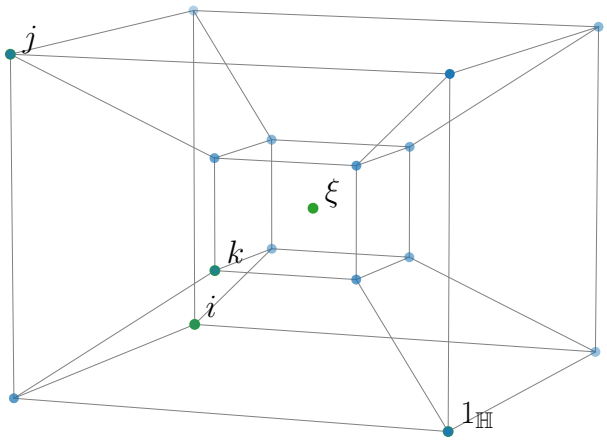
En cas d'erreur de corrigé, n'hésitez pas à me le signaler.

Contexte

L'objectif de ce problème est de démontrer le **théorème des quatre carrés** de Lagrange, affirmant que tout entier naturel peut s'écrire comme somme de quatre carrés d'entiers. La preuve proposée repose sur une étude **arithmétique** d'une **structure algébrique** issue des **matrices** carrées: celle des quaternions demi-entiers aussi appelés quaternions de Hurwitz.



1 Quaternions via les matrices réelles

On note dans ce problème

$$1_{\mathbb{H}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

et

$$\mathbb{H} = \left\{ a1_{\mathbb{H}} + bi + cj + dk,\ (a,b,c,d) \in \mathbb{R}^4 \right\} \subset \mathrm{M}_4(\mathbb{R}).$$

Ainsi,

$$\mathbb{H} = \left\{ \begin{pmatrix} a & d & c & b \\ -d & a & b & -c \\ -c & -b & a & d \\ -b & c & -d & a \end{pmatrix},\ (a,b,c,d) \in \mathbb{R}^4 \right\}.$$

1.1. Calculer les produits i^2, ij et ji.

On a

$$ii = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

ainsi

$$\boxed{i^2 = -1_{\mathbb{H}}}.$$

De même

$$ij = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

ainsi

$$\boxed{ij = k}.$$

Enfin

$$ji = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ainsi

$$\boxed{ji = -k}.$$

Remarques
- On aurait pu simplifier les calculs en effectuant des calculs par blocs 2×2.
- On aurait aussi pu simplifier les calculs en remarquant que i, j, k sont antisymétriques et par conséquent

$$(ji) = \left((ji)^\top\right)^\top = \left(i^\top j^\top\right)^T = ((-i)(-j))^\top = k^\top = -k.$$

- Enfin le résultat est donné dans la suite du sujet !
  Ainsi,
  ▷ il serait dommage d'obtenir un résultat faux,
  ▷ on ne peut évidemment pas se contenter d'affirmer le résultat sans aucune étape intermédiaire.

On admettra dans la suite les relations suivantes (il n'est pas demandé de les redémontrer) :
▷ $i^2 = j^2 = k^2 = -1_{\mathbb{H}}$,
▷ $ij = k$ et $ji = -k$,
▷ $jk = i$ et $kj = -i$,
▷ $ki = j$ et $ik = -j$.
Il est conseillé d'utiliser ces relations pour simplifier les calculs dans la suite du sujet.

1.2. Montrer que $\mathbb{H}$ est un sous-anneau de $\mathrm{M}_4(\mathbb{R})$.

- On a $I_4 = 1 1_{\mathbb{H}} + 0i + 0j + 0k \in \mathbb{H}$.
  D'où l'appartenance de l'unité.
- Soit $z \in \mathbb{H}$.
  Soient $a, b, c, d \in \mathbb{R}^4$ tels que $z = a1_{\mathbb{H}} + bi + cj + dk$.
  Alors $-z = (-a)1_{\mathbb{H}} + (-b)i + (-c)j + (-d)k \in \mathbb{H}$.
  D'où la stabilité par opposé.
  Remarque: en fait la stabilité par opposé n'est pas nécessaire il suffit de vérifier que $-I_4 \in \mathbb{H}$ et la stabilité par produit.
- Soient $z_1, z_2 \in \mathbb{H}$.
  Soient $a_1, b_1, c_1, d_1 \in \mathbb{R}^4$ et $a_2, b_2, c_2, d_2 \in \mathbb{R}^4$ tels que $z_1 = a_1 1_{\mathbb{H}} + b_1 i + c_1 j + d_1 k$ et $z_2 = a_2 1_{\mathbb{H}} + b_2 i + c_2 j + d_2 k$.
  Alors

$$\begin{aligned} z_1 + z_2 &= (a_1 1_{\mathbb{H}} + b_1 i + c_1 j + d_1 k) + (a_2 1_{\mathbb{H}} + b_2 i + c_2 j + d_2 k) \\ &= (a_1 + a_2)1_{\mathbb{H}} + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k \in \mathbb{H}. \end{aligned}$$

  d'où la stabilité par somme.
  De plus, en développant à l'aide des relations précédentes (en prenant garde que le produit est **non commutatif**),

$$\begin{aligned} z_1 z_2 &= (a_1 1_{\mathbb{H}} + b_1 i + c_1 j + d_1 k)(a_2 1_{\mathbb{H}} + b_2 i + c_2 j + d_2 k) \\ &= a_1 a_2 1_{\mathbb{H}}^2 + a_1 b_2 1_{\mathbb{H}} i + a_1 c_2 1_{\mathbb{H}} j + a_1 d_2 1_{\mathbb{H}} k \\ &\quad + b_1 a_2 i 1_{\mathbb{H}} + b_1 b_2 i^2 + b_1 c_2 ij + b_1 d_2 ik \\ &\quad + c_1 a_2 j 1_{\mathbb{H}} + c_1 b_2 ji + c_1 c_2 j^2 + c_1 d_2 jk \\ &\quad + d_1 a_2 k 1_{\mathbb{H}} + d_1 b_2 ki + d_1 c_2 kj + d_1 d_2 k^2 \\ &= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2)1_{\mathbb{H}}^2 \\ &\quad + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i \\ &\quad + (a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2)j \\ &\quad + (a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2)k \end{aligned}$$

  et donc $z_1 z_2 \in \mathbb{H}$.
  D'où la stabilité par produit.
  Remarques:
  ▷ l'expression exacte du calcul n'est pas essentielle, il suffit en fait d'utiliser que pour $\varepsilon_1, \varepsilon_2 \in \{1_{\mathbb{H}}, i, j, k\}$, on a $\varepsilon_1 \varepsilon_2 \in \mathbb{H}$,
  ▷ l'expression explicite du produit peut aider dans la résolution des questions suivantes.

Donc $\boxed{\mathbb{H} \text{ est un sous-anneau de } \mathrm{M}_4(\mathbb{R})}$.

1.3. Montrer que $\mathbb{H}$ est stable par transposée, c'est-à-dire que

$$\forall z \in \mathbb{H}, \quad z^\top \in \mathbb{H}.$$

Soit $z \in \mathbb{H}$.
Soient $a, b, c, d \in \mathbb{R}^4$ tels que $z = a1_{\mathbb{H}} + bi + cj + dk$.
Alors comme $1_{\mathbb{H}}^\top = 1_{\mathbb{H}}$, $i^\top = -i$, $j^\top = -j$ et $k^\top = -k$, on a

$$z^\top = (a1_{\mathbb{H}} + bi + cj + dk)^\top = a1_{\mathbb{H}} + (-b)i + (-c)j + (-d)k \in \mathbb{H}.$$

Donc $\boxed{\mathbb{H} \text{ est stable par transposée}}$.

