Sur les quaternions

par Jean-Philippe CORTIER,
Lycée Marie de Champagne, Troyes

Les quaternions fournissent un exemple de corps non commutatif. Ils sont une extension de **R** de degré 4. Mais ils interviennent également en géométrie où ils facilitent la composition de rotations et en arithmétique. Enfin les quaternions ont une importance considérable en mécanique quantique.

On se propose de développer trois points :

I - Historique des quaternions
II - Quaternions et Géométrie. Application à la mécanique quantique
III - Quaternions et Arithmétique.

I. Historique

Le créateur des quaternions, Sir Hamilton William Rowan, né à Dublin (1805-1865), s'est penché (outre ses travaux sur les irrationnels) sur l'algèbre des couples.

Hamilton, dans son livre *Algebra as the Science of Pure Time*, développe les nombres complexes en termes de couples de nombres réels, d'une manière identique à celle utilisée aujourd'hui :

$$(a,b)+(a',b') = (a+a',b+b')$$
$$(a,b)\times(a',b') = (aa'-bb',a'b+ab')$$

$(\mathbf{R}^2,+,\times)$ ainsi créé donne le corps des nombres complexes $(\mathbf{C},+,\times)$, avec (a,b) équivalent à la notation connue $a+ib$. Il est à noter qu'il n'existe pas de structure de corps sur $\mathbf{R}^3$ (l'addition provenant de la structure d'espace vectoriel de $\mathbf{R}^3$). Pour cela, on pourra consulter [1].

Hamilton porte ses efforts sur la recherche d'un corps qui soit un espace vectoriel de dimension 4 sur **R**, l'addition étant commune aux deux structures. C'est ainsi qu'il découvre et construit le corps H des quaternions (*Lectures on quaternions*, 1853).

Si $(1,i,j,k)$ est une base de l'espace vectoriel H sur **R**, il associe à l'élément (t,x,y,z) de $\mathbf{R}^4$ le quaternion $q=t+xi+yj+zk$; **R** se trouve alors identifié au sous-espace de H engendré par 1 et les opérations sont définies par :

$$(t,x,y,z)+(t',x',y',z') = (t+t',x+x',y+y',z+z')$$
$$i^2=j^2=k^2=-1\ ;\ ij=k=-ji\ ;\ jk=i=-kj\ ;\ ki=j=-ik$$

[1] DIEUDONNE J. *Algèbre linéaire et géométrie élémentaire.* Hermann 1964

Alors H est un corps non commutatif dont le centre est **R** (Le centre d'un anneau $(A, +, \times)$ est l'ensemble des éléments de A qui commutent au sens de la multiplication avec tous les éléments de A). **R** est donc un sous-corps de H et la dimension de H en tant qu'espace vectoriel sur **R** est 4.

Remarquons que H contient une infinité de sous-corps isomorphes à **C** : par exemple les sous-corps **R**[i] , **R**[j] et **R**[k] où, si $a \in H$, **R**[a] désigne le sous-corps engendré par i et a (**R**[a] est encore le plus petit sous-corps de H, au sens de l'inclusion, contenant i et a).

Le théorème de Frobenius précise le rôle des quaternions, vus comme exemple de corps non commutatif :

> ***Théorème 1*** : Soit K un corps non commutatif de centre le corps des nombres réels et de dimension finie sur **R**. Alors K est isomorphe au corps des quaternions.

Pour une démonstration, voir par exemple [2].

Notons enfin que, de même que l'on présente, dans certains manuels du second cycle, **C** comme un sous-ensemble de $(\mathcal{M}_2(\mathbf{R}), +, \times)$ avec

$$\mathbf{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad (a,b) \in \mathbf{R}^2 \right\},$$

l'on peut représenter H comme le sous-espace de $\mathcal{M}_2(\mathbf{C})$ constitué par les matrices $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ avec $(\alpha,\beta) \in \mathbf{C}^2$.

II. Quaternions et géométrie. Application à la mécanique quantique

Un des intérêts des quaternions est de représenter paramétriquement le groupe $O^+(3)$ des rotations de $\mathbf{R}^3$ (de même que $U = S^1 = \{z \in \mathbf{C}, |z| = 1\}$ donne une représentation de $O^+(2)$).

En effet, comme l'indique M. Berger dans [3], les paramétrisations facilitent le calcul de la composée de rotations de $\mathbf{R}^3$.

Pour cela, on identifie H à $\mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$ et $\mathbf{R}^3$ à $\mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k$.

