

DS N° 4 : EVN & Algèbre

Epreuve A :

Durée : 4 heures



Notations On note \mathbb{R} et \mathbb{C} les corps des nombres réels et complexes. Pour $z \in \mathbb{C}$ on note \bar{z} le conjugué complexe de z et $|z|$ le module de z .

Si V est un espace euclidien, on note $\text{End}(V)$ l'espace des applications \mathbb{R} -linéaires de V dans lui-même. On note aussi $\text{GL}(V)$ le groupe des applications \mathbb{R} -linéaires bijectives de V sur lui-même, et on note $\text{O}(V) \subset \text{GL}(V)$ (respectivement $\text{SO}(V) \subset \text{GL}(V)$) le groupe orthogonal (respectivement spécial orthogonal) de V .

Par convention, les \mathbb{R} -algèbres considérées dans ce problème seront non nulles, associatives et unitaires, mais pas forcément commutatives. Deux \mathbb{R} -algèbres A et B sont dites isomorphes s'il existe une bijection \mathbb{R} -linéaire $f : A \rightarrow B$ telle que $f(xy) = f(x)f(y)$ pour tous $x, y \in A$.

Soit A une \mathbb{R} -algèbre et soit $e \in A$ l'élément unité de A pour la multiplication. On notera \mathbb{R}_A la sous-algèbre $\{ae \mid a \in \mathbb{R}\}$ de A . Un élément x de A est dit inversible s'il existe $y \in A$ tel que $xy = yx = e$. On note A^\times l'ensemble des éléments inversibles de A . On admet que A^\times est un groupe pour la multiplication.

On note $M_2(\mathbb{C})$ la \mathbb{C} -algèbre des matrices de taille 2×2 à coefficients complexes. Pour $z_1, z_2 \in \mathbb{C}$ on note

$$Z(z_1, z_2) = \begin{pmatrix} z_1 & -\bar{z}_2 \\ z_2 & \bar{z}_1 \end{pmatrix}.$$

Soit $\mathbb{H} = \{Z(z_1, z_2) \mid z_1, z_2 \in \mathbb{C}\} \subset M_2(\mathbb{C})$. On admet que \mathbb{H} est un sous- \mathbb{R} -espace vectoriel de $M_2(\mathbb{C})$, admettant comme base les matrices

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

qui vérifient les relations suivantes dans $M_2(\mathbb{C})$:

$$I^2 = J^2 = K^2 = -E, IJ = -JI = K, JK = -KJ = I, KI = -IK = J.$$

On veillera à ne pas confondre l'élément i de \mathbb{C} et la matrice I de $\mathbb{H} \subset M_2(\mathbb{C})$, ni la matrice I avec la matrice identité E .

On note $\mathbb{H}^{\text{im}} = \{xI + yJ + zK \mid (x, y, z) \in \mathbb{R}^3\} \subset \mathbb{H}$.

On définit une application $N : \mathbb{H} \rightarrow \mathbb{R}$ par $N(Z(z_1, z_2)) := |z_1|^2 + |z_2|^2$.

On note $S = \{U \in \mathbb{H} \mid N(U) = 1\}$.

I Préliminaires

Si $A = (a_{ij}) \in M_2(\mathbb{C})$ on note $A^* = (\overline{a_{ji}})$.

1. a) Montrer que \mathbb{H} est une sous- \mathbb{R} -algèbre de $M_2(\mathbb{C})$ stable par $Z \mapsto Z^*$.
b) Soit $Z \in \mathbb{H}$. Calculer ZZ^* et en déduire que tout élément non nul de \mathbb{H} est inversible.
c) Soit $Z \in \mathbb{H}$. Montrer que $Z \in \mathbb{R}_{\mathbb{H}}$ si et seulement si $ZZ' = Z'Z$ pour tout $Z' \in \mathbb{H}$.
2. a) Montrer que l'on a $N(ZZ') = N(Z)N(Z')$ pour tous $Z, Z' \in \mathbb{H}$.
b) Montrer que S est un sous-groupe de \mathbb{H}^\times et que $\frac{1}{\sqrt{N(Z)}}Z \in S$ pour tout $Z \in \mathbb{H}^\times$.
3. a) Montrer que pour tous $x, y, z, t \in \mathbb{R}$ on a

$$N(xE + yI + zJ + tK) = x^2 + y^2 + z^2 + t^2.$$

- b) Montrer que pour tout $U \in \mathbb{H}^{\text{im}}$ on a $U^2 = -N(U)E$ et que

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

La question 3a) montre que l'on définit un produit scalaire $\langle \cdot, \cdot \rangle$ sur \mathbb{H} en posant, pour $Z, Z' \in \mathbb{H}$

$$\langle Z, Z' \rangle = \frac{N(Z + Z') - N(Z) - N(Z')}{2},$$

et que l'on dispose d'une isométrie

$$\psi : \mathbb{R}^4 \rightarrow \mathbb{H}, \psi(x, y, z, t) := xE + yI + zJ + tK$$

de \mathbb{R}^4 muni du produit scalaire usuel sur \mathbb{H} . On munit par la suite \mathbb{H} de sa structure d'espace euclidien induite par le produit scalaire $\langle \cdot, \cdot \rangle$. Ainsi (E, I, J, K) est une base orthonormée de \mathbb{H} .

4. Montrer que S est une partie fermée et connexe par arcs de \mathbb{H} .
5. Soient $U, V \in \mathbb{H}^{\text{im}}$.
 - a) Montrer que U et V sont orthogonaux si et seulement si $UV + VU = 0$. Dans ce cas montrer que $UV \in \mathbb{H}^{\text{im}}$ et que le déterminant de la famille (U, V, UV) dans la base (I, J, K) de \mathbb{H}^{im} est positif ou nul.
 - b) Montrer que si (U, V) est une famille orthonormale dans \mathbb{H}^{im} , alors (U, V, UV) est une base orthonormée directe de \mathbb{H}^{im} .

II Automorphismes de \mathbb{H} et rotations

On munit $S \times S$ de la loi de composition \times donnée par $(u_1, u_2) \times (v_1, v_2) = (u_1v_1, u_2v_2)$ et on admet qu'elle munit $S \times S$ d'une structure de groupe. On considère l'application

$$\begin{aligned} \alpha : S \times S &\longrightarrow GL(\mathbb{H}) \\ (u, v) &\longmapsto (Z \mapsto uZv^{-1}) \end{aligned}$$

en admettant que $\alpha(u, v)$ est bien dans $GL(\mathbb{H})$. Pour $u \in S$, on admet que l'endomorphisme $\alpha(u, u)$ de \mathbb{H} laisse stable le sous-espace \mathbb{H}^{im} de \mathbb{H} , et on note $C_u \in \text{End}(\mathbb{H}^{\text{im}})$ l'endomorphisme induit. On a donc $C_u(Z) = uZu^{-1}$ pour $Z \in \mathbb{H}^{\text{im}}$.

