

COMBINATOIRE ALGÈBRIQUE

Compilation de cardinaux en algèbre linéaire sur $\mathbb{F}_q$

On se donne $p \in \mathcal{P}$ et $s \in \mathbb{N}^*$. On pose dans toute la suite $q := p^s$ et on considère le corps à q élément $\mathbb{F}_q$.

On note dans la suite E_n (ou E quand n est clair) le $\mathbb{F}_q$ -espace vectorielle $\mathbb{F}_q^n$ et

$$g_n := |\mathrm{GL}_n(\mathbb{F}_q)|$$

DÉFINITION (q - Analogue / Nombre quantique) :

Pour deux entiers $q \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$ on définit le q -analogue de n ou *entier n quantique* (si q est clair) noté $[n]_q$ par:

$$[n]_q := \sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q - 1}$$

On définit de même le *factoriel quantique* et les *nombre binomiaux quantiques* par:

$$[n]_q! := [n]_q \times [n-1]_q \times \dots \times [1]_q$$

$$\begin{bmatrix} n \\ m \end{bmatrix}_q := \frac{[n]_q!}{[m]_q! [n-m]_q!}$$

Et pour $m_1 + \dots + m_k = n$, les *nombre multinomiaux quantiques* :

$$\begin{bmatrix} n \\ m_1 \dots m_k \end{bmatrix}_q := \frac{[n]_q!}{\prod_{i=1}^k [m_i]_q!}$$

On remarque que si l'on prenait $q = 1$ on retombe sur les définitions classiques de factoriel et de coefficient binomiaux.

LEMME 1: (Orbite-Stabilisateur)

Soit G un groupe agissant sur un ensemble X par $\cdot$. Pour $x \in X$ on note G_x le stabilisateur de x sous l'action de G et O_x son orbite.

Fixons $x \in X$, si pour $g \in G$ on note $\bar{g}$ sa classe dans G/G_x alors:

$$\begin{array}{ccc} \phi : G/G_x & \longrightarrow & O_x \\ \bar{g} & \longmapsto & g \cdot x \end{array}$$

est bien défini et bijective.

Si de plus G est fini, pour tout $x \in X$,

$$|G| = |G_x| |O_x|$$

THÉORÈME 1: (Cardinal de $\text{GL}_n(\mathbb{F}_q)$)

Pour $n \in \mathbb{N}^*$ on a:

$$|\text{GL}_n(\mathbb{F}_q)| = g_n = \prod_{k=0}^{n-1} (q^n - q^k)$$

PREUVE :

On le montre par récurrence sur $n \in \mathbb{N}^*$.

Initialisation : Pour $n = 1$ le résultat est clair.

Hérédité : Supposons $n \geq 2$ tel que le résultat est vérifié au rang $n - 1$.

$\text{GL}_n(\mathbb{F}_q)$ agit transitivement sur $\mathbb{F}_q^n \setminus \{0\}$ par multiplication à gauche. On note

$$e := {}^t(1, 0, \dots, 0) \in \mathbb{F}_q^n \setminus \{0\}$$

Par suite, $O_e = \mathbb{F}_q^n$ et si l'on note S le stabilisateur de e sous l'action de $\text{GL}_n(\mathbb{F}_q)$,

$$S = \begin{pmatrix} 1 & * & \dots & * \\ 0 & & & \\ \vdots & \text{GL}_{n-1}(\mathbb{F}_q) & & \\ 0 & & & \end{pmatrix}$$

Par le lemme 1 on a donc:

$$|\text{GL}_n(\mathbb{F}_q)| = q^{n-1} |\mathbb{F}_q^n \setminus \{0\}| |\text{GL}_{n-1}(\mathbb{F}_q)|$$

Soit, en appliquant l'hypothèse de récurrence:

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

□

On remarque alors que:

$$|\mathrm{GL}_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q-1)^n[n]_q!$$

THÉORÈME 2:(Cardinal de $\mathrm{SL}_n(\mathbb{F}_q)$)

Pour $n \in \mathbb{N}^*$ on a:

$$|\mathrm{SL}_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$$

PREUVE :

On a la suite exacte:

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{F}_q) \xrightarrow{i} \mathrm{GL}_n(\mathbb{F}_q) \xrightarrow{\det} \mathbb{F}_q^* \longrightarrow 1$$

Par suite:

$$|\mathrm{SL}_n(\mathbb{F}_q)| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathbb{F}_q^*|} = \frac{g_n}{q-1} = q^{\frac{n(n-1)}{2}}(q-1)^{n-1}[n]_q!$$

