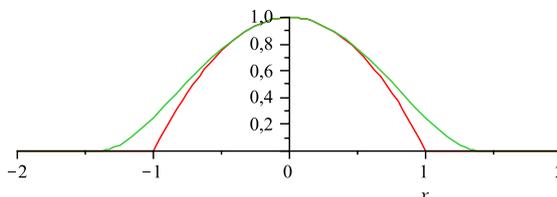


## e3a PSI B un corrigé.

### Exercice 1.

1.  $x \mapsto e^{-x^2}$  est continue sur  $\mathbb{R}$  et on a un unique problème d'existence pour l'intégrale aux voisinages de l'infini. Or, la fonction est (par croissances comparées) dominée par  $1/x^2$  en ces voisinages. Elle est finalement intégrable sur  $\mathbb{R}$  et l'intégrale existe a fortiori.

2.1.



- 2.2. Soit  $x \in \mathbb{R}$ . Pour  $n > |x|$ , on a  $f_n(x) = \exp(n \ln(1 - x^2/n))$ . Le terme dans l'exponentielle tend vers  $-x^2$  quand  $n \rightarrow +\infty$  et, par continuité de l'exponentielle,  $f_n(x) \rightarrow e^{-x^2}$ .  $(f_n)$  converge donc simplement sur  $\mathbb{R}$  vers  $x \mapsto e^{-x^2}$ .
- 2.3. Par concavité du logarithme,  $\forall v > -1$ ,  $\ln(1+v) \leq v$  (courbe de  $x \mapsto \ln(1+x)$  sous sa tangente au point d'abscisse 0). Ainsi, si  $u > n$ ,  $\ln(1+u/n) \leq u/n$ . On ne change pas le sens de l'inégalité en multipliant par  $n$ . Par croissance de l'exponentielle, on a alors  $(1 + \frac{u}{n})^n \leq e^u$ .
- 2.4.  $f_n$  est continue sur  $\mathbb{R}$  et on a donc un unique problème d'existence de l'intégrale au voisinage de  $+\infty$ . Or,  $f_n$  est nulle sur ces voisinages et donc intégrable sur ces voisinages.  $f_n$  est donc intégrable sur  $\mathbb{R}$ .
- 2.5. On veut utiliser le théorème de convergence dominée.
- Les  $f_n$  sont continues sur  $\mathbb{R}$  et  $(f_n)$  converge simplement sur  $\mathbb{R}$  vers  $x \mapsto e^{-x^2}$  elle-même continue sur  $\mathbb{R}$ .
  - $\forall n, \forall x \in ]-\sqrt{n}, \sqrt{n}[$ ,  $0 \leq f_n(x) \leq e^{-x^2}$  (question 2.3 avec  $u = -x^2 > -n$ ). L'encadrement reste vrai pour les autres  $x$  ( $0 \leq e^{-x^2}$ ). On a donc  $|f_n(x)| \leq e^{-x^2}$  et le majorant est intégrable sur  $\mathbb{R}$ .

Le théorème s'applique et indique que

$$\lim_{n \rightarrow +\infty} \int_{\mathbb{R}} f_n(x) dx = \int_{\mathbb{R}} e^{-x^2} dx$$

- 3.1.  $J_0$  et  $J_1$  se calculent immédiatement et  $\cos^2(t) = \frac{1}{2}(\cos(2t) + 1)$  permet le calcul de  $J_2$ . On obtient

$$J_0 = \frac{\pi}{2}, \quad J_1 = 1, \quad J_2 = \frac{\pi}{4}$$

**3.2.** Une intégration par parties donne (en primitivant  $\cos$  et en dérivant  $\cos^{k+1}$ )

$$J_{k+2} = \left[ \sin(t) \cos(t)^{k+1} \right]_0^{\pi/2} + (k+1) \int_0^{\pi/2} \sin(t)^2 \cos(t)^k dt$$

Le terme tout intégré est nul. Avec  $\sin^2 = 1 - \cos^2$ , on a alors

$$J_{k+2} = (k+1)(J_k - J_{k+2})$$

**3.3.** On en déduit que

$$\forall k \geq 1, J_{2k+1} = \frac{2k}{2k+1} J_{2k-1}$$

On prouve alors par récurrence que

$$J_{2n+1} = \prod_{k=1}^n \frac{2k}{2k+1}$$

est vraie pour tout  $n$ .

