Cône nilpotent sur un corps fini et q-séries hypergéométriques

Philippe Caldero

version du 23 décembre 2014

Résumé

On expose différentes méthodes pour le calcul du cardinal de divers cônes nilpotents sur un corps fini. On insiste particulièrement sur le rôle des fonctions hypergéométriques pour mener à bien ces calculs.

1 Fonctions hypergéométriques et leurs analogues quantiques

1.1 Fonctions hypergéométriques et identité de Chu-Vandermonde

Comme le chantait Barbara, "il était une fois" commence à Göttingen. Tout commence donc quand Gauss, [Gau13], présente à la Société Royale des Sciences la série infinie

$$F(a,b;c;z) = 1 + \frac{ab}{1.c}z + \frac{a(a+1)b(b+1)}{1\cdot 2\cdot c(c+1)}z^2 + \cdots + \frac{\prod_{i=0}^{k-1}(a+i)(b+i)}{k!\cdot\prod_{i=0}^{k-1}(c+i)}z^k + \cdots \quad (1)$$

où a, b, c, z sont des complexes, $c \notin \mathbb{Z}^-$. Cette série converge absolument lorsque $|z| < 1$ et pour $|z| = 1$ lorsque la partie réelle de $c - a - b$ est strictement positive. La virgule signifie que les variables a et b jouent des rôles symétriques.

Cette fonction, nommée plus tard *fonction hypergéométrique de Gauss*, possède des vertus unificatrices, puisque l'on a, entre autres

$$(1-z)^a = F(-a,b;b;z), \quad (2)$$

$$\ln(1+z) = zF(1,1;2;-z), \quad (3)$$

$$\arcsin(z) = zF(\frac{1}{2},\frac{1}{2};\frac{3}{2};z^2), \quad (4)$$

$$\arctan(z) = zF(\frac{1}{2},1;\frac{3}{2};-z^2), \quad (5)$$

$$e^z = \lim_{a\to\infty} F(a,b;b;\frac{z}{a}), \quad (6)$$

On retrouve également les polynômes de Tchebychev de premier ordre, de second ordre, ainsi que les polynômes de Legendre, respectivement

$$T_n(x) = F(-n,n;\frac{1}{2};\frac{1-x}{2}),\ U_n = (n+1)F(-n,n+2;\frac{3}{2};\frac{1-x}{2}),\ P_n = F(-n,n+1;1;\frac{1-x}{2}) \quad (7)$$

Gauss montre dans son article que

$$F(a,b;c;1) = \frac{\Gamma(c)\Gamma(c-a-b)}{\Gamma(c-a)\Gamma(c-b)} \quad (8)$$

Du lourd. Toutefois, un cas particulier de cette formule est assez naturel et remonte même à la Chine ancienne du XIV^{e} siècle. Il s'agit du cas particulier où $a = -n$ est un entier négatif. On attribue cette identité à Chu (1303) et Vandermonde (1772). On définit les factoriels montants

$$(a)_0 = 1,\ (a)_n = a(a+1)\cdots(a+n-1) = \frac{\Gamma(a+n)}{\Gamma(a)},\ a \in \mathbb{C}, n \in \mathbb{N}^*, \tag{9}$$

Proposition 1.1 (Identité de Chu-Vandermonde)**.**

$$F(-n, b; c; 1) = \frac{\Gamma(c)\Gamma(c+n-b)}{\Gamma(c+n)\Gamma(c-b)} = \frac{(c-b)_n}{(c)_n}$$

pour tout $n \in \mathbb{N}$, $b \in \mathbb{C}$, $c \in \mathbb{C}\backslash\{0, \cdots, -n+1\}$.

Démonstration. La seconde égalité est claire par construction de la fonction Γ. Quitte à changer b en $-b$, on voit facilement que cela revient à montrer l'égalité pour tous b, c complexes :

$$\sum_{k=0}^{n} \binom{n}{k} (b)_k (c)_{n-k} = (b+c)_n \tag{10}$$

qui ressemble étrangement à la formule du binôme. Remarquons par ailleurs que pour tout a dans $\mathbb{N}$, on a

$$\frac{(-a)_k}{k!} = (-1)^k \binom{a}{k}$$

Supposons maintenant que $b' := -b$ et $c' := -c$ sont des entiers plus grands que n. Alors, dans ce cas, on sait montrer :

$$\binom{b'+c'}{n} = \sum_{k=0}^{n} \binom{b'}{k}\binom{c'}{n-k}.$$

La preuve, classique, consiste à fixer, dans un ensemble E à $b'+c'$ éléments, une partition en deux sous-ensembles B' et C' de cardinaux respectifs b' et c', puis, de compter les parties P à n éléments de E selon le cardinal $k := |P \cap B'|$. Ce qui est alors équivalent à

$$\sum_{k=0}^{n} \frac{(b)_k}{k!}\frac{(c)_{n-k}}{(n-k)!} = \frac{(b+c)_n}{n!},$$

et donc à la formule désirée dans ce cas.

Maintenant, comme l'égalité voulue est polynomiale et valable sur une infinité de valeurs pour b et pour c, on a l'égalité pour tous b et c complexes, d'après le lemme

Lemme 1.2. *Soit* $\mathbb{K}$ *un corps et* P *un polynôme de* $\mathbb{K}[X, Y]$*. On suppose que* A *et* B *sont deux parties infinies de* $\mathbb{K}$ *telles que l'évaluation* $P(x, y) = 0$ *pour tout* (x, y) *dans* $A \times B$*. Alors* P *est le polynôme nul.*

Prouvons le lemme, ce qui achèvera la preuve de la proposition. On écrit $P = \sum_{i,j}(a_{ij}X^i)Y^j$. On fixe y dans B. Alors, $P(?, y) := \sum_i \sum_j (a_{ij}y^j)X^i$ est un polynôme de $\mathbb{K}[X]$ qui s'annule sur A, qui est infini. Ce polynôme est donc nul. On a donc pour tout i que le polynôme $\sum_j a_{ij}Y^j$ s'annule en y, et ce, pour tout y de B, qui est infini. Donc, tous les coefficients a_{ij} sont nuls et P est nul.

□

1.2 q-analogues des fonctions hypergéométriques

Une trentaine d'années après Gauss, Heine introduit les q-analogues des séries de Gauss (sous une forme légèrement différente que celle-ci). On note a, b, c, z, et q des nombres complexes et :

$$\phi(a, b; c; q; z) = \sum_{n=0}^{+\infty} \frac{(a;q)_n (b;q)_n}{(q;q)_n (c;q)_n} z^n, \tag{11}$$

où $(a;q)_n$ désigne le q-factoriel montant :

$$(a;q)_0 = 1,\ (a;q)_n = (1-a)(1-qa)\cdots(1-q^{n-1}a) \tag{12}$$

Pour que la série ϕ ait un sens, on supposera $q^k \neq 1$ et $q^{c+k} \neq 1$ pour tout entier naturel k. La série converge absolument pour $|q| < 1$ et $|z| < 1$.

Remarque 1.3. Si a, ou b sont de la forme q^{-m}, avec $m \in \mathbb{N}$, alors la série ne possède qu'un nombre fini de termes non nuls. Ainsi, elle sera valable pour tout q et tout z.

On ne manquera pas de remarquer que ces q-fonctions hypergéométriques se généralisent sans peine en des fonctions ${}_r\phi_s$ comportant r variables au numérateur et s variables au dénominateur, de sorte que notre fonction ϕ, avec ses variables a, b au numérateur et c au dénominateur, se note ${}_2\phi_1$ dans la littérature.

On pourra trouver amusant de montrer les formules suivantes, utiles par la suite :

$$(a;q)_n = (\frac{q^{1-n}}{a};q)_n(-a)^n q^{\binom{n}{2}} \tag{13}$$

$$(a;q)_{n-k} = \frac{(a;q)_n}{(q^{1-n}a^{-1};q)_k}\big(-qa^{-1}\big)^k q^{\binom{k}{2}-nk} \tag{14}$$

$$(q^{-n};q)_k = \frac{(q;q)_n}{(q;q)_{n-k}}(-1)^k q^{\binom{k}{2}-nk} \tag{15}$$

2 Dénombrement dans l'espace $\mathbb{F}_q^n$

2.1 Nombres q-binomiaux

Ici, q désigne la puissance d'un nombre premier et $\mathbb{K} = \mathbb{F}_q$ est un corps de cardinal q. Nous allons commencer par dénombrer quelques objets bien connus liés à l'espace vectoriel $\mathbb{K}^n$, nommément le groupe $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles de taille n et la grassmannienne $\mathrm{Gr}_{m,n}(\mathbb{K})$ des sous-espaces de dimension m dans l'espace $\mathbb{K}^n$.

