

T.I.P.E. : Nos amis les Quaternions

Clément Canonne

23 juin 2007

Table des matières

I	Introduction	3
II	Construction du corps des quaternions \mathbb{H} et premières propriétés	3
1	Construction	3
2	Norme, conjugaison	5
III	Théorème de Frobenius	7
1	Extension d'un sous-corps	7
2	Théorème de Frobenius	7
IV	Applications	9
1	Curiosité : les fractales	9
2	Traitement informatique des images	9
3	Informatique et programmation 3D	9

I Introduction

Si l'on sait que Gauss et même Euler connaissaient les lois de multiplication des quaternions, c'est à William Rowan Hamilton que l'on doit la découverte, en 1843, du corps \mathbb{H} et les premiers résultats s'appliquant à ses éléments. Après avoir tenté - en vain - d'obtenir un surcorps aux complexes qui soit une \mathbb{R} -algèbre de dimension 3 (afin de généraliser les propriétés géométriques des complexes dans l'espace à trois dimensions), on raconte que c'est au cours d'une promenade avec son épouse le long du canal royal, à Dublin, que le mathématicien eut l'idée de la relation fondamentale du corps des quaternions, à savoir

$$i^2 = j^2 = k^2 = ijk = -1$$

De peur de voir sa découverte lui sortir de l'esprit, il grava immédiatement ladite relation dans une pierre du pont de Brougham, aujourd'hui Broom Bridge. Ceci illustre la nécessité d'avoir, toujours, un pont sous la main.

II Construction du corps des quaternions \mathbb{H} et premières propriétés

1 Construction

Définition. Un quaternion est un élément $(a, b, c, d) \in \mathbb{R}^4$. On note \mathbb{H} l'ensemble de ces quadruplets, que l'on munit des lois de composition internes suivantes :

$$+ : \begin{array}{ccc} \mathbb{H} \times \mathbb{H} & \longrightarrow & \mathbb{H} \\ \left(\begin{array}{c} a \\ b \\ c \\ d \end{array} \right), \left(\begin{array}{c} a' \\ b' \\ c' \\ d' \end{array} \right) & \longmapsto & \left(\begin{array}{c} a + a' \\ b + b' \\ c + c' \\ d + d' \end{array} \right) \end{array}$$

$$\cdot : \begin{array}{ccc} \mathbb{H} \times \mathbb{H} & \longrightarrow & \mathbb{H} \\ \left(\begin{array}{c} a \\ b \\ c \\ d \end{array} \right), \left(\begin{array}{c} a' \\ b' \\ c' \\ d' \end{array} \right) & \longmapsto & \left(\begin{array}{c} aa' - bb' - cc' - dd' \\ ab' + ba' + cd' - dc' \\ ac' + ca' - bd' + db' \\ da' + ad' + bc' - cb' \end{array} \right) \end{array}$$

$(\mathbb{R}^4, +)$ est alors un espace vectoriel.

Théorème. $(\mathbb{H}, +, \cdot)$ est un corps, non commutatif.

Démonstration On montre aisément que $(\mathbb{H}, +)$ est un groupe commutatif d'élément neutre $(0, 0, 0, 0)$. L'opposé d'un élément $(a, b, c, d) \in \mathbb{H}$ est $(-a, -b, -c, -d)$. On vérifie également sans difficulté l'associativité de \times , ainsi que la distributivité à gauche et à droite (on verra plus loin que l'on peut réaliser \mathbb{H} comme sous-anneau de $\mathcal{M}_4(\mathbb{R})$). $(1, 0, 0, 0)$ est le neutre de \cdot .

