Devoir de Mathématiques n°17

Kévin Polisano
MPSI 1

Vendredi 11 Avril 2008

Exercice

Partie II

1. a) Soit π un élément d'un groupe multiplicatif G, e un entier relatif et $\alpha = \pi^e$.

On considère l'application :

$$\begin{array}{rccc} f_\alpha : & \mathbb{Z}\times G & \longrightarrow & G^2 \\ & (k,\tau) & \mapsto & (\pi^k, \tau\alpha^k) \end{array}$$

On cherche à exhiber une fonction φ_e de G^2 dans G ne dépendant que de e et vérifiant :

$$\forall (k,\tau)\in\mathbb{Z}\times G,\ \tau = \varphi_e \circ f_\alpha(k,\tau)$$

L'application suivante convient :

$$\boxed{\begin{array}{rccc} \varphi_e : & G^2 & \longrightarrow & G \\ & (a,b) & \mapsto & ba^{-e} \end{array}}$$

En effet :

$$\forall (k,\tau)\in\mathbb{Z}\times G,\ \varphi_e \circ f_\alpha(k,\tau) = \varphi_e(\pi^k, \tau\alpha^k) = \tau\alpha^k(\pi^k)^{-e} = \tau\pi^{ke}\pi^{-ke} = \tau$$

b) Les membres d'une association souhaitent pouvoir transmettre à un individu A, un message décomposé en parties telles que chacune puisse être représentée par un élément τ_i du groupe et un entier k_i choisit. Seul A connaît l'entier e et il reçoit de la part de l'auteur les couples :

$$f_\alpha(k_i,\tau_i) = (\lambda_i, \mu_i)$$

Pour pouvoir décrypter les parties et donc le message (c'est-à-dire prendre connaissance des τ_i) il suffira à A d'appliquer φ_e à chaque couple reçu dans la mesure où :

$$\boxed{\varphi_e(\lambda_i,\mu_i) = \varphi_e \circ f_\alpha(k_i,\tau_i) = \tau_i}$$

2. $\mathbb{F}_{29}$ est un corps, donc $\mathbb{F}_{29}^\star$ est un groupe pour la loi . d'ordre $29-1 = 28$.

Par voies de conséquence :

$$\forall \lambda \in \mathbb{F}_{29}^{\star}, \lambda^{28} = 1 \Leftrightarrow \lambda^{17}.\lambda^{11} = 1 \Leftrightarrow \lambda^{17} = \lambda^{-11}$$

On conjecture alors que $e = 11$. Vérifions le sachant que $\pi = 2$ et $\alpha = 18$, on a bien :

$$\boxed{\pi^e = 2^{11} = 2048 = 70 \times 29 + 18 = 18 = \alpha}$$

b) On donne la suite des couples (λ_i, μ_i) suivante :

$$(16, 17), (18, 24), (28, 22), (17, 21), (23, 23), (24, 8)$$

Décryptons ce message en cherchant les parties-ci :

$$\boxed{\tau_i = \varphi_e(\lambda_i, \mu_i) = \mu_i.\lambda_i^{-11} = \mu_i.\lambda_i^{17}}$$

A partir du tableau on a :

$$\begin{aligned}
\varphi_e(16, 17) &= 17 \times 16^{17} = 17 \times 7 = 4 \times 29 + 3 = 3 \\
\varphi_e(18, 24) &= 24 \times 18^{17} = 24 \times 26 = 21 \times 29 + 15 = 15 \\
\varphi_e(28, 22) &= 22 \times 28^{17} = 22 \times 28 = 21 \times 29 + 7 = 7 \\
\varphi_e(17, 21) &= 21 \times 17^{17} = 21 \times 17 = 12 \times 29 + 9 = 9 \\
\varphi_e(23, 23) &= 23 \times 23^{17} = 23 \times 16 = 12 \times 29 + 20 = 20 \\
\varphi_e(24, 8) &= 8 \times 24^{17} = 8 \times 20 = 5 \times 29 + 15 = 15
\end{aligned}$$

