Le corps des Quaternions

Christian d'Elbée

7 mai 2014

Every morning in the early part of October 1843, on my coming down to breakfast,
your brother William Edward and yourself used to ask me :
"Well, Papa, can you multiply triples ?"
Whereto I was always obliged to reply, with a sad shake of the head,
"No, I can only add and subtract them."

W.Hamilton à son fils Archibald

Table des matières

Introduction

L'objet de ce mémoire est une description élémentaire du *corps des quaternions*, premier exemple historique de corps dans lequel la multiplication n'est pas commutative, parfois appelé *corps gauche* ou *algèbre à division*. Il fût construit par Hamilton [1] en 1843. L'idée d'Hamilton, comme on le verra dans la section 3, est de traduire par une multiplication les rotations de l'espace, comme le font les nombres complexes avec les rotations du plan. Après de nombreuses années à essayer de définir une structure de corps sur des triplets, il parvient à le faire sur des quadruplets, qu'il nomme alors *quaternions*. L'anecdote raconte que la table de multiplication appropriée (cf 1.1.1) lui est apparu alors qu'il se balladait avec sa femme le long du pont de Brougham à Dublin, où repose à présent une plaque à son éloge. Les quaternions trouvent des applications en physique quantique où ils sont utilisés pour traduire des rotations en prenant en compte le spin d'une particule. Les quaternions servent aussi en infographie, par exemple ils ont été utilisés pour modéliser les rotations dans le jeu video en 3D *Tomb Raider (1996)*.
L'étude mathématique des quaternions fait l'objet de ce mémoire. La première section est consacrée à l'étude théorique des quaternions. Nous commencerons par en donner une description purement algébrique, où l'on montrera que c'est un corps. Un fait remarquable, qui est l'objet de la sous-section 1.2 est que la dimension 4 est maximale en ce qui concerne les extensions (non necessairement commutatives) de degrés fini de $\mathbb{R}$. Nous terminerons cette première section par un exemple de corps non commutatif de dimension 9 sur $\mathbb{Q}$. La seconde section est consacrée à l'utilisation des quaternions dans le monde de l'arithmétique, où l'on verra en introduction comment les nombres complexes peuvent être utilisés pour démontrer le théorème des deux carrés, puis la preuve du théorème des quatre carrés de Lagrange, en considérant les quaternions d'Hurwitz, un sous-anneau euclidien des quaternions. Le lien étroit entre nombres complexes et quaternions apparaîtra une première fois. Nous conclurons cette section par un autre exemple de décomposition des nombres entiers utilisant un sous-anneau euclidien des quaternions à coefficients entiers. La troisième et dernière section est consacrée aux utilisations des quaternions dans la géométrie de $\mathbb{R}^3$ et de $\mathbb{R}^4$. On verra d'abord deux autres descriptions des quaternions avec des objets familiers, respectivement des matrices carrées de taille 2 à coefficients complexes et des vecteurs de $\mathbb{R} \times \mathbb{R}^3$ munis d'une multiplication utilisant les produits scalaires et vectoriels. Nous terminons cette section et le mémoire en explicitant des isomorphismes entre des groupes liés aux quaternions et les rotations de $\mathbb{R}^3$ et $\mathbb{R}^4$, faisant ainsi apparaître une deuxième analogie entre nombres complexes et quaternions.
On pourrait alors se demander sous quelles conditions une extension finie stricte des quaternions pourrait exister. Il s'avère que si l'on fait fi de l'associativité, il existe une extension de degré 8, l'algèbre des *octonions*, découverte en 1843 par John T. Graves, un ami de William Hamilton. Citons aussi pour la culture l'algèbre des *sédénions*, de dimension 16 sur $\mathbb{R}$, dont tout élément non nul est inversible, mais contrairement aux octonions, n'a pas la propriété d'être alternative [2] ; de plus elle n'est même pas intègre.

1. William Rowan Hamilton (1805-1865) est un mathématicien physicien et astrophysicien irlandais qui est connu pour ses travaux en mécanique, optique et algèbre.
2. Une multiplication est alternative si $x(xy) = (xx)y$. C'est une propriété plus faible que l'associativité.

Remerciements

J'adresse mes remerciements à mon superviseur J.-F. Jaulent pour ses conseils avisés et sa relecture attentive et pointilleuse. Je tiens aussi à remercier M. Matignon pour l'aide qu'il m'a apporté dans la compréhension de certaines subtilités, et ce malgré l'exaspération que lui causait mon désir d'élargir le champ d'investigation de ce mémoire au lieu de préparer convenablement mon agrégation.

1 Le corps des quaternions

1.1 Construction du corps des quaternions

Nous définissons ici les quaternions de façon formelle.

Definition 1.1.1. *On définit $\mathbb{H}$ comme le $\mathbb{R}$-espace vectoriel de dimension 4 de base $(1, i, j, k)$:*

$$\mathbb{H} \triangleq \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

que l'on muni d'une loi de composition binaire, définie comme une application bilinéaire telle que :

$$1 \text{ est l'unité}$$

$$ij = -ji = k \quad jk = -kj = i \quad ki = -ik = j$$

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

On identifiera en pratique $a1$ et a pour $a \in \mathbb{R}$. Le but de cette section est d'étudier la structure de cet espace vectoriel, en particulier, on va d'abord montrer que cet ensemble est bien muni d'une structure d'anneau.

Proposition 1.1.2. *La multiplication définie en 1.1.1 est associative.*

PREUVE : Il faut vérifier que pour tout $q, r, s \in \mathbb{H}$ on a $q(rs) = (qr)s$. Or la bilinéarité impliquant la distributivité et 1 commutant avec tous les éléments, on a juste à vérifier l'associativité des produits

$$(ab)c = a(bc) \tag{†}$$

avec $a, b, c \in \{i, j, k\}$. Cela fait donc $3^3 = 27$ équations à vérifier. On va essayer de réduire ce nombre. On définit l'application : $\sigma : \mathbb{H} \longrightarrow \mathbb{H}$ par $\sigma(1) = 1$, $\sigma(i) = j$, $\sigma(j) = k$ et $\sigma(k) = i$. Il vient alors que σ respecte la structure multiplicative définie sur $\mathbb{H}$ puisque la table de i, j, k est invariante par permutation circulaire.

Comme σ est un isomorphisme pour la structure d'espace vectoriel, c'est donc un automorphisme pour la structure (encore inconnue) définie sur $\mathbb{H}$. On a alors $(ab)c = a(bc)$ si et seulement si $(\sigma(a)\sigma(b))\sigma(c) = \sigma(a)(\sigma(b)\sigma(c))$. Ainsi, il suffit de fixer $a = i$ puis vérifier (†) pour $b \in \{i, j, k\}$ et $c \in \{i, j, k\}$. Ce qui fait plus que $3^2 = 9$ vérification. On peut faire mieux. On définit l'automorphisme τ pour la structure sur $\mathbb{H}$ par $\tau(i) = -i$, $\tau(j) = k$ et $\tau(k) = j$. On peut donc vérifier les produits dans (†) en ordonnant j et k, i.e

$\vec{\Gamma}$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

$\xrightarrow{\sigma}$

$\vec{\Gamma}$	j	k	i
j	-1	i	$-k$
k	$-i$	-1	j
i	k	$-j$	-1

uniquement vérifier lorsque l'on a le produit jk. Ainsi, à $a = i$ fixé et ne considérant que les produit jk et non les produits kj il faut vérifier

$$\begin{aligned} i^2 i &= ii^2 \ (= -i) \\ i^2 j &= i(ij) \ (= -j) \\ (ij)i &= i(ji) \ (= j) \\ (ij)j &= ij^2 \ (= -i) \\ (ij)k &= i(jk) \ (= -1) \end{aligned}$$

Ceci termine la preuve. □

L'espace des quaternions est donc muni d'une structure d'anneau. Il est de plus non commutatif. On introduit à présent les outils important pour l'étude des quaternions.

Definition 1.1.3. *Soit $q = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$ on définit le* conjugué de q

$$\bar{q} = a_0 - a_1 i - a_2 j - a_3 k$$

On dira qu'un quaternion $q \in \mathbb{H}$ vérifiant $q = \bar{q}$ est *réel* c'est clairement un élément de $\mathbb{R}1$. Si $\bar{q} = -q$ on dira que c'est un *quaternion pure*. On constate de plus que si q est un quaternion non réel alors il ne commute avec aucun des i, j, k. D'autre part, les réels commutent clairement avec tous les éléments de $\mathbb{H}$. On a donc montré que le centre de $\mathbb{H}$ est $\mathbb{R}1$, que l'on notera plus naturellement $\mathbb{R}$.

Proposition 1.1.4. *Soient $q, r \in \mathbb{H}$, alors on a*

- $\overline{q + r} = \bar{q} + \bar{r}$
- $\overline{qr} = \bar{r}\bar{q}$

Preuve : Le premier point est clair. Pour le deuxième point on le vérifie pour i, j, k et le résultat s'étendra sur $\mathbb{H}$ par distributivité. On vérifie donc $\overline{ij} = \bar{k} = -k = ji = (-j)(-i) = (\bar{j})(\bar{i})$ et de même $\overline{jk} = (\bar{k})(\bar{j})$, $\overline{ki} = (\bar{i})(\bar{k})$, $\overline{ik} = (\bar{k})(\bar{i})$, $\overline{kj} = (\bar{j})(\bar{k})$, $\overline{ji} = (\bar{i})(\bar{j})$; $\bar{i^2} = -1 = (-i)(-i) = (\bar{i})(\bar{i})$, $\bar{j^2} = (\bar{j})(\bar{j})$, $\bar{k^2} = (\bar{k})(\bar{k})$. Puis on a le résultat. □

On dit que $q \mapsto \bar{q}$ est un *anti-isomorphisme* de $\mathbb{H}$. On a en particulier pour $q = a_0 + a_1 i + a_2 j + a_3 k$

$$q \cdot \bar{q} = \bar{q} \cdot q = a_0^2 + a_1^2 + a_2^2 + a_3^2$$

donc $q \cdot \bar{q} \in \mathbb{R}$ pour tout $q \in \mathbb{H}$. On appelle alors *norme de q* noté $N(q)$ le nombre réel $q \cdot \bar{q}$. On a la proposition suivante :

Proposition 1.1.5. *La norme $N : \mathbb{H} \to \mathbb{R}^{\geq 0}$ est multiplicative, autrement dit*

$$N(qr) = N(q)N(r) \quad \forall q, r \in \mathbb{H}$$

De plus $N(q) = 0$ si et seulement si $q = 0$.

Preuve : On a pour $q, r \in \mathbb{H}$ $N(qr) = (qr)(\overline{qr}) = q \cdot r \cdot \bar{r} \cdot \bar{q} = q \cdot N(r) \cdot \bar{q}$ et comme $N(r) \in \mathbb{R}$, $N(r)$ commute avec tout quaternion, donc $N(qr) = N(q)N(r)$. On a clairement $N(0) = 0$. Maintenant si $N(a_0 + a_1 i + a_2 j + a_3 k) = 0 = a_0^2 + a_1^2 + a_2^2 + a_3^2$ on a bien $a_0 = a_1 = a_2 = a_3 = 0$, ce qui conclut la preuve. □

On peut alors conclure le théorème principal de cette introduction.