- Soit $(a, b, c, d) \in \mathbb{H}^* : a^2 + b^2 + c^2 + d^2 \neq 0$. On pose

$$a_1 = \frac{a}{a^2 + b^2 + c^2 + d^2} \quad b_1 = \frac{-b}{a^2 + b^2 + c^2 + d^2}$$

$$c_1 = \frac{-c}{a^2 + b^2 + c^2 + d^2} \quad d_1 = \frac{-d}{a^2 + b^2 + c^2 + d^2}$$

En appliquant la définition de la multiplication, il vient :

$$(a, b, c, d) \cdot (a_1, b_1, c_1, d_1) = (a_1, b_1, c_1, d_1) \cdot (a, b, c, d) = 1_{\mathbb{H}}$$

Ainsi, tout élément de \mathbb{H}^* est inversible, et \mathbb{H} est un corps.

– La loi \cdot n'est pas commutative ; en effet :

$$(0, 1, 0, 0) \cdot (0, 0, 1, 0) = (0, 0, 0, 1)$$

$$(0, 0, 1, 0) \cdot (0, 1, 0, 0) = (0, 0, 0, -1)$$

Notation Pour $z \in \mathbb{H}$, on note $-z$ l'opposé de z . Si $z \neq 0$, on note $\frac{1}{z}$ son inverse, et si $z' \in \mathbb{H}$, on écrit $\frac{z'}{z}$ pour $z' \cdot \frac{1}{z}$.

Plongement de \mathbb{C} dans \mathbb{H} On pose $\mathbb{H}' = \{(a, b, 0, 0)\}_{(a,b) \in \mathbb{R}^2}$, et l'on réalise le plongement de \mathbb{C} dans \mathbb{H} grâce à l'isomorphisme de corps

$$f : \mathbb{C} \longrightarrow \mathbb{H}$$

$$a + ib \longmapsto (a, b, 0, 0)$$

les opérations sur \mathbb{C} se prolongent sur \mathbb{H} , et \mathbb{H}' est commutatif (c'est un sous-corps de \mathbb{H} comme image d'un corps par un morphisme). On plonge également \mathbb{R} dans \mathbb{H} (via le plongement de \mathbb{C}) et la multiplication dans \mathbb{H} coïncide, sur les réels, avec la multiplication externe sur \mathbb{R}^4 vu comme \mathbb{R} -espace vectoriel. Par identification, tout quaternion $(a, b, 0, 0) \in \mathbb{H}'$ sera noté $a + ib$. Par analogie, on pose

$$j = (0, 0, 1, 0) \text{ et } k = (0, 0, 0, 1)$$

ce qui permet d'écrire $(a, b, c, d) \in \mathbb{H}$ $q = a + bi + cj + dk$.

On remarque que $(1, i, j, k)$ est une base du \mathbb{R} -espace vectoriel de dimension 4 \mathbb{H} . On résume alors ainsi la loi \cdot sur \mathbb{H} par les formules :

\cdot	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Définition. Soit K un corps. Le **centre de** K est l'ensemble C des éléments de K qui commutent avec tous les autres :

$$C = \{a \in K \mid \forall x \in K, ax = xa\}$$

Théorème. Le centre de $(\mathbb{H}, +, \cdot)$ est \mathbb{R} .

Démonstration Soit \mathbb{H}_1 le centre de $(\mathbb{H}, +, \cdot)$ et $q = (x, y, z, t) \in \mathbb{H}$.

$$\begin{aligned}
q \in \mathbb{H}_1 &\Leftrightarrow \forall p \in \mathbb{H}, q \cdot p = p \cdot q \\
&\Leftrightarrow \forall (a, b, c, d) \in \mathbb{H}, \begin{cases} ax - by - cz - dt &= xa - yb - zc - td \\ ay + bx + ct - dz &= ya + xb + zb - tc \\ az + cx - bt + dy &= xc + za - yd + tb \\ dx + at + bz - cy &= ta + xd + yc - zd \end{cases} \\
&\Leftrightarrow \forall (b, c, d) \in \mathbb{R}^3, \begin{cases} ct - dz &= zd - tc \\ -bt + dy &= -yd + tb \\ bz - cy &= yc - bz \end{cases} \\
&\Leftrightarrow \forall (b, c, d) \in \mathbb{R}^3, \begin{cases} ct - dz &= 0 \\ -bt + dy &= 0 \\ bz - cy &= 0 \end{cases} \\
&\Leftrightarrow y = z = t = 0 \\
&\Leftrightarrow q = (x, y, z, t) \in \mathbb{R} \text{ (plongé dans } \mathbb{H})
\end{aligned}$$