Si $q = t + xi + yj + zk$ est un élément de H, on note

$$\bar{q} = t - xi - yj - zk \quad \text{et} \quad q \longmapsto |q| = \sqrt{t^2 + x^2 + y^2 + z^2} = \sqrt{q\bar{q}}$$

est une norme sur H dérivant du produit scalaire $q.r = \frac{1}{2}[\bar{q}r + \bar{r}q]$ qui munit H d'une structure d'espace vectoriel euclidien.

[2] BOURBAKI *Algèbre, chapitre 8, Modules et Anneaux semi-simples.* Hermann 1958

$S^3 = \{q \in H,\ |q| = 1\}$ est un sous-groupe du groupe multiplicatif $H^* = H \setminus \{0\}$, ce qui permet d'affirmer que S^3, la sphère unité de $\mathbf{R}^4$, peut être munie d'une structure de groupe ; et on a le théorème :

Théorème 2 : Soit $s \in S^3$ et φ_s l'endomorphisme de H défini par

$$\varphi_s(q) = sqs^{-1}.$$

- Alors φ_s laisse $\mathbf{R}^3$ stable et $\rho_s = \varphi_s/\mathbf{R}^3$ est un élément de $O^+(3)$.
- L'application $\begin{vmatrix} S^3 \longrightarrow O^+(3) \\ s \longmapsto \rho_s \end{vmatrix}$ est un homomorphisme surjectif de groupe de noyau $\mathbf{Z}/2\mathbf{Z}$.
- Soit $\alpha \in \mathbf{R}$, $u \in \mathbf{R}^3 \setminus \{0\}$ et $s = \alpha.u$ avec $s \in S^3$.

L'axe de la rotation ρ_s est la droite $\mathbf{R}u$ et la mesure de l'angle θ ($\theta \in [0, \pi]$) de ρ_s est donnée par

$$\begin{cases} \operatorname{tg} \dfrac{\theta}{2} = \dfrac{|u|}{|\alpha|} & \text{si } \alpha \neq 0 \\ \theta = \pi & \text{si } \alpha = 0 \end{cases}$$

Pour la démonstration, on pourra consulter [3].

Par exemple :

- si $s = k$, on obtient la rotation de π autour de l'axe des z ;
- si $s' = \dfrac{1}{\sqrt{2}}(1+k)$, $\rho_{s'}$ est la rotation de $\dfrac{\pi}{2}$ autour de l'axe des z.

Réciproquement, si r désigne la rotation de $\mathbf{R}^3$ d'axe la droite $\mathbf{R}u$ avec $u = i + j + k$ et de mesure $\dfrac{\pi}{3}$, on peut écrire $r = \rho_{s_1}$ avec

$$s_1 = \frac{1}{\sqrt{12}}(3 + i + j + k)$$

Ensuite, si on note $r' = \rho_{s'}$ avec $s' = \dfrac{1}{\sqrt{2}}(1+k)$, on a, en appliquant le théorème :

$$r' \circ r = \rho_{s'} \circ \rho_{s_1} = \rho_{s's_1} \text{ avec } s's_1 = \frac{1}{\sqrt{6}}(1 + j + 2k)$$

$r' \circ r$ est donc la rotation d'axe $\mathbf{R}(j + 2k)$ et d'angle de mesure θ avec $\operatorname{tg} \dfrac{\theta}{2} = \sqrt{5}$.

[3] BERGER M. *Géométrie*. Volume 2. Cedic Nathan

Application à la Mécanique Quantique

L'homomorphisme $S^3 \longrightarrow O^+(3)$ décrit dans le théorème 2 a présenté une importance considérable en mécanique quantique (Pauli-Dirac, vers 1927) où il est indispensable à la description du Spin S d'un électron. Pour plus de précision, on peut consulter n'importe quel livre de mécanique quantique.

En particulier, il est souvent commode d'introduire, dans cette théorie, l'opérateur σ tel que $S = \frac{h}{2}\sigma$ où h est la constante de Planck, dont les composantes sont les matrices de Pauli :

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ et } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ où } i \in \mathbf{C} \quad (i^2 = -1)$$

Elles vérifient les relations : $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$$\sigma_x \sigma_y = -\sigma_y \sigma_x = iI$$

et celles qui s'en déduisent par permutation circulaire ; et l'application :

$t + xi + yj + zk \longmapsto \frac{1}{i}\begin{pmatrix} t+z & x-iy \\ x+iy & t-z \end{pmatrix}$ définit un isomorphisme de H sur le corps des matrices carrées d'ordre 2 à coefficients complexes du type ci-dessus.

