Université Pierre et Marie Curie, année 2005-2006

Agrégation externe de Mathématiques

Quaternions réels

Nous indiquons ci-après différentes constructions et quelques applications de l'algèbre des quaternions réels. Cette algèbre est un corps non commutatif, c'est essentiellement le seul exemple de corps non commutatif dans le programme.

Première construction

Notons $(1, i, j, k)$ la base canonique de $\mathbb{R}^4$. Il existe une application $\mathbb{R}$-bilinéaire unique $m : \mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}^4$, appelée *multiplication*, telle que le produit de deux éléments quelconques de la base canonique de $\mathbb{R}^4$ soit donné par la table de multiplication suivante:

$$1.1 = 1\ ,\quad 1i = i1 = i\ ,\quad 1j = j1 = j\ ,\quad 1k = k1 = k\ ,\quad i^2 = j^2 = k^2 = -1\,, \tag{1}$$

$$ij = k\,,\ ji = -k\ ,\quad jk = i\,,\ kj = -i\ ,\quad ki = j\,,\ ik = -j\,. \tag{2}$$

On note $\mathbb{H}$ l'espace vectoriel $\mathbb{R}^4$ muni de la loi de composition m.

Lemme 1. *La multiplication m sur $\mathbb{H}$ est associative, elle fait de $\mathbb{H}$ une $\mathbb{R}$-algèbre.*

Démonstration. Pour tous $x, y \in \mathbb{R}^4$, on pose $xy = m(x, y)$. Nous devons montrer que, si $x, y, z \in \mathbb{R}^4$, on a $(xy)z = x(yz)$. Les applications $(x, y, z) \mapsto (xy)z$ et $(x, y, z) \mapsto x(yz)$ de $(\mathbb{R}^4)^3$ dans $\mathbb{R}^4$ étant $\mathbb{R}$-trilinéaires, il suffit de montrer que $(xy)z = x(yz)$ lorsque $x, y, z \in \{1, i, j, k\}$, ce qui donne a priori $4^3 = 64$ vérifications à faire. En fait, les égalités (1) montrent que $1x = x1 = x$ pour tout $x \in \{1, i, j, k\}$. Par linéarité, il en résulte que $1x = x1 = x$ pour tout $x \in \mathbb{R}^4$. Il est alors clair que l'égalité $(xy)z = x(yz)$ est vraie dès que $x, y, z \in \{1, i, j, k\}$ et l'un des éléments x, y, z vaut 1. Il reste à prouver cette égalité lorsque $x, y, z \in \{i, j, k\}$, ce qui fait encore 27 cas.

Soit φ l'automorphisme $\mathbb{R}$-linéaire de $\mathbb{R}^4$ appliquant $1, i, j, k$ sur $1, j, k, i$ respectivement. On remarque que la table de multiplication est invariante par permutation circulaire de i, j, k. En d'autres termes $m(\varphi(x), \varphi(y)) = \varphi(m(x, y))$ pour tous $x, y \in \mathbb{R}^4$. Il suffit donc de vérifier l'égalité $(xy)z = x(yz)$ lorsque par exemple $x = i$ et $y, z \in \{i, j, k\}$, d'où 9 vérifications:

$$(ii)i = (-1)i = -i\,,\ i(ii) = i(-1) = -i\ ;\quad (ii)j = (-1)j = -j\,,\ i(ij) = ik = -j\,,$$

$$(ii)k = (-1)k = -k\,,\ i(ik) = i(-j) = -(ij) = -k\ ;\quad (ij)i = ki = j\,,\ i(ji) = i(-k) = -(ik) = j\,,$$

$$(ij)j = kj = -i\,,\ i(jj) = i(-1) = -i\ ;\ \ (ij)k = kk = -1\,,\ i(jk) = ii = -1\,,$$
$$(ik)i = (-j)i = -(ji) = k\,,\ i(ki) = ij = k\ ;\ \ (ik)j = (-j)j = 1\,,\ i(kj) = i(-i) = 1\,,$$
$$(ik)k = (-j)k = -(jk) = -i\,,\ i(kk) = i(-1) = -i\,.$$

Ouf! La multiplication m sur $\mathbb{H}$ est donc associative. Comme 1 est élément neutre pour m, m fait de $\mathbb{H}$ une $\mathbb{R}$-algèbre, en particulier un anneau (rappel: la distributivité de la multiplication par rapport à l'addition résulte de la $\mathbb{R}$-bilinéarité de m). La $\mathbb{R}$-algèbre $\mathbb{H}$ est de dimension 4.

cqfd

Les éléments de $\mathbb{H}$ s'appellent des *quaternions* (réels). Tout quaternion q s'écrit donc de manière unique:

$$q \ = \ a + bi + cj + dk\ , \quad \text{où } (a,b,c,d) \in \mathbb{R}^4\,, \tag{3}$$

en identifiant $a \in \mathbb{R}$ avec $a1 \in \mathbb{H}$. Pour un tel quaternion q, on pose:

$$\bar{q} \ = \ a - bi - cj - dk\,. \tag{4}$$

Le quaternion $\bar{q}$ est appelé *conjugué* de q. La conjugaison $q \mapsto \bar{q}$ est un automorphisme du $\mathbb{R}$-espace vectoriel $\mathbb{H}$, cet automorphisme est *involutif*: $\bar{\bar{q}} = q$ pour tout $q \in \mathbb{H}$. Un quaternion q est dit *pur* si $\bar{q} = -q$, i.e. si q est combinaison linéaire de i, j, k. Tout quaternion q s'écrit donc de manière unique $q = a + q'$, où $a \in \mathbb{R}$ et q' est un quaternion pur.

Lemme 2. *La conjugaison $q \mapsto \bar{q}$ est un* antiautomorphisme *de la $\mathbb{R}$-algèbre $\mathbb{H}$. Autrement dit, pour tous quaternions q_1, q_2, on a:*

$$\overline{q_1 q_2} \ = \ \overline{q_2}\,\overline{q_1}\,.$$

Démonstration. Par $\mathbb{R}$-bilinéarité, on se ramène immédiatement au cas où $q_1, q_2 \in \{i, j, k\}$, et il s'agit de vérifier que $\overline{q_1 q_2} = q_2 q_1$. On peut même supposer que $q_1 = i$, grâce à φ. On calcule:

$$\overline{ii} = -1 = ii\ , \ \ \overline{ij} = -k = ji\ , \ \ \overline{ik} = \overline{-j} = j = ki\,.$$

Munissons maintenant l'espace vectoriel $\mathbb{R}^4$ de la norme euclidienne usuelle. Pour un quaternion q, la norme de $q \in \mathbb{R}^4$ sera notée $|q|$ plutôt que $||q||$.