2 Norme, conjugaison

Définition. Soit $q = (a, b, c, d) \in \mathbb{H}$. Le **conjugué** de q est $\bar{q} = (a, -b, -c, -d)$. L'application de \mathbb{H} dans lui-même $q \mapsto \bar{q}$ s'appelle la **conjugaison**. Ces définitions prolongent celles de la conjugaison et du conjugué sur \mathbb{C} .

Théorème. La conjugaison est un automorphisme de $(\mathbb{H}, +)$. C'est une involution.

Démonstration Soit $q = (a, b, c, d) \in \mathbb{H}$

– Caractère bijectif :

$$\bar{\bar{q}} = (a, -(-b), -(-c), -(-d)) = (a, b, c, d) = q$$

Il s'agit d'une involution, donc d'une bijection.

– Morphisme : soit $q_2 = (a', b', c', d') \in \mathbb{H}$

$$\overline{q + q'} = (a+a', -(b+b'), -(c+c'), -(d+d')) = (a, -b, -c, -d) + (a', -b', -c', -d')$$

Donc $\overline{q + q'} = \bar{q} + \bar{q}'$, et la conjugaison est un morphisme de groupes.

Proposition. Soit $q = (a, b, c, d) \in \mathbb{H}$

. Alors

$$q\bar{q} = (a^2 + b^2 + c^2 + d^2, 0, 0, 0)$$

Démonstration Fastidieux, mais sans difficulté.

Théorème. L'application

$$\begin{aligned}
n &: \mathbb{H} &\longrightarrow & \mathbb{R}_+ \\
q &\longmapsto & q \cdot \bar{q}
\end{aligned}$$

est un morphisme de monoïdes de (\mathbb{H}, \cdot) dans (\mathbb{R}_+, \cdot) .

Démonstration Soit $q = (a, b, c, d)$ et $q' = (a', b', c', d')$ deux quaternions.

$$\begin{aligned}
n(qq') &= (aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 \\
&\quad + (ac' + ca' - bd' + db')^2 + (da' + ad' + bc' - cb')^2 \\
&= a^2n(q') + b^2n(q') + c^2n(q') + d^2n(q') \\
&= n(q)n(q') \\
n(1) &= 1^2 = 1
\end{aligned}$$

Proposition. $q \in \mathbb{H} \mapsto \sqrt{n(q)}$ est une norme sur \mathbb{H} .

Démonstration On vérifie que

$$\begin{aligned}
\varphi : \quad & \mathbb{H} \times \mathbb{H} & \longrightarrow & \mathbb{R} \\
& (a, b, c, d), (a', b', c', d') & \longmapsto & aa' + bb' + cc' + dd'
\end{aligned}$$

est un produit scalaire. $q \in \mathbb{H} \mapsto \sqrt{n(q)}$ est la norme qui en dérive.

Définition. L'application $q \in \mathbb{H} \mapsto \sqrt{n(q)}$ est appelée **norme sur le corps des quaternions** \mathbb{H} . On note G son noyau en tant que morphisme de monoïdes de (\mathbb{H}, \cdot) dans (\mathbb{R}_+, \cdot) .

