Devoir surveillé n°7

Sujet donné le vendredi 2 février 2024, 4h.

L'usage de la calculatrice n'est pas autorisé.

La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées. Les réponses aux questions seront numérotées et séparées par un trait horizontal. Les résultats essentiels devront être encadrés ou soulignés.**

BON TRAVAIL

Problème - Quaternions

Objectifs du problème :

Dans tout le problème, on souhaite étudier l'anneau des quaternions.
Dans la première partie, on donne une façon de construire les éléments de base des quaternions : un certain triplet $(\mathrm{I}, \mathrm{J}, \mathrm{K})$ à partir de l'ensemble des matrices d'ordre 2 sur le corps $\mathbb{F}_3$. Dans le seconde partie, on obtient les résultats (algèbriques) fondamentaux du corps des quaternions. On peut faire le parallèle avec les corps des complexes.
En troisième partie, nous étudions l'anneau des entiers de Hamilton. Nous terminons par une première application en arithmétique sur le théorème des quatre carrés.
Nous étudions une seconde application, géométrique, dans la quatrième partie.

Notation du problème :

Soit $\mathbb{K}$, un corps quelconque. On note $\mathcal{M}_2(\mathbb{K})$, l'anneau (et espace vectoriel) des matrices à deux coefficients définies sur le corps $\mathbb{K}$.
On rappelle que $(GL_2(\mathbb{K}), \times)$ est un groupe (c'est l'anneau des inversibles de $\mathcal{M}_2(\mathbb{K})$).
On définit

- $\det : \mathcal{M}_2(\mathbb{K}) \to \mathbb{K}$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$.
  Si besoin, on pourra utiliser, sans démonstration : $\forall\, M_1, M_2 \in \mathcal{M}_2(\mathbb{K})$, $\det(M_1 \times M_2) = \det M_1 \times \det M_2$.
- $\mathrm{tr} : \mathcal{M}_2(\mathbb{K}) \to \mathbb{K}$, $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$
- Pour tout $i, j \in \{1, 2\}$, et toute matrice $M \in \mathcal{M}_2(\mathbb{K})$, $[M]_{i,j}$ désigne le coefficient en ligne i et colonne j de la matrice M.

I Groupe quaternionique

On note $(\mathbb{F}_3, +, \times)$ le corps à trois éléments $0, 1, -1(= 2)$ avec les lois d'addition et de multiplication modulo 3 (souvent appelé $\dfrac{\mathbb{Z}}{3\mathbb{Z}}$).

I.1. Etude de $SL_2(\mathbb{K})$ pour un corps $\mathbb{K}$ quelconque.

(a) Montrer que pour tout matrice $A \in \mathcal{M}_2(\mathbb{K})$,

$$A^2 - \mathrm{tr}(A)A + \det(A)I_2 = 0_2$$

(b) En déduire que A est inversible si et seulement si $\det(A) \neq 0$.
Exprimer, dans ce cas A^{-1} en fonction des coefficients de A.

(c) On note $SL_2(\mathbb{K}) = \{A \in \mathcal{M}_2(\mathbb{K}) \mid \det(A) = 1\}$.
Montrer que $(SL_2(\mathbb{K}), \times)$ est un sous-groupe de $(GL_2(\mathbb{K}), \times)$.

(d) Soit $A \in SL_2(\mathbb{K})$.
Montrer l'équivalence : $A^2 = -I_2 \iff \mathrm{tr}(A) = 0$

I.2. Ensemble $\mathcal{M}_2(\mathbb{F}_3)$ et groupe $\mathbb{H}_8$.

(a) Donner la liste des 6 éléments A de $SL_2(\mathbb{F}_3)$ tel que $A^2 = -I_2$.

(b) Construire un (le) groupe $\mathbb{H}_8$, à 8 éléments : $\mathbb{H}_8 = \{1, -1, \mathrm{I}, -\mathrm{I}, \mathrm{J}, -\mathrm{J}, \mathrm{K}, -\mathrm{K}\}$, où $1 = I_2$ et tel que le carré des 6 derniers éléments vaut bien -1.
Avec un tableau, on vérifiera bien que $\times$ est une loi de composition interne sur $\mathbb{H}_8$.
Le groupe $\mathbb{H}_8$ s'appelle le groupe quaternionique.

(c) Le groupe $(\mathbb{H}_8, \times)$ est-il commutatif ?

Par la suite, on s'intéresse aux quaternions ou nombres de Hamilton de la forme $a + bI + cJ + dK$ où $I, J, K \in \mathbb{H}$ avec $a, b, c, d \in \mathbb{R}$.
On choisit un autre type de représentation de cet ensemble en partie II.

II Anneau des quaternions

On considère le groupe $\mathbb{H}_8 = \{1, -1, \mathrm{I}, -\mathrm{I}, \mathrm{J}, -\mathrm{J}, \mathrm{K}, -\mathrm{K}\}$ défini en partie précédente, avec les propriétés caractéristiques précédentes.
On note $\mathbb{H}$ l'ensemble des quaternions. Il est défini par :

$$\mathbb{H} = \{a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \mid (a, b, c, d) \in \mathbb{R}^4\}$$

avec les règles opératoires suivantes pour $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ et $z' = a' + b'\mathrm{I} + c'\mathrm{J} + d'\mathrm{K} \in \mathbb{H}$:

$$\begin{cases} z + z' = (a + a') + (b + b')\mathrm{I} + (c + c')\mathrm{J} + (d + d')\mathrm{K} \\ z \times z' = (aa' - bb' - cc' - dd') + (ab' + a'b + cd' - c'd)\mathrm{I} + (ac' + a'c + db' - d'b)\mathrm{J} + (ad' + a'd + bc' - b'c)\mathrm{K} \end{cases}$$

On pourrait vérifier que ces règles confirment : $\mathrm{I}^2 = \mathrm{J}^2 = \mathrm{K}^2 = -1$ et $\mathrm{IJ} = \mathrm{K} = -\mathrm{JI}$, $\mathrm{JK} = \mathrm{I} = -\mathrm{KJ}$ et $\mathrm{KI} = \mathrm{J} = -\mathrm{IK}$.
On admet que l'écriture des éléments de $\mathbb{H}$ de cette façon : $a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ est unique (écriture dite *algèbrique*).
Cela signifie qu'on peut identifier :

$$z = z' \quad \Longleftrightarrow \quad \begin{cases} a = a' \\ b = b' \\ c = c' \\ d = d' \end{cases}$$

On considère également l'anneau $\mathcal{M}_2(\mathbb{C})$ des matrices carrés à coefficients dans $\mathbb{C}$.
On note $Q = \{A \in \mathcal{M}_2(\mathbb{C}) \mid [A]_{1,1} = \overline{[A]_{2,2}}$ et $[A]_{1,2} = -\overline{[A]_{2,1}}\}$ (la barre horizontale signifiant ici la conjugaison dans $\mathbb{C}$).

II.1. Etude de la structure de Q.

(a) Montrer que $(Q, +)$ est un sous-groupe de $\mathcal{M}_2(\mathbb{C})$.

(b) Montrer que si $A \in Q$, $\det A \geqslant 0$. Puis : $A = 0$ si et seulement si $\det A = 0$

(c) Montrer que $Q^* := Q \setminus \{0\}$ est un groupe (pour la loi $\times$).

II.2. On note $\Phi : A \in Q \mapsto \mathrm{Re}([A]_{1,1}) + \mathrm{Im}([A]_{1,1}) \times \mathrm{I} + \mathrm{Re}([A]_{1,2}) \times \mathrm{J} + \mathrm{Im}([A]_{1,2}) \times \mathrm{K}$.

(a) Montrer que l'image de Q par Φ est exactement $\mathbb{H}$.

(b) Montrer que $(\mathbb{H}, +, \times)$ est un anneau. Est-il commutatif ?
On déduit de cette question les propriétés de distributivité dans $\mathbb{H}$.

II.3. Conjugaison et module.

(a) On appelle conjugué dans $\mathbb{H}$, l'application $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \mapsto \overline{z} = a - b\mathrm{I} - c\mathrm{J} - d\mathrm{K}$.
Le contexte permet de différencier la conjugaison sur $\mathbb{C}$ ou sur $\mathbb{H}$.
Evaluer, pour tout $z \in \mathbb{H}$, $z \times \overline{z}$ et $\overline{z} \times z$. Montrer que $z \times \overline{z} \in \mathbb{R}_+$.

(b) Montrer que pour tout $z, z' \in \mathbb{H}$, $\overline{z \times z'} = \overline{z'} \times \overline{z}$

(c) On note $|z| = \sqrt{z\overline{z}}$.
Montrer que pour tout $z, z' \in \mathbb{H}$, $|\overline{z}| = |z|$ et que $|zz'| = |z| \times |z'| = |z'z|$.

(d) Déduire que $\mathbb{H}$ est un anneau sans diviseur de zéro et que z est inversible (pour $\times$ et dans $\mathbb{H}$) si et seulement si $z \neq 0$.
Exprimer alors z^{-1}.

(e) Déduire également la relation algébrique : $\forall\ a, b, c, d, x, y, z, t \in \mathbb{R}$

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = (ax - by - cz - dt)^2 + (ay + bx + ct - dz)^2 + (az + bx + cy - dt)^2 + (at + bx + cz - dy)^2$$

Cette relation est-elle vraie dans d'autres anneaux que $\mathbb{R}$? Lesquels ?

II.4. Quaternions unitaires et quaternions purs.
On dit que $z \in \mathbb{H}$ est unitaire si $|z| = 1$. On note $\mathbb{U}_\mathbb{H} = \{z \in \mathbb{H} \mid |z| = 1\}$.
On dit que $z \in \mathbb{H}$ est quaternion pur si $z + \overline{z} = 0$. On note $\mathbb{I}_\mathbb{H} = \{z \in \mathbb{H} \mid z + \overline{z} = 0\}$

(a) Montrer que pour tout $z \in \mathbb{H}^* := \mathbb{H} \setminus \{0\}$, il existe un unique couple $(r, u) \in \mathbb{R}_+^* \times \mathbb{U}_\mathbb{H}$ tel que $z = ru$

(b) Montrer que pour tout $z \in \mathbb{U}_\mathbb{H}$, il existe $\theta \in [0, \pi]$ et $s \in \mathbb{I}_\mathbb{H} \cap \mathbb{U}_\mathbb{H}$ tel que $z = \cos\theta + s \times \sin\theta$

III Anneau euclidien des entiers de Hamilton

Soit $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \in \mathbb{H}$.

On dit que z est entier d'Hamilton ou entier de $\mathbb{H}$ si $(a, b, c, d) \in \mathbb{Z}^4$ ou $(a - \frac{1}{2}, b - \frac{1}{2}, c - \frac{1}{2}, d - \frac{1}{2}) \in \mathbb{Z}^4$
On note $\mathbb{H}(\mathbb{Z})$ l'ensemble des entiers de $\mathbb{H}$.

III.1. Montrer que $\mathbb{H}(\mathbb{Z}) = \left\{\frac{x}{2}(1 + \mathrm{I} + \mathrm{J} + \mathrm{K}) + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}, (x, y, z, t) \in \mathbb{Z}^4\right\}$.

III.2. Montrer que si $z, z' \in \mathbb{H}(\mathbb{Z})$, alors $z + z'$ et $z \times z' \in \mathbb{H}(\mathbb{Z})$ et que si $z \in \mathbb{H}(\mathbb{Z})$ alors $|z|^2 \in \mathbb{N}$.

III.3. Un élément z de $\mathbb{H}$ est appelé une unité si z et z^{-1} sont tous les deux des entiers de $\mathbb{H}(\mathbb{Z})$.
Montrer que si z est une unité de $\mathbb{H}$ alors $|z| = 1$ i.e. $z \in \mathbb{U}_\mathbb{H}$

III.4. Donner la liste des 24 éléments de $\mathbb{H}(\mathbb{Z})^\times$, i.e. des inversibles ou unités de $\mathbb{H}(\mathbb{Z})$.

III.5. Anneau euclidien.

(a) Soit $z \in \mathbb{H}$.
Montrer qu'il existe $e \in \mathbb{H}(\mathbb{Z})$ tel que $|z - e|^2 \leqslant \frac{5}{8}$.

(b) Soient $z_1, z_2 \in \mathbb{H}(\mathbb{Z})$ avec $z_2 \neq 0$, montrer qu'il existe $q, r \in \mathbb{H}(\mathbb{Z})$ tel que $z_1 = qz_2 + r$ avec $|r| < |z_2|$.
On parle d'une division euclidienne à gauche.

