LE CORPS DES QUATERNIONS - TH. DE LAGRANGE

*On doit à **Hamilton**, mathématicien irlandais du 19ème s., la théorie des **quaternions**.*

Soit $\mathbb{H} = \mathbb{C} \times \mathbb{C}$. On définit dans $\mathbb{H}$ les lois $+$ et $\times$ par :

$$\forall (z_1,z_2) \in \mathbb{H} \quad \forall (z'_1,z'_2) \in \mathbb{H} \quad \begin{cases} (z_1,z_2) + (z'_1,z'_2) &= (z_1 + z'_1 \ \ ,z_2 + z'_2) \\ (z_1,z_2) \times (z'_1,z'_2) &= (z_1z'_1 - z_2\overline{z'_2} \ , \ z_1z'_2 + z_2\overline{z'_1}) \end{cases}$$

Les éléments de $\mathbb{H}$ s'appellent les quaternions.

PARTIE A :

1°) Montrer que $(\mathbb{H}, +, \times)$ est un anneau non commutatif.

2°) Soit $\phi : \mathbb{R} \longrightarrow \mathbb{H}$ définie par : $\forall x \in \mathbb{R}$, $\phi(x) = (x,0)$.

a) Montrer que ϕ est un morphisme injectif d'anneaux.
Ce morphisme permet donc d'identifier tout réel x à son image $\phi(x)$; on notera alors, pour tout x réel : $(x,0) = x$. Un quaternion de la forme $(x,0)$ avec x réel sera dit réel.

b) Montrer que : $\forall x \in \mathbb{R}$, $\forall q \in \mathbb{H}$, $qx = xq$ (*attention : compte tenu de la remarque précédente, il faut comprendre $(x,0) \times q$ pour xq etc...*).

c) On pose : $e_0 = (1,0)$ (soit $e_0 = 1$), $e_1 = (i,0)$, $e_2 = (0,1)$, et $e_3 = (0,i)$.
Démontrer que, pour tout $q \in \mathbb{H}$, il existe un et un seul quadruplet $(x_0,x_1,x_2,x_3) \in \mathbb{R}^4$ tel que $q = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$. A quelle condition sur (x_0,x_1,x_2,x_3) ce quaternion est-il réel ?
On dira que q est un quaternion pur si $x_0 = 0$. On note $\mathbb{P}$ l'ensemble des quaternions purs.

d) Calculer les produits e_ie_j pour $i,j \in \{0,1,2,3\}$ (on présentera les résultats sous forme d'un tableau).
En déduire, pour $x_0,x_1,x_2,x_3,y_0,y_1,y_2,y_3$ réels, une expression du produit $(x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3) \times (y_0e_0 + y_1e_1 + y_2e_2 + y_3e_3)$.

e) Démontrer que les seuls quaternions qui commutent avec tous les autres sont les réels.

3°) Pour λ réel et $q = (z_1,z_2) \in \mathbb{H}$, on pose $\lambda.q = (\lambda z_1, \lambda z_2)$. Comparer $\lambda.q$ et λq ; en déduire que $(\mathbb{H}, +, \times, .)$ est une $\mathbb{R}$-algèbre.
Quelle est la dimension du $\mathbb{R}$-espace vectoriel $(\mathbb{H}, +, .)$?

4°) Pour tout quaternion $q = x_0e_0 + x_1e_1 + x_2e_2 + x_3e_3$ $(x_i \in \mathbb{R})$, on appelle conjugué de q le quaternion $\overline{q} = x_0e_0 - x_1e_1 - x_2e_2 - x_3e_3$, et norme de q le quaternion $N(q) = q\overline{q}$.

a) Vérifier que, pour tout $q \in \mathbb{H}$, $q + \overline{q} \in \mathbb{R}$ et $q - \overline{q} \in \mathbb{P}$.

b) Montrer que l'application $q \longmapsto \overline{q}$ est un automorphisme du $\mathbb{R}$-espace vectoriel $(\mathbb{H}, +, .)$.