- Initialisation :  $J_1 = 1$  et le résultat est vrai au rang 0 avec la convention  $\prod_{k=i}^j v_k = 1$  si  $i > j$ .  
 $J_3 = \frac{2}{3} J_1 = \frac{2}{3}$  et le résultat est vrai au rang 1.

- Hérédité : soit  $n \geq 2$  tel que le résultat est vrai jusqu'au rang  $n-1$ . Le résultat au rang  $n-1$  et la relation entre  $J_{2n+1}$  et  $J_{2n-1}$  donnent le résultat au rang  $n$ .

**3.4.** On multiplie haut et bas par  $2.4.\dots(2n)$  pour obtenir

$$J_{2n+1} = \frac{(2.4.\dots(2n))^2}{(2n+1)!}$$

Le numérateur est le carré de  $2^n(n!)^2$  (après factorisation de chaque terme pr 2). Ainsi

$$J_{2n+1} = \frac{2^{2n}(n!)^2}{(2n+1)!}$$

*On pourrait vérifier cette relation par récurrence.*

**3.5.** La formule de Stirling stipule que

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

On en déduit que

$$J_n \sim \frac{2^{2n}(2\pi n)n^{2n}/e^{2n}}{\sqrt{2\pi(2n+1)}(2n+1)^{2n+1}/e^{2n+1}} = \left(\frac{2n}{2n+1}\right)^{2n} \frac{e\sqrt{2\pi n}}{(2n+1)^{3/2}}$$

$\left(\frac{2n}{2n+1}\right)^{2n} = \exp(-2n \ln(1 + \frac{1}{2n})) \rightarrow e^{-1}$  donne alors

$$J_{2n+1} \sim \frac{\sqrt{\pi}}{2\sqrt{n}}$$

**4.**  $x \mapsto \arcsin(x/\sqrt{n})$  est un  $C^1$  difféomorphisme de  $] -\sqrt{n}, \sqrt{n}[$  dans  $] -\pi/2, \pi/2[$ . On peut donc poser  $t = \arcsin(x/\sqrt{n})$  pour obtenir

$$\int_{-\sqrt{n}}^{\sqrt{n}} (1 - x^2/n)^n dx = \sqrt{n} \int_{-\pi/2}^{\pi/2} \cos(t)^{2n+1} dt$$

$f_n$  est nulle hors de  $[-\sqrt{n}, \sqrt{n}]$  et  $t \mapsto \cos(t)^{2n+1}$  est paire. On a donc aussi

$$u_n = 2\sqrt{n}J_{2n+1}$$

**5.** Il reste à passer à la limite pour obtenir

$$\int_{\mathbb{R}} e^{-x^2} dx = \sqrt{\pi}$$

## Exercice 2.

- On a  ${}^tBB = 3$  et  $u$  est donc un automorphisme orthogonal (représenté par une matrice orthogonale en base orthonormée). De plus  $\det(B) = 1$  et  $u$  est direct. C'est donc une rotation axiale. Comme  $(1, 0, 1)$  est laissé fixe, il dirige l'axe de la rotation. La trace étant un invariant de similitude, l'angle  $\theta$  de la rotation vérifie  $-1 = \text{Tr}(B) = 1 + 2 \cos(\theta)$ . Cet angle est donc égal à  $\pi$  ( $\cos(\theta) = -1$ , il n'y a ici pas ambiguïté de signe et il n'est pas nécessaire d'orienter l'axe).  $u$  est le demi-tour d'axe  $\text{Vect}((1, 0, 1))$ .
- Effectuons une étude de la fonction polynomiale  $P$ .  $P'(X) = 3X^2 + 2X = X(3X + 2)$  et on a donc le tableau de variations suivant

		-2/3	0	
$P'$	+	0	- 0 +	
$P$	-∞	↗	$d + 4/27$	↘
			$d$	↗ +∞

Si  $d > 0$  ou  $d < -4/27$ ,  $P$  admet une unique racine réelle de multiplicité 1.

Si  $d \in ]-4/27, 0[$ ,  $P$  admet trois racines réelles distinctes.

Si  $d = 0$  alors 0 est racine double de  $P$  et  $-1$  est racine simple de  $P$ .

Si  $d = -4/27$  alors  $-2/3$  est racine double de  $P$  et  $1/3$  est racine simple de  $P$ .

Finalement  $P$  est scindé sur  $\mathbb{R}$  si et seulement si  $d \in [-4/27, 0]$ .