Enfin d'après la correspondance entre les entiers $(1, 2, ..., 27, 28)$ modulo 29 et le 28-uplet $(A, B, ..., Z, '', .)$ le message décrypté est :

$$\boxed{\text{COGITO}}$$

Problème

I. L'étude d'un exemple

1. Soit A une matrice quelconque de $\mathcal{M}_2(\mathbb{R})$ donc de la forme $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Calculons A^2 :

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & ab + bd \\ ac + dc & cb + d^2 \end{pmatrix}$$

Par ailleurs $\mathrm{Det}(A) = ad - bc$ et $\mathrm{Tr}(A) = a + d$ d'où :

$$\begin{aligned} A^2 - \mathrm{Tr}(A)A + \mathrm{Det}(A)I_2 &= \begin{pmatrix} a^2+bc & ab+bd \\ ac+dc & d^2 \end{pmatrix} - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a^2+bc-(a+d)a+(ad-bc) & ab+bd-(a+d)b \\ ac+dc-(a+d)c & d^2-(a+d)d+(ad-bc) \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Donc :

$$\boxed{A^2 - \mathrm{Tr}(A)A + \mathrm{Det}(A)I_2 = 0 \quad (*)}$$

2. Soit A une matrice non scalaire ; on note $\mathbb{A}$ l'ensemble :

$$\mathbb{A} = \left\{ M \in \mathcal{M}_2(\mathbb{R}) | \exists (a,b) \in \mathbb{R}^2, M = aI_2 + bA \right\}$$

L'ensemble $\mathbb{A}$ est le sous-espace vectoriel de $\mathcal{M}_2(\mathbb{R})$ engendré par I_2 et A.

La famille (I_2, A) est libre car aI_2 est une matrice scalaire et bA ne l'est pas par hypothèse.

Donc (I_2, A) est une base de $\mathbb{A}$ donc :

$$\boxed{\mathrm{Dim}(\mathbb{A}) = 2}$$

Considérons deux matrices M et M' de $\mathbb{A}$ et calculons leur produit :

$$MM' = (aI_2 + bA)(a'I_2 + b'A) = aa'I_2 + ab'A + ba'A + bb'A^2$$

Et comme $A^2 = \mathrm{Tr}(A)A - \mathrm{Det}(A)I_2$ en reportant on a :

$$\boxed{MM' = (aa' - bb'\mathrm{Det}(A))I_2 + (ab' + ba' + bb'\mathrm{Tr}(A))A \in \mathbb{A}}$$

Donc $\mathbb{A}$ est une sous-algèbre de $\mathcal{M}_2$.

3. Soit $B \in \mathbb{A}$ i.e $B = aI_2 + bA$ qui vérifie $B^2 = -I_2$.

Remarquons que $b \neq 0$ car sinon on aurait $B = aI_2 \Rightarrow B^2 = a^2 I_2 = -I_2$ absurde car $a \in \mathbb{R}$.

$$\begin{aligned} B^2 &= (aI_2 + bA)^2 \\ &= a^2 I_2 + 2abA + b^2 A^2 \\ &= a^2 I_2 + 2abA + b^2(\mathrm{Tr}(A)A - \mathrm{Det}(A)I_2) \\ &= (a^2 - b^2\mathrm{Det}(A))I_2 + (2ab + b^2\mathrm{Tr}(A))A \end{aligned}$$

Puisque $B^2 = -I_2$ on a le système :

$$\left\{\begin{array}{l} a^2-b^2\text{Det}(A)=-1 \\ 2ab+b^2\text{Tr}(A)=0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} a^2-b^2\text{Det}(A)=-1 \\ a=-\frac{b\text{Tr}(A)}{2} \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} b^2(\text{Tr}(A)^2-4\text{Det}(A))=-4 \\ a=-\frac{b\text{Tr}(A)}{2} \end{array}\right.$$

Puisque $b^2>0$ il faut donc que : $\boxed{\text{Tr}(A)^2<4\text{Det}(A)}$

Réciproquement si $\text{Tr}(A)^2<4\text{Det}(A)$ alors la matrice suivante vérifie $B^2=-I_2$:

$$\boxed{B=\left(-\frac{\text{Tr}(A)}{\sqrt{4\text{Det}(A)-\text{Tr}(A)^2}}\right)I_2+\left(\frac{2}{\sqrt{4\text{Det}(A)-\text{Tr}(A)^2}}\right)A}$$

4. La famille (I_2,B) est libre puisque B n'est pas une matrice scalaire d'après $(*)$.

Puisque $\text{Dim}\left(\text{Vect}\left\{I_2,B\right\}\right)=2$ et $\text{Dim}(\mathbb{A})=2$ alors (I_2,B) est une base de $\mathbb{A}$.