III.6. Idéal à gauche. PGCD.
On dit que I est un idéal à gauche de l'anneau $\mathbb{H}(\mathbb{Z})$ si :
— $(I, +)$ est un sous-groupe $(\mathbb{H}(\mathbb{Z}), +)$
— $\forall\ a \in \mathbb{H}(Z)$ et $x \in I$, $ax \in I$ (l'ordre est important)

(a) Montrer que pour tout $z \in \mathbb{H}(\mathbb{Z})$, $(z) := \{az \mid a \in \mathbb{H}(\mathbb{Z})\}$ est un idéal à gauche de $\mathbb{H}(\mathbb{Z})$

(b) Montrer que si I_1 et I_2 sont deux idéaux à gauche de $\mathbb{H}(\mathbb{Z})$,
$I_1 + I_2 := \{a_1 + a_2 \mid a_1 \in I_1, a_2 \in I_2\}$ et $I_1 \cap I_2$ sont des idéaux à gauche de $\mathbb{H}(\mathbb{Z})$.

(c) Montrer que pour tout idéal à gauche I de $\mathbb{H}(\mathbb{Z})$, il existe $z \in \mathbb{H}(\mathbb{Z})$ tel que $I = (z)$.

(d) Comment pourrait-on définir le PGCD de deux nombres de $\mathbb{H}(\mathbb{Z})$.

III.7. Nombre premier.
On dit qu'un entier de Hamilton $z \in \mathbb{H}(\mathbb{Z})$ est premier si : $z = uv$ avec $u, v \in \mathbb{H}(\mathbb{Z}) \Longrightarrow u$ ou $v \in \mathbb{U}_{\mathbb{H}}$.
Montrer que les nombres 2, 3, 4,...20 ne sont pas premiers dans $\mathbb{H}(\mathbb{Z})$.

III.8. Application 1. Somme de quatre carrés d'entiers.

(a) Soit $a, b, c, d, a', b', c', d'$ huit entiers naturels, et $n = a^2 + b^2 + c^2 + d^2$, $n' = a'^2 + b'^2 + c'^2 + d'^2$.
En utilisant le module des quaternions, démontrer que le produit nn' est la somme de quatre carrés d'entiers naturels.

(b) Monter que 2 est la somme de 4 carrés.

(c) (**) Montrer que tout nombre premier impair est somme de 4 carrés d'entiers.
On pourra commencer par prouver qu'il existe $z = 1 + a\mathrm{I} + b\mathrm{J}$ tel que p divise $|z|^2 = 1 + a^2 + b^2$.

(d) En déduire que tout nombre entier positif est somme de 4 carrés d'entiers.

IV Application 2 : Géométrie de $\mathbb{R}^3$ (de $\mathbb{R}^4$?)

On note pour tout $z, z' \in \mathbb{H}$, $(z|z') = \dfrac{1}{2}(z\overline{z'} + z'\overline{z})$. On rappelle que la définition de $\mathbb{U}_{\mathbb{H}}$ et de $\mathbb{I}_{\mathbb{H}}$ a été donnée en fin de deuxième partie.

IV.1. Etude du produit scalaire.

(a) Montrer que pour tout $z, z' \in \mathbb{H}$, $(z|z') \in \mathbb{R}$ et $(z|z') = (z'|z)$.

(b) Montrer que pour tout $z \in \mathbb{H}$, $y \mapsto (z|y)$ est linéaire, i.e. vérifie :

$$\forall\ \lambda_1, \lambda_2 \in \mathbb{R}, \forall\ y_1, y_2 \in \mathbb{H} \quad : \quad (z|\lambda_1 y_1 + \lambda_2 y_2) = \lambda_1 (z|y_1) + \lambda_2 (z|y_2)$$

(c) Montrer que $(z|z) \geqslant 0$ et que $(z|z) = 0$ si et seulement si $z = 0$.
On dit que $(\cdot|\cdot)$ est un produit scalaire (compte-tenu des résultats des 3 questions (a), (b), (c)).

(d) Montrer que si $u \in \mathbb{U}_{\mathbb{H}}$, alors pour tout $z, z' \in \mathbb{H}$, $(zu|z'u) = (z|z') = (uz|uz')$.

IV.2. Soient $z, z' \in \mathbb{H}$.
Montrer que $z\overline{z'}z = -|z|^2 z' + 2(z'|z)z$ (formule du triple produit)
On pourra partir du calcul $2(z'|z)z = \ldots$.

IV.3. Produit vectoriel dans $\mathbb{I}_{\mathbb{H}}$ - *ensemble des quaternions purs* (isomorphe à $\mathbb{R}^3$).
On note pour $z = a\mathrm{I} + b\mathrm{J} + c\mathrm{K}$ et $z' = a'\mathrm{I} + b'\mathrm{J} + c'\mathrm{K} \in \mathbb{I}_{\mathbb{H}}$: $\quad z \wedge z' = \dfrac{1}{2}(zz' - z'z)$.

(a) Exprimer $z \wedge z'$ en fonction des lettres a, b, c, a', b', c'.
Quel lien avec le produit vectoriel étudié en S.I. ?

(b) Montrer que pour tout $z, z' \in \mathbb{I}_{\mathbb{H}}$, $zz' = -(z|z') + z \wedge z'$.

IV.4. Rotations (=isométrie).
Soit $q \in \mathbb{U}_{\mathbb{H}} \setminus \{-1, 1\}$ et $r_q : \mathbb{I}_{\mathbb{H}} \to \mathbb{I}_{\mathbb{H}}$, $z \mapsto qzq^{-1}$.

(a) Montrer qu'on a bien, pour tout $z \in \mathbb{I}_{\mathbb{H}}$, $r_q(z) \in \mathbb{I}_{\mathbb{H}}$.

(b) Montrer que pour tout $z, z' \in \mathbb{H}$, $\big(r_q(z)|r_q(z')\big) = (z|z')$.
On dit que r_q est une isométrie (ou rotation) de $\mathbb{I}_{\mathbb{H}}$.

(c) On sait d'après II.4.(c), qu'il existe $\theta \in]0, \pi[$ $(q \notin \{-1, 1\})$, $s \in \mathbb{I}_{\mathbb{H}} \cap \mathbb{U}_{\mathbb{H}}$ tel que $q = \cos\theta + s \times \sin\theta$.
Montrer que $r_q(s) = s$. (On pourra commencer par simplifier s^2)

(d) Soit $t \in \mathbb{I}_{\mathbb{H}} \cap \mathbb{U}_{\mathbb{H}}$ tel que $(s|t) = 0$ (t est orthogonal à s).
Montrer que $(t|r_q(t)) = \cos(2\theta)$ et $t \wedge r_q(t) = \sin(2\theta)s$.
Géométriquement, cela signifie que r_q est la rotation de l'espace $\mathbb{I}_{\mathbb{H}} \sim \mathbb{R}^3$ d'axe s et d'angle 2θ.

IV.5. (**) Justifier la formule exponentielle $q = e^{s\theta}$.
On rappelle que $e^x = \lim\limits_{n \to +\infty} \left(\sum\limits_{k=0}^{n} \dfrac{x^k}{k!} \right)$.

Correction

Problème - Quaternions

I Groupe quaternionique

On note $(\mathbb{F}_3, +, \times)$ le corps à trois éléments $0, 1, -1(=2)$ avec les lois d'addition et de multiplication modulo 3 (souvent appelé $\frac{\mathbb{Z}}{3\mathbb{Z}}$).

I.1. Etude de $SL_2(\mathbb{K})$ pour un corps $\mathbb{K}$ quelconque.

(a) Montrer que pour tout matrice $A \in \mathcal{M}_2(\mathbb{K})$,

$$A^2 - \mathrm{tr}(A)A + \det(A)I_2 = 0_2$$

On mène les calculs (en laissant des traces sur la copie ! - sinon ce sera interprété comme du bluff).

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{K})$. Alors $\mathrm{tr}(A) = a + d$ et $\det A = ad - bc$, puis

$$A^2 = \begin{pmatrix} a^2 + bc & ab + bd \\ ca + dc & bc + d^2 \end{pmatrix} = (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = \mathrm{tr}(A) \cdot A - \det A \cdot I_2$$

$$\boxed{\forall\ A \in \mathcal{M}_2(\mathbb{K}), \qquad A^2 - \mathrm{tr}(A)A + \det(A)I_2 = 0_4}$$

(b) En déduire que A est inversible si et seulement si $\det(A) \neq 0$.
Exprimer, dans ce cas A^{-1} en fonction des coefficients de A.

Si $\det(A) = 0$, on a alors $A^2 = \mathrm{tr}(A) \times A$.

Supposons que A soit inversible, on a alors $A = A^{-1} \times A^2 = \mathrm{tr}(A)A^{-1} \times A = \mathrm{tr}(A)I_2$.

Et par conséquent, on identifiant cette égalité coefficients par coefficients : $a = a + d$, $b = 0$, $c = 0$, $d = a + d$.

Ainsi A est nécessairement la matrice nulle et donc n'est pas inversible (diviseur de 0). On a une contradiction.

Donc A n'est pas inversible.

Si $\det A \neq 0$, alors, comme $A \times (\mathrm{tr}(A)I_2 - A) = \det(A)I_2$, on a

$$A \times \left(\frac{1}{\det A}(\mathrm{tr}AI_2 - A)\right) = \left(\frac{1}{\det A}(\mathrm{tr}AI_2 - A)\right) \times A = I_2$$

Donc A est inversible d'inverse $\frac{1}{\det A}(\mathrm{tr}AI_2 - A) = \frac{1}{\det(A)}\begin{pmatrix} (a+d) - a & -b \\ -c & (a+d) - d \end{pmatrix}$.

$$\boxed{\text{Ainsi } A \text{ est inversible ssi } \det A \neq 0 \text{ et dans ce cas, } A^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.}$$

(c) On note $SL_2(\mathbb{K}) = \{A \in \mathcal{M}_2(\mathbb{K}) \mid \det(A) = 1\}$.
Montrer que $(SL_2(\mathbb{K}), \times)$ est un sous-groupe de $(GL_2(\mathbb{K}), \times)$.

On a bien $I_2 \in SL_2(\mathbb{K})$ car $\det(I_2) = 1 \times 1 - 0 \times 0 = 1$, donc $SL_2(\mathbb{K})$ est non vide.

On va exploiter la caractérisation 2.

Soient $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ deux matrices de $SL_2(\mathbb{K})$.

Alors d'après la question précédente : ${A'}^{-1} = \frac{1}{\det A'}\begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix}$ car $\det A' = 1$.

Puis

$$A \times (A')^{-1} = \begin{pmatrix} ad' - bc' & -ab' + ba' \\ cd' - dc' & -cb' + da' \end{pmatrix}$$

Donc

$$\begin{aligned} \det(A{A'}^{-1}) &= (ad' - bc')(da' - cb') - (ba' - ab')(cd' - dc') \\ &= ada'd' - acd'b' - bda'c' + bcb'c' - bca'd' + bda'c' + acb'd' - adb'c' \\ &= ad(a'd' - b'c') - bc(a'd' - b'c') = ad - bc = 1 \end{aligned}$$

car $A', A \in SL_2(\mathbb{K})$, donc $a'd' - b'c' = ad - bc = 1$.

Par conséquent $A \times {A'}^{-1} \in SL_2(\mathbb{K})$

$$\boxed{(SL_2(\mathbb{K}), \times) \text{ est un sous-groupe de } (GL_2(\mathbb{K}), \times).}$$

On aurait pu aussi exploiter $\det(AB) = \det A \det B = 1 \times 1 = 1$ et $1 = \det(I_2) = \det(AA^{-1}) = \det A \times \det(A^{-1})$, donc $\det(A^{-1}) = 1$

(d) Soit $A \in SL_2(\mathbb{K})$.
Montrer l'équivalence : $A^2 = -I_2 \iff \mathrm{tr}(A) = 0$

Pour toute matrice A de $\mathcal{M}_2(\mathbb{K})$, on a $A^2 = \mathrm{tr}(A)A - \det(A)I_2$.
Donc pour toute matrice $A \in SL_2(\mathbb{K})$, $\det A = 1$ et donc $A^2 = \mathrm{tr}(A)A - I_2$.
Ainsi, on a l'équivalence :

$$\boxed{A^2 = -I_2 \iff \mathrm{tr}(A)A = 0 \iff \mathrm{tr}(A) = 0}$$

car $A \neq 0$, sinon $\det A = 0 \neq -1$

I.2. Ensemble $\mathcal{M}_2(\mathbb{F}_3)$ et groupe $\mathbb{H}_8$.

(a) Donner la liste des 6 éléments A de $SL_2(\mathbb{F}_3)$ tel que $A^2 = -I_2$.