6. Montrer que α est un morphisme de groupes et décrire son noyau.
7. Montrer que α est continu et que l'image de α est contenue dans $SO(\mathbb{H})$. On pourra commencer par montrer que $\alpha(u, v) \in O(\mathbb{H})$ pour $(u, v) \in S \times S$.
8. Soient $\theta \in \mathbb{R}$ et $v \in \mathbb{H}^{\text{im}} \cap S$, et soit $u = (\cos \theta)E + (\sin \theta)v$.
 - a) Montrer que $u \in S$ et que $u^{-1} = (\cos \theta)E - (\sin \theta)v$.
 - b) Soit $w \in \mathbb{H}^{\text{im}} \cap S$ un vecteur orthogonal à v . Décrire la matrice de C_u dans la base orthonormée directe (v, w, vw) de \mathbb{H}^{im} .
9. Montrer que l'application $u \mapsto C_u$ induit un morphisme surjectif de groupes $S \rightarrow SO(\mathbb{H}^{\text{im}})$ et décrire son noyau.
10. a) En déduire que $\alpha(S \times S) = SO(\mathbb{H})$.
 - b) Montrer que $N := \alpha(S \times \{1\})$ est un sous-groupe de $SO(\mathbb{H})$, puis que $gng^{-1} \in N$ pour tous $n \in N$ et $g \in SO(\mathbb{H})$ et que $\{\pm \text{id}\} \subsetneq N \subsetneq SO(\mathbb{H})$.

Soit $\text{Aut}(\mathbb{H})$ l'ensemble des automorphismes de la \mathbb{R} -algèbre \mathbb{H} . Un élément de $\text{Aut}(\mathbb{H})$ est donc une application \mathbb{R} -linéaire bijective $f : \mathbb{H} \rightarrow \mathbb{H}$ satisfaisant $f|_{\mathbb{R}\mathbb{H}} = \text{id}_{\mathbb{R}\mathbb{H}}$ et $f(uv) = f(u)f(v)$ pour tout $(u, v) \in \mathbb{H}^2$.

11. Montrer que $\text{Aut}(\mathbb{H})$ est un sous-groupe de $GL(\mathbb{H})$, contenant $\alpha(u, u)$ pour tout $u \in S$.
12. Montrer que $(f(I), f(J), f(K))$ est une base orthonormée directe de \mathbb{H}^{im} pour tout $f \in \text{Aut}(\mathbb{H})$.

13. a) Montrer que l'application de restriction à \mathbb{H}^{im} induit un isomorphisme de groupes

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

- b) Montrer que

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

III Normes euclidiennes sur \mathbb{R}^2

Le but de cette partie est la preuve du résultat suivant, qui sera utilisé dans la partie IV.

Théorème A. Soit $\|\cdot\|$ une norme sur le \mathbb{R} -espace vectoriel \mathbb{R}^2 . Si

$$\|x + y\|^2 + \|x - y\|^2 \geq 4$$

pour tous $x, y \in \mathbb{R}^2$ vérifiant $\|x\| = \|y\| = 1$, alors $\|\cdot\|$ provient d'un produit scalaire sur \mathbb{R}^2 .

On note $\|\cdot\|_2$ la norme euclidienne canonique sur \mathbb{R}^2 et on note

$$\mathcal{C} := \{x \in \mathbb{R}^2 \mid \|x\|_2 = 1\}.$$

On fixe une norme *quelconque* $\|\cdot\|$ sur \mathbb{R}^2 et on note

$$\mathcal{K} = \{A \in M_2(\mathbb{R}) \mid \forall x \in \mathbb{R}^2 \ \|x\|_2 \geq \|Ax\|\}.$$

14. a) Montrer que \mathcal{K} est une partie compacte et convexe de $M_2(\mathbb{R})$.

- b) Montrer qu'il existe $A \in \mathcal{K}$ tel que $\det A = \sup_{B \in \mathcal{K}} \det B$.

On fixe par la suite un élément A de \mathcal{K} tel que $\det A = \sup_{B \in \mathcal{K}} \det B$.

15. Montrer que $\det A > 0$ et qu'il existe $x \in \mathcal{C}$ tel que $\|Ax\| = 1$.

On fixe par la suite $x \in \mathcal{C}$ tel que $\|Ax\| = 1$.

16. Soit $B \in \text{SO}(\mathbb{R}^2)$ une matrice telle que $x = B \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

- a) Montrer que pour tout $r \in]0, 1[$ il existe $x_r \in \mathcal{C}$ tel que

$$\|AB \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} x_r\| > 1.$$

b) Montrer que si $x_r = \begin{pmatrix} y_r \\ z_r \end{pmatrix}$, alors $z_r^2 > \frac{r^2}{1+r^2}$.

17. En utilisant ce qui précède, montrer qu'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. Soit T une partie fermée de \mathcal{C} , telle qu'il existe $x, y \in T$ avec $y \notin \{-x, x\}$. On suppose que pour tous $a, b \in T$ avec $b \notin \{-a, a\}$, on a que $\frac{b-a}{\|b-a\|_2}$ et $\frac{b+a}{\|b+a\|_2}$ appartiennent à T . Montrer que $T = \mathcal{C}$.

19. Montrer le théorème A.

IV Algèbres valuées

Soit A une \mathbb{R} -algèbre et e son élément neutre. Dans cette partie, on identifiera \mathbb{R}_A avec \mathbb{R} , et on notera (abusivement) a l'élément ae de A pour $a \in \mathbb{R}$. On dit que A est *algébrique* si pour tout $x \in A$ il existe un entier $n \geq 1$ et $a_0, \dots, a_{n-1} \in \mathbb{R}$ tels que

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0.$$

On dit que A est *sans diviseur de zéro* si $xy \neq 0$ pour tous $x, y \in A \setminus \{0\}$. Dans cette partie, nous allons montrer le théorème B ci-dessous, puis l'utiliser pour prouver le théorème C plus loin.

Théorème B. Une \mathbb{R} -algèbre algébrique et sans diviseur de zéro est isomorphe à \mathbb{R}, \mathbb{C} ou \mathbb{H} .

Soit A une \mathbb{R} -algèbre algébrique et sans diviseur de zéro.

20. a) Montrer que $x^2 \in \mathbb{R} + \mathbb{R}x$ pour tout $x \in A$.

b) Montrer que si $x \in A \setminus \mathbb{R}$, alors $\mathbb{R} + \mathbb{R}x$ est une \mathbb{R} -algèbre isomorphe à \mathbb{C} .

On suppose que A n'est pas isomorphe à une des algèbres \mathbb{R} ou \mathbb{C} .

21. Montrer qu'il existe $i_A \in A$ tel que $i_A^2 = -1$.

On fixe par la suite un élément i_A de A tel que $i_A^2 = -1$. On note $U = \mathbb{R} + \mathbb{R}i_A$ et on définit l'application

$$T : A \rightarrow A, T(x) = i_A x i_A.$$

On note $\text{id} : A \rightarrow A$ l'application identité de A .

22. a) Montrer que $T(xy) = -T(x)T(y)$ pour tous $x, y \in A$.
 b) Calculer $T^2 = T \circ T$ et en déduire que $A = \ker(T - \text{id}) \oplus \ker(T + \text{id})$.
23. Montrer que $\ker(T + \text{id}) = U$ et en déduire que $\ker(T - \text{id}) \neq \{0\}$.
24. On fixe $\beta \in \ker(T - \text{id}) \setminus \{0\}$.
 a) Montrer que l'application $x \mapsto \beta x$ envoie $\ker(T - \text{id})$ dans $\ker(T + \text{id})$.
 En déduire que $\beta^2 \in U$ et que $\ker(T - \text{id}) = \beta U$.
 b) Montrer que $\beta^2 \in]-\infty, 0[$.
 c) Démontrer le théorème B.