Proposition 2.1. *On a les égalités suivantes :*

i $\left|\mathbb{F}_q^n\right| = q^n$,

ii $|\mathrm{GL}_n(\mathbb{F}_q)| = (-1)^n(q;q)_n q^{\binom{n}{2}}$,

iii $|\mathrm{Gr}_{m,n}(\mathbb{K})| = \frac{(q;q)_n}{(q;q)_k(q;q)_{n-k}}$.

Démonstration. La première égalité est claire. Pour la seconde, on part de la base canonique $\mathcal{B}$ de l'espace $\mathbb{F}_q^n$ et on note qu'un automorphisme γ de $\mathbb{F}_q^n$ détermine une base $\gamma(\mathcal{B})$ et inversement, il est entièrement déterminé par l'image de $\mathcal{B}$. Ainsi, l'ensemble des matrices inversibles est en bijection avec l'ensemble des bases.

Compter les bases n'est pas difficile. Le premier vecteur doit être non nul, et par récurrence sur k de 1 à n, le k-ième vecteur doit être choisi à l'extérieur du sous-espace engendré par la famille constituée des $(k-1)$ précédents, ce sous-espace étant donc de dimension $k-1$ puisque la famille qui l'engendre est libre, par construction. On a donc, par la première formule :

$$|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^k)\cdots(q^n-q^{n-1}) = (-1)^n q^{1+2+\cdots+(n-1)}(1-q^n)\cdots(1-q).$$

Ce qui donne la formule voulue.

Pour finir, on considère le m-sous-espace F_0 engendré par les m premiers vecteurs de la base canonique $(e_1,\cdots,e_m,\cdots,e_n)$. L'application qui envoie γ de $\mathrm{GL}_n(\mathbb{F}_q)$ sur $\gamma(F_0)$ est surjective. Pour voir cela, il suffit de partir d'un sous-espace F de dimension m, de construire une base $(f_1,\cdots,f_m)$ de F, puis une base $(f_{n-m},\cdots,f_n)$ de son supplémentaire. L'automorphisme γ qui envoie la base canonique $(e_1,\cdots,e_m,e_{m+1},\cdots,e_n)$ sur la base $(f_1,\cdots,f_m,f_{m+1},\cdots,f_n)$ est bien défini et envoie F_0 sur F.

De plus, γ envoie F_0 sur F si et seulement si la matrice de γ dans la base des f_i est de la forme $\left(\begin{smallmatrix} A & B \\ 0 & C \end{smallmatrix}\right)$, avec $A \in \mathrm{GL}_m(\mathbb{F}_q)$, $C \in \mathrm{GL}_{n-m}(\mathbb{F}_q)$, et où B est une matrice de taille $(m, n-m)$.

On en déduit, par le lemme du berger [1] et la proposition 2.1 :

$$|\mathrm{Gr}_{m,n}(\mathbb{K})| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{q^{m(n-m)}\,|\mathrm{GL}_m(\mathbb{F}_q)|\,|\mathrm{GL}_{n-m}(\mathbb{F}_q)|} = \frac{(q;q)_n}{(q;q)_m(q;q)_{n-m}}$$

□

Remarque 2.2. Le cardinal de la grassmannienne, appelé *nombre binomial quantique*, est noté $\begin{bmatrix} n \\ m \end{bmatrix}_q$. Il doit cette appellation et cette notation au fait que l'on retrouve le nombre binomial $\binom{n}{m}$ en le voyant comme un polynôme en q évalué en 1. Pour voir cela, il suffit de remarquer que la fraction rationnelle en q donnée par $\frac{1-q^n}{1-q}$ est un polynôme qui, évalué en 1, donne n.

2.2 Identité de Chu-Vandermonde quantifiée

Voici une jolie contribution de la géométrie finie à la combinatoire quantique. Elle est somme toute assez naturelle : l'identité de Chu-Vandermonde a été obtenue en partitionnant un ensemble E à n éléments en un ensemble B à b éléments et un ensemble C à c éléments, puis, à calculer le nombre d'ensembles à m éléments de E qui ont une intersection de cardinal k fixé avec B. Une identité quantifiée va être obtenue en travaillant sur le corps $\mathbb{K} = \mathbb{F}_q$, en considérant E comme un espace de dimension n, B et C comme des sous-espaces en somme directe dans E. On va alors calculer le nombre de sous-espaces de E, de dimension m, et qui vérifient des propriétés d'incidences avec B et C.

Soit donc, $\dim E = n$, $E = B \oplus C$, $\dim B = b$, $\dim C = c$. Soit π la projection sur C parallèlement à B. On a, pour tout sous-espace L de E,

$$\dim L = \dim\big(L \cap B\big) + \dim \pi(L). \tag{16}$$

Il suffit pour voir cela de considérer la restriction de π à L, dont le noyau est $L \cap \ker \pi = L \cap B$.

On considère alors un couple (J, K), où J, resp. K, est un sous-espace de dimension j, resp. k, de B, resp C.

On présente ici une réalisation géométrique de la formule de Chu-Vandermonde. On note ici $\mathrm{Gr}(E)$ l'ensemble de tous les sous-espaces vectoriels de l'espace E.

Proposition 2.3. *Soit*

$$\sigma : \mathrm{Gr}(B \oplus C) \to \mathrm{Gr}(B) \times \mathrm{Gr}(C), \quad \sigma(L) = \big(L \cap B, \pi(L)\big).$$

Alors,

i σ *est surjective,*

ii *Si* $\sigma(L) = (J, K)$, *alors* $\dim L = \dim J + \dim K$,

iii *On fixe un supplémentaire* J' *de* J *dans* B. *Alors, il existe une bijection entre* $\hom(K, J')$ *et* $\sigma^{-1}(J, K)$.

Démonstration. Le premier point est clair puisque $J \oplus K \in \sigma^{-1}(J, K)$. Le second provient de (16). Il reste à montrer le dernier point.

On va donc construire deux applications inverses l'une de l'autre. Pour tout f de $\hom(K, J')$, on considère le sous-espace

$$L_f := \{b + k,\, b \in B,\, k \in K,\, \pi_{J'}(b) = f(k)\},$$

où $\pi_{J'}$ désigne la projection de B sur J' parallèlement à J.

1. Le lemme du berger dit en gros que si on compte n pattes, c'est que l'on a n/4 moutons. Munitieusement vérifié par Grothendieck dans un petit village du Vaucluse.

Inversement, pour tout L dans $\sigma^{-1}(J,K)$, on définit $f_L \in \hom(K,J')$ par

$$k \in K,\ f_L(k) = \pi_{J'}(b),$$

pour tout b dans B tel que $b+k \in L$.

Maintenant, tout cela demande quelques vérifications.

1. L_f est bien dans $\sigma^{-1}(J,K)$.
   Tout d'abord, L_f est bien un sous-espace car $\pi_{J'}$ et f sont des morphismes.
   Montrons que $L_f \cap B = J$. Soit x dans $L_f \cap B$. Alors, $x = b+k$, avec $\pi_{J'}(b) = f(k)$ car $x \in L_f$ et $k = 0$ car $x \in B$. Donc, $\pi_{J'}(b) = 0$ et $b \in J$. Réciproquement, si $x \in J$, et de plus $x = b+0$, $b \in J \subset B$ et $\pi_{J'}(b) = 0 = f(0)$, et donc $x \in L_f \cap B$.
2. f_L est bien un morphisme de K dans J'.
   Il n'est pas clair que f_L soit bien défini. Supposons deux éléments $b+k \in L$, $b'+k \in L$, avec $b, b' \in B$. Il faut montrer que $\pi_{J'}(b') = \pi_{J'}(b)$. Or, $b'-b = (b'+k)-(b+k) \in L$ et donc $b'-b \in L \cap B = J$, ce qui implique $\pi_{J'}(b'-b) = 0$ comme voulu.
   Maintenant, il est clair que f_L est un morphisme.
3. On a $f_{L_f} = f$.
   Soit $f \in \hom(K,J')$ et donc $L_f := \{b+k,\ b \in B,\ k \in K,\ \pi_{J'}(b) = f(k)\}$. Alors, pour tout k dans K, soit x tel que $x = b+k \in L_f$. Il vient $f_{L_f}(k) = \pi_{J'}(b) = f(k)$. La première égalité vient de la définition de f_{L_f} et la seconde, de la construction de L_f.
4. On a $L_{f_L} = L$.
   Soit x dans L. Montrons que x est dans L_{f_L}. On peut décomposer $x = b+c$ dans $B \oplus C$. On veut montrer que $x = b+k$, avec $k \in K$, $b \in B$ et $\pi_{J'}(k) = f_L(b)$. Or, par construction, $\pi(L) = K$, et donc il existe bien x dans L tel que que $x = b+k$ comme voulu. Du coup, par définition de f_L, on a bien $\pi_{J'}(b) = f_L(k)$. Ce qui donne l'inclusion $L \subset L_{f_L}$. L'égalité provient par exemple d'une égalité de dimension par le point (ii) de la proposition.