□

DÉFINITION (Grassmanienne) :

Pour $n \in \mathbb{N}^*$ et $m \in \llbracket 1, n \rrbracket$ on note:

$$\mathrm{Gr}_{m,n}(\mathbb{F}_q) := \{F \subseteq \mathbb{F}_q^n \mid \dim(F) = m\}$$

THÉORÈME 3:(Cardinal de $\mathrm{Gr}_{m,n}(\mathbb{F}_q)$)

Soit $n \in \mathbb{N}^*$ et $m \in \llbracket 1, n \rrbracket$, alors:

$$|\mathrm{Gr}_{m,n}(\mathbb{F}_q)| = \begin{bmatrix} n \\ m \end{bmatrix}_q$$

PREUVE :

Par le théorème de la base incomplète, $\mathrm{GL}_n(\mathbb{F}_q)$ agit transitivement sur $\mathrm{Gr}_{m,n}(\mathbb{F}_q)$, si l'on note $(e_1, \dots, e_n)$ la base canonique de E et $F := \langle e_1, \dots, e_m \rangle$ alors:

$$F \in \mathrm{Gr}_{m,n}(\mathbb{F}_q) \quad \text{soit} \quad O_F = \mathrm{Gr}_{m,n}(\mathbb{F}_q)$$

$$\mathrm{Stab}(F) = \begin{pmatrix} \mathrm{GL}_m(\mathbb{F}_q) & \mathcal{M}_{m,n-m}(\mathbb{F}_q) \\ 0 & \mathrm{GL}_{n-m}(\mathbb{F}_q) \end{pmatrix}$$

Par suite,

$$|\mathrm{Gr}_{m,n}(\mathbb{F}_q)| = \frac{g_n}{q^{m(n-m)} g_m g_{n-m}} = \begin{bmatrix} n \\ m \end{bmatrix}_q$$

□

THÉORÈME 4:(Cardinal de $\mathcal{L}_{m,n}(\mathbb{F}_q)$)

On note pour $m \leq n \in \mathbb{N}^*$,

$$\mathcal{L}_{m,n}(\mathbb{F}_q) := \{(x_1, \dots, x_m) \in (\mathbb{F}_q^n)^m \mid (x_1, \dots, x_m) \text{ est libre}\}$$

Alors:

$$|\mathcal{L}_{m,n}(\mathbb{F}_q)| = \frac{g_n}{q^{m(n-m)} g_{n-m}} = q^{\frac{m(m-1)}{2}} (q-1)^m \frac{[n]_q!}{[n-m]_q!}$$

PREUVE :

Soient $m \leq n \in \mathbb{N}^*$, alors $\mathrm{GL}_n(\mathbb{F}_q)$ agit transitivement par multiplication à gauche sur $\mathcal{L}_{m,n}(\mathbb{F}_q)$ (c'est encore la base incomplète).

On note $(e_1, \dots, e_n)$ la base canonique de E_n et $F := \langle e_1, \dots, e_m \rangle$. Alors:

$$\mathrm{Stab}(F) = \begin{pmatrix} I_m & \mathcal{M}_{m,n-m}(\mathbb{F}_q) \\ 0 & \mathrm{GL}_{n-m}(\mathbb{F}_q) \end{pmatrix}$$

Par suite,

$$\begin{aligned} |\mathcal{L}_{m,n}(\mathbb{F}_q)| &= \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathcal{M}_{m,n-m}(\mathbb{F}_q)| |\mathrm{GL}_{n-m}(\mathbb{F}_q)|} \\ &= \frac{g_n}{q^{m(n-m)} g_{n-m}} \\ &= q^{\frac{m(m-1)}{2}} (q-1)^m \frac{[n]_q!}{[n-m]_q!} \end{aligned}$$

□

DÉFINITION (Drapeaux) :

Pour $n \in \mathbb{N}^*$ on note:

$$\mathcal{F}_n(\mathbb{F}_q) := \{(F_0, \dots, F_n) \mid \forall i \in \llbracket 0, n \rrbracket, \dim(F_i) = i \text{ et } F_0 \subset F_1 \dots \subset F_n = \mathbb{F}_q^n\}$$

THÉORÈME 5:(Cardinal de $\mathcal{F}_n(\mathbb{F}_q)$)

Pour $n \in \mathbb{N}^*$,

$$|\mathcal{F}_n(\mathbb{F}_q)| = [n]_q!$$

PREUVE :

