Mémoire

Auteur : Govers, Ophélie
Promoteur(s) : Mathonet, Pierre; Zenaïdi, Naïm
Faculté : Faculté des Sciences
Diplôme : Master en sciences mathématiques, à finalité didactique
Année académique : 2021-2022
URI/URL : http://hdl.handle.net/2268.2/14719

Faculté des Sciences
Département de Mathématique

Des nombres complexes aux algèbres à composition

Mémoire de fin d'études présenté en vue de l'obtention du titre de
Master en Sciences Mathématiques, à finalité didactique

Année académique 2021-2022

Auteur :
Ophélie GOVERS

Promoteur :
Pierre MATHONET

Co-Promoteur :
Naïm ZENAÏDI

"Ce n'est pas les coups que nous avons pris qui comptent,
mais ceux auxquels nous avons survécu."
Stephen King

Remerciements

Je tiens avant tout à remercier chaleureusement mon promoteur Monsieur Mathonet, pour son aide précieuse, sa disponibilité et les relectures apportées à mon mémoire. Je garderais un merveilleux souvenir de nos échanges. Je remercie également Monsieur Zenaïdi de m'avoir écoutée et guidée dans le choix de mon sujet de mémoire ainsi que Monsieur Balhan pour sa relecture attentive et son aide lors de l'élaboration de la partie didactique de ce travail. Merci à eux trois pour leur bienveillance et leur soutien depuis mon premier bachelier et plus particulièrement lors de cette dernière année.

Merci également à Monsieur Rigo et Madame Esser de prendre part au jury de ce mémoire.

Je voudrais également dire merci à mes amis Claire, Maxime, Julie, Sacha et Jeanne pour les bons moments passés ensemble lors des cinq premières années. Et un grand merci à Antoine et Elodie pour m'avoir épaulée et écoutée ces deux dernières années, elles n'auraient pas été pareilles sans vous.

Je tiens encore à remercier mes proches de m'avoir encouragée et soutenue dans chacun de mes projets et de m'avoir permis de réaliser les études que je désirais malgré les soucis de santé auxquels j'étais confrontée. J'imagine ô combien cela a dû être stressant pour vous. Je remercie tout particulièrement mon compagnon qui a vécu, presque autant que moi, toutes ces années de doutes, de peurs mais également de bonheur et de folie. Cet aboutissement qui est le mien est également le vôtre.

Finalement, je souhaite remercier toutes les personnes qui ont jugé, à tort, que je ne m'en sortirais pas. J'ai, au travers de vos jugements, puisé la détermination dont j'avais besoin pour mener mes études à bien ainsi que pour la réalisation de ce mémoire, ce qui m'a permis de montrer que vous ne me connaissiez pas.

Table des matières

Introduction

Les nombres complexes représentent, ou tout du moins représentaient, un chapitre important du programme de cours pour les élèves de dernière année de certaines filières de l'enseignement secondaire. Cette matière, présentée en dernière année, peut être perçue par les élèves comme surplombant toutes les autres, celle au-dessus de laquelle il n'y a rien, donc forcément difficile.

Ces nombres, que l'on appelle d'ailleurs complexes, sont souvent présentés comme un moyen de donner des solutions à des équations qui n'en ont pas (quelle idée !), ils ne semblent correspondre à aucune grandeur, contrairement à ceux présentés jusque là, et il est donc bien normal qu'on ne sache pas bien ce qu'ils représentent.

Ajoutez à cela qu'on ne peut plus les comparer, et que le professeur, soit demande aux élèves de faire acte de foi, en leur demandant de croire que cela existe bien, soit passe son temps à expliquer qu'ils existent bien et à en démontrer certaines propriétés (dont on ne sait pas l'utilité), et on comprend que ce chapitre puisse paraitre dénué de sens.

Dans ce mémoire, dans un premier temps, nous analysons l'histoire de l'introduction des nombres complexes, en partant de la résolution des équations du troisième et du quatrième degré par les mathématiciens italiens de la renaissance, Tartaglia, Del Ferro et Cardan. Nous détaillons la méthode de résolution aujourd'hui attribuée à Cardan. Cette méthode pourrait certainement servir en classe d'introduction au chapitre sur les nombres complexes. Cependant, elle ne donne pas de solution pour certaines équations qui en ont pourtant visiblement. C'est ce que Bombelli remarque. Il constate qu'en poursuivant les calculs, en extrayant des racines de nombres négatifs, il permet à la méthode de continuer à fonctionner. Les nombres complexes apparaissent dès lors comme une réponse à un problème donné, concret (qui possède une solution), un moyen de calcul que les mathématiciens mettrons plusieurs siècles à justifier rigoureusement.

Nous analysons ensuite plusieurs méthodes pour introduire les nombres complexes, notamment comme des similitudes du plan, qui fixent l'origine. Cette approche à l'avantage de permettre de donner un sens plus intuitif à la multiplication des nombres complexes, que l'on impose souvent aux élèves. Elle permet une approche ancrée dans le sensible des nombres complexes, et permet d'éviter le questionnement sur leur existence. Elle repose sur le fait que le module (la norme) du produit de nombres complexes est égal au produit de leurs normes.

C'est cette propriété qui guide Hamilton quand, après avoir écrit les complexes comme des couples de réels, il tente de définir une multiplication des triplets, puis se rend compte, dans le célèbre éclair de génie du pont de Broome, qu'il doit considérer des quadruplets, abandonner la commutativité, et il définit finalement les quaternions, une première généralisation des nombres complexes. C'est cette propriété qui fait des complexes et des quaternions des algèbres à composition.

Après avoir étudié les quaternions et montré qu'ils pouvaient être obtenus comme couples de nombres complexes, à l'aide d'une multiplication qui généralise celle des complexes, il est naturel de tenter de poursuivre la construction. On obtient ainsi une quatrième algèbre à composition, celle des octonions, qui n'est plus commutative, mais plus associative non plus.

On pourrait poursuivre plus loin ce processus de doublement (de Dickson), mais l'algèbre obtenue n'est alors plus une algèbre à composition. C'est en fait l'objet du théorème d'Hurwitz de démontrer que les seules algèbres à composition (avec unité) sont celles formées par les nombres réels, les nombres complexes, les quaternions et les octonions.

L'existence de ces structures, et d'autres généralisations montrent que les nombres complexes, en plus d'être omniprésents dans les théories mathématiques (et physiques), ne sont que le point de départ vers d'autres ensembles de nombres abstraits, tout aussi utiles. Je m'arrête aux algèbres à composition, tout en ayant rencontré les identités de Moufang et aperçu de loin les algèbres de Clifford.

Nous terminons avec un chapitre qui étudie quelques applications théoriques des algèbres ainsi définies : nous commençons par le lien entre les isométries en dimension 2 et la multiplication par des nombres complexes de module 1, nous étudions ensuite les isométries en dimension 3 et 4 et les liens avec les quaternions de module 1 et le groupe unitaire $SU(2)$. Cela donne des paramétrisations et isomorphismes de certains groupes de Lie de basse dimension. Enfin, nous caractérisons les groupes d'automorphismes des réels, des complexes et des quaternions, et nous donnons les premières propriétés des automorphismes des octonions, qui donnent lieu à un groupe de Lie de dimension 14.

Plus précisément, le mémoire s'articulera en quatre chapitres de la façon suivante.
Le premier chapitre traitera de l'histoire des nombres complexes. On relatera certains développements que les mathématiciens de la renaissance auraient pu faire (toutefois avec des notations anachroniques), mais nous joindrons également un brin d'analyse moderne. Ensuite, nous nous intéresserons à l'aspect didactique de leur enseignement. Pour ce faire, les méthodes d'introduction des nombres complexes comme couples de nombres réels, par les similitudes ou encore par les matrices seront présentées. Pour chacune d'entre elles, une analyse didactique succincte sera faite, présentant les atouts et les faiblesses de chaque méthode.

Le second chapitre consistera en l'introduction des quaternions et s'articulera en trois parties aussi importantes les unes que les autres. Dans un premier temps, un regard historique sur leur découverte sera fait, de l'irrésistible envie de Sir William Rowan Hamilton à effectuer des opérations sur des triplets jusqu'à la célèbre formule fondamentale des quaternions

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

présente sur le pont de Broome, en passant par l'abandon d'une propriété sur leur multiplication. Nous montrerons comment cette formule, sous réserve de propriétés fondamentales que l'on peut demander à la multiplication, conduit à la multiplication des quaternions. Ainsi, alors que pour passer de $\mathbb{R}$ à $\mathbb{C}$ nous avions perdu la notion d'ordre, pour passer de $\mathbb{C}$ à $\mathbb{H}$ nous perdons la commutativité du produit. Nous montrons comment Hamilton en est venu à considérer des produits non commutatifs.
Dans un second temps, trois définitions seront présentées. Après avoir posé les définitions et les propriétés associées, nous montrerons que l'ensemble des quaternions muni d'une addition et d'une multiplication adéquate forme une algèbre. Qui plus est, nous serons même en mesure de spécifier qu'il s'agit d'une algèbre à composition. Pour finir cette seconde partie, nous serons en mesure de prouver que l'ensemble des quaternions est également un corps, appelé corps des quaternions.
Pour terminer ce chapitre, une approche des quaternions par les matrices 2×2 à coefficients complexes permettra de re-démontrer, d'une autre façon, que l'ensemble des quaternions muni de la somme et du produit matriciel usuel est une algèbre et que celle-ci est en réalité une algèbre à division associative.

Ensuite, dans le troisième chapitre de ce mémoire nous développerons les octonions. Ceux-ci seront définis comme couples de quaternions. Une définition sera donnée pour les opérations d'addition, de multiplication, de conjugaison, de norme et d'inverse et les propriétés s'y référant seront explicitement démontrées ce qui nous permettra d'attester que l'ensemble des octonions muni des opérations adéquates est une algèbre à composition et à division. Toutefois, nous constaterons que cette algèbre possède une propriété plus faible que l'associativité, ce qu'on appelle l'alternativité. Effectivement, pour passer de $\mathbb{H}$ à $\mathbb{O}$, la multiplication a, une nouvelle fois, perdu une propriété : l'associativité. Ainsi, nous nous apercevrons que, lorsqu'on double la dimension de l'algèbre, on en perd une propriété importante. Nous pourrions donc nous demander jusqu'où ce processus pourrait nous emmener. C'est ce dont il s'agira dans la deuxième et dernière section de ce troisième chapitre. Après avoir explicité de processus de doublement de Dickson, nous enchaînerons avec la démonstration du théorème d'Hurwitz qui, comme nous l'avons déjà indiqué, stipule ceci :

Si Z est une algèbre à composition avec unité, alors $Z = \mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$.

