de $Stab_{(E_i)}$).

— On applique la formule des classes au sous-groupe $\prod_i GL(E_i)$ (diagonal par bloc) $= \prod_i GL_{n_i}(\mathbb{F}_q)$.

□

Étape 2 : caractérisation des automorphismes diagonalisables.

Lemme 2 ([5, p.176]). *Une matrice $A \in \mathcal{M}_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^q = A$.*

Démonstration. $\Rightarrow$ A diagonalisable : $A = P^{-1}\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} P$ avec $P \in GL_n(\mathbb{F}_q)$ et $(\lambda_i)_{1\leq i\leq n} \in \mathbb{F}_q$.

$$A^q = P^{-1}\begin{bmatrix} \lambda_1^q & & \\ & \ddots & \\ & & \lambda_n^q \end{bmatrix} P \text{ (puissance)} = P^{-1}\begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} P \ (\mathbb{F}_q^\times \text{ est cyclique : } x^q = x)$$

$= A$.

$\Leftarrow$ $X^q - X$ est un polynôme annulateur de A (par hypothèse). Soit ξ un générateur de $\mathbb{F}_q^\times$ (qui est cyclique), alors $X^q - X = X(X^{q-1} - 1) = X\prod_{i=1}^{q-1}(X - \xi^i)$. Le polynôme annulateur est alors scindé donc A est diagonalisable.

□

Corollaire. *Une matrice $A \in GL_n(\mathbb{F}_q)$ est diagonalisable si et seulement si $A^{q-1} - I_n = 0$.*

Démonstration. Soit $A \in GL_n(\mathbb{F}_q)$.

A est diagonalisable si et seulement si $A^q - A = 0$ (lemme 2)
si et seulement si $A^{q-1} - I_n = 0$ ($A \in GL_n(\mathbb{F}_q)$ donc A est inversible)

□

Étape 3 : preuve du théorème. Montrons maintenant le théorème. On ordonne de 1 à q les éléments de $\mathbb{F}_q = \{\xi^i, 1 \leq i \leq q\}$. Pour toute famille d'entiers positifs $(n_i)_{1\leq i\leq q}$ telle que $\sum n_i = n$, on note $\mathcal{E}_{q,(n_i)}$ l'ensemble $\mathcal{E}_k$ du lemme 1. Construisons une bijection entre l'ensemble des matrices diagonalisables et la réunion sur l'ensemble des (n_i) tel que $\sum n_i = n$ des $\mathcal{E}_{q,(n_i)}$.

→ Soit A une matrice diagonalisable de $\mathcal{M}_n(\mathbb{F}_q)$.

— On assigne à la matrice diagonalisable A la famille des sous-espaces $(E_i)_{1\leq i\leq q} = E_A$ où E_i est le sous-espace propre de A pour la valeur propre $\xi_i \in \mathbb{F}_q$ ou $E_i = 0$ sinon.

— A est diagonalisable : $A^q - A = 0$ (par le lemme 2). De plus, $X^{q-1} - 1 = \prod_{i=1}^{q-1}(X - \xi^i)$. On en déduit que $\mathbb{F}_q^n = \bigoplus_{i=1}^{q-1}\left(A - \xi^i I_n\right)$ avec $E_i = \left(A - \xi^i I_n\right)$. Donc $(E_i)_i \in \mathcal{E}_{q,\dim E_i}$.

→ Soit (n_i) tel que $\sum_{i=1}^{q} n_i = n$. Pour tout $(E_i)_i$ de $\mathcal{E}_{q,n_i}$, on fait correspondre $A_{(E_i)}$ de l'endomorphisme φ de $\mathbb{F}_q^n$ tel que $\varphi(z_i) = \xi_i z_i$.

D'où la bijection ($A \mapsto E_A$ et $(E_i) \mapsto A_{(E_i)}$). On en déduit le résultat en appliquant le lemme 1 à l'union. □

3 Quelques notions utiles

Action de groupe

Les actions de groupes [2, p.195] sont des notions importantes car elles permettent d'agir sur un ensemble. Elles ont plusieurs applications notamment en géométrie (c'est la base de la géométrie) ou en dénombrement si le groupe est fini (via les formules sur les cardinaux).

Remarque : Il y a deux monde : celui des groupes et des objets sur lesquels ils agissent. La translation dans le monde des objets (par application de l'action) se traduit par la conjugaison dans les groupes.

Définition (Action de groupes)**.** Une action de groupe d'un groupe G sur un ensemble X est une application $f : G \times X \to X$ telle que $\forall x \in X, f(e,x) = x$ et $\forall g_1, g_2 \in G, \forall x \in X, f(g_1.g_2, x) = f(g_1, f(g_2, x))$.

Une action de groupe de G sur X peut être également la donné d'un morphisme de G dans $\mathfrak{S}_{|X|}$.

Définition (Action fidèle [1, p.174])**.** Soit G un groupe agissant sur E. On dit que G agit fidèlement sur E si pour tout $g \in G$, $gx = x$ pour tout $x \in E$ implique $g = 1_G$ (le neutre). Autrement dit si le morphisme de l'action est injectif.

Exemple (Actions de groupes) : Donnons quelques exemples classiques d'actions de groupes.

— G opère sur G par translation à gauche.

— G opère sur $\mathcal{P}(G)$ par translation à gauche.

— G opère sur G par conjugaison.

— G opère sur $\mathcal{P}(G)$ par conjugaison.