Lemme 3. *Pour tout quaternion q, on a:*

$$q\,\bar{q} \ = \ \bar{q}\,q \ = \ |q|^2\,. \tag{5}$$

Démonstration. La base canonique $(1, i, j, k)$ de $\mathbb{R}^4$ est orthonormée. Il suffit donc de prouver la formule (5) lorsque q est pur, l'égalité à démontrer s'écrivant alors: $q^2 = -|q|^2$. Écrivons $q = bi + cj + dk$, où $(b, c, d) \in \mathbb{R}^3$. Alors $|q|^2 = b^2 + c^2 + d^2$, et, vu les égalités (1) et (2),

$$q^2 = (bi + cj + dk)(bi + cj + dk) = -(b^2 + c^2 + d^2)\,,$$

parce que les éléments i, j, k anticommutent: $ij + ji = jk + kj = ki + ik = 0$.

Théorème 1. *La $\mathbb{R}$-algèbre $\mathbb{H}$ est un corps. Ce corps est non commutatif, plus précisément, le centre de $\mathbb{H}$ est $\mathbb{R}$.*

Démonstration. Soit d'abord q un quaternion non nul. Les égalités (5) montrent que q possède un inverse q^{-1} donné par la formule suivante (remarquer l'analogie avec les nombres complexes):

$$q^{-1} \;=\; \frac{1}{|q|^2}\,\bar{q}\,. \tag{6}$$

Ainsi $\mathbb{H}$ est un corps. Il reste à déterminer le centre Z de $\mathbb{H}$, formé des éléments qui commutent avec tout quaternion. Puisque $\mathbb{H}$ est une $\mathbb{R}$-algèbre, Z contient déjà $\mathbb{R} = \{a1 \mid a \in \mathbb{R}\}$. Il suffit de montrer que 0 est le seul quaternion pur appartenant à Z. Soit $q = bi+cj+dk$ un tel quaternion. On a $iq = -b + ck - dj$ et $qi = -b - ck + dj$, d'où $c = d = 0$, donc $q = bi$. Ensuite $jq = -bk$ et $qj = bk$, d'où $b = 0$ et ainsi $q = 0$.

cqfd

Remarques 1) Considérons l'application $q \mapsto |q|$ de $\mathbb{H}^* = \mathbb{H} \setminus \{0\}$ dans $\mathbb{R}^*$. C'est un morphisme de groupes multiplicatifs. En effet, si $q_1, q_2 \in \mathbb{H}^*$, on a:

$$|q_1q_2|^2 \;=\; (q_1q_2)\overline{q_1q_2} \;=\; (q_1q_2)(\overline{q_2}\,\overline{q_1}) \;=\; q_1|q_2|^2\overline{q_1} \;=\; (q_1\overline{q_1})|q_2|^2 \;=\; |q_1|^2\,|q_2|^2\,.$$

2) Le corps $\mathbb{C}$ est un sous-corps de $\mathbb{H}$: tout nombre complexe $a+ib$ (où $a, b \in \mathbb{R}$) peut être identifié au quaternion $a+bi$, la multiplication de $\mathbb{C}$ étant la restriction de celle de $\mathbb{H}$. Cependant $\mathbb{H}$ n'est pas une $\mathbb{C}$-algèbre, car $\mathbb{C}$ n'est pas contenu dans le centre de $\mathbb{H}$, à savoir $\mathbb{R}$.

3) Posons:

$$\mathbb{H}_8 \;=\; \{\pm 1,\, \pm i,\, \pm j,\, \pm k\} \;\subset\; \mathbb{H}^*\,.$$

Les formules (1) et (2) montrent que $\mathbb{H}_8$ est un sous-groupe multiplicatif d'ordre 8 de $\mathbb{H}^*$, on l'appelle groupe des quaternions d'ordre 8. On sait que, si K est un corps *commutatif*, tout sous-groupe fini de K^* est cyclique. Ici, le groupe $\mathbb{H}_8$ n'est pas cyclique, il n'est en fait pas commutatif. Par ailleurs, il est classique qu'il existe, à isomorphisme près, exactement cinq groupes d'ordre 8, à savoir:

$$(\mathbb{Z}/8\mathbb{Z})\;,\quad (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})\;,\quad (\mathbb{Z}/2\mathbb{Z})^3\;,\quad \mathbb{H}_8\;,\quad D_4\,,$$

en notant D_4 le groupe diédral d'ordre 8.

Deuxième construction

Notons ici $\mathbb{H}$ l'ensemble des matrices complexes 2×2 de la forme suivante:

$$M(a,b) \;=\; \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}\;,\quad \text{où}\quad (a,b) \in \mathbb{C}^2\,.$$

Il est clair que $\mathbb{H}$ est un $\mathbb{R}$-sous-espace vectoriel de dimension 4 de $M_2(\mathbb{C})$, contenant la matrice identité I_2. C'est en fait une sous-$\mathbb{R}$-algèbre de $M_2(\mathbb{C})$: si $a, b, c, d \in \mathbb{C}$, il vient:

$$M(a,b)M(c,d) \;=\; \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \begin{pmatrix} c & -\bar{d} \\ d & \bar{c} \end{pmatrix} \;=\; \begin{pmatrix} ac-\bar{b}d & -a\bar{d}-\bar{b}\bar{c} \\ bc+\bar{a}d & -b\bar{d}+\bar{a}\bar{c} \end{pmatrix} \;=\; M(ac-\bar{b}d, bc+\bar{a}d)\,.$$