Mais qu'en est-il lorsque Z est une algèbre à composition quelconque ? Dans ce cas, on montrera que Z est une algèbre isotope de à $\mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$. Cela constituera le théorème d'Hurwitz généralisé et nous en ferons également la démonstration.

Pour finir, le quatrième chapitre commencera par une description des groupes de rotations en toute dimension. Ces résultats généraux permettront de décrire des groupes d'isométries en dimension $2, 3, 4$ à l'aide de complexes et de quaternions ou de couples de quaternions. Nous utiliserons certaines de ces caractérisations pour étudier les groupes d'automorphismes des algèbres à composition. Dans cette optique, nous montrerons que le groupe des automorphismes de $\mathbb{R}$ est l'identité, que celui de $\mathbb{C}$ est isomorphe à $\mathbb{Z}_2$, que le groupe des automorphismes de $\mathbb{H}$ est isomorphe à $SO(3)$ et nous montrerons que le groupe des automorphismes de $\mathbb{O}$ est un groupe de Lie de dimension 14.

Chapitre 1

Les nombres complexes

1.1 Analyse de l'introduction des nombres complexes par Cardan et Bombelli

Il est difficile pour toute personne ayant appris les nombres complexes d'imaginer que la solution i de l'équation quadratique $x^2 + 1 = 0$ ait pu poser problème à l'époque tant cela nous est devenu banal, un peu comme nous acceptons sans difficulté l'existence des nombres entiers négatifs. Pourtant, les nombres complexes ont mis longtemps avant d'être reconnus et acceptés par les mathématiciens comme étant des nombres, au même titre que les naturels ou encore les rationnels.
Les propos relatés dans la présente section sont principalement tirés du livre *An Imaginary Tale, the story of* $\sqrt{-1}$ écrit par Paul J. Nahin et chapitre trois du livre intitulé *Numbers* écrit par Ebbinghaus que les lecteurs de ce travail peuvent retrouver aux références [15] et [19].

C'est à la Renaissance que les quantités imaginaires ont fait leur première apparition. En 1535, Niccolo Fontana, connu aujourd'hui sous le patronyme de *Tartaglia*, mathématicien italien, trouva la résolution des équations du troisième degré lors d'une confrontation avec un des élèves de Scipione Del Ferro [1], dans laquelle il leur était demandé de résoudre un certain nombre d'équations de ce type. Conscient de la richesse de cette découverte il tint cette formule secrète plusieurs années. En 1539, un mathématicien et physicien italien du nom de Girolamo *Cardano* eu connaissance de ce secret gardé par Tartaglia, il le persuada de lui révéler la formule contre l'assurance de lui faire rencontrer le gouverneur de Milan et lui promettant de ne jamais la révéler. Cardan développa les calculs et trouva une méthode générale, la désormais célèbre "formule de Cardan". Impatient de publier sa découverte, il brisa sa promesse faite à Tartaglia prenant prétexte de la découverte d'un carnet dans lequel Del Ferro décrivait le calcul, et ce avant que Tartaglia ne la découvrit. Des conflits s'en suivirent et Cardan refusa d'en débattre avec Tartaglia. Il laissa le soin à son élève Ludovico Ferrari, qui venait de découvrir une méthode permettant de résoudre des équations du quatrième degré, de répondre publiquement à Tartaglia. Ridiculisé lors d'un débat oratoire par Ferrari en raison de ses défauts d'élocution, Tartaglia fut renvoyé de son poste de professeur de mathématiques.
Ainsi, il existe une formule universelle, appelée de nos jours *"formule de Cardan"*, permettant de déterminer une racine de l'équation particulière du troisième degré $x^3 + px + q = 0$. Cette

1. Scipione Del Ferro $(1465 - 1526)$ est un mathématicien né à Bologne, en Italie, qui enseigna l'arithmétique et l'algèbre à l'Université de cette même ville. Il est connu comme étant le premier à avoir découvert la résolution des équations du troisième degré du type $x^3 + px = q$ avec $p, q > 0$.

formule est donnée par l'expression

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{4p^3 + 27q^2}{108}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{4p^3 + 27q^2}{108}}}$$

Pour arriver à ce résultat, Cardan considéra en premier lieu l'équation du troisième degré réduite ci-dessous

$$x^3 + px + q = 0 \quad p, q \neq 0.\text{[2]} \tag{1.1}$$

La proposition suivante montre qu'il est en effet toujours possible d'arriver à une telle équation réduite à partir d'une équation polynomiale de degré 3 de la forme $ax^3 + bx^2 + cx + d = 0$.

Lemme 1.1.1 (Equation cubique réduite)**.** *Soit $P(x) = ax^3 + bx^2 + cx + d$ un polynôme de degré 3 en l'indéterminée x dont les coefficients a, b, c, d sont complexes (resp. réels). Alors, il existe $\alpha \in \mathbb{C}$ (resp. $\alpha \in \mathbb{R}$) tel que $Q(x) = P(x - \alpha)$ soit sans terme quadratique.*

Démonstration. Il suffit d'écrire le polynôme $Q(x)$. En effet,

$$\begin{aligned} P(x-\alpha) &= a(x-\alpha)^3 + b(x-\alpha)^2 + c(x-\alpha) + d \\ &= a(x^3 - 3x^2\alpha + 3x\alpha^2 - \alpha^3) + b(x^2 - 2\alpha x + \alpha^2) + c(x-\alpha) + d \\ &= ax^3 + (-3a\alpha + b)x^2 + (3a\alpha^2 - 2\alpha b + c)x + (-a\alpha^3 + b\alpha^2 - c\alpha + d). \end{aligned}$$

Dès lors, considérer $\alpha = \frac{b}{3a}$ convient. □

Remarque 1.1.2. Pour passer d'une équation polynomiale du second degré à une équation du second degré sans terme du premier degré, nous aurions dû considérer $\alpha = \frac{b}{2a}$.

Cardan considéra alors x une solution de l'équation 1.1 et posa $x = u + v$. Il considéra que ce devait être non nul sans quoi q serait égal à zéro. Ainsi il vint

$$\begin{aligned} (u+v)^3 = x^3 &\Leftrightarrow u^3 + 3u^2v + 3uv^2 + v^3 = x^3 \\ &\Leftrightarrow u^3 + v^3 + 3uv(u+v) = x^3. \end{aligned}$$

Par conséquent, en utilisant cette condition, il réécrivit l'équation cubique réduite $x^3+px+q = 0$ sous la forme

$$u^3 + v^3 + 3uv(u+v) + p(u+v) + q = 0,$$

ou encore comme

$$u^3 + v^3 + q + (u+v)(3uv + p) = 0 \tag{1.2}$$

si on regroupe les termes. Ayant un degré de liberté supplémentaire par rapport à l'équation initiale, il fit le choix de poser la condition supplémentaire $3uv + p = 0$. Ainsi, il développa l'équation 1.2 en un système de deux équations

$$\begin{cases} u^3 + v^3 + q &= 0 \\ 3uv + p &= 0. \end{cases}$$

Il résolut ce système par rapport aux inconnues u^3 et v^3 et obtint les équivalences suivantes

$$\begin{aligned} \begin{cases} u^3 + v^3 + q &= 0 \\ 3uv + p &= 0 \end{cases} &\Leftrightarrow \begin{cases} u^3 + v^3 &= -q \\ 3uv + p &= 0 \end{cases} \\ &\Leftrightarrow \begin{cases} u^3 + v^3 &= -q \\ uv &= \frac{-p}{3} \end{cases} \\ &\Leftrightarrow \begin{cases} u^3 + v^3 &= -q \\ u^3v^3 &= -\frac{p^3}{27}. \end{cases} \end{aligned}$$

2. Comme déjà dit à la note de bas de page précédente, Del Ferro considérait quant à lui l'équation cubique réduite sous la forme $x^3 + px = q$ avec $p, q > 0$. Lorsque p était négatif, il considérait alors l'équation $x^3 = px + q$ et cela constituait un autre problème. Chaque forme d'équation possédait sa propre résolution.

Par le théorème de la somme et du produit de deux racines [3], Cardan en conclut que u^3 et v^3 étaient solutions de l'équation du second degré $z^2-(u^3+v^3)z+u^3v^3=0$. Cette équation admet une solution si la condition $(u^3+v^3)^2-4u^3v^3 \geq 0$ est satisfaite. En d'autres termes, u^3 et v^3 sont solutions de l'équation du second degré

$$z^2+qz-\frac{p^3}{27}=0 \tag{1.3}$$

pour autant que la condition $q^2+\frac{4}{27}p^3 \geq 0$ soit vérifiée.
Dans ce cas, une fois qu'il eut calculé le discriminant de l'équation 1.3, les solutions prirent la forme

$$u^3=\frac{1}{2}\left(-q+\sqrt{q^2+\frac{4p^3}{27}}\right) \quad \text{et} \quad v^3=\frac{1}{2}\left(-q-\sqrt{q^2+\frac{4p^3}{27}}\right), \tag{1.4}$$

ou encore

$$u=\sqrt[3]{\frac{-q}{2}+\sqrt{\frac{4p^3+27q^2}{108}}} \quad \text{et} \quad v=\sqrt[3]{\frac{-q}{2}-\sqrt{\frac{4p^3+27q^2}{108}}}. \tag{1.5}$$

Faisons un un aparté quelques instant pour remarquer que, de nos jours on sait que u^3 et v^3 donnés par 1.4 admettent trois racines cubiques complexes. Toutefois, Cardan travaillait sur $\mathbb{R}$, et dans ce cas une seule racine cubique pour u^3 et v^3 existe et elle est donnée par 1.5. C'est dans ces conditions que nous nous plaçons.
Cardan en vint à la conclusion que, si $4p^3+27q^2 \geq 0$, l'équation du troisième degré $x^3+px+q=0$ admettait la solution réelle

$$x=\sqrt[3]{\frac{-q}{2}+\sqrt{\frac{4p^3+27q^2}{108}}}+\sqrt[3]{\frac{-q}{2}-\sqrt{\frac{4p^3+27q^2}{108}}}. \tag{1.6}$$

Avant de continuer à conter l'histoire des nombres complexes, tentons de répondre à une question qui s'offre à nous. En effet, dans le cheminement que nous venons de retracer ci-dessus, Cardan a utilisé, comme Scipione Del Ferro avant lui, le changement de variable $x=u+v$. Mais comment a-t-il su que cela résoudrait le problème ? Et, est-il toujours possible de poser un tel changement de variable qui satisfait de plus la condition choisie $3uv+p=0$?
Pour répondre à la première question, je propose simplement de faire part des propos de Mark Kac (1914 − 1984), mathématicien américano-polonais, repris à la page 9 de l'ouvrage *"An Imaginary tale, the story of* $\sqrt{-1}$ *"*, disponible à la référence [19], à propos de Del Ferro : "An ordinary genius is a fellow that you and I would be just as good as, if we were only many times better. There is no mystery as to how his mind works. Once we understand what he has done, we feel certain that we, too, could have done it. It is different with the magician (genius)... the working of their minds is for all intents and purposes incomprehensible. Even after we understand what they have done, the process by which they have done it is completely dark. Del Ferro's idea was of the magician class."
Pour répondre à la seconde question, nous continuons avec le lemme suivant.