Définition (Stabilisateur)**.** On définit le stabilisateur de l'action, pour tout élément $x \in X$, comme $\mathrm{Stab}(x) = \{g \in G, f(g,x) = x\}$.

Remarque : Le stabilisateur d'un élément x de X est vu comme l'ensemble des éléments (de G) qui stabilise, "laisse fixe" x lors de l'application de f. On vérifie facilement que $\mathrm{Stab}(x)$ est un sous-groupe de G.

Définition (Action libre [3, p.16])**.** Une action de G sur X est libre si tous les stabilisateurs des points de X sont triviaux.

Proposition ([3, p.15])**.** *Soit G un groupe opérant sur un ensemble X et $x \in X$. Alors,* $\mathrm{Stab}(g.x) = g\mathrm{Stab}(x)g^{-1}$.

Démonstration. $\left(g\mathrm{Stab}(x)g^{-1}\right).(g.x)$(Action du groupe $\left(g\mathrm{Stab}(x)g^{-1}\right)$ sur l'image) $= \left(g\mathrm{Stab}(x)\right).x$ (calcul des actions) $= g.x$ (stabilisateur). On en déduit l'inclusion $\subseteq$. En remplaçant x par $g.x$ et g par g^{-1}, on obtient par le même procédé, l'inclusion inverse. □

Proposition ([9, p.31])**.** *Soit $\varphi : G \to \mathfrak{S}(X)$ une action de G sur l'ensemble X. Alors,* $\ker(\varphi) = \bigcap_{x\in X} \mathrm{Stab}(x)$.

Démonstration. Si $g \in \ker(\varphi)$, $g.x = \varphi(g)(x) = e.x = x$ et $g \in \bigcap_{x\in X} \mathrm{Stab}(x)$. Inversement, $g.x = \varphi(g)(x) = x$ et $g \in \ker(\varphi)$. □

Remarque : On justifie ainsi la définition d'action fidèle et notamment l'injectivité du morphisme.

Proposition ([9, p.42]). *Si $m \leq n$, alors si $\mathfrak{S}_n$ agit sur $\mathfrak{S}_m$ alors $\mathfrak{S}_m \simeq \bigcap_{p\in\{m+1,\dots,n\}} \mathrm{Stab}(p)$.*

Lemme ([1, p.172]). *Soit G opérant sur un ensemble E. La relation sur E définie par $x \sim y$ s'il existe $g \in G$ tel que $y = g.x$ est une relation d'équivalence.*

Démonstration. **Reflexive** On prend $g = 1_G$
Symétrique On multiplie par g^{-1}
Transitive On utilise les propriétés de calcul
□

Définition (Orbite). L'orbite de l'action, pour tout élément $x \in X$, comme : $\mathrm{Orb}(x) = \{y \in X | \exists g \in G, f(g,x) = y\}$.

Remarque : Une orbite est une classe d'équivalence sur la relation d'équivalence définie précédemment. Une orbite d'un élément x de X comme l'ensemble des éléments (de X) atteignable à partir de x en appliquant f à un g.

Exemple (Exemples sur ces notions) : Quelques exemples sur les notions d'orbites et de stabilisateurs.
- G opère sur G par translation à gauche.
  - $\mathrm{Stab}(x) = \{e\}$
  - $\mathrm{Orb}(x) = G$ (ici $X = G$)

Définition (Action transitive [1, p.172]). On dit que G agit transitivement sur E si pour tous $x, x' \in E$, il existe $g \in G$ tel que $x' = gx$.

Lemme ([1, p.172]). *Soit G agissant sur E. Alors les propriétés suivantes sont équivalentes :*
1. *G agit transitivement sur E*
2. *$\forall x \in E, \mathrm{Orb}(x) = E$*
3. *$\exists x_0 \in E$ tel que $\mathrm{Orb}(x_0) = E$*
4. *E n'admet qu'une seule orbite : E*

Démonstration. **Montrons** $1 \Rightarrow 2$ $\mathrm{Orb}(x) \subseteq E$: définition. $\mathrm{Orb}(x) \supseteq E$: si $x' \in E$, $\exists g$ tel que $x' = g.x$, alors $x' \in \mathrm{Orb}(x)$.
Montrons $2 \Rightarrow 3$ Évident
Montrons $3 \Rightarrow 4$ Par la relation d'équivalence : les classes forment une partition.
Montrons $4 \Rightarrow 1$ Soient $x, x' \in E$, alors x, x' sont dans la même orbite. Donc, il existe g tel que $x' = gx$.
□

Définition (Points fixes). Nous définition les points fixes d'un élément g de G comme l'ensemble des éléments (de X) qui sont stabilisés par g. De manière plus formelle on définit l'orbite comme $\mathrm{Fix}(g) = \{x \in X, f(g,x) = x\}$.