Les éléments de $\mathbb{F}_3$ sont $\{0, 1, -1\}$. Il s'agit donc de matrices d'ordre dont les coefficients sont pris dans ce corps.
Par ailleurs, si $A \in SL_2(\mathbb{F}_3)$, alors $\det A = 1$ et donc pour que $A^2 = -I_2$, il faut (et il suffit) que $\mathrm{tr}(A) = 0$.
On peut faire 0 de trois façons : $0 + 0$ ou $1 + (-1)$ ou encore $(-1) + 1$.
(On note a, b, c et d les quatre coefficients de $A \in SL_2(\mathbb{F}_3)$.)

- Si $a = 0$, alors $d = 0$, donc $1 = ad - bc = -bc$ et donc $bc = -1$ ainsi ($b = 1$ et $c = -1$) ou ($b = -1$ et $c = 1$).
- Si $a = 1$, alors $d = -1$, donc $1 = ad - bc = -1 - bc$ et donc $bc = -2 = 1$ ainsi ($b = 1$ et $c = 1$) ou ($b = -1$ et $c = -1$).
- Si $a = -1$, alors $d = 1$, donc $1 = ad - bc = -1 - bc$ et donc $bc = 1$ ainsi ($b = 1$ et $c = 1$) ou ($b = -1$ et $c = -1$).

Après cette analyse, nous avons trouvé 6 matrices :

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$$

On vérifie réciproquement que chacune de ces 6 matrices appartient à $SL_2(\mathbb{F}_3)$ (à un déterminant égal à 1) et vérifie $A^2 = -I_2$.

Les matrices A de $SL_2(\mathbb{F}_3)$ tels que $A^2 = -I_2$ sont $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$

(b) Construire un (le) groupe $\mathbb{H}_8$, à 8 éléments : $\mathbb{H}_8 = \{1, -1, \mathrm{I}, -\mathrm{I}, \mathrm{J}, -\mathrm{J}, \mathrm{K}, -\mathrm{K}\}$, où $1 = I_2$ et tel que le carré des 6 derniers éléments vaut bien -1.
Avec un tableau, on vérifiera bien que $\times$ est une loi de composition interne sur $\mathbb{H}_8$.

On note (par exemple) $\mathrm{I} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\mathrm{J} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ et $\mathrm{K} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$.
L'ensemble précédent des 6 matrices de $SL_2(\mathbb{F}_3)$ tel que $A^2 = -I_2$ est donc $\{\mathrm{I}, -\mathrm{I}, \mathrm{J}, \mathrm{K}, -\mathrm{J}, -\mathrm{K}\}$.
Montrons maintenant que $\mathbb{H}_8$ est bien un groupe en calculant tous les produits.
Remarquons que $\mathrm{I} \times \mathrm{J} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = \mathrm{K}$, alors que $\mathrm{J} \times \mathrm{I} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} = -\mathrm{K}$, et ainsi de suite, on a le tableau suivant

$\nearrow_\times$	1	-1	I	$-$I	J	$-$J	K	$-$K
1	1	-1	I	$-$I	J	$-$J	K	$-$K
-1	-1	1	$-$I	I	$-$J	J	$-$K	K
I	I	$-$I	-1	1	K	$-$K	$-$J	J
$-$I	$-$I	I	1	-1	$-$K	K	J	$-$J
J	J	$-$J	$-$K	K	-1	1	I	$-$I
$-$J	$-$J	J	K	$-$K	1	-1	$-$I	I
K	K	$-$K	J	$-$J	$-$I	I	-1	1
$-$K	$-$K	K	$-$J	J	I	$-$I	1	-1

Donc la loi est bien interne. On remarque également que tous les éléments sont inversibles. Il reste à vérifier également **l'associativité**.

Si $\mathbb{H}_8 = \{1, -1, \mathrm{I}, -\mathrm{I}, \mathrm{J}, -\mathrm{J}, \mathrm{K}, -\mathrm{K}\}$, alors $(\mathbb{H}_8, \times)$ est bien un groupe à 8 éléments.

Le groupe $\mathbb{H}_8$ s'appelle le groupe quaternionique.

(c) Le groupe $(\mathbb{H}_8, \times)$ est-il commutatif ?

$\mathrm{I} \times \mathrm{J} = \mathrm{K}$ mais $\mathrm{J} \times \mathrm{I} = -\mathrm{K}$.

Donc le groupe $(\mathbb{H}_8, \times)$ n'est pas commutatif.

Par la suite, on s'intéresse aux quaternions ou nombres de Hamilton de la forme $a + bI + cJ + dK$ où $I, J, K \in \mathbb{H}$.
On choisit un autre type de représentation en partie II.

II Anneau des quaternions

On considère le groupe $\mathbb{H}_8 = \{1, -1, \mathrm{I}, -\mathrm{I}, \mathrm{J}, -\mathrm{J}, \mathrm{K}, -\mathrm{K}\}$ défini en partie précédente, avec les propriétés caractéristiques précédentes.
On note $\mathbb{H}$ l'ensemble des quaternions. Il est défini par :

$$\mathbb{H} = \{a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \mid (a, b, c, d) \in \mathbb{R}^4\}$$

avec les règles opératoires suivantes pour $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ et $z' = a' + b'\mathrm{I} + c'\mathrm{J} + d'\mathrm{K} \in \mathbb{H}$:

$$\begin{cases} z + z' = (a + a') + (b + b')\mathrm{I} + (c + c')\mathrm{J} + (d + d')\mathrm{K} \\ z \times z' = (aa' - bb' - cc' - dd') + (ab' + a'b + cd' - c'd)\mathrm{I} + (ac' + a'c + db' - d'b)\mathrm{J} + (ad' + a'd + bc' - b'c)\mathrm{K} \end{cases}$$

On pourrait vérifier que ces règles confirment : $\mathrm{I}^2 = \mathrm{J}^2 = \mathrm{K}^2 = -1$ et $\mathrm{IJ} = \mathrm{K} = -\mathrm{JI}$, $\mathrm{JK} = \mathrm{I} = -\mathrm{KJ}$ et $\mathrm{KI} = \mathrm{J} = -\mathrm{IK}$.
On admet que l'écriture des éléments de $\mathbb{H}$ de cette façon : $a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ est unique (écriture dite *algèbrique*).
Cela signifie qu'on peut identifier :

$$z = z' \quad \Longleftrightarrow \quad \begin{cases} a = a' \\ b = b' \\ c = c' \\ d = d' \end{cases}$$

On considère également l'anneau $\mathcal{M}_2(\mathbb{C})$ des matrices carrés à coefficients dans $\mathbb{C}$.
On note $Q = \{A \in \mathcal{M}_2(\mathbb{C}) \mid [A]_{1,1} = \overline{[A]_{2,2}} \text{ et } [A]_{1,2} = -\overline{[A]_{2,1}}\}$ (la barre horizontale signifiant ici la conjugaison dans $\mathbb{C}$).

II.1. Etude de la structure de Q.

(a) Montrer que $(Q, +)$ est un sous-groupe de $\mathcal{M}_2(\mathbb{C})$.

O_4, matrice nulle de $\mathcal{M}_2(\mathbb{C})$ est bien un élément de Q, donc Q est non vide.
Soit $A_1, A_2 \in Q$,

$$[A_1 - A_2]_{1,1} = [A_1]_{1,1} - [A_2]_{1,1} = \overline{[A_1]_{2,2}} - \overline{[A_2]_{2,2}} = \overline{[A_1]_{2,2} - [A_2]_{2,2}} = \overline{[A_1 - A_2]_{2,2}}$$

$$[A_1 - A_2]_{1,2} = [A_1]_{1,2} - [A_2]_{1,2} = -\overline{[A_1]_{2,1}} + \overline{[A_2]_{2,1}} = -\overline{[A_1]_{2,1} - [A_2]_{2,1}} = -\overline{[A_1 - A_2]_{2,1}}$$

Donc on a bien $A_1 - A_2 \in Q$.

$\boxed{(Q, +) \text{ est bien un sous-groupe de } \mathcal{M}_2(\mathbb{C}) \text{ (par la caractérisation 2).}}$

(b) Montrer que si $A \in Q$, $\det A \geqslant 0$. Puis : $A = 0$ si et seulement si $\det A = 0$

Soit $A \in Q$, alors

$$\det(A) = [A]_{1,1}[A]_{2,2} - [A]_{1,2}[A]_{2,1} = \overline{[A]_{2,2}}[A]_{2,2} + \overline{[A]_{2,1}}[A]_{2,1} = |[A]_{2,2}|^2 + |[A]_{2,1}|^2 \geqslant 0$$

Et on a

$$\det A = 0 \Longleftrightarrow [A]_{2,2} = 0 et [A]_{2,1} = 0 \underset{A \in Q}{\Longleftrightarrow} [A]_{1,1} = 0, [A]_{2,2} = 0, [A]_{1,2} = 0 et [A]_{2,1} = 0 \Longleftrightarrow A = 0$$

$\boxed{\text{Si } A \in Q, \det A \geqslant 0. \text{ Et, } A = 0 \text{ si et seulement si } \det A = 0.}$

(c) Montrer que $Q^* := Q \setminus \{0\}$ est un groupe (pour la loi $\times$).

Pour étudier le groupe des inversibles de Q, nous allons montrer que $(Q, +, \times)$ est un anneau. Le résultat a démontré sera alors une conséquence du cours.
On sait déjà que $(Q, +)$ est un sous-groupe de $\mathcal{M}_2(\mathbb{C})$.
Notons ensuite que $I_2 \in Q$ car $\overline{1} = 1$ et $-\overline{0} = 0$.
Reste à montrer la stabilité par produit.
Soit $A, B \in Q$,

$$\begin{aligned} \overline{[AB]_{2,2}} &= \overline{[A]_{2,1}[B]_{1,2} + [A]_{2,2}[B]_{2,2}} = \overline{[A]_{2,1}[B]_{1,2}} + \overline{[A]_{2,2}[B]_{2,2}} = (-[A]_{1,2}) \times (-[B]_{2,1}) + [A]_{1,1}[B]_{1,1} \\ &= [A]_{1,1}[B]_{1,1} + [A]_{1,2}[B]_{2,1} = [AB]_{1,1} \end{aligned}$$

$$\begin{aligned} \overline{[AB]_{2,1}} &= \overline{[A]_{2,1}[B]_{1,1} + [A]_{2,2}[B]_{2,1}} = \overline{[A]_{2,1}[B]_{1,1}} + \overline{[A]_{2,2}[B]_{2,1}} = (-[A]_{1,2}) \times [B]_{2,2} + [A]_{1,1} \times (-[B]_{1,2}) \\ &= -[A]_{1,1}[B]_{1,2} - [A]_{1,2}[B]_{2,2} = -[AB]_{1,2} \end{aligned}$$

Donc $AB \in Q$ Par conséquent Q est un sous-anneau de $\mathcal{M}_2(\mathbb{C})$.

$\boxed{Q^* := Q \setminus \{0\} \text{ est un groupe (pour la loi } \times).}$

Tous les éléments de Q, sauf 0 ont un déterminant > 0 donc sont inversibles.

II.2. On note $\Phi : A \in Q \mapsto \mathrm{Re}([A]_{1,1}) + \mathrm{Im}([A]_{1,1}) \times \mathrm{I} + \mathrm{Re}([A]_{1,2}) \times \mathrm{J} + \mathrm{Im}([A]_{1,2}) \times \mathrm{K}$.

(a) Montrer que l'image de Q par Φ est exactement $\mathbb{H}$.

Par définition de Φ, comme $\mathrm{Re}([A]_{1,1})$, $\mathrm{Im}([A]_{1,1}$, $\mathrm{Re}([A]_{1,2})$ et $\mathrm{Im}([A]_{1,2})$ sont des nombres réels, $\Phi(Q) \subset \mathbb{H}$.

Mais par ailleurs, si $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \in \mathbb{H}$, alors $z = \Phi\left(\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}\right)$

où l'on vérifie bien que cette matrice est dans Q.

Ainsi $\mathbb{H} \subset \Phi(Q)$.

$$\boxed{\Phi(Q) = \mathbb{H}}$$

(b) Montrer que $(\mathbb{H}, +, \times)$ est un anneau. Est-il commutatif ?

Montrer l'associativité est très pénible. Ici, on ne va pas la montrer mais la transférer de Q sur $\mathbb{H}$.
En effet, pour montrer que Q^* est un groupe, on a montrer que Q est un anneau (sous-anneau de $\mathcal{M}_2(\mathbb{C})$). Si on montre que Φ vérifie les propriétés de morphisme, alors $\Phi(Q)$ héritera de la structure d'anneau.