Considérons l'isomorphisme d'espace vectoriel défini de $\mathbb{A}$ vers $\mathbb{C}$ par $f(I_2,B)=(1,i)$.

La bijectivité vient du fait que l'image de la base (I_2,B) de $\mathbb{A}$ est la base $(1,i)$ de $\mathbb{C}$.

Ainsi on a bien $f(I_2)=1_{\mathbb{C}}$ et soit $(M,M')\in\mathbb{A}^2$ on a :

$$\begin{array}{rcl} MM' & = & (aI_2+bB)(a'I_2+b'B) \\ & = & aa'I_2+ab'B+ba'B+bb'B^2 \\ & = & (aa'-bb')I_2+(ab'+ba')B \end{array}$$

D'où :

$$\begin{array}{rcl} f(MM') & = & (aa'-bb')f(I_2)+(ab'+ba')f(B) \\ & = & (aa'-bb')+i(ab'+ba') \\ & = & (a+ib)(a'+ib') \\ & = & f(M)f(M') \end{array}$$

Par conséquent f est un isomorphisme d'algèbre entre $\mathbb{A}$ et le corps $\mathbb{C}$ des complexes.

5. Nous avons vu que si $M=aI_2+bA$ alors $M^2=(a^2-b^2\text{Det}(A))I_2+(2ab+b^2\text{Tr}(A))A$.

$$M^2=0\Longrightarrow\left\{\begin{array}{l} a^2-b^2\text{Det}(A)=0 \\ 2ab+b^2\text{Tr}(A)=0 \end{array}\right.$$

Donc soit $a=0$ et $b=0$ soit :

$$\left\{\begin{array}{l} a=-\frac{b\text{Tr}(A)}{2} \\ \left(\frac{\text{Tr}(A)^2}{4}-\text{Det}(A)\right)b^2=0 \end{array}\right.$$

Donc les matrices $M=\left(-\frac{b\text{Tr}(A)}{2}\right)I_2+bA$ vérifient $M^2=0$ sans être nulles.

Supposons qu'une matrice M non nulle soit inversible et vérifie $M^2=0$ alors :

$$M^{-1}(M.M)=M^{-1}.0\Rightarrow(M^{-1}.M)M=0\Rightarrow I_2.M=0\Rightarrow M=0$$

Absurde par hypothèse, donc on en déduit que toutes les matrices M non nulles de $\mathbb{A}$ ne sont pas inversibles et donc que $\mathbb{A}$ n'est pas un corps.

6. Soit B une matrice non scalaire de $\mathcal{M}_2(\mathbb{R})$. On lui associe l'algèbre $\mathbb{B}$.

Si A et B sont semblables alors il existe une matrice inversible $P \in \mathcal{M}_2(\mathbb{R})$ telle que :

$$B = P^{-1}AP$$

B est non scalaire, par suite A non plus et donc (I_2, A) est une base de $\mathbb{A}$.

Soit alors φ définie de $\mathbb{A}$ dans $\mathbb{B}$ par $\varphi(I_2, A) = (I_2, B)$.

φ transforme une base de $\mathbb{A}$ en une base de $\mathbb{B}$ donc est une bijection. Et soit $M \in \mathbb{A}$ on a :

$$\varphi(M) = \varphi(aI_2 + bA) = a\varphi(I_2) + b\varphi(A) = aI_2 + b(P^{-1}AP) = P^{-1}(aI_2 + bA)P = P^{-1}MP$$

Si $(M, M') \in \mathbb{A}^2$ on a $MM' \in \mathbb{A}$ et :

$$\boxed{\varphi(MM') = P^{-1}MM'P = P^{-1}MPP^{-1}M'P = \varphi(M)\varphi(M')}$$

Ainsi φ est un isomorphisme d'algèbre, donc $\mathbb{A}$ et $\mathbb{B}$ sont isomorphes.

