X-ENS 2023

Épreuve de mathématiques A, MP & MPI, quatre heures

(corrigé)

Remarque sur les résultats admis. Pour montrer que $\mathbb{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$, il suffit de noter que c'est l'image de l'application $\mathbb{R}$-linéaire $(z_1, z_2) \mapsto Z(z_1, z_2)$ définie sur $\mathbb{C}^2$. De plus Z est clairement injective, donc elle induit un isomorphisme de $\mathbb{C}^2$ dans son image $\mathbb{H}$. On en déduit que l'image par Z de toute base de $\mathbb{C}^2$ est une base de $\mathbb{H}$; or une base évidente de $\mathbb{C}^2$ est $((1,0),(i,0),(0,1),(0,i))$. En prenant l'image par Z de cette base, on obtient la base $(Z(1,0), Z(i,0), Z(0,1), Z(0,i)) = (E, I, -J, K)$ de $\mathbb{H}$.

1 Préliminaires

1. (a) L'énoncé demande déjà d'admettre que $\mathbb{H}$ est un sous-$\mathbb{R}$-espace vectoriel de $\mathrm{M}_2(\mathbb{C})$. Pour montrer que $\mathbb{H}$ est une sous-$\mathbb{R}$-algèbre de $\mathrm{M}_2(\mathbb{C})$, il suffit donc de démontrer la stabilité par produit, qui découle directement de l'identité facile à vérifier :

$$\forall (z_1, z_2, z_1', z_2') \in \mathbb{C}^4, \quad Z(z_1, z_2)Z(z_1', z_2') = Z(z_1 z_1' - \overline{z_2} z_2', z_2 z_1' + \overline{z_1} z_2') \in \mathbb{H}. \tag{1}$$

De plus $\mathbb{H}$ est stable par $Z \mapsto Z^*$, puisque :

$$\forall (z_1, z_2) \in \mathbb{C}^2, \quad Z(z_1, z_2)^* = \begin{pmatrix} \overline{z_1} & \overline{z_2} \\ -z_2 & z_1 \end{pmatrix} = Z(\overline{z_1}, -z_2) \in \mathbb{H}. \tag{2}$$

On peut aussi remarquer que :

$$E^* = E, \quad I^* = -I, \quad J^* = -J, \quad K^* = -K, \tag{3}$$

pour étendre ensuite le résultat de stabilité à tout élément de $\mathbb{H}$ par linéarité.

(b) Soit $(z_1, z_2) \in \mathbb{C}^2$ tel que : $Z = Z(z_1, z_2)$. On a :

$$ZZ^* \overset{(2)}{=} Z(z_1, z_2)Z(\overline{z_1}, -z_2) \overset{(1)}{=} Z(\underbrace{z_1\overline{z_1} + \overline{z_2}z_2}_{=|z_1|^2+|z_2|^2}, \underbrace{z_2\overline{z_1} - \overline{z_1}z_2}_{=0}) = \left(|z_1|^2 + |z_2|^2\right) E,$$

soit donc, avec les notations de l'énoncé :

$$\forall Z \in \mathbb{H}, \quad ZZ^* = \mathrm{N}(Z)E. \tag{4}$$

Or on remarque que si $\mathrm{N}(Z(z_1, z_2)) = 0$, alors $z_1 = z_2 = 0$ (en utilisant le fait qu'une somme de réels positifs soit nulle seulement si chaque terme est nul), et donc $Z(z_1, z_2) = 0_{\mathbb{H}}$, la réciproque étant évidente. Autrement dit :

$$\forall Z \in \mathbb{H}, \quad (\mathrm{N}(Z) = 0 \iff Z = 0_{\mathbb{H}}). \tag{5}$$

En particulier, si Z est un élément non nul de $\mathbb{H}$, alors $\mathrm{N}(Z) \neq 0$, et donc l'égalité ci-dessus équivaut à :

$$Z \cdot \left(\frac{1}{\mathrm{N}(Z)} Z^*\right) = E.$$

On en déduit que Z admet un inverse à droite dans $\mathbb{H}$, mais aussi dans $\mathrm{M}_2(\mathbb{C})$ (rappelons que E est la matrice identité : ainsi l'inversibilité est équivalente dans ces deux anneaux). Dans $\mathrm{M}_2(\mathbb{C})$, un inverse à droite est aussi un inverse à gauche, donc Z est inversible dans $\mathrm{M}_2(\mathbb{C})$ et $\mathbb{H}$ et on a :

$$\forall Z \in \mathbb{H} \setminus \{0_{\mathbb{H}}\}, \quad Z^{-1} = \frac{1}{\mathrm{N}(Z)} Z^*.$$

On a donc montré : $\mathbb{H}^\times = \mathbb{H} \setminus \{0_{\mathbb{H}}\}$ (l'inclusion directe est triviale et l'inclusion réciproque était l'objectif de cette question).

(c) Posons : $Z = aE + bI + cJ + dK$, avec $(a, b, c, d) \in \mathbb{R}^4$. Comme $Z' \mapsto ZZ'$ et $Z' \mapsto Z'Z$ sont linéaires, elles coïncident sur $\mathbb{H}$ si et seulement si elles coïncident sur une base de $\mathbb{H}$. On en déduit que $ZZ' = Z'Z$ pour tout $Z' \in \mathbb{H}$ si et seulement si :

$$ZE = EZ, \quad ZI = IZ, \quad ZJ = JZ, \quad ZK = KZ,$$

si et seulement si, d'après les règles de calcul admises dans l'énoncé :

$$\left\{ \begin{array}{rcl} aI - bE - cK + dJ & = & aI - bE + cK - dJ, \\ aJ + bK - cE - dI & = & aJ - bK - cE + dI, \\ aK - bJ + cI - dE & = & aK + bJ - cI - dE, \end{array} \right.$$

si et seulement si, en identifiant les coordonnées dans la base (E, I, J, K) :

$$-c = c, \quad d = -d, \quad b = -b,$$

si et seulement si : $b = c = d = 0$, si et seulement si : $Z = aE \in \mathbb{R}_{\mathbb{H}}$. On a montré :

$$Z \in \mathbb{R}_{\mathbb{H}} \iff \forall Z' \in \mathbb{H}, \quad ZZ' = Z'Z.$$

2. (a) Soit $(Z, Z') \in \mathbb{H}^2$. On a, d'après (4) :

$$\mathrm{N}(ZZ')E = ZZ'(ZZ')^*,$$

or : $(ZZ')^* = Z'^*Z^*$ (conséquence directe des propriétés de la conjugaison complexe et de la transposition), donc :

$$\mathrm{N}(ZZ')E = ZZ'Z'^*Z^* \overset{(4)}{=} Z(\mathrm{N}(Z')E)Z^*,$$

et comme : $\mathrm{N}(Z')E \in \mathbb{R}_{\mathbb{H}}$, d'après la question précédente $\mathrm{N}(Z')E$ commute avec Z^*, donc :

$$\mathrm{N}(ZZ')E = ZZ^*\mathrm{N}(Z')E = \mathrm{N}(Z)E \cdot \mathrm{N}(Z')E = \mathrm{N}(Z)\mathrm{N}(Z')E.$$

On en déduit :

$$\mathrm{N}(ZZ') = \mathrm{N}(Z)\mathrm{N}(Z'),$$

d'où le résultat.

(b) La question précédente et l'équivalence (5) assurent que N est un morphisme de groupes de $\mathbb{H}^\times$ dans $\mathbb{R}^*$ (et même $\mathbb{R}_+^*$). Or : $S = \ker(\mathrm{N})$, donc S est un sous-groupe de $\mathbb{H}^\times$ (en tant que noyau d'un morphisme de groupes). Montrons que $\frac{1}{\sqrt{\mathrm{N}(Z)}}Z$ appartient à S pour tout $Z \in \mathbb{H}^\times$ (toujours d'après (5), la division par $\sqrt{\mathrm{N}(Z)}$ est licite si $Z \neq 0_{\mathbb{H}}$). La définition de N implique clairement :

$$\forall (Z, \lambda) \in \mathbb{H} \times \mathbb{R}, \quad \mathrm{N}(\lambda Z) = \lambda^2 \mathrm{N}(Z).$$

Donc :

$$\forall Z \in \mathbb{H}^\times, \quad \mathrm{N}\left(\frac{1}{\sqrt{\mathrm{N}(Z)}}Z\right) = \frac{1}{\left(\sqrt{\mathrm{N}(Z)}\right)^2}\mathrm{N}(Z) = 1,$$

d'où le résultat : $\forall Z \in \mathbb{H}^\times$, $\frac{1}{\sqrt{\mathrm{N}(Z)}}Z \in S$.

3. (a) Soit $(x,y,z,t) \in \mathbb{R}^4$. On a :

$$\begin{aligned}
\mathrm{N}\left(xE+yI+zJ+tK\right)E &\overset{(4)}{=} \left(xE+yI+zJ+tK\right)\left(xE+yI+zJ+tK\right)^* \\
&= \left(xE+yI+zJ+tK\right)\left(xE^*+yI^*+zJ^*+tK^*\right) \\
&\overset{(3)}{=} \left(xE+yI+zJ+tK\right)\left(xE-yI-zJ-tK\right) \\
&= (xE)^2-(yI+zJ+tK)^2 \\
&= x^2E^2-y^2I^2-z^2J^2-t^2K^2 \\
&\quad -\left(yz\left(IJ+JI\right)+yt\left(IK+KI\right)+zt\left(JK+KJ\right)\right),
\end{aligned}$$

et grâce aux règles de calcul admises dans l'énoncé : $I^2=J^2=K^2=-E$, tandis que les termes en facteur de yz, yt et zt se simplifient. D'où :

$$\mathrm{N}\left(xE+yI+zJ+tK\right)E = \left(x^2+y^2+z^2+t^2\right)E,$$

et on conclut : $\mathrm{N}\left(xE+yI+zJ+tK\right) = x^2+y^2+z^2+t^2$.

(b) Soit $U \in \mathbb{H}^{\mathrm{im}}$. On remarque immédiatement, grâce au fait que $I^*=-I$, $J^*=-J$ et $K^*=-K$:

$$U^* = -U.$$

On en déduit :

$$U^2 = -UU^* \overset{(4)}{=} -\mathrm{N}(U)E,$$

d'où le résultat. Or : $\mathrm{N}(\mathbb{H}) \subseteq \mathbb{R}_+$, donc cette égalité implique :

$$\mathbb{H}^{\mathrm{im}} \subseteq \left\{U \in \mathbb{H} \mid U^2 \in]-\infty,0]E\right\}.$$

Montrons l'inclusion réciproque. On peut y parvenir par un calcul brut. Soit $U \in \mathbb{H}$, et soit $(x,y,z,t) \in \mathbb{R}^4$ tel que : $U = xE+yI+zJ+tK$. Alors, par un calcul similaire à celui de la question précédente :

$$U^2 = \left(x^2-y^2-z^2-t^2\right)E + 2x\left(yI+zJ+tK\right).$$

Par conséquent, s'il existe $\lambda \in]-\infty,0]$ tel que : $U^2=\lambda E$, alors en identifiant coordonnée par coordonnée on a :

$$\left\{\begin{array}{rcl} x^2-y^2-z^2-t^2 &=& \lambda, \\ xy &=& 0, \\ xz &=& 0, \\ xt &=& 0. \end{array}\right.$$

Pour avoir : $U \in \mathbb{H}^{\mathrm{im}}$, il suffit de démontrer que l'on a : $x=0$. Raisonnons par l'absurde et supposons que x est non nul. Les trois dernières égalités ci-dessus impliquent alors : $y=z=t=0$, et la première équivaut alors à : $x^2=\lambda$. Comme $x^2 \geqslant 0$ et $\lambda \leqslant 0$, cette égalité n'est possible que si $\lambda = x = 0$: absurde, puisqu'on a supposé x non nul.
Ce raisonnement par l'absurde montre que nécessairement : $x=0$. Donc : $U = yI+zJ+tK \in \mathbb{H}^{\mathrm{im}}$, d'où l'inclusion réciproque :

$$\mathbb{H}^{\mathrm{im}} = \left\{U \in \mathbb{H} \mid U^2 \in]-\infty,0]E\right\}.$$

Remarque. Ce même raisonnement permettrait de démontrer que U^2 appartient à $\mathbb{R}_{\mathbb{H}}$ si et seulement si U est dans $\mathbb{R}_{\mathbb{H}}$ ou $\mathbb{H}^{\mathrm{im}}$ (dans le premier cas, on a $U^2 \in [0,+\infty[E$).

Remarque. On a justifié que si $U \in \mathbb{H}^{\mathrm{im}}$, alors : $U^* = -U$. On a en fait mieux, ce qui nous servira plus tard (et n'est pas difficile à montrer) :

$$\left\{\begin{array}{rcl} U^* = -U &\iff& U \in \mathbb{H}^{\mathrm{im}}, \\ U^* = U &\iff& U \in \mathbb{R}_{\mathbb{H}}. \end{array}\right. \tag{6}$$

4. On a : $S = \mathrm{N}^{-1}(\{1\})$, et $\{1\}$ est une partie fermée de $\mathbb{R}$. Montrons que N est continue sur $\mathbb{H}$. Pour cela, on note que N est la composition de l'isométrie ψ^{-1} (continue sur $\mathbb{H}$ en tant qu'application linéaire sur un $\mathbb{R}$-espace vectoriel de dimension finie, et à valeurs dans $\mathbb{R}^4$) et de l'application $(x,y,z,t) \mapsto x^2+y^2+z^2+t^2$ (continue sur $\mathbb{R}^4$ en tant qu'application polynomiale), donc N est continue sur $\mathbb{H}$. Ainsi S est l'image réciproque d'un fermé par une application continue, donc c'est une partie fermée de $\mathbb{H}$.

   Montrons que S est connexe par arcs. Soit $(Z,Z') \in S^2$. Supposons d'abord que (Z,Z') est une famille libre, et posons :

$$\forall t \in [0,1], \quad \gamma(t) = \frac{1}{\sqrt{\mathrm{N}(tZ+(1-t)Z')}}(tZ+(1-t)Z').$$

   Notons que $tZ+(1-t)Z'$ est bien non nul pour tout $t \in [0,1]$, puisque Z et Z' sont supposés linéairement indépendants. Ainsi $\gamma(t)$ est correctement définie pour tout $t \in [0,1]$, et γ est à valeurs dans S par la question 2.(b). De plus γ est continue $[0,1]$ par continuité de N (justifiée ci-dessus) et de $t \mapsto tZ+(1-t)Z'$, évidente, et enfin : $\gamma(0) = Z'$, $\gamma(1) = Z$. On a donc bien montré que si (Z,Z') est libre, alors il existe un chemin continu dans S reliant Z et Z'.