Théorème 1.1.6. *La structure définie en 1.1.1 fait de $\mathbb{H}$ un corps.*

Preuve : $\mathbb{H}$ est intègre car si $qr = 0$ alors $N(qr) = 0$ par la proposition précédente et donc $N(q)N(r) = 0$ puis par intégrité de $\mathbb{R}$ $N(q) = 0$ ou $N(r) = 0$ et donc $q = 0$ ou $r = 0$. Il reste a prouver que tout élément non nul est inversible. Si $q \neq 0$, alors $N(q) \neq 0$ et donc on peut définir $q' = \frac{\bar{q}}{N(q)}$ qui vérifie $qq' = 1$ donc on a bien trouvé un inverse *à droite*. Or $q \cdot \bar{q} = \bar{q} \cdot q$ donc q' est aussi un inverse *à gauche* et donc q est inversible. On conclut que $\mathbb{H}$ est un corps. □

1.2 Le théorème de Frobenius

L'objet que l'on a construit dans la section précédente peut se voir comme une extension du corps $\mathbb{R}$ qui contient même la clôture algébrique de $\mathbb{R}$. L'objet de cette section est de savoir si une extension non commutative de $\mathbb{R}$ peut être plus grande que de dimension 4 sur $\mathbb{R}$. La réponse négative à cette question est l'objet du théorème suivant.

Admettant que $\mathbb{C}$ soit algébriquement clos, comme $\mathbb{R} \subseteq \mathbb{C}$ il vient que $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$. De plus, on a que $\mathbb{R}$ n'admet pas d'extensions finie commutative contenant strictement $\mathbb{C}$ par la proposition suivante.

Proposition 1.2.1. *Soit K un corps, algébriquement clos, alors K est la seule extension finie commutative de K.*

PREUVE : Supposons que L soit une extension finie stricte de K et soit $\alpha \in L \setminus K$. Alors, α admet un polynôme annulateur dans $K[X]$ (la famille $1, \alpha, \alpha^2 ...$ est liée) et donc un polynôme minimal $m(X)$ irréductible et unitaire. Ainsi il vient l'isomorphisme $L \cong {K[X]}\Big/{< m >}$ avec $dim_K L = deg(m)$ mais comme K est algébriquement clos, $deg(m) = 1$ et donc $L \cong K$. □

Donc il vient que $\mathbb{C}$ est la seule extension finie commutative de $\mathbb{R}$ non triviale. On prouve à présent que si un corps gauche (i.e. non nécessairement commutatif) contient strictement $\mathbb{C}$ et est de dimension finie sur $\mathbb{R}$, alors sa dimension sur $\mathbb{R}$ n'excede pas 4, et il est isomorphe à $\mathbb{H}$.

Théorème 1.2.2 (Frobenius 1878)**.** *Tout corps gauche contenant $\mathbb{R}$ dans son centre et de degré fini sur $\mathbb{R}$ est isomorphe soit à $\mathbb{R}$ soit à $\mathbb{C}$, soit à $\mathbb{H}$.*

PREUVE : Soit L un corps contenant dans son centre $Z(L)$ le corps des nombres réels $\mathbb{R}$. On suppose L de degré fini sur $\mathbb{R}$ et commutative. Ainsi si c'est une extension de degré 1, on a $L = \mathbb{R}$ et sinon, c'est une extension de degré au moins deux et donc isomorphe à $\mathbb{C}$, par la proposition précédente.

On suppose à présent que L est non commutatif, et soit donc $\alpha \in L \setminus \mathbb{R}$ on a alors que $\mathbb{R}(\alpha)$ est un corps commutatif de dimension finie sur $\mathbb{R}$ et donc, par la proposition précédente, $\mathbb{R}(\alpha) \cong \mathbb{C}$. On a alors $e_1 \in \mathbb{R}(\alpha)$ de carré -1 (puisque $X^2 + 1 \in \mathbb{R}[X]$ est scindé dans $\mathbb{R}(\alpha)$) et ainsi $\mathbb{R}(e_1) \cong \mathbb{C}$ est un sous-corps commutatif maximal de L, puisque $\mathbb{R}(e_1)$ est algébriquement clos, c'est à dire que tout élément qui commute avec e_1 est dans $\mathbb{R}(e_1)$ puisque sinon, on pourrait construire une extension algébrique et donc commutative de $\mathbb{R}(e_1)$ qui serait non triviale.

Soit alors $\beta \in L \setminus \mathbb{R}(e_1)$ et $l \triangleq \beta e_1 - e_1 \beta$. On a $l \neq 0$ puisque $l \notin \mathbb{R}(e_1)$ et donc l ne commute pas avec e_1. On a alors $e_1 l = e_1 \beta e_1 + \beta$ et $l e_1 = -(e_1 \beta e_1 + e_1)$, donc

$$e_1 l = -l e_1 \qquad (\dagger)$$

Cela implique que l ne commute pas avec e_1 et donc $l \notin \mathbb{R}(e_1)$. Par conséquent $\mathbb{R}(l)$ et $\mathbb{R}(e_1)$ ne coincident pas. Or $\mathbb{R}(l)$ est une extension de degré 2 sur $\mathbb{R}$ puisque c'est une extension algébrique non triviale de $\mathbb{R}$ (en particulier $\mathbb{R}(l) \cong \mathbb{R}(e_1) \cong \mathbb{C}$). On a $\mathbb{R}(e_1) \cap \mathbb{R}(l) = \mathbb{R}$ puisque $l \notin \mathbb{R}(e_1)$. De plus $l^2 \in \mathbb{R}(e_1)$, en effet, de (†) vient que $e_1 l^2 = -l e_1 l$ et comme $-l e_1 = e_1 l$ on a

$$e_1 l^2 = l^2 e_1$$

donc l^2 commute avec tout element de $\mathbb{R}(e_1)$ donc il appartient à $\mathbb{R}(e_1)$ (sinon on pourrait construire une extension algébrique et donc commutative de $\mathbb{R}(e_1) \cong \mathbb{C}$, ce qui est absurde par la proposition précédente.). De plus $l^2 \in \mathbb{R}(l)$ et donc $l^2 \in \mathbb{R}(e_1) \cap \mathbb{R}(l) = \mathbb{R}$.
On montre à présent que $l^2 \in \mathbb{R}^{<0}$. Si $l^2 = a > 0$ on aurait que $l - \sqrt{a} \in L \setminus \{0\}$ et $l + \sqrt{a} \in L \setminus \{0\}$ (puisque

$l \notin \mathbb{R}$ et $\sqrt{a} \in \mathbb{R}$) et $(l+\sqrt{a})(l-\sqrt{a}) = l^2 - l^2 = 0$ ce qui est exclu car cela contredit l'intégrité de L. Donc $l^2 < 0$. On pose alors $e_2 \triangleq \frac{l}{\sqrt{-l^2}}$. On a alors

$$e_2^2 = -1 \text{ et } e_1 e_2 = \frac{e_1 l}{\sqrt{-l^2}} = \frac{-l e_1}{\sqrt{-l^2}} = -e_2 e_1$$

On pose enfin $e_3 \triangleq e_1 e_2$; on a alors $e_3^2 = e_1 e_2 e_1 e_2 = e_1(-e_1 e_2)e_2 = -e_1^2 e_2^2 = -1$. Enfin $e_2 e_3 = e_2(e_1 e_2) = -e_1 e_2^2 = e_1$ et $e_3 e_1 = (e_1 e_2)e_1 = -e_1^2 e_2 = e_2$. On vérifie ainsi que e_1, e_2, e_3 a la même table que i, j, k définis dans la section précédente ; ils engendrent donc un sous-corps H de L isomorphe à $\mathbb{H}$.
Montrons à présent que $H = L$. On suppose donc le contraire : soit $\gamma \in L \setminus H$, alors on définit de la même façon que le l précédent $v = \gamma e_1 - e_1 \gamma$, et on a encore que $v \neq 0$, $v \notin H$ et est de carré réel négatif. Soit $e \triangleq \frac{v}{\sqrt{-v^2}}$.
On montre que $e \notin H$. Puisque e est défini comme e_2, on a $e_1 e = -e e_1$, donc $e \notin \mathbb{R}(e_1)$. Comme $\gamma \notin H$ on a que $\mathbb{R}(e_1, \gamma) \cap H = \mathbb{R}(e_1)$, et comme $e \in \mathbb{R}(e_1, \gamma)$ s'il était dans H il serait alors dans $\mathbb{R}(e_1)$, ce qui est exclu. On conclut donc que $e \notin H$, un fait qui sera mis en défaut dans les lignes qui suivent. On a $e_2 e \notin H$ car sinon comme $e_2^{-1} \in H$ on aurait $e \in H$. Mais on a alors

$$e_1(e_2 e) = -e_2 e_1 e = -(-e_2 e)e_1 = (e_2 e)e_1$$

donc il s'avère que $e_2 e$ commute avec e_1, donc $e_2 e \in \mathbb{R}(e_1) \subseteq H$ et donc $e \in H$ ce qui est exclu. On a donc bien $L = H \cong \mathbb{H}$.

□

1.3 Exemple d'un corps gauche de dimension 9 sur $\mathbb{Q}$

On va dans cette section construire un corps non commutatif de dimension 9 sur $\mathbb{Q}$. Il s'avère que lorsque l'on parle d'extension du corps réel on ne peut excéder la dimension 4, en revanche en se plaçant sur des extensions de $\mathbb{Q}$ comme on va le voir, on peut augmenter en dimension.

On commence par considérer le corps $L = \mathbb{Q}(cos(\frac{2\pi}{7}))$, i.e. le plus petit sur corps de $\mathbb{Q}$ qui contient $cos(\frac{2\pi}{7})$. C'est une extension $\mathbb{Q} \subseteq L \subseteq \mathbb{R}$ qui en fait est de dimension 3 sur $\mathbb{Q}$. En effet, si on pose $\zeta = e^{\frac{2i\pi}{7}}$, alors on a $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 6$ car on a $\mathbb{Q}(\zeta) \equiv \mathbb{Q}[X] \Big/ (\Phi_7(X))$ où Φ_7 est le 7-ième polynôme cyclotomique,irréductible sur $\mathbb{Q}$, de degré 6. Enfin on a

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\zeta) : L][L : \mathbb{Q}]$$

Le polynôme de $L[X]$ $X^2 - (\zeta + \zeta^{-1})X + 1$ annule ζ donc ζ a un degré d'algébricité sur L d'au plus 2, comme $\zeta \notin \mathbb{R}$ on a que $[\mathbb{Q}(\zeta) : L] = 2$ et donc $[L : \mathbb{Q}] = 3$.

On va à présent trouver une $\mathbb{Q}$-base de L. On en a déja une $1, u, u^2$ avec $u = \zeta + \zeta^{-1} = 2cos(\frac{2\pi}{7})$, mais on va en considérer une autre. Soient $v = \zeta^2 + \zeta^5$ et $w = \zeta^3 + \zeta^4$. On a

$$u + v + w = \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = -1$$

(u, v, w) est une famille génératrice de L car

$$\begin{aligned} 1 &= -(u + v + w) \\ u &= u \\ u^2 &= 2 + v = -2u - v - 2w \end{aligned}$$

C'est donc une base de L, dont la table de multiplication est donnée par

$\cdot$	u	v	w
u	$2+v$	$u+w$	$v+w$
v	$u+w$	$2+w$	$u+v$
w	$v+w$	$u+v$	$2+u$

Cette table est invariante par la permutation $u \mapsto v\ v \mapsto w\ w \mapsto u$, ainsi cette permutation s'étend en un $\mathbb{Q}$-automorphisme de L, que nous noterons σ, il est d'ordre 3, c'est-à-dire que $\sigma^3 = Id_L$.

On définit à présent la *norme* d'un élément $\xi = xu + yv + zw$ de L. Soit Ξ l'application

$$\begin{array}{rccc} \Xi : L & \longrightarrow & L \\ \theta & \longmapsto & \xi\theta \end{array}$$

C'est bien un endomorphisme de L en tant que $\mathbb{Q}$ espace vectoriel, dont la matrice dans la base (u, v, w) est :

$$\begin{pmatrix} y-2x & x-2y+z & y-z \\ z-x & z-2y & x+y-2z \\ -2x+y+z & x-y & x-2z \end{pmatrix}$$

On définit [1] alors

$$\begin{aligned} N(\xi) &\triangleq det(\Xi) && (1.1) \\ &= x^3+y^3+z^3-4(x^2z+y^2x+z^2y)+3(x^2y+y^2z+z^2x)-xyz && (1.2) \end{aligned}$$

Par définition, et comme L est un corps, il vient que $\xi \neq 0 \iff N(\xi) \neq 0$.