□

Remarque 2.4. On a beaucoup à gagner en canonicité si l'on réécrit cette proposition en remplaçant les espaces vectoriels par des modules sur une algèbre de dimension finie et en remplaçant la projection $\pi_{J'}$ par la surjection canonique $B \to B/J$. Vue sous cette forme, la proposition n'est rien d'autre que [CC04, lemme 3.8], fondamental dans la combinatoire des algèbres amassées.

Remarque 2.5. La bijection entre $\hom(K,J')$ et $\sigma^{-1}(J,K)$ gagne également à être interprétée avec un poil de recul : on a en fait une action simplement transitive de l'espace vectoriel $\hom(K,J')$ et $\sigma^{-1}(J,K)$, donnée par

$$f.L := \{b+b'+k,\ b+k \in L,\ \pi_{J'}(b') = f(k)\}.$$

Cela signifie tout simplement que $\sigma^{-1}(J,K)$ a une structure d'espace affine, d'espace vectoriel associé $\hom(K,J')$.

Voici une première mouture de l'identité de Chu-Vandermonde quantifiée.

Corollaire 2.6 (q-analogue de l'identité de Chu-Vandermonde)**.** *Soit $l \leq b,c$ trois entiers positifs. On a*

$$\begin{bmatrix} b+c \\ l \end{bmatrix}_q = \sum_{k=0}^{l} \begin{bmatrix} b \\ l-k \end{bmatrix}_q \begin{bmatrix} c \\ k \end{bmatrix}_q q^{k(b-l+k)}.$$

Démonstration. La proposition précédente donne directement $\left|\sigma^{-1}(J,K)\right| = q^{\dim K(\dim B - \dim J)}$. On a donc

$$\left|\mathrm{Gr}_l(\mathbb{F}_q^{b+c})\right| = \sum_{j+k=l} \left|\mathrm{Gr}_j(\mathbb{F}_q^b)\right| \left|\mathrm{Gr}_k(\mathbb{F}_q^c)\right| q^{\dim K(\dim B - \dim J)}$$

Ce qui donne la formule désirée.

□

2.3 Identité de q-Chu-Vandermonde et q-séries hypergéométriques

Le but de cette section est de réinterpréter la formule ci-dessus en termes de fonctions hypergéométriques. On part donc de

$$\begin{bmatrix} a+c \\ b \end{bmatrix}_q = \sum_{j=0}^{l} \begin{bmatrix} a \\ j \end{bmatrix}_q \begin{bmatrix} c \\ b-j \end{bmatrix}_q q^{j(c-b+j)}.$$

Si l'on pose

$$\alpha_j = \begin{bmatrix} a \\ j \end{bmatrix}_q \begin{bmatrix} c \\ b-j \end{bmatrix}_q q^{j(c-b+j)},$$

alors on trouve

$$\frac{\alpha_{j+1}}{\alpha_j} = \frac{(1-q^{-a}q^j)(1-q^{-b}q^j)q^{a+c+1}}{(1-q\cdot q^j)(1-q^{c-b+1}q^j)}.$$

Donc, en mettant en facteur dans la somme le terme en $j=0$, c'est-à-dire $\begin{bmatrix} c \\ b \end{bmatrix}_q$, il vient

$$\sum_{j=0}^{l} \begin{bmatrix} a \\ j \end{bmatrix}_q \begin{bmatrix} c \\ b-j \end{bmatrix}_q q^{j(c-b+j)} = \begin{bmatrix} c \\ b \end{bmatrix}_q \phi(q^{-a}, q^{-b}; q^{c-b+1}; q; q^{a+c+1}).$$

On en déduit donc

$$\begin{bmatrix} c \\ b \end{bmatrix}_q \phi(q^{-a}, q^{-b}; q^{c-b+1}; q; q^{a+c+1}) = \begin{bmatrix} a+c \\ b \end{bmatrix}_q,$$

qui se réécrit

$$(q^{c-b+1};q)_a \phi(q^{-a}, q^{-b}; q^{c-b+1}; q; q^{a+c+1}) = (q^{c+1};q)_a.$$

On peut voir cette égalité comme une égalité polynomiale évaluée en $X = q^{-b}$ et $Y = q^{c+1}$. Comme q^{-b} et $Y = q^{c+1}$ peuvent prendre une infinité de valeurs,

$$(XY;q)_a \phi(q^{-a}, X; XY; q; q^a Y) = (Y;q)_a.$$

Comme a est un entier positif, on n'a, dans la série (11) de ϕ, qu'une somme finie ; on peut restreindre le support de n à $[0, a-1]$. On peut alors changer n en $a-1-n$ dans la formule pour trouver, par (14),

$$\phi(q^{-a}, X; XY; q; q^a Y) = \frac{(-a;q)_a}{(q;q)_a} Y^a q^{a^2} \frac{(X;q)_a}{(XY;q)_a} \phi(q^{-a}, X^{-1}Y^{-1}q^{1-a}; X^{-1}q^{1-a}; q; q).$$

On pose $U := X^{-1}Y^{-1}q^{1-a}$ et $V := X^{-1}q^{1-a}$. On a alors,

$$\phi(q^{-a}, U; V; q; q) = \frac{(q;q)_a}{(-a;q)_a} V^{-a} U^a q^{-a^2} \frac{(q^{1-a}U^{-1};q)_a}{(q^{1-a}V^{-1};q)_a} \phi(q^{-a}, q^{1-a}V^{-1}; q^{1-a}U^{-1}; q; q^a VU^{-1})$$

En utilisant (13), on obtient, après une simplification étonnante, une formule appelée encore identité de Chu-Vandermonde (quantifiée)

Proposition 2.7. *Pour tout $a \in \mathbb{N}$, on a dans le corps de fractions rationnelles $\mathbb{C}(U,V)$, l'égalité*

$$\phi(q^{-a}, U; V; q; q) = U^a \frac{(VU^{-1};q)_a}{(V;q)_a}.$$

On en déduit, comme cas particulier, le corollaire :

Corollaire 2.8.

$$\sum_{k=0}^{n} (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} (q;q^2)_k q^{k^2+k-2nk} = q^n$$

Démonstration. On pose $V = 0$, $n = a$, et on remplace q par q^2. Ensuite, on évalue z en q^2 et U en q. C'est droit devant, en utilisant, dans la définition de ϕ, la formule (15) et la définition du nombre binomial quantique.

□

3 Les cônes nilpotents des algèbres de Lie semi-simples

Une matrice N est nilpotente si elle vérifie $N^k = 0$ pour k assez grand. L'ensemble des matrices nilpotentes est stable par multiplication par un scalaire et, à ce titre, forme un cône dans l'espace vectoriel de matrices. Pour comprendre l'importance du cône des matrices nilpotentes, il suffit de regarder la décomposition de Dunford, qui montre que la « composante nilpotente » d'une matrice est un obstacle à sa diagonalisabilité (sur $\mathbb{C}$). On peut aussi voir son rôle fondamental par le lemme de Fitting qui dit que pour tout endomorphisme u d'un espace E de dimension finie, il existe une décomposition de $E = F \oplus G$ telle que F et G sont stables par u, u_F étant un automorphisme de F et u_G étant nilpotent sur G. Précisons :

3.1 Lemme de Fitting

On sait que les puissances de u ont des noyaux emboîtés, *i.e.* $\ker(u^i) \subset \ker(u^{i+1})$. Soit k l'indice minimum tel que $\ker(u^k) = \ker(u^{k+1})$; k existe puisque l'on est en dimension finie et on voit aisément que l'on a alors $\ker(u^m) = \ker(u^{m+1})$ pour tout $m \geq k$. On dit que la suite des noyaux emboîtés est croissante et stationnaire. De même, la suite des images emboîtées est décroissante et stationnaire, et ce à partir du même rang k, par la formule du rang.

Notation 3.1. On note $\ker(u^\infty)$, resp. $\mathrm{Im}(u^\infty)$, le sous-espace $\ker(u^k)$, resp. $\mathrm{Im}(u^k)$. Il s'agit de la limite de la suite stationnaire $\ker(u^m)$, resp. $\mathrm{Im}(u^m)$, de sous-espaces.