7. On suppose que A est telle que $\mathrm{Tr}(A)^2 > 4\mathrm{Det}(A)$.

$\lambda \in \mathbb{R}$ est dite valeur propre de A s'il existe $X \in \mathbb{R}^n - \{0\}$ tel que $AX = \lambda X$.

X est alors un vecteur propre de A associé à la valeur propre λ.

a) On a $AX = \lambda X \Leftrightarrow (\lambda I_2 - A)X = 0$ et puisque $X \neq 0$ alors $(\lambda I_2 - A)$ n'est pas inversible.

D'où $\mathrm{Det}(\lambda I_2 - A) = 0$ donc les valeurs propres sont racines du polynôme $\mathrm{Det}(XI_2 - A)$.

Or il se trouve que : $\mathrm{Det}(XI_2 - A) = X^2 - \mathrm{Tr}(A)X + \mathrm{Det}(A)$.

Et puisque $\Delta = \mathrm{Tr}(A)^2 - 4\mathrm{Det}(A) > 0$ alors le polynôme possède deux racines distinctes.

Donc A possède deux valeurs propres.

b) Notons λ et λ' les valeurs propres de A et X, X' les vecteurs propres associés.

Soit $(\mu, \mu') \in \mathbb{R}^2$ tels que $\mu.X + \mu'X' = 0$ et f l'endomorphisme associé à A, alors :

$$\mu.f(X) + \mu'.f(X') = 0 \Leftrightarrow \mu.\lambda.X + \mu'.\lambda'.X' = 0$$

Or $\mu.X = -\mu'.X'$ d'où : $-\lambda.\mu'.X' + \mu'.\lambda'.X' = 0 \Leftrightarrow \mu'.X'(\lambda' - \lambda) = 0$.

Et puisque les valeurs propres sont distinctes et $X' \neq 0$ il vient $\mu' = 0$, de même $\mu = 0$.

Donc la famille (X, X') est libre et puisque de dimension 2 est une base de $\mathbb{R}^2$.

c) Dans la base (X, X') on a $f(X) = \lambda.X + 0.X'$ et $f(X') = 0.X + \lambda'.X'$ donc :

$$\boxed{M(f) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda' \end{pmatrix}}$$

d) $\mathbb{A}$ est isomorphe à $\mathbb{B}$ où $\mathbb{B} = \text{Vect}(I_2, B)$ et B matrice diagonale semblable à A.

Soit $\mathbb{D}$ l'algèbre des matrices diagonales d'ordre 2 à coefficient dans $\mathbb{R}$ on a :

$$\text{Dim}(\mathbb{D}) = \text{Dim}(\mathbb{B}) = 2 \text{ et } \mathbb{B} \subset \mathbb{D} \Longrightarrow \mathbb{B} = \mathbb{D}$$

e) Notons ϕ un isomorphisme de $\mathbb{A}$ dans $\mathbb{D}$.

Notons également E_{11} et E_{22} les matrices élémentaires qui forment une base de $\mathbb{D}$.

On a $(\phi^{-1}(E_{11}), \phi^{-1}(E_{22})) \neq (0, 0)$ et $\phi^{-1}(E_{11}) \circ \phi^{-1}(E_{22}) = \phi^{-1}(E_{11}E_{22}) = 0$.

Donc $\phi^{-1}(E_{11})$ et $\phi^{-1}(E_{22})$ ne sont pas inversibles, donc $\mathbb{A}$ n'est pas un corps.

II. Quelques résultats généraux

Soit $\mathbb{D}$ une algèbre de dimension finie n.

1. Soit a un élément de $\mathbb{D}$ et ϕ_a l'application définie par :

$$\begin{array}{rccc} \phi_a : & \mathbb{D} & \longrightarrow & \mathbb{D} \\ & x & \mapsto & ax \end{array}$$

Soit $(x, y) \in \mathbb{D}^2$ et $\lambda \in \mathbb{R}$ on a :

$$\boxed{\phi_a(\lambda x + y) = a(\lambda_x + y) = \lambda(ax) + ay = \lambda\phi_a(x) + \phi_a(y)}$$

Donc ϕ_a est un endomorphisme de l'espace vectoriel $\mathbb{D}$.