On va à présent trouver une expression plus agréable de la norme sur L. On suppose que $\xi \notin \mathbb{Q}$. On a que ξ annule le polyôme caractéristique P de Ξ. Par le théorème de Cayley-Hamilton, ξ est aussi racine du polynôme minimal de Ξ, notons le m. Il vient ensuite que

$$\begin{aligned} 0 &= m(\zeta) \\ &= \sigma(m(\zeta)) \\ &= m(\sigma(\zeta)) \\ &= m(\sigma^2(\zeta)) \end{aligned}$$

et ainsi $\sigma(\xi)$ et $\sigma^2(\xi)$ sont deux autres racine de P (encore par Cayley-Hamilton). Sachant que P est de degré 3, son terme constant est égal au produit $\xi\sigma(\xi)\sigma^2(\xi)$. Or le terme constant du polynôme caractéristique de Ξ est précisément $det\Xi$ on a donc montré que

$$N(\xi) = \xi \cdot \sigma(\xi) \cdot \sigma^2(\xi)$$

Si $\xi \in \mathbb{Q}$, ce produit est ξ^3 et est bien le déterminant attendu car Ξ est alors une homothétie de rapport $\xi \in \mathbb{Q}$, de matrice $\begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi & 0 \\ 0 & 0 & \xi \end{pmatrix}$.

On va maintenant énoncer un résultat sur N qui nous permettra plus tard de définir un corps de dimension 9 sur $\mathbb{Q}$.

Pour $\xi \in L \setminus \{0\}$, $N(\xi)$ *est de la forme :*

$$N(\xi) = 8^h \frac{p}{q} \quad avec\ p, q\ impairs,\ h \in \mathbb{Z}$$

1. On constate que cette définition, qui peut paraître obscure à première vue coincide en fait avec les normes que l'on définit habituellement, que ce soit sur $\mathbb{C}$ ou bien sur $\mathbb{H}$ ou encore sur $\mathbb{Z}[i]$, que l'on verra au chapitre 2.

Pour le voir, il faut d'abord remarquer que

$$\text{Si } x, y, z \text{ sont entiers non tous pairs, alors } N(xu + yv + zw) \text{ est impair}$$

Cela se vérifie facilement par l'expression de N en (1.2) en traitant les cas où il y a un, deux ou trois impairs parmis x, y, z et en utilisant l'arithmétique dans $\frac{\mathbb{Z}}{2\mathbb{Z}}$. Ensuite, en considérant les x, y, z dans $\mathbb{Q}$, on factorise par h le minimum des valuations 2-adic dans x, y, z, ce qui nous donne $x = 2^h \frac{p_1}{q}$, $y = 2^h \frac{p_2}{q}$ et $z = 2^h \frac{p_3}{q}$ avec q impair et p_i non tous pairs. On a alors

$$N(xu + yv + zw) = 2^{3h} \frac{N(p_1 u + p_2 v + p_3 w)}{q^3}$$

puisque N est un polynôme homogène de degrés 3 en x,y et z. Par le résultat précédent et le fait que q^3 soit impair, il vient que $N(\xi)$ est bien de la forme annoncée.

Définition du corps gauche $\mathbb{B}$ de dimension 9 sur $\mathbb{Q}$:

On définit $\mathbb{B}$ comme l'ensemble des combinaisons linéaires formelles d'éléments de L :

$$\mathbb{B} \triangleq \left\{ \xi_0 + a\xi_1 + a^2\xi_2 \mid \xi_i \in L \right\}$$

où a et a^2 sont deux symboles, éléments de $\mathbb{B}$, et $(1, a, a^2)$ L-linéairement indépendants [2]. On a une structure de L-module *à droite* définit par

$$(\xi_0 + \xi_1 a + \xi_2 a^2)\xi = \xi_0\xi + a\xi_1\xi + a^2\xi_2\xi$$

La structure de L-module *à gauche* est en revanche définie par

$$\xi a = a\sigma(\xi) \quad \xi a^2 = a^2\sigma^2(\xi)$$

Et enfin, la structure de multiplication de la L-base est définie par :

$\cdot$	1	a	a^2
1	1	a	a^2
a	a	a^2	2
a^2	a^2	2	$2a$

On remarque que la multiplication des éléments de la L base de $\mathbb{B}$ est commutative, en revanche c'est la structure de L-module qui est différente à gauche et à droite. On a définit $\mathbb{B}$ comme espace de dimension 3 sur L, on décrit à présent sa structure de $\mathbb{Q}$ espace vectoriel. En considérant L comme $\mathbb{Q}$ espace vectoriel de base (u, v, w) il vient que $\mathbb{B}$ est un $\mathbb{Q}$ espace vectoriel de dimension 9 et il est entièrement décrit par la table de multiplication de la base produit $(u, v, w, au, av, aw, a^2u, a^2v, a^2w)$. Il est évident que c'est une base dans le monde commutatif, pour remarquer que c'en est une ici, il suffit de voir que $ua = av$, $va = aw$, $wa = au$,$ua^2 = a^2w$, $va^2 = a^2u$, $wa^2 = a^2v$. Autrement dit, les produits peuvent être ordonnés. La table de multiplication de cette base est donnée en annexe.

Il faut encore vérifier que cette structure fait de $\mathbb{B}$ un anneau, ce qui laisse l'associativité à vérifier, soit quelques $9^3 = 729$ vérifications à faire. Il est laissé le soin au lecteur de les vérifier. On a donc une structure de $\mathbb{Q}$ algèbre de dimension 9. On montre à présent que $\mathbb{B}$ est un corps.

Considérons un élément $\gamma = \xi_0 + a\xi_1 + a^2\xi_2 \in \mathbb{B} \setminus \{0\}$, et $\Gamma : \mathbb{B} \to \mathbb{B}$ définit par la multiplication par γ *à gauche*, soit $\Gamma(\delta) = \gamma\delta$ Cette application est un endomorphisme de $\mathbb{B}$ pour la structure de L espace vectoriel de dimension 3, et si on montre que cette application est bijective, on aura bien γ inversible.
On considère donc la matrice de Γ dans la base $(1, a, a^2)$

2. Dans le sens ou ces combinaisons linéaires ne sont jamais nuls à part si tous les coefficients sont nuls.

$$\begin{pmatrix} \xi_0 & 2\sigma(\xi_2) & 2\sigma^2(\xi_1) \\ \xi_1 & \sigma(\xi_0) & 2\sigma^2(\xi_2) \\ \xi_2 & \sigma(\xi_1) & \sigma^2(\xi_0) \end{pmatrix}$$

Son déterminant est un élément de L égal à :

$$N(\xi_0) + 2N(\xi_1) + 4N(\xi_2) - 2(\xi_2\sigma(\xi_0)\sigma^2(\xi_1) + \xi_1\sigma(\xi_2)\sigma^2(\xi_0) + \xi_0\sigma(\xi_1)\sigma^2(\xi_2)) \quad (\ddagger)$$

Pour montrer qu'il est non nul avec γ non nul, on considère d'abord le cas simple ou $\xi_0 \in L$ a ses composantes dans $\mathbb{Z}$ non toutes paires. Dans ce cas, par un résultat précédent $N(\xi_0)$ est impair, or tous les autres termes sont pairs donc le determinant est non nul. Pour se ramener à ce cas particulier, on commence par multiplier γ par le ppcm des dénominateurs des coefficients (dans $\mathbb{Q}$) de ξ_0, ξ_1 et ξ_2, les coefficients sont donc dans $\mathbb{Z}$ et non tous pairs, donc il existe un $l \in \{0, 1, 2\}$ tel que ξ_l ai ses composantes non toutes paires. Si c'est ξ_1, on multiplie par a^{-1} ($\triangleq \frac{1}{2}a^2$) pour se ramener au bon cas, et si c'est ξ_2 on multiplie par $a^{-2}(\triangleq \frac{1}{2}a)$. On a donc bien que $det\Gamma$ est non nul et donc que γ est inversible à droite notons le γ'. De plus, γ' est aussi un inverse à gauche, car $\gamma\gamma' = 1$ donc $\gamma'\gamma\gamma' = \gamma'$ donc en multipliant à droite par l'inverse de γ', on a bien $\gamma'\gamma = 1$. On en déduit que $\mathbb{B}$ est un corps.
On montre un dernier résultat sur $\mathbb{B}$:

Le centre de $\mathbb{B}$ *est* $\mathbb{Q}$

Tout d'abord, le centre $Z(\mathbb{B})$ n'est pas $\mathbb{B}$ car $\mathbb{B}$ n'est pas commutatif, il est donc de dimension 3 ou 1 sur $\mathbb{Q}$. Pour $x \in \mathbb{B}$, $\mathbb{Q}(x)$ est un sous corps commutatif donc sa dimension sur $\mathbb{Q}$ n'excède pas 3 car on a

$$9 = [\mathbb{B} : \mathbb{Q}] = [\mathbb{B} : Z(\mathbb{Q})][Z(\mathbb{Q}) : \mathbb{Q}]$$

Si $x \notin \mathbb{Q}$, $\mathbb{Q}(x)$ est donc de $\mathbb{Q}$-dimension 3, c'est un sous-corps commutatif maximal de $\mathbb{B}$ et il est nécessairement distinct de $Z(\mathbb{B})$ car sinon, on pourrait prendre un élément n'appartenant pas à $Z(\mathbb{B})$ et faire une extension commutative stricte qui serait alors égale à $\mathbb{B}$ ce qui est absurde. On a donc montré le résultat, de plus on a montré que tout élément $x \in \mathbb{B} \setminus \mathbb{Q}$ était algébrique de degré 3 sur $\mathbb{Q}$.

2 Application arithmétique : Le théorème des quatres carrés

Le but de cette partie est d'établir le théorème des quatres carrés conjecturé par Claude Gaspard Bachet en 1621 puis prouvé en 1770 par Joseph Louis Lagrange. La preuve proposée ici utilise un sous-anneau des quaternions appellé *quaternions d'Hurwitz*, c'est une preuve proposée par Hurwitz qui fonctionne sur le même principe que la preuve du théorème des deux carrés, introduite ci-après.

2.1 Introduction : Le théorème des deux carrés

On commence par donner une preuve du classique théorème des deux carrés. On rappelle que $\mathbb{Z}[i] = \{a+ib|a,b \in \mathbb{Z}\}$ est muni d'une structure d'anneau et on définit $N : \mathbb{Z}[i] \to \mathbb{Z}$ tel que $N(z) = z\bar{z}$ ou $\overline{a+ib} = a-ib$. On vérifie que N est *multiplicative*, $N(z) = 0 \iff z = 0$, de plus on voit que pour tout $z \in \mathbb{Z}[i]$, $N(z)$ est une somme de deux carrés d'entiers.

On énonce maintenant la stratégie de la preuve du théorème des deux carrés. Si $x = a^2+b^2$ et $y = c^2+d^2$ sont somme de deux entiers. Alors en posant $z_x = a+ib$ et $z_y = c+id \in \mathbb{Z}[i]$ il vient que $x = N(z_x)$ et $y = N(z_y)$. De plus, par multiplicativité de N, $xy = N(z_x z_y)$ donc xy est aussi une somme de deux carrés. On voit donc que *l'ensemble des nombre entiers somme de deux carrés est stable par produit.* Sachant que tout nombre entier est produit de nombres premiers, il s'agit de determiner quels sont les nombres premiers qui sont somme de deux carrés. Sachant que $2 = 1^2+1^2$ on va s'interesser aux nombres premiers impairs. D'abord une proposition sur la structure de $\mathbb{Z}[i]$.