1.4. Soient $a, b, c, d \in \mathbb{R}$.
Soit $z = a1_{\mathbb{H}} + bi + cj + dk$.
Montrer qu'il existe un et unique $r \in \mathbb{R}$ tel que

$$zz^\top = z^\top z = r1_{\mathbb{H}}$$

et exprimer r en fonction de a, b, c, d.

Comme $z = a1_{\mathbb{H}} + bi + cj + dk$ on a $z^\top = a1_{\mathbb{H}} - bi - cj - dk$, d'où par l'expression explicite du produit obtenue à la question **1.2.**, on a

$$zz^\top = (a1_{\mathbb{H}} + bi + cj + dk)(a1_{\mathbb{H}} - bi - cj - dk) = \left(a^2 + b^2 + c^2 + d^2\right) 1_{\mathbb{H}}$$

et

$$z^\top z = (a1_{\mathbb{H}} - bi - cj - dk)(a1_{\mathbb{H}} + bi + cj + dk) = \left(a^2 + b^2 + c^2 + d^2\right) 1_{\mathbb{H}}.$$

D'où $\boxed{\text{l'existence}}$ avec $\boxed{r = a^2 + b^2 + c^2 + d^2}$.
De plus comme $1_{\mathbb{H}} \neq 0_4$, par pseudo-intégrité on a pour tous $r_1, r_2 \in \mathbb{R}$ on a si $r_1 1_{\mathbb{H}} = r_2 1_{\mathbb{H}}$ alors $r_1 = r_2$.
D'où $\boxed{\text{l'unicité}}$.

Dans la suite, pour $z \in \mathbb{H}$, on note $N(z)$ l'unique réel tel que

$$zz^\top = N(z)1_{\mathbb{H}}.$$

1.5. Montrer que :

- pour tout $z \in \mathbb{H}$,
$$N(z) = 0 \iff z = 0_{\mathbb{H}},$$
- pour tous $z_1, z_2 \in \mathbb{H}$,
$$N(z_1 z_2) = N(z_1)N(z_2).$$

- Soit $z \in \mathbb{H}$.
On procède par double implication.
▷ $\boxed{\Leftarrow}$
Supposons $z = 0_{\mathbb{H}}$.
Alors $zz^\top = 0_{\mathbb{H}}0_{\mathbb{H}} = 01_{\mathbb{H}}$ et donc $N(z) = 0$.
▷ $\boxed{\Rightarrow}$
Supposons $N(z) = 0$.
Soient $a, b, c, d \in \mathbb{R}$ tels que $z = a1_{\mathbb{H}} + bi + cj + dk$.
Par la question **1.4.**, on a $N(z) = a^2 + b^2 + c^2 + d^2$.
Comme un carré est positif et que si une somme de termes positifs est nulle alors tous les termes sont nuls, on a $a^2 = b^2 = c^2 = d^2 = 0$, et donc $a = b = c = d = 0$. D'où $z = 0_{\mathbb{H}}$.
Par conséquent on a bien $\boxed{N(z) = 0 \iff z = 0_{\mathbb{H}}}$.
- Soient $z_1, z_2 \in \mathbb{H}$.
On a alors, comme $1_{\mathbb{H}}$ commute avec tout élément,

$$\begin{aligned}(z_1 z_2)(z_1 z_2)^\top &= z_1 z_2 z_2^\top z_1^\top \\ &= z_1 (N(z_2)1_{\mathbb{H}}) z_1^\top \\ &= N(z_2) z_1 1_{\mathbb{H}} z_1^\top \\ &= N(z_2)N(z_1)1_{\mathbb{H}}\end{aligned}$$

et donc (comme $\mathbb{R}$ commutatif)

$$\boxed{N(z_1 z_2) = N(z_1)N(z_2)}.$$

Remarque: on aurait pu aussi effectuer un calcul explicite, mais ce calcul est extrêmement pénible, en effet il faut

constater que

$$\begin{aligned}(a_1{}^2+b_1{}^2+c_1{}^2+d_1{}^2)(a_2{}^2+b_2{}^2+c_2{}^2+d_2{}^2) &= (a_1a_2-b_1b_2-c_1c_2-d_1d_2)^2\\ &+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)^2\\ &+(a_1c_2-b_1d_2+c_1a_2+d_1b_2)^2\\ &+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)^2.\end{aligned}$$

1.6. En déduire que tout élément non nul de $\mathbb{H}$ est inversible.

Soit $z\in\mathbb{H}\backslash\{0_{\mathbb{H}}\}$.
Alors, par la question **1.5.**

$$N(z)\in\mathbb{R}\backslash\{0\}.$$

Et par définition de $N(z)$ on a donc

$$z\left(N(z)^{-1}z^\top\right)=zz^\top N(z)^{-1}=N(z)N(z)^{-1}1_{\mathbb{H}}=1_{\mathbb{H}}.$$

Et de même (ce n'est pas nécessaire de le vérifier pour les matrices, car tout inverse à gauche est inverse à droite)

$$\left(N(z)^{-1}z^\top\right)z=N(z)^{-1}z^\top z=N(z)N(z)^{-1}1_{\mathbb{H}}=1_{\mathbb{H}}.$$

D'où $\boxed{z \text{ est inversible}}$ et

$$\boxed{z^{-1}=N(z)^{-1}z^\top}.$$

1.7. L'ensemble $\mathbb{H}$ muni des opérations $+$ et $\times$ est-il un corps ?

Ce n'est $\boxed{\textbf{pas un corps}}$, car $\mathbb{H}$ n'est pas commutatif pour la multiplication, par exemple $ij=k\neq -k=ji$.
Remarque: on observe néanmoins qu'il s'agit d'un anneau dans lequel tout élément non nul est inversible.
On parle parfois d'«anneau à division» ou de «corps gauche» pour désigner une telle structure algébrique.

Remarque culturelle:
On observe que la construction des quaternions $\mathbb{H}$ est très proche de celui des nombres complexes $\mathbb{C}$.
Ainsi avec $1_{\mathbb{C}}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$ et $i_{\mathbb{C}}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$, on obtient $\mathbb{C}=\left\{a1_{\mathbb{C}}+bi_{\mathbb{C}},\ (a,b)\in\mathbb{R}^2\right\}$.
Ainsi $z^\top$ correspond à $\overline{z}$ et $N(z)$ à $|z|^2$.