- $Q = (X - \alpha)(X - \beta)(X - \gamma)$  ( $Q$  est unitaire). En développant, on obtient les relations entre coefficients et racines :

$$a = -\alpha - \beta - \gamma, \quad b = \alpha\beta + \alpha\gamma + \beta\gamma, \quad c = -\alpha\beta\gamma$$

- Pour la suite, on remarque que

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = a^2 - 2b$$

Raisonnons par analyse et synthèse.

- Supposons que  $A \in O_3^+(\mathbb{R})$ . Les colonnes de  $A$  sont normées et deux à deux orthogonales.

Ainsi

$$\alpha^2 + \beta^2 + \gamma^2 = 1, \quad \alpha\beta + \alpha\gamma + \beta\gamma = 0$$

et avec la remarque faite, on a  $a^2 - 2b = 1$  et  $b = 0$ . Ainsi,  $a = \pm 1$  et  $b = 0$ . Par ailleurs,

$$1 = \det(A) = -(\alpha + \beta + \gamma)(\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta - \alpha\gamma - \beta\gamma) = a$$

A ce niveau,  $Q = X^3 + X^2 + c$  et on sait que les racines de  $Q$  sont réelles ce qui donne  $c \in [-4/27, 0]$ .

- Réciproquement, si  $c \in [-4/27, 0]$ ,  $b = 0$  et  $a = 1$ , on a bien  $\alpha, \beta, \gamma$  réels et, avec les calculs des conditions nécessaires, les colonnes de  $A$  forment une b.o.n. directe de  $\mathbb{R}^3$ .  $A$  est donc orthogonale directe et  $u$  est une rotation.

La condition nécessaire et suffisante pour que  $u$  soit une rotation est

$$a = 1, \quad b = 0, \quad c \in [-4/27, 0]$$

## Exercice 3.

- $u$  et  $v$  sont à termes strictement positifs et  $v_n = \ln(1 + 1/n) \sim 1/n = u_n$ . Comme  $\sum(u_n)$  diverge, on peut utiliser  $(R)$  pour obtenir (la somme se simplifiant par télescopage)

$$H_n \sim \sum_{k=1}^n v_k = \ln(n + 1)$$

Enfin,  $\ln(n+1) = \ln(n) + \ln(1+1/n) \sim \ln(n)$  permet de conclure que

$$H_n \sim \ln(n)$$

- 2.1.** On pose cette fois  $u_n = \frac{1}{n \ln(n)}$  et  $v_n = \ln(\ln(n+1)) - \ln(\ln(n))$  (définies pour  $n \geq 2$ ). On a des suites à termes strictement positifs. De plus, par télescopage,

$$\sum_{k=2}^n v_k = \ln(\ln(n+1)) - \ln(\ln(2)) \rightarrow +\infty$$

ce qui montre que  $\sum(v_k)$  diverge. Enfin,

$$v_n = \ln\left(\frac{\ln(n) + \ln(1+1/n)}{\ln(n)}\right) = \ln\left(1 + \frac{\ln(1+1/n)}{\ln(n)}\right) \sim \frac{\ln(1+1/n)}{\ln(n)} \sim \frac{1}{n \ln(n)} = u_n$$

On peut donc encore utiliser (R) pour conclure que

$$\sum_{k=2}^n \frac{1}{k \ln(k)} \sim \ln(\ln(n+1)) - \ln(\ln(2)) \sim \ln(\ln(n+1))$$

Bien sûr, le fait que les séries soient définies à partir du rang 2 seulement ne change rien au fait que l'on peut utiliser (R).

Comme  $\ln(\ln(n+1)) = \ln(\ln(n) + \ln(1+1/n)) = \ln(\ln(n)) + \ln(1 + \frac{\ln(1+1/n)}{\ln(n)}) \sim \ln(\ln(n))$  on conclut que

$$\sum_{k=2}^n \frac{1}{k \ln(k)} \underset{+\infty}{\sim} \ln(\ln(n))$$

- 2.2.** En particulier, la suite des sommes partielles de la série  $\sum(w_n)$  est de limite infinie et la série diverge.
- 2.3.** De façon alternative, on peut considérer la fonction  $f : x \mapsto \frac{1}{x \ln(x)}$ .  $f$  est décroissante sur  $[2, +\infty[$  et on peut donc utiliser une comparaison série-intégrale pour montrer que

$$\forall n \geq 2, \sum_{k=2}^n \frac{1}{k \ln(k)} \geq \int_2^{n+1} \frac{dx}{x \ln(x)} = \ln(\ln(n+1)) - \ln(\ln(2)) \rightarrow +\infty$$

On retrouve que la suite des sommes partielles de la série  $\sum(w_n)$  est de limite infinie et donc la série diverge.