On se propose maintenant de démontrer le résultat suivant:

Théorème C. Soit A une \mathbb{R} -algèbre. S'il existe une norme $\|\cdot\|$ sur le \mathbb{R} -espace vectoriel A telle que

$$\forall x, y \in A \quad \|xy\| = \|x\| \cdot \|y\|,$$

alors A est isomorphe à \mathbb{R}, \mathbb{C} ou \mathbb{H} .

On fixe une \mathbb{R} -algèbre comme dans l'énoncé du théorème ci-dessus.

25. Soient $x, y \in A$ tels que $xy = yx$ et tels que $V = \mathbb{R}x + \mathbb{R}y$ soit de dimension 2 sur \mathbb{R} . Montrer que

$$\forall u, v \in V \quad \|u + v\|^2 + \|u - v\|^2 \geq 4\|u\| \cdot \|v\|$$

et que la restriction de $\|\cdot\|$ à V provient d'un produit scalaire sur V .

26. Montrer que $x^2 \in \mathbb{R} + \mathbb{R}x$ pour tout $x \in A$. On pourra utiliser le résultat de la question 25 avec $y = 1$.
27. Conclure.

Corrigé DS N° 4 : EVN & Algèbre

X 2023

1 Préliminaires

1. (a) Il a été admis que \mathbb{H} est un sous- \mathbb{R} -espace vectoriel de $M_2(\mathbb{C})$. Soit $z_1, z_2, z'_1, z'_2 \in \mathbb{C}$, on a

$$\begin{aligned} Z(z_1, z_2)Z(z'_1, z'_2) &= \begin{pmatrix} z_1 z'_1 - z_2 \overline{z'_2} & -z_1 \overline{z'_2} - \overline{z_2} z'_1 \\ z_2 z'_1 + \overline{z_1} z_2 & -z_2 z'_2 + \overline{z_1} z'_1 \end{pmatrix} \\ &= Z(z_1 z'_1 - \overline{z_2} z'_2, z_2 z'_1 + \overline{z_1} z_2) \end{aligned}$$

Ainsi, \mathbb{H} est stable par produit.

Soit $A = \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix}$, alors $A^* = \begin{pmatrix} \overline{z_1} & \overline{z_2} \\ -z_2 & z_1 \end{pmatrix} = Z(\overline{z_1}, -z_2)$. Donc, \mathbb{H} est aussi stable par $Z \mapsto Z^*$.

(b) Soit $Z = Z(z_1, z_2) \in \mathbb{H}$, alors on fait le calcul :

$$\begin{aligned} ZZ^* &= Z(z_1, z_2)Z(\overline{z_1}, -z_2) \\ &= Z(|z_1|^2 + |z_2|^2, 0) \\ &= (|z_1|^2 + |z_2|^2)E \end{aligned}$$

Ainsi, tout élément non nul $Z \in \mathbb{H}$ est inversible et

$$Z^{-1} = \frac{1}{N(Z)} Z^*$$

(c) Soit $Z(a, b) \in \mathbb{H}$, on suppose que $Z(a, b)$ commute avec tous les éléments de \mathbb{H} . En particulier, elle commute avec J et K . On a

$$\begin{aligned} \begin{cases} Z(a, b)J &= JZ(a, b) \\ Z(a, b)K &= KZ(a, b) \end{cases} &\iff \begin{cases} Z(a, b)Z(0, -1) &= Z(0, -1)Z(a, b) \\ Z(a, b)Z(0, i) &= Z(0, i)Z(a, b) \end{cases} \\ &\iff \begin{cases} Z(\overline{b}, -\overline{a}) &= Z(b, -a) \\ Z(-i\overline{b}, i\overline{a}) &= Z(ib, ia) \end{cases} \end{aligned}$$

Ainsi, on en déduit d'une part que $\overline{b} = b$ et $\overline{a} = a$, autrement dit $a, b \in \mathbb{R}$. D'autre part, $-\overline{b} = b$, d'où $b = 0$.

On en déduit que Z est de la forme aE pour $a \in \mathbb{R}$: $Z \in \mathbb{R}\mathbb{H}$.

Réciproquement, les matrices de cette forme commutent bien avec tous les éléments de \mathbb{H} .

2. (a) On a

$$\begin{aligned} N(ZZ')E &= (ZZ')(ZZ')^* \\ &= (ZZ')(Z'^*Z^*) \\ &= Z(Z'Z'^*)Z^* \\ &= N(Z')ZZ^* \\ &= N(Z')N(Z)E \end{aligned}$$

Et donc, on a $N(ZZ') = N(Z')N(Z) = N(Z)N(Z')$.

- (b) $E \in S$ de façon immédiate. Si $Z, Z' \in S$, on a $N(ZZ') = N(Z)N(Z') = 1$ et donc $ZZ' \in S$.
 Finalement, si $Z \in S$, alors $Z^{-1} = Z^*$ et un calcul rapide donne $N(Z^*) = N(Z)$, donc $Z^{-1} \in S$. Ainsi, S est un sous-groupe de \mathbb{H}^\times .

Soit $\lambda \in \mathbb{R}$ et $Z \in \mathbb{H}^*$, on a $N(\lambda Z)E = (\lambda Z)(\lambda Z)^* = \lambda^2 N(Z)E$ et donc $N(\lambda Z) = \lambda^2 N(Z)$. Ainsi, on a

$$N\left(\frac{1}{\sqrt{N(Z)}}Z\right) = \frac{1}{N(Z)}N(Z) = 1$$

Donc, $\frac{1}{\sqrt{N(Z)}}Z \in S$.

3. (a) On calcule

$$\begin{aligned} N(xE + yI + zJ + tK) &= N(Z(x + iy, -z + it)) \\ &= |x + iy|^2 + |-z + it|^2 \\ &= x^2 + y^2 + z^2 + t^2 \end{aligned}$$

- (b) Soit $U = xI + yJ + zK \in \mathbb{H}^{\text{im}}$, on a

$$\begin{aligned} U^2 &= x^2 I^2 + y^2 J^2 + z^2 K^2 + xy(IJ + JI) + xz(IK + KI) + yz(KJ + JK) \\ &= -(x^2 + y^2 + z^2)E \\ &= -N(U)E \end{aligned}$$

Réciproquement, si $U \in \mathbb{U}$ tel que $U^2 = -\lambda E$ avec $\lambda < 0$. On écrit $U = xE + \underbrace{yI + zJ + tK}_{:=\tilde{U}}$ de sorte que

$$\begin{aligned} U^2 &= x^2 E^2 + \tilde{U}^2 + 2x\tilde{U} \\ &= (x^2 - N(\tilde{U}))E + 2x\tilde{U} \end{aligned}$$

Ainsi, pour que U^2 puisse être colinéaire à E , cela impose $x = 0$. Et donc, $U \in \mathbb{H}^{\text{im}}$.

4. D'après 3a., l'application ψ réalise une isométrie entre S et la sphère unité \mathbb{S}^3 de \mathbb{R}^4 qui est immédiatement fermée comme image réciproque de $\{1\}$ par la norme euclidienne canonique.