Remarque 3.2. Cette notation classique nécessite tout de même un garde-fou. Si l'on est sur le corps des réels ou celui des complexes, la limite de u^m peut avoir un sens. Or, la limite du noyau n'est pas égale au noyau de la limite. Par exemple, si u est l'homothétie de rapport $\frac{1}{2}$, alors u est un automorphisme et u^m tend vers l'endomorphisme nul. Il en résulte que $\ker(u^\infty)$ est nul alors que $\ker(\lim_{m\to+\infty} u^m)$ est l'espace E tout entier.

Lemme 3.3 (Décomposition de Fitting)**.** *Soit u un endomorphisme de l'espace E de dimension finie sur un corps quelconque. Alors,*

i les sous-espaces $\ker(u^\infty)$ *et* $\mathrm{Im}(u^\infty)$ *sont stables par u,*

ii $E = \mathrm{Im}(u^\infty) \oplus \ker(u^\infty)$,

iii u est nilpotent sur $\ker(u^\infty)$,

iv u définit un automorphisme de $\mathrm{Im}(u^\infty)$ *dans lui-même.*

Démonstration. (i) On voit que l'image directe de $\ker(u^m)$ par u est dans $\ker(u^{m-1})$, pour tout m, donc $\ker(u^\infty) = \ker(u^k)$ est stable par u. De plus, l'image directe de $\mathrm{Im}(u^m)$ par u est dans $\mathrm{Im}(u^{m+1})$, et donc l'image directe de l'image directe de $\mathrm{Im}(u^k)$ par u est dans (et même égale à) $\mathrm{Im}(u^{k+1}) = \mathrm{Im}(u^k)$.

(ii) Par la formule du rang, $\dim \mathrm{Im}(u^\infty) + \dim \ker(u^\infty) = \dim E$. Il suffit donc de montrer que $\ker(u^k) \cap \mathrm{Im}(u^k)$ est nul. Soit $x \in \ker(u^k) \cap \mathrm{Im}(u^k)$, on a $x = u^k(y)$ pour un y, et $u^k(x) = 0$. Ainsi, $u^k\big(u^k(y)\big) = 0$, et donc $y \in \ker(u^{2k}) = \ker(u^k)$. Ainsi, $x = u^k(y) = 0$ comme annoncé.

(iii) Clair, par construction.

(iv) Cherchons le noyau de la restriction de u à $\mathrm{Im}(u^\infty)$. C'est par définition $\ker(u) \cap \mathrm{Im}(u^k)$. Or, $\ker(u) \cap \mathrm{Im}(u^k) \subset \ker(u^k) \cap \mathrm{Im}(u^k) = 0$. Donc, le noyau de la restriction est nul, et comme cette restriction est un endomorphisme de $\mathrm{Im}(u^\infty)$, il s'agit d'un automorphisme. □

On appellera la décomposition de E ci-dessus, décomposition de Fitting de u. On peut donc associer, à tout endomorphisme u de $E := \mathbb{K}^n$, un couple (F, G) de sous-espaces supplémentaires de E, $0 \leq \dim G = k \leq n$, un automorphisme de F, et un endomorphisme nilpotent de G. Inversement, la donnée de deux sous-espaces supplémentaires, F et G, d'un automorphisme v de F et d'un endomorphisme nilpotent w de G, permet de construire un unique endomorphisme u de E tel que $u_F = v$ et $u_G = w$. Et de plus, on voit facilement que $F \oplus G$ est la décomposition de Fitting de u. Soit $S_{k,n}(\mathbb{F}_q) \subset \mathrm{Gr}_{n-k}(\mathbb{F}_q) \times \mathrm{Gr}_k(\mathbb{F}_q)$ l'ensemble des couples de sous-espaces supplémentaires (F, G) de $\mathbb{F}_q^n$. Notons $A_k(\mathbb{F}_q)$ le cône des matrices de taille k nilpotente sur $\mathbb{F}_q$. On a montré :

Corollaire 3.4. *La décomposition de Fitting, voir lemme 3.3, fournit une bijection*

$$\mathrm{End}(\mathbb{F}_q^n) \xrightarrow{\sim} \cup_{k=0}^n S_{k,n}(\mathbb{F}_q) \times \mathrm{GL}_{n-k}(\mathbb{F}_q) \times A_k(\mathbb{F}_q)$$

$$u \mapsto \left((\mathrm{Im}\, u^\infty, \ker u^\infty), u_{\mathrm{Im}\, u^\infty}, u_{\ker u^\infty}\right)$$

3.2 Cardinal du cône nilpotent. Le cas $\mathbf{A}_n$.

Nous allons calculer le cardinal de l'ensemble $A_n(q)$ des matrices nilpotentes de taille n sur un corps $\mathbb{K} = \mathbb{F}_q$ de cardinal q. Le résultat est étonnamment simple, voir section 4.2 pour une explication haute en couleurs.

Commençons par une formule classique :

$$\sum_{k=0}^{n} \frac{(-1)^k q^{\binom{k}{2}}}{(q;q)_k} = \frac{(-1)^n q^{\binom{n+1}{2}}}{(q;q)_n}, \tag{17}$$

valable pour tout q complexe et n entier positif.

Pour la montrer, une récurrence suffit. Pour $n = 0$, c'est clair, pour l'hérédité, il suffit de montrer l'égalité

$$\frac{(-1)^{n-1} q^{\binom{n}{2}}}{(q;q)_{n-1}} + \frac{(-1)^n q^{\binom{n}{2}}}{(q;q)_n} = \frac{(-1)^n q^{\binom{n+1}{2}}}{(q;q)_n},$$

ce qui revient, après multiplication par $(-1)^n (q;q)_n q^{-\binom{n}{2}}$ à vérifier l'égalité $-(1-q^n)+1 = q^n$, qui ne posera de problème à personne.

On déduit :

Théorème 3.5. *Le cardinal de l'ensemble $A_n(q)$ des matrices nilpotentes de taille n sur le corps $\mathbb{F}_q$ est donné par*

$$|A_n(q)| = q^{n(n-1)}.$$

Démonstration. On le montre par récurrence sur n. Le cas $n = 0$ est clair. Supposons donc $|A_m(q)| = q^{m(m-1)}$ pour tout $m < n$. Alors, la bijection ci-dessus donne, par égalité des cardinaux,

$$q^{n^2} = \sum_{k=0}^{n} |S_{k,n}(\mathbb{F}_q)| \cdot |\mathrm{GL}_{n-k}(\mathbb{F}_q)| \cdot |A_k(\mathbb{F}_q)|\,.$$

Calculons tout d'abord $|S_{k,n}(\mathbb{F}_q)|$. Pour cela, on fixe un couple (F_0, G_0) dans $S_{k,n}(\mathbb{F}_q)$. On procède comme dans la preuve de la proposition 2.1 (iii) : l'application qui à g dans $\mathrm{GL}(\mathbb{F}_q^n)$ associe $\big(g(F_0), g(G_0)\big)$ dans $S_{k,n}(\mathbb{F}_q)$ est surjective par le théorème de la base incomplète. De plus, l'image réciproque de $(F, G) \in S_{k,n}(\mathbb{F}_q)$ s'écrit matriciellement dans une base bien choisie $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$, avec $A \in \mathrm{GL}_{n-k}(\mathbb{F}_q)$, $B \in \mathrm{GL}_k(\mathbb{F}_q)$. Ce qui prouve, par le lemme du berger, l'égalité

$$|S_{k,n}(\mathbb{F}_q)| = \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n-k}(\mathbb{F}_q)|\,|\mathrm{GL}_k(\mathbb{F}_q)|}$$

L'égalité devient

$$q^{n^2} = \sum_{k=0}^{n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_k(\mathbb{F}_q)|} \cdot |A_k(\mathbb{F}_q)| = \sum_{k=0}^{n} \frac{(-1)^{n-k}(q;q)_n q^{\binom{n}{2}-\binom{k}{2}}}{(q;q)_k} \cdot |A_k(\mathbb{F}_q)|\,.$$

Et donc,

$$\frac{(-1)^n q^{\binom{n+1}{2}}}{(q;q)_n} = \sum_{k=0}^{n} \frac{(-1)^k q^{-\binom{k}{2}}}{(q;q)_k} \cdot |A_k(\mathbb{F}_q)|\,.$$

Ceci nous donne l'égalité voulue par récurrence et par (17).

□

3.3 Lemme de Fitting et formes bilinéaires.

On suppose maintenant que l'espace E est doté d'une forme bilinéaire non dégénérée et on va montrer un lemme de Fitting adapté à la géométrie de E induite par cette forme.

Définition 3.6. Soit $\epsilon = \pm 1$. Une forme (bilinéaire) ϵ-symétrique $\langle\ ,\ \rangle$ est une forme bilinéaire symétrique, resp. antisymétrique, si $\epsilon = 1$, resp. $\epsilon = -1$. On supposera dans la suite que l'espace E est muni d'une forme $\langle\ ,\ \rangle$ ϵ-symétrique non dégénérée.