   Supposons à présent (Z,Z') liée (ce qui équivaut ici à : $Z = \pm -Z'$). Soit $W \in \mathbb{H}$ tel que (Z,W) soit libre (un tel élément existe puisque $\mathbb{H}$ est de dimension 4). Quitte à remplacer W par $\frac{1}{\sqrt{\mathrm{N}(W)}}W$, on peut supposer que W appartient à S. Comme (Z,W) est libre (et donc (Z',W) aussi), par le raisonnement ci-dessus il existe deux chemins continus $\gamma_1, \gamma_2 : [0,1] \to S$ tels que : $\gamma_1(0) = Z'$, $\gamma_1(1) = W$, et : $\gamma_2(0) = W$, $\gamma_2(1) = Z$. Posons alors :

$$\forall t \in [0,1], \quad \gamma(t) = \begin{cases} \gamma_1(2t) & \text{si} \quad t \in \left[0, \frac{1}{2}\right], \\ \gamma_2\left(2\left(t-\frac{1}{2}\right)\right) & \text{si} \quad t \in \left[\frac{1}{2}, 1\right]. \end{cases}$$

   L'application γ est continue sur $[0,1]$ par continuité de γ_1 et γ_2 (notons de plus que $\gamma_1(1) = \gamma_2(0) = W$, ce qui assure la continuité de γ en $\frac{1}{2}$), est à valeurs dans S, et vérifie : $\gamma(0) = \gamma_1(0) = Z'$, $\gamma(1) = \gamma_2(1) = Z$. Ainsi, si $Z = -Z'$, il existe encore un chemin continu dans S reliant Z et Z'.

   Nous avons donc montré que pour tout $(Z,Z') \in S^2$, il existe un chemin continu à valeurs dans S reliant Z et Z', donc S est connexe par arcs : d'où le résultat.

5. (a) Remarquons d'abord que l'on a, sans hypothèse sur U et V :

$$\begin{aligned} \langle U,V\rangle E &= \frac{\mathrm{N}(U+V)-\mathrm{N}(U)-\mathrm{N}(V)}{2}E \\ &\overset{(4)}{=} \frac{1}{2}\left((U+V)(U+V)^* - UU^* - VV^*\right) \\ &= \frac{1}{2}\left(UU^* + UV^* + VU^* + VV^* - UU^* - VV^*\right) \\ &= \frac{1}{2}\left(UV^* + VU^*\right), \end{aligned} \tag{7}$$

   et donc, toujours sans hypothèse sur U et V :

$$U \perp V \iff UV^* + VU^* = 0_{\mathbb{H}}.$$

   Or U et V sont dans $\mathbb{H}^{\mathrm{im}}$, donc $U^* = -U$ et $V^* = -V$ comme nous l'avons justifié dans la question 3.(b). Donc :

$$U \perp V \iff UV + VU = 0_{\mathbb{H}},$$

   d'où le résultat. Pour montrer la seconde partie de l'énoncé, il suffit de vérifier que l'on a : $(UV)^* = -UV$, comme nous l'avons souligné à la fin de la résolution de la question 6. Or,

sous l'hypothèse que U et V sont orthogonaux, on a $VU = -UV$ d'après ce qui précède, donc :

$$(UV)^* = V^*U^* = (-V)(-U) = VU = -UV,$$

d'où le résultat : $UV \in \mathbb{H}^{\mathrm{im}}$. Enfin, montrons que le déterminant de la famille (U, V, UV) dans la base (I, J, K) de $\mathbb{H}^{\mathrm{im}}$ est positif ou nul. Soient $(a, b, c) \in \mathbb{R}^3$ et $(d, e, f) \in \mathbb{R}^3$ tels que :

$$U = aI + bJ + cK, \quad V = dI + eJ + fK.$$

Un calcul direct donne :

$$UV = -(ad + be + cf)E + (bf - ce)I + (cd - af)J + (ae - bd)K,$$

et puisque $UV \in \mathbb{H}^{\mathrm{im}}$, le coefficient de E est nul, donc :

$$UV = (bf - ce)I + (cd - af)J + (ae - bd)K.$$

Pour alléger la rédaction des calculs qui suivent, on note que $X \mapsto \det_{(I,J,K)}(U, V, X)$ est une forme linéaire sur $\mathbb{H}^{\mathrm{im}}$ qui est de dimension finie sur $\mathbb{R}$, donc par le théorème de représentation de Riesz il existe $W \in \mathbb{H}^{\mathrm{im}}$ tel que : $\forall Z \in \mathbb{H}^{\mathrm{im}}$, $\det_{(I,J,K)}(U, V, Z) = \langle W, Z\rangle$. En posant successivement $Z = I$, $Z = J$ et $Z = K$, on a :

$$\langle W, I\rangle = \det_{(I,J,K)}(U, V, I) = \begin{vmatrix} a & d & 1 \\ b & e & 0 \\ c & f & 0 \end{vmatrix} = \begin{vmatrix} b & e \\ c & f \end{vmatrix} = bf - ce,$$

et de même :

$$\langle W, J\rangle = -\begin{vmatrix} a & d \\ c & f \end{vmatrix} = cd - af, \quad \langle W, K\rangle = \begin{vmatrix} a & d \\ b & e \end{vmatrix} = ae - bd$$

On en déduit, puisque (I, J, K) est une base orthonormée de $\mathbb{H}^{\mathrm{im}}$:

$$W = \langle W, I\rangle I + \langle W, J\rangle J + \langle W, K\rangle K = (bf - ce)I + (cd - af)J + (ae - bd)K = UV.$$

En résumé, on a montré :

$$\forall Z \in \mathbb{H}^{\mathrm{im}}, \quad \det_{(I,J,K)}(U, V, Z) = \langle UV, Z\rangle,$$

et en posant $Z = UV \in \mathbb{H}^{\mathrm{im}}$ on obtient : $\det_{(I,J,K)}(U, V, UV) = \langle UV, UV\rangle \geqslant 0$, ce qu'il fallait démontrer.

Remarque. L'identité : $\forall Z \in \mathbb{H}^{\mathrm{im}}$, $\det_{(I,J,K)}(U, V, Z) = \langle UV, Z\rangle$, permet de comprendre par ailleurs que UV représente le produit vectoriel de U et V (puisqu'il est défini sur $\mathbb{R}^3$ par une égalité analogue). Pour expliquer comment on peut avoir l'idée de reconnaître le produit vectoriel, et ainsi proposer cette résolution : les égalités $IJ = K$, $JK = I$, $KI = J$, etc., font écho aux égalités $\vec{i} \wedge \vec{j} = \vec{k}$, etc. Ainsi il semble (et cela se démontrerait en utilisant la bilinéarité) que l'application naturelle $f : a\vec{i} + b\vec{j} + c\vec{k} \mapsto aI + bJ + cK$ transforme le produit vectoriel de $\mathbb{R}^3$ en le produit dans $\mathbb{H}^{\mathrm{im}}$, c'est-à-dire : $\forall (\vec{x}, \vec{y}) \in (\mathbb{R}^3)^2$, $\vec{x} \wedge \vec{y} = f(\vec{x})f(\vec{y})$.

(b) Supposons que (U, V) est une famille orthonormale dans $\mathbb{H}^{\mathrm{im}}$. Montrons que UV est unitaire et orthogonal à U et V. Comme U et V sont unitaires, on a :

$$\mathrm{N}(UV) \overset{(q.25)}{=} \mathrm{N}(U)\mathrm{N}(V) = 1,$$

donc UV est unitaire. Montrons l'orthogonalité. D'après la question précédente, UV est dans $\mathbb{H}^{\text{im}}$, et :

$$U \perp UV \iff U(UV) + (UV)U = 0_{\mathbb{H}},$$

or on sait que U et V sont orthogonaux, donc : $UV = -VU$. Donc :

$$U(UV) + (UV)U = -U(VU) + (UV)U = -UVU + UVU = 0_{\mathbb{H}},$$

donc U et UV sont orthogonaux. On montre de même que V et UV sont orthogonaux. Ainsi (U, V, UV) est bien une base orthonormée, de même orientation que la base (I, J, K) d'après la question précédente : c'est donc une base orthonormée directe de $\mathbb{H}^{\text{im}}$ (si cet espace vectoriel est orienté de sorte que la base (I, J, K) soit directe). D'où le résultat.

2 Automorphismes de $\mathbb{H}$ et rotations

6. Soit $((u_1, u_2), (v_1, v_2)) \in (S \times S)^2$. On doit montrer : $\alpha((u_1, u_2) \times (v_1, v_2)) = \alpha(u_1, u_2) \circ \alpha(v_1, v_2)$. On a :

$$\begin{aligned} \forall Z \in \mathbb{H}, \quad \alpha(u_1, u_2) \circ \alpha(v_1, v_2)(Z) &= \alpha(u_1, u_2)\left(v_1 Z v_2^{-1}\right) \\ &= u_1\left(v_1 Z v_2^{-1}\right) u_2^{-1} \\ &= (u_1 v_1) Z (u_2 v_2)^{-1} \\ &= \alpha(u_1 v_1, u_2 v_2)(Z) \\ &= \alpha((u_1, u_2) \times (v_1, v_2))(Z), \end{aligned}$$

d'où : $\alpha((u_1, u_2) \times (v_1, v_2)) = \alpha(u_1, u_2) \circ \alpha(v_1, v_2)$, ce qu'il fallait démontrer. Ainsi α est un morphisme de groupes de $S \times S$ dans $\mathrm{GL}(\mathbb{H})$. Déterminons son noyau. Soit $(u_1, u_2) \in S \times S$. Alors :

$$\alpha(u_1, u_2) = \mathrm{id}_{\mathbb{H}} \iff \forall Z \in \mathbb{H},\ u_1 Z u_2^{-1} = Z \iff \forall Z \in \mathbb{H},\ u_1 Z = Z u_2.$$

Comme $Z \mapsto u_1 Z$ et $Z \mapsto Z u_2$ sont linéaires, ces deux applications coïncident sur $\mathbb{H}$ si et seulement si elles coïncident sur une base de $\mathbb{H}$. On en déduit :

$$\alpha(u_1, u_2) = \mathrm{id}_{\mathbb{H}} \iff \begin{cases} u_1 E = E u_2 \\ u_1 I = I u_2 \\ u_1 J = J u_2 \\ u_1 K = K u_2 \end{cases} \iff \begin{cases} u_1 = u_2 \\ u_1 I = I u_1 \\ u_1 J = J u_1 \\ u_1 K = K u_1 \end{cases}$$

$$\iff \begin{cases} u_1 = u_2 \\ \forall Z \in \mathbb{H}, \quad u_1 Z = Z u_1 \end{cases}$$

D'après la question 1.(c), on a donc :

$$\alpha(u_1, u_2) = \mathrm{id}_{\mathbb{H}} \iff \begin{cases} u_1 = u_2 \\ u_1 \in \mathbb{R}_{\mathbb{H}} \cap S = \{-E, E\} \end{cases},$$

donc : $\ker(\alpha) = \{(E, E), (-E, -E)\}$.

7. Justifions la continuité de α. Notons d'abord que si l'on définit, pour tout $(u, v) \in \mathbb{H}^2$, l'application $m_{u,v} : Z \mapsto uZv$, alors $(u, v) \mapsto m_{u,v}$ est continue sur $\mathbb{H}^2$ en tant qu'application bilinéaire sur $\mathbb{H}^2$ (qui est de dimension finie sur $\mathbb{R}$), et à valeurs dans $\mathrm{GL}(\mathbb{H})$ si on la restreint à $S \times S$. Par un argument analogue (mais de linéarité cette fois-ci), les applications $p_1 : (u, v) \mapsto u$ et $p_2 : (u, v) \mapsto v$ sont continues sur $\mathbb{H}^2$. Enfin, par la question 1.(b), on a : $\forall v \in S,\ v^{-1} = v^*$,

et $v \mapsto v^*$ est continue sur $\mathbb{H}$ (donc aussi sur S par restriction) en tant qu'application linéaire. On en déduit, par composition avec p_1 ou p_2, la continuité des applications $(u,v) \mapsto u$ et $(u,v) \mapsto v^{-1}$ sur $S \times S$. Par composition des applications continues $(u,v) \mapsto (u, v^{-1})$ et $(u,v) \mapsto m_{u,v}$, l'application $\alpha : (u,v) \mapsto m_{u,v^{-1}}$ est continue sur $S \times S$.
Montrons que l'image de α est contenue dans $\mathrm{O}(\mathbb{H})$, puis dans $\mathrm{SO}(\mathbb{H})$. Soit $(u,v) \in S \times S$. On sait déjà que $\alpha(u,v)$ est linéaire. On va montrer que $\alpha(u,v)$ conserve la norme, c'est-à-dire :

$$\forall Z \in \mathbb{H}, \quad \langle \alpha(u,v)Z, \alpha(u,v)Z \rangle = \langle Z, Z \rangle.$$

Soit $Z \in \mathbb{H}$. On a :

$$\langle \alpha(u,v)Z, \alpha(u,v)Z \rangle = \mathrm{N}(\alpha(u,v)Z) = \mathrm{N}\left(uZv^{-1}\right) = \mathrm{N}(u)\mathrm{N}(Z)\mathrm{N}\left(v^{-1}\right),$$

et comme $u \in S$, on a : $\mathrm{N}(u) = 1$. Comme $v \in S$, on a $v^{-1} \in S$ (on a en effet montré que S est un groupe), donc on a aussi : $\mathrm{N}\left(v^{-1}\right) = 1$. On a donc :

$$\langle \alpha(u,v)Z, \alpha(u,v)Z \rangle = \mathrm{N}(Z) = \langle Z, Z \rangle,$$

donc $\alpha(u,v)$ conserve la norme. Ainsi α est bien à valeurs dans $\mathrm{O}(\mathbb{H})$. Pour en déduire que α est à valeurs dans $\mathrm{SO}(\mathbb{H})$, on utilise le déterminant : l'application $\det \circ \alpha : S \times S \to \mathbb{R}$ est continue et $S \times S$ est connexe par arcs par la question 4 (il n'est pas difficile de montrer que si S est connexe par arcs, alors $S \times S$ l'est aussi), donc son image est une partie connexe par arcs de $\mathbb{R}$: c'est donc un intervalle. Mais l'image de $\det \circ \alpha$ est incluse dans $\{-1, 1\}$, puisque α est à valeurs dans $\mathrm{O}(\mathbb{H})$. Ainsi : $\det \circ \alpha(S \times S) = \{1\}$, ou : $\det \circ \alpha(S \times S) = \{-1\}$. On exclut cette deuxième possibilité en notant que $(E,E) \in S \times S$, et on a : $\det(\alpha(E,E)) = \det(\mathrm{id}_{\mathbb{H}}) = 1 \neq -1$. On a donc :

$$\alpha(S \times S) \subseteq \mathrm{O}(\mathbb{H}), \quad \text{et :} \quad \forall (u,v) \in S \times S,\ \det(\alpha(u,v)) = 1,$$

donc : $\alpha(S \times S) \subseteq \mathrm{SO}(\mathbb{H})$. D'où le résultat.