Pour la connexité par arcs, il suffit de montrer que la sphère unité \mathbb{S}^3 est connexe par arcs. Soit $u, v \in \mathbb{S}^3$ qui ne sont pas colinéaires, alors $\gamma : t \in [0, 1] \mapsto \frac{tu + (1-t)v}{\|tu + (1-t)v\|}$ est un chemin entre v et u qui est bien défini car $tu + (1-t)v \neq 0$ pour tout $t \in [0, 1]$.

Si maintenant u et v sont colinéaires, on peut trouver $w \in \mathbb{S}^3$ non colinéaire à u (car \mathbb{R}^4 est de dimension ≥ 2) et on passe de u à v en passant par w .

5. (a) On calcule

$$\begin{aligned} \langle U, V \rangle E &= \frac{1}{2}(N(U+V) - N(U) - N(V))E \\ &= -\frac{1}{2}((U+V)^2 - U^2 - V^2) \\ &= -(UV + VU) \end{aligned}$$

Ainsi, U et V sont orthogonaux si, et seulement si, $UV + VU = 0$.

On a alors $(UV)^2 = U(VU)V = -U(UV)V = -U^2V^2 = -N(U)N(V)E$ car $U, V \in \mathbb{H}^{\text{im}}$ et donc d'après 3b., $UV \in \mathbb{H}^{\text{im}}$.

On écrit $U = x_U I + y_U J + z_U K$ et $V = x_V I + y_V J + z_V K$ de sorte que

$$UV = (x_U y_V - y_U x_V)K + (y_U z_V - z_U y_V)I + (z_U x_V - x_U z_V)J$$

De sorte que la matrice de (U, V, UV) dans la base (I, J, K) est $\begin{pmatrix} x_U & x_V & y_U z_V - z_U y_V \\ y_U & y_V & z_U x_V - x_U z_V \\ z_U & z_V & x_U y_V - y_U x_V \end{pmatrix}$.

On développe par rapport à la dernière colonne :

$$\det_{(I, J, K)}(U, V, UV) = (y_U z_V - z_U y_V)^2 + (z_U x_V - x_U z_V)^2 + (x_U y_V - y_U x_V)^2 \geq 0$$

Remarque : Ce n'est pas au programme, mais on reconnaît en fait dans UV les coordonnées du produit vectoriel $u \wedge v$... Rappelons que dans \mathbb{R}^3 , on a l'expression suivante : $\det(u, v, w) = (u \wedge v) \cdot w$, ce qui donnerait ici $\det(u, v, u \wedge v) = \|u \wedge v\|^2$, ce qui est bien en accord avec ce qu'on a trouvé.

- (b) D'après le calcul précédent, si (U, V, UV) est une base orthonormée, alors elle est directe, car son déterminant est > 0 .

Reste à vérifier que $UV \perp U$ et $UV \perp V$. Pour cela, on calcule :

$$U(UV) + (UV)U = U^2V - U^2V = 0 \quad \text{et} \quad V(UV) + UV(V) = -UV^2 + UV^2 = 0$$

Ainsi, (U, V, UV) est une famille orthonormée et donc une base orthonormée directe de \mathbb{H}^{im} (car \mathbb{H}^{im} est de dimension 3).

2 Automorphismes de \mathbb{H} et rotations

6. Soit $(u_1, v_1), (u_2, v_2) \in S$ et $Z \in \mathbb{H}$, alors

$$\begin{aligned} \alpha(u_1, v_1) \circ \alpha(u_2, v_2) \cdot Z &= \alpha(u_1, v_1) \cdot (u_2 Z v_2^{-1}) \\ &= u_1 u_2 Z v_2^{-1} v_1^{-1} \\ &= (u_1 u_2) Z (v_1 v_2)^{-1} \\ &= \alpha(u_1 u_2, v_1 v_2) \cdot Z \end{aligned}$$

Ainsi, on a montré que α est un morphisme de groupes.

On a

$$\text{Ker}(\alpha) = \{(u, v) \in S, \forall Z \in \mathbb{H}, u Z v^{-1} = Z\} = \{(u, v) \in S, \forall Z \in \mathbb{H}, u Z = Z v\}$$

Soit $(u, v) \in \text{Ker}(\alpha)$, en prenant $Z = u$, on trouve $u = v$. Ainsi, u commute avec tous les éléments de S , donc, en renormalisant, avec tous les éléments de \mathbb{H} . Ainsi, $u \in \mathbb{R}_{\mathbb{H}}$ et $u \in S$, on a $u = \pm 1$. La réciproque étant immédiate, on a

$$\text{Ker}(\alpha) = \{(1, 1), (-1, -1)\}$$

7. L'application α est continu par continuité de l'inverse matriciel et du produit matriciel. Soit $(u, v) \in S \times S$, on montre que $\alpha(u, v)$ est une isométrie. Soit $Z \in \mathbb{H}$, on calcule

$$N(\alpha(u, v) \cdot Z) = N(u Z v^{-1}) = N(u)N(Z)N(v^{-1}) = N(Z)$$

car $u, v \in S$. Ainsi, $\alpha(u, v)$ est une isométrie et donc $\alpha(u, v) \in O(\mathbb{H})$.

On a vu S est connexe par arcs et $S \times S$ est connexe par arcs, donc par continuité, $\alpha(S \times S)$ est connexe par arcs et contient l'identité.

Comme \det est continu, $\det(\alpha(S \times S))$ est une partie connexe de \mathbb{R}^* contenant 1 : c'est $]0, +\infty[$. Donc, $\det(\alpha(S \times S)) > 0$ et donc $\alpha(S \times S) \in SO(\mathbb{H})$.

8. (a) D'après ce qui a été dit à la question 3., $\mathbb{R}_{\mathbb{H}} \perp \mathbb{H}^{\text{im}}$, donc

$$N(u) = \cos(\theta)^2 N(E) + \sin(\theta)^2 N(v) = \cos(\theta)^2 + \sin(\theta)^2 = 1$$

On calcule

$$(\cos \theta E + \sin \theta v)(\cos \theta E - \sin \theta v) = \cos(\theta)^2 E - \sin(\theta)^2 v^2 = \cos(\theta)^2 E + \sin(\theta)^2 N(v) E = E$$

Ainsi, l'inverse de u est bien $\cos(\theta)E - \sin(\theta)v$.