$\mathrm{GL}_n(\mathbb{F}_q)$ agit par $\cdot$ sur $\mathcal{F}_n(\mathbb{F}_q)$ définis comme:

$$\begin{aligned} \cdot : \mathrm{GL}_n(\mathbb{F}_q) \times \mathcal{F}_n(\mathbb{F}_q) &\longrightarrow \mathcal{F}_n(\mathbb{F}_q) \\ (M, (F_i)_i) &\longmapsto (GF_i)_i \end{aligned}$$

Montrons que l'action est transitive:

Si l'on note $\underline{e} = (e_1, \dots, e_n)$ la base canonique de E alors on définit le *drapeau standard* :

$$F_{\mathrm{std}} = (F_{\mathrm{std}}^0, \dots, F_{\mathrm{std}}^n) := (\langle e_1, \dots, e_k \rangle)_{k \in \llbracket 0, n \rrbracket}$$

Pour un drapeau $F := (F_0, \dots, F_n)$ on note pour $k \in \llbracket 1, n \rrbracket$ f_k un vecteur tel que:

$$\langle f_k \rangle \oplus F_{k-1} = F_k$$

Alors, $\underline{f} := (f_1, \dots, f_n)$ est une base de E et l'on dispose donc de $P \in \mathrm{GL}_n(\mathbb{F}_q)$ tel que:

$$M\underline{e} = \underline{f}$$

Par suite,

$$M \cdot F_{\mathrm{std}} = F$$

Puis:

$$O_{F_{\mathrm{std}}} = \mathcal{F}_n(\mathbb{F}_q)$$

Or le stabilisateur de F_{std} est le sous-groupe B de $\mathrm{GL}_n(\mathbb{F}_q)$ composé des matrices triangulaires supérieures inversibles: en effet on veut que pour $k \in \llbracket 1, n \rrbracket$ e_k soit envoyé sur une combinaison linéaire de e_l tel que $e_l \in F_{\mathrm{std}}^k$ soit $l \leq k$. Aussi:

$$|B| = (q-1)^n q^{\frac{n(n-1)}{2}}$$

En effet on choisit des éléments non nul sur la diagonal, ce que l'on veut au dessus et des 0 en dessous.

Finalement:

$$|\mathcal{F}_n(\mathbb{F}_q)| = \frac{g_n}{(q-1)^n q^{\frac{n(n-1)}{2}}} = [n]_q!$$

□

THÉORÈME 6:(Cardinal de $\mathcal{N}_n(\mathbb{F}_q)$)

On note $\mathcal{N}_n(\mathbb{F}_q) \subset \mathcal{M}_n(\mathbb{F}_q)$ l'ensembles des matrices nilpotentes. Alors:

$$|\mathcal{N}_n(\mathbb{F}_q)| = q^{n(n-1)}$$

LEMME 2:

Soient $n \in \mathbb{N}^*$ et $N \in \mathcal{N}_n(\mathbb{F}_q)$. Pour $x \in E_n \setminus \{0\}$ on note:

$$r_x := \max(\{k \in \mathbb{N}^* \mid (x, Nx, \dots, N^{k-1}x) \text{ est libre}\})$$

Alors, pour tout $x \in E_n \setminus \{0\}$,

$$N^{r_x}x = 0$$

PREUVE :(Du lemme 2)

Soit $x \in E_n \setminus \{0\}$, notons $r := r_x$ et $a_0, \dots, a_{r-1} \in \mathbb{F}_q$ tel que:

$$N^r x = \sum_{i=0}^{r-1} a_i N^i x$$

Notons, $F := \langle x, \dots, N^{r-1}x \rangle$. F stable par l'endomorphisme associé à N et l'on peut donc considérer $\tilde{N} \in \mathcal{M}_r(\mathbb{F}_q)$ la matrice de l'endomorphisme induit sur F dans la base $(x, \dots, N^{r-1}x)$ de F . Par ce qui précède,

$$\tilde{N} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & 0 & \dots & 0 & a_1 \\ 0 & 1 & 0 & \dots & 0 & a_2 \\ 0 & 0 & 1 & \dots & 0 & a_3 \\ 0 & 0 & 0 & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_{r-1} \end{pmatrix}$$

On reconait une matrice compagnon et ainsi,

$$\chi_{\tilde{N}} = X^r - \sum_{i=0}^{r-1} a_i X^i$$

Mais comme $\tilde{N} \in \mathcal{N}_r(\mathbb{F}_q)$, $\chi_{\tilde{N}} = X^r$ ainsi $a_0 = \dots = a_{r-1} = 0$ puis:

$$N^r x = 0$$

□

PREUVE : (Du théorème 6)