---

2 Arithmétique sur les quaternions de Hurwitz

On note dans la suite

$$\mathbb{H}_{\mathbb{Z}}=\left\{a1_{\mathbb{H}}+bi+cj+dk,\ (a,b,c,d)\in\mathbb{Z}^4\right\}$$

et on remarque alors (il n'est pas demandé de le démontrer) qu'il s'agit d'un sous-anneau stable par transposée de $(\mathbb{H},+,\times)$.
On note aussi

$$\xi=\frac{1_{\mathbb{H}}+i+j+k}{2}.$$

Enfin, on note

$$\mathcal{H}=\mathbb{H}_{\mathbb{Z}}+\mathbb{Z}\xi=\left\{h+k\xi,\ (h,k)\in\mathbb{H}_{\mathbb{Z}}\times\mathbb{Z}\right\}.$$

2.8. Montrer que $\mathcal{H}$ est un sous-anneau stable par transposée de $(\mathbb{H},+,\times)$.

- On a $1_{\mathcal{H}}=1_{\mathbb{H}}+0\xi\in\mathcal{H}$, d'où l'appartenance de l'unité.
- Soit $\alpha\in\mathcal{H}$.
  Soient $h\in\mathbb{H}_{\mathbb{Z}}$ et $k\in\mathbb{Z}$ tels que $\alpha=h+k\xi$.
  Alors $-\alpha=(-h)+(-k)\xi\in\mathcal{H}$.
  d'où la stabilité par opposé.
- Soient $\alpha_1,\alpha_2\in\mathcal{H}$.
  Soient $h_1,h_2\in\mathbb{H}_{\mathbb{Z}}$ et $k_1,k_2\in\mathbb{Z}$ tels que $\alpha_1=h_1+k_1\xi$ et $\alpha_2=h_2+k_2\xi$.
  Alors

$$\begin{aligned}\alpha_1+\alpha_2 &= (h_1+k_1\xi)+(h_2+k_2\xi)\\ &= (h_1+h_2)+(k_1+k_2)\xi \in \mathcal{H}.\end{aligned}$$

D'où la stabilité par somme.
De plus, on

$$\begin{aligned}\alpha_1\alpha_2 &= (h_1+k_1\xi)(h_2+k_2\xi)\\ &= h_1h_2+k_2h_1\xi+k_1\xi h_2+k_1k_2\xi^2.\end{aligned}$$

Par stabilité par somme il suffit alors de démontrer que $h_1\xi$, ξh_2 et ξ^2 sont dans $\mathcal{H}$.
Quitte à décomposer $h_{1/2}$ en la somme $h_{1/2} = a_{1/2}1_{\mathbb{H}} + b_{1/2}i + c_{1/2}j + d_{1/2}k$ et à développer, on est donc ramené à montrer que $i\xi$, $j\xi$, $k\xi$, ξi, ξj, ξk et ξ^2 sont dans $\mathcal{H}$.
Vérifions cela:

$$\begin{aligned}i\xi &= i\frac{1_{\mathbb{H}}+i+j+k}{2}\\ &= \frac{i1_{\mathbb{H}}+ii+ij+ik}{2}\\ &= \frac{i-1_{\mathbb{H}}+k-j}{2}\\ &= (i+k)-\xi \in \mathcal{H},\end{aligned} \qquad \begin{aligned}\xi i &= \frac{1_{\mathbb{H}}+i+j+k}{2}i\\ &= \frac{1_{\mathbb{H}}i+ii+ji+ki}{2}\\ &= \frac{i-1_{\mathbb{H}}-k+j}{2}\\ &= (i+j)-\xi \in \mathcal{H},\end{aligned}$$

et de même

$$\begin{aligned}j\xi &= \frac{j1_{\mathbb{H}}+ji+jj+jk}{2}\\ &= \frac{j-k-1_{\mathbb{H}}+i}{2}\\ &= (j+i)-\xi \in \mathcal{H},\end{aligned} \qquad \begin{aligned}\xi j &= \frac{1_{\mathbb{H}}j+ij+jj+kj}{2}\\ &= \frac{j+k-1_{\mathbb{H}}-i}{2}\\ &= (j+k)-\xi \in \mathcal{H},\end{aligned}$$

ainsi que

$$\begin{aligned}k\xi &= \frac{k1_{\mathbb{H}}+ki+kj+kk}{2}\\ &= \frac{k+j-i-1_{\mathbb{H}}}{2}\\ &= (k+j)-\xi \in \mathcal{H},\end{aligned} \qquad \begin{aligned}\xi k &= \frac{1_{\mathbb{H}}k+ik+jk+kk}{2}\\ &= \frac{k-j+i-1_{\mathbb{H}}}{2}\\ &= (k+i)-\xi \in \mathcal{H},\end{aligned}$$

et finalement

$$\begin{aligned}\xi^2 &= \frac{\xi+i\xi+j\xi+k\xi}{2}\\ &= \frac{\xi+i+k-\xi+j+i-\xi+k+j-\xi}{2}\\ &= \frac{\xi+2(2\xi-1)-3\xi}{2}\\ &= \xi-1 \in \mathcal{H}.\end{aligned}$$

D'où la stabilité par produit.
Ainsi $\boxed{\mathcal{H} \text{ est un sous-anneau de } \mathbb{H}}$.
Enfin soit $\alpha \in \mathcal{H}$.
Soient $h \in \mathbb{H}_{\mathbb{Z}}$ et $k \in \mathbb{Z}$ tels que $\alpha = h + k\xi$.
On a comme

$$\xi^\top = \frac{1_{\mathbb{H}}^\top + i^\top + j^\top + k^\top}{2} = \frac{1_{\mathbb{H}} - i - j - k}{2} = 1_{\mathbb{H}} - \xi,$$

et comme $\mathbb{H}_{\mathbb{Z}}$ est stable par transposée,

$$\alpha^\top = (h+k\xi)^\top = h^\top + k\xi^\top = h^\top + k(1_{\mathbb{H}} - \xi) = (h^\top + k1_{\mathbb{H}}) + (-k)\xi \in \mathcal{H}.$$

Donc $\boxed{\mathcal{H} \text{ est stable par transposée}}$.

2.9. Soient $a, b, c, d \in \mathbb{Z}$ des entiers **de même parité** (c'est à dire tous pairs ou tous impairs).
Montrer que

$$a^2+b^2+c^2+d^2 \equiv 0\ [4].$$

On a la table de congruence des carrés modulo 4:

k [4]	0	1	2	3
k^2 [4]	0	1	0	1

par conséquent le carré d'un nombre impair est congru à 1 modulo 4 et le carré d'un nombre pair est congru à 0 modulo 4.

Remarque: plutôt qu'un tableau de congruence, il suffit de remarquer que pour tout entier k, $(2k+1)^2 = 4(k^2+k)+1$ et $(2k)^2 = 4k^2$.
Comme $1+1+1+1 \equiv 0\ [4]$ et $0+0+0+0 \equiv 0\ [4]$ on a donc $\boxed{a^2+b^2+c^2+d^2 \equiv 0\ [4]}$.

2.10. En déduire que

$$\forall \alpha \in \mathcal{H}, \quad N(\alpha) \in \mathbb{N}.$$

Soit $\alpha \in \mathcal{H}$. On sait déjà que $N(\alpha) \in \mathbb{R}_+$ comme somme de carrés.
Soient $h \in \mathbb{H}_\mathbb{Z}$ et $k \in \mathbb{Z}$ tels que $\alpha = h + k\xi$.
Soient $a, b, c, d \in \mathbb{Z}$ tels que $h = a1_\mathbb{H} + bi + cj + dk$.
Alors

$$\alpha = \frac{2a+k}{2}1_\mathbb{H} + \frac{2b+k}{2}i + \frac{2c+k}{2}j + \frac{2d+k}{2}k.$$

et donc d'après l'expression explicite de N de la question **1.4.**, on a

$$N(\alpha) = \left(\frac{2a+k}{2}\right)^2 + \left(\frac{2b+k}{2}\right)^2 + \left(\frac{2c+k}{2}\right)^2 + \left(\frac{2d+k}{2}\right)^2 = \frac{(2a+k)^2+(2b+k)^2+(2c+k)^2+(2d+k)^2}{4} \in \mathbb{N}.$$

Or $2a+k$, $2b+k$, $2c+k$ et $2d+k$ sont de même parité, donc d'après la question **2.9.**, on a $4|(2a+k)^2+(2b+k)^2+(2c+k)^2+(2d+k)^2$ et donc

$$\boxed{N(\alpha) \in \mathbb{N}}.$$

2.11. Montrer que

$$\mathcal{H}^\times = \{\alpha \in \mathcal{H} \mid N(\alpha) = 1\}$$

où $\mathcal{H}^\times$ est l'ensemble des éléments inversibles de $\mathcal{H}$.