Par ailleurs, pour tous $a, b \in \mathbb{C}$, on a:

$$\det\Big(M(a,b)\Big) \;=\; |a|^2+|b|^2\,. \tag{7}$$

Il en résulte que, si $M \in \mathbb{H}$ n'est pas nulle, M appartient à $\mathrm{GL}_2(\mathbb{C})$. De plus, pour tout $(a,b) \in \mathbb{C}^2 \setminus \{(0,0)\}$, on a:

$$M(a,b)^{-1} \;=\; \frac{1}{|a|^2+|b|^2} \begin{pmatrix} \bar{a} & \bar{b} \\ -b & a \end{pmatrix} \;=\; M(a',b')\,,$$

en posant $a' = \bar{a}/(|a|^2+|b|^2)$ et $b' = -b/(|a|^2+|b|^2)$. Ainsi l'inverse, dans $M_2(\mathbb{C})$, de tout élément non nul de $\mathbb{H}$ appartient à $\mathbb{H}$, et donc $\mathbb{H}$, en tant que sous-anneau de $M_2(\mathbb{C})$, est un corps. Noter que, si $M \in \mathbb{H}^*$, les calculs ci-dessus donnent, en notant M^* la transconjuguée de M, i.e. la transposée de la conjuguée de M (ou la conjuguée de la transposée de M):

$$M^{-1} \;=\; \frac{1}{\det(M)}\, M^*\,.$$

Considérons maintenant les trois matrices suivantes, appartenant à $\mathbb{H}$:

$$I \;=\; \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = M(0,1)\;,\quad J \;=\; \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = M(i,0)\;,\quad K \;=\; \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = M(0,i)\,.$$

Remarquons d'abord que, si M est l'une des matrices I, J, K, $M^* = -M$, i.e. M est antihermitienne; ensuite $M^2 = -I_2$, comme le montre un calcul direct ou l'application du théorème de Caylay-Hamilton (M est de trace nulle et de déterminant 1).

On constate que $IJ = K$. Alors $-K = K^* = (IJ)^* = J^*I^* = JI$, et l'on en déduit successivement $JK = J(IJ) = (JI)J = (-IJ)J = -IJ^2 = I$, puis $KJ = (JK)^* = -I$, de même $KI = (IJ)I = -(JI)I = -JI^2 = J$ et $IK = (KI)^* = J^* = -J$. Ainsi les matrices $I_2, I, J, K \in \mathbb{H}$ vérifient les égalités (1) et (2), dans lesquelles on remplace $1, i, j, k$ par I_2, I, J, K respectivement. Par ailleurs, $\mathbb{H}$ est une sous-$\mathbb{R}$-algèbre de dimension 4 de $M_2(\mathbb{C})$, car elle est isomorphe (comme $\mathbb{R}$-algèbre) à $\mathbb{C}^2$. On vérifie de plus que (I_2, I, J, K) est une $\mathbb{R}$-base de $\mathbb{H}$. Au total, les deux constructions de $\mathbb{H}$ sont les mêmes: d'une part, si $q = a + bi + cj + dk$ est un quaternion ($a, b, c, d \in \mathbb{R}$), on identifie q à la matrice:

$$aI_2 + bI + cJ + dK \;=\; \begin{pmatrix} a+ic & -b+id \\ b+id & a-ic \end{pmatrix} \;=\; M(a+ic, b+id)\,.$$

En sens inverse, si $(\alpha, \beta) \in \mathbb{C}^2$, la matrice $M(\alpha,\beta)$ est identifiée au quaternion suivant:

$$q \;=\; \mathrm{Re}\,(\alpha) + \mathrm{Re}\,(\beta)i + \mathrm{Im}\,(\alpha)j + \mathrm{Im}\,(\beta)k\,.$$

Dans cette identification, la conjugaison $q \mapsto \bar{q}$ qui a été définie dans la première construction de $\mathbb{H}$ correspond matriciellement à l'application $M \mapsto M^*$. En particulier, les quaternions purs correspondent aux matrices appartenant à $\mathbb{H}$ dont la trace est imaginaire pure, i.e. aux matrices $M(a,b)$, où $b \in \mathbb{C}$ et $a \in i\,\mathbb{R}$.

Cette deuxième construction offre un avantage évident: l'associativité de la multiplication de $\mathbb{H}$ résulte de l'associativité de la multiplication dans $M_2(\mathbb{C})$. Retenons aussi la formule suivante, valable pour toute matrice $M \in \mathbb{H}$:

$$\det(M) \;=\; |M|^2\,.$$

Troisième construction

Notons ici E l'espace vectoriel euclidien standard $\mathbb{R}^3$. Orientons E à l'aide de la base canonique (i,j,k), qui est orthonormée. Si (u,v,w) est une base orthonormée de E, le déterminant de (u,v,w) dans la base (i,j,k) vaut ± 1 (parce que la matrice de passage de la base (i,j,k) à la base (u,v,w) est orthogonale, donc de déterminant ± 1). Ainsi ce déterminant vaut 1 si (u,v,w) est une base orthonormée directe et -1 sinon.

Nous noterons $(u|v)$ le produit scalaire de deux vecteurs de E et $||u||$ la norme d'un vecteur de E: $||u|| = (u|u)^{1/2}$.

Puisque E est un espace vectoriel euclidien orienté de dimension 3, on sait définir le *produit vectoriel* de deux vecteurs de E. Rappelons ce dont il s'agit. Tout d'abord, de façon explicite,

$$u \wedge u' = \begin{pmatrix} yz' - y'z \\ zx' - z'x \\ xy' - x'y \end{pmatrix} \quad \text{si} \quad u \;=\; \begin{pmatrix} x \\ y \\ z \end{pmatrix}\;,\quad u' \;=\; \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}\;.$$

En particulier, on a:

$$i \wedge j \;=\; k\;,\quad j \wedge k \;=\; i\;,\quad k \wedge i \;=\; j\,. \tag{8}$$

Une définition plus conceptuelle est la suivante. Rappelons que, si $u,v,w \in E$, le *produit mixte* $[u,v,w]$ de u,v,w est le déterminant de (u,v,w) dans n'importe quelle base orthonormée directe de E, par exemple (i,j,k). Cela étant, soient $u,v \in E$. Le vecteur $u \wedge v$ est le seul vecteur de E vérifiant la condition ci-dessous:

$$(u \wedge v|w) \;=\; [u,v,w] \;\text{ pour tout } w \in E\,.$$

Si $u,v \in E$, on a $v \wedge u = -(u \wedge v)$, et $u \wedge v = 0$ si et seulement si u,v sont colinéaires. Dans le cas contraire, $u \wedge v$ est un vecteur directeur de la droite orthogonale $P^\perp$, où $P = \mathrm{Vect}(u,v)$ est le plan engendré par u et v.