2. On note $\mathfrak{B}$ une base de $\mathbb{D}$.

$\text{Mat}_{\mathfrak{B}}(\phi_a)$ désigne la matrice de l'endomorphisme ϕ_a dans la base $\mathfrak{B}$.

Soit l'application :

$$\begin{array}{rccc} \Psi : & \mathbb{D} & \longrightarrow & \mathcal{M}_n(\mathbb{R}) \\ & a & \mapsto & \text{Mat}_{\mathfrak{B}}(\phi_a) \end{array}$$

Décomposons là en deux autres applications :

$$\begin{array}{rccccc} \Psi : & \mathbb{D} & \xrightarrow{\phi} & \mathcal{L}(\mathbb{D}) & \xrightarrow{\varphi} & \mathcal{M}_n(\mathbb{R}) \\ & a & \mapsto & \phi_a & \mapsto & \text{Mat}_{\mathfrak{B}}(\phi_a) \end{array}$$

D'une part on a :

$$\boxed{\phi_{\lambda a+\mu b} = \lambda\phi_a + \mu\phi_b}$$

Et d'autre part :

$$\boxed{\phi_{ab} = \phi_a \circ \phi_b}$$

Avec $\phi(1_{\mathbb{D}}) = \phi_{1_{\mathbb{D}}}$ neutre de $\mathcal{L}(\mathbb{D})$. Donc ϕ est un morphisme de l'algèbre $\mathbb{D}$ sur $\mathcal{L}(\mathbb{D})$.

D'après le cours les algèbres $\mathcal{L}(\mathbb{D})$ et $\mathcal{M}_n(\mathbb{R})$ sont isomorphes.

Donc par composition Ψ est un morphisme d'algèbre. Montrons que son noyau est réduit à 0 :

Soit a tel que $\Psi(a) = 0$ i.e $\mathcal{M}_{\mathfrak{B}}(\phi_a) = 0 \Rightarrow \phi_a = 0$.

L'application ϕ_a est identiquement nulle donc en particulier on a $\phi_a(1_{\mathbb{D}}) = a = 0$

Donc $\mathrm{Ker}(\Psi) = \{0_{\mathbb{D}}\}$ et on en déduit que Ψ est injective.

Ainsi par morphisme $\Psi(\mathbb{D})$ est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$ et donc $\mathbb{D}$ est isomorphe à $\Psi(\mathbb{D})$.

3. On considère que $\mathbb{D} = \mathbb{C}$ corps des complexes.

On munit $\mathbb{C}$, considéré comme $\mathbb{R}$-espace vectoriel, de la base $\mathfrak{B} = (1, i)$.

Soit $z = a + ib$ avec $(a, b) \in \mathbb{R}^2$, on a :

$$\phi_z(1) = z \times 1 = a + ib \quad \text{et} \quad \phi_z(i) = z \times i = (a + ib) \times i = -b + ia$$

D'où :

$$\boxed{\mathrm{Mat}_{\mathfrak{B}}(\phi_z) = \begin{array}{c} \begin{array}{cc} \phi_z(1) & \phi_z(i) \end{array} \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{array}{c} 1 \\ i \end{array} \end{array}}$$

4. Soit maintenant $\mathbb{A}$ une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$.

On s'intéresse à quelques cas où on peut affirmer que $\mathbb{A}$ est, ou n'est pas, un corps.

(a) On suppose que $\mathbb{A}$ contient une matrice non scalaire A qui a une valeur propre réelle λ.

Puisque $(A, I_n) \in \mathbb{A}^2$ alors $A - \lambda I_n \in \mathbb{A}$ par combinaison linéaire.

Or on a vu dans la première partie que $A - \lambda I_n$ est non nulle et non inversible.

Donc $\mathbb{A}$ n'est pas un corps.

(b) Traitons simultanément les cas où A est diagonalisable ou trigonalisable.

Soit l'élément $a_{11} = \lambda$ de D , D représente la matrice diagonale ou triangulaire semblable :

$$A - \lambda I_n = PDP^{-1} - \lambda PP^{-1} = P(D - \lambda I_n)P^{-1}$$

Ainsi :

$$\mathrm{Det}(A - \lambda I_n) = \mathrm{Det}(P(D - \lambda I_n)P^{-1}) = \mathrm{Det}(P)\mathrm{Det}(D - \lambda I_n)\mathrm{Det}(P^{-1}) = \mathrm{Det}(D - \lambda I_n)$$

Or l'élément b_{11} de $D - \lambda I_n$ est nul et par suite $\mathrm{Det}(D - \lambda I_n) = 0$.