Proposition 2.1.1. *Soit $\mathbb{Z}[i]$ l'anneau des entiers de Gauss. Alors $\mathbb{Z}[i]$ est un anneau* euclidien. *En particulier, tout idéal est principal. De plus $z \in \mathbb{Z}[i]$ est inversible si et seulement si $N(z) = 1$.*

Preuve : Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$, on montre que N est un stathme Euclidien, ie. que il existe $q, r \in \mathbb{Z}[i]$ tels que $z = tq + r$ avec $N(r) < N(t)$. Si $z = tq$ alors $r = 0$ et $N(r) = 0 < N(t)$ car $t \neq 0$. Sinon, on considère l'idéal $I = \mathbb{Z}[i]t$, qui forme un réseau du plan complexe et z est dans un des carrés (de longueur $|t| = \sqrt{t \cdot \bar{t}}$) que forme ce réseau. Il existe donc (au moins) un élément qt dans I de distance inférieur ou égale à la demi diagonale des carrés (qui est $\frac{\sqrt{2}}{2}|t|$). On pose alors $r = z - qt$ et on a

$$N(r) = |z-qt|^2 \leq (\frac{\sqrt{2}}{2}|t|)^2 = \frac{\sqrt{2}}{2}N(t) < N(t)$$

Ainsi, $\mathbb{Z}[i]$ est un anneau Euclidien, il est donc en particulier principal [1]. Si $z, t \in \mathbb{Z}[i]$ sont tels que $1 = zt$ alors $N(1) = 1 = N(z)N(t)$ donc $N(z)$ et $N(t)$ divisent 1 dans $\mathbb{Z}$, comme ils sont positifs on a $N(t) = N(z) = 1$. Réciproquement si $N(a+ib) = a^2+b^2 = 1$ alors $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$ donc ce ne sont que les éléments ± 1 et $\pm i$, qui sont bien inversible.

1. Ce résultat est en fait vrai pour tout anneau Euclidien, pour le voir, considérer un idéal J d'un anneau Euclidien E de stathme ν. Alors comme ν est à valeur dans $\mathbb{N}$ on peut prendre $\alpha \in \mathbb{N}$ la plus petite valeur de ν prise par un élément non nul a de J. Clairement $Ea \subset J$. Soit maintenant $x \in J$ et $q, r \in E$ tels que $x = aq + r$ avec $\nu(r) < \nu(a)$, alors comme $r \in J$ il vient que $r = 0$ car a est de stathme minimal dans J, donc $J = Ea$.

□

On va alors avoir besoin de trois lemmes. On note $\mathbb{F}_p \triangleq \mathbb{Z}/p\mathbb{Z}$, le corps à p éléments. $\mathbb{F}_p^\times$ le groupe de ses éléments inversibles et $\mathbb{F}_p^{\times 2}$ l'ensemble de ses carrésnon nuls.

Lemme 2.1.2. *On a les equivalences suivante pour p nombre premier impair :*

- $a \in \mathbb{F}_p^{\times 2}$ *ssi* $a^{\frac{p-1}{2}} = 1$
- $a \notin \mathbb{F}_p^{\times 2}$ *ssi* $a^{\frac{p-1}{2}} = -1$

PREUVE : On a que

$$\begin{array}{rccc} \phi : & \mathbb{F}_p^\times & \longrightarrow & \mathbb{F}_p^\times \\ & x & \longmapsto & x^2 \end{array}$$

est un homomorphisme pour la structure de groupe. De plus, comme $\mathbb{F}_p$ est un corps, on a $ker\phi = \{-1, 1\}$ et donc par factorisation

$$\mathbb{F}_p^{\times 2} \cong \mathbb{F}_p^\times \Big/ \{-1, 1\}$$

En particulier $\mathbb{F}_p^{\times 2}$ est un groupe d'ordre $|\mathbb{F}_p^{\times 2}| = \frac{p-1}{2}$ donc tout élément $a \in \mathbb{F}_p^{\times 2}$ vérifie $a^{\frac{p-1}{2}} = 1$. Réciproquement l'ensemble des racines dans $\mathbb{F}_p[X]$ de $X^{\frac{p-1}{2}} - 1$ est de cardinalité inférieur ou égal à $\frac{p-1}{2}$, on conclut donc que $a \in \mathbb{F}_p^{\times 2}$ si et seulement si $a^{\frac{p-1}{2}} = 1$. Si a n'est pas un carré, comme $a^{\frac{p-1}{2}^2} = 1$ on a $a^{\frac{p-1}{2}} = 1$ ou -1. Mais par le premier point ce ne peut être 1 donc $a^{\frac{p-1}{2}} = -1$. □

Lemme 2.1.3. *Soit p un nombre premier impair. Alors p est une somme de deux carrés d'entiers si et seulement si $p \equiv 1$ mod 4.*

PREUVE : On commence par montrer le sens direct. Supposons donc que $p = a^2 + b^2$ avec $a, b \in \mathbb{Z}$. On vérifie que $\left(\mathbb{Z}/4\mathbb{Z}\right)^2 = \{\bar{0}, \bar{1}\}$, $\bar{x}$ désignant la classe de $x \in \mathbb{Z}$ modulo 4. Ainsi une somme de deux carrés de $\mathbb{Z}/4\mathbb{Z}$ est dans $\{\bar{0}, \bar{1}, \bar{2}\}$. En réduisant $p = a^2 + b^2$ modulo 4, on voit que $p \equiv 0$, 1, ou 2 *mod* 4. 0 et 2 étant exclus puisque p est impair, on conclut que $p \equiv 1$ *mod* 4.

On suppose à présent que $p \equiv 1$ *mod* 4. On a alors que $\frac{p-1}{2}$ est pair et ainsi $(-1)^{\frac{p-1}{2}} = 1$ donc par le lemme 2.1.2, -1 est un carré dans $\mathbb{F}_p$, ie il existe $x \in \mathbb{Z}$ tel que $\bar{x}^2 = -1 \in \mathbb{F}_p$ donc $p|x^2+1$. On fait à présent intervenir l'anneau $\mathbb{Z}[i]$.
On a $x^2 + 1 = (x - i)(x + i)$, de plus p ne divise ni $x - i$, ni $x + i$ (en particulier, p n'est pas premier dans $\mathbb{Z}[i]$) donc $x - i \notin \mathbb{Z}[i]p$ alors que $x^2 - 1 \in \mathbb{Z}[i]p$. Soit alors $I = \mathbb{Z}[i](x - i) + \mathbb{Z}[i]p$. Si $y \in I$, $y = \lambda(x - i) + \mu p$ et

$$N(y) = y \cdot \bar{y} = (\lambda(x - i) + \mu p)(\bar{\lambda}(x + i) + \bar{\mu}p) = \lambda\bar{\lambda}(x^2 + 1) + \lambda(x - i)\bar{\mu}p + \mu\bar{\lambda}(x + i)p + \mu\bar{\mu}p^2$$

On a donc que pour tout $z \in I$, p divise $N(z)$. En particulier $I \subsetneq \mathbb{Z}[i]$. Maintenant, par 2.1.1 il existe $z \in I$ tel que $I = \mathbb{Z}[i]z$. Comme $p \in I$ il existe $z' \in I$ tel que $p = z'z$, et donc

$$p^2 = N(z')N(z)$$

Cependant, z n'est pas inversible puisque $I \subsetneq \mathbb{Z}[i]$, donc $N(z) \neq 1$. De même, supposons z' inversible, on aurait $z = z'^{-1}p \in \mathbb{Z}[i]p$ et donc $I \subseteq \mathbb{Z}[i]p$, or $x - i \notin \mathbb{Z}[i]p$ et $x - i \in I$, contradiction. Donc z' n'est pas inversible et donc $N(z') \neq 1$. Comme $N(z)$ et $N(z')$ sont dans $\mathbb{Z}$, on conclut que $N(z) = p$, donc p est une somme de deux carrés. □

Lemme 2.1.4. *Soit p un nombre premier impair. Si p n'est pas somme de deux carrés (i.e. $p \equiv 3$ mod 4), alors $p|a^2 + b^2$ implique $p|a$ et $p|b$ et donc $p^2|a^2 + b^2$.*

PREUVE : On réduit dans $\mathbb{F}_p$: $\bar{a}^2 + \bar{b}^2 = 0$. En supposant $\bar{b} \neq 0$, comme $\mathbb{F}_p$ est un corps, $\bar{b}$ est inversible et on a

$$\bar{a}^2\bar{b}^{-2} = (\bar{a}\bar{b}^{-1})^2 = -1$$

Mais ceci est absurde car $\frac{p-1}{2} \equiv 1 \ mod\ 4$ donc $(-1)^{\frac{p-1}{2}} \equiv -1 \ mod\ p$ ie -1 n'est pas un carré dans $\mathbb{F}_p$ par 2.1.2. On a donc $\bar{b} = 0$ et donc $\bar{a} = 0$ d'où p divise a et b. □

On peut à présent prouver le théorème des deux carrés.

Théorème 2.1.5. *Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r} \in \mathbb{N}$. Alors n est une somme de deux carrés d'entiers si et seulement si $\forall i\ p_i \equiv 1\ mod\ 4$ ou $p_i = 2$ ou $\alpha_i \equiv 0\ mod\ 2$.*

PREUVE : Si $n = a^2 + b^2$, $a, b \in \mathbb{Z}$. Alors soit p premier impair divisant n. Si $p \equiv 3 \mod 4$, alors par le lemme 2.2.4 on a $p|a$ et $p|b$ donc $a = pa'$ et $b = pb'$ et donc $n = p^2(a'^2 + b'^2)$, on montre ainsi que la valuation de p dans n est paire, donc le résultat.
Supposons maintenant les hypothèses de la réciproque. On réordonne $n = 2^\alpha m^2 p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec $p_i \equiv 1\ mod\ 4$. Alors par le lemme 2.1.3, p_i est une somme de deux carrés, et par stabilité par multiplication $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ aussi et donc comme 2^α est une somme de deux carrés, $2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ est une somme de deux carrés. On multiplie enfin par m^2 et cela reste une somme de deux carrés. On a donc montré le résultat. □

2.2 Les quaternions d'Hurwitz

La preuve du théorème des quatres carrés s'inspire grandement de celle du théorème des deux carrés, seulement, il faut se placer dans un anneau euclidien dans lequel la norme nous donnera quatre carrés. On pense alors immédiatement aux quaternions.

Definition 2.2.1 (Quaternions entiers)**.** *On appelle* quaternions entiers *(où encore* quaternions de Lipschitz*) le sous-anneau de $\mathbb{H}$ définit par :*

$$\mathbb{H}_\mathbb{Z} \triangleq \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

Cet ensemble est clairement stable par multiplication, contient l'élément neutre et est plongé dans $\mathbb{H}$, c'est donc bien un sous-anneau de $\mathbb{H}$. On utilise a nouveaux la norme de $\mathbb{H}$ restreinte à $\mathbb{H}_\mathbb{Z}$ pour montrer que tout produit d'entier somme de quatre carrés d'entiers est somme de quatres carrés d'entiers. Autrement dit l'ensemble $\mathcal{L}$ des sommes de quatres carrés d'entiers est stable par multiplication.