- (b) On calcule, en utilisant les propriétés $xy = -yx$ (quand $x, y \in \mathbb{H}^{\text{im}}$ sont orthogonaux) et $x^2 = -E$:

$$\begin{aligned} C_u(v) &= uvu^{-1} \\ &= (\cos \theta E + \sin \theta v)v(\cos \theta E - \sin \theta v) \\ &= (\cos(\theta)^2 E - \sin(\theta)^2 v)v \\ &= v \end{aligned}$$

puis,

$$\begin{aligned}
C_u(w) &= u w u^{-1} \\
&= (\cos \theta E + \sin \theta v) w (\cos \theta E - \sin \theta v) \\
&= \cos(\theta)^2 w - \cos(\theta) \sin(\theta) w v + \sin(\theta) \cos(\theta) v w - \sin(\theta)^2 v w v \\
&= (\cos(\theta)^2 - \sin(\theta)^2) w + \cos(\theta) \sin(\theta) (v w - w v) \\
&= \cos(2\theta) w + \sin(2\theta) v w
\end{aligned}$$

et enfin,

$$\begin{aligned}
C_u(vw) &= u v w u^{-1} \\
&= (\cos \theta E + \sin \theta v) v w (\cos \theta E - \sin \theta v) \\
&= \cos(\theta)^2 v w + \sin(\theta) \cos(\theta) v^2 w - \cos(\theta) \sin(\theta) v w v - \sin(\theta)^2 v^2 w v \\
&= (\cos(\theta)^2 - \sin(\theta)^2) v w - 2 \sin(\theta) \cos(\theta) w \\
&= \cos(2\theta) v w - \sin(2\theta) w
\end{aligned}$$

ce qui donne finalement

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

9. Soit $V \in SO(\mathbb{H}^{\text{im}})$ une rotation d'axe dirigée par v et d'angle θ , on définit de même u comme dans la question

précédente. Alors, la rotation associée à la matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\theta) & -\sin(2\theta) \\ 0 & \sin(2\theta) & \cos(2\theta) \end{pmatrix}$ écrite dans la base (v, w, vw)

vérifie $C_u = V$.

Il est immédiat de vérifier que $u \mapsto C_u$ est un morphisme de groupes et il est surjectif d'après ce qu'on vient de dire.

Enfin, on a

$$\text{Ker}(C) = \{u \in S, \forall Z \in \mathbb{H}^{\text{im}}, u Z u^{-1} = Z\} = \{u \in S, \forall Z \in \mathbb{H}^{\text{im}}, u Z = Z u\}$$

Soit $u \in \text{Ker}(C)$, alors u commute avec tous les éléments de \mathbb{H}^{im} et donc de \mathbb{H} , donc $u \in \mathbb{R}_{\mathbb{H}}$ et est unitaire, donc $u = \pm 1$. La réciproque étant immédiate, on a

$$\text{Ker}(C) = \{\pm 1\}$$

10. (a) Soit $r \in SO(\mathbb{H})$. On distingue deux cas :

- Si $r(1) = 1$, alors r stabilise \mathbb{H}^{im} par orthogonalité et donc il existe $v \in S$ tel que $r|_{\mathbb{H}^{\text{im}}} = C_v$. Alors, on a

$$r = \alpha(v, v)$$

- Sinon, on note $r(1) = p \in S$ de sorte qu'on ait :

$$\alpha(\bar{p}, 1) \circ r(1) = \alpha(\bar{p}, 1) \cdot p = 1$$

Par le point précédent, il existe alors $v \in S$ tel que $\alpha(\bar{p}, 1) \circ r = \alpha(v, v)$ et donc, on a

$$r = \alpha(pv, v)$$

Ainsi, $\alpha : S \times S \rightarrow SO(\mathbb{H})$ est surjective.

(b) $S \times \{E\}$ est un sous-groupe de $S \times S$, donc son image directe par le morphisme α est un sous-groupe de $SO(\mathbb{H})$.

Soit $n \in N$ et $g \in SO(\mathbb{H})$, on écrit $n = \alpha(p, 1)$ avec $u \in S$. De plus, comme α est surjective, on peut écrire $g = \alpha(u, v)$. Le reste est de l'écriture :

$$g n g^{-1} = \alpha(u, v) \alpha(p, 1) \alpha(u^{-1}, v^{-1}) = \alpha(upu^{-1}, 1) \in N$$

On a vu dans la question précédente qu'un élément de N stabilise \mathbb{H}^{im} est y induit une rotation. On en déduit déjà que N est un sous-groupe strict de $SO(\mathbb{H})$.

Enfin, en prenant une rotation non triviale, qui n'est pas un retournement de \mathbb{H}^{im} , elle induit un élément de $SO(\mathbb{H})$ qui n'est pas $\pm \text{Id}$.

11. Si $f \in \text{Aut}(\mathbb{H})$, alors $(f^{-1})|_{\mathbb{R}\mathbb{H}} = \text{Id}_{\mathbb{R}\mathbb{H}}$ et que $f^{-1}(uv) = f^{-1}(u)f^{-1}(v)$, en effet

$$f(f^{-1}(uv)) = uv = f(f^{-1}(u)f^{-1}(v))$$

Enfin, $\text{Aut}(\mathbb{H})$ est clairement stable par composition. Donc, $\text{Aut}(\mathbb{H})$ est un sous-groupe de $GL(\mathbb{H})$.
Si $Z \in \mathbb{R}\mathbb{H}$, alors Z commute avec u , donc $\alpha(u, u) \cdot Z = Z$ et $\alpha(u, u)|_{\mathbb{R}\mathbb{H}} = \text{Id}_{\mathbb{R}\mathbb{H}}$. Enfin, si $Z, Z' \in \mathbb{H}$, alors

$$\alpha(u, u) \cdot (ZZ') = u(ZZ')u^{-1} = (uZu^{-1})(uZ'u^{-1}) = (\alpha(u, u) \cdot Z)(\alpha(u, u) \cdot Z')$$

Et donc, $\alpha(u, u) \in \text{Aut}(\mathbb{H})$.

12. Si $U, V \in \mathbb{H}^{\text{im}}$ sont orthogonaux, alors $f(U)f(V) + f(V)f(U) = f(UV + VU) = f(0) = 0$, donc f préserve l'orthogonalité. De même, f préserve la norme : en effet, la relation $f(U^2) = f(U)^2$ s'écrit d'une part $f(-N(U)E)$ et d'autre part $-N(f(U))E$.

Ainsi, $(f(I), f(J), f(K))$ est une base orthonormée de \mathbb{H}^{im} . Il existe alors un signe $\varepsilon = \pm 1$ tel que $(f(I), f(J), \varepsilon f(K))$ est une base directe de \mathbb{H}^{im} .

Mais alors il existe $u \in S$ tel que

$$\alpha(u, u) \cdot I = f(I), \quad \alpha(u, u) \cdot J = f(J) \quad \text{et} \quad \alpha(u, u) \cdot K = \varepsilon f(K)$$

Mais alors, la relation $f(I)f(J) = f(K)$ s'écrit

$$(\alpha(u, u) \cdot I)(\alpha(u, u) \cdot J) = f(K) \quad \text{et} \quad (\alpha(u, u) \cdot I)(\alpha(u, u) \cdot J) = \alpha(u, u) \cdot K = \varepsilon f(K)$$

Donc, $\varepsilon = 1$. Ainsi, $(f(I), f(J), f(K))$ est directe.

13. (a) Il s'agit de montrer que l'application $u \in \text{Aut}(\mathbb{H}) \mapsto u|_{\mathbb{H}^{\text{im}}} \in SO(\mathbb{H}^{\text{im}})$ est un isomorphisme. Déjà elle est bien définie, en effet, on a vu à la question précédente qu'un automorphisme transforme une base orthonormée directe en une base orthonormée directe, donc $u|_{\mathbb{H}^{\text{im}}} \in SO(\mathbb{H}^{\text{im}})$.
On a déjà vu qu'il était surjectif à la question 8.
Enfin, si u induit l'identité sur \mathbb{H}^{im} , alors, comme il induit l'identité déjà sur $\mathbb{R}\mathbb{H}$, on en déduit que u est l'identité. Autrement dit, la restriction est injective. On a ainsi un isomorphisme de groupes

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

- (b) Soit u un automorphisme de \mathbb{H} , alors il existe $v \in S$ tel que $u|_{\mathbb{H}^{\text{im}}} = \alpha(v, v)|_{\mathbb{H}^{\text{im}}}$, ces deux applications coïncident sur $\mathbb{R}\mathbb{H}$, ainsi $u = \alpha(v, v)$.