3. Le théorème de la somme et du produit de deux racines nous dit que si le trinôme $ax^2+bx+c=0$ admet deux racines distinctes ou confondues, alors leur somme S et leur produit P vérifient $S=\frac{-b}{a}$ et $P=\frac{c}{a}$ respectivement.

Lemme 1.1.3 (Astuce de Tartaglia-Cardan). *Soient $p \neq 0$ et x deux nombres complexes. Alors il existe $u, v \in \mathbb{C}_0$ tels que*

$$\begin{cases} x &= u+v \\ uv &= -\frac{p}{3} \end{cases} \tag{1.7}$$

Démonstration. En substituant la première équation dans la seconde, nous obtenons l'équation du second degré en l'inconnue v suivante

$$v^2 - vx - \frac{p}{3} = 0, \tag{1.8}$$

dont le discriminant est $\Delta = x^2 + \frac{4p}{3}$. Dès lors, les solutions de l'équation ci-dessus sont données par

$$v = \frac{x \pm \sqrt{x^2 + \frac{4p}{3}}}{2}.$$

où $\sqrt{x^2 + \frac{4p}{3}}$ désigne un des deux nombres dont le carré est $x^2 + \frac{4p}{3}$. Par exemple, on constate que les nombres complexes u et v définis par

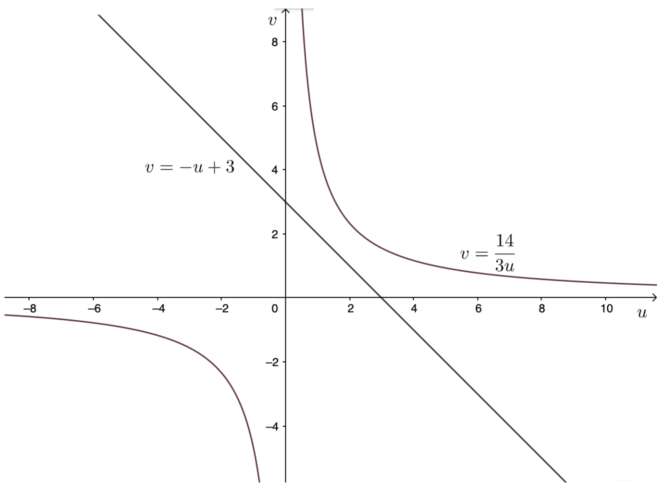
$$\begin{cases} u &= x - v \\ v &= \frac{x - \sqrt{x^2 + \frac{4p}{3}}}{2} \end{cases}$$

satisfont au système (1.7). □

Ainsi, dans le cas où x et p sont deux nombres complexes non nuls, l'astuce proposée par Del Ferro (et Cardan) prend tout son sens. Cependant, ce n'est plus le cas lorsque x et p désignent des nombres réels. En effet, dans ce cas, si $x^2 + \frac{4p}{3}$ est négatif alors la racine carrée de ce nombre n'est pas définie. Une autre justification serait d'en faire une interprétation graphique dans laquelle l'axe des abscisses représente la variable u et l'axe des ordonnées la variable v. Le système 1.7 peut alors se réécrire sous la forme

$$\begin{cases} v &= -u + x \\ v &= -\frac{p}{3u} \end{cases} \tag{1.9}$$

Si nous supposons que $x = 3$ et $p = -14$, le système d'équations 1.9 se traduit graphiquement comme ci-dessous où il est alors évident que ce système ne possède pas de solution.



Finalement, grâce à ces deux lemmes, nous sommes désormais en mesure de prouver le théorème suivant permettant de résoudre les équations polynomiales de troisième degré par radicaux.

Théoreme 1.1.4 (Formule de Del Ferro-Cardan-Tartaglia)**.** *Soit*

$$P(x) = x^3 + px + q \tag{1.10}$$

un polynôme du troisième degré réduit à coefficients p et q complexes. Alors, l'équation

$$P(x) = 0 \tag{1.11}$$

admet exactement 3 solutions complexes x_0, x_1, x_2 données par les formules suivantes

$$\begin{cases} x_0 &= u_0 + v_0 \\ x_1 &= ju_0 + \bar{j}v_0 \\ x_2 &= j^2u_0 + \bar{j}^2v_0 \end{cases}$$

où $j = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$ et

$$\begin{cases} u_0 \text{ est une racine cubique de } \frac{-q+\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} \\ v_0 \text{ est une racine cubique de } \frac{-q-\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} \end{cases}$$

satisfont la condition $u_0v_0 = -\frac{p}{3}$.

Démonstration. Tout d'abord, le lemme 1.1.1 nous indique que tout polynôme du troisième degré peut prendre la forme escomptée 1.10.
Si $p = 0$ alors l'équation 1.11 se réécrit

$$x^3 + q = 0,$$

ce qui est équivalent à

$$x = \sqrt[3]{-q}.$$

Ensuite, si $p \neq 0$, les équivalences logiques ci-dessous ont bien lieu :

$$\begin{aligned}
\begin{cases} x_0 \in \mathbb{C} \\ P(x_0) = 0 \end{cases} &\Leftrightarrow \exists u_0, v_0 \in \mathbb{C} : \begin{cases} x_0 = u_0 + v_0 \\ u_0v_0 = -\frac{p}{3} \\ P(u_0 + v_0) = 0 \end{cases} \\
&\Leftrightarrow \exists u_0, v_0 \in \mathbb{C} : \begin{cases} x_0 = u_0 + v_0 \\ u_0v_0 = -\frac{p}{3} \\ u_0^3 + v_0^3 = -q \end{cases} \\
&\Leftrightarrow \exists u_0, v_0 \in \mathbb{C} : \begin{cases} x_0 = u_0 + v_0 \\ u_0v_0 = -\frac{p}{3} \\ u_0^3v_0^3 = -\frac{p^3}{27} \\ u_0^3 + v_0^3 = -q \end{cases} \\
&\Leftrightarrow \exists u_0, v_0 \in \mathbb{C} : \begin{cases} x_0 = u_0 + v_0 \\ u_0^3 \text{ et } v_0^3 \text{ sont solutions de l'équation } z^2 + qz - \frac{p^3}{27} = 0 \end{cases} \\
&\Leftrightarrow \exists u_0, v_0 \in \mathbb{C} : \begin{cases} x_0 = u_0 + v_0 \\ u_0v_0 = -\frac{p}{3} \\ u_0^3 = \frac{-q+\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} \text{ et } v_0^3 = \frac{-q-\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} \\ \text{ou} \\ u_0^3 = \frac{-q-\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} \text{ et } v_0^3 = \frac{-q+\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} \end{cases} \\
&\Leftrightarrow \begin{cases} u_0 (\text{resp. } v_0) \text{ est une racine cubique de } \frac{-q+\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} (\text{resp. } \frac{-q-\sqrt[3]{q^2+\frac{4p^3}{27}}}{2}) \\ \text{ou} \\ u_0 (\text{resp. } v_0) \text{ est une racine cubique de } \frac{-q-\sqrt[3]{q^2+\frac{4p^3}{27}}}{2} (\text{resp. } \frac{-q+\sqrt[3]{q^2+\frac{4p^3}{27}}}{2}) \end{cases}
\end{aligned}$$

□

Ainsi, si $4p^3 + 27q^2 \geq 0$, alors l'équation cubique réduite admet la solution réelle donnée en 1.6. Mais qu'advenait-il lorsque $4p^3 + 27q^2 \leq 0$? Pour les mathématiciens de l'époque, l'équation considérée n'admettait tout simplement pas de solution. C'est *Bombelli*, mathématicien italien $(1526 - 1572)$ qui, quelques années plus tard, permit de résoudre toutes les équations du troisième degré. À l'époque, il travaillait sur l'équation cubique $x^3 = 15x + 4$. Il appliqua la méthode de Cardan à cette équation et obtint la solution

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Nous savons aujourd'hui que nous ne pouvons écrire de telles expressions, mais à l'époque les mathématiques n'étaient pas aussi rigoureuses qu'elles ne le sont aujourd'hui, et ce résultat traduit simplement la "solution" que Bombelli avait obtenue en appliquant la formule de Cardan à l'équation $x^3 = 15x + 4$. Bombelli était perplexe face à ce résultat. En effet, il savait que 4 était solution de l'équation et pourtant, la méthode de Cardan ne permettait de la voir. C'est alors qu'il décida de contourner l'obstacle face auquel il se trouvait en procédant comme si la racine carrée de -121 était un nombre comme un autre. Il comprit que l'expression étrange donnée par la formule de Cardan est un nombre réel, simplement écrit d'une manière qui ne lui était pas familière. Bombelli observa que si la solution donnée par Cardan est réelle alors c'est que $\sqrt[3]{2 + \sqrt{-121}}$ et $\sqrt[3]{2 - \sqrt{-121}}$ sont deux conjugués. En d'autres mots, si a et b désignent des nombres réels tels que

$$\sqrt[3]{2 + \sqrt{-121}} = a + b\sqrt{-1} \quad \text{et} \quad \sqrt[3]{2 - \sqrt{-121}} = a - b\sqrt{-1},$$

alors $x = 2a$, désigne bel et bien une solution réelle. Dans ces conditions et après calculs, Bombelli en vint à considérer que a était égal à 2 et que b était égal à 1. Ainsi, il fit la conclusion que

$$\sqrt[3]{2 + \sqrt{-121}} = 2 + \sqrt{-1} \quad \text{et} \quad \sqrt[3]{2 - \sqrt{-121}} = 2 - \sqrt{-1}.$$

Ce faisant, il pu réécrire l'expression de la solution de l'équation $x^3 = 15x + 4$ sous la forme

$$x = 2 + \sqrt{-1} + 2 - \sqrt{-1} = 2 + 2 = 4,$$

et il obtint la valeur de x qu'il espérait tant.