8. (a) Comme $v \in \mathbb{H}^{\mathrm{im}}$, on a : $v^* = -v$. Donc :

$$uu^* = ((\cos(\theta))E + (\sin(\theta))v)\,((\cos(\theta))E - (\sin(\theta))v) = (\cos(\theta))^2 E - (\sin(\theta))^2 v^2.$$

De plus, toujours parce que $v \in \mathbb{H}^{\mathrm{im}}$, on sait grâce à la question 3.(b) que : $v^2 = -\mathrm{N}(v)E$, et $\mathrm{N}(v) = 1$ parce que v appartient à S. Donc finalement :

$$uu^* = \left((\cos(\theta))^2 + (\sin(\theta))^2\right) E = E.$$

Ceci montre à la fois que $u \in S$ (puisque $\mathrm{N}(u)E = uu^* = E$, ce qui équivaut à $\mathrm{N}(u) = 1$) et que : $u^{-1} = u^* = (\cos(\theta))E - (\sin(\theta))v$. D'où le résultat.

(b) Rappelons que la question 5.(b) assure effectivement que (v, w, vw) est une base orthonormée directe. Pour obtenir la matrice de C_u dans cette base, on doit exprimer :

$$C_u(v) = uvu^{-1}, \quad C_u(w) = uwu^{-1}, \quad C_u(vw) = uvwu^{-1}.$$

en fonction de v, w et vw. Nous aurons besoin de quelques calculs effectués dans la question précédente. On a montré que $v^2 = -E$, et par le même argument : $w^2 = -E$. Enfin, on a montré que : $u^{-1} = u^* = (\cos(\theta))E - (\sin(\theta))v$. Donc :

$$\begin{aligned} C_u(v) &= (\cos(\theta)E + \sin(\theta)v)\, v\, (\cos(\theta)E - \sin(\theta)v) \\ &= (\cos(\theta)v - \sin(\theta)E)\,(\cos(\theta)E - \sin(\theta)v) \\ &= \cos(\theta)\sin(\theta)\left(-v^2 - E\right) + \left((\cos(\theta))^2 + (\sin(\theta))^2\right) v \\ &= v. \end{aligned}$$

Ensuite, comme v et w sont orthogonaux, on a $vw = -wv$ d'après la question 5.(a), donc :

$$\begin{aligned} C_u(w) &= (\cos(\theta)w + \sin(\theta)vw)\,(\cos(\theta)E - \sin(\theta)v) \\ &= (\cos(\theta))^2 w - \cos(\theta)\sin(\theta)wv + \sin(\theta)\cos(\theta)vw - (\sin(\theta))^2 vwv \\ &= (\cos(\theta))^2 w + 2\cos(\theta)\sin(\theta)vw + (\sin(\theta))^2 wv^2 && (v \perp w) \\ &= \left((\cos(\theta))^2 - (\sin(\theta))^2\right) w + 2\cos(\theta)\sin(\theta)vw && (v^2 = -E) \\ &= \cos(2\theta)w + \sin(2\theta)vw. \end{aligned}$$

Pour en déduire $C_u(vw)$, on peut se dispenser de faire un calcul analogue, en écrivant :

$$C_u(vw) = uvu^{-1}uwu^{-1} = C_u(v)C_u(w) = v\,(\cos(2\theta)w + \sin(2\theta)vw) = -\sin(2\theta)w + \cos(2\theta)vw.$$

Finalement :

$$\mathrm{M}_{(v,w,vw)}(C_u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\theta) & -\sin(2\theta) \\ 0 & \sin(2\theta) & \cos(2\theta) \end{pmatrix}.$$

On reconnaît une matrice de rotation, d'axe orienté et dirigé par v, de mesure d'angle 2θ.

Remarque. Il n'est pas étonnant de trouver une matrice de rotation. On pouvait le démontrer *a priori* en utilisant le fait que $\alpha(u,u) \in \mathrm{SO}(\mathbb{H})$, puis en écrivant que la matrice de $\alpha(u,u)$ dans la base orthonormée (E, v, w, vw) de $\mathbb{H} = \mathbb{R}_{\mathbb{H}} \oplus \mathbb{H}^{\mathrm{im}}$ est de la forme :

$$\begin{pmatrix} 1 & 0_{\mathrm{M}_{1,3}(\mathbb{R})} \\ 0_{\mathrm{M}_{3,1}(\mathbb{R})} & \mathrm{M}_{(v,w,vw)}(C_u) \end{pmatrix},$$

on trouve : $1 = \det(\alpha(u,u)) = 1 \times \det(C_u)$, donc C_u, qui est une isométrie puisqu'elle s'obtient à partir de l'isométrie $\alpha(u,u)$ par restriction à $\mathbb{H}^{\mathrm{im}}$, est aussi de déterminant 1 : c'est une matrice de rotation de $\mathbb{H}^{\mathrm{im}}$.

9. Pour tout $(u, u') \in S^2$, on a :

$$C_{u\cdot u'} = \alpha(uu', uu') \overset{(q.6)}{=} \alpha(u,u) \circ \alpha(u',u') = C_u \circ C_{u'},$$

donc l'application $u \mapsto C_u$ induit bien un morphisme de groupes de S dans $\mathrm{SO}(\mathbb{H}^{\mathrm{im}})$. On veut montrer qu'il est surjectif et décrire son noyau. Soit $R \in \mathrm{SO}(\mathbb{H}^{\mathrm{im}})$. Appelons v un vecteur qui oriente son axe et $\vartheta \in \mathbb{R}$ une mesure d'angle de R. Si l'on pose : $u = \left(\cos\left(\frac{\vartheta}{2}\right)\right)E + \left(\sin\left(\frac{\vartheta}{2}\right)\right)v \in S$, et si w est un vecteur de $\mathbb{H}^{\mathrm{im}} \cap S$ orthogonal à v, alors d'après la question précédente on a :

$$\mathrm{M}_{(v,w,vw)}(C_u) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\left(2\frac{\vartheta}{2}\right) & -\sin\left(2\frac{\vartheta}{2}\right) \\ 0 & \sin\left(2\frac{\vartheta}{2}\right) & \cos\left(2\frac{\vartheta}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\vartheta) & -\sin(\vartheta) \\ 0 & \sin(\vartheta) & \cos(\vartheta) \end{pmatrix} = \mathrm{M}_{(v,w,vw)}(R).$$

Pour la dernière égalité, on utilise le fait que la matrice d'une rotation d'un espace euclidien de dimension 3 soit la même dans toute base orthonormée directe dont le premier vecteur v oriente l'axe et les deux autres vecteurs forment une base orthonormée directe de $v^\perp$ (ce qui est le cas ici, vu que w et vw sont unitaires et orthogonaux à v et entre eux). Deux endomorphismes ayant la même matrice dans une base donnée sont égaux, donc : $C_u = R$. Ceci montre que l'application $u \mapsto C_u$ est une surjection de S dans $\mathrm{SO}(\mathbb{H}^{\mathrm{im}})$.

Déterminons enfin son noyau. On imite le raisonnement de la question 6. Soit $u \in S$. Alors u appartient au noyau de $u \mapsto C_u$ si et seulement si :

$$C_u = \mathrm{id}_{\mathbb{H}^{\mathrm{im}}} \iff \begin{cases} uI &= Iu \\ uJ &= Ju \\ uK &= Ku \end{cases} \iff \forall Z \in \mathbb{H},\ uZ = Zu \overset{(q.1.(c))}{\iff} u \in \mathbb{R}_{\mathbb{H}} \cap S = \{-E, E\}.$$

Le noyau de $u \mapsto C_u$ est donc $\{-E, E\}$, ce qui achève la résolution de cette question.

10. (a) Il a déjà été démontré l'inclusion $\alpha(S \times S) \subseteq \mathrm{SO}(\mathbb{H})$ dans la question 7. Au tour de l'inclusion réciproque. Soit R un élément de $\mathrm{SO}(\mathbb{H})$.

Si $R(E) = E$, alors R laisse stable $\mathbb{R}_{\mathbb{H}}$ et donc son supplémentaire orthogonal $\mathbb{H}^{\mathrm{im}}$ également (parce que R est une isométrie). Par la question précédente il existe $u \in S$ tel que : $R_{|\mathbb{H}^{\mathrm{im}}} = C_u = \alpha(u,u)_{|\mathbb{H}^{\mathrm{im}}}$. On vérifie que $\alpha(u,u)$ et R coïncident également sur $\mathbb{R}_{\mathbb{H}}$ (en effet on a trivialement : $\alpha(u,u)(E) = uEu^{-1} = E = R(E)$, donc par linéarité les deux applications coïncident sur $\mathbb{R}_{\mathbb{H}}$), donc elles coïncident sur $\mathbb{H} = \mathbb{R}_{\mathbb{H}} \oplus \mathbb{H}^{\mathrm{im}}$. On a montré que si $R(E) = E$, alors : $R = \alpha(u,u) \in \alpha(S,S)$.

Supposons à présent que R est une isométrie directe quelconque, et soit $v = R(E)$ (notons que v appartient à S car R conserve la norme). Nous allons nous ramener au cas précédent. Considérons :

$$R' = \alpha(E,v) \circ R.$$

C'est une composition d'isométries directes par la question 7, donc c'est une isométrie directe. On a de plus :

$$R'(E) = \alpha(E,v)(v) = Evv^{-1} = E,$$

donc R' vérifie : $R'(E) = E$. Par le premier cas traité ci-dessus, il existe $u' \in S$ tel que : $R' = \alpha(u',u')$. On en déduit R en écrivant :

$$R = \alpha(E,v)^{-1} \circ R' = \alpha(E,v^{-1}) \circ \alpha(u',u') = \alpha(u', v^{-1}u') \in \alpha(S \times S).$$

On a donc, dans tous les cas : $R \in \alpha(S \times S)$, ce qui prouve : $\mathrm{SO}(\mathbb{H}) \subseteq \alpha(S \times S)$. Ayant la double inclusion, on a montré :

$$\alpha(S \times S) = \mathrm{SO}(\mathbb{H}).$$

(b) Il est clair que $S \times \{E\}$ est un groupe puisque S et $\{E\}$ en sont. L'image par un morphisme d'un sous-groupe est encore un sous-groupe, donc $N = \alpha(S \times \{E\})$ est un sous-groupe de $\mathrm{SO}(\mathbb{H})$. Soient $n \in N$ et $g \in \mathrm{SO}(\mathbb{H})$. Montrons : $gng^{-1} \in N$. Comme $n \in N$, il existe $u \in S$ tel que : $n = \alpha(u,E)$. Par la question précédente, il existe aussi $(v,w) \in S^2$ tel que : $g = \alpha(v,w)$. Alors, par propriété de morphisme de α :

$$gng^{-1} = \alpha(v,w) \circ \alpha(u,E) \circ \alpha(v^{-1},w^{-1}) = \alpha(vuv^{-1}, ww^{-1}) = \alpha(vuv^{-1}, E) \in N,$$

d'où le résultat. Il reste à montrer :

$$\{\pm \mathrm{id}_{\mathbb{H}}\} \subsetneq N \subsetneq \mathrm{SO}(\mathbb{H}).$$

Chaque inclusion est aisée à obtenir : pour N c'est conséquence directe de la définition (et du fait que l'image de α soit dans $\mathrm{SO}(\mathbb{H})$), et pour la première inclusion il suffit de remarquer que $\mathrm{id}_{\mathbb{H}} = \alpha(E,E) \in N$ et $-\mathrm{id}_{\mathbb{H}} = \alpha(-E,E) \in N$. Le reste du travail consiste à montrer que ces inclusions ne sont pas des égalités.

Soit $g = \alpha(E,I)$. Alors $g \in \mathrm{SO}(\mathbb{H})$, mais $g \notin N$. En effet, si c'était le cas, alors il existerait $u \in S$ tel que : $\alpha(E,I) = \alpha(u,E)$, et donc : $\alpha(u^{-1},I) = \mathrm{id}_{\mathbb{H}}$. Ainsi : $(u^{-1},I) \in \ker(\alpha) = \{(E,E),(-E,-E)\}$, ce qui est impossible car $I \neq \pm E$. Ainsi $N \neq \mathrm{SO}(\mathbb{H})$.

Enfin, soit $n = \alpha(I,E)$. Alors $n \in N$, mais : $\forall Z \in \mathbb{H}$, $n(Z) = IZ$, qui n'est pas égal à $\mathrm{id}_{\mathbb{H}}$ ni $-\mathrm{id}_{\mathbb{H}}$ (puisque $n(I) = I^2 = -E \neq \pm I$). Ainsi : $\{\pm \mathrm{id}\} \neq N$.

Ceci achève de démontrer que l'on a : $\{\pm \mathrm{id}\} \subsetneq N \subsetneq \mathrm{SO}(\mathbb{H})$.