Notons ici $\mathbb{H}$ l'espace vectoriel réel $\mathbb{R} \times E$. On définit une multiplication $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$ comme suit: si $\lambda,\mu \in \mathbb{R}$ et $u,v \in E$, on pose:

$$(\lambda,u)(\mu,v) \;=\; \Big(\lambda\mu - (u|v),\, \lambda v + \mu u + u \wedge v\Big)\,. \tag{9}$$

La multiplication de $\mathbb{H}$ utilise donc le produit scalaire et le produit vectoriel sur E. Il est immédiat que cette multiplication est $\mathbb{R}$-bilinéaire: cela vient essentiellement de la $\mathbb{R}$-bilinéarité du produit scalaire et du produit vectoriel.

Lemme 4. *Pour tous vecteurs $u, v, w \in E$, on a la formule du double produit vectoriel suivante:*

$$(u \wedge v) \wedge w \;=\; (u|w)v - (v|w)u\,. \tag{10}$$

Démonstration. Chacun des deux membres est trilinéaire en u, v, w, il suffit de faire la démonstration lorsque $u, v, w \in \{i, j, k\}$. Lorsque w est fixé, chacun des deux membres est une forme bilinéaire alternée en u, v. Compte tenu des formules (8), on peut se limiter au cas où $u = i$ et $v = j$, la formule à vérifier s'écrivant alors: $k \wedge w = (i|w)j - (j|w)i$. Si $w = ai + bj + ck$, où $a, b, c \in \mathbb{R}$, il vient $k \wedge w = a(k \wedge i) + b(k \wedge j) = -bi + aj$, et par ailleurs $(i|w) = a,\ (j|w) = b$, d'où la conclusion.

cqfd

Lemme 5. *La multiplication de $\mathbb{H}$, définie par la formule (9), est associative.*

Démonstration. Soient $\lambda, \mu, \nu \in E$ et $u, v, w \in E$. On a:

$$\Big((\lambda, u)(\mu, v)\Big)(\nu, w) = \Big(\lambda\mu - (u|v),\ \lambda v + \mu u + u \wedge v\Big)(\nu, w)$$

$$= \Big(\lambda\mu\nu - \nu(u|v) - (\lambda v + \mu u + u \wedge v|w),\ \lambda\mu w - (u|v)w + \lambda\nu v + \mu\nu u + \nu(u \wedge v) + (\lambda v + \mu u + u \wedge v) \wedge w\Big)\,.$$

De même,

$$(\lambda, u)\Big((\mu, v)(\nu, w)\Big) \;=\; (\lambda, u)\Big(\mu\nu - (v|w),\ \mu w + \nu v + v \wedge w\Big)$$

$$= \Big(\lambda\mu\nu - \lambda(v|w) - (u|\mu w + \nu v + v \wedge w),\ \lambda(\mu w + \nu v + v \wedge w) + \mu\nu u - (v|w)u + u \wedge (\mu w + \nu v + v \wedge w)\Big)\,.$$

La conclusion résulte alors des formules suivantes:

$$((u \wedge v)|w) \;=\; [u, v, w] \;=\; [v, w, u] \;=\; ((v \wedge w)|u) \;= (u|(v \wedge w)) \;\text{ et}$$

$$(u \wedge v) \wedge w - (u|v)w \;=\; u \wedge (v \wedge w) - (v|w)u\,.$$

Vu la formule du double produit vectoriel, les deux membres de l'égalité précédente valent:

$$(u|w)v - (u|v)w - (v|w)u\,.$$

cqfd

Ainsi $\mathbb{H}$ est à nouveau une $\mathbb{R}$-algèbre, dont l'élément neutre multiplicatif est $(1,0)$. Un cas particulier important de la formule (9) est celui où $\lambda = \mu = 0$: si $u, v \in E$, on a:

$$(0,u)(0,v) \;=\; (-(u|v),\, u \wedge v)\,. \tag{11}$$

On en déduit, en échangeant les rôles de u et v:

$$(0,u)(0,v) + (0,v)(0,u) \;=\; (-2(u|v),0)\;,\quad (0,u)(0,v) - (0,v)(0,u) \;=\; ((0,2(u \wedge v))\,.$$

Ainsi u, v sont orthogonaux si et seulement si les éléments $(0,u)$ et $(0,v)$ de $\mathbb{H}$ anticommutent. Par ailleurs, en prenant $v = u$, on obtient la formule suivante, valable pour tout $u \in E$:

$$(0,u)^2 \;=\; (-||u||^2, 0)\,. \tag{12}$$

Il est facile de retrouver la première construction de $\mathbb{H}$: les vecteurs $(1,0), (0,i), (0,j), (0,k)$ forment une base de $\mathbb{H} = \mathbb{R} \times E$ sur $\mathbb{R}$, il suffit de les identifier aux quaternions $1, i, j, k$ respectivement. On retrouve alors les formules (1) et (2), à cause des formules (8), (11) et (12). Une fois cette identification faite on a, pour tous $u, v \in E$:

$$uv \;=\; -(u|v) + u \wedge v \;\text{ et }\; u^2 \;=\; -||u||^2\,. \tag{13}$$

Les quaternions purs sont simplement les vecteurs de E, plus précisément, pour tout quaternion q écrit sous la forme $q = a + u$ où $a \in \mathbb{R}$ et $u \in E$, on a:

$$\bar{q} \;= a - u\,. \tag{14}$$

Rappelons que, comme espace vectoriel réel, $\mathbb{H} = \mathbb{R}^4$ a été muni de sa structure usuelle d'espace vectoriel euclidien. Vu l'identification ci-dessus, on peut écrire, de façon un peu abusive, $\mathbb{H} = \mathbb{R} \oplus E$. En outre, E est l'orthogonal de $\mathbb{R}$ dans $\mathbb{H}$. Pour tout quaternion $q = a + u$, où $a \in \mathbb{R}$ et $u \in E$, on a:

$$|q|^2 \;=\; ||q||^2 \;=\; a^2 + ||u||^2 \;=\; a^2 - u^2\,. \tag{15}$$

Considérons un second quaternion $r = b + v$, où $b \in \mathbb{R}$ et $v \in E$. Dans la première construction, on a vu que $|qr| = |q|\,|r|$. En particulier, si $a = b = 0$, il vient, compte tenu de la formule (9):

$$||u||^2\,||v||^2 \;=\; (u|v)^2 + ||u \wedge v||^2\,. \tag{16}$$

C'est là un cas particulier d'une formule de Lagrange. La formule de Lagrange générale s'obtient en exprimant la multiplicativité du module pour deux quaternions $q = a + bi + cj + dk$ et $q' = a' + b'i + c'j + d'k$. Compte tenu des formules (1) et (2), il vient:

$$(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) \;=$$

$$(aa' - bb' - cc' - dd')^2 + (ab' + ba' + cd' - dc')^2 + (ac' + ca' - bd' + db')^2 + (ad' + da' + bc' - cb')^2\,.$$