3 Normes euclidiennes sur \mathbb{R}^2

14. (a) Soit $A \in \mathcal{K}$, on considère la norme subordonnée à la norme $\|\cdot\|$, ie $\|A\| = \sup_{\|x\|=1} \|Ax\|$, prenons x unitaire de sorte que $\|A\| = \|Ax\|$, alors on a $\|A\| \leq \|x\|_2$ et donc \mathcal{K} est borné.
Soit $x \in \mathbb{R}^2$, on note $f_x : A \mapsto \|Ax\|$ continue, alors $f_x^{-1}([0, \|x\|_2])$ est un fermé comme image réciproque d'un fermé. Alors, \mathcal{K} est fermé comme intersection de fermés.
Ainsi, \mathcal{K} est un fermé borné, donc compact de $M_2(\mathbb{R})$.

Soit $A, B \in \mathcal{K}$ et $\lambda \in [0, 1]$. Soit $x \in \mathbb{R}^2$, alors

$$\|(\lambda A + (1 - \lambda)B)x\| \leq \lambda \|Ax\| + (1 - \lambda) \|Bx\| \leq \lambda \|x\|_2 + (1 - \lambda) \|x\|_2 = \|x\|_2$$

Ainsi, $\lambda A + (1 - \lambda)B \in \mathcal{K}$ et donc \mathcal{K} est convexe.

- (b) L'application \det est continue sur le compact \mathcal{K} , ainsi elle réalise sa borne supérieure en un point de \mathcal{K} .
15. Comme $\|\cdot\|$ et $\|\cdot\|_2$ sont équivalentes, il existe une constante C tel que $\|\cdot\| \leq C\|\cdot\|_2$. Alors, la matrice $A = \frac{1}{C}I_n$ est un élément de \mathcal{K} , donc le déterminant est > 0 . Ainsi, $\det(A) > 0$.

\mathcal{C} étant compact, il existe $x \in \mathcal{C}$ pour lequel $\|Ax\|$ est maximal, on note $\alpha = \|Ax\|$. Par hypothèse, on a $\alpha \leq 1$. Supposons par l'absurde que $\alpha < 1$, alors $\frac{1}{\alpha}A \in \mathcal{K}$. En effet, si $x \in \mathcal{C}$, on a

$$\left\| \frac{1}{\alpha}Ax \right\| \leq 1 = \|x\|_2$$

Si $y \in \mathbb{R}^2 \setminus \{0\}$, $x = \frac{y}{\|y\|_2} \in \mathcal{C}$ et donc, on a

$$\left\| \frac{1}{\alpha}Ay \right\| = \left\| \frac{\|y\|_2}{\alpha}Ax \right\| \leq \|y\|_2$$

Et donc, on a $\frac{1}{\alpha}A \in \mathcal{K}$ et $\frac{1}{\alpha} > 1$, donc $\det\left(\frac{1}{\alpha}A\right) > \det(A)$, ce qui contredit la maximalité de $\det(A)$. Ainsi, $\|Ax\| = 1$.

16. (a) On remarque que $AB \in K$, en effet, $\|ABx\| \leq \|Bx\|_2 = \|x\|_2$ car B est orthogonale.

Supposons par l'absurde que pour tout $x_r \in \mathcal{C}$, $\left\| AB \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} x_r \right\| \leq 1$, c'est-à-dire $AB \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix}$. Par convexité, on a

$$C_r := (1-r)AB \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} + rAB \in K$$

Or,

$$\det(C_r) = \det(AB) \begin{vmatrix} (1-r)r + r & 0 \\ 0 & \frac{1-r}{r} + r \end{vmatrix} = \det(A)(2-r)(r^2 - r + 1)$$

Une étude de la fonction $r \mapsto (2-r)(r^2 - r + 1)$ montre qu'elle est strictement décroissante sur $]0, 1[$, donc $g(r) > g(1) = 1$, ie $\det(C_r) > \det(A)$, ce qui contredit la maximalité de $\det(A)$.

(b) Comme $x_r \in \mathcal{C}$, on a déjà $y_r^2 + z_r^2 = 1$. De plus,

$$1 < \left\| AB \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} x_r \right\|^2 \leq \left\| \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} x_r \right\|_2^2 = r^2 y_r^2 + \frac{z_r^2}{r^2}$$

Cette inégalité s'écrit $z_r^2(r^{-2} - r^2) + r^2 > 1$, ie $z_r^2 > \frac{1-r^2}{r^{-2} - r^2}$. Or, on a $\frac{1-r^2}{r^{-2} - r^2} = \frac{r^2 - r^4}{1 - r^4} = \frac{r^2}{1 + r^2}$. D'où l'inégalité

$$z_r^2 > \frac{r^2}{1 + r^2}$$

17. Soit (r_n) une suite d'éléments de $]0, 1[$ qui converge vers 1. Alors la suite $(x_{r_n})_{n \in \mathbb{N}}$ est à valeurs dans le compact \mathcal{C} et donc, quitte à extraire, on suppose qu'elle converge vers $x^* \in \mathcal{C}$. On passe à la limite dans

l'inégalité $1 < \left\| AB \begin{pmatrix} r_n & 0 \\ 0 & \frac{1}{r_n} \end{pmatrix} x_{r_n} \right\|$ pour obtenir $1 \leq \|ABx^*\|$.

Mais d'autre part, $\|ABx^*\| \leq \|Bx^*\|_2 = \|x^*\|_2 = 1$, donc en fait on a égalité :

$$\|ABx^*\| = 1$$

De plus, l'inégalité $z_{r_n} > \frac{r_n^2}{1 + r_n^2}$ passe à la limite en $z^* \geq \frac{1}{2}$, donc (e_1, x^*) est une base de \mathbb{R}^2 (où e_1 est le premier vecteur de la base canonique). On considère $x_1 = Be_1 = x$ et $x_2 = Bx^*$, on a alors par construction :

$$\|Ax_1\| = 1 = \|x_1\|_2 \quad \text{et} \quad \|Ax_2\| = \|ABx^*\| = 1 = \|x_2\|_2$$

18. L'idée est de raisonner géométriquement en paramétrisant le cercle par l'exponentielle complexe qui permet plutôt de raisonner sur les angles, puis de raisonner par dichotomie sur les angles.

- Soit $T' = \{x \in T, -x \in T\}$. On montre que si $a \in T'$ et $b \in T$ avec $a \neq \pm b$, alors $\frac{a+b}{\|a+b\|_2} \in T'$.
En effet, on a $-a \in T$ et $-a \neq \pm(-b)$, donc $\frac{-a-b}{\|a+b\|_2} = -\frac{a+b}{\|a+b\|_2} \in T$ et donc $\frac{a+b}{\|a+b\|_2} \in T'$.