La méthode pourrait d'ailleurs donner, en écrivant un encadrement, l'équivalent de **2.1**.

- 3.1.** Les trois premiers points de (P) sont immédiats et le quatrième aussi (on a une série géométrique de raison 1 qui diverge). Ici,  $A_n = n$  et

$$b_n = \frac{1}{\ln(n)} \sum_{k=1}^n \frac{1}{k} = \frac{H_n}{\ln(n)}$$

La question 1 indique que

$$\lim_{n \rightarrow +\infty} b_n = 1$$

- 3.2.** Les quatre points de la propriété (P) sont immédiats (la suite est à valeurs dans  $]0, 1]$  et la série associée, de Riemann, est divergente). On a  $A_k = H_k$  et donc

$$b_n = \frac{1}{\ln(H_n)} \sum_{k=1}^n \frac{1}{k H_k}$$

Posons  $u_n = \frac{1}{nH_n}$ ;  $u$  et  $w$  (définies à partir du rang 2) sont strictement positives à partir du rang 3. Ce sont des suites équivalentes (question 1) de séries divergente (question 2.2). La propriété (R) indique que

$$\sum_{k=3}^n \frac{1}{kH_k} \sim \sum_{k=3}^n \frac{1}{k \ln(k)}$$

Ajouter les termes d'indices 1 et 2 ne change rien à l'équivalence car les sommes sont de limites infinies (les constantes sont alors négligeables) et avec la question 2.1 on a

$$\sum_{k=1}^n \frac{1}{kH_k} \sim \ln(\ln(n))$$

Enfin,  $\ln(H_n) = \ln(\ln(n)) + \ln\left(\frac{\ln(n)}{H_n}\right) \sim \ln(\ln(n))$  (le second terme, de limite nulle, est négligeable devant le premier, de limite infinie). On a finalement

$$\lim_{n \rightarrow +\infty} b_n = 1$$

- 4.1. On a  $A_n = A_{n-1} + a_n$ . Par ailleurs  $A_n \rightarrow +\infty$  (suite croissante car  $(a_n)$  est à termes positives, et non convergente car  $\sum(a_n)$  diverge) et  $(a_n)$  est bornée donc  $a_n = o(A_n)$ . Ainsi,  $A_n = A_{n-1} + o(A_n)$  et donc

$$A_n \sim A_{n-1}$$

- 4.2. On en déduit que  $\frac{A_n}{A_{n-1}} \rightarrow 1$  et donc  $\ln\left(\frac{A_n}{A_{n-1}}\right) \sim \frac{A_n}{A_{n-1}} - 1 = \frac{a_n}{A_{n-1}}$ . Enfin,  $A_{n-1} \sim A_n$  donne

$$\ln\left(\frac{A_n}{A_{n-1}}\right) \underset{+\infty}{\sim} \frac{a_n}{A_n}$$

- 4.3.  $u_n = \ln\left(\frac{A_n}{A_{n-1}}\right)$  est le terme général ( $n \geq 2$ ) d'une suite strictement positive de série divergente ( $\sum_{k=2}^n u_k = \ln(A_n) - \ln(A_1) = \ln(A_n) \rightarrow +\infty$ ). Comme  $u_n \sim \frac{a_n}{A_n}$  qui est aussi à termes  $> 0$ , on peut utiliser (R) pour obtenir

$$\sum_{k=2}^n \ln\left(\frac{A_k}{A_{k-1}}\right) \sim \sum_{k=2}^n \frac{a_k}{A_k}$$

Ces suites sont de limite infinie et ainsi  $\sum(a_k/A_k)$  diverge.