On note G le groupe des automorphismes de E qui respectent la forme et $\mathfrak{g} := \mathfrak{g}(E)$ le sous-espace des endomorphismes de E antisymétriques pour la forme.

$$G := \{g \in \mathrm{GL}(E),\ \langle g(x), y\rangle = \langle x, g(y)\rangle,\ x, y \in E\},$$

$$\mathfrak{g} := \{u \in \mathrm{End}(E),\ \langle u(x), y\rangle = -\langle x, u(y)\rangle,\ x, y \in E\}$$

On vérifie que G agit sur $\mathfrak{g}$ par conjugaison. Si $g \in G$, $u \in \mathfrak{g}$, alors

$$\langle gu\big(g^{-1}(x)\big), y\rangle = \langle u\big(g^{-1}(x)\big), g^{-1}(y)\rangle = -\langle g^{-1}(x), u\big(g^{-1}(y)\big)\rangle = -\langle x, gu\big(g^{-1}(y)\big)\rangle,$$

ce qui prouve l'assertion.

Proposition 3.7. *Soit u dans $\mathfrak{g}$ et $E = \mathrm{Im}(u^\infty) \oplus \ker(u^\infty)$ sa décomposition de Fitting. Alors,*

i Cette décomposition est orthogonale pour $\langle\ ,\ \rangle$,

ii La restriction de $\langle\ ,\ \rangle$ à $\mathrm{Im}(u^\infty)$, resp. $\ker(u^\infty)$, est non dégénérée.

Démonstration. Soit $x \in \mathrm{Im}(u^\infty)$, $x' \in \ker(u^\infty)$. Alors, $x = u^k(y)$ pour un y dans E et un k assez grand, et

$$\langle x, x'\rangle = \langle u^k(y), x\rangle = (-1)^k\langle y, u^k(x)\rangle = (-1)^k\langle y, 0\rangle = 0.$$

Comme la forme $\langle\ ,\ \rangle$ est non dégénérée, $\dim \mathrm{Im}(u^\infty)^\perp = n - \dim \mathrm{Im}(u^\infty)$. Donc, l'inclusion $\ker(u^\infty) \subset \mathrm{Im}(u^\infty)^\perp$ devient une égalité. Ainsi, $\mathrm{Im}(u^\infty) \cap \mathrm{Im}(u^\infty)^\perp = 0$ et donc la restriction de $\langle\ ,\ \rangle$ à $\mathrm{Im}(u^\infty)$ est non dégénérée. L'assertion sur $\ker(u^\infty)$ est analogue.

□

Réciproquement, on peut construire un élément de $\mathfrak{g}$ à partir d'une décomposition orthogonale $E = F \oplus G$.

Proposition 3.8. *Soit F un sous-espace de E tel que la restriction de $\langle\ ,\ \rangle$ à F soit non dégénérée, alors $E = F \oplus F^\perp$. Soit v dans $\mathrm{GL}(F) \cap \mathfrak{g}(F)$ et w un endomorphisme nilpotent de $\mathfrak{g}(F^\perp)$. Alors, il existe un unique endomorphisme u de $\mathfrak{g}(E)$ tel que $u_F = v$ et $u_{F^\perp} = w$. La décomposition de Fitting de u est donnée par $F \oplus F^\perp$.*

Démonstration. L'équivalence $\langle\ ,\ \rangle_{F\times F}$ non dégénérée $\Leftrightarrow$ $E = F \oplus F^\perp$ est classique, voir par exemple [CG12, Lemme V-A.1.13].

L'existence et l'unicité de u comme endomorphisme, ainsi que sa décomposition de Fitting ont déjà été vue. Le fait que u soit dans $\mathfrak{g}(E)$ provient de $v \in \mathfrak{g}(F)$, et $w \in \mathfrak{g}(F^\perp)$.

□

On en déduit le corollaire

Corollaire 3.9. *La décomposition de Fitting fournit une bijection*

$$\mathfrak{g}(E) \xrightarrow{\sim} \cup_{k=0}^{n} \mathrm{Gr}_k^0(E) \times \big(\mathrm{GL}_k(\mathbb{F}_q) \cap \mathfrak{g}(\mathbb{F}_q^k)\big) \times \big(A_{n-k}(\mathbb{F}_q) \cap \mathfrak{g}(\mathbb{F}_q^{n-k})\big),$$

où $\mathrm{Gr}_k^0(E)$ désigne l'ensemble des sous-espaces de dimension k de E sur lesquels la forme $\langle\ ,\ \rangle$ est non dégénérée.

3.4 Classification des formes ϵ-symétriques sur $\mathbb{F}_q$.

On ne peut plus se passer à ce stade du langage des actions de groupes ainsi que de quelques théorèmes de base sur les formes bilinéaires. En ce qui concerne les actions de groupes, on pourra se référer à [CG12, I-A].

Soit E un espace vectoriel de dimension finie sur le corps $\mathbb{F}_q$ de cardinal q *impair*. Le groupe $\mathrm{GL}_n(\mathbb{F}_q)$ agit par l'action, dite de congruence, sur l'espace $\mathcal{S}_+$ des matrices symétriques , resp. l'espace $\mathcal{S}_-$ des matrices antisymétriques, de taille n :

$$P \cdot A = PA\,{}^tP,\ P \in \mathrm{GL}_n(\mathbb{F}_q),\ A \in \mathcal{S}_\epsilon$$

Cette action matricielle permet de classifier les formes bilinéaires ϵ-symétriques à changement de base près.

Cas symétrique.

Sur $\mathbb{F}_q$, il existe exactement deux orbites de formes non dégénérées, c'est-à-dire de matrices inversibles, pour cette action. Une matrice inversible est dans une des deux orbites selon si son déterminant est un carré (non nul) ou non. Il s'agit donc des orbites de la matrice identité $\mathrm{I} = \mathrm{I}_n = \mathrm{diag}(1, \cdots, 1)$, et de la matrice $\mathrm{I}_\zeta := \mathrm{diag}(1, \cdots, 1, \zeta)$, où ζ désigne un élément fixé de $\mathbb{F}_q$ qui n'est pas un carré [2].

On dira que la forme est de *discriminant* 1 dans le premier cas et ζ dans le second.

On s'intéresse donc aux stabilisateurs de ces matrices ; ce sont les groupes qui respectent les formes symétriques non dégénérées correspondantes :

$$\mathrm{O}_n(\mathbb{F}_q) := \{P \in \mathrm{GL}_n(\mathbb{F}_q),\ P\,{}^tP = \mathrm{I}_n\},\ \mathrm{O}_n^\zeta(\mathbb{F}_q) := \{P \in \mathrm{GL}_n(\mathbb{F}_q),\ P\mathrm{I}_\zeta\,{}^tP = \mathrm{I}_\zeta\}.$$

A l'instar du cas réel, ces groupes orthogonaux agissent transitivement sur les « sphères » définies par les formes. En calculant le cardinal de ces sphères ainsi que celui de leur stabilisateur, on montre, voir [CG14, Théorème IV-2.1],

Théorème 3.10. *On pose* $\alpha := (-1)^{\frac{q-1}{2}}$.

Alors, l'ordre des groupes orthogonaux finis est donné par :

$$|\mathrm{O}_{2n+1}(\mathbb{F}_q)| = 2(-1)^n q^{n^2}(q^2;q^2)_n,\ |\mathrm{O}_{2n}(\mathbb{F}_q)| = 2(-1)^{n-1}(q^n - \alpha^n)q^{n(n-1)}(q^2;q^2)_{n-1}$$

$$\left|\mathrm{O}_{2n+1}^\zeta(\mathbb{F}_q)\right| = 2(-1)^n q^{n^2}(q^2;q^2)_n,\ \left|\mathrm{O}_{2n}^\zeta(\mathbb{F}_q)\right| = 2(-1)^{n-1}(q^n + \alpha^n)q^{n(n-1)}(q^2;q^2)_{n-1}$$

On peut alors en déduire le nombre s_n de matrices symétriques inversibles de taille n : elles se divisent, d'après ce qui précède, en deux orbites pour l'action de $\mathrm{GL}_n(\mathbb{F}_q)$ de stabilisateurs respectifs $\mathrm{O}_n(\mathbb{F}_q)$ et $\mathrm{O}_n^\zeta(\mathbb{F}_q)$. On a donc, après simplification

$$s_{2n+1} = \frac{|\mathrm{GL}_{2n+1}(\mathbb{F}_q)|}{|\mathrm{O}_{2n+1}(\mathbb{F}_q)|} + \frac{|\mathrm{GL}_{2n+1}(\mathbb{F}_q)|}{\left|\mathrm{O}_{2n+1}^\zeta(\mathbb{F}_q)\right|} = (-1)^{n+1}q^{n(n+1)}(q;q^2)_{n+1} \tag{18}$$

$$s_{2n} = \frac{|\mathrm{GL}_{2n}(\mathbb{F}_q)|}{|\mathrm{O}_{2n}(\mathbb{F}_q)|} + \frac{|\mathrm{GL}_{2n}(\mathbb{F}_q)|}{\left|\mathrm{O}_{2n}^\zeta(\mathbb{F}_q)\right|} = (-1)^n q^{n(n+1)}(q;q^2)_n \tag{19}$$

On va maintenant calculer le nombre $g_{k,n}(b)$ de sous-espaces de $\mathbb{F}_q^n$ de dimension k sur lesquels la restriction d'une forme bilinéaire symétrique (non dégénérée) est elle-même non dégénérée.