Proposition 2.2.2. *Soit $q, r \in \mathbb{H}_\mathbb{Z}$ alors $N(qr) = N(q)N(r)$. En particulier l'ensemble $\mathcal{L}$ est stable par multiplication.*

PREUVE : Le premier point est immédiat par restriction de N à $\mathbb{H}_\mathbb{Z}$, par la première partie. De plus une somme de quatres carrés d'entiers $z = a^2 + b^2 + c^2 + d^2$ définit un quaternions entier par $q_z = a + ib + jc + kd$ avec $N(q_z) = z$, donc pour $z, z' \in \mathcal{L}$ on a

$$zz' = N(q_z)N(q_{z'}) = N(zz') \in \mathcal{L}$$

□

Sachant que tout entier positif est produit de nombres premiers, il suffit donc de prouver que tous les nombres premiers sont dans $\mathcal{L}$, et par stabilité multiplicative, on aura $\mathcal{L} = \mathbb{N}$, le résultat attendu.

Definition 2.2.3 (Quaternions d'Hurwitz)**.** *Soit $\epsilon \triangleq \frac{1+i+j+k}{2} \in \mathbb{H}$. On appelle* quaternion d'hurwitz *tout élément de l'ensemble*

$$\widehat{\mathbb{H}_\mathbb{Z}} \triangleq \mathbb{H}_\mathbb{Z} \cup (\epsilon + \mathbb{H}_\mathbb{Z})$$

$\widehat{\mathbb{H}_\mathbb{Z}}$ est l'ensemble des quaternions d'Hurwitz.

Lemme 2.2.4. *Tout élément de $q \in \widehat{\mathbb{H}_\mathbb{Z}}$ s'écrit sous la forme $2r + \frac{\pm 1 \pm i \pm j \pm k}{2}$ avec $r \in \mathbb{H}_\mathbb{Z}$.*

PREUVE : Soit $q \in \widehat{\mathbb{H}_\mathbb{Z}}$ si q n'est pas un quaternion entier, il est de la forme $r + \epsilon = \frac{a_0 + a_1 i + a_2 j + a_3 k}{2}$ avec a_l impairs, donc $a_l \equiv \pm 1 \ mod\ 4$, ainsi $a_l = 4b_l \pm 1$ et donc $q = 2(b_0 + b_1 i + b_2 j + b_3 k) + \frac{\pm 1 \pm i \pm j \pm k}{2}$, ce qu'il fallait démontrer. □

Proposition 2.2.5. *$\widehat{\mathbb{H}_\mathbb{Z}}$ est un anneau, $N(q) \in \mathbb{N}\ \forall q \in \widehat{\mathbb{H}_\mathbb{Z}}$, il suit de cela que $q \in \widehat{\mathbb{H}_\mathbb{Z}}$ est inversible dans $\widehat{\mathbb{H}_\mathbb{Z}}$ si et seulement si $N(q) = 1$.*

PREUVE : Montrons que $\widehat{\mathbb{H}_\mathbb{Z}}$ est un anneau. On a que $\widehat{\mathbb{H}_\mathbb{Z}}$ est stable par addition puisque $\epsilon + \epsilon \in \mathbb{H}_\mathbb{Z}$, et c'est clairement un sous groupe additif. Pour la stabilité par multiplication, il s'agit de montrer que les produits ϵa pour $a \in \{i, j, k\}$ sont dans $\widehat{\mathbb{H}_\mathbb{Z}}$ ainsi que ϵ^2. On a $\epsilon^2 = \epsilon - 1 \in \widehat{\mathbb{H}_\mathbb{Z}}$, de plus on calcule $\epsilon i = \epsilon - 1 - k \in \widehat{\mathbb{H}_\mathbb{Z}}$ et $i\epsilon = \epsilon - 1 - j \in \widehat{\mathbb{H}_\mathbb{Z}}$. En appliquant la permutaion circulaire σ définie en 1.1.2, on a la vérification pour tous les produits. Par distributivité de la multiplication, le résultat s'étend sur tout $\widehat{\mathbb{H}_\mathbb{Z}}$. Si $q \in \mathbb{H}_\mathbb{Z}$, le second résultat est clair. Si $q = \frac{a_0 + a_1 i + a_2 j + a_3 k}{2}$ avec a_i impairs, $N(q) = q \cdot \bar{q} = \frac{1}{4}(a_0^2 + a_1^2 + a_2^2 + a_3^2)$, et comme $a_i \equiv \pm 1 \ mod\ 4$ on a bien que la somme de quatre carrés d'impairs est un multiple de 4 donc $N(q) \in \mathbb{N}$. Ainsi si $qq' = 1$, $N(q)N(q') = 1$ et comme par le point précédent $N(q), N(q') \in \mathbb{N}$ il vient $N(q), N(q') \in \mathbb{Z}^\times \cap \mathbb{N} = 1$. Réciproquement, si $N(q) = q \cdot \bar{q} = 1$ alors $\bar{q} \in \widehat{\mathbb{H}_\mathbb{Z}}$ est l'inverse de q à gauche et à droite. □

Théorème 2.2.6. *$\widehat{\mathbb{H}_\mathbb{Z}}$ est un anneau* euclidien à gauche et à droite*, et est donc* principal à gauche et à droite*. Autrement dit pour tout $q, s \in \widehat{\mathbb{H}_\mathbb{Z}}$ il existe $\beta, \rho, \beta', \rho' \in \widehat{\mathbb{H}_\mathbb{Z}}$ tels que*

$$\begin{aligned} q &= \beta s + \rho \\ q &= s\beta' + \rho' \end{aligned}$$

et $N(\rho) < N(s)$, $N(\rho') < N(s)$. De plus tout idéal à gauche (resp. à droite) est de la forme $\widehat{\mathbb{H}_\mathbb{Z}} q$ (resp. $q\widehat{\mathbb{H}_\mathbb{Z}}$) avec $q \in \widehat{\mathbb{H}_\mathbb{Z}}$.

PREUVE : On va montrer que $\forall s \in \mathbb{H}$ il existe $t \in \widehat{\mathbb{H}_\mathbb{Z}}$ tel que $N(s - t) \leq \frac{5}{8}$. Si $x \in \mathbb{R}$ alors l'entier le plus proche de x est $\lfloor x + \frac{1}{2} \rfloor$, en effet ce nombre est $\lfloor x \rfloor$ si $|x - \lfloor x \rfloor| < \frac{1}{2}$ et $\lceil x \rceil$ si $|x - \lfloor x \rfloor| \geq \frac{1}{2}$. Ainsi, tout nombre $x \in \mathbb{R}$ est compris entre $\lfloor x + \frac{1}{2} \rfloor$ (entier) et $\lfloor x \rfloor + \frac{1}{2}$ (demi-entier), et est à une distance $\leq \frac{1}{2}$ des deux et $\leq \frac{1}{4}$ de l'un des deux. Soit maintenant $s = a_0 + a_1 i + a_2 j + a_3 k$, alors deux cas sont possible,
Soit deux des a_l sont à distance $\leq \frac{1}{4}$ des *entiers* les plus proches, en ce cas, on pose

$$t = \lfloor a_0 + \frac{1}{2} \rfloor + \lfloor a_1 + \frac{1}{2} \rfloor i + \lfloor a_2 + \frac{1}{2} \rfloor j + \lfloor a_3 + \frac{1}{2} \rfloor k \in \widehat{\mathbb{H}_\mathbb{Z}}$$

et on a

$$N(s - t) \leq + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{5}{8}$$

Dans le cas contraire, trois des a_l sont à distance $\leq \frac{1}{4}$ des *demi-entiers* les plus proches, et on pose

$$t = \left(\lfloor a_0 \rfloor + \frac{1}{2}\right) + \left(\lfloor a_1 \rfloor + \frac{1}{2}\right) i + \left(\lfloor a_2 \rfloor + \frac{1}{2}\right) j + \left(\lfloor a_3 \rfloor + \frac{1}{2}\right) k \in \widehat{\mathbb{H}_\mathbb{Z}}$$

et on a

$$N(s - t) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{7}{16} \leq \frac{5}{8}$$

Soient à présent $q, s \in \widehat{\mathbb{H}_\mathbb{Z}}$, alors $qs^{-1}, s^{-1}q \in \mathbb{H}$ et par précédement il existe $\beta, \beta' \in \widehat{\mathbb{H}_\mathbb{Z}}$ tels que

$$N(\beta - qs^{-1}) \leq \frac{5}{8} \quad N(\beta' - s^{-1}q) \leq \frac{5}{8}$$

On pose alors $\rho = q - \beta s \in \widehat{\mathbb{H}_\mathbb{Z}}$ et $\rho' = q - s\beta \in \widehat{\mathbb{H}_\mathbb{Z}}$, ce qui donne bien $q = \beta s + \rho$ et $q = \beta' s + \rho'$ avec

$$N(\rho) = N(q - \beta s) = N(qs^{-1} - \beta)N(s) \leq \frac{5}{8}N(s) < N(s)$$

et

$$N(\rho) = N(q - s\beta') = N(s^{-1}q - \beta')N(s) \leq \frac{5}{8}N(s) < N(s)$$

On a donc la première partie du théorème. Pour la seconde partie sachant que la norme d'un quaternion d'hurwitz est entière, le résultat suit du fait que les anneaux euclidiens sont principaux, démontré en note de bas de page, page 6 ; (il faut traiter les cas *à gauche* et *à droite*, mais le raisonnement est le même). □

On comprend ici le besoin de considérer les quaternions d'Hurwitz plutôt que les quaternions entiers, en effet on voit que si $s = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$, le quaternion entier le plus proche de s a ses composantes à une distance $\leq \frac{1}{2}$ de celle de s puisque l'on ne peut pas considérer les demi-entiers, ainsi, pour

$$t = \lfloor a_0 + \frac{1}{2} \rfloor + \lfloor a_1 + \frac{1}{2} \rfloor i + \lfloor a_2 + \frac{1}{2} \rfloor j + \lfloor a_3 + \frac{1}{2} \rfloor k \in \mathbb{H}_\mathbb{Z}$$

On a

$$N(s - t) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 1$$

On ne peut donc pas définir de division Euclidienne avec un reste *strictement* inférieur au diviseur.

2.3 Le théorème de Lagrange

On montre dans cette section que tout nombre premier est dans $\mathcal{L}$. On traite d'abord le cas du nombre premier pair puis le cas des nombres premiers impaires. Trivialement $2 = 1^2 + 1^2 + 0 + 0$ donc $2 \in \mathcal{L}$. Pour les nombres premiers impairs on utilise le résultat suivant :

Proposition 2.3.1. *Pour tout nombre premier impair p il existe $q \in \widehat{\mathbb{H}_\mathbb{Z}}$ tel que $N(q) = p$.*

PREUVE : On utilise pour montrer cela le lemme suivant :

Lemme. *Si p est un nombre premier impair, il existe $a, b \in \mathbb{N}$ tels que p divise $a^2 + b^2 + 1$.*

PREUVE : [du lemme] Soit $A \triangleq \left\{x^2 | x \in \mathbb{F}_p\right\}$ et $B \triangleq \left\{-1 - y^2 | y \in \mathbb{F}_p\right\}$. Examinant la preuve de 2.1.2, on voit que $|A \setminus \{0\}| = |B \setminus \{0\}| = |\mathbb{F}_p^{\times 2}| = \frac{p-1}{2}$. Donc $|A| = |B| = \frac{p+1}{2}$. Ces deux ensembles ne pouvant pas être disjoints dans $\mathbb{F}_p$ par un simple argument de cardinalité, on conclut à l'existence de deux éléments $x, y \in \mathbb{Z}$ tels que $x^2 + y^2 + 1 = 0 \ mod\ p$, ce qui prouve le lemme. □

On prouve à présent la proposition. Soient donc $a, b \in \mathbb{N}$ tels que p divise $a^2 + b^2 + 1$ et

$$J \triangleq \widehat{\mathbb{H}_\mathbb{Z}}p + \widehat{\mathbb{H}_\mathbb{Z}}(1 + ai + bj) \subseteq \widehat{\mathbb{H}_\mathbb{Z}}$$