- 4.4. L'équivalence obtenue ci-dessus s'écrit

$$\sum_{k=2}^n \frac{a_k}{A_k} \sim \ln(A_n)$$

Ajouter le terme pour  $k = 1$  ne change rien car les termes tendent vers  $+\infty$ . Ainsi

$$\lim_{n \rightarrow +\infty} b_n = 1$$

5. On va essayer d'utiliser le résultat précédent pour construire  $(v_n)$ . Pour cela, il nous faut une suite vérifiant (P) et je distingue donc deux cas.
- Si  $(u_n)$  est bornée, je pose  $a_1 = 1$  et  $\forall n \geq 1$ ,  $a_n = u_n$ . On a alors  $(a_n)$  qui vérifie (P)  $\cdot \sum(a_n/A_n)$  diverge (question 4.3) et  $\frac{a_n}{A_n} = o(a_n)$  (le quotient vaut  $1/A_n$  et tend vers 0). La suite de terme général  $v_n = \frac{a_n}{A_n}$  convient donc.
  - Sinon, je pose  $w_n = \min(u_n, 1)$ ; on a  $w_n > 0$  et  $\sum(w_n)$  diverge (car  $u_n$  est régulièrement plus grand que 1 et il existe une extraite de  $w$  qui est constante égale à 1 ce qui donne la divergence grossière de la série). Le premier cas donne une suite  $v_n = o(u_n)$  à termes  $> 0$  et de série divergente. On a a fortiori  $v_n = o(u_n)$  (puisque  $0 \leq w_n \leq u_n$ ).
6. Si  $x \in [0, 1[$ ,  $(a_n x^n)$  est de limite nulle (car  $(a_n)$  est bornée). Le rayon cherché est donc  $\geq 1$ . Comme  $\sum(a_n)$  diverge, le rayon de convergence est  $\leq 1$ . Le rayon de convergence est donc égal à 1. On n'utilise pas ce qui précède pour conclure simplement.

## Exercice 4.

1. Si  $A$  est nilpotente alors il existe un entier  $k \geq 1$  tel que  $X^k$  annule  $A$ . Or, les valeurs propres d'une matrice sont racines de tout polynôme annulateur. Ainsin 0 est la seule valeur propre possible de  $A$ . Comme  $0 = \det(A^k) = \det(A)^k$ ,  $A$  n'est pas inversible et 0 est bien valeur propre. Finalement  $\{0\}$  est le spectre d'une matrice nilpotente.
2. Une matrice dont le spectre est réduit à une valeur  $\lambda$  n'est diagonalisable que si elle est scalaire (puisque  $X - \lambda$  annule cette matrice, elle vaut  $\lambda I_n$ ). Ainsi,  $O_n$  est la seule matrice nilpotente diagonalisable.
- 3.1.  $\chi_A = X^2 - \text{Tr}(A)X + \det(A)$  annule  $A$  (théorème de Cayley-Hamilton). On peut donc choisir

$$\alpha = \text{Tr}(A) \quad \text{et} \quad \beta = -\det(A)$$

- 3.2. Si  $A$  est nilpotente alors 0 est sa seule valeur propre. Comme est trigonalisable (le corps de base étant  $\mathbb{C}$ )  $A$  est semblable à une matrice de diagonale nulle. Il en est alors de même de  $A^2$  ( $P^{-1}A^2P = (P^{-1}AP)^2$ ). Les traces de  $A$  et  $A^2$  sont donc nulles. Réciproquement, si  $A$  et  $A^2$  sont de trace nulle alors  $A^2 = \det(A)I_2$  (3.1) donne  $\det(A) = 0$  en passant à la trace. Ainsi, le polynôme annulateur de  $A$  trouvé en question précédente est  $X^2$ .  $A^2 = 0$  et  $A$  est nilpotente.
- 4.1.  $E$  est un sous-espace de  $\mathcal{M}_n(\mathbb{C})$  qui est de dimension finie (égale à  $n^2$ ). Ainsi,  $E$  est de dimension finie.
- 4.2. Le théorème de la base incomplète indique que l'on peut compléter une famille libre d'un espace vectoriel avec des éléments d'une famille génératrice de cet espace pour obtenir une base. On part de la famille libre  $(M_1)$  ( $M_1$  est non nulle car inversible) et on peut la compléter avec des éléments de  $G$  pour obtenir une base de  $E$  composée avec des éléments de  $G$ .  $r$  est le cardinal de cette famille, c'est à dire la dimension de  $E$ .
- 5.1.  $\text{card}(U_p) = p$  et  $U_p = \{e^{\frac{2ik\pi}{p}} / k \in \{0, \dots, p-1\}\}$ .
- 5.2. Soit  $X \in G$ . Par hypothèse,  $X^p = I_n$ . Si  $\lambda$  est valeur propre de  $X$  alors il existe un vecteur non nul tel que  $XE = \lambda E$ . Une récurrence immédiate donne  $X^k E = \lambda^k E$ . Ainsi  $(\lambda^p - 1)E = 0$  et comme  $E$  n'est pas le vecteur nul (c'est un vecteur propre), on a  $\lambda^p = 1$ .
6. Soit  $M \in G$ .  $X^p - 1$  est un polynôme annulateur de  $M$ . Comme il est scindé à racines simples (dans  $\mathbb{C}$ ),  $M$  est diagonalisable.
7. Soit  $X \in G$ ;  $X$  est semblable à une matrice diagonale dont les éléments diagonaux sont des éléments de  $U_p$ . La trace de  $X$  est donc la somme de  $n$  éléments de  $U_p$  (éventuellement répétés). Il y a au plus  $p^n$  diagonales possibles ( $p$  choix pour chaque élément) et donc au plus  $p^n$  éléments dans  $\mathcal{S}$  (certainement moins car deux diagonales différentes peuvent avoir même somme).
- 8.1.  $G$  étant un groupe est stable par multiplication et passage à l'inverse. Ainsi  $AB^{-1}$  est dans  $G$ . En particulier, c'est une matrice diagonalisable et il existe une matrice inversible  $P$  telle que  $D = PAB^{-1}P$  est diagonale. On a alors  $PNP = D - I_n$  qui est aussi diagonale et  $N$  est donc diagonalisable.
- 8.2.  $\varphi(A)$  et  $\varphi(B)$  sont deux  $p$ -uplets égaux et leurs coordonnées sont donc égales. Ceci donne