Pour $n \in \mathbb{N}^*$ on note $\mathcal{N}_n := \mathcal{N}_n(\mathbb{F}_q)$, $\nu_n := |\mathcal{N}_n|$ et pour $m \in \llbracket 1, n \rrbracket$, $\mathcal{L}_{m,n} := \mathcal{L}_{m,n}(\mathbb{F}_q)$. On note enfin:

$$\widetilde{\mathcal{N}}_n := \{(N, (x_0, \dots, x_{m-1})) \mid Nx_i = x_{i+1} \text{ et } Nx_{m-1} = 0\} \subseteq \mathcal{N}_n \times \bigsqcup_{m \in \llbracket 1, n \rrbracket} \mathcal{L}_{m,n}$$

Si $(N, \underline{x}) \in \widetilde{\mathcal{N}}_n$ on dit que N respecte $\underline{x}$.

On dénombre $\widetilde{\mathcal{N}}_n$ de deux manières différentes:

Fixons $N \in \mathcal{N}_n$, et pour $x \in E_n \setminus \{0\}$ notons $r_x \in \mathbb{N}^*$ comme dans le lemme. Le lemme assure donc que, pour tout $x \in E_n \setminus \{0\}$,

$$(N, (x, Nx, \dots, N^{r_x-1}x)) \in \widetilde{\mathcal{N}}_n$$

et on se convainc facilement que si

$$(N, (x_0, \dots, x_{m-1})) \in \widetilde{\mathcal{N}}_n$$

alors $(x_0, \dots, x_{m-1})$ est de la forme $(x, Nx, \dots, N^{r_x-1}x)$.

Finalement pour tout $N \in \mathcal{N}_n$ chaque $x \in E_n \setminus \{0\}$ nous fournit un élément de $\widetilde{\mathcal{N}}_n$ soit:

$$|\widetilde{\mathcal{N}}_n| = \nu_n(q^n - 1)$$

Fixons maintenant $m \in \llbracket 1, n \rrbracket$ et $\underline{x} = (x_0, \dots, x_{m-1}) \in \mathcal{L}_{m,n}$. On complète la famille $\underline{x}$ en une base $\underline{b}$ de E_n , par suite, si l'on note $u \in \mathcal{L}(E_n)$ nilpotent tel que u respecte $\underline{x}$, alors:

$$\text{mat}_{\underline{b}}(u) = \begin{pmatrix} J_m & B \\ 0 & A \end{pmatrix}$$

Où J_m est le bloc de Jordan de taille m , $B \in \mathcal{M}_{m,n-m}(\mathbb{F}_q)$ et $A \in \mathcal{N}_{n-m}$. Par suite, chaque élément de $\mathcal{L}_{m,n}$ fournit $|\mathcal{M}_{m,n-m}(\mathbb{F}_q)| |\mathcal{N}_{n-m}|$ éléments de $\widetilde{\mathcal{N}}_n$, soit:

$$\begin{aligned} |\widetilde{\mathcal{N}}_n| &= \sum_{m=1}^n |\mathcal{L}_{m,n}| |\mathcal{M}_{m,n-m}(\mathbb{F}_q)| |\mathcal{N}_{n-m}| \\ &= \sum_{m=1}^n \frac{g_n}{q^{m(n-m)} g_{n-m}} q^{m(n-m)} \nu_{n-m} \end{aligned}$$

En combinant les expressions trouvées:

$$\nu_n(q^n - 1) = \sum_{m=0}^{n-1} \frac{g_n}{g_m} \nu_m$$

Si l'on note $(\gamma_n)_n := \left(\frac{\nu_n}{g_n} \right)_n$, on trouve, pour $n \geq 2$,

$$\begin{aligned} \gamma_n(q^n - 1) &= \sum_{m=0}^{n-1} \gamma_m \\ &= \gamma_{n-1} + \sum_{m=0}^{n-2} \gamma_m \\ &= \gamma_{n-1} + (q^{n-1} - 1)\gamma_{n-1} \\ &= q^{n-1}\gamma_{n-1} \end{aligned}$$

Or comme $\gamma_1 = \frac{1}{q-1}$, par récurrence immédiate sur n :

$$\gamma_n = \frac{q^{\frac{n(n-1)}{2}}}{\prod_{m=1}^n (q^m - 1)} = \frac{q^{n(n-1)}}{g_n}$$

Finalement:

$$|\mathcal{N}_n(\mathbb{F}_q)| = q^{n(n-1)}$$

□