11. Montrons que $\mathrm{Aut}(\mathbb{H})$ est un sous-groupe de $\mathrm{GL}(\mathbb{H})$. Il est clair que $\mathrm{id}_{\mathbb{H}}$ appartient bien à $\mathrm{Aut}(\mathbb{H})$ et que $\mathrm{Aut}(\mathbb{H})$ est inclus dans $\mathrm{GL}(\mathbb{H})$ (en effet les éléments de $\mathrm{Aut}(\mathbb{H})$ sont supposés être $\mathbb{R}$-linéaires et bijectifs).

Soit $(f,g) \in \mathrm{Aut}(\mathbb{H})$. Alors g^{-1} existe car g est dans $\mathrm{GL}(\mathbb{H})$, et est $\mathbb{R}$-linéaire et bijective comme g. De plus :

$$\forall (Z,Z') \in \mathbb{H}^2, \quad ZZ' = g(g^{-1}(Z))g(g^{-1}(Z')) = g(g^{-1}(Z)g^{-1}(Z'))$$

car g est dans $\mathrm{Aut}(\mathbb{H})$. En composant par g^{-1}, on en déduit : $g^{-1}(ZZ') = g^{-1}(Z)g^{-1}(Z')$.
Enfin, $f \circ g$ est $\mathbb{R}$-linéaire et bijectif parce que f et g le sont, et on sait déjà que $\mathrm{GL}(\mathbb{H})$ est un groupe. De plus :

$$\forall (Z,Z') \in \mathbb{H}^2, \quad f\circ g(ZZ') = f\left(g(ZZ')\right) = f(g(Z)g(Z')) = f(g(Z))f(g(Z')) = f\circ g(Z) f\circ g(Z'),$$

ce qui achève de démontrer que $f \circ g \in \mathrm{Aut}(\mathbb{H})$. Ainsi cet ensemble est non vide, stable par produit et inversion, et inclus dans $\mathrm{GL}(\mathbb{H})$: c'est bien un sous-groupe de $\mathrm{GL}(\mathbb{H})$.
Vérifions à présent que $\alpha(u,u)$ appartient à $\mathrm{Aut}(\mathbb{H})$ pour tout $u \in S$. Soit $u \in S$. On a :

$$\begin{aligned} \forall (Z,Z') \in \mathbb{H}^2, \quad \alpha(u,u)(ZZ') &= uZZ'u^{-1} \\ &= uZu^{-1}uZ'u^{-1} \\ &= \alpha(u,u)(Z)\alpha(u,u)(Z') \end{aligned}$$

donc $\alpha(u,u)$ est un automorphisme de $\mathbb{H}$ (on sait déjà que $\alpha(u,u)$ est bijectif et $\mathbb{R}$-linéaire par définition, donc seule la multiplicativité restait à démontrer). D'où le résultat.

12. Soit $f \in \mathrm{Aut}(\mathbb{H})$. Montrons d'abord que $f(I)$ et $f(J)$ sont dans $\mathbb{H}^{\mathrm{im}} \cap S$ et orthogonaux. On a : $(f(I))^2 = f(I^2) = f(-E) = -E$ (la dernière égalité découle du fait que $f_{|\mathbb{R}_\mathbb{H}} = \mathrm{id}_{\mathbb{R}_\mathbb{H}}$), et de même $(f(J))^2 = -E$, donc $f(I)$ et $f(J)$ sont dans $\mathbb{H}^{\mathrm{im}}$ par la question 3.(b), et de norme 1 car $\left(\mathrm{N}(f(I))\right)^2 = \mathrm{N}\left((f(I))^2\right) = \mathrm{N}(-E) = 1$ (de même pour $f(J)$). Ils sont donc bien dans $\mathbb{H}^{\mathrm{im}} \cap S$: vérifions qu'ils sont orthogonaux. C'est immédiat en écrivant :

$$f(I)f(J) + f(J)f(I) = f(IJ) + f(JI) = f(IJ + JI) = f\left(0_{\mathbb{R}_\mathbb{H}}\right) = 0_{\mathbb{R}_\mathbb{H}}$$

et en utilisant la question 5.(a). Alors, par la question 5.(b), la famille $(f(I), f(J), f(I)f(J))$ est une base orthonormée directe de $\mathbb{H}^{\mathrm{im}}$. Or : $f(I)f(J) = f(IJ) = f(K)$, d'où le résultat.

13. (a) La question précédente montre que si $f \in \mathrm{Aut}(\mathbb{H})$, alors f transforme une base orthonormée directe de $\mathbb{H}^{\mathrm{im}}$ en une base orthonormée directe de $\mathbb{H}^{\mathrm{im}}$, ce qui prouve en même temps la stabilité par f de $\mathbb{H}^{\mathrm{im}}$ et le fait que f induise une isométrie directe de cet espace vectoriel, c'est-à-dire un élément de $\mathrm{SO}(\mathbb{H}^{\mathrm{im}})$. L'application de restriction :

$$r : \begin{cases} \mathrm{Aut}(\mathbb{H}) & \to & \mathrm{SO}(\mathbb{H}^{\mathrm{im}}) \\ f & \mapsto & f_{|\mathbb{H}^{\mathrm{im}}} \end{cases}$$

est donc correctement définie, et il est facile de se convaincre que c'est un morphisme de groupes. Elle est injective puisque de noyau trivial : si $r(f) = \mathrm{id}_{\mathbb{H}^{\mathrm{im}}}$, alors l'image par f de la base (I,J,K) est elle-même, mais on a aussi $f(E) = E$ puisque $f_{|\mathbb{R}_\mathbb{H}} = \mathrm{id}_{\mathbb{R}_\mathbb{H}}$, donc f coïncide avec l'identité sur (E,I,J,K) et on en déduit : $f = \mathrm{id}_\mathbb{H}$.
Justifions qu'elle est surjective : soit R un élément de $\mathrm{SO}(\mathbb{H}^{\mathrm{im}})$, et soit f l'unique endomorphisme du $\mathbb{R}$-espace vectoriel $\mathbb{H} = \mathbb{R}_\mathbb{H} \oplus \mathbb{H}^{\mathrm{im}}$ défini par : $f_{|\mathbb{R}_\mathbb{H}} = \mathrm{id}_{\mathbb{R}_\mathbb{H}}$, et : $f_{|\mathbb{H}^{\mathrm{im}}} = R$. Vérifions que f est un automorphisme de $\mathbb{H}$. C'est évidement une application $\mathbb{R}$-linéaire par construction : nous devons vérifier que f est bijective et que : $\forall (u,v) \in \mathbb{H}^2$, $f(uv) = f(u)f(v)$. La bijectivité est facile, par exemple par un calcul de déterminant dans une base adaptée à $\mathbb{H} = \mathbb{R}_\mathbb{H} \oplus \mathbb{H}^{\mathrm{im}}$. On obtient alors : $\det(f) = \det(\mathrm{id}_{\mathbb{R}_\mathbb{H}})\det(R) = 1 \neq 0$. Mieux : puisque f induit une isométrie sur deux sous-espaces supplémentaires, c'est une isométrie de $\mathbb{H}$, directe par le calcul de déterminant qui précède, donc c'est un élément de $\mathrm{SO}(\mathbb{H})$. Par la

question 10.(a), il existe donc $(u,v) \in S \times S$ tel que : $f = \alpha(u,v)$. Et comme : $f_{|\mathbb{R}_\mathbb{H}} = \mathrm{id}_{\mathbb{R}_\mathbb{H}}$, on doit avoir :

$$\forall Z \in \mathbb{R}_\mathbb{H}, \quad f(Z) = Z = \alpha(u,v)(Z) = uZv^{-1},$$

ce qui n'est possible que si : $u = v$ (prendre $Z = E$ pour s'en convaincre). Alors $f = \alpha(u,u)$ est un automorphisme de $\mathbb{H}$ d'après la question 11. On a bien montré que pour tout $R \in \mathrm{SO}(\mathbb{H}^{\mathrm{im}})$, il existe $f \in \mathrm{Aut}(\mathbb{H})$ tel que $R = f_{|\mathbb{H}^{\mathrm{im}}} = r(f)$. Donc r est injective et surjective : c'est un morphisme de groupes bijectif, donc un isomorphisme :

$$\mathrm{Aut}(\mathbb{H}) \simeq \mathrm{SO}(\mathbb{H}^{\mathrm{im}}).$$

D'où le résultat.

(b) On reprend le raisonnement de la question précédente. Soit $f \in \mathrm{Aut}(\mathbb{H})$. Comme : $f_{|\mathbb{R}_\mathbb{H}} = \mathrm{id}_{\mathbb{R}_\mathbb{H}}$, et : $f_{|\mathbb{H}^{\mathrm{im}}} \in \mathrm{SO}(\mathbb{H}^{\mathrm{im}})$ (par l'isomorphisme précédent), f est une isométrie directe de $\mathbb{H}$, donc par la question 10.(a) il existe $(u,v) \in S \times S$ tel que : $f = \alpha(u,v)$, et par le raisonnement ci-dessus on a : $u = v$. D'où : $f = \alpha(u,u)$. Réciproquement, si $u \in S$ alors $\alpha(u,u)$ est un automorphisme de $\mathbb{H}$ d'après la question 11. D'où :

$$\mathrm{Aut}(\mathbb{H}) = \{\alpha(u,u) \mid u \in S\}.$$

3 Normes euclidiennes sur $\mathbb{R}^2$

14. (a) On a :

$$\mathcal{K} = \bigcap_{x \in \mathbb{R}^2} \{A \in \mathrm{M}_2(\mathbb{R}) \mid \|x\|_2 \geqslant \|Ax\|\}.$$

Pour tout $x \in \mathbb{R}^2$, montrons que $\mathcal{K}_x = \{A \in \mathrm{M}_2(\mathbb{R}) \mid \|x\|_2 \geqslant \|Ax\|\}$ est fermé. Soit $x \in \mathbb{R}^2$, et soit f l'application $f : A \mapsto \|Ax\|$. On a : $\mathcal{K}_x = f^{-1}(]-\infty, \|x\|_2])$, et $]-\infty, \|x\|_2]$ est fermé dans $\mathbb{R}$. Montrons que f est continue sur $\mathbb{R}^2$. La norme $\|\cdot\|$ est 1-lipschitzienne donc continue sur $\mathbb{R}^2$, et $A \mapsto Ax$ est continue car linéaire sur $\mathrm{M}_2(\mathbb{R})$ qui est de dimension finie, et à valeurs dans $\mathbb{R}^2$. Par composition, f est continue sur $\mathrm{M}_2(\mathbb{R})$. En tant qu'image réciproque d'un fermé par une application continue, $\mathcal{K}_x$ est une partie fermée de $\mathrm{M}_2(\mathbb{R})$. Ainsi $\mathcal{K}$ est une intersection de fermés, donc c'est une partie fermée de $\mathrm{M}_2(\mathbb{R})$.
Montrons qu'elle est bornée. Soit N la norme de $\mathrm{M}_2(\mathbb{R})$ subordonnée à $\|\cdot\|$. Comme toutes les normes sont équivalentes sur $\mathbb{R}^2$, il existe $\alpha > 0$ tel que : $\|\cdot\|_2 \leqslant \alpha\|\cdot\|$. Alors, pour tout $x \in \mathbb{R}^2$ non nul et tout $A \in \mathcal{K}$, on a :

$$\frac{\|Ax\|}{\|x\|} \leqslant \frac{\|x\|_2}{\|x\|} \leqslant \alpha,$$

donc : $\forall A \in \mathcal{K}$, $\mathrm{N}(A) \leqslant \alpha$, ce qui montre que $\mathcal{K}$ est bornée. En tant que partie fermée et bornée, dans un espace vectoriel de dimension finie, $\mathcal{K}$ est une partie compacte de $\mathrm{M}_2(\mathbb{R})$.
Il reste à démontrer que $\mathcal{K}$ est une partie convexe de $\mathrm{M}_2(\mathbb{R})$. Soit $(A,B) \in \mathcal{K}^2$, et soit $t \in [0,1]$. Pour tout $x \in \mathbb{R}^2$, on a :

$$\|(tA + (1-t)B)x\| \leqslant |t|\|Ax\| + |1-t|\|Bx\| \leqslant t\|x\|_2 + (1-t)\|x\|_2 = \|x\|_2$$

donc $tA + (1-t)B \in \mathcal{K}$. Ceci vaut pour tout $(A,B) \in \mathcal{K}^2$ et tout $t \in [0,1]$, donc $\mathcal{K}$ est convexe.

(b) D'après la question précédente, $\mathcal{K}$ est une partie compacte de $\mathrm{M}_2(\mathbb{R})$, non vide puisque la matrice nulle y appartient trivialement. Comme le déterminant est continu sur $\mathrm{M}_2(K)$ (c'est une application polynomiale en les coefficients), donc sur $\mathcal{K}$, par le théorème des bornes atteintes il existe $A \in \mathcal{K}$ tel que : $\det(A) = \sup_{B \in \mathcal{K}} \det(B)$. D'où le résultat.

15. Pour montrer : $\det(A) > 0$, il suffit de montrer l'existence d'au moins une matrice de déterminant strictement positif dans $\mathcal{K}$. Rappelons que par équivalence des normes, il existe $\beta > 0$ tel que : $\|\cdot\| \leqslant \beta\|\cdot\|_2$. Posons alors : $A_0 = \frac{1}{\beta}\mathrm{I}_2$. On a :

$$\|A_0 x\| = \left\|\frac{1}{\beta}\mathrm{I}_2 x\right\| = \frac{1}{\beta}\|x\| \leqslant \|x\|_2,$$

donc $A_0 \in \mathcal{K}$, et on a : $\det(A_0) = \beta^{-2} > 0$. Donc : $\det(A) \geqslant \det(A_0) > 0$.
Pour montrer qu'il existe $x \in \mathcal{C}$ tel que : $\|Ax\| = 1$, notons d'abord que pour tout $x \in \mathcal{C}$ on a : $\|x\|_2 = 1$ (par définition) et : $\|Ax\| \leqslant 1$. Il s'agit de démontrer qu'un vecteur x réalise le cas d'égalité. Tout d'abord, la continuité de $x \mapsto \|Ax\|$ sur le compact $\mathcal{C}$ assure qu'il existe $m \in \mathbb{R}$ tel que : $\forall x \in \mathcal{C}$, $\|Ax\| \leqslant m$ (et de plus ce maximum est atteint). Montrons : $m = 1$. Pour cela, on raisonne par l'absurde : si $m \neq 1$, alors d'après ce qui précède on a même : $m < 1$. Posons donc : $A' = \frac{1}{m}A$. Alors, pour tout $x \in \mathbb{R}^2$ non nul, on a $\frac{x}{\|x\|_2} \in \mathcal{C}$, et donc :

$$\|A'x\| = \frac{1}{m}\|Ax\| = \frac{\|x\|_2}{m}\left\|A\frac{x}{\|x\|_2}\right\| \leqslant \frac{\|x\|_2}{m}\cdot m = \|x\|_2,$$

et cette égalité vaut trivialement aussi pour $x = 0$. Ainsi : $\forall x \in \mathbb{R}^2$, $\|A'x\| \leqslant \|x\|_2$, donc $A' \in \mathcal{K}$, et pourtant : $\det(A') = \frac{1}{m^2}\det(A) > \det(A)$, ce qui contredit la maximalité de $\det(A)$. Par l'absurde, on a montré que $m = 1$, et donc $x \mapsto \|Ax\|$ admet 1 pour maximum sur $\mathcal{C}$, et il est atteint. D'où l'existence de $x \in \mathcal{C}$ tel que $\|Ax\| = 1$.