Plus tard, dans son oeuvre intitulée "La géométrie", *René Descartes*, mathématicien, physicien et philosophe français du $XVII^e$ siècle, développa l'idée selon laquelle il n'est pas absurde d'imaginer que toute équation polynomiale possède un nombre de racines égal au degré de son polynôme correspondant, mais que toutefois ces racines imaginaires n'ont pas toujours leur pendant en nombre réel. Dans les années 1670, *Gottfried Wilhem Liebniz* nota l'étonnante relation

$$\sqrt{1 + \sqrt{-3}} + \sqrt{1 - \sqrt{-3}} = \sqrt{6},$$

ce qui contribua à l'enrichissement de la théorie des imaginaires. Vint ensuite la période d'*Euler*, mathématicien suisse (1707-1783) qui n'avait aucune crainte à utiliser les nombres complexes dans ses calculs. Il ne se souciait guère de démontrer des résultats qui lui semblaient intuitifs et c'est notamment pour cela qu'il éprouva de grandes difficultés à expliquer et à définir les nombres imaginaires (comme ils étaient appelés à l'époque). Euler était seulement capable de dire que la racine carrée d'un nombre négatif ne peut être comparée à zéro, elle n'est ni plus grande, ni plus petite, ni égale à zéro. Il nota que, étant donné que la racine carrée d'un nombre négatif ne pouvait être reconnue comme un nombre possible, c'est qu'elle devait être un nombre impossible, un nombre imaginaire qui n'existait que dans notre imagination. À la fin de sa vie, en 1777, Euler éclaira la dernière notation ambigüe $\sqrt{-1}$ en la remplaçant par la lettre i. Jusqu'alors, les nombres complexes n'avaient pas d'interprétation géométrique. Nous devons à *John Wallis*, mathématicien anglais $(1616 - 1703)$, la première notion d'une correspondance entre les nombres complexes et les points du plan. Néanmoins ses idées n'eurent exercé aucune influence majeure sur les autres mathématiciens de son époque. C'est le norvégien *Caspar Wessel* $(1745 - 1818)$ qui, pour la première fois, représenta les points du plan comme des nombres complexes et contrairement à son homologue anglais, ses résultats eurent plus d'impact dans le monde des mathématiques. Son objectif premier fut de pouvoir réaliser des opérations sur des segments de droite orientés et pour ce faire, ayant une certaine connaissance des nombres complexes, il décida de représenter lesdits segments sous forme de nombres complexes, et non l'inverse. Pour ce faire, Caspar Wessel introduisit un axe imaginaire perpendiculaire à l'axe des réels et interpréta les vecteurs du plan comme des nombres complexes. Seulement, malgré ses considérables résultats, son travail resta discret auprès de la communauté scientifique jusqu'à sa traduction en français en 1897. Début du XIX^e siècle, un comptable suisse du nom de *Jean Robert Argand* $(1768 - 1822)$ présenta une autre interprétation géométrique des nombres complexes. Argand était un mathématicien amateur et il interpréta de façon un peu saugrenue $\sqrt{-1}$ comme une rotation de 90 degrés du point $(1, 0)$ dans le plan, justifiant cela par le fait que composer deux telles rotations donnait le résultat escompté de -1. En réalité, cette interprétation géométrique avait été découverte quelques années plus tôt par Wessel qui avait publié un article sur le sujet mais il n'eut cependant pas la reconnaissance de la communauté mathématique.

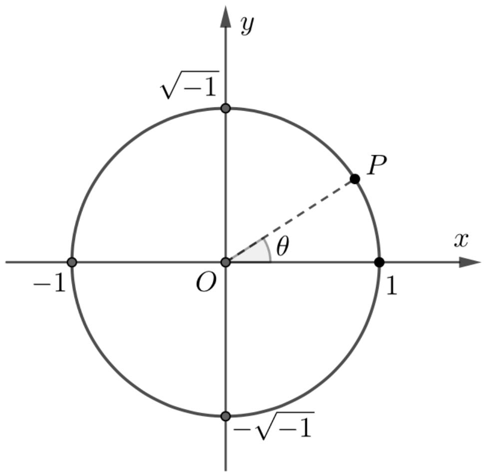


FIGURE 1.1 – Illustration du plan de Jean Robert Argand

Carl Friedrich Gauss, astronome, mathématicien et physicien allemand (1777-1855), connaissait l'interprétation des nombres complexes comme points du plan dès 1796. Grâce à lui, les nombres complexes prirent progressivement une place de plus en plus importante dans le domaine de la science. L'année 1811, il écrivit notamment à *Bessel*, astronome, mathématicien, géodésien et physicien allemand, ceci (Werke 8, p.90) : "... Just as one can think of the whole domain of real magnitudes as being represented by an infinite straight line, so the complete domain of all magnitudes, real and imaginary numbers alike, can be visualized as an infinite plane, in which the point definied by the ordinate b and the abscissa a, likewize represents the magnitude $a + ib$." Quatre années plus tard, la théorie de la géométrie des nombres complexes n'avait plus de secret pour Gauss, mais il lui fallut attendre 1831 et la publication de son ouvrage intitulé "Theoria Residorum Biquadraticorum" pour que la diffusion de la théorie des nombres complexes se produise. Gauss essaya de démystifier les nombres complexes en déclarant

que la part de mystère qui les entoure n'était due qu'à une terminologie inadaptée. Il écrivit notamment (Werke 2, p. 177-178) : "Had $+1, -1$ and $\sqrt{-1}$, instead of being called positive, negative and imaginary (or worse still impossible) unity, been given the names, say, of direct, inverse and lateral unity, there would hardly have been any scope for such obscurity." Ainsi, Gauss fut le premier à ôter le côté mystérieux, presque mystique, des nombres complexes. Il leur conféra aussi les mêmes droits, la même reconnaissance aux yeux du monde mathématique, que ceux dont disposent les nombres réels.
Les nombres complexes furent ensuite étudiés par le mathématicien français *Augustin-Louis Cauchy*. Toutefois, il ne s'arrêta pas à leur interprétation géométrique et continua à les étudier plus en profondeur. Aussi, il considéra qu'une équation imaginaire n'est rien d'autre que la représentation de deux équations entre quantités réelles (*"Cours d'Analyse de l'Ecole Royale Polytechnique"*, 1821). Sa conception purement algébrique des nombres complexes est donc à mettre en contraste avec la conception géométrique de Gauss. Il tenta également de transformer les expressions imaginaires, notamment la lettre i elle-même, en quantité réelle en utilisant le concept d'équivalence. Ainsi, il identifia le champ des complexes $\mathbb{C}$ au champ quotient $\mathbb{R}[X]/(X^2+1)$, ce qui lui permit d'interpréter les opérations impliquant des nombres complexes comme des opérations avec des polynômes réels quotientés par le polynôme du second degré X^2+1.
Bien que très utile, l'interprétation géométrique des nombres complexes comme étant des points ou des vecteurs du plan n'est pas totalement satisfaisante. En effet, on ne cherche pas uniquement à voir mais bien à comprendre. C'est en 1835 que *Sir William Rowan Hamilton* établit la définition d'un nombre complexe comme étant une paire ordonnée de nombres réels. Il posa également la définition des opérations d'addition et de multiplication de nombres complexes de telle façon que les lois de distributivité, d'associativité et de commutativité furent conservées. Cette définition constitua un réel tournant dans l'interprétation des nombres complexes et elle est encore bien présente de nos jour.
Après cela, les nombres complexes furent rapidement utilisés en physique, ainsi 1823, *Fresnel* utilisait déjà les nombres complexes dans sa théorie sur la réflexion totale. De nos jours, les nombres complexes sont partout en physique comme par exemple dans les équations de base de la mécanique quantique.
Les nombres complexes, ou encore les nombres impossibles comme ils étaient désignés à l'époque, se sont développés de plus plus, prenant une place importante en science et en ingénierie. Les questions philosophiques sous-jacentes que se posaient les mathématiciens de l'époque n'ont désormais plus lieu d'être, c'est pourquoi les scientifiques d'aujourd'hui utilisent ces nombres sans se poser de questions, avec confiance et conviction.

Finalement, remarquons qu'aux $XVIII^e$ et XIX^e siècles les nombres complexes ont présentés de grandes difficultés du fait qu'on ne puisse pas les ordonner. En effet, la petite proposition ci-dessous traduit cette particularité.

Proposition 1.1.5. *Il est impossible de définir une relation ">0" de telle façon que les conditions*

1) *Pour tout $z \in \mathbb{C}$, une seule des trois relations $z > 0, z = 0$ ou $z < 0$ est valide,*
2) *Si $w > 0$ et si $z > 0$ alors $w + z > 0$ et $wz > 0$,*

soient simultanément vérifiées.

Démonstration. Supposons que nous avons la relation ">0" sur le champ des complexes $\mathbb{C}$. Dès lors, pour tout complexe z non nul, on devrait avoir $z^2 > 0$. Ainsi, $1^2 > 0$ et $i^2 > 0$ et il s'en suit l'absurdité puisque $i^2 + 1^2 = 0$.

□

1.2 La méthode de Ferrari

Dans la section précédente, nous avons présenté la résolution d'équations du troisième degré via la méthode de Cardan. Nous avons également mentionné qu'un élève de Cardan, prénommé Ludovico Ferrari, avait découvert une méthode permettant de déterminer les solutions d'une équation de degré 4. Ainsi, dans cette section, il sera question de développer la méthode découverte par *Ludovico Ferrari*, mathématicien italien du XVI^e siècle.