Lemme ([1, p.172]). *Soit G agissant sur E. Alors les propriétés suivantes sont équivalentes :*
1. *x est un point fixe sous l'action de G*
2. *$\mathrm{Orb}(x) = \{x\}$*
3. *$|\mathrm{Orb}(x)| = 1$*
4. *$\mathrm{Stab}(x) = G$*

Démonstration. **Montrons** $1 \Rightarrow 2$ Définition orbite et point fixe.
Montrons $2 \Rightarrow 3$ Évident
Montrons $3 \Rightarrow 4$ $\mathrm{Stab}(x) \subseteq G$: ok ; $\mathrm{Stab}(x) \supseteq G$: comme $|\mathrm{Orb}(x)| = 1$, $\forall g$, $g.x = x$. Donc $\forall g$, $g \in \mathrm{Stab}(x)$.
Montrons $4 \Rightarrow 1$ Définition orbite et point fixe.
□

Lemme. *Soit G un groupe et X un ensemble sur lequel G agit. Pour tout élément $x \in X$, on a la relation suivante : $|\mathrm{Stab}(x)|\,|\mathrm{Orb}(x)| = |G|$*

Démonstration. On prouve cette relation à l'aide d'une bijection entre Orb et G/Stab.
Soit $x \in X$. On pose

$$\begin{array}{rccc} \varphi_x : & G/\mathrm{Stab} & \to & \mathrm{Orb} \\ & g & \mapsto & f(g,x) \end{array}$$

Cette application est bien définie car Stab est un sous-groupe de G donc le quotient est bien un groupe. (Attention : ce n'est pas un morphisme car Orb est un sous-ensemble de X.) De plus, elle est surjective par définition de l'orbite.

Elle est injective. En effet, si $g_1, g_2 \in G$ tels que $f(g_1,x) = f(g_2,x)$. On a alors, en composant par g_1^{-1}, $f(g_1^{-1}, f(g_1,x)) = f(g_1^{-1}, f(g_2,x))$. Par les propriétés sur f, on a $f(g_1^{-1}g_1, x) = f(g_1^{-1}g_2, x)$. Or, comme $f(e,x) = x$, on a $f(g_1^{-1}g_2, x) = f(g_1^{-1}g_1, x) = f(e,x) = x$.

On a donc bien une bijection entre ces deux ensembles finis et on conclut en passant aux cardinaux. □

Lemme. *Soit G un groupe et X un ensemble sur lequel G agit. On a la relation suivante $\sum_{g\in G} |\mathrm{Fix}(g)| = \sum_{x\in X} |\mathrm{Stab}(x)|$*

Démonstration. On pose un ensemble $S = \{(g,x) \in G \times X | f(g,x) = x\}$. On pose ensuite l'application S définie telle que :

$$\begin{array}{rccc} S : & G \times X & \to & \{0,1\} \\ & g, x & \mapsto & \begin{cases} 1 & \text{si } (g,x) \in S \\ 0 & \text{sinon} \end{cases} \end{array}$$

Comme $\mathrm{Stab}(x)$ et $\mathrm{Fix}(g)$ forment des partitions respectivement de X et de G, on a $S(.,x) = \mathbb{1}_{\mathrm{Stab}(x)}$ et $S(g,.) = \mathbb{1}_{\mathrm{Fix}(g)}$. On a alors $|S| = \sum_{g\in G} |\mathrm{Fix}(g)| = \sum_{x\in X} |\mathrm{Stab}(x)|$. D'où le résultat. □

Théorème (Formule du Burnside). *Soit G un groupe et X un ensemble sur lequel G agit. Le nombre d'orbite de l'action est $t = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$*

Démonstration. On va alors montrer que $t\,|G| = \sum_{g\in G}|Fix(g)|$. On remarque que $X = \sqcup_{i=1}^{t}\mathrm{Orb}(x_i)$ où x_i est un représentant d'un des orbites. Comme on a $\sum_{g\in G}|\mathrm{Fix}(g)| = \sum_{x\in X}|\mathrm{Stab}(x)|$ (lemme 3) $= \sum_{i=1}^{t}|\mathrm{Orb}(x_i)|\,\frac{|G|}{|\mathrm{Orb}(x_i)|}$ (lemme 3) $= t\,|G|$ (G indépendant somme). D'où le résultat. □

Remarque : On voit apparaître une version de la formule des classes.

Actions associées à l'action d'un groupe et invariants [7, p.47]

Proposition. *Soit G un groupe opérant sur un ensemble E, $p \in \mathbb{N}*$, alors G opère de façon naturelle sur $E^p = E_\times \cdots \times$ par $g(x_1,\ldots,g_p) = (gx_1,\ldots gx_p)$.*
G opère aussi sur $\mathcal{P}(E)$, l'ensemble des sous-ensembles de E par l'action : si $A \in \mathcal{P}(E)$, $gA = \{ga, a \in A\}$.

De plus, si G opère sur E et F, il opère sur l'ensemble des fonctions de E dans F.

Définition. Soit G un groupe opérant sur E. Un élément $x \in E$ est dit invariant quand : $\forall g \in G, gx = x$.

Si on se donne un espace homogène (G, E), un ensemble K et qu'on fait opérer G sur K de manière triviale, on cherche le plus petit entier p et une (ou plusieurs) fonction invariante $f : E^p \to K$. Cette recherche est la recherche d'invariant pour notre action de groupe et dans ce cas précis pour la géométrie que l'on considère.

Cette recherche d'invariant permet la classification des figures. Si on se donne une géométrie par un espace homogène (G, E). On considère l'espace des orbites $\mathcal{P}(E)/G$ (définit par l'action de G sur $\mathcal{P}(E)$) et on cherche suffisamment d'invariant sur chaque orbite pour les caractériser (puisqu'une figure en géométrie correspond à une orbite de cette action).