Représentation matricielle \mathbb{H} possède une structure d'algèbre sur \mathbb{R} , de dimension 4, et $\mathcal{B}(1, i, j, k)$ en est une base. Ainsi, à $q = a + bi + cj + dk \in \mathbb{H}$ fixé, $p \in \mathbb{H} \mapsto q \cdot p$ est linéaire, et sa matrice dans \mathcal{B} est

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

En fait, \mathbb{H} est isomorphe à l'ensemble des matrices de cette forme. Si l'on note, pour $p \in \mathbb{H}$, $M(p)$ la matrice qui est associée à la multiplication par p à gauche, on a par composition que $M(p_1) \cdot M(p_2)$ est la matrice associée à la multiplication par $p_1 \cdot p_2$. \mathbb{H} s'identifie donc à la sous-algèbre de $\mathcal{M}_4(\mathbb{R})$ des matrices de la forme ci-dessus, avec

$$\begin{aligned}
1 = I_4 & & i = & \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\
j = & \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} & k = & \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}
\end{aligned}$$

On démontre ainsi plus aisément :

Proposition. $p \in \mathbb{H} \mapsto \bar{p}$ est un anti-automorphisme d'algèbre (i.e., $\overline{p \cdot q} = \bar{q} \cdot \bar{p}$).

Démonstration On sait que c' est un automorphisme de $(\mathbb{H}, +)$.

- $\forall x \in \mathbb{R}, \forall p \in \mathbb{H} \quad \overline{x \cdot p} = x \cdot \bar{p}$ (immédiat en écrivant $p = a + ib + jc + kd$).
- Soit $(p, q) \in \mathbb{H}^2$. En fait, la matrice de \bar{p} est $M(p)^T$. On a immédiatement

$$\overline{p \cdot q} = (M(p) \cdot M(q))^T = M(q)^T \cdot M(p)^T = \bar{q} \cdot \bar{p}$$

III Théorème de Frobenius

On a construit, dans la partie précédente, le corps des quaternions \mathbb{H} , un surcorps non commutatif de \mathbb{C} (et \mathbb{R}). Le but de cette partie est d'établir un résultat fondamental sur l'existence de surcorps à \mathbb{R} , le **théorème de Frobenius** (mathématicien allemand du XIXe siècle).

1 Extension d'un sous-corps

Définition. Soit K un corps (non supposé commutatif), L un sous-corps de K , P une partie de K .

Le plus petit sous-corps de K contenant L et P est appelé **l'extension de L engendrée par P** , et noté $L(P)$. Si $L(P) \neq K$, on parle d'**extension propre**. On montre que $L(P)$ est l'intersection de tous les sous-corps de K contenant P . De plus, si L est commutatif et si $P = \{x\}$ où x commute avec L tout entier, alors $L(x)$ est commutatif.

Proposition. Soit K un surcorps (non supposé commutatif) de \mathbb{R} distinct de \mathbb{R} , et $\alpha \in K \setminus \mathbb{R}$. Alors $\mathbb{R}(\alpha) \simeq \mathbb{C}$, et c'est un \mathbb{R} -espace vectoriel de dimension 2.

Démonstration Exercice.

Théorème. Il n'existe pas de surcorps commutatif de dimension finie à \mathbb{C} distinct de \mathbb{C} .

Démonstration Soit K un surcorps commutatif de \mathbb{C} de dimension finie, et $\alpha \in K$. On considère $\mathbb{C}[\alpha]$ la \mathbb{C} -algèbre engendrée par les puissances de α : elle est de dimension finie. Il est donc possible de trouver un polynôme P à coefficients complexes qui annule α (en effet, il existe n entier tel que $(1, \alpha, \alpha^2, \dots, \alpha^n)$ est lié).

Or, ce polynôme est scindé sur \mathbb{C} , car \mathbb{C} est algébriquement clos ; ses racines sont donc complexes, et ainsi $\alpha \in \mathbb{C}$.

Bilan : $K = \mathbb{C}$

2 Théorème de Frobenius

Nous disposons donc de trois corps de dimension finie contenant \mathbb{R} en leur centre, à savoir \mathbb{R} lui-même, \mathbb{C} et \mathbb{H} . Il s'agit à présent de démontrer qu'il n'en existe pas d'autre : c'est l'objet du théorème de Frobenius.