.
Soit $q \in J$, on a que $p|N(q)$. En effet $q = rp + s(1 + ai + bj)$ donc $N(q) = q\bar{q} = (\star)p + (\star)(1 + a^2 + b^2)$ qui est divisible par p.
On montre a présent que $\widehat{\mathbb{H}_\mathbb{Z}}p \subsetneq J \subsetneq \widehat{\mathbb{H}_\mathbb{Z}}$.
Comme tous les elements de J sont de norme divisible par p, on a que $J \subsetneq \widehat{\mathbb{H}_\mathbb{Z}}$. De plus $\widehat{\mathbb{H}_\mathbb{Z}}p \subsetneq J$ puisque $1 + ai + bj \notin \widehat{\mathbb{H}_\mathbb{Z}}p$ (sinon on aurait $p|1$).
J est un idéal à gauche de $\widehat{\mathbb{H}_\mathbb{Z}}$ donc, en vertu du théorème 2.2.6 on a l'existence de $q_0 \in \widehat{\mathbb{H}_\mathbb{Z}}$ tel que $J = \widehat{\mathbb{H}_\mathbb{Z}}q_0$.
On a $N(q_0) \neq 1$ car si c'était le cas, on aurait que q_0 serait inversible dans $\widehat{\mathbb{H}_\mathbb{Z}}$ et que J serait $\widehat{\mathbb{H}_\mathbb{Z}}$ tout entier,

ce qui est exclu. Comme $p \in J$, il existe $q' \in \widehat{\mathbb{H}_\mathbb{Z}}$ tel que $q'q_0 = p$. On a $N(q') \neq 1$ en effet, en supposant le contraire on aurait q' inversible et donc $q_0 = q'^{-1}p \in \widehat{\mathbb{H}_\mathbb{Z}}p$ ce qui est exclus. On a donc

$$N(q_0)N(q') = p^2$$

avec $N(q_0), N(q') \in \mathbb{Z} \setminus \{1\}$, donc on a necessairement $N(q_0) = p$. □

On a à présent tous les résultats pour prouver le théorème des quatres carrés.

Théorème 2.3.2 (Lagrange 1770)**.** *Tout entier est somme de quatres carrés d'entiers.*

PREUVE : Soit p un nombre premier, par la proposition précédente, il existe $q \in \widehat{\mathbb{H}_\mathbb{Z}}$ tel que $N(q) = p$. Si $q \in \mathbb{H}_\mathbb{Z}$ alors $N(q)$ est une somme de quatres carrés d'entiers et on a le résultat. Sinon, q s'écrit sous la forme $q = 2r + \omega$ par le lemme 2.2.4, avec $\omega = \frac{\pm 1 \pm i \pm j \pm k}{2}$ et $r \in \mathbb{H}_\mathbb{Z}$. De plus

$$\begin{aligned} q\bar{\omega} &= 2r\bar{\omega} + \omega\bar{\omega} \\ &= r(2\bar{\omega}) + 1 \end{aligned}$$

Donc $q\bar{\omega} \in \mathbb{H}_\mathbb{Z}$, de plus $N(q\bar{\omega}) = N(q)N(\bar{\omega}) = N(q) = p$. On a donc bien un élément de $\mathbb{H}_\mathbb{Z}$ de norme p, donc p est une somme de quatres carrés d'entiers. Enfin, tout nombre premier est dans $\mathcal{L}$ et par multiplicativité de $\mathcal{L}$, il vient $\mathbb{N} = \mathcal{L}$, ce qui démontre le théorème.

□

Exemple 2.3.3. *On peut de la même façon démontrer que tout entier positif peut s'écrire sous la forme :*

$$x^2 + xy + y^2 + u^2 + uv + v^2 \quad x, y, u, v \in \mathbb{Z} \tag{$*$}$$

La stratégie est exactement la même que pour le théorème de Lagrange, il suffit juste de trouver le sous-anneau de $\mathbb{H}$ dans lequel l'expression de la norme traduira la formule désirée. Soient $f, g, h \in \mathbb{H}$ définis par

$$f = \frac{1 + \sqrt{3}i}{2} \quad g = j \quad h = \frac{1}{2}j + \frac{\sqrt{3}}{2}k$$

On a $N(f) = N(g) = N(h) = 1$ et pour $x = x_0 + x_1 f + x_2 g + x_3 h$ il vient

$$N(x) = x_0^2 + x_0x_1 + x_1^2 + x_2^2 + x_2x_3 + x_3^2$$

Ainsi il paraît judicieux de considérer l'anneau $B = \mathbb{Z} + \mathbb{Z}f + \mathbb{Z}g + \mathbb{Z}h$. On a la table suivante (qui montre aussi la stabilité de B par multiplication)

$\vec{\cdot}$	f	g	h
f	$f-1$	h	$h-g$
g	$g-h$	-1	$f-1$
h	g	$-f$	-1

B est donc bien un anneau et cela montre déjà que l'ensemble des entiers s'écrivant sous la forme $(*)$ est stable par multiplication, ainsi on comprend qu'il faut prouver que tout nombre premier s'écrit sous la forme $(*)$, et donc est la norme d'un élément de B. Suivant la preuve du théorème de Lagrange,on va montrer que B est euclidien à droite et à gauche et donc principal à droite et à gauche. Pour ce faire on prend $x \in \mathbb{H}$, comme $(1, f, g, h)$ est clairement génératrice, c'est une base de $\mathbb{H}$ on peut donc écrire $x = x_0 + x_1 f + x_2 g + x_3 k$. On cherche donc $s \in B$ tel que $N(x - s) \leq c$ avec $0 < c < 1$. On a déja vu que pour les quaternions entiers, un tel c n'était pas possible car on ne peut approcher au plus pres qu'à une distance d'$\frac{1}{2}$ chaque composante par des entiers et comme la norme donne une somme de 4 carrés, on ne peut se rapprocher suffisement. En

revanche, pour B la norme donne des produits croisés, ce qui va nous permettre de faire baisser la norme. On réécrit l'expression de la norme :

$$N(x) = (x_0 + \frac{1}{2}x_1)^2 + \frac{3}{4}x_1^2 + (x_2 + \frac{1}{2}x_3)^2 + \frac{3}{4}x_3^2$$

On note alors $\{x_i\}$ l'entier naturel tel que $|x_i - \{x_i\}| \leq \frac{1}{2}$ (ie $\{x_i\} = \lfloor x_i + \frac{1}{2} \rfloor$). On choisit alors $s_1 = \{x_1\}$ et $s_3 = \{x_3\}$.

$$N(x-s) \quad = \quad (x_0 - s_0 + \frac{x_1 - s_1}{2})^2 + \frac{3}{4}(x_1 - s_1)^2 + (x_2 - s_2 + \frac{x_3 - s_3}{2})^2 + \frac{3}{4}(x_3 - s_3)^2$$

On voit alors qu'en choisissant $s_0 = \{x_0 + \frac{x_1 - s_1}{2}\}$ et $s_3 = \{x_2 + \frac{x_3 - s_3}{2}\}$, on a

$$N(x-s) \leq \frac{1}{4} + \frac{3}{4}\frac{1}{4} + \frac{1}{4} + \frac{3}{4}\frac{1}{4} = \frac{7}{8}$$

Ainsi B est un anneau euclidien.
Le résultat suivant est l'analogue du lemme de la preuve de 2.3.1

Lemme. *Pour tout nombre premier $p \geq 5$ il existe a, b tels que p divise $a^2 + ab + b^2 + 1$.*

Pour montrer cela, on remarque que les ensembles $\{\alpha^2 | \alpha \in \mathbb{F}_p\}$ et $\{-3\beta^2 - 1 | \beta \in \mathbb{F}_p\}$ s'intersectent donc il existe $\alpha, \beta \in \mathbb{N}$ tels que p divise $\alpha^2 + 3\beta^2 + 1$ et on a

$$\alpha^2 + 3\beta^2 + 1 = (\alpha - \beta)^2 + (2\beta)(\alpha - \beta) + (2\beta)^2 + 1$$

et on en déduit le lemme en posant $a = \alpha - \beta$ et $b = 2\beta$.

On a $2 = 1^2 + 1.0 + 0^2 + 1^2 + 1.0 + 0^1$ et $3 = 2^2 + 2(-1) + (-1)^2 + 0^2 + 0.0 + 0^2$ donc on montre que tout nombre premier ≥ 5 est norme d'un élément de B [2]. Soient donc $p \geq 5$ premier, $a, b \in \mathbb{Z}$ comme dans le lemme, $z = 1 + af + bg$, et $I \triangleq Bp + Bz$. On que $I \subsetneq B$ car tous les éléments de I sont de norme divisible par p, de plus $Bp \subsetneq I$ puisque $z \notin Bp$ car p ne divise pas z (son terme réel est 1). Comme B est euclidien à gauche, il est principal à gauche et donc l'idéal à droite I s'écrit Bt pour $t \in B$ et comme $p \in B$ il existe $s \in B$ tel que $st = p$ donc $N(s)N(t) = p^2$. Comme $Bp \subsetneq I \subsetneq B$, t et s ne sont pas inversible et donc leur norme est différente de 1, ainsi $N(s) = N(t) = p$ on conclut donc le résultat.

2. On a exclu le premier 3 pour être en carctéristique $\neq 3$ dans la preuve du lemme.

3 Application géométrique : Les rotations de $\mathbb{R}^3$ et $\mathbb{R}^4$

3.1 Les quaternions dans $\mathcal{M}_2(\mathbb{C})$

On rappelle la notation $\mathcal{M}_2(\mathbb{C})$ pour la $\mathbb{R}$-algèbre de dimension 8, des matrices carrées de taille 2 a coefficient dans $\mathbb{C}$. Dans cette section nous allons décrire le corps des quaternions comme sous algèbre de $\mathcal{M}_2(\mathbb{C})$.

Definition 3.1.1. *On définit*

$$\mathcal{M}_{\mathbb{H}} \triangleq \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} | \alpha, \beta \in \mathbb{C} \right\}$$

Cet ensemble muni de l'addition et de la multiplication des matrices est un corps non commutatif, et une $\mathbb{R}$-algèbre de dimension 4. Il est isomorphe à $\mathbb{H}$.