Considérons une équation type du quatrième degré

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \quad a \neq 0. \tag{1.12}$$

Remarque 1.2.1. Remarquons que si cette équation admet au moins une racine double alors nous résolvons cette équation par le méthode de Cardan que nous connaissons désormais. En effet, si une racine double existe, celle-ci annule le polynôme $P(x) = ax^4 + bx^3 + cx^2 + dx + e$ ainsi que sa dérivée. Dès lors, il nous suffirait de considérer le polynôme dérivé et nous serions amenés à résoudre une équation de troisième degré.

Tout comme c'est le cas pour les équations de degré 3, l'équation 1.12 peut s'écrire sous une forme réduite, cela fait l'objet de la proposition suivante.

Proposition 1.2.2 (Equation quadratique réduite)**.** *Soit $P(x) = ax^4 + bx^3 + cx^2 + dx + e$ un polynôme de degré 4 en l'indéterminée x dont les coefficients a, b, c, d, e sont des nombres complexes (resp. réels). Alors, il existe $y \in \mathbb{C}$ (resp. $y \in \mathbb{R}$) tel que $Q(x) = P(x - y)$ soit sans terme cubique.*

Démonstration. Il suffit de calculer le polynôme $P(x - y)$. On a

$$\begin{aligned}
P(x-y) &= a(x-y)^4 + b(x-y)^3 + c(x-y)^2 + d(x-y) + e \\
&= a(x^4 - 4x^3y + 6x^2y^2 - 4xy^3 + y^4) + b(x^3 - 3x^2y + 3xy^3 - y^3) \\
&\quad + c(x^2 - 2xy + y^2) + d(x-y) + e \\
&= ax^4 - 4ax^3y + 6ax^2y^2 - 4axy^3 + ay^4 + bx^3 - 3bx^2y + 3bxy^2 - by^3 \\
&\quad + cx^2 - 2cxy + cy^2 + dx - dy + e \\
&= ax^4 + (-4ay + b)x^3 + (6ay^2 - 3by + c)x^2 + (-4ay^3 + 3by^2 - 2cy + d)x \\
&\quad + (ay^4 - by^3 + cy^2 - dy + e).
\end{aligned}$$

Par conséquent, considérer $y = \frac{b}{4a}$ convient. □

Remarque 1.2.3. Par ailleurs, sous la condition $y = \frac{b}{4a}$, le polynôme Q de la proposition précédente peut se réécrire sous la forme

$$Q(x) = ax^4 + \left(\frac{-3b^2}{8a} + c\right)x^2 + \left(\frac{b^3}{8a^2} - \frac{cb}{2a} + d\right)x + \left(\frac{-3b^4}{256a^3} + \frac{cb^2}{16a^2} - \frac{db}{4a} + e\right).$$

Ainsi, cette proposition nous indique que l'équation 1.12 peut être ramenée à l'équation sans terme cubique ci-dessous

$$ax^4 + \left(\frac{-3b^2}{8a} + c\right)x^2 + \left(\frac{b^3}{8a^2} - \frac{cb}{2a} + d\right)x + \left(\frac{-3b^4}{256a^3} + \frac{cb^2}{16a^2} - \frac{db}{4a} + e\right) = 0.$$

Or, puisque a est non nul, en divisant chacun des deux membres par a nous obtenons une équation du type

$$x^4 + px^2 + qx + r = 0, \tag{1.13}$$

où

$$\begin{aligned}
p &= \frac{-3b^2}{8a^2} + \frac{c}{a},\\
q &= \frac{b^3}{8a^3} - \frac{cb}{2a^2} + \frac{d}{a},\\
r &= -\frac{3b^4}{256a^4} + \frac{cb^2}{16a^3} - \frac{bd}{4a^2} + \frac{e}{a}.
\end{aligned}$$

Ensuite, afin de pouvoir continuer à présenter la méthode de résolution des équations du quatrième degré en toute généralité, nous constatons qu'il est bon de supposer que le coefficient de x est non nul, sans quoi nous nous ramènerions à une équation bicarrée et il suffirait de poser $z = x^2$. Ce cas particulier n'est donc pas intéressant pour l'élaboration de cette section.

La méthode de Ferrari consiste à comparer le polynôme $P'(x) = x^4 + px^2 + qx + r$ avec le polynôme $Q'(x)$ défini par $Q'(x) = x^2 + \lambda$ où λ est un nombre réel. Tentons donc d'exprimer $P'(x)$ en fonction de $Q'(x)$. On calcule et on constate que l'on a

$$P'(x) = (x^2 + \lambda)^2 + x^2(p - 2\lambda) + qx + r - \lambda^2.$$

Donc,

$$P'(x) = Q'(x)^2 - R(x)$$

où R est le polynôme du second degré en x défini par $R(x) = -x^2(p - 2\lambda) - qx - r + \lambda^2$. L'astuce de Ludovico Ferrari est alors de vouloir écrire $R(x)$ comme le carré d'un polynôme du premier degré en x. En d'autres mots, il cherche un polynôme S de premier degré en x tel que $R(x) = S(x)^2$. Pour qu'un tel polynôme existe, il faut et il suffit que R ait une racine double, autrement dit, que son discriminant soit nul. Si nous désignons par Δ le discriminant, $\Delta = 0$ si et seulement si

$$8\lambda^3 - 4p\lambda^2 - 8r\lambda + 4rp - q^2 = 0. \tag{1.14}$$

Dès lors, son but est alors de résoudre cette équation en λ par la méthode de Cardan. De nos jours, on sait, par le Théorème de d'Alembert-Gauss, qu'une telle équation possède exactement 3 racines complexes comptées avec leur multiplicité et qu'au moins l'une d'entre elles est réelle. Or, à l'époque, Ferrari travaillait sur $\mathbb{R}$, il se devait donc de considérer une solution réelle. D'ailleurs, il n'avait pas connaissance des autres solutions. Il devait donc considérer la solution qui était donnée par la méthode de Cardan, pour autant qu'elle présente une forme qui lui était connue. Supposons que ce soit le cas, et que λ_1 soit solution réelle telle que $2\lambda_1 - p \geq 0$. Dès lors, le polynôme P' s'écrit sous la forme

$$\begin{aligned}
P'(x) &= (x^2 + \lambda_1)^2 - (-x^2(p - 2\lambda_1) - qx + r - \lambda_1^2)\\
&= (x^2 + \lambda_1)^2 - (2\lambda_1 - p)\left(x - \frac{q}{2(2\lambda_1 - p)}\right)^2\\
&= (x^2 + \lambda_1)^2 - \left(\sqrt{2\lambda_1 - p}\left(x - \frac{q}{2(2\lambda_1 - p)}\right)\right)^2
\end{aligned}$$

L'importance d'avoir $2\lambda_1 - p \geq 0$ apparaît donc clairement. Il faut aussi se rendre compte que lorsque cette condition n'était pas satisfaite, les mathématiciens contemporains à Ferrari ne savaient tout simplement pas continuer les développements. Sur le champ des complexes en revanche ce résultat est toujours applicable.
Nous nous retrouvons donc avec un polynôme P' du quatrième degré pouvant s'écrire comme

la différence de deux polynômes mis au carré. Le polynôme S souhaité tel que $R(x) = S(x)^2$ s'écrit sous la forme $S(x) = \sqrt{2\lambda_1 - p}\,(x - \frac{q}{2\sqrt{2\lambda_1 - p}})$. Par conséquent il vient,

$$\begin{aligned}
P'(x) &= Q'(x)^2 - S(x)^2 \\
&= (Q'(x) + S(x))(Q'(x) - S(x)) \\
&= \left(x^2 + \lambda_1 + x\sqrt{2\lambda_1 - p} - \frac{q}{2\sqrt{2\lambda_1 - p}}\right)\left(x^2 + \lambda_1 - x\sqrt{2\lambda_1 - p} + \frac{q}{2\sqrt{2\lambda_1 - p}}\right)
\end{aligned}$$

Ainsi, $P'(x) = 0$ si et seulement si

$$x^2 + \lambda_1 + x\sqrt{2\lambda_1 - p} - \frac{q}{2\sqrt{2\lambda_1 - p}} = 0 \quad \text{ou} \quad x^2 + \lambda_1 - x\sqrt{2\lambda_1 - p} + \frac{q}{2\sqrt{2\lambda_1 - p}} = 0$$

Il reste alors à déterminer les solutions de ces deux équations quadratiques pour obtenir les quatre solutions de notre équation initiale.

En conclusion, la méthode de Ferrari permet de remplacer le calcul des racines d'un polynôme du quatrième degré par le calcul des racines d'un polynôme du troisième degré et celui des racines de deux polynômes de degré 2.

Nous venons de (re)découvrir l'introduction et l'évolution des nombres complexes au travers des siècles. Nous allons désormais nous intéresser aux différentes façons de les introduire de nos jours.

1.3 Analyse de l'introduction des nombres complexes dans le secondaire

Dans la présente section de ce travail nous nous intéresserons à la place occupée par l'enseignement des nombres complexes dans l'enseignement secondaire général et de transition et il sera également question d'apporter un éclairage didactique quant aux différentes méthodes mises en application par les enseignants pour l'introduction des nombres complexes.

Force est de constater que dans le référentiel définissant les compétences terminales et les savoirs requis à l'issue de la filière "générale" ou de transition, disponible à la référence [6], les nombres complexes ne figurent au programme que pour les élèves de sixième année mathématiques ayant choisi l'orientation scientifique [4]. Remarquons également que les nombres complexes sont le dernier point de matière abordé dans ce référentiel. Toutefois, il est bon de constater que les nombres complexes figurent aussi au programme de certaines sections de l'enseignement qualifiant, comme la section électronique par exemple.
Le référentiel précise également que la seule compétence obligatoire à développer consiste "simplement" à utiliser les nombres complexes pour démontrer ou obtenir des résultats. Les différentes applications des nombres complexes demandées consistent essentiellement à la résolution d'équations, la recherche de racines n-ièmes et leur représentation dans le plan de Gauss ainsi que la conversion écriture trigonométrique - écriture algébrique d'un nombre complexe.