On procède par double inclusion.

- $\boxed{\subset}$ Soit $\alpha \in \mathcal{H}^\times$.
  On a alors
  $$\alpha\alpha^{-1} = 1_\mathbb{H}$$
  et par conséquent
  $$N(\alpha\alpha^{-1}) = N(1_\mathbb{H}) = 1.$$
  Or d'après la question **1.5.**, on a
  $$N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$$
  et d'après la question **2.10.** on a
  $$N(\alpha) \in \mathbb{N} \quad \text{et} \quad N(\alpha^{-1}) \in \mathbb{N}.$$
  Par conséquent (le seul inversible pour le produit dans $\mathbb{N}$ étant 1) on a
  $$N(\alpha) = 1.$$
- $\boxed{\supset}$ Soit $\alpha \in \mathcal{H}$ tel que $N(\alpha) = 1$.
  On a déjà vu (par exemple à la question **1.6.**) que par la définition de N,
  $$\alpha\alpha^\top = \alpha^\top\alpha = N(\alpha)1_\mathbb{H} = 1_\mathbb{H}.$$
  Comme $\mathcal{H}$ est stable par transposée (question **2.8.**), on a $\alpha^\top \in \mathcal{H}$.
  Par conséquent α est inversible (d'inverse $\alpha^\top$) et donc $\alpha \in \mathcal{H}^\times$.

On a donc bien

$$\boxed{\mathcal{H}^\times = \{\alpha \in \mathcal{H} \mid N(\alpha) = 1\}}.$$

Remarque: On pourrait aussi expliciter les éléments $\mathcal{H}^\times$ formant un groupe non commutatif à 24 éléments, mais cela n'est pas demandé.

2.12. Soit $z \in \mathbb{H}$.
Montrer qu'il existe $\gamma \in \mathcal{H}$ tel que

$$N(z-\gamma) < 1.$$

Indication : une intuition géométrique sur les hypercubes en dimension 4 peut être utile.
Alternativement, on pourra admettre cette question en première lecture.

Étant donné un réel x, on note dans cette question $[x]$ l'entier le plus proche de x, en prenant la partie entière dans le cas d'un demi-entier. Plus précisément, on pose

$$[x] = \begin{cases} \lfloor x \rfloor & \text{si } x \leq \lfloor x \rfloor + \frac{1}{2} \\ \lfloor x \rfloor + 1 & \text{sinon} \end{cases}$$

On remarque qu'en particulier pour tout $x \in \mathbb{R}$, on a

$$[x] \in \mathbb{Z} \quad \text{et} \quad |x - [x]| \leq \frac{1}{2}$$

et que $|x - [x]| = \frac{1}{2}$ ssi $x = [x] + \frac{1}{2}$.
Soient $a, b, c, d \in \mathbb{R}^4$ tels que $z = a1_{\mathbb{H}} + bi + cj + dk$.
Posons $\gamma_0 = [a]1_{\mathbb{H}} + [b]i + [c]j + [d]k$.
Alors

$$z - \gamma_0 = (a - [a])1_{\mathbb{H}} + (b - [b])i + (c - [c])j + (d - [d])k$$

et alors

$$N(z - \gamma_0) = (a - [a])^2 + (b - [b])^2 + (c - [c])^2 + (d - [d])^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1.$$

De plus l'inégalité est une égalité ssi tous les carré valent $\frac{1}{4}$, c'est à dire ssi $a = [a] + \frac{1}{2}$, $b = [b] + \frac{1}{2}$, $c = [c] + \frac{1}{2}$ et $d = [d] + \frac{1}{2}$.
Par conséquent on procède par disjonction de cas:
- Si $N(z - \gamma_0) < 1$, on pose $\gamma = \gamma_0$,
- Sinon on pose $\gamma = \gamma_0 + \xi$. Alors $N(z - \gamma) = 0$.

Dans tous les cas on a bien $\boxed{\gamma \in \mathcal{H}}$ et $\boxed{N(z - \gamma) < 1}$.

2.13. Soient $\alpha, \beta \in \mathcal{H}$ tels que $\beta \neq 0_{\mathcal{H}}$.
Déduire de la question précédente qu'il existe $\gamma, \rho \in \mathcal{H}$ tels que

$$\alpha = \beta\gamma + \rho \quad \text{et} \quad N(\rho) < N(\beta).$$

Comme tout élément non nul de $\mathbb{H}$ est inversible dans $\mathbb{H}$, on pose

$$z = \beta^{-1}\alpha \in \mathbb{H}.$$

Par la question **2.12.**, il existe $\gamma \in \mathcal{H}$ tel que

$$N(z - \gamma) < 1$$

c'est à dire $N(\beta^{-1}\alpha - \gamma) < 1$.
Alors (comme $N(\beta) > 0$)

$$\begin{aligned} N(\alpha - \beta\gamma) &= N\left(\beta(\beta^{-1}\alpha - \gamma)\right) \\ &= N(\beta)N(\beta^{-1}\alpha - \gamma) \\ &< N(\beta). \end{aligned}$$

En posant $\rho = \alpha - \beta\gamma$, on a bien $\boxed{\alpha = \beta\gamma + \rho}$ et $\boxed{N(\rho) < N(\beta)}$.

On dit que $\mathcal{I} \subset \mathcal{H}$ est un **idéal à droite** de $\mathcal{H}$ ssi
- $\mathcal{I}$ est un sous-groupe de $(\mathcal{H}, +)$,
- pour tout $\lambda \in \mathcal{H}$ et tout $\beta \in \mathcal{I}$, on a $\beta\lambda \in \mathcal{I}$.

2.14. Soit $\mathcal{I}$ un idéal à droite de $\mathcal{H}$.
Montrer qu'il existe $\delta \in \mathcal{H}$ tel que

$$\mathcal{I} = \delta\mathcal{H}$$

où

$$\delta\mathcal{H} = \{\delta\lambda,\ \lambda \in \mathcal{H}\}.$$

Remarque: il s'agit presque d'une question de cours: en effet la question précédente montrait l'existence d'une division euclidienne. Il suffit donc de reprendre la preuve que l'on a vu en cours pour les entiers.
Si $\mathcal{I} = \{0_{\mathcal{H}}\}$, alors en posant $\delta = 0_{\mathcal{H}}$ et on a bien $\mathcal{I} = \delta\mathcal{H}$.

Supposons désormais que $\mathcal{I} \neq \{0_{\mathcal{H}}\}$.
Alors $\mathcal{I}$ contient un élément non nul, et donc

$$\{N(\alpha), \alpha \in \mathcal{I} \backslash \{0_{\mathbb{H}}\}\}$$

est une partie non vide de $\mathbb{N}$.
Elle admet donc un minimum.
Fixons $\delta \in \mathcal{I}\backslash\{0_{\mathbb{H}}\}$ tel que $N(\delta)$ soit minimal, c'est à dire

$$N(\delta) = \min\{N(\alpha), \alpha \in \mathcal{I}\backslash\{0_{\mathbb{H}}\}\}.$$

Montrons par double inclusion que $\mathcal{I} = \delta\mathcal{H}$.