La formule (16) est le cas particulier $a = a' = 0$. Une application classique de la formule de Lagrange est la suivante: si deux entiers sont sommes de quatre carrés (d'entiers), leur produit

l'est aussi. D'une certaine manière, que nous ne détaillons pas ici, $\mathbb{H}$ joue pour le «théorème des quatre carrés» le même rôle que joue $\mathbb{C}$ pour le «théorème des deux carrés». Pour plus de détails sur une preuve du théorème des quatre carrés à l'aide des quaternions, voir par exemple «Théorie algébrique des nombres», de P. Samuel.

Quaternions et rotations de l'espace

Notons ici $\mathrm{Aut}(\mathbb{H})$ le groupe des automorphismes de la $\mathbb{R}$-algèbre $\mathbb{H}$. Ce groupe contient en particulier les *automorphismes intérieurs* de $\mathbb{H}$. Plus précisément, soit $q \in \mathbb{H}^*$. L'application $\omega_q : t \mapsto qtq^{-1}$ de $\mathbb{H}$ dans $\mathbb{H}$ est un élément de $\mathrm{Aut}(\mathbb{H})$, appelé automorphisme intérieur défini par q (ou conjugaison par q). Si $q, q' \in \mathbb{H}^*$, on a aussitôt $\omega_{qq'} = \omega_q \circ \omega_{q'}$, autrement dit $\omega : q \mapsto \omega_q$ est un morphisme de groupes du groupe multiplicatif $\mathbb{H}^*$ dans $\mathrm{Aut}(\mathbb{H})$.

Le noyau de ω est évidemment $\mathbb{R}^*$. Soit en effet $q \in \mathbb{H}^*$. Pour que ω_q soit égal à l'identité, il faut et il suffit que $qtq^{-1} = t$, soit $qt = tq$, pour tout $t \in \mathbb{H}$, ce qui revient à dire que q appartient au centre de $\mathbb{H}$, qui n'est autre que $\mathbb{R}$ (théorème 1).

Lemme 6. *Pour tout $q \in \mathbb{H}^*$, ω_q est une transformation orthogonale de l'espace euclidien $\mathbb{H} = \mathbb{R}^4$.*

Démonstration. C'est une conséquence immédiate de la multiplicativité de la norme (module): pour tous $t \in \mathbb{H}$ et $q \in \mathbb{H}^*$, on a $1 = |qq^{-1}| = |q||q^{-1}|$, d'où $|q^{-1}| = |q|^{-1}$, puis

$$|\omega_q(t)| \;=\; |qtq^{-1}| \;=\; |q|\,|t|\,|q^{-1}| \;=\; |q|\,|t|\,|q|^{-1} \;=\; |t|\,.$$

Dans $\mathbb{R}^4$, la droite $\mathbb{R}$ et l'espace E sont orthogonaux l'un de l'autre. Si $q \in \mathbb{H}^*$, ω_q est une transformation orthogonale de $\mathbb{R}^4$ laissant stable $\mathbb{R}$, puisque $\omega_q(1) = q1q^{-1} = 1$. Il en résulte que ω_q laisse stable E, donc induit une transormation orthogonale de E, que nous noterons θ'_q. En notant $\mathrm{O}(E)$ le groupe orthonal de E, on obtient ainsi un morphisme de groupes $\theta' : q \mapsto \theta'_q$ de $\mathbb{H}^*$ dans $\mathrm{O}(E)$. Le noyau de θ' est toujours $\mathbb{R}^*$, car chaque ω_q induit l'identité sur $\mathbb{R}$.

Considérons les quaternions de module 1. Puisque $q \mapsto |q|$ est un morphisme de groupes multiplicatifs de $\mathbb{H}^*$ dans $\mathbb{R}^*$, ces quaternions de module 1 forment un sous-groupe (distingué) de $\mathbb{H}^*$. En fait, si $q = a + bi + cj + dk \in \mathbb{H}$, on a $|q|^2 = a^2 + b^2 + c^2 + d^2$. Ainsi q est de module 1 si et seulement si $a^2 + b^2 + c^2 + d^2 = 1$, i.e. si (a, b, c, d) appartient à la sphère unité S^3 de $\mathbb{R}^4$. Nous identifierons donc désormais le groupe des quaternions de module 1 à S^3. Enfin, nous noterons $\theta : S^3 \to \mathrm{O}(E)$ la restriction de θ' à S^3.

Proposition 1. *Le noyau de θ est $\{-1, 1\}$. L'image de θ est le sous-groupe $SO(E)$ des* rotations *de E (transformations orthogonales de déterminant 1). De plus, θ est continu.*

Démonstration. Soient $q \in \mathbb{H}$ et $t \in E$, autrement dit $\bar{t} = -t$. Vérifions que $qt\bar{q} \in E$:

$$\overline{qt\bar{q}} \;=\; q\bar{t}\bar{q} = -(qt\bar{q})\,.$$

L'application $(q,t) \mapsto qt\bar{q}$ de $\mathbb{H} \times E$ dans E est $\mathbb{R}$-bilinéaire, elle est donc continue (on est en dimension finie). Il en résulte que l'application de $\mathbb{H}$ dans $M_3(\mathbb{R})$ associant à tout quaternion q la matrice de $(qi\bar{q}, qj\bar{q}, qk\bar{q})$ dans la base (i,j,k) est continue, ce qui montre que l'application $q \mapsto (t \mapsto qt\bar{q})$ de $\mathbb{H}$ dans $L(E)$ est continue. Par ailleurs, si $q \in S^3$ et $t \in E$, on a, vu la formule (6), $\theta_q(t) = qt\bar{q}$, ce qui montre que $\theta : S^3 \to \mathrm{O}(E)$ est continu (la topologie de $\mathrm{O}(E)$ est induite par la topologie naturelle de $L(E)$).