c) Montrer que : $\forall (q,q') \in \mathbb{H}^2 \quad \overline{qq'} = \overline{q'}\,\overline{q}$.

d) Montrer que, pour tout $q \in \mathbb{H}$, $N(q)$ est un réel positif, et que $N(q)=0$ si et seulement si $q = 0$.

e) Montrer que $\forall (q,q') \in \mathbb{H}^2 \quad N(qq') = N(q'q) = N(q)N(q')$.

f) Démontrer que, si $q \in \mathbb{H}$ et $q \neq 0$, alors q est inversible, et exprimer son inverse en fonction de $N(q)$ et de $\overline{q}$.
Que peut-on en conclure pour la structure de $(\mathbb{H}, +, \times)$?

5°) **a)** Montrer que, pour tout $q \in \mathbb{H}$: $q \in \mathbb{R} \ \Leftrightarrow \ q = \overline{q}$ et que : $q \in \mathbb{P} \ \Leftrightarrow q = -\overline{q}$.

b) Montrer que, pour tout $q \in \mathbb{H}$: $q \in \mathbb{R} \ \Leftrightarrow \ q^2 \in \mathbb{R}_+$.

c) Montrer que, pour tout $q \in \mathbb{H}\setminus\mathbb{R}$, $a = q+\overline{q}$ et $b = q\overline{q}$ sont les seuls réels tels que $q^2-aq+b=0$ (*on pourra montrer que, a et b étant réels, si* $a \neq q+\overline{q}$ *et si* $q^2-aq+b=0$, *alors* $q \in \mathbb{R}$).
En déduire, pour tout $q \in \mathbb{H}$: $q \in \mathbb{P} \Leftrightarrow q^2 \in \mathbb{R}_-$.

PARTIE B :

Le but de cette partie est de caractériser les automorphismes du corps $(\mathbb{H}, +, \times)$. On notera $\mathrm{Aut}(\mathbb{H})$ l'ensemble de ces automorphismes.

1°) Montrer que $\mathrm{Aut}(\mathbb{H},\mathbf{o})$ est un groupe.

2°) Soit $\sigma \in \mathrm{Aut}(\mathbb{H})$.

a) Montrer que : $\forall r \in \mathbb{Q}$, $\sigma(r) = r$.

b) En utilisant A.2.e, montrer que $\sigma(\mathbb{R}) \subset \mathbb{R}$.

c) Montrer que $\sigma(\mathbb{R}_+) \subset \mathbb{R}_+$, et en déduire que la restriction de σ à $\mathbb{R}$ est une application croissante de $\mathbb{R}$ dans $\mathbb{R}$.

d) Montrer que : $\forall x \in \mathbb{R}$, $\sigma(x) = x$ (*utiliser des approximations de x par des rationnels*).

e) En utilisant A.5.c, montrer que : $\sigma(\mathbb{P}) \subset \mathbb{P}$.

f) Montrer que, pour tout $q \in \mathbb{H}$, $\sigma(q)+\sigma(\overline{q}) \in \mathbb{R}$ et que $\sigma(q)-\sigma(\overline{q}) \in \mathbb{P}$.

En déduire que : $\sigma(\overline{q}) = \overline{\sigma(q)}$, puis que $N(\sigma(q)) = N(q)$.

3°) Pour tout $a \in \mathbb{H}$, $a \neq 0$, on définit $\phi_a : \mathbb{H} \longrightarrow \mathbb{H}$ par : $\phi_a(q) = aqa^{-1}$.

a) Montrer que, pour tout $a \in \mathbb{H}$, $a \neq 0$, ϕ_a est élément de $\mathrm{Aut}(\mathbb{H})$.

b) Montrer que l'application $\Phi : \begin{cases} (\mathbb{H}\setminus\{0\},\times) & \longrightarrow & (\mathrm{Aut}(\mathbb{H}),\mathbf{o}) \\ a & \longmapsto & \phi_a \end{cases}$
est un morphisme de groupes. Quel est son noyau ?