- $\boxed{\supset}$ On a $\delta \in \mathcal{I}$, et comme $\mathcal{I}$ est un idéal à droite, on a donc pour tout $\lambda \in \mathcal{H}$, $\delta\lambda \in \mathcal{I}$.
  D'où

$$\boxed{\delta\mathcal{H} \subset \mathcal{I}}$$

- $\boxed{\subset}$ Soit $\alpha \in \mathcal{I}$.
  D'après la question **2.13.** (comme $\delta \neq 0_{\mathbb{H}}$), il existe $\gamma, \rho \in \mathcal{H}$ tels que

$$\alpha = \delta\gamma + \rho \quad \text{et} \quad N(\rho) < N(\delta).$$

  Or $\alpha \in \mathcal{I}$ et comme on a déjà vu que $\delta\mathcal{H} \subset \mathcal{I}$, on a $\delta\gamma \in \mathcal{I}$. D'où ($\mathcal{I}$ est un idéal)

$$\rho = \alpha - \delta\gamma \in \mathcal{I}.$$

  Mais comme $N(\rho) < N(\delta)$, par minimalité de $N(\delta)$, on a $\rho = 0_{\mathbb{H}}$.
  Ainsi $\alpha = \delta\gamma \in \delta\mathcal{H}$.
  D'où

$$\boxed{\mathcal{I} \subset \delta\mathcal{H}}.$$

---

3 Intermède: somme de puissances modulo p

Dans cette partie on fixe p un nombre premier.
Pour tout $m \in \mathbb{N}$, on note

$$S_m = \sum_{a=0}^{p-1} a^m.$$

3.15. Soit $m \in \mathbb{N}$,
Montrer que

$$\sum_{a=0}^{p-1} \left((a+1)^{m+1} - a^{m+1}\right) \equiv 0\ [p].$$

Par somme télescopique on a ($m+1 > 0$)

$$\sum_{a=0}^{p-1} \left((a+1)^{m+1} - a^{m+1}\right) = ((p-1)+1)^{m+1} - 0^{m+1} = p^{m+1}$$

et donc en particulier

$$\boxed{\sum_{a=0}^{p-1} \left((a+1)^{m+1} - a^{m+1}\right) \equiv 0\ [p]}.$$

3.16. Soit $m \in \mathbb{N}$,
En utilisant la question précédente, montrer que

$$\sum_{\ell=0}^{m} \binom{m+1}{\ell} S_\ell \equiv 0\ [p].$$

En développant par binôme, on a pour tout $a \in [\![0, p-1]\!]$,

$$\begin{aligned}(a+1)^{m+1} - a^{m+1} &= \sum_{\ell=0}^{m+1} \binom{m+1}{\ell} a^\ell - a^{m+1} \\ &= \sum_{\ell=0}^{m} \binom{m+1}{\ell} a^\ell.\end{aligned}$$

Et donc par somme double,

$$\begin{aligned}\sum_{a=0}^{p-1} \left((a+1)^{m+1} - a^{m+1}\right) &= \sum_{a=0}^{p-1} \sum_{\ell=0}^{m} \binom{m+1}{\ell} a^\ell \\ &= \sum_{\ell=0}^{m} \binom{m+1}{\ell} \sum_{a=0}^{p-1} a^\ell. \\ &= \sum_{\ell=0}^{m} \binom{m+1}{\ell} S_\ell.\end{aligned}$$

Or par la question **3.15.**, on a

$$\sum_{a=0}^{p-1} \left((a+1)^{m+1} - a^{m+1}\right) \equiv 0 \ [p]$$

et donc

$$\boxed{\sum_{\ell=0}^{m} \binom{m+1}{\ell} S_\ell \equiv 0 \ [p]}.$$

3.17. En déduire que, pour tout $m \in [\![0, p-2]\!]$,

$$S_m \equiv 0 \ [p].$$

On procède par récurrence forte finie sur $m \in [\![0, p-2]\!]$.

- **Initialisation**
  Pour $m = 0$, on a $S_0 = p$ et donc $S_0 \equiv 0 \ [p]$.
- **Hérédité**
  Soit $m \in [\![1, p-2]\!]$.
  Supposons que pour tout $\ell \in [\![0, m-1]\!]$,
  $$S_\ell \equiv 0 \ [p].$$
  Par la question **3.16.**, on a
  $$\binom{m+1}{m} S_m + \sum_{\ell=0}^{m-1} \binom{m+1}{\ell} S_\ell \equiv 0 \ [p]$$
  c'est à dire par l'hypothèse de récurrence,
  $$\binom{m+1}{m} S_m \equiv 0 \ [p].$$
  Or $\binom{m+1}{m} = m+1$ est premier avec p car $1 \leq m+1 \leq p-1$.
  Par conséquent
  $$S_m \equiv 0 \ [p].$$
- **Conclusion**
  On a montré par récurrence que pour tout $m \in [\![0, p-2]\!]$,
  $$\boxed{S_m \equiv 0 \ [p]}.$$

3.18. Montrer que

$$S_{p-1} \equiv -1 \ [p].$$

Par le petit théorème de Fermat on a

$$\begin{aligned} S_{p-1} &\equiv \sum_{a=0}^{p-1} a^{p-1} \ [p] \\ &\equiv 0^{p-1} + \sum_{a=1}^{p-1} a^{p-1} \ [p] \\ &\equiv 0 + \sum_{a=1}^{p-1} 1 \ [p] \\ &\equiv p-1 \ [p] \\ &\equiv -1 \ [p] \end{aligned}.$$

On a donc bien

$$\boxed{S_{p-1} \equiv (-1) \ [p]}.$$

Remarques:
- On pourrait ensuite à l'aide d'une division euclidienne déterminer S_m modulo p pour tout $m \in \mathbb{N}$.
- Le résultat de cette question n'est pas utilisée dans le reste du sujet. Elle permet juste d'introduire l'idée que $a^{p-1} \equiv \delta_{a\not\equiv 0 \ [p]} \ [p]$ d'après le petit théorème de Fermat, utilisée à la question **3.20.**. (Et permet aussi d'équilibrer le nombre de questions de chaque partie).

3.19. En utilisant la question **3.17.**, montrer que

$$\sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} \left(a^2+b^2+c^2+d^2\right)^{p-1} \equiv 0 \ [p].$$

Indication : ne pas avoir peur de développer l'expression.