De plus, il existe $a, b \in T'$ tels que $a \neq \pm b$. En effet, soit $x, y \in T$ tels que $x \neq \pm y$, qui existent pas hypothèse sur T . Soit $a = \frac{x-y}{\|x-y\|_2} \in T$ et comme $-a$ est aussi dans T par symétrie, on en déduit que $a \in T'$. Et on prend pour b soit x , soit y . En effet, si on avait $a \in \{\pm x, \pm y\}$, alors $x = \pm y$, ce qui est exclu.

- On considère $e : \theta \in \mathbb{R} \mapsto e^{2i\pi\theta} \in \mathcal{C}$. On note $R = e^{-1}(T')$. Dire que $e(\theta) = \pm e(\psi)$ revient à dire que $\theta \notin \psi + \frac{1}{2}\mathbb{Z}$.

Si $\theta \in R$ et $\psi \in e^{-1}(T)$ avec $\theta \notin \psi + \frac{1}{2}\mathbb{Z}$. On va montrer que $\frac{\theta+\psi}{2} \in R$.

Comme $e(\theta) + e(\psi) = 2 \cos\left(\frac{\theta-\psi}{2}\right) e\left(\frac{\theta+\psi}{2}\right)$, on a $\frac{e(\theta) + e(\psi)}{\|e(\theta) + e(\psi)\|_2} = \pm e\left(\frac{\theta+\psi}{2}\right)$.

Si le signe est positif, alors $\frac{\theta+\psi}{2} \in R$, sinon le signe est négatif, mais comme on a $-\frac{e(\theta) + e(\psi)}{\|e(\theta) + e(\psi)\|_2} \in T'$

et on en déduit que $\frac{\theta+\psi}{2} \in R$.

- On fixe $x \in \mathbb{R}$ un angle quelconque. On va construire deux suites d'angles (θ_k) et (ψ_k) d'éléments de R telles que $\theta_k \leq x \leq \psi_k$, $\theta_k \notin \psi_k + \frac{1}{2}\mathbb{Z}$, $|\theta_k - \psi_k| \leq \frac{1}{2^k}|\theta_0 - \psi_0|$ avec (θ_k) croissante et (ψ_k) décroissante.

On commence par choisir $\theta \in R$ quelconque et $\psi \in e^{-1}(T)$ quelconque tel que $\theta \notin \psi + \frac{1}{2}\mathbb{Z}$. On sait que $\frac{\theta+\psi}{2} \in R$. Si de plus, on avait $\frac{\theta+\psi}{2} \in \theta + \frac{1}{2}\mathbb{Z}$, alors $\psi \in \theta + \frac{1}{2}\mathbb{Z}$, ce qui n'est pas.

En particulier, il existe $\theta, \theta' \in R$ tels que $\theta \notin \theta' + \frac{1}{2}\mathbb{Z}$. Ceci reste vrai en prenant θ et θ' modulo 1, on peut alors trouver $k, \ell \in \mathbb{Z}$ tels que $\theta_0 := \theta + k \leq x \leq \psi_0 := \theta' + \ell$.

Supposons que les deux suites (θ_k) et (ψ_k) ont leur n premiers termes construits. Alors $\frac{\theta_n + \psi_n}{2} \in R$ et n'est ni dans $\theta_n + \frac{1}{2}\mathbb{Z}$, ni dans $\psi_n + \frac{1}{2}\mathbb{Z}$.

Si $\theta_n \leq x \leq \frac{\theta_n + \psi_n}{2}$, on pose $\theta_{n+1} = \theta_n$ et $\psi_{n+1} = \frac{\theta_n + \psi_n}{2}$. Dans l'autre cas, $\frac{\theta_n + \psi_n}{2} \leq x \leq \psi_n$ et on pose $\psi_{n+1} = \psi_n$ et $\theta_{n+1} = \frac{\theta_n + \psi_n}{2}$. Dans les deux cas, on a $|\psi_{n+1} - \theta_{n+1}| \leq \frac{1}{2}|\psi_n - \theta_n| \leq \frac{1}{2^{n+1}}|\psi_0 - \theta_0|$ et $\theta_{n+1} \leq x \leq \psi_{n+1}$ et $\theta_{n+1} \notin \psi_{n+1} + \frac{1}{2}\mathbb{Z}$ et $\psi_{n+1} \leq \psi_n$ et $\theta_{n+1} \geq \theta_n$.

On a ainsi construit de suites d'angles (θ_k) et (ψ_k) avec les propriétés voulues, elles sont alors adjacentes, donc convergent vers la même limite. Et comme $\theta_k \leq x \leq \psi_k$, on en déduit que cette limite est x . On a ainsi montré que R est dense dans \mathbb{R} et donc par continuité et surjectivité de e , T est dense dans \mathcal{C} et comme T est fermé : $T = \mathcal{C}$.

19. Supposons qu'on ait une norme telle que pour tout x, y unitaire (pour cette norme), $\|x+y\|^2 + \|x-y\|^2 \geq 4$. On prend A, x_1, x_2 des questions précédentes et $T = \{x \in \mathcal{C}, \|Ax\| = 1\}$. Par construction via la question 17., T contient une base (y_1, y_2) de \mathbb{R}^2 où chaque y_i est unitaire (pour la norme $\|\cdot\|$). Si $a, b \in T$ avec $b \neq \pm a$, alors

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

et $\|A(a \pm b)\| \leq \|a \pm b\|_2$, on a

$$4 \leq \|A(a+b)\|^2 + \|A(a-b)\|^2 \leq \|a+b\|_2^2 + \|a-b\|_2^2 = 4$$

On a donc en fait égalité partout, ie $\|A(a \pm b)\| = \|a \pm b\|_2$ et donc $\frac{a \pm b}{\|a \pm b\|_2} \in T$. De plus, T est fermé. Donc, par la question précédente, $T = \mathcal{C}$, ie

$$\forall x \in \mathcal{C}, \|Ax\| = 1$$

ce qui implique en particulier que

$$\forall x \in \mathbb{R}^2, \|Ax\| = \|x\|_2$$

Comme A est inversible, on a $\|x\| = \|A^{-1}x\|_2$ et donc $\|\cdot\|$ est euclidienne qui vient du produit scalaire $\langle x|y \rangle = \langle A^{-1}x, A^{-1}y \rangle$.

