Corrigé du devoir n°6 (puissances de matrices)

1 Les définitions générales se traduisent dans l'anneau $(\mathcal{M}_n(\mathbf{R}),+,\times)$ par : M est unipotente si il existe un entier $k>0$ tel que $M^k=\underbrace{M\times M\times\cdots\times M}_{k\text{ fois}}=I_n$ (la matrice unité de $\mathcal{M}_n(\mathbf{R})$ définie par $I_n=(\delta_{ij})_{1\leq i,j\leq n}$; où δ_{ij} est le symbole de Kronecker); M est nilpotente si il existe un entier $k>0$ tel que $M^k=O_n$ (la matrice nulle, c'est-à-dire celle dont tous les termes sont nuls).

2 Si x est unipotent, on a $x^k=x\star(x^{k-1})=(x^{k-1})\star x=1_A$ (avec $k\geq 1$); la définition des éléments inversibles (a est inversible $\iff\exists b\in A$, $a\star b=b\star a=1_A$) montre donc que x est inversible et que $x^{-1}=x^{k-1}$. Supposons que x soit nilpotent et inversible, on aura $(x^{-1})^k\star x^k=(x^{-1}\star x)^k=1_A$ (puisque x et x^{-1} commutent) et comme $x^k=0_A$, on aurait donc $1_A=0_A$ ce qui est absurde (sauf si l'anneau n'a qu'un élément !); aucun élément nilpotent n'est donc inversible.

3 Calculons par récurrence $(y\star x\star y^{-1})^n$: supposons (hypothèse de récurrence) que l'on ait $(y\star x\star y^{-1})^k=y\star x^k\star y^{-1}$, on aura alors

$$\begin{aligned}(y\star x\star y^{-1})^{k+1}&=(y\star x\star y^{-1})^k\star(y\star x\star y^{-1})\\&=y\star x^k\star y^{-1}\star y\star x\star y^{-1}=y\star x^{k+1}\star y^{-1}\,.\end{aligned}$$

La formule étant évidemment vraie pour $k=1$, elle est vraie par récurrence pour tout n. Supposons alors que x soit unipotent, et que $x^k=1_A$; on aura donc $(y\star x\star y^{-1})^k=y\star 1_A\star y^{-1}=1_A$, et $y\star x\star y^{-1}$ sera donc également unipotent; de même, si $x^k=0_A$, on aura $(y\star x\star y^{-1})^k=y\star 0_A\star y^{-1}=0_A$.

4 Soit $A=\begin{pmatrix}a&b\\0&d\end{pmatrix}$ une matrice triangulaire supérieure 2×2, on sait (et on le vérifie aisément par récurrence) que $A^n=\begin{pmatrix}a^n&b_n\\0&d^n\end{pmatrix}$ (b_n peut aussi être obtenu par récurrence, mais la formule compliquée correspondante n'est pas nécessaire pour la suite du problème). Si alors A est nilpotente, cela veut dire qu'il existe un k pour lequel $a^k=d^k=b_k=0$; on a donc $a=d=0$, et comme réciproquement on a alors $A^2=O$, on voit qu'on a donc trouvé toutes les matrices nilpotentes de la forme cherchée (le cas général passerait par la théorie de la diagonalisation), que l'on se place dans $\mathbf{R}$ ou dans $\mathbf{C}$. Si on veut $A^k=I$, on voit qu'on doit avoir $a^k=d^k=1$, et donc (dans $\mathbf{R}$) $a=\pm1$ et $d=\pm1$. Prenant au besoin $-A$ (et remarquant que $A^k=I\Rightarrow(-A)^{2k}=I$), on voit qu'on peut supposer $a=1$. Si alors $d=1$, on a $A=I+B$, avec $B^2=O$, et d'après la formule du binôme $(I+B)^n=I+nB\neq I$ si $B\neq O$. I et $-I$ sont donc les seules matrices unipotentes pour lesquelles $a=d$. Si par contre on prend $a=1$ et $d=-1$, on vérifie aisément que $A^2=I$ pour toute valeur de b; les matrices $\pm\begin{pmatrix}1&b\\0&-1\end{pmatrix}$ sont donc toutes unipotentes. Ces calculs ne sont plus valables dans $\mathbf{C}$, puisqu'on pourrait alors avoir $a=e^{2i\pi/n}$ par exemple; il est alors plus facile d'utiliser la théorie de la diagonalisation, et le résultat final est que les matrices unipotentes (de la forme demandée) sont du type $e^{2i\pi/n}I$, d'une part, et du type $\begin{pmatrix}e^{2i\pi/p}&b\\0&e^{2i\pi/q}\end{pmatrix}$, d'autre part.

5 Si $X^2=I_n$, on a $(X+aI_n)^2=2aX+(a^2+1)I_n$; ainsi, si $Y=X+I_n$, on aura $Y^2=2Y$. Réciproquement, si $Y^2=2Y$, posant $X=Y-I$, on aura $(X+I)^2=X^2+2X+I=2X+2I$, donc $X^2=I$.