L'application $q \mapsto \det(\theta_q)$ de S^3 dans $\mathbb{R}^*$ est continue, et elle prend ses valeurs dans $\{-1,1\}$. Comme la sphère S^3 est connexe, son image par θ l'est aussi, ce qui prouve l'inclusion $\theta(S^3) \subset \mathrm{SO}(E)$. Quant au noyau de θ, c'est l'intersection de S^3 avec $\mathbb{R}^*$, c'est bien $\{-1,1\}$.

Il reste à prouver l'inclusion $\mathrm{SO}(E) \subset \theta(S^3)$. Considérons pour cela un vecteur unitaire arbitraire $u \in E$: $||u|| = 1$. L'image de u par θ est une rotation non triviale r de E, nous allons montrer que c'est la symétrie orthogonale de E par rapport à la droite $D = \mathbb{R}u$ (demi-tour d'axe D). Puisque $u^2 = -1$ appartient au noyau de θ, r^2 est l'identité, i.e. r est un élément d'ordre 2 de $\mathrm{SO}(E)$. On sait alors que r est la symétrie orthogonale par rapport à une certaine droite vectorielle D' de E, à savoir le noyau de $r - \mathrm{id}_E$. Mais $\theta_u(u) = uuu^{-1} = u$, donc $u \in D'$, d'où $D' = D$, comme désiré.

Ce qui précède montre que $\theta(S^3)$ contient la symétrie orthogonale par rapport à n'importe quelle droite de E. Or on sait que ces symétries engendrent le groupe $\mathrm{SO}(E)$, ce qui démontre l'inclusion $\mathrm{SO}(E) \subset \theta(S^3)$.

cqfd

Compte tenu du théorème d'isomorphisme, θ induit un isomorphisme de groupes Θ de $S^3/\mathrm{Ker}(f) = S^3/\{-1,1\}$ sur $\mathrm{SO}(E)$. Munissons $S^3/\{-1,1\}$ de la topologie quotient de celle de S^3. Alors:

Proposition 2. *En fait Θ est un homéomorphisme, i.e. un isomorphisme de groupes topologiques.*

Démonstration. Puisque $\mathrm{SO}(E)$ est compact, il suffit de montrer que $S^3/\{-1,1\}$ est un espace *séparé*. Modulo un lemme classique, cela revient à dire que $\{-1,1\}$ est un sous-groupe fermé de S^3. C'est évident, car $\{-1,1\}$ est fini, en particulier compact.

Revenons aux rotations de $E = \mathbb{R}^3$, qui est un espace vectoriel euclidien orienté de dimension 3. Soit r une rotation non triviale de E, i.e. un élément non trivial de $\mathrm{SO}(E)$. On sait que $D = \mathrm{Ker}(r - \mathrm{id}_E)$ est une droite vectorielle de E, qu'on pourrait appeler axe de r. En fait le mot axe a en général un sens un peu différent. Choisissons un des deux vecteurs unitaires dirigeant D, notons-le u. Soit $P = D^\perp = u^\perp$ le plan orthogonal à D, et soit $v \in P$ un vecteur unitaire quelconque; posons enfin $w = u \wedge v$, de sorte que (u,v,w) est une base orthonormée directe de E. La rotation r laisse fixe u, elle laisse donc stable P. La restriction de r à P est donc une rotation non triviale du plan P, orienté par la base orthonormée (v,w). Notons $\alpha \in \mathbb{R}$ une mesure de l'angle de cette rotation. Nous dirons que r est la rotation ayant pour axe $\mathbb{R}_+u$ et pour angle α.

La matrice de r dans la base (u, v, w) est:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix} .$$

En particulier, $\mathrm{tr}\,(r) = 1 + 2\cos\alpha$.

Un problème naturel se pose: soit $q \in S^3$, $q \neq \pm 1$. Nous savons que $r = \theta_q$ est une rotation non triviale de E. Comment déterminer l'axe et l'angle de cette rotation? Voici la réponse:

Proposition 3. *Soit $q \in S^3$ un quaternion de module 1, distinct de ± 1. Écrivons $q = a + x$, où $a \in \mathbb{R}$ et $x \in E$. Alors θ_q est la rotation de E ayant pour axe $\mathbb{R}_+ x$ et pour angle $2\arccos(a)$.*

Démonstration. Puisque $q \neq \pm 1$ et $|q| = 1$, on a $x \neq 0$ et donc $|a| < 1$. Ensuite x commute avec lui-même et avec a, donc avec $q = a + x$, i.e. $\theta_q(x) = x$. D'où $\mathrm{Ker}(r - \mathrm{id}_E) = \mathbb{R}x$. Il existe donc, modulo 2π, un unique α tel que θ_q soit la rotation ayant pour axe $\mathbb{R}_+ x$ et pour angle α. Voyons comment déterminer α.

Soit (u, v, w) une base orthonormée directe de E telle que $u = x/||x||$. On a:

$$\theta_q(v) \;=\; qv\bar{q} \;= (a + x)v(a - x) \;=\; a^2 v + a(xv - vx) - xvx\,.$$

Nous avons vu page 6 que $xv - vx = 2(x \wedge v) = 2||x||(u \wedge v) = 2||x||w$. Par ailleurs,

$$-xvx \;= xv\bar{x} \;=\; ||x||^2(uv\bar{u}) \;=\; ||x||^2\theta_u(v)\,.$$

Mais, comme nous l'avons vu dans la preuve de la proposition 1, θ_u est le demi-tour d'axe $\mathbb{R}u$, de sorte que $\theta_u(v) = -v$, puisque $(u|v) = 0$. Nous obtenons:

$$\theta_q(v) \;=\; (a^2 - ||x||^2)v + 2a||x||w\,.$$

Posons alors $t = \arccos(a) \in]0, \pi[$. Ainsi $\cos t = a$ et $\sin t = \sqrt{1 - a^2}$. Comme $a^2 + ||x||^2 = 1$, on a $a^2 - ||x||^2 = 2a^2 - 1 = \cos(2t)$ et $2a||x|| = 2\cos t \sin t = \sin(2t)$. D'où:

$$\theta_q(v) \;=\; \cos(2t)v + \sin(2t)w\,.$$

Cela montre que la restriction de θ_q au plan orthogonal à x est la rotation d'angle (de mesure) $2\arccos(a)$, d'où la conclusion.

cqfd

Remarque. À l'aide de la proposition 2, le calcul de la composée de deux rotations de l'espace peut se ramener à la multiplication de deux quaternions. Soient par exemple r la rotation d'axe Ox d'angle $\pi/2$ et r' la rotation d'axe Oy d'angle $\pi/2$. Explicitons la composée $r \circ r'$. La proposition 2 montre que $r = \theta_q$ et $r' = \theta_{q'}$, en posant:

$$q \;=\; \frac{\sqrt{2}}{2}\,(1 + i) \quad \text{et} \quad q' \;=\; \frac{\sqrt{2}}{2}\,(1 + j)\;.$$

Comme $ij = i \wedge j = k$, on a $qq' = \frac{1}{2}(1 + i + j + k)$. La proposition 2 montre alors que $r \circ r'$ est la rotation d'axe $\mathbb{R}_+(i + j + k)$ et d'angle $2\pi/3$.