- $\Phi(I_2) = 1$
- $\Phi(A+B) = \mathrm{Re}([A+B]_{1,1}) + \mathrm{IIm}([A+B]_{1,1}) + \mathrm{JRe}([A+B]_{1,2}) + \mathrm{KIm}([A+B]_{1,2}) = \cdots = \Phi(A) + \Phi(B)$
- $\Phi(A \times B) = \mathrm{Re}([A\times B]_{1,1}) + \mathrm{IIm}([A\times B]_{1,1}) + \mathrm{JRe}([A\times B]_{1,2}) + \mathrm{KIm}([A\times B]_{1,2})$
$= \mathrm{Re}([A]_{1,1}[B]_{1,1} + [A]_{1,2}[B]_{2,1}) + \mathrm{IIm}([A]_{1,1}[B]_{1,1} + [A]_{1,2}[B]_{2,1}) + \mathrm{JRe}([A]_{1,1}[B]_{1,2} + [A]_{1,2}[B]_{2,2})$
$\quad + \mathrm{KIm}([A]_{1,1}[B]_{1,2} + [A]_{1,2}[B]_{2,2})$
$= \mathrm{Re}([A]_{1,1})\mathrm{Re}([B]_{1,1}) - \mathrm{Im}([A]_{1,1})\mathrm{Im}([B]_{1,1}) + \mathrm{Re}([A]_{1,2})\mathrm{Re}([B]_{2,1}) - \mathrm{Im}([A]_{1,2})\mathrm{Im}([B]_{2,1})$
$+ [\mathrm{Re}([A]_{1,1})\mathrm{Im}([B]_{1,1}) + \mathrm{Im}([A]_{1,1})\mathrm{Re}([B]_{1,1}) + \mathrm{Re}([A]_{1,2})\mathrm{Im}([B]_{2,1}) + \mathrm{Im}([A]_{1,2})\mathrm{Re}([B]_{2,1})]\,\mathrm{I}$
$+ [\mathrm{Re}([A]_{1,1})\mathrm{Re}([B]_{1,2}) - \mathrm{Im}([A]_{1,1})\mathrm{Im}([B]_{1,2}) + \mathrm{Re}([A]_{1,2})\mathrm{Re}([B]_{2,2}) - \mathrm{Im}([A]_{1,2})\mathrm{Im}([B]_{2,2})]\,\mathrm{J}$
$+ [\mathrm{Re}([A]_{1,1})\mathrm{Im}([B]_{1,2}) + \mathrm{Im}([A]_{1,1})\mathrm{Re}([B]_{1,2}) + \mathrm{Re}([A]_{1,2})\mathrm{Im}([B]_{2,2}) + \mathrm{Im}([A]_{1,2})\mathrm{Re}([B]_{2,2})]\,\mathrm{K}$
$= (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - c'd)\mathrm{I} + (ac' - bd' + ca' + db')\mathrm{J} + (ad' + bc' - cb' + da')\mathrm{K}$
$= (a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}) \times (a' + b'\mathrm{I} + c'\mathrm{J} + d'\mathrm{K})$
$= (\mathrm{Re}([A]_{1,1}) + \mathrm{Im}([A]_{1,1})\mathrm{I} + \mathrm{Re}([A]_{1,2})\mathrm{J} + \mathrm{Im}([A]_{1,2})\mathrm{K}) \times (\mathrm{Re}([B]_{1,1}) + \mathrm{Im}([B]_{1,1})\mathrm{I} + \mathrm{Re}([B]_{1,2})\mathrm{J} + \mathrm{Im}([B]_{1,2})\mathrm{K})$
$= \Phi(A) \times \Phi(B)$

car $\mathrm{Re}(z_1 z_2) = \mathrm{Re}(z_1)\mathrm{Re}(z_2) - \mathrm{Im}(z_1)\mathrm{Im}(z_2)$ et $\mathrm{Im}(z_1 z_2) = \mathrm{Re}(z_1)\mathrm{Im}(z_2) + \mathrm{Im}(z_1)\mathrm{Re}(z_2)$ et avec :
$a = \mathrm{Re}([A]_{1,1})$, $a' = \mathrm{Re}([B]_{1,1}) = \mathrm{Re}([B]_{2,2})$, $b = \mathrm{Im}([A]_{1,1})$, $b' = \mathrm{Im}([B]_{1,1}) = -\mathrm{Im}([B]_{2,2})$,
$c = \mathrm{Re}([A]_{1,2})$, $c' = -\mathrm{Re}([B]_{2,1}) = \mathrm{Re}([B]_{1,2})$, $d = \mathrm{Im}([A]_{1,2})$, $d' = \mathrm{Im}([B]_{2,1}) = \mathrm{Im}([B]_{1,2})$ Ainsi, Φ transporte de Q sur $\mathbb{H}$ la structure d'anneau.
Comme $\mathrm{I} \times \mathrm{J} = \mathrm{K}$ et $\mathrm{J} \times \mathrm{I} = -\mathrm{K}$, l'anneau $\mathbb{H}$ n'est pas commutatif.

$$\boxed{(\mathbb{H}, +, \times) \text{ est un anneau non commutatif.}}$$

On déduit de cette question les propriétés de distributivité dans $\mathbb{H}$.

II.3. Conjugaison et module.

(a) On appelle conjugué dans $\mathbb{H}$, l'application $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \mapsto \overline{z} = a - b\mathrm{I} - c\mathrm{J} - d\mathrm{K}$.
Le contexte permet de différencier la conjugaison sur $\mathbb{C}$ ou sur $\mathbb{H}$.
Evaluer, pour tout $z \in \mathbb{H}$, $z \times \overline{z}$ et $\overline{z} \times z$. Montrer que $z \times \overline{z} \in \mathbb{R}_+$.

On applique la formule donnée en début de partie II :

$$z\overline{z} = (a^2 + b^2 + c^2 + d^2) + (-ab + ab - cd + cd)\mathrm{I} + (-ac + ac - db + db)\mathrm{J} + (-ad + ad - bc + bc)\mathrm{K} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_+$$

(Rappelons que $a, b, c, d \in \mathbb{R}$, donc $a^2, b^2, c^2, d^2 \in \mathbb{R}_+$).
De même : $\overline{z}z = a^2 + b^2 + c^2 + d^2$.

$$\boxed{\text{Si } z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \text{ alors } z\overline{z} = \overline{z}z = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_+}$$

(b) Montrer que pour tout $z, z' \in \mathbb{H}$, $\overline{z \times z'} = \overline{z'} \times \overline{z}$

Supposons que $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ et $z' = a' + b'\mathrm{I} + c'\mathrm{J} + d'\mathrm{K} \in \mathbb{H}$.
Alors $z \times z' = (aa' - bb' - cc' - dd') + (ab' + a'b + cd' - c'd)\mathrm{I} + (ac' + a'c + db' - d'b)\mathrm{J} + (ad' + a'd + bc' - b'c)\mathrm{K}$.
Donc

$$\overline{zz'} = (aa' - bb' - cc' - dd') - (ab' + a'b + cd' - c'd)\mathrm{I} - (ac' + a'c + db' - d'b)\mathrm{J} - (ad' + a'd + bc' - b'c)\mathrm{K}$$

Alors que

$$\begin{aligned}\overline{z'}\overline{z} &= (a' - b'\mathrm{I} - c'\mathrm{J} - d')(a - b\mathrm{I} - c\mathrm{J} - d\mathrm{K}) = \big(a'a - (-b')(-b) - (-c')(-c) - (-d')(-d)\big) \\ &\quad + \big((a')(-b) + (a)(-b') + (-c')(-d) - (-c)(-d')\big)\mathrm{I} + \big(-a'c - ac' + d'b - db'\big)\mathrm{J} + \big(-a'd - ad' + b'c - bc'\big)\mathrm{K} \\ &= \big(aa' - bb' - cc' - dd'\big) - \big(a'b + ab' - c'd - cd'\big)\mathrm{I} - \big(a'c + ac' - d'b + db'\big)\mathrm{J} - \big(a'd + ad' - b'c + bc'\big)\mathrm{K}\end{aligned}$$

On retrouve deux fois la même expression, par transitivité :

$$\boxed{\overline{zz'} = \overline{z'} \times \overline{z}}$$

(c) On note $|z| = \sqrt{z\overline{z}}$.
Montrer que pour tout $z, z' \in \mathbb{H}$, $|\overline{z}| = |z|$ et que $|zz'| = |z| \times |z'| = |z'z|$.

Soit $z, z' \in \mathbb{H}$, alors $\overline{\overline{z}} = z$, donc

$$|\overline{z}| = \sqrt{\overline{z}\overline{\overline{z}}} = \sqrt{\overline{z}z} = \sqrt{z\overline{z}} = |z|$$

(en exploitant la commutativité relative entre z et $\overline{z}$ démontrée en 3.(a)). Puis

$$|zz'| = \sqrt{zz'\overline{zz'}} = \sqrt{zz'\overline{z'}\overline{z}} = \sqrt{z|z'|^2\overline{z}} = \underbrace{|z'|}_{\in\mathbb{R}}\sqrt{z\overline{z}} = \underbrace{|z'|}_{\in\mathbb{R}} \times \underbrace{|z|}_{\in\mathbb{R}} = |z| \times |z'|$$

Par symétrie du résultat final, on a $|zz'| = |z'z|$.

$$\boxed{\text{Pour tout } z, z' \in \mathbb{H},\ |\overline{z}| = |z| \text{ et que } |zz'| = |z| \times |z'| = |z'z|.}$$

On peut montrer que $|z|^2 = \det(A)$ si $\Phi(A) = z$, puis exploiter les propriétés de déterminant.

(d) Déduire que $\mathbb{H}$ est un anneau sans diviseur de zéro et que z est inversible (pour $\times$ et dans $\mathbb{H}$) si et seulement si $z \neq 0$.
Exprimer alors z^{-1}.

Soient $z, z' \in \mathbb{H}$ tels que $z \times z' = 0$.
Alors, en passant au module, d'après la relation précédente :

$$0 = |0| = |zz'| = |z| \times |z'|$$

Ce dernier produit est dans $\mathbb{R}$, intègre ; donc $|z| = 0 (\Leftrightarrow z = 0)$ ou $|z'| = 0 (\Leftrightarrow z' = 0)$.
Donc $z \times z' = 0 \Longrightarrow z = 0$ ou $z' = 0$.

$$\boxed{\mathbb{H} \text{ est un anneau sans diviseur de zéro.}}$$

Si z est inversible, alors il existe z^{-1} tel que $zz^{-1} = 1$, donc $|z| \times |z^{-1}| = |1| = 1$. Nécessairement $|z| \neq 0$.
Réciproquement, si $|z| \neq 0$, alors $z \times \dfrac{1}{|z|^2}\overline{z} = \dfrac{|z|^2}{|z|^2} = \dfrac{1}{|z|^2}\overline{z} \times z$.

On a alors trouvé l'inverse de z, nécessairement inversible : c'est $\dfrac{1}{|z|^2}\overline{z}$.

$$\boxed{z \text{ est inversible si et seulement si } z \neq 0. \text{ Dans ce cas } z^{-1} = \frac{1}{|z|^2}\overline{z} = \frac{1}{a^2+b^2+c^2+d^2}(a - b\mathrm{I} - c\mathrm{J} - d\mathrm{K}).}$$

(e) Déduire également la relation algébrique : $\forall\ a, b, c, d, x, y, z, t \in \mathbb{R}$

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax-by-cz-dt)^2 + (ay+bx+ct-dz)^2 + (az+bx+cy-dt)^2 + (at+bx+cz-dy)^2$$

Cette relation est-elle vraie dans d'autres anneaux que $\mathbb{R}$? Lesquels ?

En élevant au carré, on a donc : $|z|^2 \times |z'|^2 = |zz'|^2$, donc avec $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ et $z' = x + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}$, on trouve :

$$\begin{aligned}(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) &= |z|^2|z'|^2 = |zz'|^2 \\ &= \big|(ax-by-cz-dt) + (ay+bx+ct-dz)\mathrm{I} + (az+cx+dy-bt)\mathrm{J} + (at+dx+bz-cy)\mathrm{K}\big|^2 \\ &= (ax-by-cz-dt)^2 + (ay+bx+ct-dz)^2 + (az+cx+dy-bt)^2 + (at+dx+bz-cy)^2\end{aligned}$$

$$\boxed{\begin{array}{l}\forall\ a, b, c, d, x, y, z, t \in \mathbb{R}, \\ (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax-by-cz-dt)^2 + (ay+bx+ct-dz)^2 + (az+bx+cy-dt)^2 + (at+bx+cz-dy)^2\end{array}}$$

Ce résultat n'est en réalité qu'un calcul formel,

$$\boxed{\text{il est vrai dans tous les anneaux commutatifs.}}$$

II.4. Quaternions unitaires et quaternions purs.
On dit que $z \in \mathbb{H}$ est unitaire si $|z| = 1$. On note $\mathbb{U}_{\mathbb{H}} = \{z \in \mathbb{H} \mid |z| = 1\}$.
On dit que $z \in \mathbb{H}$ est quaternion pur si $z + \overline{z} = 0$. On note $\mathbb{I}_{\mathbb{H}} = \{z \in \mathbb{H} \mid z + \overline{z} = 0\}$

(a) Montrer que pour tout $z \in \mathbb{H}^* := \mathbb{H} \setminus \{0\}$, il existe un unique couple $(r,u) \in \mathbb{R}_+^* \times \mathbb{U}_\mathbb{H}$ tel que $z = ru$

Soit $z \in \mathbb{H}^*$. Commençons par montrer l'existence.

soit $u = \dfrac{1}{|z|}z$, alors $|u| = \left|\dfrac{1}{|z|}z\right| = \left|\dfrac{1}{|z|}\right| \times |z| = \dfrac{1}{|z|}|z| = 1$.

