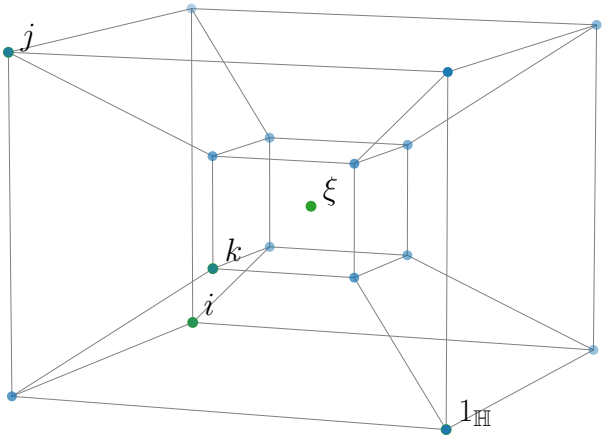
Quaternions et théorème des quatre carrés

On portera une attention particulière à **la rédaction** et à **la propreté** de la copie.
En particulier tout **graphe ou schéma** pertinent et correctement annoté sera **valorisé**.
Les résultats devront être mis en valeur dès que possible.

Indiquez sur votre copie le temps approximatif pris pour le devoir.

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 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 $\mathrm{M}_4(\mathbb{R})$.

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

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

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.

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 $z_1, z_2 \in \mathbb{H}$,
$$N(z_1 z_2) = N(z_1)N(z_2).$$

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

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

---

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

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

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

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

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

2.10. En déduire que

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

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 $\mathcal{H}$.

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.

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

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

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

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

---

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

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

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

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

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

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

3.18. Montrer que

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

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.

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

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

---

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

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

4.22. En déduire que $\mathfrak{C}_4$ 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 $\mathbb{Z}1_\mathbb{H} = \{a1_\mathbb{H},\ a \in \mathbb{Z}\}$.

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.

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

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

4.25. En déduire que

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

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

$$\alpha = p\eta.$$

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

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

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

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

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

$$\beta = \varepsilon h.$$

4.30. Conclure que

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

c'est-à-dire que tout entier naturel s'écrit comme la somme de quatre carrés.