On montre que cette définition a du sens. On constate que pour $\alpha = a + bi$ et $\beta = c + di$

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

En notant $1_2, I, J, K$ les matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ respectivement, il apparaît clairement que l'on a un $\mathbb{R}$ espace vectoriel de dimension 4. De plus, la table de multiplication

$\vec{\cdot}$	I	J	K
I	-1_2	K	$-J$
J	$-K$	-1_2	I
K	J	$-I$	-1_2

étant la même que celle de i, j, k du premier chapitre, cela nous montre d'une part la stabilité par multiplication de $\mathcal{M}_{\mathbb{H}}$ mais surtout que $\mathcal{M}_{\mathbb{H}}$ et $\mathbb{H}$ sont isomorphes, par l'isomorphisme de $\mathbb{R}$-algèbre :

$$\begin{array}{rcl} \phi : \mathbb{H} & \longrightarrow & \mathcal{M}_{\mathbb{H}} \\ a + bi + cj + dk & \longmapsto & a1_2 + bI + cJ + dK \end{array}$$

Comme $\mathbb{H}$ est un corps, $\mathcal{M}_{\mathbb{H}}$ en est un aussi. Pour s'en convaincre, il suffit de remarquer que

$$det \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = |\alpha|^2 + |\beta|^2 \neq 0 \iff \alpha \neq 0 \ ou \ \beta \neq 0$$

L'algèbre linéaire élémentaire nous donne l'expression de l'inverse, mais il est bon de voir le lien avec ce que l'on a fait dans le premier chapitre. Ainsi, soit $q = a + bi + cj + dk \in \mathbb{H} \setminus \{0\}$ et $Q = \phi(q)$. On a alors $Q^{-1} = \phi(q^{-1})$ et on a que $q^{-1} = \frac{1}{N(q)}\bar{q}$. On constate d'abord que $detQ = a^2 + b^2 + c^2 + d^2 = N(q)$ donc on a montré que

$$N(q) = det\phi(q)$$

De plus une vérification immédiate montre que $\phi(\bar{q}) = \phi(a-bi-cj-dk) = {}^t\,\overline{Q} = {}^t\,ComQ$, où $\overline{Q}$ est la matrice des coefficients conjugués de Q. On retrouve bien l'expression de l'inverse de Q

$$Q^{-1} = \phi(\frac{1}{N(q)}\bar{q}) = \frac{1}{detQ}\,{}^t\,ComQ$$

Remarque 3.1.2. *On rappelle quelques définitions sur certain sous groupes de $\mathcal{M}_2(\mathbb{C})$. Le* groupe unitaire *$U_2(\mathbb{C})$ est le groupe des matrices $M \in \mathcal{M}_2(\mathbb{C})$ telles que $M\,{}^t\overline{M} = 1_2$. C'est le groupe des isométries de $\mathbb{C}^2$. On s'interessera plus précisément au* groupe spéciale linéaire*, ie le groupe des isométries de determinant 1, ie le groupe des rotations de $\mathbb{C}^2$, noté*

$$SU_2(\mathbb{C}) = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} | \alpha, \beta \in \mathbb{C}, \alpha\bar{\alpha} + \beta\bar{\beta} = 1 \right\}$$

On constate immédiatement que c'est un sous-groupe du groupe multiplicatif de $\mathcal{M}_{\mathbb{H}}$, et il est isomorphe à l'ensemble des quaternions de norme 1.

3.2 Description via le calcul vectoriel élémentaire

On donne ici une dernière description des quaternions en utilisant le calcul vectoriel. $\mathbb{H}$ apparaît comme un espace vectoriel de dimension 4 sur $\mathbb{R}$, ainsi, il existe une structure multiplicative sur $\mathbb{R}^4$ ou plus précisément $\mathbb{R} \times \mathbb{R}^3$ (pour séparer la partie réelle et la partie quaternion pure) qui le rende isomorphe en tant que $\mathbb{R}$-algèbre à $\mathbb{H}$. On notera $\cdot$ le produit scalaire usuel et $\wedge$ le produit vectoriel de $\mathbb{R}^3$: $(x_1, x_2, x_3) \wedge (y_1, y_2, y_3) = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$.
On va exprimer avec $\cdot$ et $\wedge$ le produit quaternionien dans $\mathbb{R} \times \mathbb{R}^3$. On note l'isomorphisme entre $\mathbb{H}$ et $\mathbb{R} \times \mathbb{R}^3$:

$$\begin{array}{rcl} \iota : \mathbb{H} & \longmapsto & \mathbb{R} \times \mathbb{R}^3 \\ a + bi + cj + dk & \longmapsto & (a, (b, c, d)) \end{array}$$

Proposition 3.2.1. *Soient $q = a + a_1i + a_2j + a_3k, r = b + b_1i + b_2j + b_3k \in \mathbb{H}$ et $(a, v) = \iota(q), (b, w) = \iota(r) \in \mathbb{R} \times \mathbb{R}^3$. Alors on a*

$$\iota(qr) = (ab - v \cdot w, aw + bv + v \wedge w)$$

Ainsi le produit définit sur $\mathbb{R} \times \mathbb{R}^3$ par

$$(a, v)(b, w) \triangleq (ab - v \cdot w, aw + bv + v \wedge w)$$

muni $\mathbb{R} \times \mathbb{R}^3$ d'une structure isomorphe à celle de $\mathbb{H}$.

Preuve : C'est une vérification immédiate par calcule : soient $(a, v) = \iota(a + a_1i + a_2j + a_3k)$ et $(b, w) = \iota(b + b_1i + b_2j + b_3k)$ on a alors

$$\begin{array}{rcl} \iota((a + a_1i + a_2j + a_3k)(b + b_1i + b_2j + b_3k)) & = & \iota(ab - a_1b_1 - a_2b_2 - a_3b_3 + a(b_1i + b_2j + b_3ky) \\ +b(a_1i + b_2j + b_3k) & + & [(a_2b_3 - a_3b_2)i + (a_3b_1 - a_1b_3)j + (a_1b_2 - a_2b_1)k]) \\ & = & (ab - v \cdot w, 0) + a\iota(b_1i + b_2j + b_3ky) \\ +b\iota(a_1i + b_2j + b_3k) & + & \iota((a_2b_3 - a_3b_2)i + (a_3b_1 - a_1b_3)j + (a_1b_2 - a_2b_1)k \\ & = & (ab - v \cdot w, 0) + (0, aw) + (0, bv) + (0, v \wedge w) \\ & = & (ab - v \cdot w, aw + bv + v \wedge w) \end{array}$$

L'isomorphisme en question est bien entendu ι. □

On a alors pour $(a, v) = \iota(q)$, $\iota(\bar{q}) = (a, -v)$ et $N((a, v)) = (N(q), 0_{\mathbb{R}^3})$.

En identifiant $\mathcal{M}_{\mathbb{H}}$ et $\mathbb{H}$, l'isomorphisme ci-dessus fournit une bijection entre $SU_2(\mathbb{C})$ et la sphere $\mathbb{S}^3$ de $\mathbb{R}^4$

$$\mathbb{S}^3 = \left\{(x,y,z,t) \in \mathbb{R}^4 | x^2+y^2+z^2+t^2 = 1\right\}$$

De plus, on peut munir $\mathcal{M}_{\mathbb{H}}$ d'une norme définie par $\sqrt{detM}$, et il est immédiat que la bijection est un homéomorphisme pour la topologie définie par la norme sur $SU_2(\mathbb{C})$ et la topologie de $\mathbb{R}^4$ restreinte à $\mathbb{S}^3$. On voit ainsi que $SU_2(\mathbb{C})$ est connexe.

Il est a noter que $\mathbb{H}$ est un espace vectoriel normé isomorphe à $\mathbb{R}^4$. La norme canonique dans le cadre de la définition du premier chapitre est $\sqrt{N(\cdot)}$ ce qui correspond à la norme euclidienne pour $\mathbb{R}^4$.

3.3 Deux isomorphismes remarquables

Dans cette dernière partie, nous allons montrer comment les quaternions peuvent être utilisés pour traduire des rotations de $\mathbb{R}^3$ et de $\mathbb{R}^4$. L'analogue étant l'utilisation des nombres complexes pour traduire les rotations du plan [1].
On utilisera sans distinction les isomorphismes définis précédemment $\mathbb{H} \cong \mathcal{M}_{\mathbb{H}} \cong \mathbb{R} \times \mathbb{R}^3$.

Le premier isomorphisme va mettre en jeu $SU_2(\mathbb{C})$, donc les quaternions de norme 1 et $SO_3(\mathbb{R})$ les rotations de $\mathbb{R}^3$. On va identifier ici $\mathbb{R}^3$ et $\{0\} \times \mathbb{R}^3$ les quaternions purs en notant $*v \in \mathbb{R}^3$ et $v \in \mathbb{H}$ le quaternion pur correspondant (ie tel que $*v = \iota(v)$). Il est important de constater que dans le cas des quaternions purs, on a $*v \wedge *w = *(vw)$, et que donc le calcule quaternionien se ramène au calcul vectoriel (et inversement).

Soit $\theta \in [0, \pi[$ et $*u \in \mathbb{R}^3$ tel que $N(u) = 1$ (ie en fait $*u \in \{0\} \times \mathbb{R}^3 \cap \mathbb{S}^3$). On considère l'automorphisme intérieur de $\mathbb{H}$ définit avec $s = cos\theta + sin\theta\ u$ par

$$\begin{array}{rccc} \overline{R_s} : \mathbb{H} & \longrightarrow & \mathbb{H} \\ q & \longmapsto & sqs^{-1} \end{array}$$

On a $N(s) = N(u) = 1$ donc $s^{-1} = \bar{s}$ et même $u^{-1} = \bar{u} = -u$. $\overline{R_s}$ est une application $\mathbb{R}$-linéaire, et une isométrie de $\mathbb{H}$, puisque $N(sqs^{-1}) = N(s)N(q)N(s^{-1}) = N(q)$. On constate que $\overline{R_s}$ est l'identité sur $\mathbb{R}$ donc l'espace des quaternions purs est stable par $\overline{R_s}$ (une isométrie laisse stable l'orthogonal). On note donc

$$\begin{array}{rccc} R_s : \mathbb{H} \setminus \mathbb{R} \cong \mathbb{R}^3 & \longrightarrow & \mathbb{H} \setminus \mathbb{R} \cong \mathbb{R}^3 \\ q & \longmapsto & sqs^{-1} \end{array}$$

C'est une isométrie de $\mathbb{H} \setminus \mathbb{R}$ et donc induit une isométrie $*R_s$ de $\mathbb{R}^3$. Pour l'identifier, on se place dans une base orthonormée directe complétée de $*u$ $(*u, *v, *w)$. On a donc $uv = -vu = w$, $vw = -wv = u$ et $wu = -uw = v$ (on a en fait fait un changement de base direct de la base (i,j,k) des quaternions purs à travers l'identification dans $\mathbb{R}^3$). On calcule alors la matrice de R_s dans la base (u,v,w) : (on rappelle que $u^2 = -1$ et que $s^{-1} = \bar{s} = cos\theta - sin\theta\ u$)

$$\begin{array}{rcl} R_s(u) & = & sus^{-1} \\ & = & (cos\theta + sin\theta\ u)u(cos\theta - sin\theta\ u) \\ & = & cos^2\theta\ u - sin^2\theta\ u^2u + sin\theta cos\theta(uu - uu) \\ & = & u \end{array}$$

1. En effet les nombres complexes de module 1 et les éléments de $SO_2(\mathbb{R})$ sont en bijection par l'application $e^{i\theta} \mapsto \begin{pmatrix} cos\theta & sin\theta \\ -sin\theta & cos\theta \end{pmatrix}$ cf [Fr] p.76.