Dénombrement sur des ensembles de matrices

Nous donnons ici une batterie de cardinaux [4, p.57] liés au groupe linéaire $GL_n(\mathbb{F}_q)$. On note l'entier n quantique $[n]_q = 1 + \cdots + q^{n-1}$ que l'on peut considérer comme une q-déformation du nombre n : si $q = 1$, on retrouve n.

On définit de même le factoriel et le coefficient binomial quantique. Pour $m_1,\ldots,m_k$ dans $\mathbb{N}$ tels que $m_1 + \cdots + m_k = n$, on définit le nombre multinomial quantique :

$$[n]_q! = [n]_q[n-1]_q\ldots[1]_q \qquad [0]_q! = 1 \qquad \begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{[n_q]!}{[m]_q![n-m]_q!} \qquad \begin{bmatrix} n \\ m_1\ldots m_k \end{bmatrix}_q = \frac{[n]_q!}{\prod_{i=1}^{k}[m_i]_q!}$$

Lemme (Espace et sous-espace). *Soit $n, q \in \mathbb{N}$.*

1. *L'espace vectoriel : $|E| = |\mathbb{F}_q^n| = q^n$*
2. *L'espace projectif : $|\mathbb{P}(E)| = [n]_q$*
3. *Grassmannienne : $|Gr_{m,n}(\mathbb{F}_q)| = \begin{bmatrix} n \\ m \end{bmatrix}_q$*

Démonstration.
1. Existence d'une base.
2. On fait agir le groupe multiplicatif $\mathbb{K}^*$ sur $\mathbb{K}^{n+1}\setminus\{0\}$ par homothéties ($\lambda \in \mathbb{K}^*$ agit sur v par $\lambda.v = \lambda v$). L'action est libre : $\forall v \neq 0, Stab_{\mathbb{K}^*}(v) = \{1\}$. On en déduit que : $|\mathbb{P}^n(\mathbb{F}_q)| = \frac{|\mathbb{F}_{q^{n+1}}\setminus\{0\}|}{|\mathbb{F}_q^*|} = \frac{q^{n+1}-1}{q-1} = 1 + q + \cdots + q^n$.
3. $GL_n(\mathbb{K})$ agit transitivement sur la grassmannienne $Gr_{m,n}(\mathbb{K})$. Le stabilisateur d'un sous-espace F est donné par $Stab(F) = (GL_m(\mathbb{K}) \times GL_{n-m}(\mathbb{K}) \ltimes \mathcal{M}_{m,n-m}(\mathbb{K})$.

□

Lemme (Groupes et sous-groupes). *Soit $n, q \in \mathbb{N}$.*

1. *Groupe linéaire : $|GL_n(\mathbb{F}_q)| = g_n = q^{\frac{n(n-1)}{2}}(q-1)^n[n]_q!$*
2. *Groupe spécial linéaire : $|SL_n(\mathbb{F}_q)| = \frac{g_n}{q-1} = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$*
3. *Groupe projectif : $|PGL_n(\mathbb{F}_q)| = \frac{g_n}{q-1} = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$*
4. *Groupe spécial projectif : $|PSL_n(\mathbb{F}_q)| = \frac{g_n}{(q-1)d} = \frac{1}{d}q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$ avec $d = \gcd(q-1, n)$*
5. *Groupe orthogonal impair : si $ch \neq 2$, $|O_{2n+1}(\mathbb{F}_q)| = 2q^n\prod_{k=0}^{n-1}\left(q^{2n} - q^{2k}\right) = 2q^{n^2}(q^2-1)^n[n]_{q^2}!$*

6. *Groupe orthogonal pair :*
$$|O_{2n}(\mathbb{F}_q)| = 2\left(q^n - (-1)^{\frac{n(q-1)}{2}}\right)\prod_{k=0}^{n-1}\left(q^{2n} - q^{2k}\right) = 2q^{n(n-1)}\left(q^n - (-1)^{\frac{n(q-1)}{2}}\right)(q^2-1)^{n-1}[n]_{q^2}!$$
7. *Groupe symplectique :* $|Sp_{2n}(\mathbb{F}_q)| = q^{n^2}\prod_{k=1}^{n}(q^{2k}-1) = q^{n^2}(q^2-1)^n[n]_{q^2}!$

Démonstration. 1. Deux démonstrations.
   — On fait agir transitivement $GL_n(\mathbb{K})$ sur $\mathbb{K}^n \setminus \{0\}$. On a $Stab(e_1) \simeq GL_{n-1}(\mathbb{K}) \ltimes \mathbb{K}^{n-1}$. On en déduit que $|GL_n(\mathbb{F}_q)| = |GL_{n-1}(\mathbb{F}_q)|q^{n-1}(q^n-1)$. On conclut par récurrence.
   — On compte le nombre de bases de l'espace $\mathbb{F}_q^n$. Pour cela, on fait agir simplement transitivement $Gl_n(\mathbb{F}_q)$ sur l'ensemble des bases. On raisonne ensuite par récurrence.
2. $|SL_n(\mathbb{F}_q)| = |GL_n(\mathbb{F}_q)| \setminus |\mathbb{F}_q^*|$ par la suite exacte suivante : $1 \longrightarrow SL_n(\mathbb{K}) \longrightarrow GL_n(\mathbb{K}) \longrightarrow \mathbb{K}^* \longrightarrow 1$.
3. $PGL_n(\mathbb{K}) \simeq GL_n(\mathbb{K}) \setminus \mathbb{K}^*$ ou on compte le nombre de repère projectif (de la même manière que le précédent).
4. Le groupe spécial projectif est le quotient du groupe spécial par son sous groupe distingué des homothéties. On cherche donc à montrer que le nombre de racine $n^{\text{ième}}$ de l'unité dans $\mathbb{F}_q$ vaut $d = \gcd(n, q-1)$ (on applique Lagrange et Bézout). (Les autres voir le tome 1) □