Soit b la forme bilinéaire sur $\mathbb{F}_q^n$ ayant pour matrice I_n dans la base canonique. On note $\mathrm{Gr}_k^0(b)$ l'ensemble des sous-espaces F de dimension k de $\mathbb{F}_q^n$ tels que la restriction de b sur F est non dégénérée.

Si $0 < k < n$, et F dans $\mathrm{Gr}_k^0(b)$, alors, la restriction de b à F peut être de discriminant 1 ou ζ, on notera $\mathrm{Gr}_k^{0,1}(b)$ et $\mathrm{Gr}_k^{0,\zeta}(b)$ la partition de $\mathrm{Gr}_k^0(b)$ correspondante. Effectivement, par [CG12, Théorème V-1.2], [3], $\mathrm{diag}(1, \cdots, 1)$ est congruente à $\mathrm{diag}(1, \cdots, 1, \zeta, \zeta)$. Par le

2. Comme q est impair, le morphisme de $\mathbb{F}_q^*$ est non injectif et donc non surjectif.
3. En fait, il suffit de voir que leurs déterminants respectifs sont des carrés non nuls.

théorème de Witt, [CG12, Chap. V, Théorème 3.4], le groupe $\mathrm{O}_n(\mathbb{F}_q)$ agit sur $\mathrm{Gr}_k^0(b)$, et l'action possède deux orbites, nommément $\mathrm{Gr}_k^{0,1}(b)$ et $\mathrm{Gr}_k^{0,\zeta}(b)$. Soit F dans $\mathrm{Gr}_k^{0,1}(b)$, alors, la restriction de b à $F^\perp$ (qui est un supplémentaire de F) est également de discriminant 1, et tout g de $\mathrm{O}_n(\mathbb{F}_q)$ stabilisant F stabilise aussi $F^\perp$. Le stabilisateur de F dans $\mathrm{O}_n(\mathbb{F}_q)$ est alors isomorphe au produit direct $\mathrm{O}_k(\mathbb{F}_q) \times \mathrm{O}_{n-k}(\mathbb{F}_q)$, [4]. De même, si F est dans $\mathrm{Gr}_k^{0,\zeta}(b)$, alors, la restriction de b à $F^\perp$ (qui est un supplémentaire de F) est également de discriminant ζ, et tout g de $\mathrm{O}_n(\mathbb{F}_q)$ stabilisant F stabilise aussi $F^\perp$. Le stabilisateur de F dans $\mathrm{O}_n(\mathbb{F}_q)$ est alors isomorphe au produit direct $\mathrm{O}_k^\zeta(\mathbb{F}_q) \times \mathrm{O}_{n-k}^\zeta(\mathbb{F}_q)$. On en déduit :

$$g_{k,n}(b) = \frac{|\mathrm{O}_n(\mathbb{F}_q)|}{|\mathrm{O}_k(\mathbb{F}_q)| \cdot |\mathrm{O}_{n-k}(\mathbb{F}_q)|} + \frac{|\mathrm{O}_n(\mathbb{F}_q)|}{\left|\mathrm{O}_k^\zeta(\mathbb{F}_q)\right| \cdot \left|\mathrm{O}_{n-k}^\zeta(\mathbb{F}_q)\right|}$$

Le développement de ce calcul demande une étude cas par cas selon la parité de n et k. Par exemple, on trouve après simplification

$$g_{2k,2n}(b) = q^{2k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_{q^2}$$

On trouve également

$$g_{2k,2n+1}(b) = q^{2k(n+1-k)} \begin{bmatrix} n \\ k \end{bmatrix}_{q^2}$$

Cas antisymétrique.

Le cas antisymétrique est plus simple. Sur $\mathbb{F}_q$, en dimension paire $2n$, il existe exactement une seule orbite de formes non dégénérées, c'est-à-dire de matrices inversibles, pour l'action de $\mathrm{GL}_{2n}(\mathbb{F}_q)$ par congruence. Il s'agit donc de l'orbite de la matrice $J := J_n$ (de taille $2n$) donnée par

$$J := \begin{pmatrix} 0_n & -\mathrm{I}_n \\ \mathrm{I}_n & 0_n \end{pmatrix}.$$

On s'intéresse donc aux stabilisateurs de cette matrice ; c'est le groupe symplectique :

$$\mathrm{Sp}_{2n}(\mathbb{C}) = \left\{P \in \mathrm{GL}_{2n}(\mathbb{K}),\ {}^tPJP = J\right\}.$$

Soit ω la forme antisymétrique sur $\mathbb{F}_q^n$ dont la matrice dans la base canonique est la matrice J. Le groupe symplectique agit transitivement sur les couples (u, v) tels que $\omega(u, v) = 1$. En calculant le cardinal de l'ensemble de ces couples ainsi que celui de leur stabilisateur, on montre, voir [CG14, Exercice IV-8],

Théorème 3.11. *L'ordre du groupe symplectique est donné par :*

$$|\mathrm{Sp}_{2n}(\mathbb{F}_q)| = (-1)^n q^{n^2} (q^2; q^2)_n$$

On peut alors en déduire le nombre a_{2n} de matrices antisymétriques inversibles de taille $2n$ (il est bien sûr nul en cas impair) : elles forment, d'après ce qui précède, une seule orbite pour l'action de $\mathrm{GL}_{2n}(\mathbb{F}_q)$ de stabilisateur $\mathrm{Sp}_{2n}(\mathbb{F}_q)$. On a donc, après simplification

$$a_{2n} = \frac{|\mathrm{GL}_{2n}(\mathbb{F}_q)|}{|\mathrm{Sp}_{2n}(\mathbb{F}_q)|} = (-1)^n q^{n^2-n} (q; q^2)_n \tag{20}$$

On va maintenant calculer le nombre $h_{2k,2n}(b)$ de sous-espaces de $\mathbb{F}_q^{2n}$ de dimension $2k$ sur lesquels la restriction de la forme bilinéaire antisymétrique (non dégénérée) ω est elle-même non dégénérée (on sait qu'il n'y en a pas en dimension impaire).

On note $\mathrm{Gr}_{2k}^0(\omega)$ l'ensemble des sous-espaces F de dimension $2k$ de $\mathbb{F}_q^{2n}$ tels que la restriction de ω sur F est non dégénérée.

4. L'isomorphisme est donné par $u \mapsto (u_F, u_{F^\perp})$ car $F \oplus F^\perp = E$.

Par [CG12, Proposition V-4.1], on voitque le groupe $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ agit sur $\mathrm{Gr}^0_{2k}(\omega)$, et que l'action possède une seule orbite. Soit F dans $\mathrm{Gr}^0_{2k}(\omega)$, alors, la restriction de ω à $F^\perp$ (qui est un supplémentaire de F) est également non dégénérée, et tout g de $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ stabilisant F stabilise aussi $F^\perp$. Le stabilisateur de F dans $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ est alors isomorphe au produit direct $\mathrm{Sp}_{2k}(\mathbb{F}_q) \times \mathrm{Sp}_{2n-2k}(\mathbb{F}_q)$, [5] . On en déduit :

$$h_{2k,2n}(\omega) = \frac{|\mathrm{Sp}_{2n}(\mathbb{F}_q)|}{|\mathrm{Sp}_{2k}(\mathbb{F}_q)| \cdot |\mathrm{Sp}_{2n-2k}(\mathbb{F}_q)|} = q^{2k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix}_{q^2}$$

3.5 Matrices nilpotentes associées à une forme ϵ-bilinéaire.

On va calculer le nombre de matrices nilpotentes de $\mathfrak{g}(E)$ pour les différentes formes non dégénérées rencontrées.