16. (a) Pour alléger les notations, posons : $A' = AB$, et : $\forall r \in]0,1[$, $D_r = \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix}$. On note que $A' \in \mathcal{K}$, puisque $A \in \mathcal{K}$ et B préserve la norme euclidienne :

$$\forall x \in \mathbb{R}^2, \quad \|A'x\| = \|A(Bx)\| \leqslant \|Bx\|_2 = \|x\|_2.$$

Raisonnons par l'absurde. Supposons qu'il existe $r \in]0,1[$ tel que :

$$\forall x \in \mathcal{C}, \quad \|A'D_r x\| \leqslant 1.$$

Par homogénéité, pour un tel r la matrice $A'D_r$ vérifie donc : $\forall x \in \mathbb{R}^2$, $\|A'D_r x\| \leqslant \|x\|_2$, c'est-à-dire : $A'D_r \in \mathcal{K}$. Par convexité de $\mathcal{K}$, on a aussi : $\frac{1}{2}(A' + A'D_r) \in \mathcal{K}$. Comme $\det(A) = \sup_{B\in\mathcal{K}} \det(B)$, on a donc :

$$\det\left(\frac{1}{2}(A' + A'D_r)\right) \leqslant \det(A).$$

Or :

$$\begin{aligned}\det\left(\frac{1}{2}(A' + A'D_r)\right) &= \frac{1}{2^2}\det(A')\det(\mathrm{I}_2 + D_r) \\ &= \frac{1}{4}\det(A)\begin{vmatrix} 1+r & 0 \\ 0 & 1+\frac{1}{r}\end{vmatrix} \\ &= \frac{1}{4}\det(A)\left(2 + r + \frac{1}{r}\right),\end{aligned}$$

donc, en divisant l'inégalité ci-dessus par $\det(A) > 0$, et en faisant quelques menus arrangements, on obtient :

$$r + \frac{1}{r} \leqslant 2.$$

Or, pour $r<1$, on a : $r+\dfrac{1}{r}=\dfrac{r^2+1}{r}=\dfrac{(r-1)^2+2r}{r}>2$, donc l'inégalité ci-dessus est impossible.

Ce raisonnement par l'absurde montre que pour tout $r\in]0,1[$, il existe $x_r\in\mathcal{C}$ tel que : $\|A'D_rx_r\|>1$. Ce qu'il fallait démontrer.

(b) Soit $r\in]0,1[$. On reprend les notations de la question précédente. Comme $A'\in\mathcal{K}$, on a :

$$1<\|A'D_rx_r\|^2\leqslant(\|D_rx_r\|_2)^2=\left(\left\|\left(ry_r,\frac{z_r}{r}\right)\right\|_2\right)^2=(ry_r)^2+\left(\frac{z_r}{r}\right)^2.$$

Or (y_r,z_r) appartient à $\mathcal{C}$, donc : $y_r^2=1-z_r^2$. Partant de là, on montre facilement qu'on a :

$$\left(\frac{1}{r^2}-r^2\right)z_r^2>1-r^2,$$

et en divisant par $\dfrac{1}{r^2}-r^2=\dfrac{1-r^4}{r^2}>0$ on a le résultat voulu :

$$z_r^2>r^2\frac{1-r^2}{1-r^4}=r^2\frac{1}{1+r^2}.$$

17. Grâce aux questions précédentes, nous allons construire un autre point que $(\pm1,0)$ dans $\mathcal{C}$ et vérifiant $\|Ax\|=1$. Posons : $\forall n\in\mathbb{N}$, $r_n=1-\frac{1}{n+1}$. La suite $(x_{r_n})_{n\in\mathbb{N}}$ est à valeurs dans $\mathcal{C}$, qui est compact, donc elle admet une sous-suite convergente. Pour ne pas alourdir les notations, notons toujours $(x_{r_n})_{n\in\mathbb{N}}$ cette suite extraite convergente. Soit $\ell\in\mathcal{C}$ sa limite. Par construction des x_r, on a : $\forall n\in\mathbb{N}$, $\|A'D_{r_n}x_{r_n}\|>1$. Or : $\lim\limits_{n\to+\infty}D_{r_n}=\mathrm{I}_2$ et donc, par continuité du produit matriciel : $\lim\limits_{n\to+\infty}A'D_{r_n}x_{r_n}=A'\ell$. Par continuité de la norme, l'inégalité précédente devient, quand $n\to+\infty$: $\|A'\ell\|\geqslant1$. Or $A'\in\mathcal{K}$ et $\ell\in\mathcal{C}$, donc on a aussi : $\|A'\ell\|\leqslant1$. En conclusion : $\|A'\ell\|=1$.

Ainsi on peut poser $e_1=x$ et $e_2=\ell$. On a bien : $\|Ae_1\|=\|e_1\|_2=1$, et : $\|Ae_2\|=\|e_2\|_2=1$. Justifions que (e_1,e_2) est une base de $\mathbb{R}^2$; pour une raison de cardinal, il suffit de démontrer que c'est une famille libre. Or on a montré, dans la question précédente : $\forall n\in\mathbb{N}$, $z_{r_n}^2>\frac{r_n^2}{1+r_n^2}$. Quand $n\to+\infty$, la suite $(z_{r_n})_{n\in\mathbb{N}}$ ayant bien une limite vu que $(x_{r_n})_{n\in\mathbb{N}}$ en admet une (et la convergence dans un espace vectoriel réel de dimension finie équivaut à la convergence coordonnée par coordonnée), on a : $\lim\limits_{n\to+\infty}z_{r_n}^2\geqslant\frac{1}{2}$. En particulier : $\lim\limits_{n\to+\infty}z_{r_n}\neq0$, donc $e_1=x=(1,0)$ et $e_2=\ell=\left(\lim\limits_{n\to+\infty}y_n,\lim\limits_{n\to+\infty}z_n\right)$ ne peuvent pas être linéairement dépendants.

D'où le résultat : il existe une base (e_1,e_2) de $\mathbb{R}^2$ telle que : $\|Ax\|=\|x\|_2$ pour $x\in\{e_1,e_2\}$.

18. Par hypothèse, on a : $T\subseteq\mathcal{C}$. Montrons l'inclusion réciproque. Soit $c\in\mathcal{C}$. Nous allons obtenir c comme suite d'éléments de T par passage à la limite. Pour cela, observons d'abord comment fabriquer des suites d'éléments de $\mathcal{C}$.

Par commodité, nous raisonnons ci-dessous dans le plan complexe.

Pour tout $a\in T$, notons $z_a\in\mathbb{C}$ l'affixe de a, et soit : $T_{\mathbb{C}}=\{z_a\mid a\in T\}$. Soient $a,b\in T$ tels que $b\neq\pm a$. Comme $a,b\in T\subseteq\mathcal{C}$, il existe $(\theta_a,\theta_b)\in\mathbb{R}^2$ tel que : $z_a=e^{i\theta_a}$, $z_b=e^{i\theta_b}$. Alors : $z_b+z_a=2e^{i\frac{\theta_b+\theta_a}{2}}\cos\left(\frac{\theta_b-\theta_a}{2}\right)$, et : $z_b-z_a=2ie^{i\frac{\theta_b+\theta_a}{2}}\sin\left(\frac{\theta_b-\theta_a}{2}\right)$. Comme, par hypothèse, $\frac{b+a}{\|b+a\|_2}$ et $\frac{b-a}{\|b-a\|_2}$ sont dans T (et donc $\frac{a-b}{\|b-a\|_2}$ aussi, puisque a et b jouent des rôles symétriques), on a :

$$\frac{z_b+z_a}{|z_b+z_a|}=\frac{\cos\left(\frac{\theta_b-\theta_a}{2}\right)}{\left|\cos\left(\frac{\theta_b-\theta_a}{2}\right)\right|}e^{i\frac{\theta_b+\theta_a}{2}}\in T_{\mathbb{C}},\quad\pm\frac{z_b-z_a}{|z_b-z_a|}=e^{i\frac{\theta_b+\theta_a}{2}+\frac{\pi}{2}}\in T_{\mathbb{C}},\quad-e^{i\frac{\theta_b+\theta_a}{2}+\frac{\pi}{2}}\in T_{\mathbb{C}}.\quad(8)$$

Si $\theta_b - \theta_a \in [-\pi, \pi]$, alors la première appartenance devient simplement : $e^{i\frac{\theta_b+\theta_a}{2}} \in T_{\mathbb{C}}$. Dans la construction d'une suite ci-dessous, nous serons systématiquement dans cette configuration.

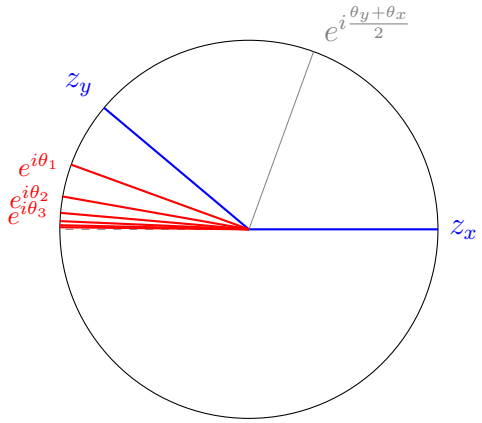
Revenons à notre question initiale. Quitte à remplacer $T_{\mathbb{C}}$ par $z_x^{-1}T_{\mathbb{C}}$ (qui, on le montrerait aisément, vérifie exactement les mêmes hypothèses que $T_{\mathbb{C}}$, et est égal à $\mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ si et seulement si $T_{\mathbb{C}}$ l'est), on peut supposer : $z_x = 1$. Soit $\theta_y \in \mathbb{R}$ un argument de z_y. Partant de là, on peut déjà démontrer que $-z_x = -1$ est dans T. Posons en effet :

$$\theta_0 = \theta_y, \quad \text{et :} \quad \forall n \in \mathbb{N}, \quad \theta_{n+1} = \frac{\theta_n}{2} + \frac{\pi}{2}.$$

D'après la seconde appartenance de (8), on a $e^{i\theta_n} \in T_{\mathbb{C}}$ pour tout $n \in \mathbb{N}$ (récurrence facile : prendre $\theta_a = 0$ et $\theta_b = \theta_n$ dans l'hérédité). Or $(\theta_n)_{n\in\mathbb{N}}$ est une suite arithmético-géométrique dont l'explicitation donne :

$$\exists a \in \mathbb{R},\ \forall n \in \mathbb{N}, \quad \theta_n = \frac{a}{2^n} + \pi,$$

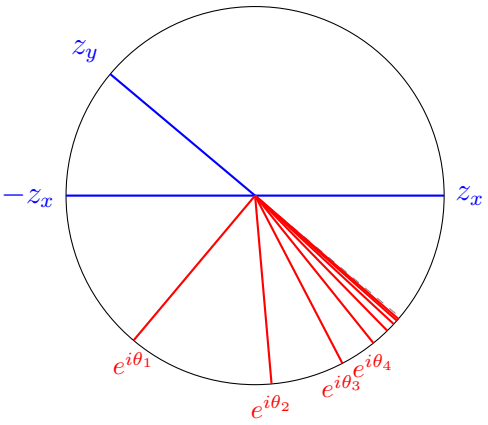
donc : $\lim\limits_{n\to+\infty} \theta_n = \pi$. Par continuité de l'exponentielle, on a donc : $\lim\limits_{n\to+\infty} e^{i\theta_n} = e^{i\pi} = -1$. Or $T_{\mathbb{C}}$ est fermé parce que T l'est (et $T_{\mathbb{C}}$ est l'image réciproque de T par l'application continue $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$), donc : $-1 \in T_{\mathbb{C}}$.



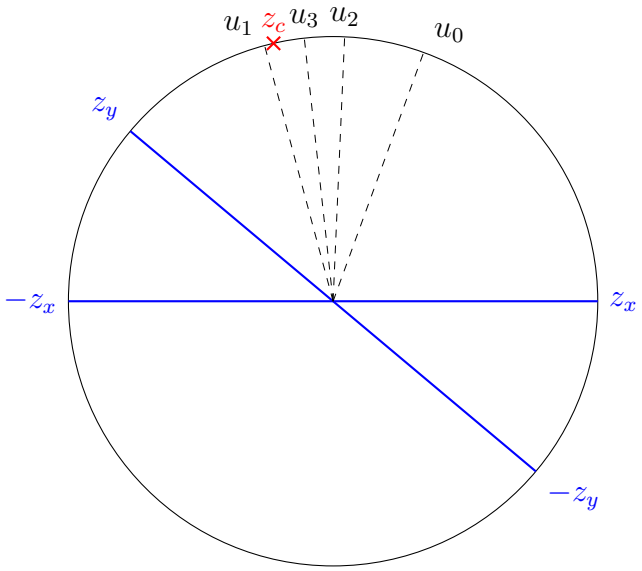
Le même raisonnement, en prenant :

$$\theta_0 = \pi, \quad \text{et :} \quad \forall n \in \mathbb{N}, \quad \theta_{n+1} = \frac{\theta_y + \theta_n}{2} + \frac{\pi}{2}$$

donne : $\forall n \in \mathbb{N}$, $e^{i\theta_n} \in T_{\mathbb{C}}$, et cette fois : $\lim\limits_{n\to+\infty} e^{i\theta_n} = e^{i(\pi+\theta_y)} = -z_y \in T_{\mathbb{C}}$.