Notons pour tout $k_a, k_b, k_c, k_d \in [\![0, p-1]\!]$

$$\binom{p-1}{k_a, k_b, k_c, k_d} \in \mathbb{N}$$

le nombre de partitionner un ensemble de $p-1$ éléments en 4 ensembles de k_a, k_b, k_c et k_d éléments.
Remarque: l'expression explicite, et même l'usage, de $\binom{p-1}{k_a,k_b,k_c,k_d}$ n'est pas nécessaire il s'agit seulement d'une notation pour regrouper efficacement les termes du produit. On remarque qu'en fait $\binom{p-1}{k_a,k_b,k_c,k_d} = \frac{(p-1)!}{k_a!k_b!k_c!k_d!}$, et que par exemple $\binom{n}{k,n-k}$ est le coefficient binomial $\binom{n}{k}$ habituel.
En développant le carré somme quadruple on a,

$$\begin{aligned} &\sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} \left(a^2+b^2+c^2+d^2\right)^{p-1} \\ &= \sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} \sum_{\substack{(k_a,k_b,k_c,k_d)\in[\![0,p-1]\!]^4 \\ k_a+k_b+k_c+k_d=p-1}} \binom{p-1}{k_a,k_b,k_c,k_d} (a^2)^{k_a}(b^2)^{k_b}(c^2)^{k_c}(d^2)^{k_d} \\ &= \sum_{\substack{(k_a,k_b,k_c,k_d)\in[\![0,p-1]\!]^4 \\ k_a+k_b+k_c+k_d=p-1}} \binom{p-1}{k_a,k_b,k_c,k_d} \sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} a^{2k_a}b^{2k_b}c^{2k_c}d^{2k_d} \\ &= \sum_{\substack{(k_a,k_b,k_c,k_d)\in[\![0,p-1]\!]^4 \\ k_a+k_b+k_c+k_d=p-1}} \binom{p-1}{k_a,k_b,k_c,k_d} \left(\sum_{a=0}^{p-1} a^{2k_a}\right)\left(\sum_{b=0}^{p-1} b^{2k_b}\right)\left(\sum_{c=0}^{p-1} c^{2k_c}\right)\left(\sum_{d=0}^{p-1} d^{2k_d}\right). \end{aligned}$$

Montrons désormais que tous les termes de la somme intérieure sont congrus à 0 modulo p.
Soit $(k_a, k_b, k_c, k_d) \in [\![0, p-1]\!]^4$ tel que $k_a + k_b + k_c + k_d = p-1$.
En particulier $k_a \leq \frac{p-1}{4}$ ou $k_b \leq \frac{p-1}{4}$ ou $k_c \leq \frac{p-1}{4}$ ou $k_d \leq \frac{p-1}{4}$.
D'où parmi les puissances $2k_a$, $2k_b$, $2k_c$ et $2k_d$, il y en a au moins une qui est inférieure à $\frac{p-1}{2}$ et donc inférieure à $p-2$.
Quitte à permuter les termes on peut supposer que

$$2k_a \leq p-2.$$

Alors par la question **3.17.**, on a

$$\sum_{a=0}^{p-1} a^{2k_a} \equiv 0\ [p]. \quad .$$

Par conséquent, pour tout $(k_a, k_b, k_c, k_d) \in [\![0, p-1]\!]^4$ on a

$$\left(\sum_{a=0}^{p-1} a^{2k_a}\right)\left(\sum_{b=0}^{p-1} b^{2k_b}\right)\left(\sum_{c=0}^{p-1} c^{2k_c}\right)\left(\sum_{d=0}^{p-1} d^{2k_d}\right) \equiv 0\ [p]$$

et donc

$$\boxed{\sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} \left(a^2+b^2+c^2+d^2\right)^{p-1} \equiv 0\ [p]}.$$

3.20. Conclure de la question **3.19.** qu'il existe $(a, b, c, d) \in [\![0, p-1]\!]^4$ tels que

$$a^2 + b^2 + c^2 + d^2 \equiv 0\ [p]$$

et vérifiant de plus

$$a \not\equiv 0\ [p].$$

Soit $A \in \mathbb{Z}$.
Par le petit théorème de Fermat,

$$A^{p-1} \equiv \delta_{A\not\equiv 0\ [p]}\ [p]$$

c'est à dire $A^{p-1} \equiv 1\ [p]$ si $A \not\equiv 0\ [p]$ et $A^{p-1} \equiv 0\ [p]$ si $A \equiv 0\ [p]$.
Par conséquent

$$\begin{aligned}\sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} \left(a^2+b^2+c^2+d^2\right)^{p-1} &\equiv \sum_{(a,b,c,d)\in[\![0,p-1]\!]^4} \delta_{(a^2+b^2+c^2+d^2)\not\equiv 0\ [p]}\ [p] \\ &\equiv \operatorname{card}\left(\left\{(a,b,c,d)\in[\![0,p-1]\!]^4 \mid a^2+b^2+c^2+d^2 \not\equiv 0\ [p]\right\}\right)\ [p]\end{aligned}.$$

Notons

$$M = \operatorname{card}\left(\left\{(a,b,c,d)\in[\![0,p-1]\!]^4 \mid a^2+b^2+c^2+d^2 \equiv 0\ [p]\right\}\right)$$

le nombre de solutions modulo p de l'équation $a^2 + b^2 + c^2 + d^2 \equiv 0\ [p]$.
La congruence précédente montre que

$$p \mid p^4 - M$$

et donc

$$p \mid M.$$

De plus

$$0^2 + 0^2 + 0^2 + 0^2 \equiv 0\ [p]$$

et donc

$$M \geq 1.$$

On a donc $M \geq p$ et donc $M \geq 2$.
En particulier

$$\exists (a,b,c,d) \in [\![0,p-1]\!]^4 \backslash \{(0,0,0,0)\},\ a^2+b^2+c^2+d^2 \equiv 0\ [p]$$

et étant donné une telle solution, quitte à permuter a, b, c, d, comme ils ne sont pas tous nuls modulo p on peut supposer a non nul modulo p.
Par conséquent $\boxed{\text{il existe } (a,b,c,d) \in [\![0,p-1]\!]^4}$ tels que $\boxed{a \not\equiv 0\ [p]}$ et $\boxed{a^2+b^2+c^2+d^2 \equiv 0\ [p]}$.

---

4 Conclusion: théorème des quatre carrés

On note

$$\mathfrak{C}_4 = \left\{n \in \mathbb{N} \mid \exists (a,b,c,d) \in \mathbb{Z}^4,\ n = a^2+b^2+c^2+d^2\right\}$$

l'ensemble des entiers naturels qui s'écrivent comme somme de quatre carrés.

4.21. Montrer que

$$\mathfrak{C}_4 = \{N(h),\ h \in \mathbb{H}_\mathbb{Z}\}\,.$$

On procède par double inclusion.
- $\boxed{\subset}$ Soit $n \in \mathfrak{C}_4$.
  Soit $(a,b,c,d) \in \mathbb{Z}^4$ tel que $n = a^2+b^2+c^2+d^2$.
  En posant
  $$h = a1_\mathbb{H} + bi + cj + dk \in \mathbb{H}_Z,$$
  on a alors $N(h) = a^2+b^2+c^2+d^2 = n$.
  D'où $n \in \{N(h),\ h \in \mathbb{H}_\mathbb{Z}\}$.
- $\boxed{\supset}$ Soit $h \in \mathbb{H}_\mathbb{Z}$.
  Soient $a,b,c,d \in \mathbb{Z}$ tels que $h = a1_\mathbb{H} + bi + cj + dk$.
  Par la question **1.4.** on a alors $N(h) = a^2+b^2+c^2+d^2 \in \mathfrak{C}_4$.