Lemme (Famille). *Soient $q, n, m \in \mathbb{N}$.*
1. *Famille libre à m éléments ($m \leq n$) :* $q^{\frac{m(m-1)}{2}}(q-1)^m\frac{[n]_q!}{[n-m]_q!}$
2. *Famille génératrice à m éléments ($m \geq n$) :* $q^{\frac{n(n-1)}{2}}(q-1)^n\frac{[m]_q!}{[m-n]_q!}$
3. *Bases :* $q^{\frac{n(n-1)}{2}}(q-1)^n[n]_q! = g_n$

Démonstration. 1. On fait agir transitivement $GL_n(\mathbb{F}_q)$ sur l'ensemble des systèmes libres de cardinal m (théorème de la base incomplète). On trouve un premier cardinal que l'on simplifie avec les résultats précédents.
2. Dualité
3. Lorsqu'on compte le nombre de base de $\mathbb{F}_q^n$ pour trouver $|GL_n(\mathbb{F}_q)|$.
□

Lemme (Application linéaire). *Soient $q, n, m \in \mathbb{N}$.*
1. *Générale :* $\left|\mathcal{L}\left(\mathbb{F}_q^m, \mathbb{F}_q^n\right)\right| = q^{mn}$
2. *Injective de $\mathbb{F}_q^m$ vers $\mathbb{F}_q^n$ ($m \leq n$) :* $q^{\frac{m(m-1)}{2}}(q-1)^m\frac{[n]_q!}{[n-m]_q!}$
3. *Surjective de $\mathbb{F}_q^m$ vers $\mathbb{F}_q^n$ ($n \leq m$) :* $q^{\frac{n(n-1)}{2}}(q-1)^n\frac{[m]_q!}{[m-n]_q!}$
4. *De rang r de $\mathbb{F}_q^m$ vers $\mathbb{F}_q^n$ ($r \leq m$ et $r \leq n$) :* $g_r\begin{bmatrix} m \\ r \end{bmatrix}_q\begin{bmatrix} n \\ r \end{bmatrix}_q = q^{\frac{r(r-1)}{2}}(q-1)^r[r]_q!\begin{bmatrix} m \\ r \end{bmatrix}_q\begin{bmatrix} n \\ r \end{bmatrix}_q$

Démonstration. 1. Argument de dimension
2. Application linéaire entièrement caractérisé par l'image d'une base. Le nombre d'application injective est donc le nombre de système libre.
3. Dualité via la transposition
4. On fait agir par multiplication à droite $GL_n(\mathbb{F}_q)$ sur $\mathcal{M}_{m,n}(\mathbb{F}_q)$. L'ensemble des matrices dont l'image est F un sous-espace de dimension r est une orbite qui ne dépend ni de r ni de F. On conclut via le stabilisateur.
□

Lemme (Endomorphisme). *Soient $q, n, m \in \mathbb{N}$.*
1. *Généraux :* $|End(E)| = q^{n^2}$
2. *Diagonalisable :* $|\mathcal{D}_n| = \sum_{\substack{n_1+\cdots+n_q=n \\ n_i \geq 0}} \frac{g_n}{\prod_{i=1}^q g_{n_i}}$
3. *Niloptents :* $|\mathcal{N}_n| = q^{n(n-1)}$
4. *Trigonalisable :* $|\mathcal{T}_n| = \sum_{\substack{n_1+\cdots+n_q=n \\ n_i \geq 0}} \frac{g_n}{q^{-n}\prod_{i=1}^q g_{n_i}}$

Démonstration. 1. Par dimension
2. On fait agir $GL_n(\mathbb{F}_q)$ sur l'ensemble des sous-espaces propres.
3.
4. Mêmes arguments que pour la diagonalisation mais le lemme des noyaux est différents donc on n'utilise pas les sous-espaces propres.
□

Somme directe

Nous allons maintenant présenter quelques résultats sur les sommes et les sommes directes de sous-espaces vectoriels [6, p.21].

Cas de deux sous-espaces vectoriel Nous nous intéressons à ces notions pour deux sous-espaces. Nous en profiterons pour définir les sous-espaces supplémentaires.

Définition. Soient E_1, E_2 deux sous-espaces vectoriels d'un espace vectoriel E. On appelle somme de E_1 et E_2, le sous-espace de E défini par :

$$E_1 + E_2 = \{x \in E \mid \exists x_1 \in E_1, x_2 \in E_2 : x = x_1 + x_2\}$$

Remarque : Cette décomposition n'est à priori pas unique. Elle ne peut être unique que si $E_1 \cap E_2 = \{0\}$.

Définition. Soient E_1, E_2 deux sous-espaces vectoriels d'un espace vectoriel E et soit $\mathcal{E} = E_1 + E_2$. La décomposition de tout élément de $\mathcal{E}$ en somme d'un élément de E_1 et d'un élément de E_2 est unique, si et seulement si $E_1 \cap E_2 = \{0\}$. On écrit alors $\mathcal{E} = E_1 \oplus E_2 : \mathcal{E}$ est somme directe de E_1 et de E_2.