Ainsi $z_x = 1$, $-z_x = -1$, z_y et $-z_y$ sont dans $T_{\mathbb{C}}$.
On va maintenant obtenir c quelconque comme limite d'une suite à valeurs dans T. L'intérêt d'avoir fait les deux cas particuliers ci-dessus est que nous pouvons, grâce aux quatre points de $T_{\mathbb{C}}$ ci-dessus, diviser le cercle unité en quartiers de sorte que : 1° z_c soit nécessairement dans l'un de ces quartiers, 2° l'angle entre c et au moins l'un des quatre points soit aigu, ce qui va faciliter la construction de la suite ci-dessous par dichotomie (en gros : on utilise la stabilité de $T_{\mathbb{C}}$ quand on fait la moyenne des arguments).



Faisons. Tous les arguments considérés ci-après ont leur représentant choisi dans $[-\pi, \pi]$. Quitte à échanger y et $-y$, on peut supposer qu'un argument de z_y est dans $]0, \pi[$. Soit θ_c un argument de z_c. Si c est égal à x, y, $-x$ ou $-y$, alors $c \in \mathcal{C}$ et il n'y a rien à démontrer. Sinon, θ_c appartient nécessairement à l'intérieur d'exactement l'un des quatre intervalles de la réunion $[-\pi, \pi] = [-\pi, -\theta_y] \cup [-\theta_y, 0] \cup [0, \theta_y] \cup [\theta_y, \pi]$. Notons $]a_0, b_0[$ celui de ces quatre intervalles auquel θ_c appartient ; comme c'est un intervalle de longueur au plus π (par hypothèse faite sur θ_y), θ_c est à distance au plus $\frac{\pi}{2}$ de l'une de ses deux extrémités. On pose alors :

$$(\vartheta_0, \phi_0) = \begin{cases} \left(a_0, \frac{a_0+b_0}{2}\right) & \text{si} \quad \theta_c - a_0 \leqslant \frac{\pi}{2}, \\ \left(\frac{a_0+b_0}{2}, b_0\right) & \text{si} \quad \theta_c - a_0 > \frac{\pi}{2}. \end{cases}$$

Par (8), on a dans les deux cas : $e^{i\vartheta_0} \in T_{\mathbb{C}}$, $e^{i\phi_0} \in T_{\mathbb{C}}$ (c'est ici qu'il était important de se ramener à des intervalles de longueur au plus π : pour bien avoir $e^{i\frac{a_0+b_0}{2}} \in T_{\mathbb{C}}$ et non $-e^{i\frac{a_0+b_0}{2}} \in T_{\mathbb{C}}$). Notons aussi que l'intervalle $[\vartheta_0, \phi_0]$ est de longueur au plus $\frac{\pi}{2}$. Ainsi ces deux réels vérifient les cinq propriétés suivantes (celles qui n'ont pas été démontrées sont faciles à obtenir) :

$$e^{i\vartheta_0} \neq \pm e^{i\phi_0}, \quad e^{i\vartheta_0} \in T_{\mathbb{C}}, \quad e^{i\phi_0} \in T_{\mathbb{C}}, \quad 0 \leqslant \phi_0 - \vartheta_0 \leqslant \frac{\pi}{2}, \quad \theta_c \in [\vartheta_0, \phi_0].$$

Soit $n \in \mathbb{N}$. Supposons avoir défini $(\vartheta_0, \phi_0), \ldots, (\vartheta_n, \phi_n)$, de sorte que l'on ait :

$$e^{i\vartheta_n} \neq \pm e^{i\phi_n}, \quad e^{i\vartheta_n} \in T_{\mathbb{C}}, \quad e^{i\phi_n} \in T_{\mathbb{C}}, \quad 0 \leqslant \phi_n - \vartheta_n \leqslant \frac{\pi}{2^{n+1}}, \quad \theta_c \in [\vartheta_n, \phi_n].$$

Comme l'intervalle $[\vartheta_n, \phi_n]$ est de longueur au plus $\frac{\pi}{2^{n+1}}$, le réel θ_c est à distance au plus $\frac{\pi}{2^{n+2}}$ d'une de ses extrémités. On pose :

$$(\vartheta_{n+1}, \phi_{n+1}) = \begin{cases} \left(\vartheta_n, \frac{\vartheta_n+\phi_n}{2}\right) & \text{si} \quad \theta_c - \vartheta_n \leqslant \frac{\pi}{2^{n+2}}, \\ \left(\frac{\vartheta_n+\phi_n}{2}, \phi_n\right) & \text{si} \quad \theta_c - \vartheta_n > \frac{\pi}{2^{n+2}}. \end{cases}$$

Par (8) et des raisonnements analogues à ceux ci-dessus, on a :

$$e^{i\vartheta_{n+1}} \neq \pm e^{i\phi_{n+1}}, \quad e^{i\vartheta_{n+1}} \in T_{\mathbb{C}}, \quad e^{i\phi_{n+1}} \in T_{\mathbb{C}}, \quad 0 \leqslant \phi_{n+1} - \vartheta_{n+1} \leqslant \frac{\pi}{2^{n+2}}, \quad \theta_c \in [\vartheta_{n+1}, \phi_{n+1}].$$

Par récurrence, on définit ainsi deux suites $(\vartheta_n)_{n\in\mathbb{N}}$ et $(\phi_n)_{n\in\mathbb{N}}$. On a alors :

$$\forall n \in \mathbb{N}, \quad 0 \leqslant \phi_n - \theta_c \leqslant \phi_n - \vartheta_n \leqslant \frac{\pi}{2^{n+1}}.$$

Les deux extrémités de cet encadrement convergent vers 0. Par le théorème des gendarmes : $\lim\limits_{n\to+\infty} e^{i\phi_n} = e^{i\theta_c}$. Or $e^{i\phi_n} \in T_{\mathbb{C}}$ pour tout $n \in \mathbb{N}$ et $T_{\mathbb{C}}$ est fermé, donc : $z_c = e^{i\theta_c} \in T_{\mathbb{C}}$. Ceci équivaut à $c \in T$, d'où le résultat : $\mathcal{C} \subseteq T$.

Ayant la double inclusion, on conclut : $T = \mathcal{C}$.

Remarque. Je pense qu'il est possible de reprendre la démonstration de la stabilité de $T_{\mathbb{C}}$ par passage à l'inverse pour en déduire que cet ensemble est stable par produit. Auquel cas il devient plus facile de conclure en utilisant le fait que les sous-groupes de $(\mathbb{R}, +)$ soient denses ou de la forme $a\mathbb{Z}$. On en déduit que les sous-groupes de $\mathbb{U}$ sont soit finis soit denses (la stabilité par $e^{i\theta} \mapsto \pm e^{\frac{i\theta}{2}}$ assurant qu'on ne peut être dans le premier cas), en passant par le morphisme $\theta \mapsto e^{i\theta}$. Ainsi $T_{\mathbb{C}}$ serait à la fois fermé et dense, donc : $T_{\mathbb{C}} = \mathbb{U}$.

Ces résultats sur les sous-groupes de $\mathbb{R}$ et $\mathbb{U}$ sont cependant hors-programme et il aurait fallu les redémontrer dans ce cas particulier : c'est pourquoi j'ai préféré opter pour le raisonnement ci-dessus, qui n'invoque aucun résultat sophistiqué (au prix d'une solution peu élégante).

19. Soit $\|\cdot\|$ une norme vérifiant l'hypothèse du théorème A, et soit A la matrice dont l'existence est démontrée par la question 14.(b). Par la question 17, il existe une base (e_1, e_2) de $\mathbb{R}^2$ telle que : $\|Ae_1\| = \|e_1\|_2$, et : $\|Ae_2\| = \|e_2\|_2$. Il s'agit de démontrer que ces deux égalités s'étendent à tout vecteur de $\mathbb{R}^2$. Étendons-la d'abord à tout vecteur de $\mathcal{C}$: nous aurons alors le cas général par homogénéité. Posons :

$$T = \{x \in \mathcal{C} \mid \|Ax\| = 1\} \subseteq \mathcal{C}.$$

C'est une partie fermée de $\mathcal{C}$, puisqu'elle est l'image réciproque de $\{1\}$ par l'application continue $x \mapsto \|Ax\|$ (la continuité de cette application découle de la continuité des normes et des applications linéaires en dimension finie), et elle contient au moins deux points (à savoir $\frac{1}{\|e_1\|_2}e_1$ et $\frac{1}{\|e_2\|_2}e_2$) qui ne sont pas égaux ni opposés, puisque (e_1, e_2) est libre. Montrons que T vérifie la propriété suivante :

$$\forall a \in T,\ \forall b \in T \setminus \{a, -a\}, \quad \frac{b-a}{\|b-a\|_2} \in T,\ \frac{b+a}{\|b+a\|_2} \in T.$$

C'est ici que l'hypothèse sur $\|\cdot\|$ va nous servir. Soient a et b dans T tels que $b \neq \pm a$. Il est clair que $\frac{b-a}{\|b-a\|_2}$ et $\frac{b+a}{\|b+a\|_2}$ sont dans $\mathcal{C}$. On veut montrer : $\left\|A\frac{b-a}{\|b-a\|_2}\right\| = 1$. Il revient au même de vouloir démontrer : $\|A(b-a)\| = \|b-a\|_2$. De même, on veut : $\|A(b+a)\| = \|b+a\|_2$. Toute l'étude de cette partie permet déjà de s'assurer qu'on a : $\|A(b-a)\| \leqslant \|b-a\|_2$, et : $\|A(b+a)\| \leqslant \|b+a\|_2$. On voudrait les inégalités inverses. Or, par hypothèse sur $\|\cdot\|$, appliquée à $x = Aa$ et $y = Ab$ qui sont de norme 1 pour $\|\cdot\|$:

$$\|A(b-a)\|^2 + \|A(b+a)\|^2 \geqslant 4,$$

mais on a aussi :

$$\|b-a\|_2^2 + \|b+a\|_2^2 = 2\left(\|b\|_2^2 + \|a\|_2^2\right) = 4,$$

donc :

$$\|A(b-a)\|^2 + \|A(b+a)\|^2 \geqslant \|b-a\|_2^2 + \|b+a\|_2^2,$$

ou encore :

$$\left(\|A(b-a)\|^2 - \|b-a\|_2^2\right) + \left(\|A(b+a)\|^2 - \|b+a\|_2^2\right) \geqslant 0.$$

Le membre de gauche est aussi négatif, d'après les inégalités rappelées plus haut. On en déduit que $\left(\|A(b-a)\|^2 - \|b-a\|_2^2\right)+\left(\|A(b+a)\|^2 - \|b+a\|_2^2\right)$ est nul. Or une somme de réels négatifs est nulle si et seulement si chaque terme est nul, donc :

$$\|A(b-a)\| = \|b-a\|_2, \quad \|A(b+a)\| = \|b+a\|_2,$$

ce qu'il fallait démontrer. Ainsi : $\frac{b-a}{\|b-a\|_2} \in T$, $\frac{b+a}{\|b+a\|_2} \in T$, donc T vérifie les hypothèses de la question précédente. On en déduit : $T = \mathcal{C}$. Autrement dit : $\forall x \in \mathcal{C}$, $\|Ax\| = 1$. Or pour tout $x \in \mathbb{R}^2$ non nul, on a $\frac{x}{\|x\|_2} \in \mathcal{C}$ donc, par homogénéité : $\|Ax\| = \|x\|_2$. Le résultat est aussi vrai pour $x = 0$, trivialement. Puisque cette égalité est vraie pour tout $x \in \mathbb{R}^2$, elle est aussi vraie en remplaçant x par $A^{-1}x$ (rappelons que A^{-1} existe puisque $\det(A) > 0$), donc :

$$\forall x \in \mathbb{R}^2, \quad \|x\| = \|A^{-1}x\|_2.$$

D'où le théorème A : $\|\cdot\|$ est la norme euclidienne associée au produit scalaire défini ainsi :

$$\forall (x,y) \in \mathbb{R}^2, \quad \langle x, y\rangle = \left(A^{-1}x \mid A^{-1}y\right),$$

où $(\cdot \mid \cdot)$ désigne le produit scalaire usuel sur $\mathbb{R}^2$.

4 Algèbres valuées

20. (a) Soit $x \in A$. Alors l'ensemble :

$$\{P \in \mathbb{R}[X] \mid P(x) = 0_A\}$$

est un idéal de $\mathbb{R}[X]$, non réduit à $0_{\mathbb{R}[X]}$ puisque A est algébrique (donc il existe bien $P \in \mathbb{R}[X]$ non nul tel que $P(x) = 0$), donc il admet un générateur $\pi_x \in \mathbb{R}[X]$ non nul. Puisque l'on a :

$$\{P \in \mathbb{R}[X] \mid P(x) = 0_A\} = (\pi_x),$$

alors en particulier :

$$\forall P \in \mathbb{R}[X], \quad (P(x) = 0_A \iff \pi_x | P)\,.$$

Montrons que π_x est de degré au plus 2 ; nous en déduirons aisément le résultat voulu.

Cela revient à démontrer que π_x est irréductible : en effet, on sait que les seuls polynômes irréductibles sur $\mathbb{R}[X]$ sont de degré 1 ou 2. Or, si π_x n'était pas irréductible, il existerait des polynômes non constants $P_1, P_2 \in \mathbb{R}[X]$ tels que : $\pi_x = P_1P_2$. En évaluant cette égalité en x, on aurait : $\pi_x(x) = 0_A = P_1(x)P_2(x)$. Or $P_1(x) \in A$ et $P_2(x) \in A$, et A est supposé sans diviseur de zéro, donc $P_1(x)P_2(x) = 0_A$ n'est possible que si $P_1(x) = 0_A$ ou $P_2(x) = 0_A$: d'après l'équivalence ci-dessus, π_x diviserait soit P_1 soit P_2, ce qui est impossible pour des raisons de degré. Par l'absurde, on a montré que π_x est un polynôme irréductible de $\mathbb{R}[X]$, et il est donc de degré 1 ou 2.