Qu'en est-il de leur exploitation dans d'autres domaines scientifiques tels qu'en électricité ou encore pour l'étude des phénomènes périodiques comme les ondes ? A priori, rien n'interdit

4. Les unités d'acquis d'apprentissage sont identiques à tous les élèves du second degré. Pour celles du troisième degré, trois orientations sont possibles : mathématiques de base (équivalent à 2h/semaine), mathématiques générales (équivalent à 4h/semaine) et mathématiques pour scientifiques (équivalent à 6h et plus par semaine).

aux enseignants de s'engager dans une telle démarche didactique puisque le référentiel indique simplement les compétences sur lesquelles les élèves doivent être évalués.

Dans la section suivante, nous allons faire une analyse d'une première vision de l'introduction des nombres complexes. Cette dernière est explicitée dans le syllabus pour le cours de mathématiques élémentaires de premier bachelier mathématiques à l'Université de Liège que nous retrouvons à la référence [18]. Elle est également présentée dans divers manuels scolaires mais la version présentée ici en comble les lacunes.

1.3.1 Introduction des nombres complexes comme couple de nombres réels

Dans le syllabus *Mathématiques élémentaires*, on part du constat que toutes les équations du second degré n'admettent pas nécessairement des solutions dans $\mathbb{R}$. On indique qu'il est parfois utile de disposer de solutions à toutes ces équations, sans pour autant mentionner les questions historiques qui ont amené à l'introduction des nombres complexes.
Après avoir rappelé la méthode de résolution des équations du second degré dans $\mathbb{R}$ et la condition d'existence de solutions, on se propose d'étendre la méthode. On part alors de l'équation

$$x^2 + 2x + 5 = 0 \tag{1.15}$$

contrairement à une habitude répandue de considérer l'équation $x^2 + 1 = 0$.
On constate que le discriminant Δ de l'équation 1.15 est $\Delta = -16$, et que si on avait un nombre supplémentaire i dont le carré vaut -1, on pourrait extraire une racine carrée de -16, à savoir $4i$ et ainsi la méthode se prolongerait. L'équation considérée 1.15 admettrait alors les solutions $x_1 = -1 + 2i$ et $x_2 = -1 - 2i$. L'auteur analyse ensuite certaines conditions qui ont permis de résoudre les équations du second degré dans $\mathbb{R}$, et indique ce que l'on devrait avoir comme propriétés pour ces nouveaux nombres de la forme de $-1 + 2i$. Par exemple, l'addition doit permettre à tout élément d'admettre un opposé, le produit doit être commutatif, associatif, distributif sur l'opération "+", ... toutes les conditions nécessaires sont reprises et expliquées à la page 30 du syllabus. En bref, connaissant les opérations indispensables à la résolution d'équations sur l'ensemble des réels, nous souhaiterions que ces propriétés restent valides pour les nombres de la forme $a + ib$ où les paramètres a et b sont réels. C'est sur base de ce souhait que se fonde l'approche proposée ici. Dans ce cas, l'addition et la multiplication serait alors définies respectivement comme suit :

$$(a + ib) + (a' + ib') = (a + a') + i(b + b'), \tag{1.16}$$

et

$$(a + ib)(a' + ib') = aa' + bb'i^2 + (ab' + a'b)i = (aa' - bb') + i(ab' + a'b). \tag{1.17}$$

Il serait alors assez naturel de vouloir définir l'ensemble des nombres complexes comme l'ensemble

$$\mathbb{C} = \{a + ib : a, b \in \mathbb{R}\} \tag{1.18}$$

Toutefois, cette définition pose quelques difficultés en ce sens que l'on ignore si un tel nombre i existe. D'ailleurs, s'agit-il réellement d'un nombre ? Aussi cette définition utilise des opérations qui ne sont pas définies. Ainsi, puisque nous ne connaissons réellement que a et b dans l'expression $a + ib$, il convient plutôt d'écrire le nombre complexe $a + ib$ sous la forme d'un couple de réels (a, b) et de définir les opérations somme et produit sur les couples en se souvenant que l'on souhaite arriver aux opérations définies plus haut. Il s'agit donc d'un subterfuge de calcul que nous utilisons pour définir proprement les opérations de base et une fois cela fait, nous pourrons transposer ces résultats selon la définition d'un nombre complexe 1.18.

Définition 1.3.1. L'ensemble des nombres complexes est défini par

$$\mathbb{C} = \{(a, b) : a, b \in \mathbb{R}\}$$

Remarquons que cette vision algébrique des nombres complexes qui consiste à les définir sous forme d'un couple de nombres réels est due en grande partie à Hamilton.
Ainsi, en tant qu'ensemble, $\mathbb{C}$ est identifié à $\mathbb{R}^2$, qui peut être représenté dans le plan, comme on le fait d'habitude en géométrie. Etant donné que l'on souhaite aboutir aux formules 1.16 et 1.17 , et que l'on garde en tête que le couple (a, b) définira à terme $a + ib$, il est alors naturel de définir les opérations comme suit.

Définition 1.3.2. Pour tous a, b, c, d réels, l'addition de nombres complexes est définie par

$$+ : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} : ((a, b), (a', b')) \mapsto (a + a', b + b')$$

Définition 1.3.3. Pour tous réels a, b, c, d, la multiplication de nombres complexes est définie par

$$. : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{C} : ((a, b), (a', b')) \mapsto (aa' - bb', ab' + a'b)$$

Dans la suite, nous ne noterons plus le symbole $\cdot$ de la multiplication, celui-ci sera sous-entendu. A cela, on montre que l'addition et la multiplication sur $\mathbb{C}$ possèdent les mêmes propriétés que sur $\mathbb{R}$.

Puisque le champ des complexes $\mathbb{C}$ est une extension du champ des réels $\mathbb{R}$ il paraît alors naturel d'identifier un réel comme un couple particulier de nombres réels. Tout naturellement on définira un nombre réel x par le couple $(x, 0)$.

Définition 1.3.4. Le plongement de $\mathbb{R}$ dans $\mathbb{C}$ est défini par

$$\phi : \mathbb{R} \longrightarrow \mathbb{C} : x \mapsto (x, 0).$$

Aussi, puisqu'en tant qu'ensemble les complexes sont identifiés au plan $\mathbb{R}^2$, la multiplication d'un nombre complexe par un nombre réel correspond à la multiplication habituelle d'un élément de $\mathbb{R}^2$ par un nombre réel. De fait, cette identification nous permet d'écrire des expressions de la forme az, où a est réel et z est complexe. En effet, supposons que $z = (x, y)$, on a

$$az = (a, 0)(x, y) = (ax - 0y, ay + 0x) = (ax, ay)$$

Rappelons que notre but était de pouvoir définir proprement le nombre $a + ib$. Pour cela, nous nous sommes ramenés aux couples de nombres réels (a, b) et nous avons établi les premières définitions et propositions s'y attenant. En particulier, nous venons de considérer que le couple de réels $(x, 0)$ pouvait être identifié au nombre réel x, ainsi, le couple $(1, 0)$ est identifié au réel 1, le neutre pour la multiplication sur $\mathbb{R}$. L'étape importante maintenant est de pouvoir revenir à l'écriture $a + ib$ d'un nombre complexe en partant de l'écriture (a, b) de ce même nombre. On a

$$(a, b) = a(1, 0) + (0, 1)b = a1 + (0, 1)b = a + (0, 1)b.$$

Un choix naturel s'offre alors directement à nous concernant l'écriture du symbole i.

Définition 1.3.5. Nous désignons par i le nombre complexe $(0, 1)$ et nous l'appelons *unité imaginaire.*

Cela étant, nous arrivons au but souhaité. En effet, une définition vient d'être posée pour le symbole i et, l'addition et la multiplication de deux nombres complexes ont également été définies proprement. La proposition suivante suit directement.

Proposition 1.3.6. *Tout nombre complexe z s'écrit de manière unique sous la forme $x + iy$ avec $x, y \in \mathbb{R}$. De plus, $i^2 = -1$.*

Démonstration. Par définition, tout nombre complexe z s'écrit de façon unique $z = (x, y)$ pour x et y deux nombres réels. De plus, on a

$$(x, y) = (x + 0, 0 + y) = (x, 0) + (0, y) = x(1, 0) + (y, 0)(0, 1) = x1 + y(0, 1) = x + yi = x + iy,$$

où nous avons utilisé la multiplication dans $\mathbb{C}$ et l'identification (1.3.4).
Pour l'unicité, supposons que z s'écrive sous la forme $x + iy$ et $x' + iy'$, autrement dit $z = x + iy = x' + iy'$. Dès lors, vu ce qu'il vient d'être fait, $(x, y) = (x', y')$ et donc $x = x'$ et $y = y'$ ce qui justifie l'unicité d'écriture.
Finalement,

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1.$$

□

Analyse didactique

Analysons maintenant cette approche d'un point de vue didactique. Cette vision des nombres complexes par les couples de nombres réels comme détaillé ci-dessus possède plusieurs atouts. En effet, faire l'introduction de cette façon permet de rendre légitime les définitions d'addition et de multiplication. Evidemment, la somme et le produit de deux nombres complexes présentent la forme explicitée plus haut car ces opérations doivent répondre à plusieurs contraintes. Comme nous souhaitons que ces opérations possèdent les mêmes propriétés que celles correspondantes dans le cas réel, nous n'avons d'autre choix que d'adopter les définitions 1.3.2 et 1.3.3. La subtilité dédiée à l'introduction des nombres complexes réside dans le fait qu'ils ne sont pas introduits arbitrairement par le professeur. Au contraire, ils sont introduit délibérément *a priori* et justifié *a postériori*[5]

En revanche, pour pallier la notation $a + ib$, on s'est proposé de définir un nombre complexe sous la forme d'un couple de nombres réels. Là, figure un obstacle d'apprentissage lié à la conception des élèves qu'un nombre ne peut être un couple de deux nombres. Pourtant, lorsqu'ils ont vu les fractions à l'école primaire il n'ont pas manifesté d'incompréhension à la vue d'un nombre s'écrivant à l'aide de deux nombres. Par exemple, $\frac{2}{3}$ est constitué des nombres 2 et 3. Dès lors, pourquoi en serait-il autrement pour les complexes ? Aussi, bien que l'égalité $i^2 = -1$ soit justifiée, cette justification n'est que mesurée puisqu'il est important et même nécessaire que les élèves comprennent qu'il s'agit là de prendre le carré d'un nombre soumis à une nouvelle définition, puisque c'est un couple de nombres, et soumis à une nouvelle définition pour la multiplication. Ainsi, les règles ayant été modifiées, pourquoi le carré d'un nombre (complexe) ne pourrait-il pas être négatif ?