Caractérisation algébrique des quaternions

Le principal résultat que nous avons en vue est le théorème suivant, dû à Frobenius:

Théorème 2. *À isomorphisme près, il n'y a que trois $\mathbb{R}$-algèbres de dimension finie qui sont des corps, à savoir $\mathbb{R}, \mathbb{C}$ et $\mathbb{H}$.*

Démonstration. Soit donc K une $\mathbb{R}$-algèbre de dimension finie qui soit un corps. Comme d'habitude, chaque réel a est identifié à $a.1_K \in K$, de sorte que $\mathbb{R}$ est considéré comme sous-corps de K. Par définition d'une algèbre, $\mathbb{R}$ est contenu dans le centre de K (qui est un sous-corps de K). Supposons désormais $K \neq \mathbb{R}$.

a) Soit $x \in K$, supposons que $x^2 \in \mathbb{R}_+$. Il existe donc un réel a tel que $x^2 = a^2$, et alors $0 = x^2 - a^2 = (x + a)(x - a)$, donc $x = \pm a \in \mathbb{R}$, puisque K est intègre. Ce raisonnement ne marche pas lorsque x^2 est un nombre réel strictement négatif. Nous poserons en fait:

$$V \;=\; \{x \in K \mid x^2 \in \mathbb{R}_-\}\,.$$

b) Soit $x \in K \setminus \mathbb{R}$, considérons la sous-algèbre $\mathbb{R}[x]$ de K engendrée par x, c'est l'image de $\mathbb{R}[X]$ par le morphisme de substitution de x à X. En particulier $\mathbb{R}[x]$ est commutative et contient strictement $\mathbb{R}$. Puisque $\mathbb{R}[x]$ est une $\mathbb{R}$-algèbre intègre de dimension finie, c'est un corps (argument classique), c'est donc une extension de $\mathbb{R}$, de degré fini > 1. Il résulte du théorème de d'Alembert-Gauss que $\mathbb{R}[x]$ est isomorphe (comme $\mathbb{R}$-algèbre, donc comme corps) à $\mathbb{C}$. Dans $\mathbb{C}$, les éléments dont le carré est un réel négatif forment une droite vectorielle réelle, à savoir $\mathbb{R}i$. On en déduit que $V \cap \mathbb{R}[x]$ est une droite réelle, elle contient exactement deux vecteurs (opposés) dont le carré vaut -1.

Soit maintenant $y \in K$ un élément commutant avec x. Montrons que $y \in \mathbb{R}[x]$. La sous-algèbre $\mathbb{R}[x, y]$ de K engendrée par x et y est encore une extension finie de $\mathbb{R}$, contenant $\mathbb{C}$, d'où $\mathbb{R}[x, y] = \mathbb{R}[x]$, toujours à cause du théorème de d'Alembert-Gauss. Notre assertion en résulte. Ainsi, pour tout $x \in K \setminus \mathbb{R}$, on a:

$$\mathbb{R}[x] \;=\; \{y \in K \mid xy = yx\}\,.$$

c) Montrons que V est un sous-$\mathbb{R}$-espace vectoriel de K. Il est clair que $\lambda x \in V$ dès que $x \in V$ et $\lambda \in \mathbb{R}$. Il suffit donc de montrer que, si $x, y \in V$ sont linéairement indépendants, $x+y$ appartient à V. Puisque $x \pm y \notin \mathbb{R}$, l'alinéa b) prouve l'existence de nombres réels a, b, c, d tels que

$$(x+y)^2 = a(x+y)+b\,,\;\; (x-y)^2 = c(x-y)+d\,,\;\; \text{d'où}\;\; (a+c)x+(a-c)y+(b+d-2x^2-2y^2) = 0\,.$$

Or $x, y, 1$ sont linéairement indépendants sur $\mathbb{R}$: dans le cas contraire, y appartiendrait à $\mathbb{R} + \mathbb{R}x = \mathbb{R}[x]$, donc à $\mathbb{R}[x] \cap V = \mathbb{R}x$, toujours en vertu de b). L'égalité ci-dessus montre

alors que $a = c = 0$, d'où $(x+y)^2 = b \in \mathbb{R}$. Comme $x + y \notin \mathbb{R}$, b est strictement négatif, et donc $x + y \in V$.

Notons maintenant que $K = \mathbb{R} \oplus V$. D'abord, si $x \in V \cap \mathbb{R}$, on a $x^2 \in \mathbb{R}_+ \cap \mathbb{R}_- = \{0\}$. Soit ensuite $x \in K \setminus \mathbb{R}$. D'après b), $\mathbb{R}[x] = \mathbb{R} \oplus \mathbb{R}x$ est de dimension 2, et $\mathbb{R}[x] \cap V$ est une droite, soit t un vecteur directeur de cette droite. Il existe $a, b \in \mathbb{R}$ tels que $t = a + bx$, et $b \neq 0$ car $t \notin \mathbb{R}$. D'où $x \in \mathbb{R} + \mathbb{R}t \subset \mathbb{R} + V$.

d) Pour tout $x \in V$, posons $q(x) = -x^2 \in \mathbb{R}_+$. Pour tous $x, y \in V$, posons:

$$(x|y) \;=\; \frac{1}{2}\Big[q(x+y) - q(x) - q(y)\Big] \;=\; \frac{-1}{2}\Big[xy + yx\Big] \in \mathbb{R}\,.$$

L'application $(x, y) \mapsto (x|y)$ de $V \times V$ dans $\mathbb{R}$ est $\mathbb{R}$-bilinéaire symétrique, donc q est une forme quadratique sur le $\mathbb{R}$-espace vectoriel V. En outre, si $x \in V$ n'est pas nul, $q(x) \neq 0$, i.e. $q(x) > 0$, donc q est définie positive. Autrement dit, $(x, y) \mapsto (x|y)$ est un produit scalaire sur V, i.e. V (muni de q) est un espace vectoriel euclidien.