Déduisons-en : $x^2 \in \mathbb{R} + \mathbb{R}x$. Pour cela, il suffit d'effectuer la division euclidienne de X^2 par π_x, ce qui est possible puisque π_x est non nul : il existe $(Q, R) \in \mathbb{R}[X]^2$ tel que : $X^2 = \pi_x Q + R$, avec : $\deg(R) \leqslant \deg(\pi_x) - 1 \leqslant 1$. En évaluant cette égalité en x, on obtient : $x^2 = \pi_x(x)Q(x) + R(x) = R(x) \in \mathbb{R} + \mathbb{R}x$: d'où le résultat.

(b) Soit $x \in A\backslash\mathbb{R}$. Pour construire l'isomorphisme demandé, l'idée est de trouver un antécédent de i dans $\mathbb{R}+\mathbb{R}x$ (il suffit en effet de définir une application linéaire sur une base, donc sur $(1,i)$ par exemple). Comme un isomorphisme conserve tout ce qui est relatif à la structure de $\mathbb{R}$-algèbre, cet antécédent doit être une racine carrée de -1 dans A. C'est ce que nous allons chercher à construire dans ce qui suit.

On a : $x^2 \in \mathbb{R}+\mathbb{R}x$, d'après la question précédente. Soit, donc, $(a,b) \in \mathbb{R}^2$ tel que : $x^2 = b + ax$. On peut classiquement réécrire cette égalité ainsi :

$$\left(x - \frac{a}{2}\right)^2 = \frac{4b-a^2}{4}.$$

On a : $4b - a^2 < 0$, sinon on aurait : $x = \frac{a}{2} \pm \frac{\sqrt{4b-a^2}}{2} \in \mathbb{R}$, ce qui est faux par hypothèse (le fait que $u^2 = v^2$ implique $u = \pm v$ ne va pas de soi, et est faux si u et v ne commutent pas ; on utilise de plus le fait que A soit sans diviseur de zéro : ainsi $u^2 - v^2 = (u+v)(u-v) = 0$ implique $u + v = 0$ ou $u - v = 0$, l'identité remarquable étant valable si et seulement si $uv = vu$). En revanche $a^2 - 4b > 0$, ce qui permet d'écrire :

$$\left(\frac{2x-a}{\sqrt{a^2-4b}}\right)^2 = -1.$$

Posons : $x' = \dfrac{2x-a}{\sqrt{a^2-4b}}$, qui est un élément de A car $x \in A$, $\mathbb{R} \subseteq A$, et A est stable par produit et somme en tant qu'algèbre. Considérons l'application $\mathbb{R}$-linéaire de $\mathbb{C}$ dans $\mathbb{R}+\mathbb{R}x$ définie sur la $\mathbb{R}$-base $(1,i)$ de $\mathbb{C}$ par :

$$f(1) = 1, \quad f(i) = x'.$$

Montrons que f est un isomorphisme de $\mathbb{R}$-algèbres. Comme c'est une application $\mathbb{R}$-linéaire, il suffit de vérifier qu'elle est multiplicative et bijective.

Montrons qu'elle est multiplicative : soient $z = \alpha + i\beta \in \mathbb{C}$ et $z' = \alpha' + i\beta' \in \mathbb{C}$, avec $(\alpha, \beta, \alpha', \beta') \in \mathbb{R}^4$. On a d'une part, par $\mathbb{R}$-linéarité :

$$\begin{aligned} f(zz') = f(\alpha\alpha' - \beta\beta' + i(\alpha\beta' + \alpha'\beta)) &= (\alpha\alpha' - \beta\beta')f(1) + (\alpha\beta' + \alpha'\beta)f(i) \\ &= (\alpha\alpha' - \beta\beta') + (\alpha\beta' + \alpha'\beta)x', \end{aligned}$$

et d'autre part, par un calcul analogue :

$$f(z)f(z') = f(\alpha + i\beta)f(\alpha' + i\beta') = (\alpha + x'\beta)(\alpha' + x'\beta') = (\alpha\alpha' + \beta\beta'x'^2) + (\alpha\beta' + \alpha'\beta)x'.$$

Or, par construction : $x'^2 = -1$, d'où :

$$f(z)f(z') = (\alpha\alpha' - \beta\beta') + (\alpha\beta' + \alpha'\beta)x' = f(zz'),$$

donc f est multiplicative. On en déduit aisément qu'elle est de noyau réduit à 0_A : en effet, si $z \in \mathbb{C}^*$ vérifie : $f(z) = 0_A$, alors on a : $0_A = f(z)f\left(\frac{1}{z}\right) = f(1) = 1$, ce qui est absurde. Par conséquent seul $z = 0$ vérifie $f(z) = 0_A$, donc f est injective. Il reste à montrer qu'elle est surjective : soit $(a,b) \in \mathbb{R}^2$, montrons que $a + bx \in \mathbb{R}+\mathbb{R}x$ admet un antécédent par f. Nous avons :

$$x' = f(i) \iff \frac{2x-a}{\sqrt{a^2-4b}} = f(i) \iff x = \frac{\sqrt{a^2-4b}}{2}f(i) + \frac{a}{2} = f\left(\frac{i\sqrt{a^2-4b}+a}{2}\right),$$

ce qui montre que x admet $\frac{i\sqrt{a^2-4b}+a}{2}$ pour antécédent. Cela nous permet d'en déduire que l'application $\mathbb{R}$-linéaire de $\mathbb{R}+\mathbb{R}x$ dans $\mathbb{C}$ définie sur la $\mathbb{R}$-base $(1,x)$ de $\mathbb{R}+\mathbb{R}x$ par :

$$g(1)=1, \quad g(x)=\frac{i\sqrt{a^2-4b}+a}{2}$$

vérifie : $f\circ g = \mathrm{id}_{\mathbb{R}+\mathbb{R}x}$ (c'est vrai sur une base, donc c'est vrai partout), donc f est surjective.

Ainsi il existe bien un morphisme de $\mathbb{R}$-algèbres bijectif de $\mathbb{C}$ dans $\mathbb{R}+\mathbb{R}x$, donc ces deux algèbres sont isomorphes.

Remarque. Nous n'avons pas démontré que $(1,x)$ est une $\mathbb{R}$-base de $\mathbb{R}+\mathbb{R}x$. Faisons-le à présent. C'est une famille génératrice par définition de $\mathbb{R}+\mathbb{R}x$, il suffit donc de montrer qu'elle est libre : soit $(\alpha,\beta)\in\mathbb{R}^2$ tel que : $\alpha+\beta x = 0_A$. Si $\beta\neq 0$, alors : $x=-\frac{\alpha}{\beta}\in\mathbb{R}$, ce qui est faux par hypothèse. Donc $\beta=0$, et il en résulte aisément $\alpha=0$.

Remarque. Il découle de cette question que tout élément non nul de A est inversible : si $x\in\mathbb{R}^*$ alors c'est trivial car $\frac{1}{x}\in\mathbb{R}^*\subseteq A$, et si $x\in A\setminus\mathbb{R}$ alors $\mathbb{R}+\mathbb{R}x$ est isomorphe en tant que $\mathbb{R}$-algèbre à $\mathbb{C}$. Or tout élément non nul de $\mathbb{C}$ admet un inverse, donc par cet isomorphisme c'est aussi le cas de x, d'où le résultat.

Une autre démonstration, très instructive et qui n'utilise pas l'isomorphisme avec $\mathbb{C}$: il découle de la question précédente que l'application $y\mapsto xy$ est un endomorphisme de $\mathbb{R}+\mathbb{R}x$, qui est de dimension finie puisqu'il admet une famille génératrice finie (à savoir $(1,x)$). Elle est de plus injective puisque $\mathbb{R}+\mathbb{R}x$ n'admet pas de diviseur de zéro (et $x\neq 0$), donc surjective par un argument dimensionnel : soit y un antécédent de 1 par cet endomorphisme. Alors $xy=1$, donc x est inversible à droite. Le même argument avec l'endomorphisme $y\mapsto yx$ montre que x est inversible à gauche. On en déduit classiquement que x est inversible.

21. L'élément x' de la question précédente répond à la question. Nous proposons une façon de faire pour le candidat qui aurait proposé un autre isomorphisme entre $\mathbb{R}+\mathbb{R}x$ et $\mathbb{C}$.

Soit $x\in A\setminus\mathbb{R}$. Un tel élément existe, puisque A n'est pas isomorphe à $\mathbb{R}$ par hypothèse. Alors d'après la question précédente, il existe un isomorphisme de $\mathbb{R}$-algèbres, noté f, de $\mathbb{R}+\mathbb{R}x$ dans $\mathbb{C}$. Posons : $i_A=f^{-1}(i)\in A$. Alors, f étant un isomorphisme de $\mathbb{R}$-algèbres, f^{-1} aussi et on a :

$$i_A^2=\left(f^{-1}(i)\right)^2=f^{-1}(i^2)=f^{-1}(-1)=-1,$$

d'où le résultat.

22. (a) Soit $(x,y)\in A^2$. Comme $i_A^2=-1$, on a :

$$T(xy)=i_Axyi_A=i_Ax(-i_A^2)yi_A=-i_Axi_Ai_Ayi_A=-T(x)T(y),$$

d'où le résultat.

(b) Soit $x\in A$. On a :

$$T^2(x)=T(T(x))=i_AT(x)i_A=i_A(i_Axi_A)i_A=i_A^2xi_A^2=(-1)^2x=x,$$

donc : $T^2=\mathrm{id}$. Or T est clairement $\mathbb{R}$-linéaire, donc c'est une symétrie de A. On en déduit : $A=\ker(T-\mathrm{id})\oplus\ker(T+\mathrm{id})$.

Remarque. Il nous sera plusieurs fois utile de remarquer la propriété suivante. Soit $(\varepsilon_1,\varepsilon_2)\in\{-1,1\}^2$. Alors :

$$\forall(x,y)\in\ker(T-\varepsilon_1\mathrm{id})\times\ker(T-\varepsilon_2\mathrm{id}), \quad xy\in\ker(T+\varepsilon_1\varepsilon_2\mathrm{id}). \tag{9}$$

Supposons en effet que $(x, y) \in \ker(T - \varepsilon_1 \mathrm{id}) \times \ker(T - \varepsilon_2 \mathrm{id})$, et utilisons la question 22.(a). On a :

$$T(xy) = -T(x)T(y) = -\varepsilon_1 x \varepsilon_2 y = -\varepsilon_1\varepsilon_2 xy,$$

donc $xy \in \ker(T + \varepsilon_1\varepsilon_2 \mathrm{id})$ comme annoncé.

23. Remarque préliminaire : en appliquant la question 20.(b) à U, et du fait qu'un isomorphisme conserve tout ce qui est relatif à la structure, on obtient immédiatement que U est commutatif (car $\mathbb{C}$ l'est) et qu'une $\mathbb{R}$-base de U est $(1, i_A)$.

Pour alléger les notations, posons : $K = \ker(T + \mathrm{id})$. Montrons d'abord que $U \subseteq K$. Comme T est $\mathbb{R}$-linéaire et U admet pour $\mathbb{R}$-base $(1, i_A)$, il suffit de montrer : $T(1) = -1$, $T(i_A) = -i_A$. On a d'une part : $T(1) = i_A \cdot 1 \cdot i_A = i_A^2 = -1$, et d'autre part :

$$T(i_A) = i_A i_A i_A = i_A^2 i_A = -i_A,$$

d'où le résultat : $U \subseteq K$. Montrons l'inclusion réciproque. Soit $z \in K$. Comme K est inclus dans A, on a aussi : $z \in A$, ce qui permet d'appliquer la question 20.(a) : soit $(a, b) \in \mathbb{R}^2$ tel que : $z^2 = b + az$. Cette égalité peut se réécrire :

$$\left(z - \frac{a}{2}\right)^2 - \frac{4b - a^2}{4} = 0_A.$$

Notons $\delta \in U$ une racine carrée de $\dfrac{4b - a^2}{4} \in \mathbb{R} \subseteq U$ dans U. Il en existe car U est une $\mathbb{R}$-algèbre isomorphe à $\mathbb{C}$, et tout élément admet une racine carrée dans $\mathbb{C}$. L'égalité précédente implique :

$$\left(\left(z - \frac{a}{2}\right) - \delta\right)\left(\left(z - \frac{a}{2}\right) + \delta\right) = 0_A.$$

Pour que cette identité remarquable soit valable, encore faut-il que δ et $z - \frac{a}{2}$ commutent. Si δ est réel alors c'est trivial, et sinon on a : $\delta = \pm i_A \sqrt{a^2 - 4b}$. Or le fait que z soit dans K implique, par définition : $i_A z i_A = -z$, c'est-à-dire (en multipliant par $-i_A$ à gauche de chaque membre de l'égalité) : $z i_A = i_A z$, ce qui assure que z et δ commutent après multiplication par $\pm\sqrt{a^2 - 4b} \in \mathbb{R}$.

Chaque membre de ce produit est dans A, puisque A contient z et U, et est stable par somme et produit. Comme A est sans diviseur de zéro, on en déduit que ce produit est nul si et seulement si l'un des deux termes est nul. Cela donne donc :

$$z = \frac{a}{2} \pm \delta \in U,$$

d'où le résultat : $K \subseteq U$. Ayant démontré la double inclusion, on a : $K = U$, ce qu'il fallait démontrer.

On en déduit que si : $\ker(T - \mathrm{id}) = \{0\}$, alors par la question précédente : $A = U \simeq \mathbb{C}$. C'est absurde par hypothèse sur A, donc $\ker(T - \mathrm{id}) \neq \{0\}$.

24. (a) Soit $\varepsilon \in \{-1, 1\}$, et soit $x \in \ker(T - \varepsilon \mathrm{id})$. Alors βx appartient à $\ker(T + \varepsilon \mathrm{id})$ par l'identité (9) démontrée en remarque dans la résolution de la question 22.(b) (on a en effet $\beta \in \ker(T - \mathrm{id})$). Ainsi l'application $m_\beta : x \mapsto \beta x$ envoie $\ker(T - \mathrm{id})$ dans $U = \ker(T + \mathrm{id})$, et elle envoie aussi $U = \ker(T + \mathrm{id})$ dans $\ker(T - \mathrm{id})$. On en déduit, par composition, que $(m_\beta)^2 : x \mapsto \beta^2 x$ induit une application de U dans lui-même. En prenant $x = 1$ (qui appartient bien à U, comme on l'a montré dans la question précédente), on a donc : $\beta^2 = \beta^2 \cdot 1 \in U$.