Ensuite, une question demeure toujours. Pourquoi s'obstiner à déterminer des solutions là où il n'y en a visiblement pas ? Effectivement, alors qu'une équation du second degré ne possède pas nécessairement de racine réelle, ce n'est pas le cas d'une équation cubique qui en possède toujours au moins une. Ainsi, le choix de l'équation qui introduit la section est important. En effet, c'est grâce à des équations de degré 3 que le recours à des quantités imaginaires apparaîtra et c'est donc de telles équations qui créeront un déséquilibre cognitif. L'introduction des nombres complexes provoquera alors une rééquilibration. Une approche essentiellement déductive présente donc l'inconvénient de masquer la motivation de l'introduction de nouveau(x) concept(s) et par conséquent empêche la compréhension profonde du sujet. Pour pallier cela, il serait donc intéressant de commencer par une note historique reprenant les faits principaux que j'ai explicité dans l'introduction historique de ce mémoire. En conséquence, les motivations qui

5. Des informations complémentaires sont disponibles à la référence [11].

ont permis d'introduire ces concepts sont claires pour les élèves et ils peuvent s'en servir pour approfondir et/ou améliorer leur compréhension et pour faire l'étude de résultats plus avancés ne faisant pas forcément partie de la matière théorique. [6].

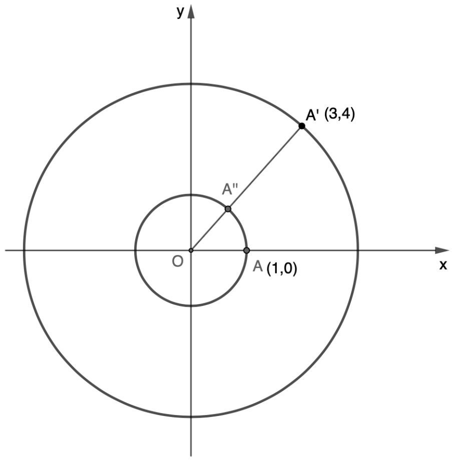
Finalement, il reste un obstacle empirique, autrement dit un obstacle qui se base sur l'expérience et sur l'observation, à cette approche. On a toujours associé les nombres à des "grandeurs", des objets que l'on peut presque toucher. Ce n'est pas le cas des nombres complexes dans cette introduction. Effectivement, même si ce sont des couples de nombres, on peut toujours se demander ce qu'ils représentent comme "grandeur".

1.3.2 Introduction des nombres complexes par les similitudes

Tout comme l'approche par les couples, l'approche par les similitudes est une approche qui pourrait être développée en secondaire car elle ne présente pas de trop grande(s) difficulté(s) et qu'elle justifie bien la définition prise pour le produit de nombres complexes en mettant l'accent sur la composition de similitudes. Maggy Schneider et Hilda Rosseel en font la présentation et analysent les points forts et les points faibles de cette approche dans leur ouvrage intitulé *Ces nombres que l'ont dit imaginaires sont-ils vraiment des nombres ?* disponible à la référence [21]. Je vous propose d'en développer les grandes étapes et d'y apporter un regard didactique.

L'approche par les similitudes commence par la notion de rotation. Dans leur livre, M. Schneider et H. Rosseel considèrent en premier lieu le cas où l'image du point $(1,0)$ est un point situé sur le cercle trigonométrique. Ainsi, en considérant un système d'axes orthonormés, l'image du point de coordonnées $(1,0)$ par une rotation de centre $O(0,0)$ et d'angle α est le point de coordonnées $(\cos\alpha, \sin\alpha)$. Evidemment, le raisonnement inverse est possible également. De fait, une rotation de centre O est déterminée une fois que l'on connait le point du cercle trigonométrique sur lequel elle envoie le point $(1,0)$.
Dans un second temps, elles traitent le cas où l'image du point $(1,0)$ n'est plus située sur le cercle trigonométrique. C'est alors qu'il devient indispensable de composer rotations et homothéties. Pour illustrer leur propos, les deux autrices développent l'exemple suivant.

Exemple 1.3.7. Il n'existe pas de rotation de centre O qui envoie le point $A(1,0)$ sur le point $A'(3,4)$ puisque ces deux points se trouvent sur des cercles de centre $O(0,0)$ et de rayons différents. Cependant, la droite OA' coupe le cercle trigonométrique en un point A''. Ainsi, pour trouver les coordonnées du point A' à partir de celles de A, il faut commencer par considérer une rotation qui envoie A sur A'' et puis une homothétie qui envoie A'' sur A'. La situation est représentée ci-dessous.



6. Ces informations se retrouvent aux références [12] et [7]

Alors, en suivant les étape de construction, on peut commencer par déterminer les coordonnées du point A''. La droite OA' a pour équation $y = \frac{4}{3}x$. Les coordonnées du point d'intersection situé dans le premier quadrant entre le cercle trigonométrique et la droite OA' peuvent être obtenues en résolvant le système d'équations suivant :

$$\left\{\begin{array}{c} y = \frac{4}{3}x \\ x^2 + y^2 = 1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{c} y = \frac{4}{3}x \\ x^2 + \frac{16}{9}x^2 = 1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{c} y = \frac{4}{3}x \\ x^2 = \frac{9}{25} \end{array}\right. \Leftrightarrow \left\{\begin{array}{c} y = \frac{4}{5} \\ x = \frac{3}{5} \end{array}\right.$$

Les coordonnées du point A'' sont donc $(\frac{3}{5}, \frac{4}{5})$. Ensuite, en appliquant une homothétie de centre O et de rapport 5 au point A'' nous obtenons le point A'. En conclusion, on passe du point A au point A' en composant une rotation et une homothétie, c'est-à-dire en appliquant une similitude.

Définition 1.3.8. On appelle similitude directe de centre $(0, 0)$, d'angle θ et de rapport $\rho > 0$ la composée, dans un ordre quelconque, d'une rotation de centre $(0, 0)$ et d'angle θ et d'une homothétie de centre $(0, 0)$ et de rapport ρ.

Une remarque importante que font M. Schneider et H. Rosseel dans leur ouvrage est qu'il faut exclure le cas où le point P, image du point $(1, 0)$, serait l'origine du repère. En effet, si c'était le cas, l'angle de rotation ne serait pas unique puisque le point P pourrait être obtenu en composant une rotation d'angle quelconque avec une homothétie de rapport nul. Dès lors, afin d'éviter cette ambiguïté, elles proposent de ne considérer que le cas où $(a, b) \neq (0, 0)$.

Finalement, elles clôturent le premier chapitre en faisant remarquer aux lecteurs/lectrices que tout point du plan, différent de l'origine du repère, admet deux écritures équivalentes. Une écriture en termes de coordonnées cartésiennes $P(a, b)$ et une seconde écriture sous forme trigonométrique $P(\rho\cos(\theta), \rho\sin(\theta))$ où ρ et θ sont appelées coordonnées polaires du point P.

À ce stade nous pourrions nous interroger sur le lien entre les similitudes et les nombres complexes. Il faut introduire les similitudes quelconques, autrement dit les similitudes qui partent d'un point quelconque du plan, pour que ce lien apparaisse. Comme nous le verrons, c'est à partir de la forme cartésienne de la composition de deux similitudes que nous allons obtenir la forme du produit complexe.

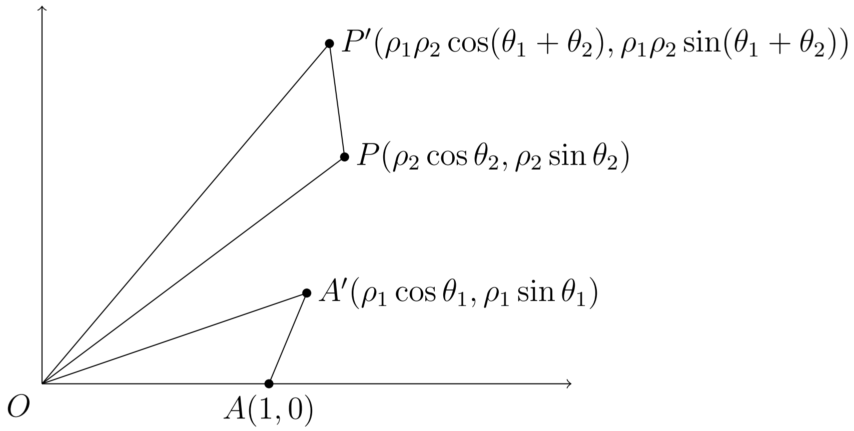
Pour étayer leur propos les deux autrices de ce livre proposent une nouvelle fois de partir d'un exemple théorique. Pour ce faire, elles considèrent la similitude s de centre O qui envoie le point $A(1, 0)$ sur un point quelconque du plan $A'(a_1, b_1)$, ainsi qu'un autre point quelconque $P(a_2, b_2)$. En passant par les écritures trigonométriques des points A' et P, à savoir

$$A'(a_1, b_1) = (\rho_1 \cos\theta_1, \rho_1 \sin\theta_1),$$
$$P(a_2, b_2) = (\rho_2 \cos\theta_2, \rho_2 \sin\theta_2),$$

on peut facilement voir que l'image P' de P par la similitude s a pour coordonnées

$$P'(\rho_1\rho_2 \cos(\theta_1 + \theta_2), \rho_1\rho_2 \sin(\theta_1 + \theta_2)).$$

Pour le voir, illustrons la situation :



Les triangles OAA' et OPP' étant semblables, on en conclut qu'appliquer la similitude s à P consiste à additionner θ_1 et θ_2 et à multiplier ρ_1 par ρ_2.
Par conséquent, elles concluent cette section de leur ouvrage en faisant remarquer que pour déterminer l'image d'un point P quelconque du plan par une similitude s directe de centre $O(0,0)$, il est suffisant de connaitre l'image A' du point $A(1,0)$ par cette similitude.