On se propose, dans la fin de cette partie, de montrer que Φ *est surjectif, c'est-à-dire que tous les automorphismes du corps* $\mathbb{H}$ *sont de la forme* ϕ_a. *Pour cela, considérons un automorphisme* σ *de* $(\mathbb{H}, +, \times)$

4°) On va montrer, dans cette question, qu'il existe $a \in \mathbb{H}\setminus\{0\}$ tel que $\phi_a \mathbf{o} \sigma(e_1) = e_1$.

a) Montrer que $(\sigma(e_1))^2 = -1$.

b) Montrer que $(\sigma(e_1)e_1 - 1)e_1 = \sigma(e_1)(\sigma(e_1)e_1 - 1)$.
En déduire un élément a qui répond à la question dans le cas où $\sigma(e_1)e_1 \neq 1$.

c) Si $\sigma(e_1)e_1 = 1$, montrer que $\sigma(e_1) = -e_1$, et déterminer un élément a qui répond à la question.

5°) Soi $\sigma' = \phi_a \mathbf{o} \sigma$. On se propose de montrer qu'il existe $b \in \mathbb{H}\setminus\{0\}$ tel que $\phi_b \mathbf{o} \sigma'(e_1) = e_1$ et $\phi_b \mathbf{o} \sigma'(e_2) = e_2$.

a) Montrer que $(\sigma'(e_2)e_2 - 1)e_1 = \sigma'(e_1)(\sigma'(e_2)e_2 - 1)$ (remarquer que $\sigma'(e_1) = e_1$).
En déduire un élément b qui convient dans le cas où $\sigma'(e_2)e_2 \neq 1$.

b) Si $\sigma'(e_2)e_2 = 1$, montrer que l'on peut prendre $b = e_1$.

6°) Soit $\sigma" = \phi_b \mathbf{o} \phi_a \mathbf{o} \sigma$.

a) Montrer que $\sigma"(e_3) = e_3$.

b) En déduire que $\sigma" = \mathrm{Id}_{\mathbb{H}}$, et conclure.

PARTIE C :

Le but de cette partie est de donner une interprétation géométrique des quaternions. Pour cela, on notera $\mathcal{E}$ un espace vectoriel euclidien de dimension 3, rapporté à une base orthonormale directe

$(\vec{i},\vec{j},\vec{k})$. On rappelle que, si deux vecteurs $\vec{U}$ et $\vec{V}$ ont respectivement pour coordonnées (x_1,x_2,x_3) et (y_1,y_2,y_3) dans cette base, le produit scalaire $\vec{U}.\vec{V}$ est le réel $x_1y_1+x_2y_2+x_3y_3$, et le produit vectoriel $\vec{U}\wedge\vec{V}$ est le vecteur de coordonnées $(x_2y_3-x_3y_2,x_3y_1-x_1y_3,x_1y_2-x_2y_1)$.

A tout quaternion $q=x_0e_0+x_1e_1+x_2e_2+x_3e_3$ (x_i réels), on associe le couple $\Psi(q)=(x_0,\vec{U})$ de $\mathbb{R}\times\mathcal{E}$, où $\vec{U}$ est le vecteur de coordonnées (x_1,x_2,x_3).

1°) Vérifier que Ψ est un isomorphisme du $\mathbb{R}$-espace vectoriel $\mathbb{H}$ dans le $\mathbb{R}$-espace vectoriel $\mathbb{R}\times\mathcal{E}$.

2°) Soient q et q' deux quaternions. On pose $\Psi(q)=(x_0,\vec{U})$ et $\Psi(q')=(y_0,\vec{V})$.

a) Vérifier que : $\Psi(qq')=(x_0y_0-\vec{U}.\vec{V},x_0\vec{V}+y_0\vec{U}+\vec{U}\wedge\vec{V})$.

b) Retrouver ainsi la formule du double produit vectoriel :

$$\forall(\vec{U},\vec{V},\vec{W})\in\mathcal{E}^3\ ,\ (\vec{U}\wedge\vec{V})\wedge\vec{W}=(\vec{U}.\vec{W})\vec{V}-(\vec{V}.\vec{W})\vec{U}$$

3°) Donner une condition nécessaire et suffisant portant sur $\Psi(q)$ pour que q soit un quaternion pur. Comment interpréter $N(q)$ dans ce cas ?