Observons que deux vecteurs x, y de V sont orthogonaux si et seulement s'ils anticommutent, i.e. si $xy + yx = 0$. En outre $x \in V$ est unitaire si et seulement si $x^2 = -1$.

e) Si $\dim(V) = 1$, i.e. si K est de dimension 2 sur $\mathbb{R}$, l'alinéa b) montre que K est isomorphe à $\mathbb{C}$ comme $\mathbb{R}$-algèbre. Supposons donc $\dim(V) > 1$. Soient $i, j \in V$ deux vecteurs unitaires orthogonaux. On a donc $i^2 = j^2 = -1$ et $ij + ji = 0$. Posons $k = ij \in K$. Alors:

$$k^2 \;=\; (ij)(ij) \;=\; i(ji)j \;=\; -i(ij)j \;=\; -i^2j^2 \;=\; -1\,,$$

donc k est un vecteur unitaire de V. De plus $ki = (ij)i = -(ji)i = -ji^2 = j$ et $ik = i(ij) = -j$, donc $ki + ik = 0$: k est orthogonal à i. De même $kj = (ij)j = -i$ et $jk = j(ij) = -j(ji) = i$, donc $jk + kj = 0$: k est orthogonal à j. Ainsi (i, j, k) est une famille orthonormée de V, en particulier cette famille est libre. Les éléments $1, i, j, k$ de K vérifient les égalités (1) et (2), donc engendrent une sous-$\mathbb{R}$-algèbre de K isomorphe à $\mathbb{H}$. En d'autres termes, nous pouvons désormais supposer que K contient $\mathbb{H}$.

Pour conclure, il suffit maintenant de montrer que $K = \mathbb{H}$. Supposons que ce ne soit pas le cas. Alors $\dim(V) > 3$, de sorte qu'il existe un vecteur unitaire u de V orthogonal à i, j, k. Dans ces conditions, il vient: $ui = u(jk) = -(ju)k = j(ku) = (jk)u = ik$, i.e. u commute avec i. D'après l'alinéa b), $u \in \mathbb{R}[i]$, donc $u \in \mathbb{R}[i] \cap V = \mathbb{R}i$, ce qui est absurde puisque u est non nul et orthogonal à i. Cette contradiction achève la démonstration du théorème.

cqfd

Signalons sans démonstration un théorème dû à Gelfand-Mazur et généralisant le théorème de Frobenius:

Théorème 3. *Soit K une $\mathbb{R}$-algèbre normée qui soit un corps. Alors K est isomorphe à $\mathbb{R}, \mathbb{C}$ ou $\mathbb{H}$.*

Dire que K est une $\mathbb{R}$-algèbre normée signifie que K est muni d'une norme vérifiant: $||xy|| \leq ||x||\,||y||$ pour tous $x, y \in K$. À titre d'exercice, le lecteur montrera que le théorème de Frobenius résulte du théorème de Gelfand-Mazur.

Terminons par un résultat algébrique sur $\mathbb{H}$:

Proposition 4. *Tout automorphisme du* corps $\mathbb{H}$ *est intérieur.*

Démonstration. Soit donc s un automorphisme du corps $\mathbb{H}$ (a priori, s n'est pas forcément $\mathbb{R}$-linéaire). Tout d'abord, puisque $\mathbb{R}$ est le centre de $\mathbb{H}$, on a $s(\mathbb{R}) = \mathbb{R}$. La restriction de s à $\mathbb{R}$ est donc un automorphisme du corps $\mathbb{R}$. On sait que le seul automorphisme du corps $\mathbb{R}$ est l'identité, et ainsi $s(a) = a$ pour tout $a \in \mathbb{R}$. Cela montre a posteriori que s est un automorphisme de la $\mathbb{R}$-algèbre $\mathbb{H}$, i.e. que s est $\mathbb{R}$-linéaire.

Soit $V = \mathrm{Vect}(i, j, k)$ l'espace des quaternions purs. En fait, comme on l'a vu dans la preuve du théorème de Frobenius, V est formé des $x \in \mathbb{H}$ tels que $x^2 \in \mathbb{R}_-$. Vu ce qui précède, $s(V) = V$. Soit f la restriction de s à V, c'est un automorphisme du $\mathbb{R}$-espace vectoriel V. De plus, si $x \in V$, $q(x) = -x^2 \in \mathbb{R}_+$, et $q(f(x)) = -s(x)^2 = s(-x^2) = -x^2 = q(x)$, de sorte que f est une transformation orthogonale de V (si l'on identifie V à $\mathbb{R}^3$ comme dans la première construction de $\mathbb{H}$, la structure euclidienne de V est la structure euclidienne usuelle de $\mathbb{R}^3$).

Ainsi $f \in \mathrm{O}(V)$. Supposons d'abord que $\det(f) = 1$, soit $f \in \mathrm{SO}(V)$. D'après la proposition 1, il existe un quaternion x de module 1 tel que $f = \theta_x$, c'est-à-dire $s(t) = xtx^{-1}$ pour tout $t \in V$. Cette égalité est aussi vraie lorsque $t \in \mathbb{R}$, donc $s(t) = xtx^{-1}$ pour tout $t \in \mathbb{H}$. Il en résulte que s est l'automorphisme intérieur de $\mathbb{H}$ défini par x.

Supposons maintenant que $\det(f) = -1$. Dans ce cas, $-f \in \mathrm{SO}(V)$. D'après la proposition 1, il existe un quaternion x de module 1 tel que $-f = \theta_x$, c'est-à-dire $s(t) = -xtx^{-1}$ pour tout $t \in V$. En particulier $s(i) = -xix^{-1}$, $s(j) = -xjx^{-1}$, et $s(k) = -xkx^{-1}$. Mais $ij = k$ et s est un automorphisme du corps $\mathbb{H}$, d'où:

$$-xkx^{-1} = s(k) = s(ij) = s(i)s(j) = [-xix^{-1}][-xjx^{-1}] = x(ij)x^{-1} = xkx^{-1}\,,$$

ce qui conduit à une contradiction.

cqfd