Remarque :

$$\mathcal{E} = E_1 \oplus E_2 \Leftrightarrow \begin{cases} \mathcal{E} = E_1 + E_2 \\ E_1 \cap E_2 = \{0\} \end{cases} \Leftrightarrow \begin{cases} \mathcal{E} = E_1 + E_2 \\ \text{décomposition unique des éléments de } \mathcal{E} \end{cases}$$

Proposition. *Soit E un espace vectoriel et E_1, E_2 deux sous-espaces vectoriels de E. Alors $E = E_1 \oplus E_2$ si et seulement si pour tout base $\mathcal{B}_1$ de E_1 et $\mathcal{B}_2$ de E_2, $\{\mathcal{B}_1, \mathcal{B}_2\}$ est une base de E.*

Démonstration. $\Leftarrow$ Décomposition unique d'un vecteur dans une base : $x = x_1 + x_2$, $x_1 \in E_1$ et $x_2 \in E_2$.

$\Rightarrow$ Décomposition unique d'un vecteur dans une somme directe et décomposition unique dans leur base respective donne une décomposition unique dans la base recherchée.

□

Définition. Soient E_1, E_2 deux sous-espaces vectoriels d'un espace vectoriel E et soit $\mathcal{E} = E_1 + E_2$. On dit que E_1 et E_2 sont supplémentaires si $E = E_1 \oplus E_2$.

Corollaire. *Soit E un espace vectoriel. Pour tout sous-espace vectoriel E_1, il existe toujours un supplémentaire. Ce supplémentaire n'est pas unique, mais si E est de dimension finie, tous les supplémentaires de E_1 ont même dimension.*

Démonstration. On raisonne en dimension finie : on applique le théorème de la base incomplète et la proposition précédente nous permet d'obtenir le dit supplémentaire. Comme le choix des vecteurs n'est pas unique, l'unicité n'est pas garantie. Cependant le nombre de vecteur choisi est toujours le même (base incomplète). □

Théorème. *Soit E un espace vectoriel de dimension finie. Alors*

$$E = E_1 \oplus E_2 \Leftrightarrow \begin{cases} E_1 \cup E_2 = \{0\} \\ \dim E = \dim E_1 + \dim E_2 \end{cases}$$

Démonstration. $\Rightarrow$ Propositions précédentes

$\Leftarrow$ On prend deux bases de E_1 et E_2 et on montre que la concaténation de ces deux bases forme une base pour E.

□

Proposition. *Soit E un espace vectoriel de dimension finie et E_1, E_2 deux sous-espaces vectoriels de E. On a*

$$\dim(E_1 + E_2) = \dim E_1 + \dim E_2 - \dim(E_1 \cap E_2) \quad \textit{(Formule de Grassmann)}$$
$$\dim(E_1 \oplus E_2) = \dim E_1 + \dim E_2$$

Démonstration. On prend une base de $E_1 \cap E_2$ que l'on complète dans E_1 puis dans E_2. On prend un vecteur de $E_1 + E_2$ et on montre qu'on l'écrit avec ces deux bases : on prouve ainsi que c'est une base de E.

Pour la somme directe, on applique la formule précédente avec $E_1 \cap E_2 = \{0\}$. □

Cas de plusieurs sous-espaces On généralise maintenant les concepts suivants dans le cas où on a plus de deux sous-espaces vectoriels.

Définition. Soient $E_1, \ldots, E_p$ des sous-espaces vectoriels d'un espace vectoriel E. On appelle somme de $E_1, \ldots, E_p$, le sous-espace de E défini par :

$$E_1 + \cdots + E_p = \{x \in E \mid \exists x_1 \in E_1, \ldots, x_p \in E_p : x = x_1 + \cdots + x_p\}$$

Proposition. *Si $\mathcal{G}_1, \ldots, \mathcal{G}_p$ sont des familles génératrices respectivement de $E_1, \ldots, E_p$, alors $\{\mathcal{G}_1, \ldots, \mathcal{G}_p\}$ est une famille génératrice de $E_1 + \cdots + E_p$.*

Démonstration. Décomposition de l'élément par la somme puis par la combinaison linéaire des familles génératrices : combinaison linéaire pour l'élément. □

Définition. Soient $E_1, \dots, E_p$ dessous-espaces vectoriels d'un espace vectoriel E. On dit qu'ils sont en somme directe si tout vecteur $\mathcal{E} = E_1 + \cdots + E_p$ se décompose d'une manière unique en somme d'un vecteur de $E_1, \dots,$ d'un vecteur de E_p. On écrit alors $\mathcal{E} = E_1 \oplus \cdots \oplus E_p$.

Proposition. *Soit E un espace vectoriel et $E_1, \dots, E_p$ des sous-espaces vectoriels de E. Alors $E = E_1 \oplus \cdots \oplus E_p$ si et seulement si pour tout base $\mathcal{B}_1, \dots, \mathcal{B}_p$ de $E_1, \dots, E_p$, $\{\mathcal{B}_1, \dots, \mathcal{B}_p\}$ est une libre.*

Démonstration. $\Leftarrow$ Généralisation du cas de deux sous-espaces vectoriels.

$\Rightarrow$ Par unicité de la décomposition des éléments d'une somme directe et par le fait qu'une base est une famille libre.