Par conséquent on a bien

$$\boxed{\mathfrak{C}_4 = \{N(h),\ h \in \mathbb{H}_\mathbb{Z}\}}.$$

4.22. En déduire que $\mathfrak{C}_4$ est stable par produit.

Soient $n_1, n_2 \in \mathfrak{C}_4$.
Par la question **4.21.** il existe alors $h_1, h_2 \in \mathbb{H}_\mathbb{Z}$ tels que $n_1 = N(h_1)$ et $n_2 = N(h_2)$.
D'où par la question **1.5.**

$$n_1 n_2 = N(h_1)N(h_2) = N(h_1h_2).$$

Or comme $\mathbb{H}_\mathbb{Z}$ est stable par produit, on a $h_1h_2 \in \mathbb{H}_\mathbb{Z}$.
Et donc par l'autre sens de la question **4.21.**, on a $n_1n_2 \in \mathfrak{C}_4$.
Ainsi $\boxed{\mathfrak{C}_4 \text{ est stable par produit}}$.

4.23. Soit $\eta \in \mathcal{H}$.
Montrer que

$$\eta^\top + \eta = \frac{1}{2}\operatorname{tr}(\eta)1_\mathbb{H} \in \mathbb{Z}1_\mathbb{H}$$

où $\mathbb{Z}1_\mathbb{H} = \{a1_\mathbb{H},\ a \in \mathbb{Z}\}$.

Soient $a,b,c,d,k \in \mathbb{Z}$ tels que

$$\begin{aligned}\eta &= a1_\mathbb{H} + bi + cj + dk + k\xi \\ &= \left(a+\frac{k}{2}\right)1_\mathbb{H} + \left(b+\frac{k}{2}\right)i + \left(c+\frac{k}{2}\right)j + \left(d+\frac{k}{2}\right)k.\end{aligned}$$

Comme $1_\mathbb{H}^\top = 1_\mathbb{H}$, $i^\top = -i$, $j^\top = -j$, $k^\top = -k$ et $\xi^\top = 1_\mathbb{H} - \xi$, on a alors

$$\eta^\top + \eta = 2\left(a+\frac{k}{2}\right)1_\mathbb{H} + 0i + 0j + 0k$$

et de plus comme $\operatorname{tr}(1_\mathbb{H}) = 4$, $\operatorname{tr}(i) = \operatorname{tr}(j) = \operatorname{tr}(k) = 0$ on a aussi

$$\operatorname{tr}(\eta) = 4\left(a+\frac{k}{2}\right).$$

Ainsi

$$\boxed{\eta^\top + \eta = \frac{1}{2}\operatorname{tr}(\eta)1_\mathbb{H}}$$

et comme $2a+k \in \mathbb{Z}$ on a aussi

$$\boxed{\frac{1}{2}\operatorname{tr}(\eta) \in \mathbb{Z}}.$$

Dans les questions **4.24.** à **4.28.**, on fixe p un **nombre premier impair**.
De la question **3.20.**, on fixe $(a,b,c,d) \in [\![0, p-1]\!]^4$ tels que $a^2+b^2+c^2+d^2 \equiv 0\ [p]$ et $a \not\equiv 0\ [p]$.

On pose alors

$$\alpha = a1_{\mathbb{H}} + bi + cj + dk \in \mathcal{H}.$$

On remarque alors (il n'est pas demandé de le démontrer) que

$$p\mathcal{H} + \alpha\mathcal{H} = \left\{p\lambda + \alpha\mu,\ (\lambda,\mu) \in \mathcal{H}^2\right\}$$

est un idéal à droite de $\mathcal{H}$.
Par la question **2.14.**, il existe donc $\delta \in \mathcal{H}$ tel que

$$p\mathcal{H} + \alpha\mathcal{H} = \delta\mathcal{H}.$$

On fixe dans la suite un tel δ.

On a envie de noter δ le **pgcd** (à droite) de p et α dans $\mathcal{H}$.

4.24. Montrer qu'il existe $\lambda, \mu \in \mathcal{H}$ tels que

$$p\lambda + \alpha\mu = N(\delta)1_{\mathbb{H}}.$$

Par définition de δ il existe (comme $\delta = 1_{\mathbb{H}}\delta \in \mathcal{H}\delta$) $\widetilde{\lambda}, \widetilde{\mu} \in \mathcal{H}$ tels que

$$\delta = p\widetilde{\lambda} + \alpha\widetilde{\mu}.$$

Par conséquent, en multipliant à droite par $\delta^\top$,

$$\delta\delta^\top = p\widetilde{\lambda}\delta^\top + \alpha\widetilde{\mu}\delta^\top.$$

En posant

$$\begin{cases} \lambda = \widetilde{\lambda}\delta^\top \\ \mu = \widetilde{\mu}\delta^\top \end{cases}$$

on a alors (par définition de $N(\delta)$),

$$\boxed{N(\delta)1_{\mathbb{H}} = p\lambda + \alpha\mu}.$$

4.25. En déduire que

$$p \mid N(\delta)^2.$$

Soient $\lambda, \mu \in \mathcal{H}$ tels qu'à la question **4.24.**.
On a alors

$$\alpha\mu = N(\delta)1_{\mathbb{H}} - p\lambda.$$

Par conséquent, en passant à la norme N,

$$N(\alpha\mu) = N\left(N(\delta)1_{\mathbb{H}} - p\lambda\right).$$

Or par définition, en prenant garde à la non commutativité du produit, tout en constatant que $p \in \mathbb{R}$ pseudo-commute avec tout élément et $1_{\mathbb{H}}$ commute avec tout élément,

$$\begin{aligned}(N(\delta)1_{\mathbb{H}} - p\lambda)^\top (N(\delta)1_{\mathbb{H}} - p\lambda) &= \left(N(\delta)1_{\mathbb{H}} - p\lambda^\top\right)(N(\delta)1_{\mathbb{H}} - p\lambda) \\ &= N(\delta)^2 1_{\mathbb{H}} - p\lambda^\top N(\delta) - pN(\delta)\lambda + p^2\lambda^\top\lambda \\ &= N(\delta)^2 1_{\mathbb{H}} - pN(\delta)(\lambda^\top + \lambda) + p^2 N(\lambda)1_{\mathbb{H}}.\end{aligned}$$

Or par la question **4.23.**, il existe $r \in \mathbb{Z}$ tel que $\lambda^\top + \lambda = r1_{\mathbb{H}}$.
On a donc

$$(N(\delta)1_{\mathbb{H}} - p\lambda)^\top (N(\delta)1_{\mathbb{H}} - p\lambda) = \left(N(\delta)^2 - pN(\delta)r + p^2N(\lambda)\right)1_{\mathbb{H}}$$

c'est à dire

$$N\left(N(\delta)1_{\mathbb{H}} - p\lambda\right) = N(\delta)^2 - pN(\delta)r + p^2N(\lambda).$$