Le déterminant d'une matrice diagonale ou trigonale égal le produit des éléments diagonaux.

Donc :

$$\boxed{\mathrm{Det}(A - \lambda I_n) = 0}$$

La matrice $A - \lambda I_n \in \mathbb{A}$ est non inversible et donc $\mathbb{A}$ n'est pas un corps.

(c) On suppose que $\mathbb{A}$ est intègre, soit A une matrice non nulle.

L'application ϕ_a est un endomorphisme de $\mathbb{A}$ d'après 1. et de plus :

$$AX = 0 \Longrightarrow X = 0 \text{ car A intègre et } A \neq 0$$

Donc $\mathrm{Ker}(\phi_a) = \{0_{\mathbb{A}}\}$ implique ϕ_a injective. Puis on utilise la formule du rang :

$$\mathrm{Dim}(\mathbb{A}) = \underbrace{\mathrm{Dim}(\mathrm{Ker}\phi_a)}_{=0} + \mathrm{Dim}(\mathrm{Im}\phi_a) \text{ et } \mathrm{Im}\phi_a \subset \mathbb{A} \Rightarrow \mathrm{Im}\phi_a = \mathbb{A}$$

Et donc ϕ_a est surjective. C'est un isomorphisme de $\mathbb{A}$.

De là on en déduit qu'il existe une matrice $M \in \mathbb{A}$ telle que :

$$\phi_a(M) = I_n \Leftrightarrow AM = I_n$$

Donc A est inversible, et c'est le cas pour toutes les matrices de $\mathbb{A}$.

Donc $\mathbb{A}$ est un corps.

III. L'algèbre des quaternions

On suppose qu'il existe deux matrices A et B de $\mathcal{M}_n(\mathbb{R})$ telles que :

$$A^2 = -I_n \qquad B^2 = -I_n \qquad AB + BA = 0 \quad (*)$$

1. On a $A^2 = -I_n$ donc par morphisme :

$$\boxed{\mathrm{Det}(A^2) = \mathrm{Det}(-I_n) \Leftrightarrow \mathrm{Det}(A)^2 = (-1)^n}$$

Et donc n est nécessairement pair.

2. Considérons l'ensemble suivant :

$$\mathbb{H} = \left\{ M \in \mathcal{M}_n(\mathbb{R}), \exists (t,x,y,z) \in \mathbb{R}^4, M = tI_n + xA + yB + zAB \right\}$$

$\mathbb{H}$ est clairement un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$, en effet :

Soit $(\lambda, \mu) \in \mathbb{R}^2$ et $(M, M') \in \mathbb{H}^2$ on a :

$$\lambda M + \mu M' = (\lambda t + \mu t')I_n + (\lambda x + \mu x')A + (\lambda y + \mu y')B + (\lambda z + \mu z')$$

Par ailleurs :

$$\begin{aligned} MM' &= (tI_n + xA + yB + zAB)(t'I_n + x'A + y'B + z'AB) \\ &= (tt'I_n + tx'A + ty'B + tz'AB) + (xt'A + xx'A^2 + xy'AB + xz'A^2B) \\ &+ (yt'B + yx'BA + yy'B^2 + yz'BAB) + (zt'AB + zx'ABA + zy'AB^2 + zz'(AB)^2) \end{aligned}$$

Or telles que sont définies A et B on a :

$$BAB = -(-BA)B = -(AB)B = -AB^2 = -A(-I_n) = A$$

$$ABA = -A(-BA) = -A(AB) = -A^2B = -(-I_n)B = B$$

$$(AB)^2 = (AB)(AB) = A(BA)B = -A(AB)B = -A^2B^2 = -I_n$$

Il vient alors :

$$MM' = (tt'-xx'-yy'-zz')I_n+(tx'+xt'+yz'-zy')A+(ty'-xz'+yt'+zx')B+(tz'+xy'-yx'+zt')AB$$

Et puisque $I_n \in \mathbb{H}$ alors $\mathbb{H}$ est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$.