Donc $u \in \mathbb{U}_\mathbb{H}$. et par ailleurs, $|z| > 0$ (car $z \neq 0$), donc $r = \dfrac{1}{|z|} > 0$.

Ainsi, on a trouvé un couple $(r,u) \in \mathbb{R}_+^* \times \mathbb{U}_\mathbb{H}$ tel que $z = ru$.

Montrons l'unicité. Supposons que $z = ru = r'u'$, avec $r, r' \in \mathbb{R}_+^*$ et $u, u' \in \mathbb{U}_\mathbb{H}$.

Alors en prenant le module : $r = |r| = |r||u| = |ru| = |r'u'| = |r'||u'| = |r'| = r'$.

On peut alors simplifier par r (inversible car $r > 0$) et donc $u = u'$.

Pour tout $z \in \mathbb{H}^* := \mathbb{H} \setminus \{0\}$, il existe un unique couple $(r,u) \in \mathbb{R}_+^* \times \mathbb{U}_\mathbb{H}$ tel que $z = ru$.

(b) Montrer que pour tout $z \in \mathbb{U}_\mathbb{H}$, il existe $\theta \in [0,\pi]$ et $s \in \mathbb{I}_\mathbb{H} \cap \mathbb{U}_\mathbb{H}$ tel que $z = \cos\theta + s \times \sin\theta$

Soit $z \in \mathbb{U}_\mathbb{H}$, alors il existe $a,b,c,d \in \mathbb{R}$ tel que $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$, avec $a^2+b^2+c^2+d^2 = 1$.

On a donc $a^2 \in [0,1]$ et $a \in [-1,1]$. Notons $\theta = \arccos a$. On a $\theta \in [0,\pi]$.

Puis $b^2+c^2+d^2 = 1-a^2 = 1-\cos^2\theta = \sin^2\theta$.

• Si $\theta \neq 0$ et $\theta \neq \pi$, alors $\sin\theta \neq 0$. On peut donc diviser par $\sin\theta$.

Soit $s = \dfrac{b}{\sin\theta}\mathrm{I} + \dfrac{c}{\sin\theta}\mathrm{J} + \dfrac{d}{\sin\theta}\mathrm{K}$.

Alors $s \in \mathbb{I}_\mathbb{H}$, $\cos\theta + s\sin\theta = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} = z$.

Enfin, $|s|^2 = \dfrac{b^2}{\sin^2\theta} + \dfrac{c^2}{\sin^2\theta} + \dfrac{d^2}{\sin^2\theta} = \dfrac{b^2+c^2+d^2}{\sin^2\theta} = \dfrac{1-a^2}{\sin^2\theta} = \dfrac{1-\cos^2\theta}{\sin^2\theta} = 1$. Donc $s \in \mathbb{U}_\mathbb{H}$.

• Si $\theta = 0$, ou $\theta = \pi$, alors cela signifie que $a = \pm 1$ et donc $b = c = d = 0$.

On peut prendre s quelconque dans $\mathbb{I}_\mathbb{H} \cap \mathbb{U}_\mathbb{H}$ (qui n'est pas vide) et on a $z = a = \cos\theta + s\sin\theta$ (car $\sin\theta = 0$).

Dans tous les cas :

Pour tout $z \in \mathbb{U}_\mathbb{H}$, il existe $\theta \in [0,\pi]$ et $s \in \mathbb{I}_\mathbb{H} \cap \mathbb{U}_\mathbb{H}$ tel que $z = \cos\theta + s \times \sin\theta$

III Anneau euclidien des entiers de Hamilton

Soit $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K} \in \mathbb{H}$.

On dit que z est entier d'Hamilton ou entier de $\mathbb{H}$ si $(a,b,c,d) \in \mathbb{Z}^4$ ou $(a-\frac{1}{2}, b-\frac{1}{2}, c-\frac{1}{2}, d-\frac{1}{2}) \in \mathbb{Z}^4$

On note $\mathbb{H}(\mathbb{Z})$ l'ensemble des entiers de $\mathbb{H}$.

III.1. Montrer que $\mathbb{H}(\mathbb{Z}) = \left\{ \dfrac{x}{2}(1+\mathrm{I}+\mathrm{J}+\mathrm{K}) + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}, (x,y,z,t) \in \mathbb{Z}^4 \right\}$.

Notons $H' = \left\{ \dfrac{x}{2}(1+\mathrm{I}+\mathrm{J}+\mathrm{K}) + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}, (x,y,z,t) \in \mathbb{Z}^4 \right\}$

Soit $z = (a+\epsilon\frac{1}{2}) + (b+\epsilon\frac{1}{2})\mathrm{i} + (c+\epsilon\frac{1}{2})\mathrm{J} + (d+\epsilon\frac{1}{2})\mathrm{K}$, avec $a,b,c,d \in \mathbb{Z}$ et $\epsilon \in \{0,1\}$.

Alors $z = \dfrac{2a+\epsilon}{2}(1+\mathrm{I}+\mathrm{J}+\mathrm{K}) + (b-2a)\mathrm{I} + (c-2a)\mathrm{J} + (d-2a)\mathrm{K} \in H'$.

Réciproquement, si $z \in H'$, alors il existe $(x,y,z,t) \in \mathbb{Z}^4$ tel que $z = \dfrac{x}{2}(1+\mathrm{I}+\mathrm{J}+\mathrm{K}) + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}$ il existe $(x,y,z,t) \in \mathbb{Z}^4$.

• Si x est pair, on considère $a = \dfrac{x}{2} \in \mathbb{Z}$ et on a $z = a + (y+a)\mathrm{I} + (z+a)\mathrm{J} + (t+a)\mathrm{K} \in \mathbb{H}(\mathbb{Z})$.

• Si x est impair, on considère $a = \dfrac{x+1}{2} \in \mathbb{Z}$ et on a $z = (a-\frac{1}{2}) + (y+a-\frac{1}{2})\mathrm{I} + (z+a-\frac{1}{2})\mathrm{J} + (t+a-\frac{1}{2})\mathrm{K} \in \mathbb{H}(\mathbb{Z})$.

Ainsi, par double inclusion :

$$\mathbb{H}(\mathbb{Z}) = H' = \left\{ \frac{x}{2}(1+\mathrm{I}+\mathrm{J}+\mathrm{K}) + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}, (x,y,z,t) \in \mathbb{Z}^4 \right\}.$$

III.2. Montrer que si $z, z' \in \mathbb{H}(\mathbb{Z})$, alors $z+z'$ et $z \times z' \in \mathbb{H}(\mathbb{Z})$ et que si $z \in \mathbb{H}(\mathbb{Z})$ alors $|z|^2 \in \mathbb{N}$.

Soient $z, z' \in \mathbb{H}(\mathbb{Z})$. Il existe $\epsilon, \epsilon' \in \{0,1\}$ tel que

$z = (a+\epsilon\frac{1}{2}) + (b+\epsilon\frac{1}{2})\mathrm{i} + (c+\epsilon\frac{1}{2})\mathrm{J} + (d+\epsilon\frac{1}{2})\mathrm{K}$, avec $a,b,c,d \in \mathbb{Z}$,

et $z' = (a'+\epsilon'\frac{1}{2}) + (b'+\epsilon'\frac{1}{2})\mathrm{i} + (c'+\epsilon'\frac{1}{2})\mathrm{J} + (d'+\epsilon'\frac{1}{2})\mathrm{K}$, avec $a',b',c',d' \in \mathbb{Z}$.

Alors $z+z' = (a+a'+(\epsilon+\epsilon')\frac{1}{2}) + (b+b'+(\epsilon+\epsilon')\frac{1}{2})\mathrm{i} + (c+c'+(\epsilon+\epsilon')\frac{1}{2})\mathrm{J} + (d+d'+(\epsilon+\epsilon')\frac{1}{2})$

Comme, $a+a'$, $b+b'$, $c+c'$ et $d+d' \in \mathbb{Z}$ et que $\epsilon+\epsilon' \in \{0,1,2\}$, on a $z+z' \in \mathbb{H}(\mathbb{Z})$.

$$\begin{aligned} z\times z' = \;& (aa'+-bb'-cc'-dd') + (ab'+a'b+cd'-c'd)\mathrm{I} + (ac'+a'c+db'-d'b)\mathrm{J} + (ad'+a'd+bc'-b'c)\mathrm{K} \\ & + \frac{\epsilon}{2}\big[(a'-b'-c'-d') + (b'+a'+d'-c')\mathrm{I} + (c'+a'+b'-d')\mathrm{J} + (d'+a'+c'-b')\mathrm{K}\big] \\ & + \frac{\epsilon'}{2}\big[(a-b-c-d) + (b+a+d-c)\mathrm{I} + (c+a+b-d)\mathrm{J} + (d+a+c-b)\mathrm{K}\big] \\ & + \frac{\epsilon\epsilon'}{4}\big[(-2) + (2)\mathrm{I} + (2)\mathrm{J} + (2)\mathrm{K}\big] \end{aligned}$$

Puis, comme $(a-b-c-d)+(b+a+d-c) = 2(a-c)$, est un nombre pair, $(a-b-c-d)$ et $(b+a+d-c)$ ont même parité.
De même $(a-b-c-d)$, $(b+a+d-c)$, $(c+a+b-d)$ et $(d+a+c-b)$ ont tous les quatre la même parité.
Et $(a'-b'-c'-d')$, $(b'+a'+d'-c')$, $(c'+a'+b'-d')$ et $(d'+a'+c'-b')$ ont même parité.
Ainsi, les nombres additionnés selon 1, I, J et K sont tous ensemble des entiers ou tous ensemble des demi-entiers.

Par conséquent, si $z, z' \in \mathbb{H}(\mathbb{Z})$, alors $z+z' \in \mathbb{H}(\mathbb{Z})$ et $z\times z' \in \mathbb{H}(\mathbb{Z})$.

Soit $z = a+b\mathrm{I}+c\mathrm{J}+d\mathrm{K} \in \mathbb{H}(\mathbb{Z})$.
- Si $(a,b,c,d) \in \mathbb{Z}^4$, alors $|z|^2 = a^2+b^2+c^2+d^2$, somme de 4 carrés d'entiers. Il s'agit donc d'un entier naturel.
- Si $(a-\frac{1}{2}, b-\frac{1}{2}, c-\frac{1}{2}, d-\frac{1}{2}) \in \mathbb{Z}^4$, alors $|z|^2 = a^2-2a+\frac{1}{4}+b^2-2b+\frac{1}{4}+c^2-2c+\frac{1}{4}+d^2-2d+\frac{1}{4} = 1+a^2+b^2+c^2+d^2-2(a+b+c+d)$.
  Il s'agit également d'un entier naturel.

Donc, si $z \in \mathbb{H}(\mathbb{Z})$, $|z|^2 \in \mathbb{N}$.

III.3. Un élément z de $\mathbb{H}$ est appelé une unité si z et z^{-1} sont tous les deux des entiers de $\mathbb{H}(\mathbb{Z})$.
Montrer que si z est une unité de $\mathbb{H}$ alors $|z| = 1$ i.e. $z \in \mathbb{U}_{\mathbb{H}}$.

Soit z une unité de $\mathbb{H}$. Alors $|z|^2 \in \mathbb{N}$ et de même $z^{-1} \in \mathbb{H}(\mathbb{Z})$ donc $|z^{-1}|^2 \in \mathbb{N}$. Puis

$$1 = |1|^2 = |zz^{-1}|^2 = |z|^2 \times |z^{-1}|^2$$

Ainsi, $|z|^2$ (ainsi que $|z^{-1}|^2$) est un nombre inversible de $\mathbb{Z}$, donc $|z|^2 \in \{-1, 1\}$.
Enfin, comme $|z|^2 \geqslant 0$, on a $|z|^2 = 1$ et donc $|z| = 1$.

Si z est une unité de $\mathbb{H}$ alors $|z| = 1$ i.e. $z \in \mathbb{U}_{\mathbb{H}}$.

III.4. Donner la liste des 24 éléments de $\mathbb{H}(\mathbb{Z})^\times$, i.e. des inversibles ou unités $\mathbb{H}(\mathbb{Z})$.