En particulier

$$N\left(N(\delta)1_{\mathbb{H}} - p\lambda\right) \equiv N(\delta)^2\ [p].$$

Or

$$\begin{aligned} N(\mu\alpha) &= N(\mu)N(\alpha) \\ &= N(\mu)(a^2+b^2+c^2+d^2) \end{aligned}$$

et par définition de α,

$$a^2+b^2+c^2+d^2 \equiv 0\ [p].$$

Par conséquent on a bien

$$\boxed{N(\delta)^2 \equiv 0\ [p]}.$$

4.26. On suppose dans cette question que $N(\delta) = p^2$.
Montrer qu'il existe $\eta \in \mathcal{H}$ tel que

$$\alpha = p\eta.$$

Par définition de δ on a

$$p1_{\mathbb{H}} \in \delta\mathcal{H}$$

et par conséquent il existe $\lambda \in \mathcal{H}$ tel que

$$p1_{\mathbb{H}} = \delta\lambda.$$

En passant à la norme N, on a alors

$$N(p1_{\mathbb{H}}) = N(\delta\lambda)$$

c'est à dire

$$p^2 = N(\delta)N(\lambda).$$

Or on a supposé que $N(\delta) = p^2$ et donc (p^2 simplifiable dans $\mathbb{Z}$),

$$1 = N(\lambda).$$

Par la question **2.11.**, on a donc λ inversible.(dans $\mathcal{H}$)
Par conséquent en multipliant à droite par $\lambda^{-1} \in \mathcal{H}$, on a

$$p\lambda^{-1} = \delta.$$

Mais, toujours par définition de δ,

$$\alpha \in \delta\mathcal{H}$$

et par conséquent il existe $\mu \in \mathcal{H}$ tel que

$$\alpha = \delta\mu.$$

Par conséquent

$$\alpha = p\lambda^{-1}\mu$$

et en posant

$$\eta = \lambda^{-1}\mu$$

on a bien (par stabilité par produit de $\mathcal{H}$), $\boxed{\eta \in \mathcal{H}}$ et

$$\boxed{\alpha = p\eta}.$$

4.27. À l'aide des questions **4.26.** et **4.23.**, montrer que

$$N(\delta) \neq p^2.$$

Supposons par l'absurde que $N(\delta) = p^2$.
Par la question **4.26.**, il existe alors $\eta \in \mathcal{H}$ tel que $\alpha = p\eta$.
En particulier

$$\mathrm{tr}(\alpha) = \mathrm{tr}(p\eta) = p\,\mathrm{tr}(\eta).$$

Or on a (cf question **4.23.**),

$$\mathrm{tr}(\alpha) = 4a$$

et

$$\mathrm{tr}(\eta) \in 2\mathbb{Z}.$$

En particulier on en déduit donc que

$$2a \equiv 0\ [p]$$

ce qui est absurde car par définition de a on a

$$a \not\equiv 0\ [p]$$

et p est premier impair.
Ainsi

$$\boxed{N(\delta) \neq p^2}.$$

4.28. À l'aide des questions précédentes, conclure que

$$N(\delta) = p.$$

On a
- Par la question **4.25.**,
$$p \mid N(\delta).$$
- Par la question **4.27.**,
$$N(\delta) \neq p^2$$
car sinon $2a \equiv 0\ [p]$, ce qui est absurde par définition de a ($a \not\equiv 0\ [p]$) et p premier impair.
- Comme $p1_{\mathbb{H}} \in \delta\mathcal{H}$, il existe $\lambda \in \mathcal{H}$ tel que $p1_{\mathbb{H}} = \delta\lambda$. D'où $p^2 = N(\delta)N(\lambda)$ et donc
$$N(\delta) \mid p^2.$$

Et par conséquent

$$\boxed{N(\delta) = p}.$$

4.29. Soit $\beta \in \mathcal{H}$.
Montrer qu'il existe $\varepsilon \in \mathcal{H}^\times$ et $h \in \mathbb{H}_\mathbb{Z}$ tels que

$$\beta = \varepsilon h.$$

Remarquons tout d'abord que

$$2\mathcal{H} \subset \mathbb{H}_\mathbb{Z}.$$

Supposons temporairement qu'il existe $\gamma \in \mathcal{H}$ et $\rho \in \mathcal{H}$ tels que

$$\beta = 2\gamma + \rho$$

et

$$N(\rho) \leq 1.$$

Alors
- Si $N(\rho) = 0$, alors $\rho = 0$ d'où $\beta \in \mathbb{H}_\mathbb{Z}$, et par conséquent $\varepsilon = 1$ et $h = \beta$ conviennent.
- Si $N(\rho) = 1$, alors ρ est inversible d'où $\beta = \rho(2\rho^{-1}\gamma + 1_{\mathbb{H}})$ et donc $\varepsilon = \rho$ et $h = 2\rho^{-1}\gamma + 1_{\mathbb{H}}$ conviennent.

et dans tous les cas on a bien la décomposition voulue.
Il ne reste plus qu'à montrer le résultat présupposé.
Soient $a, b, c, d, k \in \mathbb{Z}$ tels que $\beta = a1_{\mathbb{H}} + bi + cj + dk + k\xi$.
Si k est pair, alors $\beta \in \mathbb{H}_\mathbb{Z}$ et il n'y a rien à faire.
Si k est impair, alors quitte à effectuer une division euclidienne par 2, on peut supposer $k = 1$.
Alors

$$\beta = \frac{2a+1}{2}1_{\mathbb{H}} + \frac{2b+1}{2}i + \frac{2c+1}{2}j + \frac{2d+1}{2}k.$$

En posant

$$\gamma = \left[\frac{2a+1}{4}\right] 1_{\mathbb{H}} + \left[\frac{2b+1}{4}\right] i + \left[\frac{2c+1}{4}\right] j + \left[\frac{2d+1}{4}\right] k \in \mathbb{H}_{\mathbb{Z}}$$

on a

$$\gamma \in \mathbb{H}_{\mathbb{Z}} \subset \mathcal{H}$$

et $\beta - 2\gamma \in \mathcal{H}$ (comme $\mathcal{H}$ est un groupe) de la forme

$$\left(\pm\frac{1}{2}\right) 1_{\mathbb{H}} + \left(\pm\frac{1}{2}\right) i + \left(\pm\frac{1}{2}\right) j + \left(\pm\frac{1}{2}\right) k$$

(en effet chaque coordonnée de $\beta - 2\gamma$ s'écrit $2\left(\frac{2x+1}{4} - \left[\frac{2x+1}{4}\right]\right)$ avec $x \in \{a, b, c, d\}$, et $\frac{2x+1}{4}$ est à distance exactement $\frac{1}{4}$ de l'entier le plus proche, l'entier $2x+1$ étant impair)
et en particulier

$$N(\beta - 2\gamma) = \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1.$$

En conclusion, on a bien

$$\boxed{\exists (\varepsilon, h) \in \mathcal{H}^\times \times \mathbb{H}_{\mathbb{Z}},\ \beta = \varepsilon h}.$$

4.30. Conclure que

$$\mathfrak{C}_4 = \mathbb{N}$$

c'est-à-dire que $\boxed{\text{tout entier naturel s'écrit comme la somme de quatre carrés}}$.

Par la question **4.22.**, l'ensemble $\mathfrak{C}_4$ est stable par produit.
Il suffit donc de montrer qu'il contient tous les nombres premiers pour montrer qu'il contient tous les entiers (par existence de la Décomposition en produit de Facteurs Premiers).
Tout d'abord (à ne pas oublier)

$$2 = 1^2 + 1^2 + 0^2 + 0^2 \in \mathfrak{C}_4.$$

Soit désormais p un nombre premier impair.
Par la question **4.28.**, il existe $\delta \in \mathcal{H}$ tel que $N(\delta) = p$.
De plus par la question **4.29.**, il existe $\varepsilon \in \mathcal{H}^\times$ et $h \in \mathbb{H}_{\mathbb{Z}}$ tels que $\delta = \varepsilon h$.
En particulier $N(\delta) = N(\varepsilon)N(h)$ et donc $N(h) = p$.
D'où par la question **4.21.** on a $p \in \mathfrak{C}_4$.
Par conséquent on a bien

$$\boxed{\mathfrak{C}_4 = \mathbb{N}}.$$