6 La formule demandée peut s'obtenir par récurrence, mais il est plus simple de remarquer que A commute avec I, et qu'on peut donc appliquer la formule de Newton; comme $A^k = O$ pour tout $k \geq 3$, elle devient ici $(I+A)^n = I + nA + \frac{n(n-1)}{2}A^2$.

7 A et I commutant, on peut appliquer l'identité des suites géométriques : $(I + A + A^2 + \cdots + A^n)(I - A) = I - A^{n+1}$. Prenant $n = k-1$, où k est le plus petit entier tel que $A^k = O$, on voit que $(I + A + \cdots + A^{k-1})(I - A) = I$, ce qui montre que $I - A$ est inversible. La matrice $B = -A$ étant également nilpotente, on aura de même $I - B = I + A$ inversible (et $(I+A)^{-1} = I - A + A^2 - \cdots + (-1)^{k-1}A^{k-1}$). Un calcul analogue aboutissant, si A est unipotente, à $(I+A+\cdots+A^{k-1})(I-A) = O$, on pourrait penser que $I-A$ n'est pas inversible, mais en fait, cela montre seulement qu'alors $(I+A+\cdots+A^{k-1})$ est nulle, ce qui peut se produire : prendre par exemple $A = -I$!

8 Supposons que A et B commutent; on sait qu'on peut alors appliquer la formule du binôme $(A+B)^n = \sum_{k=0}^{n} C_n^k A^k B^{n-k}$. Si on a $A^p = O$ et $B^q = O$, prenons alors $n = p + q$, et décomposons la sommation précédente en $\sum_{k=0}^{p} C_n^k A^k B^{q+(p-k)} + \sum_{k=p+1}^{n} C_n^k A^k B^{n-k}$. Il est clair que toutes les puissances de B sont nulles dans la première somme, et que toutes les puissances de A sont nulles dans la seconde; on aura donc $(A+B)^{p+q} = O$, et $A+B$ sera bien nilpotente. Ce résultat n'est plus valable si A et B ne commutent pas : ainsi, prenant $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, on a $A^2 = B^2 = O$, mais $C = A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ vérifie $C^2 = I$, et donc C^n, qui vaut C ou I (suivant la parité de n), n'est jamais nulle.

9 On peut en fait sans inconvénient poser $\exp(A) = \sum_{k=0}^{n} \frac{A^k}{k!}$, en prenant n supérieur au premier k pour lequel $A^k = 0$. Comme on a supposé que A et B commutent (ce qui est de toute façon nécessaire pour que $\exp(A+B)$ ait un sens, comme on l'a vu plus haut), on peut d'une part appliquer la formule du binôme aux $(A+B)^k$, d'autre part effectuer le produit $\exp(A)\exp(B)$ (par distributivité) sans prendre de précautions (d'ailleurs inutiles dans ce cas). On aboutit d'une part à

$$\exp(A)\exp(B) = \left(\sum_{j=0}^{n} \frac{A^j}{j!}\right)\left(\sum_{k=0}^{n} \frac{B^k}{k!}\right) = \sum_{0 \leq j,k \leq n} \frac{A^j B^k}{j!k!}$$

(en prenant n assez grand comme plus haut) et d'autre part à

$$\exp(A+B) = \sum_{k=0}^{n} \frac{(A+B)^k}{k!} = \sum_{k=0}^{n} \frac{\sum_{j=0}^{k} C_k^j A^j B^{k-j}}{k!}$$

Cherchons alors dans la seconde expression les termes correspondant à un monôme $A^p B^q$ donné : il est clair que le seul terme convenable se trouve dans le développement de $(A+B)^{p+q}$, et vaut $C_{p+q}^p A^p B^q/(p+q)!$; mais comme $C_{p+q}^p/(p+q)! = 1/p!q!$, on en déduit que ce terme est identique à celui correspondant à la première expression, et donc que $\exp(A+B) = \exp(A)\exp(B)$. O étant nilpotente, on a

$\exp(O) = I$; la formule précedente montre donc que $\exp(A)\exp(-A) = \exp(O) = I$, ce qui prouve que $\exp(A)$ est inversible, et que $(\exp(A))^{-1} = \exp(-A)$.

10 Les résultats des questions **5, 6** et **7** sont valables dans un anneau quelconque (au prix d'un changement de notation : ainsi, par exemple, si $a^k = 0_A$, $1_A - a$ est inversible, et $(1_A - a)^{-1} = 1 + a + a^2 + \cdots + a^{k-1}$) ; mais on ne peut (dans le cas général) définir l'exponentielle d'un élément nilpotent, car, même en convenant que les entiers sont «plongés» dans l'anneau, et en identifiant 3 avec $3_A = 1_A + 1_A + 1_A$, la notation $x/k!$ ne signifie rien (par exemple, dans $\mathbf{Z}$, $n/5!$ n'est défini que si n est un multiple de 120).