3. En prenant $t' = t$, $x' = -x$, $y' = -y$ et $z' = -z$ on a directement :

$$\boxed{(tI_n + xA + yB + zAB)(tI_n - xA - yB - zAB) = (t^2 + x^2 + y^2 + z^2)I_n \quad (\star)}$$

4. (a) Considérons la relation linéaire $tI_n + xA + yB + zAB = 0$, on a alors d'après $(\star)$:

$$(tI_n + xA + yB + zAB)(tI_n - xA - yB - zAB) = 0 \Longrightarrow (t^2 + x^2 + y^2 + z^2)I_n = 0$$

Et comme $I_n \neq 0$:

$$\boxed{t^2 + x^2 + y^2 + z^2 = 0 \Longrightarrow t = x = y = z = 0}$$

Donc la famille (I_n, A, B, AB) est libre et forme donc une base de $\mathbb{H}$.

(b) Si $M = aI_n + xA + yB + zAB \in \mathbb{H}$ alors d'après $(\star)$ on a :

$$\boxed{M^{-1} = \frac{1}{t^2 + x^2 + y^2 + z^2}(tI_n - xA - yB - zAB) \in \mathbb{H}}$$

Ceci étant vérifié pour toute matrice on en conclut que $\mathbb{H}$ est un corps.

5. On suppose dans toute la suite du problème que $n = 4$.

En notant J la matrice $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et 0 la matrice nulle de $\mathcal{M}_2(\mathbb{R})$ on définit :

$$A = \begin{pmatrix} J & 0 \\ 0 & -J \end{pmatrix} \qquad B = \begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix}$$

On pose également $C = AB$.

(a) On calcule facilement :

$$J^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -I_2 & 0 \\ 0 & -I_2 \end{pmatrix}$$

$$B^2 = \begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix}\begin{pmatrix} 0 & -I_2 \\ I_2 & 0 \end{pmatrix} = \begin{pmatrix} -I_2 & 0 \\ 0 & -I_2 \end{pmatrix} = -I_4$$

$$A^2 = \begin{pmatrix} J & 0 \\ 0 & -J \end{pmatrix}\begin{pmatrix} J & 0 \\ 0 & -J \end{pmatrix} = \begin{pmatrix} J^2 & 0 \\ 0 & J^2 \end{pmatrix} = -I_4$$

$$AB + BA = \begin{pmatrix} 0 & -J \\ -J & 0 \end{pmatrix} + \begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix} = 0$$

Donc les matrices A et B satisfont la condition $(*)$.

On appelera donc $\mathbb{H}$ le sous-espace vectoriel de $\mathcal{M}_4(\mathbb{R})$ engendré par I_4, A, B et C.

Ses éléments sont appelés quaternions et la base (I_4, A, B, C) de $\mathbb{H}$ sera notée $\mathfrak{B}$.

(b) Soit M une matrice non nulle de $\mathbb{H}$, elle s'écrit dans la base $\mathfrak{B}$:

$$M = tI_4 + xA + yB + zC$$

Or les matrices A, B et C sont antisymétrique et on sait que pour une telle matrice X :

$${}^tX = -X$$

Donc :

$$\boxed{{}^tM = tI_4 - xA - yB - zC \in \mathbb{H}}$$

Mais alors on remarque que :

$$M\,{}^tM = (tI_4 + xA + yB + zC)(tI_4 - xA - yB - zC) = (t^2 + x^2 + y^2 + z^2)I_4$$

On a vu précédemment que :

$$M^{-1} = \frac{1}{t^2 + x^2 + y^2 + z^2}(tI_4 - xA - yB - zC) = \frac{{}^tM}{t^2 + x^2 + y^2 + z^2}$$

On sait de surcroît que $\mathrm{Det}(M) = \mathrm{Det}({}^tM)$ donc :

$$\mathrm{Det}(M)^2 = \mathrm{Det}((t^2+x^2+y^2+z^2)I_4) = (t^2+x^2+y^2+z^2)^4$$

Et finalement :

$$\boxed{M^{-1} = \frac{{}^tM}{\sqrt{\mathrm{Det}(M)}}}$$