Théorème. Tout corps K de dimension finie contenant \mathbb{R} en son centre est isomorphe à \mathbb{R} , \mathbb{C} ou \mathbb{H} .

Démonstration Deux cas se présentent :

- Si K est commutatif : comme il n'existe pas d'autre surcorps de dimension finie commutatif à \mathbb{R} que \mathbb{R} et \mathbb{C} , $K \simeq \mathbb{R}$ ou $K \simeq \mathbb{C}$
- Si K n'est pas commutatif : en particulier, $\mathbb{C} \subsetneq K$. Prenons $\alpha \in K \setminus \mathbb{R}$, et identifions \mathbb{C} à $\mathbb{R}(\alpha)$.
- Comme il n'existe pas d'extension propre de \mathbb{C} commutative (ADMIS), \mathbb{C} est un sous-corps commutatif maximal de K .
Soit $z \in K$ commutant avec tout complexe (i.e, avec i) : $\mathbb{C}(z)$ est un sous-corps commutatif de K contenant \mathbb{C} , donc $\mathbb{C}(z) = \mathbb{C}$ et ainsi $z \in \mathbb{C}$.

- Soit $y \in K \setminus \mathbb{C}$; on pose $z = yi - iy \neq 0$ (car sinon y et i commutent, et $y \in \mathbb{C}$). On a

$$iz = iyi + y = -(-y - iyi) = -zi$$

d'où

$$iz^2 = -ziz = -z(-zi) = z^2i$$

Ainsi, z^2 commute avec i , et $z^2 \in \mathbb{C}$.

$\mathbb{R} \subset \mathbb{R}(z) \cap \mathbb{C} \subset \mathbb{C}$, et $\mathbb{R}(z) \cap \mathbb{C}$ est un corps : c'est donc \mathbb{R} ou \mathbb{C} . Supposons que ce soit \mathbb{C} : alors $\mathbb{C} \subset \mathbb{R}(z)$; et comme $\mathbb{R}(z)$ est un \mathbb{R} -espace vectoriel de dimension 2 (car z commute avec tous les éléments de \mathbb{R} et n'est pas lui-même réel), on a $\mathbb{R}(z) = \mathbb{C}$. Ce qui est exclu, car $z \notin \mathbb{C}$. Donc $\mathbb{R}(z) \cap \mathbb{C} = \mathbb{R}$.

On a du coup $z^2 \in \mathbb{R}$ (car $z^2 \in \mathbb{C}$ et $z^2 \in \mathbb{R}(z)$); et même $z^2 \in \mathbb{R}_-$ (sinon, si $z^2 = a > 0$, le polynôme $X^2 - a$ aurait 4 racines distinctes $z, -z, \sqrt{a}$ et $-\sqrt{a}$ dans $\mathbb{R}(z)$, ce qui peut se révéler gênant au vu de son degré).

Posons $z^2 = -r$ avec $r \in \mathbb{R}_+$, et $j = z/\sqrt{r}$.

$$ij = \frac{iz}{\sqrt{r}} = \frac{-zi}{\sqrt{r}} = -ji$$

et

$$j^2 = \frac{z^2}{r} = -1$$

En posant $k = ij$, on obtient $\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k \subset K$, d'où $\mathbb{H} \subset K$ (on a vu précédemment que $\mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k \simeq \mathbb{H}$).

- Supposons $\mathbb{H} \subsetneq K$: on peut prendre $v \in K \setminus \mathbb{H}$. De la même manière, on pose $w = vi - iv$, puis $l = w/\sqrt{-w^2}$: on a à nouveau $li = -il$ et $l^2 = -1$.

$jli = j(-il) = (-ji)l = ijl$: jl et i commutent, donc $jl \in \mathbb{C}$: $jl \in \mathbb{H}$, et par conséquent (car $j \in \mathbb{H}$) $l \in \mathbb{H}$ et $w \in \mathbb{H}$.

