Matrices de carrés nuls

Jean-François Burnol, 18 février 2018

Soit $\mathbb{K}$ un corps fini de caractéristique p et de cardinalité q (qui est une puissance de p). Soit n un entier, on demande de déterminer :

$$A(n,q) = \#\{N \in \mathrm{Mat}_n(\mathbb{K}), N^2 = \mathbf{0}_n\} \tag{1}$$

1 Forme normale (en toute caractéristique, corps quelconque)

Soit dans cette section $\mathbb{K}$ un corps quelconque et $N \in \mathrm{Mat}_n(\mathbb{K})$ telle que $N^2 = \mathbf{0}_n$. On veut montrer

Théorème 1. *Il existe un entier* a *unique, avec* $2a \leqslant n$*, tel que* N *est semblable à la matrice*

$$N_{n,a} = \begin{pmatrix} \mathbf{0}_a & & \mathbf{1}_a \\ & \mathbf{0}_b & \\ & & \mathbf{0}_a \end{pmatrix} \tag{2}$$

où l'on a posé $b = n - 2a$ *(et les entrées laissées délibérement vides sont nulles).*

Notons φ l'endomorphisme de matrice N dans la base canonique de $\mathbb{K}^n$. Bien sûr dans le théorème, $a = \dim \mathrm{Im}(\varphi)$ et $b + a = \dim \mathrm{Ker}(\varphi)$, donc

$$n = b + 2a = \dim \mathrm{Ker}(\varphi) + \dim \mathrm{Im}(\varphi) \tag{3}$$

Ah, connu !

1. On pose $a = \dim \mathrm{Im}(\varphi)$. Montrer qu'il existe $u_1, \dots, u_a$ tels que leurs images par φ sont une base de $\mathrm{Im}\,\varphi$.
2. On pose $v_1 = \varphi(u_1)$, …, $v_a = \varphi(u_a)$. Montrer que u_1, …, u_a, v_1, …, v_a sont linéairement indépendants.
3. Soit V l'espace vectoriel engendré par u_1, …, u_a, v_1, …, v_a. Quelle est la dimension de $V \cap \mathrm{Ker}\,\varphi$?
4. En déduire (avec $b = n - 2a$) qu'il existe une base (u_1, …, u_a, v_1, …, v_a, w_1, …, w_b) de $\mathbb{K}^n$ avec w_1, …, w_b dans le noyau de φ.
5. Conclure la preuve du Théorème 1.

2 Cardinalité des stabilisateurs (corps fini)

On revient à $\mathbb{K}$ fini de cardinalité q et on considère l'action par conjugaison de $GL(n,\mathbb{K})$ sur l'ensemble $\mathcal{A}$ des matrices de $Mat_n(\mathbb{K})$ de carrés nuls, dont on cherche la cardinalité $A(n,q)$. Il y $1+\lfloor\frac{n}{2}\rfloor$ orbites d'après le Théorème 1. La cardinalité de l'orbite de $N_{n,a}$ est

$$\frac{\#GL(n,\mathbb{K})}{\#\{X\in GL(n,\mathbb{K}), XN_{n,a}=N_{n,a}X\}} \tag{4}$$

1. En utilisant une décomposition par blocs avec $A, I \in Mat_a(\mathbb{K})$, $E \in Mat_b(\mathbb{K})$,
$$X=\begin{pmatrix} A & B & C\\ D & E & F\\ G & H & I\end{pmatrix} \tag{5}$$
donner les conditions nécessaires et suffisantes pour que la matrice X soit inversible et commute avec $N_{n,a}$. (on a choisi la forme normale du théorème 1 pour simplifier au maximum la discussion ici)
2. En déduire
$$\#\{X\in GL(n,\mathbb{K}), XN_{n,a}=N_{n,a}X\} = \#GL(a,\mathbb{K})\cdot\#GL(n-2a,\mathbb{K})\cdot q^{a(2n-3a)} \tag{6}$$

3 Conclusion et tabulation numérique

Que vaut $n(n-1)/2-a(2n-3a)-a(a-1)/2-(n-2a)(n-2a-1)/2$? [1] Montrer en conclusion

Théorème 2. *On a (chaque fraction dans la somme étant un entier) :*

$$A(n,q)=\sum_{0\leqslant a\leqslant\frac{n}{2}} q^{a(a-1)/2}\frac{\prod_{a<i\leqslant n}(q^i-1)}{\prod_{1\leqslant k\leqslant n-2a}(q^k-1)} \tag{7}$$

Faites un tableau donnant les $A(n,2)$, pour $1\leqslant n\leqslant 20$.

Comparer avec la spécialisation en $q=2$ de la formule $B(n,q)$ donnant pour $2\nmid q$ le nombre de matrices de carré la matrice identité.

1. cette simplification miraculeuse laisse songeur, avons-nous raté une approche autre aboutissant plus directement au Théorème 2 ?