4°) On suppose ici que q et q' qu'elle sont deux quaternions purs.
Démontrer que les vecteurs $\vec{U}$ et $\vec{V}$ associés à q et q' sont orthogonaux si et seulement si : $qq'=-q'q$.

PARTIE C :

Le but de cette partie est de démontrer le théorème de Lagrange : *Tout entier positif est somme de quatre carrés (dont certains peuvent être nuls).*

1°) **a)** Démontrer que l'ensemble $\mathbb{H}(\mathbb{Q})$ des quaternions de la forme $q=x_0e_0+x_1e_1+x_2e_2+x_3e_3$ avec x_0,x_1,x_2,x_3 dans $\mathbb{Q}$ est un sous-corps de $\mathbb{H}$.

b) Démontrer que l'ensemble $\mathbb{H}(\mathbb{Z})$ des quaternions de la forme $q=x_0e_0+x_1e_1+x_2e_2+x_3e_3$ avec x_0,x_1,x_2,x_3 dans $\mathbb{Z}$ est un sous-anneau de $\mathbb{H}$.

c) Déduire alors de A.4.e que tout produit de somme de quatre carrés d'entiers est somme de quatre carrés d'entiers.

2°) **a)** Soit W l'ensemble des quaternions $q=x_0e_0+x_1e_1+x_2e_2+x_3e_3$ avec $(x_0,x_1,x_2,x_3)\in\mathbb{Z}^4$ ou $(x_0,x_1,x_2,x_3)\in(\frac{1}{2}+\mathbb{Z})^4$.
Démontrer que W est un sous-anneau de $\mathbb{H}$ (*appelé anneau des quaternions d'Hurwitz*).

b) Vérifier que, si $q\in W$, alors $\overline{q}\in W$, $q+\overline{q}\in\mathbb{Z}$, et $N(q)\in\mathbb{Z}$.

c) Démontrer que $q\in W$ est inversible dans W si et seulement si $N(q)=1$.

d) Démontrer que, pour tout quaternion $q\in\mathbb{H}(\mathbb{Q})$ il existe un quaternion $a\in W$ tel que $N(q-a)<1$. En déduire que, pour tous quaternions $a\in W$ et $q\in W$, il existe deux couples (b,r) et (b',r') de quaternions de W (non nécessairement uniques!) tels que :

$$a=bq+r\quad,\quad a=qb'=r'\quad,\text{ avec } N(r)<N(q)\text{ et }N(r')<N(q')$$

e) Soit I un idéal à droite (resp. à gauche) de W. Démontrer que I est principal.

3°) Soit p un nombre premier impair.

a) Dans le corps Z/pZ, on considère la relation binaire $\mathcal{R}$ définie par : $x\mathcal{R}y \iff y^2 = x^2$. Démontrer qu'il s'agit d'une relation d'équivalence. Quelle est la classe d'équivalence d'un élément x? En déduire que le nombre de carrés dans Z/pZ est égal à $\dfrac{p+1}{2}$.

b) En déduire qu'il existe a et b éléments de $\mathbb{Z}$ tels que $a^2 + b^2 + 1$ soit divisible par p.

c) Soient a et b déterminés comme ci-dessus. Soit alors I l'idéal à gauche de W engendré par p et $1 + ae_1 + be_2$ ($I = Wp + W(1 + ae_1 + be_2)$).
Démontrer que I est distinct de W et de Wp. En déduire qu'il existe q, non inversible dans W, tel que $I = Wq$.
Montrer ensuite qu'il existe $q' \in W$, non inversible dans W, tel que $p = q'q$. En déduire $N(q) = p$.

d) En déduire qu'il existe un élément $q'' \in \mathbb{H}(\mathbb{Z})$ tel que $N(q'') = p$.

4°) Conclure.