On considère à présent $u = vi + iv$: $ui = -v + ivi = iu$, donc u et i commutent et $u \in \mathbb{C} \subset \mathbb{H}$. On a alors

$$v = \frac{w + u}{2i} \in \mathbb{H}$$

Ce qui est contraire à l'hypothèse. Ainsi, au final, $K \simeq \mathbb{H}$.

IV Applications

1 Curiosité : les fractales

Il est possible de remplacer, dans les équations décrivant des ensembles de fractales tels que l'ensemble de Julia ou l'ensemble de Mandelbrot, la variable complexe par des quaternions (ici, pour l'ensemble de Julia, constitué de l'ensemble des $z_0 \in \mathbb{H}$ pour lesquels, à $q \in \mathbb{H}$ fixé, la suite $(z_n)_{n \geq 0}$ est bornée) :

$$z_{n+1} = z_n^2 + q$$

Le résultat n'est plus, bien entendu, assimilable à une partie du plan ; on peut toutefois tenter une interprétation graphique en considérant l'espace à 3 dimensions *évoluant dans le temps* (l'une des composantes sert de paramètre aux 3 autres).



Rendu à l'aide de POV-Ray

2 Traitement informatique des images

Bien que ce domaine semble n'avoir *a priori* rien à voir, de près ou de loin, avec les quaternions, ces derniers peuvent être utilisés dans le traitement numérique d'images.

À chaque pixel peut être attribué un vecteur, dont les composantes sont par exemple les valeurs RVB (valeurs de rouge, vert et bleu) correspondantes. On dispose ainsi d'une liste de vecteurs ; toutefois, afin d'être en mesure de les manipuler, il est nécessaire de les identifier à des quaternions purs. Il est alors possible de manipuler les valeurs des pixels, via leur représentation dans \mathbb{H} , de manière *géométrique*.

En généralisant des outils tels que la transformation de Fourier aux quaternions, on dispose alors d'outils de traitement (obtention et décomposition du spectre de l'image, notamment).

3 Informatique et programmation 3D

Une grande partie des moteurs ou logiciels 3D, afin de manipuler des rotations arbitraires dans l'espace, ont recours aux quaternions - une autre possibilité résidant dans les matrices. En effet, un quaternion peut être vu comme un couple (réel, vecteur), ou, en d'autres termes, un vecteur et un angle de rotation autour de celui-ci.

Plus précisément, on s'intéressera uniquement aux quaternions normalisés (de norme 1). Tenter d'appliquer les algorithmes habituels avec des quaternions non normalisés résulte généralement - dans le cas des moteurs 3D - en modèles étrangement déformés à l'écran après une rotation.

Soit $\theta \in [0, \pi]$ et $\vec{h} = (x, y, z)$ un vecteur normé. Alors, le quaternion associé à

la rotation d'angle θ et d'axe orienté \vec{h} est $q = a + bi + cj + dk$ avec a, b, c, d réels tels que :

$$\begin{aligned} a &= \cos \frac{\theta}{2} \\ b &= x \sin \frac{\theta}{2} \\ c &= y \sin \frac{\theta}{2} \\ d &= z \sin \frac{\theta}{2} \end{aligned}$$

Ou, en d'autres termes : $q = \cos(\theta/2) + \sin(\theta/2)\vec{h}$. Muni de cela, on peut appliquer une rotation à un vecteur en effectuant le produit du quaternion et du vecteur (ce qui renvoie le nouveau vecteur), composer deux rotations juste en multipliant les quaternions associés (*le produit n'étant pas commutatif, l'ordre de multiplication importe*), interpoler une rotation (par exemple, programmer une rotation de $\pi/2$ autour d'un vecteur qui se fasse progressivement, en 12 secondes) ...



Il y a un tas de quaternions derrière ça.