III. Quaternions et arithmétique

Les quaternions interviennent en arithmétique ; témoin ce théorème :

> ***Théorème 3*** : Tout entier naturel s'écrit comme "somme de quatre carrés". Autrement dit :
> pour tout n de N, il existe $(x,y,z,t) \in \mathbf{Z}^4$ tel que $n = x^2 + y^2 + z^2 + t^2$.

La démonstration en est simple et repose sur la norme d'un quaternion. On appelle *quaternion entier* tout élément q de H s'écrivant

$$q = t + xi + yj + zk \quad \text{avec} \quad (t,x,y,z) \in \mathbf{Z}^4.$$

On notera $H_1 = \mathbf{Z} \oplus \mathbf{Z}i \oplus \mathbf{Z}j \oplus \mathbf{Z}k$ l'ensemble des quaternions entiers.

On pose

$$N(q) = q\bar{q} = \|q\|^2 = t^2 + x^2 + y^2 + z^2$$

On a $N(qq') = N(q)\,N(q')$ pour $(q,q') \in H^2$. Enfin l'on note $S = \{n \in \mathbf{N}^*,\ n$ s'écrivant comme somme de quatre carrés$\}$.

On a :

L_1 • $n \in S$ si et seulement si $n = N(q)$ avec $q \in H_1$ • Ceci est clair.

L_2 • Si $(n,n') \in S^2$, alors $n.n' \in S$.

En effet, $n = N(q)$ et $n' = N(q')$ avec $(q,q') \in H_1^2$.

$nn' = N(q)\,N(q') = N(qq')$ avec $qq' \in H_1$ donc $nn' \in S$.

L_3 • Tout nombre premier p est élément de S.

Supposons pour l'instant ce point démontré ; le théorème 3 en découle aisément :

Un entier naturel n non nul étant donné, il se décompose en un produit d'éléments premiers, donc d'éléments de S. S étant stable pour la multiplication, on a $\boxed{n \in S}$.

Revenons à L_3 : si $p = 2$, alors $p = 1^2 + 1^2 + 0^2 + 0^2 \in S$.

Soit désormais p un nombre premier impair ; alors $\frac{p-1}{2} \in \mathbf{N}$

Les applications $\varphi, \psi : E = \{0,\ldots,\frac{p-1}{2}\} \longrightarrow \mathbf{Z}/p\mathbf{Z}$

$$x \longrightarrow \varphi(x) = \overline{x^2}$$
$$x \longrightarrow \psi(x) = \overline{-(1+x^2)}$$

sont injectives.

On ne peut avoir $\varphi(E) \cap \psi(E) = \phi$: en effet, on aurait alors

$$\text{card}\,(\varphi(E) \cup \psi(E)) = \text{card}\,(\varphi(E)) + \text{card}\,(\psi(E))$$
$$= \frac{p+1}{2} + \frac{p+1}{2} = p+1 \leqslant \text{card}\,\mathbf{Z}/p\mathbf{Z} = p$$

car $\varphi(E) \cup \psi(E) \subset \mathbf{Z}/p\mathbf{Z}$.

Donc $\varphi(E) \cap \psi(E) \neq \phi$: il existe $(x,y) \in \left\{0,\ldots,\frac{p-1}{2}\right\}^2$ tel que :

$\varphi(x) = \overline{x^2} = \psi(y) = \overline{-(1+y^2)}$; d'où l'existence de $m \in \mathbf{Z}$ tel que $1 + x^2 + y^2 = mp$. Remarquons que

$$0 < m < p. \quad \left((x,y) \in \left\{0,\ldots,\frac{p-1}{2}\right\}^2 \Rightarrow 1 + x^2 + y^2 < p^2\right)$$

Si $m = 1$, L_3 est démontré ; sinon $m > 1$ et on a :

L_4 • Si $n \in [2,p-1]$ est tel que $np \in S$, alors il existe $n' \in [1,p-1]$ tel que $n' < n$ et $n'p \in S$.

En appliquant à m ($m \in [1,p-1]$ et $mp \in S$) L_4 un nombre fini de fois, on obtiendra $1.p \in S$, d'où L_3.