4 Algèbres valuées

20. (a) Soit $x \in A$, par hypothèse, il existe un polynôme non nul $P \in \mathbb{R}[X]$ tel que $P(x) = 0$. Ainsi, l'idéal $\{P \in \mathbb{R}[X], P(x) = 0\}$ est non réduit à 0 et est donc engendré par un unique polynôme Q unitaire de degré minimal. Q est irréductible, en effet sinon, un de ses facteurs annulerait x , ce qui n'est pas possible. Ainsi, $\deg(Q) \leq 2$, ie $x^2 \in \mathbb{R} + \mathbb{R}x$.
- (b) Comme $x \notin \mathbb{R}$, on prend un polynôme de degré 2 irréductible tel que $P(x) = 0$. Son discriminant $\Delta < 0$ admet alors une racine carrée (forme canonique d'un polynôme de degré 2) et donc -1 aussi, que l'on note abusivement $\sqrt{-1}$. Alors $a + b\sqrt{-1} \in \mathbb{R} + \mathbb{R}x \mapsto a + ib \in \mathbb{C}$ est un isomorphisme d'algèbres.
21. Comme A n'est pas isomorphe à \mathbb{R} , on peut prendre $x \in A \setminus \mathbb{R}$ et par le même procédé que précédemment, on trouve que $i_A^2 = -1$.
22. (a) Soit $x, y \in A$, on calcule :

$$T(xy) = i_A x y i_A = -(i_A x i_A)(i_A y i_A) = -T(x)T(y)$$

(b) Soit $x \in A$, on a

$$T^2(x) = i_A(i_A x i_A)i_A = x$$

Donc, $T^2 = \text{Id}$ qui est une symétrie. Ainsi, on en déduit immédiatement que

$$A = \text{Ker}(T - \text{Id}) \oplus \text{Ker}(T + \text{Id})$$

23. On a

$$\text{Ker}(T + \text{Id}) = \{x \in A, i_A x i_A = -x\}$$

On a $1, i_A \in \text{Ker}(T + \text{Id})$, de sorte que $U \subset \text{Ker}(T + \text{Id})$.

Réciproquement, si $x \in \text{Ker}(T + \text{Id})$, alors $i_A x i_A = -x$ et en multipliant à gauche par i_A , on remarque que x commute avec i_A .

Fixons x non nul qui commute avec i_A . En décomposant $(i_A x)^2$ de deux manières, on trouve via la question 20. :

$$a + b i_A x = c + dx \iff (b i_A - d)x = c - b$$

Comme U est un corps (isomorphe à \mathbb{C}), $b - i_A d$ est inversible dans U , donc $x = \frac{c - d}{b i_A d} \in U$. Sauf dans le cas où $b = d = 0$ et dans ce cas, $(i_A x)^2 = -x^2 \in \mathbb{R}$, donc $x^2 \in \mathbb{R}$. Et donc, si $x^2 \geq 0$, $x \in \mathbb{R}$, sinon, $x = \pm i_A \sqrt{-x^2} \in U$.

Dans tous les cas, $x \in U$ et donc, on a montré que $\text{Ker}(T + \text{Id}) \subset U$. D'où l'égalité par double inclusion :

$$\text{Ker}(T + \text{Id}) = U$$

Ainsi, comme A n'est pas isomorphe à \mathbb{C} et que $\text{Ker}(T - \text{Id})$ est de dimension 2, nécessairement, $\text{Ker}(T - \text{Id})$ ne peut être réduit à 0.

24. (a) Soit $x \in \text{Ker}(T - \text{Id})$, de sorte que

$$T(\beta x) = -T(\beta)T(x) = -T(\beta)x = -\beta x$$

Donc, $\beta x \in \text{Ker}(T + \text{Id})$.

On a alors en prenant $x = \beta$ que $\beta^2 \in \text{Ker}(T + \text{Id}) = U$.

Par intégrité, $x \in \text{Ker}(T - \text{Id}) \mapsto \beta x \in \text{Ker}(T + \text{Id})$ est injectif. On en déduit que $\text{Ker}(T - \text{Id})$ est de dimension finie, de dimension 1 ou 2.

Si $\text{Ker}(T - \text{Id})$ était de dimension 1, alors on a $T(i_A\beta) = -T(i_A)T(\beta) = i_A\beta$, donc $i_A\beta \in \text{Ker}(T - \text{Id})$ et donc, il existe $\lambda \in \mathbb{R}$ tel que $i_A\beta = \lambda\beta$, ce qui donne $i_A = \lambda \in \mathbb{R}$, contradiction.

Ainsi, $\text{Ker}(T - \text{Id})$ est de dimension 2. Si $y \in \beta U$, on écrit $y = \beta x$ avec $x \in U$. On a alors

$$\begin{aligned} T(y) - y &= T(\beta x) - \beta x \\ &= -T(\beta)T(x) - \beta x \\ &= \beta x - \beta x = 0 \end{aligned}$$

D'où l'inclusion $\beta U \subset \text{Ker}(T - \text{Id})$ et par égalité de dimension, on a égalité $\text{Ker}(T - \text{Id}) = \beta U$.

(b) On a $U \cap (\mathbb{R} + \mathbb{R}\beta) = \mathbb{R}$, et donc $\beta^2 \in \mathbb{R}$. Si $\beta^2 > 0$, alors on peut écrire $\beta = \pm\gamma \in \mathbb{R}$. Mais alors, β ne peut pas anticommute avec i_A , donc $\beta \notin \text{Ker}(T + \text{Id})$. On en déduit alors que $\beta^2 < 0$.

(c) Quitte à remplacer β par $\frac{\beta}{-\beta^2}$, on suppose que $\beta^2 = -1$. On considère alors $(1, i_A)$ une base de U et $(\beta, \beta i_A)$ qui est une base de $\beta U = \text{Ker}(T - \text{Id})$, ainsi comme $A = U \oplus \beta U$, on a que $(1, i_A, \beta, i_A\beta)$ est une base de A . On a

$$(i_A\beta)^2 = (i_A\beta i_A)\beta = \beta^2 = -1$$

et

$$i_A\beta(i_A\beta) = (i_A\beta)^2 = -1$$

Ainsi, on considère le morphisme d'algèbres $A \longrightarrow \mathbb{H}$ tel que

$$1 \longmapsto E, \quad i_A \longmapsto I, \quad \beta \longmapsto J \quad \text{et} \quad i_A\beta \longmapsto K$$

qui est alors un isomorphisme de \mathbb{R} -algèbres, car elle envoie une base sur une base. On en déduit que

$$A \simeq \mathbb{H}$$

en tant que \mathbb{R} -algèbres.

On en déduit que les seules \mathbb{R} -algèbres algébrique et sans diviseur de zéros sont isomorphes à \mathbb{R} , \mathbb{C} ou \mathbb{H} .

25. Soit $u, v \in V$, alors comme x et y commutent, u et v aussi et on a $(u + v)^2 + (u - v)^2 = 4uv$. On en déduit donc par inégalité triangulaire et multiplicativité que :

$$4\|u\|\|v\| = 4\|uv\| \leq \|u + v\|^2 + \|u - v\|^2$$

Ainsi, prenant u et v unitaires, on en déduit par le Théorème A, $\|\cdot\|$ restreinte à V provient d'un produit scalaire.

26. On applique le résultat précédent avec $V = \mathbb{R}1 + \mathbb{R}x$. Soit y un vecteur non nul orthogonal unitaire à 1 dans V de sorte qu'on puisse écrire $x = a + by$. Afin de voir que $x^2 \in \mathbb{R} + \mathbb{R}x$, on montre que $y^2 = -1$.

On a $\|1 + y\|^2 = \|1 - y\|^2 = 2$ et donc par produit $\|1 - y^2\|^2 = 4$ et donc $\langle 1, y^2 \rangle = -1$. L'angle entre 1 et y^2 dans le plan V est plat, donc $y^2 = -1$.

27. On a ainsi montré que A était algébrique. Reste à montrer que A est intègre : si $xy = 0$, alors $\|xy\| = \|x\|\|y\| = 0$ et donc $\|x\|$ ou $\|y\| = 0$ et donc x ou y est nul. D'après le théorème B, A est isomorphe à \mathbb{R} , \mathbb{C} ou \mathbb{H} .