On calcule de même :

$$\begin{aligned} R_s(v) &= svs^{-1} \\ &= (cos\theta + sin\theta\ u)v(cos\theta - sin\theta\ u) \\ &= cos^2\theta v - sin^2\theta\ uvu + cos\theta sin\theta(uv - vu) \\ &= (cos^2\theta - sin^2\theta)v + 2cos\theta sin\theta w \\ &= cos(2\theta)v + sin(2\theta)w \end{aligned}$$

et

$$R_s(w) = -sin(2\theta)v + cos(2\theta)w$$

Ce qui donne la matrice de R_s dans la base (u, v, w) (où la matrice de $*R_s$ dans la base $(*u, *v, *v)$) :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(2\theta) & -sin(2\theta) \\ 0 & sin(2\theta) & cos(2\theta) \end{pmatrix}$$

Donc $*R_s$ est la rotation d'angle 2θ autour de la droite $\mathbb{R}u$.
On a donc presque prouvé le resultat suivant. On note $\mathcal{U} = \{s \in \mathbb{H} | N(s) = 1\}$

Théorème 3.3.1 ($SU_2(\mathbb{C})$ et $SO_3(\mathbb{R})$)**.** *L'application*

$$\begin{aligned} \mathcal{U} &\longrightarrow SO_3(\mathbb{R}) \\ s &\longmapsto *R_s \end{aligned}$$

est un homomorphisme de groupe bien définie, surjective et de noyau $\{\pm 1_{\mathbb{H}}\}$*. Autrement dit, par les résultats précédents, on a*

$$SU_2(\mathbb{C}) \Big/ \{\pm 1_2\} \cong SO_3(\mathbb{R})$$

Preuve : Il faut d'abord prouver que tout quaternion de norme 1 s'écrit sous la forme $cos\theta + sin\theta\ u$ avec $u \in \mathbb{H} \setminus \{0\}$ et $N(v) = 1$. Si $s = a + v$ avec $a \in \mathbb{R} \setminus \{0\}$ et v quaternion pur, alors si $N(s) = 1$, comme $\bar{v} = -v$ on a $1 = N(s) = a^2 + N(v)$. Il existe un unique $\theta \in [0, \pi[$ tel que $a = cos\theta$, on pose alors $u = \frac{v}{sin\theta}$ et on a trouvé le bon u. Si $a = 0$ on prend $u = v$. Donc l'application du théorème est bien définie pour tout quaternion de norme 1. Pour montrer que c'est bien un homomorphisme de groupe, on vérifie pour s, t quaternion de norme 1

$$R_t(R_s(q)) = R_t(sqs^{-1}) = tsqs^{-1}t^{-1} = (ts)q(ts)^{-1} = R_{ts}(q)$$

Cet homomorphisme de groupe est surjective par le travaille précédent le théorème, enfin, $R_s = Id$ si et seulement si $\theta \equiv 0\ mod\pi$ et donc $s = cos\theta + sin\theta\ u = \pm 1_{\mathbb{H}}$. □

L'interêt de cet isomorphisme réside dans le fait de pouvoir traduire par une simple multiplication quaternionnienne la composée de deux rotations de $\mathbb{R}^3$.

Corollaire 3.3.2. *Pour* $i = 1$ *ou* 2 *soit* r_i *la rotation de* $\mathbb{R}^3$ *d'angle* $2\theta_i$ *autour de la droite* $\mathbb{R}(*v_i)$ *avec* $N(v_i) = 1$*. Alors la rotation* $r_1 \circ r_2$ *est* R_s *avec*

$$s = (cos\theta_1 + sin\theta_1\ v_1)(cos\theta_2 + sin\theta_2\ v_2) \in \mathbb{H}$$

Vectoriellement :

$$\iota(s) = (cos\theta_1 cos\theta_2 - sin\theta_1 sin\theta_2\ v_1 \cdot v_2, cos\theta_2 sin\theta_1\ v_1 + cos\theta_1 sin\theta_2\ v_2 + sin\theta_1 sin\theta_2\ v_1 \wedge v_2) \in \mathbb{R} \times \mathbb{R}^3$$

Le second isomorphisme remarquable concerne le groupe des rotations de $\mathbb{R}^4$ $SO_4(\mathbb{R})$. Pour $s,t \in \mathcal{U}$, on définit

$$\begin{array}{rccc} R_{s,t} : \mathbb{H} & \longrightarrow & \mathbb{H} \\ q & \longmapsto & sqt^{-1} = sq\bar{t} \end{array}$$

On a encore $N(R_{s,t}(q)) = N(q)$ donc $R_{s,t}$ est bien une isométrie de $\mathbb{H}$. On montre d'abord que c'est bien une isométrie positive, ie un élément de $SO(\mathbb{H})$, qui correspondra à un élément $*R_{s,t} \in SO_4(\mathbb{R})$. Comme $s,t \in \mathcal{U}$ il existe u,u' quaternions purs de norme 1, $\theta,\theta' \in \mathbb{R}$ tels que

$$s = cos\theta + sin\theta\ u \quad t = cos\theta' + sin\theta' u'$$

On peut alors compléter $*u \in \mathbb{R}^3$ et $*u' \in \mathbb{R}^3$ en deux bases orthonormées directe $(*u, *v, *w)$ et $(*u', *v', *w')$ de sorte que $uv = -vu = w$ etc... On exprime alors les matrices des applications $q \mapsto sq$ et $q \mapsto q\bar{t}$ dans les bases $(1,u,v,w)$ et $(1,u',v',w')$ respectivement. Cela donne par calcul,

$$\begin{pmatrix} cos\theta & -sin\theta & 0 & 0 \\ sin\theta & cos\theta & 0 & 0 \\ 0 & 0 & cos\theta & -sin\theta \\ 0 & 0 & sin\theta & cos\theta \end{pmatrix} \quad \begin{pmatrix} cos(\pi-\theta') & -sin(\pi-\theta') & 0 & 0 \\ sin(\pi-\theta') & cos(\pi-\theta') & 0 & 0 \\ 0 & 0 & cos(\pi-\theta') & sin(\pi-\theta') \\ 0 & 0 & -sin(\pi-\theta') & cos(\pi-\theta') \end{pmatrix}$$

Ce sont deux éléments de $SO_4(\mathbb{R})$ donc la composée de ces deux applications $*R_{s,t}$ est bien dans $SO_4(\mathbb{R})$ donc $R_{s,t} \in SO(\mathbb{H})$.

On va montrer que

$$\begin{array}{rccc} R : \mathcal{U} \times \mathcal{U} & \longrightarrow & SO(\mathbb{H}) \\ (s,t) & \longmapsto & R_{s,t} \end{array}$$

est un homomorphisme de groupe surjectif et on va determiner son noyau. On a $R_{s,t} \circ R_{s',t'} = R_{ss',tt'}$, donc R est un homomorphisme de groupe. Maintenant soit $f \in SO(\mathbb{H})$. On va trouver un élément $(x,y) \in \mathcal{U} \times \mathcal{U}$ tel que $f = R_{x,y}$. On pose $s = f(1_{\mathbb{H}}) \in \mathbb{H} \setminus \{0\}$. On a $N(s) = 1$, de plus

$$(R_{s^{-1},1_{\mathbb{H}}} \circ f)(1_{\mathbb{H}}) = s^{-1}s = 1_{\mathbb{H}}$$

Donc $R_{s^{-1},1_{\mathbb{H}}} \circ f$ est une isométrie laissant stable $\mathbb{R}$ et donc son orthogonal les quaternions purs $\mathbb{H} \setminus \mathbb{R} \cong \mathbb{R}^3$. D'apres les résultats précédents le théorème précédent, il existe $r \in \mathcal{U}$ tel que $R_{s^{-1},1_{\mathbb{H}}} \circ f = \overline{R_r}$, donc pour $q \in \mathbb{H}$ on a

$$s^{-1}f(q) = R_{s^{-1},1_{\mathbb{H}}} \circ f(q) = \overline{R_r}(q) = rq\bar{r}$$

On en déduit $f(q) = srq\bar{r}$ donc $f = R_{sr,r}$. On a donc bien la surjectivité de R. On détermine à présent le noyau de R. On suppose que $R_{s,t} = Id$. En évaluant en $1_{\mathbb{H}}$ il vient que $s\bar{t} = st^{-1} = 1$ (car $\bar{t} = t^{-1}$). On a donc $s = t$. En utilisant le théorème précédent, et puisque $R_{s,s} = \overline{R_s} = Id$ il vient que $s = \pm 1_{\mathbb{H}}$. Les éléments du noyau sont donc $(1_{\mathbb{H}}, 1_{\mathbb{H}})$ et $(-1_{\mathbb{H}}, -1_{\mathbb{H}})$. On a finalement montré le théorème suivant :

Théorème 3.3.3 ($SU_2(\mathbb{C})$ et $SO_4(\mathbb{R})$)**.** *L'homomorphisme R définit ci-dessus induit un isomorphisme pour la structure de groupe*

$$SU_2(\mathbb{C}) \times SU_2(\mathbb{C}) \Big/ \{(1_{\mathbb{H}}, 1_{\mathbb{H}}), (-1_{\mathbb{H}}, -1_{\mathbb{H}})\} \cong SO_4(\mathbb{R})$$

Nota Bene. *On a utilisé dans les deux théorèmes le liens étroit entre les quaternions purs et le calcul vectoriel dans $\mathbb{R}^3$. Plus précisément, on s'est ramené pour un quaternion pur u de norme 1 à un vecteur unitaire $*u \in \mathbb{R}^3$, pour construire une base orthonormée $(*u, *v, *w)$ et en déduire 3 quaternions purs (u,v,w) avec lesquels les calculs étaient simplifiés, en vertu du fait que $*(uv) = *u \wedge *v$. Ceci peut se faire directement dans le monde quaternionien en définissant la notion de quaternion pur orthogonal et en montrant que l'on peut construire une base orthogonale à partir d'un quaternion pur. C'est fait dans [Bl] à la page 10. Nous avons dans la section 3.2 fait apparaître le lien direct entre quaternion pur et vecteur de $\mathbb{R}^3$, aussi nous semblait-il plus judicieux de l'utiliser directement.*

Annexe

Voici la table de multiplication de la base de $\mathbb{B}$.

$\curvearrowright$	u	v	w	au	av	aw	a^2u	a^2v	a^2w
u	$2+v$	$u+w$	$v+w$	$au+aw$	$-2au-2av-aw$	$au+av$	a^2v+a^2w	a^2u+a^2v	$-a^2u-2a^2v-2a^2w$
v	$u+w$	$2+w$	$u+v$	$av+aw$	$au+av$	$-au-2av-2aw$	$-2a^2u-a^2v-2a^2w$	a^2u+a^2w	a^2v+a^2w
w	$v+w$	$u+v$	$2+u$	$-2au-av-2aw$	$au+aw$	$av+aw$	a^2u+a^2w	$-2a^2u-2a^2v-a^2w$	a^2u+a^2v
au	$-2au-av-2aw$	$au+aw$	$av+aw$	a^2u+a^2w	$-2a^2u-2a^2v-a^2w$	a^2u+a^2v	$2v+2w$	$2u+2v$	$-2u-4v-4w$
av	$au+aw$	$-2au-2av-aw$	$au+av$	a^2v+a^2w	a^2u+a^2v	$-a^2u-2a^2v-2a^2w$	$-4u-2v-4w$	$2u+2w$	$2v+2w$
aw	$av+aw$	$au+av$	$-au-2av-2aw$	$-2a^2u-a^2v-2a^2w$	a^2u+a^2w	a^2v+a^2w	$2u+2w$	$-4u-4v-2w$	$2v+2w$
a^2u	$-2au-av-2aw$	a^2u+a^2v	a^2v+a^2w	$2u+2v$	$-4u-4v-2w$	$2u+2v$	$2av+2aw$	$2au+2av$	$-2au-4av-4aw$
a^2v	a^2u+a^2w	$-2a^2u-2a^2v-a^2w$	a^2u+a^2v	$2v+2w$	$2u+2v$	$-2u-4v-4w$	$-4au-2av-4aw$	$2au+2av$	$2av+2aw$
a^2w	a^2v+a^2w	a^2u+a^2v	$-a^2u-2a^2v-2a^2w$	$-4u-2v-4w$	$2u+2w$	$2v+2w$	$2au+2aw$	$-4au-4av-2aw$	$2v+2w$

Références

[Bl] A. Blanchard, *Les corps non commutatifs*, PUF (1972)

[L3] A. Szpirglas, *Mathématique L3 Algèbre*, Pearson Education (2009)

[Fr] J. Fresnel, *Espaces quadratiques, euclidiens, hermitiens*, Hermann (1999)

La description des quaternions de façon formelle est entièrement tirée de [Bl] ainsi que le théorème de Frobenius et l'exemple du corps $\mathbb{B}$. La preuve du théorème des deux carrés est inspirée de celle de [L3] et adaptée de façon à ressembler à celle du théorème des quatres carrés par les quaternions d'Hurwitz, que nous avons prise dans [Bl]. L'exemple (2.3.3) est un exercice tiré de [Bl]. Le troisième et dernier chapitre vient de [L3], dont la compréhension à été fortement aidée par [Bl] et [Fr].