$$\forall i \in \{1, \dots, r\}, \quad \text{Tr}(AM_i) = \text{Tr}(BM_i)$$

La forme linéaire  $X \mapsto \text{Tr}(AX) - \text{Tr}(BX)$  est donc nulle sur une base de  $E$ . Par linéarité, elle l'est sur  $E$  et

$$\forall X \in E, \quad \text{Tr}(AX) = \text{Tr}(BX)$$

- 8.3. Montrons par récurrence que la propriété

$$\text{Tr}((AB^{-1})^k) = n$$

est vraie pour tout entier  $k$ .

- Initialisation :  $(AB^{-1})^0 = I_n$  est de trace  $n$  ce qui prouve le résultat pour  $k = 0$ .
- Hérédité : soit  $k \geq 0$  tel que le résultat soit vrai jusqu'au rang  $k$ . On a alors  $(AB^{-1})^{k+1} = AB^{-1}(AB^{-1})^k$ . Avec la question précédente utilisée avec  $X = B^{-1}(AB^{-1})^k$  (qui est dans  $G$  comme produit d'éléments de  $G$ ) on a

$$\text{Tr}(AB^{-1})^{k+1} = \text{Tr}(BB^{-1}(AB^{-1})^k) = \text{Tr}(AB^{-1})^k$$

et on conclut directement avec le résultat au rang  $k$ .

**8.4.**  $(AB)^{-1}$  et  $I_n$  commutant, on a

$$\forall k \in \{1, \dots, n\}, N^k = \sum_{i=0}^k \binom{k}{i} (-1)^{k-i} (AB^{-1})^i$$

La trace étant linéaire, on a donc (avec la question précédente)

$$\forall k \in \{1, \dots, n\}, \text{Tr}(N^k) = \sum_{i=0}^k \binom{k}{i} (-1)^{k-i} \text{Tr}(AB^{-1})^i = n \sum_{i=0}^k \binom{k}{i} (-1)^{k-i} = n(1-1)^k = 0$$

Avec le résultat admis par l'énoncé,  $N$  est nilpotente. Etant diagonalisable, elle est nulle (question **2.**).

- 8.5.** On a donc  $AB^{-1} = I_n$  et donc  $A = B$  ce qui montre que  $\varphi$  est injective (deux éléments qui ont la même image sont égaux).
- 9.** Si  $X \in G$  alors pour tout  $i$ ,  $XM_i \in G$  (car  $G$  est un groupe). Ainsi  $\text{Tr}(XM_i) \in \mathcal{S}$  et  $\varphi(X) \in \mathcal{S}^r$ . On a montré que  $\varphi(G) \subset \mathcal{S}^r$ .
- 10.**  $\varphi$  est injective et son image est finie. On peut conclure que  $G$  est un groupe fini.