Soit $z = a+b\mathrm{I}+c\mathrm{J}+d\mathrm{K} \in \mathbb{H}(\mathbb{Z})^\times$ alors $a^2+b^2+c^2+d^2 = 1$.
- Supposons que z est un entier exact (pas de $\frac{1}{2}$),
  donc un des quatre nombres vaut 1 ou -1, les autres sont nuls.
  On trouve dans ce cas 8 nombres : ± 1, $\pm\mathrm{I}$, $\pm\mathrm{J}$ et $\pm\mathrm{K}$.
  Réciproquement : ces 8 nombres sont bien des éléments de $\mathbb{H}(\mathbb{Z})^\times$.
- Supposons que z entier non exact : $z = a+\frac{1}{2}+(b+\frac{1}{2})\mathrm{I}+(c+\frac{1}{2})\mathrm{J}+(d+\frac{1}{2})\mathrm{K}$ avec $a,b,c,d \in \mathbb{Z}$.
  Nécessairement (on multiplie par 4) : $(2a+1)^2+(2b+1)^2+(2c+1)^2+(2d+1)^2 = 4$.
  Or la somme de 4 entiers au carré donne 4 ssi il s'agit de $2^2+0^2+0^2+0^2$ ou de $1^2+1^2+1^2+1^2$.
  Premier cas : supposons que l'un des nombres $2a+1$...vaut ± 2 et les autres son nuls.
  Alors, sans perte de généralité, on peut supposer $2a+1 = \pm 2$, i.e. $a = \frac{1}{2}$ ou $a = -\frac{3}{2}$.
  Ceci est impossible car a est un entier. Donc ce premier cas ne se produit pas.
  Second cas : supposons que l'on ait : $2a+1 = \pm 1$, ...$2d+1 = \pm 1$.
  Cela donne $a = 0$ ou $a = -1$ et $b = 0$ ou $b = -1$, $c = 0$ ou $c = -1$ et $d = 0$ ou $d = -1$.
  Cela conduit donc à $2^4 = 16$ nombres distincts.
  Et réciproquement, pour chacun de ces 16 nombres :
  $z = a+\frac{1}{2}+(b+\frac{1}{2})\mathrm{I}+(c+\frac{1}{2})\mathrm{J}+(d+\frac{1}{2})\mathrm{K}$ avec $a,b,c,d \in \{-1,0\}$, on trouve $|z| = 1$.

Donc $\mathbb{H}(\mathbb{Z})^\times$ a 24 éléments :

$$\mathbb{H}(\mathbb{Z})^\times = \big\{a+b\mathrm{I}+c\mathrm{J}+d\mathrm{K} \mid a,b,c,d = \pm 1\big\} \cup \big\{a+\tfrac{1}{2}+(b+\tfrac{1}{2})\mathrm{I}+(c+\tfrac{1}{2})\mathrm{J}+(d+\tfrac{1}{2})\mathrm{K} \mid a,b,c,d \in \{-1,0\}\big\}$$

III.5. Anneau euclidien.

(a) Soit $z \in \mathbb{H}$.
Montrer qu'il existe $e \in \mathbb{H}(\mathbb{Z})$ tel que $|z-e|^2 \leqslant \frac{5}{8}$.

Soient $z = a+b\mathrm{I}+c\mathrm{J}+d\mathrm{K}$ et $e = \alpha+\beta\mathrm{I}+\gamma\mathrm{J}+\delta\mathrm{K}$.
Alors $|z-e|^2 = (a-\alpha)^2+(b-\beta)^2+(c-\gamma)^2+(d-\delta)^2$.

Le nombre $a - \lfloor a \rfloor \in [0,1]$. Notons $\theta(a) = \begin{cases} 0 & \text{si } a - \lfloor a \rfloor \in [0, \frac{1}{4}] \\ \frac{1}{2} & \text{si } a - \lfloor a \rfloor \in]\frac{1}{4}, \frac{3}{4}[\\ 1 & \text{si } a - \lfloor a \rfloor \in [\frac{3}{4}, 1[\end{cases}$. On définit de même $\theta(b)$, $\theta(c)$ et $\theta(d)$.

Si au moins deux des quatre nombres $\theta(a)$, $\theta(b)$, $\theta(c)$ et $\theta(d)$ est égal à $\frac{1}{2}$,

alors on considère $\alpha = \lfloor a \rfloor + \frac{1}{2}$, $\beta = \lfloor b \rfloor + \frac{1}{2}$, $\gamma = \lfloor c \rfloor + \frac{1}{2}$ et $\delta = \lfloor d \rfloor + \frac{1}{2}$, Alors pour au moins deux nombres $|x - \xi| \leqslant \frac{1}{4}$ (ceux pour lesquels $\theta(x) = \frac{1}{2}$) et pour les autres nombres (au plus deux) on a $|x - \xi| \leqslant \frac{1}{2}$.

Sinon (et donc au moins deux des quatre nombres $\theta(a)$, $\theta(b)$, $\theta(c)$ et $\theta(d)$ est égal à 0 ou 1),

alors on considère $\alpha = \lfloor a \rfloor$ si $\theta(a) = 0$ ou $\alpha = \lfloor a \rfloor + 1$ si $\theta(a) = 1$. De même pour β, γ et δ Alors pour au moins deux nombres $|x - \xi| \leqslant \frac{1}{4}$ (ceux pour lesquels $\theta(x) = 1$ ou 0) et pour les autres nombres (au plus deux) on a $|x - \xi| \leqslant \frac{1}{2}$.

Dans tous les cas :

$$|z - e|^2 \leqslant 2 \times \left(\frac{1}{2}\right)^2 + 2 \times \left(\frac{1}{4}\right)^2 = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

$$\boxed{\forall\, z \in \mathbb{H}, \exists\, e \in \mathbb{H}(\mathbb{Z}) \text{ tel que } |z - e|^2 \leqslant \frac{5}{8}}$$

(b) Soient $z_1, z_2 \in \mathbb{H}(\mathbb{Z})$ avec $z_2 \neq 0$, montrer qu'il existe $q, r \in \mathbb{H}(\mathbb{Z})$ tel que $z_1 = qz_2 + r$ avec $|r| < |z_2|$.
On parle d'une division euclidienne à gauche.

Soit $z_1, z_2 \in \mathbb{H}(\mathbb{Z})$ avec $z_2 \neq 0$.

Alors z_2 est inversible et $z_1 z_2^{-1} \in \mathbb{H}$. D'après la question précédente, il existe $q \in \mathbb{H}(\mathbb{Z})$ tel que $z_1 z_2^{-1} - q| \leqslant \frac{\sqrt{10}}{4} < 1$.

Notons $r = z_1 - qz_2 \in \mathbb{H}(\mathbb{Z})$, d'après la question III.1..

On a alors $|rz_2^{-1}| = |z_1 z_2^{-1} - q| < 1$ et donc $|r||z_2^{-1}| = |r| \times |z_2|^{-1} < 1$, donc $|r| < |z_2|$.

$$\boxed{\text{Donc pour tout } z_1, z_2 \in \mathbb{H}(\mathbb{Z}) \text{ avec } z_2 \neq 0, \text{ il existe } q, r \in \mathbb{H}(\mathbb{Z}) \text{ tel que } z_1 = qz_2 + r \text{ avec } |r| < |z_2|.}$$

III.6. Idéal à gauche. PGCD.

On dit que I est un idéal à gauche de l'anneau $\mathbb{H}(\mathbb{Z})$ si :
— $(I, +)$ est un sous-groupe $(\mathbb{H}(\mathbb{Z}), +)$
— $\forall\, a \in \mathbb{H}(Z)$ et $x \in I$, $ax \in I$

(a) Montrer que pour tout $z \in \mathbb{H}(\mathbb{Z})$, $(z) := \{az \mid a \in \mathbb{H}(\mathbb{Z})\}$ est un idéal à gauche de $\mathbb{H}(\mathbb{Z})$

$(\mathbb{H}(\mathbb{Z}), +)$ est un groupe (sous-groupe de $\mathbb{H}$). Soit $z \in \mathbb{H}(Z)$

Notons donc $(z) = \{az \mid a \in \mathbb{H}(\mathbb{Z})\}$.

Pour x_1 et $x_2 \in (z)$, il existe $a_1, a_2 \in \mathbb{H}(\mathbb{Z})$ tels que $x_1 = a_1 z$ et $x_2 = a_2 z$,

alors $x_1 - x_2 = (a_1 - a_2)z \in (z)$ car $\mathbb{H}(\mathbb{Z})$ est un groupe donc $a_1 - a_2 \in \mathbb{H}(\mathbb{Z})$.

Pour $a \in \mathbb{H}(\mathbb{Z})$ et $x \in (z)$, il existe $a' \in \mathbb{H}(\mathbb{Z})$ tel que $x = a'z$

et donc $a \times x = (aa')z \in \mathbb{H}(\mathbb{Z})$ par associativité dans $\mathbb{H}$ (anneau).

$$\boxed{\text{Pour tout } z \in \mathbb{H}(\mathbb{Z}),\ \{az \mid a \in \mathbb{H}(\mathbb{Z})\} := (z) \text{ est un idéal à gauche de } \mathbb{H}(\mathbb{Z}).}$$

(b) Montrer que si I_1 et I_2 sont deux idéaux à gauche de $\mathbb{H}(\mathbb{Z})$,
$I_1 + I_2 := \{a_1 + a_2 \mid a_1 \in I_1, a_2 \in I_2\}$ et $I_1 \cap I_2$ sont des idéaux à gauche de $\mathbb{H}(\mathbb{Z})$.

Pour t et $t' \in I_1 + I_2$, il existe $(x_1, x_2) \in I_1 \times I_2$, $(x_1', x_2') \in I_1 \times I_2$ tels que $t = x_1 + x_2$ et $t' = x_1' + x_2'$,

alors $t - t' = (x_1 - x_1)\prime) + (x_2 - x_2') \in I_1 + I_2$ car I_1 et I_2 sont des sous-groupe de $(\mathbb{H}(\mathbb{Z}), +)$.

Puis par distributivité (à gauche) pour tout $a \in \mathbb{H}(\mathbb{Z})$,

$at = a(x_1 + x_2) = ax_1 + ax_2 \in I_1 + I_2$ car I_1 et I_2 sont des idéaux.

$$\boxed{I_1 + I_2 \text{ est donc un idéal à gauche de } \mathbb{H}(\mathbb{Z}).}$$

Pour t et $t' \in I_1 \cap I_2$, $t, t' \in I_1$ donc $t - t' \in I_1$ et de même $t, t' \in I_2$ donc $t - t' \in I_2$.

alors $t - t' \in I_1 \cap I_2$.

Pour tout $a \in \mathbb{H}(\mathbb{Z})$,

$at \in I_1$ car $t \in I_1$ et I_1 est un idéal ; $at \in I_2$ car $t \in I_2$ et I_2 est un idéal

$$\boxed{I_1 \cap I_2 \text{ est donc un idéal à gauche de } \mathbb{H}(\mathbb{Z}).}$$

(c) Montrer que pour tout idéal à gauche I de $\mathbb{H}(\mathbb{Z})$, il existe $z \in \mathbb{H}(\mathbb{Z})$ tel que $I = (z)$.

Soit I un idéal à gauche de $\mathbb{H}(\mathbb{Z})$, (non vide).
L'ensemble $M = \{|z|^2, z \in I \setminus \{0\}\}$ est un sous-ensemble non de $\mathbb{N}^*$ (car $I \subset \mathbb{H}(\mathbb{Z})$), donc admet un plus petit élément, noté $m_0 > 0$.
Il existe $z \in I$ tel que $|z|^2 = m_0$.
Soit $x \in I$. Comme $z \neq 0$, on peut faire la division de x par z.
Il existe $q, r \in \mathbb{H}(\mathbb{Z})$ tel que $x = qz + r$ avec $|r| < |z|$.
Puis comme I est un idéal à gauche et $z \in I$, $qz \in I$, et $x \in I$, donc $r = x - qz \in I$ (sous-groupe).
Si $x \neq 0$, alors $|x|^2 \in M$ et $|x|^2 < |z|^2 = m_0$, impossible. Donc $x = 0$.
Et par conséquent $x = qz$. Donc $I \subset (z)$.
Réciproquement, si $a \in (z)$, alors il existe $x \in \mathbb{H}(\mathbb{Z})$ tel que $a = xz$. Comme $z \in I$, $a \in I$.
Donc $(z) \subset I$.

Pour tout idéal à gauche I de $\mathbb{H}(\mathbb{Z})$, il existe $z \in \mathbb{H}(\mathbb{Z})$ tel que $I = (z)$.

(d) Comment pourrait-on définir le PGCD de deux nombres de $\mathbb{H}(\mathbb{Z})$.