Déduisons-en : $\ker(T - \mathrm{id}) = \beta U$. Pour cela, on note que l'application $m_{\beta|U} : U \to \ker(T - \mathrm{id})$ est injective parce que $U \subseteq A$ est sans diviseur de zéro par hypothèse sur A, donc :

$\dim_{\mathbb{R}}(U) \leqslant \dim_{\mathbb{R}}(\ker(T-\mathrm{id}))$. Par le même argument, appliqué à $m_{\beta|\ker(T-\mathrm{id})}$, on a : $\dim_{\mathbb{R}}(\ker(T-\mathrm{id})) \leqslant \dim_{\mathbb{R}}(U)$. Donc : $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}(\ker(T-\mathrm{id}))$. Ainsi $m_{\beta|U} : U \to \ker(T-\mathrm{id})$ est une application linéaire et injective entre deux espaces vectoriels de même dimension, donc elle est surjective. Autrement dit : $\ker(T-\mathrm{id}) = m_{\beta|U}(U) = \beta U$. D'où le résultat.

(b) On sait que $\beta^2 \in U = \mathbb{R} + \mathbb{R}i_A$, mais on a aussi $\beta^2 \in \mathbb{R} + \mathbb{R}\beta$ d'après la question 20.(a). Soit, donc, $(a,b,c,d) \in \mathbb{R}^4$ tel que :

$$\beta^2 = a + bi_A = c + d\beta.$$

On a alors :

$$(a-c) + bi_A = d\beta.$$

Or $(a-c)+bi_A \in U$ et $d\beta \in \ker(T-\mathrm{id})$. Comme U et $\ker(T-\mathrm{id})$ sont en somme directe, cela implique : $a - c + bi_A = d\beta = 0_A$. Comme $\beta \neq 0_A$, ceci implique : $d = 0$. Ainsi $\beta^2 = c \in \mathbb{R}$. Ce ne peut pas être égal à un réel positif ou nul, sinon on aurait, du fait que $\sqrt{c} \in \mathbb{R}$ et β commutent : $\beta = \pm\sqrt{c}$ (on a déjà expliqué l'importance de la commutation dans les questions 20.(b) et 23). Donc β serait dans U, ce qui est impossible encore par un argument de somme directe. Ainsi c est strictement négatif, donc : $\beta^2 \in]-\infty, 0[$.

(c) Rappelons que $\ker(T+\mathrm{id}) = U = \mathbb{R}+\mathbb{R}i_A$, et on sait que l'application $m_\beta : x \mapsto \beta x$ induit un isomorphisme de U dans $\ker(T-\mathrm{id})$: il transforme donc une $\mathbb{R}$-base de U en une $\mathbb{R}$-base de $\ker(T-\mathrm{id})$; on en déduit que $(m_\beta(1), m_\beta(i_A)) = (\beta, \beta i_A)$ est une $\mathbb{R}$-base de $\ker(T-\mathrm{id})$. Le fait que β soit dans $\ker(T-\mathrm{id})$ implique : $\beta i_A = -i_A\beta$, donc $(\beta, -\beta i_A) = (\beta, i_A\beta)$ est aussi une $\mathbb{R}$-base de $\ker(T-\mathrm{id})$. Comme :

$$A = \ker(T-\mathrm{id}) \oplus \ker(T+\mathrm{id}),$$

on en déduit qu'une $\mathbb{R}$-base de A est : $(1, i_A, \beta, i_A\beta)$. Nous allons l'utiliser pour conclure.
On a montré l'existence de $\lambda < 0$ tel que : $\beta^2 = \lambda$. Posons : $j_A = \frac{\beta}{\sqrt{-\lambda}}$ (cette définition est faite de sorte que $j_A^2 = -1$), et : $k_A = i_A j_A$. Alors $(1, i_A, j_A, k_A)$ est une $\mathbb{R}$-base de A (nous n'avons fait que multiplier les deux derniers vecteurs de la base précédente par des scalaires non nuls), et l'application $\mathbb{R}$-linéaire $f : A \to \mathbb{H}$ définie sur cette base par :

$$f(1) = E, \quad f(i_A) = I, \quad f(j_A) = J, \quad f(k_A) = K$$

est bijective (puisqu'elle transforme une base de A en une base de $\mathbb{H}$). Il reste à vérifier qu'elle est un morphisme de $\mathbb{R}$-algèbres, c'est-à-dire : $\forall (x,y) \in A^2$, $f(xy) = f(x)f(y)$. Par $\mathbb{R}$-linéarité, on se convainc qu'il suffit de le vérifier pour les éléments d'une base. Or c'est bien le cas puisque :

$$i_A^2 = j_A^2 = k_A^2 = -1,$$
$$i_A j_A = k_A,\ j_A i_A = -k_A,\ j_A k_A = i_A,\ k_A j_A = -i_A,\ k_A i_A = j_A,\ i_A k_A = -j_A,$$

tandis que leurs images par f vérifient exactement les mêmes identités d'après ce qui fut admis dans l'énoncé. La vérification de toutes ces identités est relativement aisée grâce à tout ce qui précède (dès qu'on a démontré l'une des identités de la seconde ligne, la première découlant de la définition de k_A, une multiplication adéquate à gauche et à droite de chaque membre de l'égalité donne l'identité suivante ; de plus n'oublions pas que j_A et k_A sont dans $\ker(T-\mathrm{id})$, ce qui signifie exactement que $j_A i_A = -i_A j_A$ et $k_A i_A = -i_A k_A$).
Faisons seulement la vérification pour k_A^2, qui est la seule non triviale de la liste ; on a : $k_A^2 = i_A j_A i_A j_A = T(j_A) j_A = j_A j_A = j_A^2 = -1$.
Ceci étant dit : f est un isomorphisme de $\mathbb{R}$-algèbres entre A et $\mathbb{H}$, ce qui démontre que si A n'est pas isomorphe à $\mathbb{R}$ ou $\mathbb{C}$, alors A est isomorphe à $\mathbb{H}$. En bref : A est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$, ce qui démontre le théorème B.

25. Soit $(u,v) \in V^2$. On a :
$$4uv = (u+v)^2 - (u-v)^2.$$
Cette identité ne va pas tout à fait de soi, et découle du fait que x et y commutent ; par linéarité, tous les éléments de V commutent, et donc on a bien $(u+v)^2 = u^2+uv+vu+v^2 = u^2+2uv+v^2$.
D'après l'inégalité triangulaire, on a donc :
$$4\|uv\| \leqslant \|(u+v)^2\| + \|(u-v)^2\|.$$
Or la norme $\|\cdot\|$ est supposée être multiplicative, donc : $\|uv\| = \|u\|\|v\|$, et on affecte de même les normes de la majoration pour obtenir :
$$4\|u\| \cdot \|v\| \leqslant \|u+v\|^2 + \|u-v\|^2.$$
Déduisons-en que $\|\cdot\|$ provient d'un produit scalaire sur V. L'objectif est d'utiliser le théorème A. Supposons : $\|u\| = \|v\| = 1$. Alors l'inégalité précédente devient :
$$\|u+v\|^2 + \|u-v\|^2 \geqslant 4.$$
Le théorème A fut démontré sur $\mathbb{R}^2$, or ici V n'est pas égal à $\mathbb{R}^2$ *a priori*. Pas grave : l'application $f : (a,b) \mapsto ax+by$ est un isomorphisme d'espaces vectoriels de $\mathbb{R}^2$ dans V (elle est bien sûr surjective et on conclut parce que $\dim(V) = \dim(\mathbb{R}^2) = 2$), et en posant :
$$\forall (a,b) \in \mathbb{R}^2, \quad \|(a,b)\|' = \|f(a,b)\|,$$
alors on obtient une norme sur $\mathbb{R}^2$ (vérification facile ; la propriété de séparation utilise le fait que f soit injective) vérifiant la même inégalité que $\|\cdot\|$. En effet, si (a,b) et (c,d) sont des couples de $\mathbb{R}^2$ tels que : $\|(a,b)\|' = \|(c,d)\|' = 1$, alors :
$$\begin{aligned}
\left(\|(a,b)+(c,d)\|'\right)^2 + \left(\|(a,b)-(c,d)\|'\right)^2 &= \|f((a,b)+(c,d))\|^2 + \|f((a,b)-(c,d))\|^2 \\
&= \|f(a,b)+f(c,d)\|^2 + \|f(a,b)-f(c,d)\|^2 \\
&\geqslant 4\|f(a,b)\|\|f(c,d)\| \\
&= 4\|(a,b)\|'\|(c,d)\|' \\
&= 4,
\end{aligned}$$
donc elle provient d'un produit scalaire $\langle\cdot,\cdot\rangle$ sur $\mathbb{R}^2$ par le théorème A. On en déduit que l'application définie par :
$$\forall (u,v) \in V^2, \quad \langle u,v\rangle_V = \frac{1}{2}\left(\|u+v\|^2 - \|u\|^2 - \|v\|^2\right)$$
est un produit scalaire sur V, puisque :
$$\begin{aligned}
\forall (u,v) \in V^2, \quad \langle u,v\rangle_V &= \frac{1}{2}\left(\left(\left\|f^{-1}(u+v)\right\|'\right)^2 - \left(\left\|f^{-1}(u)\right\|'\right)^2 - \left(\left\|f^{-1}(v)\right\|'\right)^2\right) \\
&= \frac{1}{2}\left(\left(\left\|f^{-1}(u)+f^{-1}(v)\right\|'\right)^2 - \left(\left\|f^{-1}(u)\right\|'\right)^2 - \left(\left\|f^{-1}(v)\right\|'\right)^2\right) \\
&= \langle f^{-1}(u), f^{-1}(v)\rangle,
\end{aligned}$$
et de la dernière égalité il découle trivialement que les propriétés d'un produit scalaire sont vérifiées par $\langle\cdot,\cdot\rangle_V$ parce que $\langle\cdot,\cdot\rangle$ les vérifie et f est $\mathbb{R}$-linéaire (pour le caractère défini, on passe de $f^{-1}(u) = 0$ à $u = 0$ en composant par f).
D'où le résultat : la restriction de $\|\cdot\|$ à V provient d'un produit scalaire sur V.

26. Si $x \in \mathbb{R}$ alors le résultat est évident. Supposons donc $x \in A \setminus \mathbb{R}$. Utilisons le résultat de la question 25 avec $y = 1$. Les hypothèses sont bien vérifiées : on a bien sûr $x \cdot 1 = 1 \cdot x = x$, et $V = \mathbb{R} + \mathbb{R}x$ est de dimension 2 car $(1, x)$ est $\mathbb{R}$-libre (si ce n'était pas le cas, alors x serait proportionnel à 1 et donc réel). Par la question précédente, V est muni d'un produit scalaire $\langle \cdot, \cdot \rangle_V$ dont la norme euclidienne est $\| \cdot \|_{|V}$. Elle vérifie en particulier l'identité du parallélogramme. Posons $x' = \frac{1}{\|x\|} x \in V$. Alors :

$$\|x' + 1\|^2 + \|x' - 1\|^2 = 2\left(\|x'\|^2 + \|1\|^2\right) = 4. \tag{10}$$

Justifions que 1 est effectivement unitaire pour ce produit scalaire. On a : $\|1\|^2 = \|1^2\| = \|1\|$, et on a $\|1\| \neq 0$ car $1 \neq 0_A$. Ainsi $\|1\| = 1$ est la seule possibilité.
Mais on a aussi, comme la norme est multiplicative :

$$\|x' + 1\|^2 + \|x' - 1\|^2 = \|(x' + 1)^2\| + \|(x' - 1)^2\| = \|(x')^2 + 2x' + 1\| + \|(x')^2 - 2x' + 1\|. \tag{11}$$

En comparant (10) et (11), on a donc :

$$4 = \|(x')^2 + 2x' + 1\| + \|(x')^2 - 2x' + 1\|.$$

On est donc dans le cas d'égalité de l'inégalité triangulaire. On a en effet :

$$4 = 4\|x'\| = \|4x'\| = \|((x')^2 + 2x' + 1) - ((x')^2 - 2x' + 1)\|,$$

or le cas d'égalité est vérifié si et seulement si les deux vecteurs en jeu sont (positivement) liés. On en déduit qu'il existe $\lambda \in \mathbb{R}_-$ tel que : $(x')^2 + 2x' + 1 = \lambda((x')^2 - 2x' + 1)$. On n'a pas $\lambda = 1$, sinon l'égalité précédente impliquerait $4x' = 0$, qui est faux (en effet on a supposé $x \notin \mathbb{R}$, donc x' n'est pas dans $\mathbb{R}$ non plus et ne peut pas être nul). L'égalité précédente implique donc :

$$(x')^2 = \frac{1}{1 - \lambda}\left(-2(\lambda + 1)x' + (\lambda - 1)\right).$$

Or : $x = \|x\|x'$, donc :

$$x^2 = \frac{\|x\|^2}{1 - \lambda}\left(-\frac{2(\lambda + 1)}{\|x\|}x + (\lambda - 1)\right) \in \mathbb{R} + \mathbb{R}x,$$

d'où le résultat.

27. Utilisons les questions précédentes pour montrer que A est une $\mathbb{R}$-algèbre algébrique sans diviseur de zéro.

Montrons qu'elle est algébrique. Soit $x \in A$. Par la question précédente, on a : $x^2 \in \mathbb{R} + \mathbb{R}x$. On en déduit qu'il existe $(a, b) \in \mathbb{R}^2$ tel que : $x^2 = b + ax$. Donc : $x^2 - ax - b = 0$. Par conséquent tout élément de A est annulé par un polynôme réel unitaire, donc A est algébrique.

Montrons qu'elle n'admet pas de diviseur de zéro. Soit $(x, y) \in A^2$. Si $xy = 0$, alors on a : $0 = \|xy\| = \|x\| \cdot \|y\|$, et comme le produit est dans $\mathbb{R}$ ceci implique : $\|x\| = 0$, ou : $\|y\| = 0$. Par conséquent, si $xy = 0$ alors $x = 0$ ou $y = 0$. Par contraposée, si x et y sont non nuls alors $xy \neq 0$, donc A n'admet pas de diviseur de zéro.

Ainsi A vérifie les hypothèses du théorème B, donc A est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. Le théorème C est démontré.