□

Remarque : Bien distinguer : les E_i sont en sommes directes et E est somme directe des E_i (dans ce cas, la somme directe des E_i "remplie" E tout entier).

Corollaire. *Si E est de dimension finie :* $\dim(E_1 \oplus \cdots \oplus E_p) = \dim E_1 + \cdots + \dim E_p$

Corollaire. *Soit E un espace vectoriel de dimension finie. Alors*

$$E = E_1 \oplus \cdots \oplus E_p \Leftrightarrow \begin{cases} E_1 + \cdots + E_p = E \\ \dim E = \dim E_1 + \cdots + \dim E_p \end{cases}$$

Théorème. *Les sous-espaces $E_1, \dots, E_p$ sont en somme directe, si et seulement si $E_1 \cap E_2 = \{0\}$, $(E_1 + E_2) \cap E_3 = \{0\}, \dots, (E_1 + \cdots + E_{p-1}) \cap E_p = \{0\}$.*

Démonstration. On utilise la décomposition unique des éléments. □

Remarque : Cette condition est minimale : des conditions plus faibles ne suffisent pas à montrer la somme directe.

Valeurs propres, espaces propres

Les valeurs et les vecteurs propres apparaissent dès que nous cherchons à donner à un endomorphisme des représentations agréable [1, p.958]. Nous cherchons à les définir et à en donner quelques propriétés.

Définition. Soit $u \in \mathcal{L}(E)$. On dit que $\lambda \in K$ est valeur propre de u s'il existe $x \in E \setminus \{0\}$ tel que $u(x) = \lambda x$. Un tel vecteur x est alors appelé un vecteur propre associé à la valeur propre λ.

Remarque : Dans ce cas, nous somme entrain de dire que Kx est une droite stable par u.

Définition. Soit $u \in \mathcal{L}(E)$. Si $\lambda \in K$ est une valeur propre de u, le sous-espace propre E_λ associé est le sous-espace vectoriel $E_\lambda = \ker(u - \lambda Id_E)$.

Remarque : Un sous-espace propre est l'ensemble des vecteurs propres auquel on ajoute le vecteur nul.

Définition. Soit $u \in \mathcal{L}(E)$. L'ensemble des valeurs propres de u est appelé le spectre de u, et est noté $Sp_K(u)$. Il est éventuellement vide.

Remarque : Si $M \in \mathcal{M}_n(K)$, on définit les valeurs propres et les vecteurs propres de la matrice comme étant ceux de l'endomorphisme de $K^n \to K^n$ et qui $X \mapsto MX$.

Lemme. *Soit $u \in \mathcal{L}(E)$. Alors, $\lambda \in K$ est une valeurs propre de u, si et seulement si, $\chi_u(\lambda) = 0$. En particulier, $Sp_K(u)$ est un ensemble fini.*

Démonstration. λ est une valeur propre si et seulement si $\ker(\lambda Id_E - u) \neq \{0\}$ (définition) soit $(\lambda Id_E - u)$ est non inversible d'où $\det(\lambda Id_E - u) = 0$. $Sp_K(u)$ est un ensemble fini car un polynôme non nul possède un ensemble fini de racine. □

Définition. Soient $u \in \mathcal{L}(E)$ et $\lambda \in Sp_K(u)$. La multiplicité de λ est sa multiplicité en tant que racine de χ_u.

Remarque : Autrement dit, c'est la plus grand entier $m \geq 1$ tel que $(X - \lambda)^m$ divise χ_u.

Proposition. *Soit $u \in \mathcal{L}(E)$. Pour tout $\lambda \in Sp_K(u)$, on a $1 \leq \dim_K(E_\lambda) \leq m_\lambda$ où m_λ est la multiplicité de λ.*

Démonstration. Provient des définitions de vecteur propre et de leurs multiplicité. □

Lemme. *Soit $u \in \mathcal{L}(E)$. Alors, les sous-espace propres de u sont en somme directe.*

Lemme. *Soient $u \in \mathcal{L}(E)$, x un vecteur propre de u associé à la valeur propre λ. Alors, pour tout $P \in K[X]$, on a $P(u)(x) = P(\lambda)(x)$. En particulier, si P annule u alors λ est racine de P.*

Démonstration. On montre par récurrence que $u^m(x) = \lambda^m x$. On évalue alors P en u. □

Diagonalisation

On cherche à écrire une matrice sous une forme plus agréable afin de facilité sa manipulation (comme lorsque nous voulons la mettre à la puissance, lors d'un calcul d'exponentielle) [1, p.956]. Cette opération revient à diagonaliser la matrice, c'est-à-dire trouver une base dans laquelle la matrice est diagonale.

Critères de diagonalisation Commençons par définir les matrices diagonalisables puis donnons les différentes caractérisations à la diagonalisation.

Lemme. *Soient E un K-espace vectoriel de dimension finie non nulle n, $u \in \mathcal{L}(E)$ et e une base de E. Les propriétés suivantes sont équivalentes :*

1. *la matrice $Mat(u; e)$ est diagonale.*
2. *il existe $\lambda_1, \dots, \lambda_n \in K$ tels que $\forall i \in [\![1; n]\!], u(e_i) = \lambda_i$ si $u_i \in e$*

Démonstration. Définition d'une matrice représentative. On remarque de plus que les e_i sont non nuls car ils proviennent d'une base. □

Définition. Soit $u \in \mathcal{L}(E)$. On dit que u est diagonalisable s'il existe une base de E dans laquelle la matrice représentative de u soit diagonale.