Soit $z_1, z_2 \in \mathbb{H}(\mathbb{Z})$. Alors (z_1) et (z_2) sont deux idéaux à gauche de $\mathbb{H}(\mathbb{Z})$.
Donc $(z_1) + (z_2)$ est un idéal de $\mathbb{H}(\mathbb{Z})$. Donc il existe $Z \in \mathbb{H}(\mathbb{Z})$ tel que $(z_1) + (z_2) = (Z)$.

Z est UN PGCD de z_1 et de z_2. Les autres lui sont égaux à une multiplication par une des 24 unités près.

III.7. Nombre premier.
On dit qu'un entier de Hamilton $z \in \mathbb{H}(\mathbb{Z})$ est premier si : $z = uv$ avec $u, v \in \mathbb{H}(\mathbb{Z}) \Longrightarrow u$ ou $v \in \mathbb{U}_{\mathbb{H}}$.
Montrer que les nombres 2, 3, 4,...20 ne sont pas premiers dans $\mathbb{H}(\mathbb{Z})$.

Commençons par une remarque simple (et réductrice) : un nombre qui n'est pas premier dans $\mathbb{Z}$ ne peut pas être premier dans $\mathbb{H}(\mathbb{Z})$.
On peut, en effet, utiliser la même décomposition que dans $\mathbb{Z}$, par exemple : $8 = 2 \times 4 \ldots$
Concentrons nous donc sur les nombres premiers de $\mathbb{N}$.
$2 = (1 + \mathrm{I}) \times (1 - \mathrm{I})$ avec $(1 + \mathrm{I}), (1 - \mathrm{I}) \notin \mathbb{U}_{\mathbb{H}}$, donc 2 n'est pas premier.
$3 = (1 + \mathrm{I} + \mathrm{J}) \times (1 - \mathrm{I} - \mathrm{J})$ avec $(1 + \mathrm{I} + \mathrm{J}), (1 - \mathrm{I} - \mathrm{J}) \notin \mathbb{U}_{\mathbb{H}}$, donc 3 n'est pas premier.
$5 = (2 + \mathrm{I}) \times (2 - \mathrm{I})$ avec $(2 + \mathrm{I}), (2 - \mathrm{I}) \notin \mathbb{U}_{\mathbb{H}}$, donc 5 n'est pas premier.
$7 = (2 + \mathrm{I} + \mathrm{J} + \mathrm{K}) \times (2 - \mathrm{I} - \mathrm{J} - \mathrm{K})$ avec $(2 + \mathrm{I} + \mathrm{J} + \mathrm{K}), (2 - \mathrm{I} - \mathrm{J} - \mathrm{K}) \notin \mathbb{U}_{\mathbb{H}}$, donc 7 n'est pas premier.
$11 = (3 + \mathrm{I} + \mathrm{J}) \times (3 - \mathrm{I} - \mathrm{J})$ avec $(3 + \mathrm{I} + \mathrm{J}), (3 - \mathrm{I} - \mathrm{J}) \notin \mathbb{U}_{\mathbb{H}}$, donc 11 n'est pas premier.
$13 = (2 + 2\mathrm{I} + 2\mathrm{J} + \mathrm{K}) \times (2 - 2\mathrm{I} - 2\mathrm{J} - \mathrm{K})$ avec $(2 + 2\mathrm{I} + 2\mathrm{J} + \mathrm{K}), (2 - 2\mathrm{I} - 2\mathrm{J} - \mathrm{K}) \notin \mathbb{U}_{\mathbb{H}}$,
donc 13 n'est pas premier.
$19 = (3 + 3\mathrm{I} + \mathrm{J}) \times (3 - 3\mathrm{I} - \mathrm{J})$ avec $(3 + 3\mathrm{I} + \mathrm{J}), (3 - 3\mathrm{I} - \mathrm{J}) \notin \mathbb{U}_{\mathbb{H}}$, donc 19 n'est pas premier.

Donc les nombres 2, 3, 4,...20 ne sont pas premiers dans $\mathbb{H}(\mathbb{Z})$.

III.8. Application 1. Somme de quatre carrés d'entiers.

(a) Soit $a, b, c, d, a', b', c', d'$ huit entiers naturels, et $n = a^2 + b^2 + c^2 + d^2$, $n' = a'^2 + b'^2 + c'^2 + d'^2$.
En utilisant le module des quaternions, démontrer que le produit nn' est la somme de quatre carrés d'entiers naturels.

On peut reprendre directement la formule montrée en II.3.e. Ou bien considérer de nouveau $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$, $z' = a' + b'\mathrm{I} + c'\mathrm{J} + d'\mathrm{K} \in \mathbb{H}(\mathbb{Z})$. Alors $n = |z|^2$ et $n' = |z'|^2$. Donc

$$n \times n' = |z|^2 \times |z'|^2 = |zz'|^2 = (aa' - bb' - cc' - dd')^2 + (ab' + a'b + cd' - c'd')^2 + (ac' + a'c + db' - d'b)^2 + (ad' + a'd + bc' - b'c)^2$$

Il s'agit d'une somme de 4 carrés d'entiers.

Si $n, n' \in \mathbb{N}$ sont somme de quatre carrés d'entiers, il en est de même de $n \times n'$.

(b) Monter que 2 est la somme de 4 carrés.

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

(c) (**) Montrer que tout nombre premier impair est somme de 4 carrés d'entiers.
On pourra commencer par prouver qu'il existe $z = 1 + a\mathrm{I} + b\mathrm{J}$ tel que p divise $|z|$.

Soit p un entier impair. a et $p-a$ ont le même carré modulo p : $(p-a)^2 = p^2 - 2ap + a^2 \equiv a^2[p]$.

Pour $a \neq b$, avec $a, b \in [\![1, \frac{p-1}{2}]\!]$, on a $a^2 \neq b^2$, sinon $X^2 - a^2$ admettrait 4 racines dans le corps $\mathbb{F}_p$, impossible.

Donc $\{-a^2; a \in \mathbb{F}_p\}$ contient exactement $\frac{p-1}{2} + 1$ éléments (+1, à cause de 0^2).

Pour les mêmes raisons $\{b^2+1; b \in \mathbb{F}_p\}$ contient exactement $\frac{p+1}{2}$ éléments également.

Donc nécessairement, ces deux ensembles ne sont pas disjoints car ils sont à valeurs dans $[\![0, p-1]\!]$.

Considérons $c \in \{-a^2; a \in \mathbb{F}_p\} \cap \{b^2+1; b \in \mathbb{F}_p\}$. Il existe donc $a, b \in \mathbb{F}_p$ tel que $c = -a^2 = b^2 + 1$

Ainsi $a^2 + b^2 + 1 = 0$ dans $\mathbb{F}_p$, ou encore $p | a^2 + b^2 + 1$.

Ensuite, considérons $z = 1 + a\mathrm{I} + b\mathrm{J} \in \mathbb{H}(\mathbb{Z})$, on a donc $p \big| |z|^2$ (p divise le carré de la norme de z) et considérons $I = (z) + (p)$.

Soit $a \in I$, alors il existe $x_1, x_2 \in \mathbb{H}(\mathbb{Z})$ tel que $a = x_1 z + x_2 p$ donc p divise $|a|^2$.

en effet : $|a|^2 = (x_1 z + x_2 p)(\overline{z}\,\overline{x_2} + p\overline{x_2}) = (x_1 |z|^2 \overline{x_1} + p(|x_2|^2 p + x_1 z\overline{x_2} + x_2 \overline{z}\,\overline{x_1})$ factorisable par p/ Cet idéal (à gauche) admet un générateur $q : I = (q)$ d'après 6.(c). On a toujours p divise $|q|^2$.

Alors $p \in (q)$ donc il existe $x \in \mathbb{H}(\mathbb{Z})$ tel que $p = xq$ et donc $|x|^2 |q|^2 = |p|^2$, donc $|q|^2$ divise $|p|^2$.

Donc $|q|^2$ vaut p ou p^2, car p est premier.

Or si $|q|^2 = p^2$, cela signifie que $p = xq$ avec $|x| = 1$, et donc $z = 1 + a\mathrm{I} + b\mathrm{J} \in (p)$. Impossible

(on ne peut avoir 1 comme constante en multipliant p par un entier d'Hamilton).

Donc $|q|^2 = p$. A partir de $q \in \mathbb{H}(\mathbb{Z})$ et son calcul de norme.

(Petite difficulté, en fait q peut être à coordonnée demi-entière. Mais on montre qu'il existe alors $u \in \mathbb{U}_{\mathbb{H}} \cap \mathbb{H}(\mathbb{Z})$ tel que uq soit à coordonnées entières.)

Tout nombre premier impair est somme de 4 carrés d'entiers.

(d) En déduire que tout nombre entier positif est somme de 4 carrés d'entiers.

Tout entiers positifs est un produit de nombres premiers, décomposable en somme de 4 carrées d'entiers. Par stabilité de cette propriété par produit,

Tout nombre entier positif est somme de 4 carrés d'entiers.

IV Application 2 : Géométrie de $\mathbb{R}^3$ (de $\mathbb{R}^4$?)

On note pour tout $z, z' \in \mathbb{H}$, $(z|z') = \frac{1}{2}(z\overline{z'} + z'\overline{z})$. On rappelle que la définition de $\mathbb{U}_{\mathbb{H}}$ et de $\mathbb{I}_{\mathbb{H}}$ a été donnée en fin de deuxième partie.

IV.1. Etude du produit scalaire.

(a) Montrer que pour tout $z, z' \in \mathbb{H}$, $(z|z') \in \mathbb{R}$ et $(z|z') = (z'|z)$.

Soient $z, z' \in \mathbb{H}$. Supposons que $z = a + b\mathrm{I} + c\mathrm{J} + d\mathrm{K}$ et $z' = a' + b'\mathrm{I} + c'\mathrm{J} + d'\mathrm{K}$ et $\overline{z'} = a' - b'\mathrm{I} - c'\mathrm{J} - d'\mathrm{K}$.

$$z\overline{z'} = (aa' + bb' + cc' + dd') + (-ab' + a'b - cd' + c'd)\mathrm{I} + (-ac' + a'c - db' + d'b)\mathrm{J} + (-ad' + a'd - bc' + b'c)\mathrm{K}$$
$$z'\overline{z} = (a'a + b'b + c'c + d'd) + (-a'b + ab' - c'd + cd')\mathrm{I} + (-a'c + ac' - d'b + db')\mathrm{J} + (-a'd + ad' - b'c + bc')\mathrm{K}$$

Ainsi (et comme l'expression est symétrique en $g \leftrightarrow g'$) :

$$(z|z') = (aa' + bb' + cc' + dd') = (z'|z) \in \mathbb{R}$$

(b) Montrer que pour tout $z \in \mathbb{H}$, $y \mapsto (z|y)$ est linéaire, i.e. vérifie :

$$\forall\ \lambda_1, \lambda_2 \in \mathbb{R}, \forall\ y_1, y_2 \in \mathbb{H} \quad : \quad (z|\lambda_1 y_1 + \lambda_2 y_2) = \lambda_1 (z|y_1) + \lambda_2 (z|y_2)$$

Soient $z \in \mathbb{H}$ (fixé) et $y_1, y_2 \in \mathbb{H}$ et $\lambda_1, \lambda_2 \in \mathbb{R}$:

$$\begin{aligned}(z|\lambda_1 y_1 + \lambda_2 y_2) &= \frac{1}{2}\left(z\overline{\lambda_1 y_1 + \lambda_2 y_2} + (\lambda_1 y_1 + \lambda_2 y_2)\overline{z}\right) \\ &= \frac{1}{2}\left(\lambda_1 z\overline{y_1} + \lambda_2 z\overline{y_2} + \lambda_1 y_1 \overline{z} + \lambda_2 y_2 \overline{z}\right) \\ &= \lambda_1 \frac{1}{2}(z\overline{y_1} + y_1\overline{z}) + \lambda_2 \frac{1}{2}(z\overline{y_2} + y_2\overline{z}) = \lambda_1 (z|y_1) + \lambda_2 (z|y_2)\end{aligned}$$

Pour tout $z \in \mathbb{H}$, $y \mapsto (z|y)$ est linéaire.

(c) Montrer que $(z|z) \geqslant 0$ et que $(z|z) = 0$ si et seulement si $z = 0$.

D'après un calcul précédent, avec $z' = z$, on a $(z|z) = a^2 + b^2 + c^2 + d^2 = |z|^2$.
On peut donc exploiter la réponse à la question II.1.(b), en notant que $\det(A) = |z|^2$ si $z = \Phi(A)$.

$$\boxed{\text{Et donc } (z|z) \geqslant 0 \text{ et que } (z|z) = 0 \text{ si et seulement si } z = 0.}$$

On dit que $(\cdot|\cdot)$ est un produit scalaire (compte-tenu des résultats des 3 questions (a), (b), (c)).