Notation 3.12. On fixe une base de E, et soit M la matrice de la forme $\langle\,,\,\rangle$ dans cette base. Alors on notera

1. $B_n(q)$ l'ensemble des matrices nilpotentes de $\mathfrak{g}(E)$ pour $\dim E = 2n+1$ et $M = \mathrm{I}_{2n+1}$
2. $C_n(q)$ l'ensemble des matrices nilpotentes de $\mathfrak{g}(E)$ pour $\dim E = 2n$ et $M = J$
3. $D_n(q)$ l'ensemble des matrices nilpotentes de $\mathfrak{g}(E)$ pour $\dim E = 2n$ et $M = \mathrm{I}_{2n}$

Nous allons calculer ces différents cardinaux. On retrouve dans [BGS14] le lien entre ces formules et l'identité de q-Chu-Vandermonde.

Théorème 3.13. *Le cardinal des ensembles $B_n(q)$, $C_n(q)$, $D_n(q)$ de matrices nilpotentes de $\mathfrak{g}(E)$ sur le corps $\mathbb{F}_q$ est donné par*

$$|B_n(q)| = q^{2n^2},\ |C_n(q)| = q^{2n^2},\ |D_n(q)| = q^{2n(n-1)}.$$

Démonstration. On commence par un lemme qui relie les matrices ϵ-symétriques inversibles aux éléments inversibles de $\mathfrak{g}(E)$.

On voit facilement que si A vérifie ${}^tAM + MA = 0$ avec M inversible et ϵ-symétrique, alors $B := {}^tAM$ vérifie $B + \epsilon\,{}^tB = 0$. On a donc :

Lemme 3.14. *Soit M une matrice inversible et ϵ-symétrique et $E = \mathbb{K}^n$ l'espace muni de la forme $\langle\,,\,\rangle$ définie par M dans la base canonique de E. Alors, $A \mapsto {}^tAM$ fournit un isomorphisme entre $\mathfrak{g}(E)$ et l'espace des matrices ϵ-symétriques de taille n. De plus, on obtient ainsi une bijection entre les inversibles de ces deux espaces.*

Cas orthogonal impair. On suppose ici que la forme non dégénérée sur $\mathbb{F}_q^{2n+1}$ est donnée par la matrice I_{2n+1}. Le nombre de matrices de $\mathrm{GL}_{2k}(\mathbb{F}_q) \cap \mathfrak{g}(\mathbb{F}_q^{2k})$ est égal à a_{2k}.

D'après le lemme de Fitting adapté au cas orthogonal par le corollaire 3.9 :

$$|\mathfrak{g}(E)| = \sum_{k=0}^{n} |B_{n-k}(q)|\, g_{2k,2n+1} a_{2k}.$$

Par le lemme 3.14, l'espace $\mathfrak{g}(E)$ est de dimension $(2n+1)(2n)/2 = 2n^2 + n$.

On a donc

$$q^{2n^2+n} = \sum_{k=0}^{n} |B_{n-k}(q)| \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} q^{2k(n+1-k)} (-1)^k q^{k^2-k} (q;q^2)_k.$$

Ce qui donne :

$$q^n = \sum_{k=0}^{n} \big(|B_{n-k}(q)|\, q^{-2(n-k)^2} \big) (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} (q;q^2)_k q^{k(k+1)-2nk}.$$

5. L'isomorphisme est une fois de plus donné par $u \mapsto (u_F, u_{F^\perp})$.

En comparant avec le corollaire 2.8, on obtient par récurrence l'égalité $|B_k(q)| = q^{2k^2}$.

Cas symplectique. On suppose ici que la forme non dégénérée sur $\mathbb{F}_q^{2n}$ est donnée par la matrice J. D'après le lemme qui précède, le nombre de matrices de $\mathrm{GL}_k(\mathbb{F}_q) \cap \mathfrak{g}(\mathbb{F}_q^{2k})$ est égal à s_{2k}.

D'après le lemme de Fitting adapté au cas orthogonal par le corollaire 3.9 :

$$|\mathfrak{g}(E)| = \sum_{k=0}^{n} |C_{n-k}(q)|\, h_{2k,2n} s_{2k}.$$

Par le lemme 3.14, l'espace $\mathfrak{g}(E)$ est de dimension $2n(2n+1)/2 = 2n^2 + n$.
On a donc

$$q^{2n^2+n} = \sum_{k=0}^{n} |C_{n-k}(q)| \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} q^{2k(n-k)} (-1)^k (q;q^2)_k q^{k(k+1)}.$$

Ce qui donne :

$$q^n = \sum_{k=0}^{n} \big(|C_{n-k}(q)|\, q^{-2(n-k)^2} \big) (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} (q;q^2)_k q^{k(k+1)-2nk}.$$

En comparant avec le corollaire 2.8, on obtient par récurrence l'égalité $|C_k(q)| = q^{2k^2}$.

Cas orthogonal pair.

On suppose ici que la forme non dégénérée sur $\mathbb{F}_q^{2n}$ est donnée par la matrice I_{2n}. Le nombre de matrices de $\mathrm{GL}_{2k}(\mathbb{F}_q) \cap \mathfrak{g}(\mathbb{F}_q^{2k})$ est égal à a_{2k}.

D'après le lemme de Fitting adapté au cas orthogonal par le corollaire 3.9 :

$$|\mathfrak{g}(E)| = \sum_{k=0}^{n} |C_{n-k}(q)|\, g_{2k,2n} a_{2k}.$$

Par le lemme 3.14, l'espace $\mathfrak{g}(E)$ est de dimension $2n(2n-1)/2 = 2n^2 - n$.
On a donc

$$q^{2n^2-n} = \sum_{k=0}^{n} |D_{n-k}(q)| \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} q^{2k(n-k)} (-1)^k q^{k^2-k} (q;q^2)_k.$$

Ce qui donne :

$$q^n = \sum_{k=0}^{n} \big(|D_{n-k}(q)|\, q^{-2(n-k)(n-k-1)} \big) (-1)^k \begin{bmatrix} n \\ k \end{bmatrix}_{q^2} (q;q^2)_k q^{k(k+1)-2nk}.$$

En comparant avec le corollaire 2.8, on obtient par récurrence l'égalité $|D_k(q)| = q^{2k(k-1)}$.

□

4 Méthodes alternatives

Nous allons voir d'autres approches pour le calcul du cardinal du cône nilpotent. Une, naturelle, mais sans espoir. Une autre, beaucoup plus sybilline, liée aux conjectures de Weyl.

4.1 Approche orbitale.

Une approche plus instinctive pour calculer le cardinal $|A_n(q)|$ du cône nilpotent aurait été de faire agir le groupe $\mathrm{GL}_n(\mathbb{F}_q)$.

Pour une matrice nilpotente A, d'indice[6] k, on définit la partition $\lambda(A)$ de n

$$\lambda(A) := \left(\dim A \geq \dim A^2 - \dim A \geq \dim A^3 - \dim A^2 \geq \cdots \geq \dim A^k - \dim A^{k-1}\right)$$

On sait, voir [CG12, Théorème III-2.5.1], que deux matrices A et A' sont nilpotentes de taille n sont conjuguées si et seulement si leurs partitions associées sont égales.

Soit $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k)$ une partition de n, avec $k = k(\lambda)$. On peut montrer en exercice, à partir des indications données par la suite, que le cardinal du stabilisateur d'une matrice nilpotente associée à A, pour l'action de conjugaison, est égal à

Proposition 4.1.

$$n_\lambda := q^{d(\lambda)} \prod_{i=1}^{k(\lambda)} \left|\mathrm{GL}_{\lambda_i - \lambda_{i+1}}\right|, \text{ avec } d(\lambda) = \sum_{i=1}^{k(\lambda)} \lambda_i^2 - \sum_{i=1}^{k} (\lambda_i - \lambda_{i+1})^2,$$

en convenant que $\lambda_{k+1} = 0$.

Esquisse de preuve.