Voici quelques résultats numériques, à propos, mes calculs des $A(n,2)$ sont confirmés par https://oeis.org/A053722. Ça fait du bien…

Et en ce qui concerne les $B(n,2)$ nous les trouvons à l'adresse https://oeis.org/A132186, et nous apprenons au passage qu'ils comptent le nombre de solutions à l'équation matricielle $A^2 = A$ dans $\mathrm{Mat}_n(\mathbb{K})$, lorsque $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$!

J'ai utilisé la formule suivante pour les $B(n,q)$:

$$B(n,q) = \sum_{0 \leqslant a \leqslant n} q^{a(n-a)} \frac{\prod_{a<i\leqslant n}(q^i - 1)}{\prod_{1\leqslant k \leqslant n-a}(q^k - 1)} \tag{8}$$

Pouvez-vous démontrer le résultat suivant :

Théorème 3. *Pour tout* q *et* n*, la quantité* $B(n,q)$ *compte le nombre de solutions à l'équation* $A^2 = A$ *dans* $\mathrm{Mat}_n(\mathbb{K})$ *(pour* $2 \nmid q$*, c'est la même chose que le nombre de solutions à* $A^2 = \mathbf{1}_n$*). De plus pour* $q = 2$ *c'est aussi exactement le nombre des matrices diagonalisables dans* $\mathrm{Mat}_n(\mathbb{K})$*.*

La dernière colonne indique le quotient A/B.

	A(n,2)	B(n,2)	
1	1	2	(0.500...)
2	4	8	(0.500...)
3	22	58	(0.379...)
4	316	802	(0.394...)
5	6976	20834	(0.334...)
6	373024	1051586	(0.354...)
7	32252032	102233986	(0.315...)
8	6619979776	19614424834	(0.337...)
9	2253838544896	7355623374338	(0.306...)
10	1810098020122624	5494866505497602	(0.329...)
11	2442718932612677632	8087844439442585602	(0.302...)
12	7758088894129169760256	23834930674299549249538	(0.325...)
13	41674675294431186817908736	138978138716920276085366786	(0.299...)
14	526370120583359572695165435904	1626809921636911219317749563394	(0.323...)

A(15,2) B(15,2)	11281778621698661853306239290703872 37757678575184051755732304668884994	 (0.298...)
A(16,2) B(16,2)	568308926792457695112522895542458515456 1761649195978153883884792119981684752386	 (0.322...)
A(17,2) B(17,2)	486605158660299096741260219353231231245352 96 1631473925897894944673413801057885399567564 82	 (0.298...)
A(18,2) B(18,2)	979049827887496059390682197400478677092004161126 4 303936931273542664916223638172346492896184314101 78	 (0.322...)
A(19,2) B(19,2)	3351026232183254583568035236260622522590626609419517952 11245243498285853502702192695088762323107153927694974978	 (0.297...)
A(20,2) B(20,2)	269491956580165683606628554208957453681617091275789285562 7776 837232562694641672632824898956891595257347185982656170426 3682	 (0.321...)

Voici les valeurs suivantes du ratio, pour $n = 21, ..., 40$:

$A(21,2)/B(21,2) = 0.2978620831\dots$
$A(22,2)/B(22,2) = 0.3217651049\dots$
$A(23,2)/B(23,2) = 0.2977956622\dots$
$A(24,2)/B(24,2) = 0.3217055712\dots$
$A(25,2)/B(25,2) = 0.2977624601\dots$
$A(26,2)/B(26,2) = 0.3216758113\dots$
$A(27,2)/B(27,2) = 0.2977458610\dots$
$A(28,2)/B(28,2) = 0.3216609330\dots$
$A(29,2)/B(29,2) = 0.2977375620\dots$
$A(30,2)/B(30,2) = 0.3216534943\dots$
$A(31,2)/B(31,2) = 0.2977334127\dots$
$A(32,2)/B(32,2) = 0.3216497751\dots$
$A(33,2)/B(33,2) = 0.2977313380\dots$
$A(34,2)/B(34,2) = 0.3216479155\dots$
$A(35,2)/B(35,2) = 0.2977303007\dots$
$A(36,2)/B(36,2) = 0.3216469857\dots$
$A(37,2)/B(37,2) = 0.2977297820\dots$
$A(38,2)/B(38,2) = 0.3216465208\dots$
$A(39,2)/B(39,2) = 0.2977295227\dots$
$A(40,2)/B(40,2) = 0.3216462884\dots$

On a l'impression qu'il y a deux limites l'une pour les n pairs, l'autre pour les impairs, mais c'est peut-être trompeur, encore que comme ça semble y aller en décroissant on ne soupçonne pas une oscillation, néanmoins ça pourrait tendre vers zéro doucement !

(je ne connais pas la réponse ; je ne l'ai pas cherchée, mais ce n'est pas une excuse...)