(d) Montrer que si $u \in \mathbb{U}_{\mathbb{H}}$, alors pour tout $z, z' \in \mathbb{H}$, $(zu|z'u) = (z|z') = (uz|uz')$.

Soit $u \in \mathbb{U}_{\mathbb{H}}$, donc $u\overline{u} = \overline{u}u = |u|^2 = 1$. Puis, pour tout $z, z' \in \mathbb{H}$, (en exploitant la réponse à la question II.3.(b) :

$$\begin{aligned}(zu|z'u) &= \frac{1}{2}\big(zu\overline{z'u} + z'u\overline{zu}\big) = \frac{1}{2}\big(zu\overline{u}\,\overline{z'} + z'u\overline{u}\,\overline{z}\big)\\ &= \frac{1}{2}\big(z|u|^2\overline{z'} + z'|u|^2\overline{z}\big) = \frac{1}{2}\big(z\overline{z'} + z'\overline{z}\big) = (z|z')\end{aligned}$$

Et de même :

$$(uz|uz') = \frac{1}{2}\big(uz\overline{uz'} + uz'\overline{uz}\big) = \frac{1}{2}\big(uz\overline{z'}\,\overline{u} + uz'\overline{z}\,\overline{u}\big)$$

Comme $(uz|uz')$ est un nombre réel, en multipliant à gauche par $\overline{u}$ et à droite par u, on a :

$$\overline{u}(uz|uz')u = (uz|uz')\overline{u}u = (uz|uz')|u|^2 = (uz|uz')$$

Et parallèlement :

$$\begin{aligned}\overline{u}(uz|uz')u &= \overline{u}\frac{1}{2}\big(uz\overline{z'}\overline{u} + uz'\overline{z}\,\overline{u}\big)u = \frac{1}{2}\big(\overline{u}uz\overline{z'}\overline{u}u/\overline{u}uz'\overline{z}\,\overline{u}u\big)\\ &= \frac{1}{2}\big(|u|^2z\overline{z'}|u|^2 + |u|^2z'\overline{z}|u|^2\big) = \frac{1}{2}\big(z\overline{z'} + z'\overline{z}\big) = (z|z')\end{aligned}$$

$$\boxed{\text{Par transitivité : si } u \in \mathbb{U}_{\mathbb{H}}, \text{ alors pour tout } z, z' \in \mathbb{H},\ (zu|z'u) = (z|z') = (uz|uz').}$$

IV.2. Soient $z, z' \in \mathbb{H}$.
Montrer que $z\overline{z'}z = -|z|^2z' + 2(z'|z)z$ (formule du triple produit).
On pourra partir du calcul $2(z'|z)z = \ldots$.

Par définition : $(z'|z) = \dfrac{1}{2}(z'\overline{z} + z\overline{z'})$.
Si on multiplie par z à droite :

$$2(z'|z)z = z'\overline{z}z + z\overline{z'}z = |z|^2z' + z\overline{z'}z$$

$$\boxed{\text{Donc } z\overline{z'}z = 2(z'|z)z - |z|^2z'.}$$

IV.3. Produit vectoriel dans $\mathbb{I}_{\mathbb{H}}$ - *ensemble des quaternions purs* (isomorphe à $\mathbb{R}^3$).
On note pour $z = a\mathrm{I} + b\mathrm{J} + c\mathrm{K}$ et $z' = a'\mathrm{I} + b'\mathrm{J} + c'\mathrm{K} \in \mathbb{I}_{\mathbb{H}}$: $\quad z \wedge z' = \dfrac{1}{2}(zz' - z'z)$.

(a) Exprimer $z \wedge z'$ en fonction des lettres a, b, c, a', b', c'.
Quel lien avec le produit vectoriel étudié en S.I. ?

On garde les mêmes notations

$$\begin{aligned}z \wedge z' &= \frac{1}{2}\Big(\big[(-bb' - cc' - dd') + (cd' - c'd)\mathrm{I} + (db' - d'b)\mathrm{J} + (bc' - b'c)\mathrm{K}\big]\\ &\quad - \big[(-b'b - c'c - d'd) + (c'd - cd')\mathrm{I} + (d'b - db')\mathrm{J} + (b'c - bc')\mathrm{K}\big]\Big)\end{aligned}$$

$$\boxed{z \wedge z' = (cd' - c'd)\mathrm{I} + (db' - d'b)\mathrm{J} + (bc' - b'c)\mathrm{K}}$$

• Remarquons que la formule n'est pas symétrique (mais antisymétrique).
• Si les nombres devant I, J et K sont les coordonnées d'un vecteur de $\mathbb{R}^3$, alors $z \wedge z'$ donne les coordonnées du produit vectoriel (vu en SI) des vecteurs associés à z et à z'.

(b) Montrer que pour tout $z, z' \in \mathbb{I}_{\mathbb{H}}$, $zz' = -(z|z') + z \wedge z'$.

Pour $z, z' \in \mathbb{I}_{\mathbb{H}}$, on a vu que

$$zz' = (-bb' - cc' - dd') + (cd' - c'd)\mathrm{I} + (db' - d'b)\mathrm{J} + (bc' - b'c)\mathrm{K} = -(z|z') + z \wedge z'$$

d'après des calculs précédents (en prenant $a = 0$ et $a' = 0$)

$$\boxed{\text{Pour tout } z, z' \in \mathbb{I}_{\mathbb{H}},\ zz' = -(z|z') + z \wedge z'.}$$

IV.4. Rotations (=isométrie).
Soit $q \in \mathbb{U}_{\mathbb{H}} \setminus \{-1,1\}$ et $r_q : \mathbb{I}_{\mathbb{H}} \to \mathbb{I}_{\mathbb{H}}$, $z \mapsto qzq^{-1} = qz\overline{q}$ car $|q|^2 = 1$.

(a) Montrer qu'on a bien, pour tout $z \in \mathbb{I}_{\mathbb{H}}$, $r_q(z) \in \mathbb{I}_{\mathbb{H}}$.

Vérifions d'abord que l'image de $\mathbb{I}_{\mathbb{H}}$ par r_q est bien incluse dans $\mathbb{I}_{\mathbb{H}}$.

Pour tout $z \in \mathbb{I}_{\mathbb{H}}$, puisque $q \in \mathbb{U}_{\mathbb{H}}$, ainsi que $q^{-1} = \dfrac{\overline{q}}{|q|^2} = \overline{q}$ d'après la formule II.3.(d), on a donc $r_q(z) = qzq^{-1} = qz\overline{q}$.

Pour savoir si il s'agit d'un quaternion pure, il suffit de montrer que $r_q(z) + \overline{r_q(z)} = 0$.
Notons d'abord que $\overline{abc} = \overline{ab \times c} = \overline{c} \times \overline{ab} = \overline{c}\,\overline{b}\,\overline{a}$. Donc

$$r_q(z) + \overline{r_q(z)} = qz\overline{q} + \overline{qz\overline{q}} = qz\overline{q} + \overline{\overline{q}}\,\overline{z}\,\overline{q} = qz\overline{q} + q\,\overline{z}\,\overline{q} = q(\underbrace{z+\overline{z}}_{=0 \text{ car } z\in\mathbb{I}_{\mathbb{H}}})\overline{q} = 0$$

$$\boxed{r_q(\mathbb{I}_{\mathbb{H}}) \subset \mathbb{I}_{\mathbb{H}}}$$

(b) Montrer que pour tout $z, z' \in \mathbb{H}$, $\big(r_q(z)|r_q(z')\big) = (z|z')$.
On dit que r_q est une isométrie (ou rotation) de $\mathbb{I}_{\mathbb{H}}$.

Soient $z, z' \in \mathbb{H}$. D'après IV.1.(d), pour $u \in \mathbb{U}_{\mathbb{Z}}$, $(uz|uz') = (z|z') = (zu|zu')$.
Ici, $q \in \mathbb{U}_{\mathbb{Z}}$, donc $q^{-1} = \overline{q} \in \mathbb{U}(\mathbb{Z})$

$$\big(r_q(z)|r_q(z')\big) = (qzq^{-1}|qz'q^{-1}) = (zq^{-1}|zq^{-1}) = (z|z')$$

$$\boxed{\text{Pour tout } z, z' \in \mathbb{H},\ \big(r_q(z)|r_q(z')\big) = (z|z').}$$

(c) On sait d'après II.4.(c), qu'il existe $\theta \in]0,\pi[$ $(q \notin \{-1,1\})$, $s \in \mathbb{I}_{\mathbb{H}} \cap \mathbb{U}_{\mathbb{H}}$ tel que $q = \cos\theta + s \times \sin\theta$.
Montrer que $r_q(s) = s$. (On pourra commencer par simplifier s^2)

Comme $s \in \mathbb{I}_{\mathbb{H}}$, $\overline{s} = -s$, donc $s^2 = -s\overline{s} = -|s|^2 = -1$ car $s \in \mathbb{U}_{\mathbb{H}}$.
Donc
$r_q(s) = (\cos\theta + s\sin\theta)s(\cos\theta - s\sin\theta) = \cos^2\theta s + (\sin\theta\cos\theta - \sin\theta\cos\theta)s^2 - \sin^2\theta s^3 = \cos^2\theta s + \sin^2\theta s = (\cos^2\theta + \sin^2\theta)s = s$

$$\boxed{r_q(s) = s}$$

(d) Soit $t \in \mathbb{I}_{\mathbb{H}} \cap \mathbb{U}_{\mathbb{H}}$ tel que $(s|t) = 0$ (t est orthogonal à s).
Montrer que $(t|r_q(t)) = \cos(2\theta)$ et $t \wedge r_q(t) = \sin(2\theta)s$.

Comme $t, r_q(t) \in \mathbb{I}_{\mathbb{H}}$, ces deux nombres figurant dans le seul calcul $t \times r_q(t)$, on va se concentrer sur ce calcul.
(Il s'agit des parties réelles (opposés) et imaginaires quaternioniques).
Par ailleurs, comme $(s|t) = 0$, on a $s\overline{t} + t\overline{s} = 0$, donc $t\overline{s} = -s\overline{t}$.
Mais comme $s, t \in \mathbb{I}_{\mathbb{H}}$, $\overline{s} = -s$ et $\overline{t} = -t$, donc $ts = -st$.
Ainsi $tq = t(\cos\theta + s\sin\theta) = \cos\theta t + \sin\theta ts = \cos\theta t - \sin\theta st = (\cos\theta - s\sin\theta) \times t = \overline{q}t$. Donc

$$t \times r_q(t) = tqt\overline{q} = \overline{q}t^2q = -\overline{q}t\overline{t}q = -\overline{q}^2 = -(\cos\theta - s\sin\theta)^2$$

car $t \in \mathbb{U}_{\mathbb{H}}$, donc $|t|^2 = t\overline{t} = 1$.
Donc de même comme $s^2 = -1$:

$$t \times r_q(t) = -((\cos^2\theta - \sin^2\theta) - 2s\cos\theta\sin\theta = -\cos(2\theta) + s\sin(2\theta)$$

On prend les parties réelles et imaginaires, pour obtenir respectivement $-(t|r_q(t))$ et $t \wedge r_q(t)$.

$$\boxed{\text{Ainsi } (t|r_q(t)) = \cos(2\theta) \text{ et } t \wedge r_q(t) = \sin(2\theta)s.}$$

Géométriquement, cela signifie que r_q est la rotation de l'espace $\mathbb{I}_{\mathbb{H}} \sim \mathbb{R}^3$ d'axe s et d'angle 2θ.

IV.5. (**) Justifier la formule exponentielle : $q = e^{s\theta}$.
On rappelle que $e^x = \lim\limits_{n\to+\infty}\left(\sum\limits_{k=0}^{n}\dfrac{x^k}{k!}\right)$.

On a vu que $s^2 = -s\overline{s} = -|s|^2 = -1$.
Et donc, par récurrence rapide : $s^k = \begin{cases} s & \text{si } k \equiv 1[4] \\ -1 & \text{si } k \equiv 2[4] \\ -s & \text{si } k \equiv 3[4] \\ 1 & \text{si } k \equiv 4[4] \end{cases}$.
Ainsi,

$$\exp(s\theta) = \sum_{k=0}^{+\infty}\frac{s^k\theta^k}{k!} = \sum_{h=0}^{+\infty}(-1)^h\frac{\theta^{2h}}{(2h)!} + \sum_{h=0}^{+\infty}(-1)^{h+1}\frac{s\theta^{2h+1}}{(2h+1)!} = \cos\theta + s\ \sin\theta = q$$

$$\boxed{\text{On peut donc noter, pour tout } q \in \mathbb{U}_{\mathbb{H}},\ q = e^{s\theta}, \text{ si } q = \cos\theta + s\ \sin\theta.}$$