Soit donc ι un endomorphisme associé à la partition λ de n. On sait, voir [CG12, III-2.4], que l'on peut munir l'espace $\mathbb{F}_q^n$ d'une base

$$(v_m^1, \iota(v_m^1), \ldots, \iota^{m-1}(v_m^1), v_m^2, \ldots, \iota^{m-1}(v_m^2), \ldots, v_1^{\lambda_1}),$$

de sorte que, dans le tableau ci-dessous, la i-ème ligne, en partant du bas, possède λ_i boîtes.

v_m^1	v_m^2	$\cdots$	$v_m^{\lambda_m}$							
ιv_m^1	ιv_m^2	$\cdots$	$\iota v_m^{\lambda_m}$	$v_{m-1}^{\lambda_m+1}$	$\cdots$	$v_{m-1}^{\lambda_{m-1}}$				
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$			
$\iota^{n-r} v_m^1$	$\iota^{n-r} v_m^2$	$\cdots$	$\iota^{n-r} v_m^{\lambda_m}$		$\cdots$			$v_r^{\lambda_r}$		
$\vdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	
$\iota^{m-1} v_m^1$		$\cdots$			$\cdots$					$v_1^{\lambda_1}$

Soit ψ dans le commutant de ψ, dont on rappelle qu'il est de dimension $\sum_i \lambda_i^2$. Notons que ψ laisse stable le drapeau des noyaux itérés de ϕ. Soit A la matrice de ψ dans la base. On pose $(A_1, A_2, \cdots, A_k) \in \prod_i \mathcal{M}_{\lambda_i - \lambda_{i+1}}$, où A_i est le bloc diagonal de A correspondant à $(v_i^{\lambda_{i+1}+1}, \cdots, v_i^{\lambda_i})$.

On vérifie alors sans mal les assertions suivantes :

1. L'application Ξ qui, à un élément ψ du commutant de ϕ associe $(A_1, A_2, \cdots, A_k) \in \prod_i \mathcal{M}_{\lambda_i - \lambda_{i+1}}$ est un morphisme surjectif d'algèbres.
2. Son noyau est donc un idéal de dimension $\sum_i \lambda_i^2 - \sum_i (\lambda_i - \lambda_{i+1})^2 = d(\lambda)$.
3. Le stabilisateur de ι est exactement l'image réciproque de $\prod_i \mathrm{GL}_{\lambda_i - \lambda_{i+1}}$ par Ξ.

□

6. L'indice d'une matrice nilpotente A est le plus petit entier tel que $A^k = 0$.

On obtient alors

Corollaire 4.2.

$$|A_n(q)| = \sum_{\lambda \vdash n} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{n_\lambda}$$

Exemple 4.3. Par exemple, pour $n = 4$. La formule donne bien

$$q^3(q^4-1)(q^3-1)(q^2-1)+q^2(q^4-1)(q^3-1)(q+1)+q(q^4-1)(q^3-1)+(q^4-1)(q^2+q+1)+1 = q^{12}.$$

Il est pourtant assez difficile d'en obtenir la formule pour $|A_n(q)| = q^{n(n-1)}$.

En revanche, si on remarque que

$$|\mathrm{GL}_n(\mathbb{F}_q)| = q^{n^2}(q^{-1};q^{-1})_n,$$

alors on voit que cette formule, *i.e.* le théorème 3.5, est équivalente à

$$\frac{q^{-n}}{(q^{-1};q^{-1})_n} = \sum_{\lambda \vdash n} \frac{q^{-\sum_i \lambda_i^2}}{\prod_i (q^{-1};q^{-1})_{\lambda_i - \lambda_{i+1}}}$$

C'est-à-dire, pour tout z :

$$\frac{z^n}{(z;z)_n} = \sum_{\lambda \vdash n} \frac{z^{\sum_i \lambda_i^2}}{\prod_i (z;z)_{\lambda_i - \lambda_{i+1}}}$$

Exemple 4.4. Pour $n = 2$, on obtient avec les partitions $\lambda = (2)$, et $(1 \geq 1)$

$$\frac{z^2}{(1-z)(1-z^2)} = \frac{z^4}{(1-z)(1-z^2)} + \frac{z^2}{1-z}$$

Cette dernière formule est expliquée dans [FH$^+$58]. Le membre de gauche est la fonction génératrice du nombre de partitions d'un entier N en n parts. La formule reflète alors une correspondance entre partitions à n parts et partitions de n munis d'une famille de carrés de Durfee.

4.2 Approche par la cohomologie d'intersection

Nous avons vu que le cardinal du cône nilpotent était égal à q^d, où d était la dimension du cône. En fait, ce petit « miracle » dans la simplification du calcul est de nature cohomologique. Plus précisément, il provient de la cohomologie d'intersection et de la validité des conjectures de Weil. En une phrase, disons que la cohomologie d'intersection permet de calculer le cardinal du cône nilpotent sur le corps $\mathbb{F}_q$ et que le cône nilpotent possède la même cohomologie qu'un espace vectoriel ; ainsi, son cardinal est celui d'un espace vectoriel.

En voici une explication un peu plus détaillée :

Tout d'abord, Borho et McPherson ont montré dans [BM83] que le cône nilpotent $\mathcal{C}$ était rationnellement lisse. Soit $\mathcal{X} = \mathbb{P}(\mathcal{C}\backslash\{0\})$ le projectivisé du cône. On va déduire, dans un premier temps, que la cohomologie d'intersection de $\mathcal{X}$ est celle de l'espace projectif de dimension $\dim \mathcal{X}$, en suivant [Bri98].

Par une remarque de [BM83], la lissité rationnelle implique que l'homologie relative $H^i(\mathcal{C}, \mathcal{C}\backslash\{0\})$ est nulle pour $i \neq 2d$, avec $H^{2d}(\mathcal{C}, \mathcal{C}\backslash\{0\}) = \mathbb{Q}$. Comme $\mathcal{C}$ est contractile, on obtient par une suite longue en cohomologie relative, que $\mathcal{C}\backslash\{0\}$ est une sphère en cohomologie rationnelle de dimension $2d-1$. Maintenant, soit $S^1 \subset \mathbb{C}^*$ agissant naturellement sur $\mathcal{C}$. Il est clair que $\mathcal{X}$ et $(\mathcal{C}\backslash\{0\})/S^1$ ont la même cohomologie rationnelle. Donc, une suite exacte de Gysin donne $H^0(\mathcal{X}) \simeq H^2(\mathcal{X}) \simeq \cdots H^{2(d-1)}(\mathcal{X}) \simeq \mathbb{Q}$ and $H^{2k+1}(\mathcal{X}) = 0$. Ce qui prouve l'assertion.

On utilise dans la suite les résultats de [KW06, 10.4]. La cohomologie d'intersection l-adique de $\mathcal{X}$ est donc $\mathbb{Q}_l$ en degré pair de 0 à $2(d-1)$, et nulle sinon. Il en résulte que le

nombre de points fixes (avec multiplicité) du Frobenius $X \mapsto X^{q^m}$ sur le cône nilpotent de $\overline{F}_q$ est égal à $\sum_{j=0}^{d-1} \alpha_j^m$, pour des complexes α_j tels que $|\alpha_j| = q^j$. Or, la multiplicité de ces points fixes est toujours 1, puisque la différentielle de $M^{q^m} - M$ en tout point est $-\mathrm{I}_n$. Ainsi, le cardinal $|\mathcal{X}(\mathbb{F}_{q^m})|$ de $\mathcal{X}$ sur $\mathbb{F}_{q^n}$ est égal à $\sum_{j=0}^{d-1} \alpha_j^m$.

D'autre part, on sait, par l'approche « orbitale » que $|\mathcal{X}(\mathbb{F}_{q^m})| = P(q)$, avec $P = \sum_j a_j X^j$ dans l'anneau de polynômes $\mathbb{Z}[X]$. On en déduit que les α_j sont exactement égaux à q^j et donc que $|\mathcal{X}(\mathbb{F}_q| = \sum_{j=0}^{d-1} q^j$, puis que $|\mathcal{C}(\mathbb{F}_q)| = q^d$.

Références

[BGS14] Andries E Brouwer, Rod Gow, and John Sheekey. Counting symmetric nilpotent matrices. *The Electronic Journal of Combinatorics*, 21(2) :P2–4, 2014.

[BM83] Walter Borho and Robert MacPherson. Partial resolutions of nilpotent varieties. *Astérisque*, 101(102) :23–74, 1983.

[Bri98] Michel Brion. Equivariant cohomology and equivariant intersection theory. In *Representation theories and algebraic geometry*, pages 1–37. Springer, 1998.

[CC04] Philippe Caldero and Frédéric Chapoton. Cluster algebras as hall algebras of quiver representations. *arXiv preprint math/0410187*, 2004.

[CG12] Philippe Caldero and Jérôme Germoni. Histoires hédonistes de groupes et de géométries, tome premier, 2012.

[CG14] Philippe Caldero and Jérôme Germoni. Histoires hédonistes de groupes et de géométries, tome second, 2014.

[FH+58] NJ Fine, IN Herstein, et al. The probability that a matrix be nilpotent. *Illinois Journal of Mathematics*, 2(4A) :499–504, 1958.

[Gau13] Karl Friedrich Gauß. *Disquisitiones generales circa seriem infinitam.* Dieterich, 1813.

[KW06] Frances Kirwan and Jonathan Woolf. *An introduction to intersection homology theory.* CRC Press, 2006.