Si n est pair, alors $n = 2n'$, $n' \in \mathbf{N}$, $n' < n$; par hypothèse

$$np = 2n'p = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \text{ avec } (\alpha,\beta,\gamma,\delta) \in \mathbf{Z}^4 ;$$

en regroupant, puisque $\alpha^2+\beta^2+\gamma^2+\delta^2$ est pair, les paires de termes $\alpha,\beta,\gamma,\delta$ ayant même parité, l'on a par exemple :

$$np = 2n'p = 2\left[\left(\frac{\alpha+\beta}{2}\right)^2+\left(\frac{\alpha-\beta}{2}\right)^2+\left(\frac{\gamma+\delta}{2}\right)^2+\left(\frac{\gamma-\delta}{2}\right)^2\right]$$

d'où $\qquad n'p\in S$

Si n' est impair : on écrit $np = x_1^2+x_2^2+x_3^2+x_4^2$, $x_i\in\mathbf{Z}$

On ne peut avoir $\overline{x_i} = \overline{0}$ pour tout i dans $\mathbf{Z}/n\mathbf{Z}$, sinon $np\equiv 0(n^2)$ et n diviserait p avec $1<n<p-1$ et p premier, ce qui ne se peut.

D'autre part : pour tout $i\in[1,\ldots,4]$, $\frac{x_i}{n}\in\mathbf{Q}$ et l'on peut trouver $\alpha_i\in\mathbf{Z}$ tel que $\left|\frac{x_i}{n}-\alpha_i\right|\leqslant\frac{1}{2}$; il suffit pour cela de prendre

$$\alpha_i = \mathrm{E}\left(\frac{x_i}{n}\right) \qquad \text{si } \left|\frac{x_i}{n}-\mathrm{E}\left(\frac{x_i}{n}\right)\right| \leqslant \frac{1}{2}$$

$$\alpha_i = \mathrm{E}\left(\frac{x_i}{n}\right)+1 \qquad \text{si } \left|\frac{x_i}{n}-\mathrm{E}\left(\frac{x_i}{n}\right)\right| > \frac{1}{2}$$

En fait, on ne peut avoir $\left|\frac{x_i}{n}-\alpha_i\right| = \frac{1}{2}$ car dans ce cas $\frac{x_i}{n}-\alpha_i = \varepsilon.\frac{1}{2}$ où $\varepsilon = \pm 1$ et $2(x_i-\alpha_i n) = \varepsilon n$, donc n serait pair. On pose $y_i = x_i - n\alpha_i\in\mathbf{Z}$ avec donc $|y_i|<\frac{n}{2}$. Dans $\mathbf{Z}/n\mathbf{Z}$, $\overline{y_i}=\overline{x_i}$ et par suite

$$\overline{y_1^2+y_2^2+y_3^2+y_4^2} = \overline{x_1^2}+\overline{x_2^2}+\overline{x_3^2}+\overline{x_4^2} = \overline{0}$$

Il existe donc $n'\in\mathbf{N}$ tel que $y_1^2+y_2^2+y_3^2+y_4^2 = nn' < 4\left(\frac{n}{2}\right)^2 = n^2$

Donc $0\leqslant n'<n$ et $n'\neq 0$, car $n'=0$ donne $y_i=0$ pour tout i et donc $x_i = n\alpha_i$ pour tout i , ce qui ne se peut.

Conclusion : $\qquad 0<n'<n\leqslant p-1.$

On écrit alors

$$q = x_1+x_2\mathbf{i}+x_3\mathbf{j}+x_4\mathbf{k} \qquad \mathrm{N}(q) = \sum_{i=1}^{4} x_i^2 = np$$

$$q' = y_1+y_2\mathbf{i}+y_3\mathbf{j}+y_4\mathbf{k} \qquad \mathrm{N}(q') = \sum_{i=1}^{4} y_i^2 = nn',\ y_i = x_i-n\alpha_i$$

$q' = q-nu$ avec $u=\alpha_1+\alpha_2\mathbf{i}+\alpha_3\mathbf{j}+\alpha_4\mathbf{k}\in\mathrm{H}_1$ car $\alpha_i\in\mathbf{Z}$ pour tout i .

$q\bar{q}' = q(\bar{q}-n\bar{u}) = q\bar{q}-nq\bar{u} = \mathrm{N}(q)-nq\bar{u} = np-nq\bar{u} = n(p-q\bar{u})$

$q\bar{q}' = nh_1$ avec $h_1 = p-q\bar{u}\in\mathrm{H}_1$ car p,q et $\bar{u}$ sont des éléments de H_1.

$\mathrm{N}(q\bar{q}') = \mathrm{N}(q)\mathrm{N}(\bar{q}') = \mathrm{N}(q)\mathrm{N}(q') = npnn' = n^2pn' = \mathrm{N}(nh_1) = n^2\mathrm{N}(h_1)$.

Donc $n'p = \mathrm{N}(h_1)\in S$ car $h_1\in\mathrm{H}_1$, ce qui démontre L_4.