Remarque : Cela revient à dire qu'il existe une base de E formée de vecteur propre de u, ou encore de que E se décompose en somme directe de droites stables par u.

Théorème. *Soit $u \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes :*

1. *l'endomorphisme u est diagonalisable*
2. *on a $E = \bigoplus_{\lambda \in Sp_K(u)} E_\lambda$*
3. *le polynôme χ_u est scindé, et pour tout $\lambda \in Sp_K(u)$, on a $\dim_K(E_\lambda) = m_\lambda$, où m_λ est la multiplicité de λ.*

Démonstration. **Montrons** $3 \Rightarrow 2$ χ_u est scindé et les valeurs propres de u sont exactement ses racines : $\chi_u = \prod_{\lambda \in Sp_K(u)} (X - \lambda)^m_\lambda$. En comparant les degré, $\sum_{\lambda \in Sp_K(u)} m_\lambda = n$, on en déduit que $\dim_K(\bigoplus_{\lambda \in Sp_K(u)} E_\lambda) = \dim_K(E)$.

Montrons $2 \Rightarrow 1$ Clair en recollant les bases des sous-espaces propres.

Montrons $1 \Rightarrow 3$ On calcul le polynôme caractéristique sur le représentation diagonale de l'endomorphisme.

□

Corollaire. *Soit $u \in \mathcal{L}(E)$. Si u possède $n = \dim_K(E)$ valeurs propres distinctes, alors u est diagonalisable.*

Démonstration. Application des propositions et théorèmes précédents. □

Théorème. *Soit $u \in \mathcal{L}(E)$. Les propriétés suivantes sont équivalentes :*

1. *l'endomorphisme u est diagonalisable*
2. *le polynôme $\prod_{\lambda \in Sp_K(u)} (X - \lambda)$ annule u*
3. *il existe un polynôme P annulant u scindé sans racines multiples. Dans ce cas $Sp_K(u)$ est contenu dans ces racines*
4. *le polynôme minimal μ_u est scindé sans racines multiples*
5. *$\mu_u = \prod_{\lambda \in Sp_K(u)} (X - \lambda)$*

Démonstration. **Montrons** $1 \Rightarrow 2$ Le théorème précédent et le lemme des noyaux nous donne l'existence de $P = \prod_{\lambda \in Sp_K(u)} (X - \lambda)$ tel que $e = \ker(P(u))$. Dans ce cas $P(u) = 0$.

Montrons $2 \Rightarrow 3$ Clair par propriétés des valeurs propres et des polynômes.

Montrons $3 \Rightarrow 4$ Le polynôme minimal μ_u divise P.

Montrons $4 \Rightarrow 5$ Les polynômes μ_u et χ_u ont exactement les même racines qui sont les valeurs propres de u.

Montrons $5 \Rightarrow 1$ On applique le lemme de décomposition des noyaux.

□

Lemme. *Soient $u \in \mathcal{L}(E)$ et F un sous-espace stable par u. Si u est diagonalisable, alors $u_F \in \mathcal{L}(F)$ est diagonalisable.*

Démonstration. On applique le théorème précédent à la restriction du polynôme minimal de u_F qui est un restriction de celui de u. □

Théorème. *Soient $u, u' \in \mathcal{L}(E)$ tels que u et u' commutent. S'ils sont diagonalisables, alors ils le sont dans la même base.*

Démonstration. Si λ est une valeur propre de u alors E_λ est stable par u'. Par ce qui précède, u'_{E_λ} est diagonalisable : il existe donc une base qui diagonalise u'_{E_λ}. En recollant les différentes base, comme u et u' sont diagonalisables, on obtient cette base. □

Applications de la diagonalisation Il y a trois grandes applications à la diagonalisation [6, p.170].

Calcul d'une puissance Le calcul de A^m où A est une matrice diagonalisable s'effectue en diagonalisant A puis $A^m = P^{-1}D^mP$ où D^m consiste à mettre ses coefficients à la puissance (ce qui est facile).

Résolution d'un système de suites récurrentes On se ramène au calcul d'une puissance de la matrice sous-jacente au système.

Système différentiel linéaire à coefficients constants Si on met le système sous la forme d'une matrice A, on souhaite résoudre $\frac{dX}{dt} = AX$. On raisonne comme suit

1. on diagonalise A et on trouve D comme matrice diagonale et P comme matrice de passage : $D = P^{-1}DP$
2. on intègre le système $\frac{dX'}{dt} = DX'$ (plus facile car D est diagonale)
3. on revient à X par $X = PX'$.

Références

[1] G. Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018.

[2] J. Calais. *Éléments de la théorie des groupes*. puf, 1984.

[3] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries, tome 1*. Calvage et Mounet, 2013.

[4] P. Caldero and J. Germoni. *Nouvelles histoires hédonistes de groupes et de géométries, tome 2*. Calvage et Mounet, 2018.

[5] X. Gourdon. *Algèbre*. Les maths en tête. Ellipses, 2009.

[6] J. Grifone. *Algèbre linéaire*. Cépaduès édition, 2015.

[7] G. Laville. *Géométrie pour le capes et l'agrégation*. ellipse, 1998.

[8] S.Nicolas S. Francinou, H. Gianella. *Oraux X-ENS, Algèbre 1*. Cassini.

[9] F. Ulmer. *Théorie des groupes*. ellipses, 2012.