Dans la section suivante, M. Schneider et H. Rosseel s'attèlent à étudier, en termes de coordonnées cartésiennes, la composée de deux similitudes de centre O qu'elles appellent s_1 et s_2 où s_1 envoie le point $(1,0)$ sur le point (a_1,b_1) et s_2 envoie le point (a_1,b_1) sur le point (a_2,b_2). Vu ce qui a été fait précédemment, on sait qu'une première similitude s_1 de centre $O(0,0)$ peut être codée par les coordonnées $(a_1,b_1) = (\rho_1\cos\theta_1, \rho_1\sin\theta_1)$, et la seconde par le couple $(a_2,b_2) = (\rho_2\cos\theta_2, \rho_2\sin\theta_2)$. Ainsi, par s_1, $A(1,0)$ est envoyé sur le point $A'(\rho_1\cos\theta_1, \rho_1\sin\theta_1)$ et ce point A' est à son tour envoyé sur le point $A''(\rho_1\rho_2\cos(\theta_1+\theta_2), \rho_1\rho_2\sin(\theta_1+\theta_2))$ par s_2. Dès lors, la similitude $s_3 = s_2\circ s_1$ est codée par le couple $(\rho_1\rho_2\cos(\theta_1+\theta_2), \rho_1\rho_2\sin(\theta_1+\theta_2))$. Le but de cette section étant d'interpréter la composée de deux similitudes de centre $O(0,0)$ en termes de coordonnées cartésiennes, il vient

$$\begin{aligned}
&(\rho_1\rho_2\cos(\theta_1+\theta_2), \rho_1\rho_2\sin(\theta_1+\theta_2))\\
&\quad= (\rho_1\rho_2(\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2), \rho_1\rho_2(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2))\\
&\quad= (\rho_1\cos\theta_1\rho_2\cos\theta_2 - \rho_1\sin\theta_1\rho_2\sin\theta_2, \rho_1\sin\theta_1\rho_2\cos\theta_2 + \rho_1\cos\theta_1\rho_2\sin\theta_2)\\
&\quad= (a_1a_2 - b_1b_2, b_1a_2 + a_1b_2).
\end{aligned}$$

Dès lors, elles établissent que composer deux similitudes s_1 et s_2 centrées en l'origine du repère consiste à définir une nouvelle opération sur les couples qui les représentent. Avec les notations utilisées précédemment, elles définissent

$$s_2\circ s_1 \to (a_1,b_1)\times(a_2,b_2) = (a_1a_2 - b_1b_2, b_1a_2 + a_1b_2).$$

Fait remarquable, l'opération $\times$ se comporte d'une manière particulière lorsqu'on considère des couples de la forme $(a,0)$ avec a un nombre réel. En effet, le résultat du calcul $(a,0)\times(b,0)$ est le couple $(ab,0)$, autrement dit, il s'agit d'un couple dont la première composante est le produit des premières composantes des couples considérés et la deuxième composante est nulle. Ces couples un peu particulier font l'objet de cette quatrième et dernière section du chapitre 2 de l'ouvrage considéré ici.

Tout d'abord, il est bon de constater que les couples de nombres réels (a,b), désignant le point P dans le repère, ont la particularité de représenter les composantes du vecteur $\overrightarrow{OP}$. Ainsi, les couples de la forme $(a,0)$ désignent en réalité les points de l'axe des abscisses. Et comme on le sait, ces derniers sont identifiés par leur seule abscisse a, autrement dit par le nombre réel

a. Aussi, le calcul vectoriel a une importance capitale dans cette approche des nombres complexes puisqu'il nous apprend que pour additionner des vecteurs, il suffit d'additionner leurs composantes respectives. À partir des vecteurs $\overrightarrow{OP}(a,b)$ et $\overrightarrow{OP'}(a',b')$, on obtient

$$\overrightarrow{OP}+\overrightarrow{OP'}=\overrightarrow{OP''}(a'',b'') \text{ où } a''=a+a' \text{ et } b''=b+b',$$

ce qui nous permet d'obtenir la règle d'addition des couples :

$$(a,b)+(a',b')=(a+a',b+b').$$

Lorsqu'on s'intéresse a l'addition de deux couples de la forme $(a,0)$ on retrouve l'addition des nombres réels :

$$(a,0)+(a',0)=(a+a',0).$$

Une autre opération a été définie juste avant, à savoir l'opération "$\times$" :

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

opération que l'on appellera bien multiplication de couples. Regardons ce qu'il advient si on s'intéresse à la multiplication de couples de la forme $(a,0)$:

$$(a,0)\times(a',0)=(aa',0),$$

on retrouve bien la multiplication des réels.
À partir de cette opération, on peut définir les puissances n^{iemes}. En particulier, on peut définir le carré d'un couple :

$$(a,b)^2=(a,b)\times(a,b)=(a^2-b^2,ab+ba)=(a^2-b^2,2ab).$$

On vient de voir que les couples de nombres pouvaient s'additionner et se multiplier, tout comme les nombres normaux. Cependant, pour ne pas les confondre avec les nombres "normaux", les mathématiciens ont baptisés les couples (a,b) de nombres complexes. Parmi ces couples, ceux de la forme $(a,0)$ sont assimilés aux nombres réels a puisqu'ils se comportent comme des nombres réels lorsqu'on les additionne ou les multiplie.
Nous retombons alors sur le même schéma que celui suivit pour introduire les nombres complexes par les couples de nombres réels. Toutefois, dans cette nouvelle approche, des justifications complémentaires peuvent être apportés grâce à l'aspect visuel à accorder aux vecteurs.

Finalement, M. Schneider et H. Rosseel repartent une nouvelle fois du calcul vectoriel pour comprendre comment, à partir de deux couples de nombres, il est possible d'obtenir tous les autres. Si le couple (a,b) représente le vecteur $\overrightarrow{OP}$, le couple (ra,rb) représente le vecteur $r\overrightarrow{OP}$. Il parait donc tout à fait raisonnable de définir la multiplication d'un couple par un réel comme suit,

$$r(a,b)=(ra,rb).$$

Ainsi, si on suppose avoir en notre possession cette opération ainsi que l'opération d'addition des couples, on peut écrire tout couple (a,b) sous la forme

$$(a,b)=(a,0)+(0,b)=a(1,0)+b(0,1).$$

On se rend compte a cette étape que les couples $(1,0)$ et $(0,1)$ jouent un rôle particulier puisqu'en les combinant, on peut retrouver tous les autres couples.

Comme on l'a vu, le couple $(1,0)$ est assimilé au réel 1. En revanche, nous n'avons pas encore d'identification à proposer pour le couple $(0,1)$. Ce qui est constaté, c'est qu'il possède une propriété particulière. En effet, lorsqu'il est multiplié par lui-même, où la multiplication sous-entend l'opération $\times$ définie plus haut, on obtient

$$(0,1)^2 = (0,1) \times (0,1) = (-1,0).$$

Ainsi, si on définit une notation i pour le couple $(0,1)$, le calcul précédent devient donc

$$i^2 = i \times i = -1.$$

Cette écriture aurait pu choquer les élèves, mais d'après le travail que nous venons de réaliser, elle devient totalement légitime. Effectivement, comme pour l'approche par les couples de nombres, il est nécessaire de comprendre que cette égalité s'exprime en fait en termes de couples et qu'il faut donc la décoder. Il ne faut pas perdre de vue que i désigne le couple $(0,1)$, que 1 représente le couple $(1,0)$ et que le carré renvoie à la composition d'une similitude avec elle-même.
Grâce à cette nouvelle notation, nous pourrons écrire tous les nombres complexes (a,b) sous la forme bien connue $a+ib$. En effet, on a

$$(a,b) = (a,0) + (0,b) = a(1,0) + b(0,1) = a1 + bi = a + bi.$$

Cette nouvelle notation des couples permet de retrouver la multiplication des couples par une forme de distributivité

$$\begin{aligned}(a+bi)(a'+b'i) &= aa' + ab'i + ba'i + bb'i^2\\ &= aa' + i(ab'+ba') - bb'\\ &= aa' - bb' + i(ab'+ba').\end{aligned}$$

Analyse didactique

L'avantage non négligeable de cette approche est qu'elle s'inscrit d'abord dans un cadre géométrique et seulement après dans un cadre algébrique. Cela permet de donner davantage de sens à une matière qui reste abstraite pour bon nombre d'élèves. Aussi, la formule de multiplication de deux nombres complexes apparaît clairement.
En revanche, dans cette optique on mélange les notions de vecteur, point et ensuite nombre pour désigner le même objet. Il est donc important que l'exposé soit clair pour les élèves afin que ces derniers ne confondent pas toutes les notions utilisées. Cela engendre un saut conceptuel relativement important à faire de la part des élèves.
Un second désavantage de cette introduction des nombres complexes réside en la restriction que les deux autrices se sont imposée. En effet, rappelons que pour éviter toute ambiguïté, le point $(0,0)$, image par une similitude du point $(1,0)$, n'avait pas été pris en compte dans cette démarche. Le nombre complexe 0 ne serait donc pas défini par cette approche. Dès lors, sans le point $(0,0)$, l'opération $\times$ introduite ici pourrait être vue comme la seule opération et dans ce cas $(\mathbb{R}^2, \times)$ serait un groupe commutatif et non un champ. Détaillons ces propos. La seule différence entre la multiplication et l'addition réside en l'existence d'un unique opposé, communément appelé inverse, pour tout élément non nul, et c'est cette restriction qui fait la différence. Dès lors, si l'origine $(0,0)$ n'est plus prise en compte, rien ne peut distinguer la multiplication de l'addition, donc la multiplication peut très bien être, en réalité une addition. Par conséquent, il est essentiel de prendre en compte l'origine du repère et poser une contrainte dans le cas où l'image du point $(1,0)$ serait le point $(0,0)$ en vue de contrer l'ambiguïté.

1.3.3 Introduction des nombres complexes par les matrices 2×2

La dernière approche des nombres complexes que je souhaite présenter est l'approche par les matrices. Cette dernière est très intéressante du fait qu'elle justifie parfaitement la définition de la multiplication et de l'addition ainsi que l'expression souvent incomprise des élèves $i^2 = -1$. En vue d'étayer mes propos, les résultats qui suivent sont tirés de l'article de H. Rosseel et M. Schneider intitulé *Les nombres complexes comme modèles algébriques de similitudes directes : avec ou sans matrices ?*. Cet article est consultable à la référence [22].

Pour introduire les nombres complexes par les matrices de dimension 2×2 nous avons besoin de connaitre la théorie des transformations linéaires. Rappelons la définition suivante.

Définition 1.3.9. Soient V et W deux espaces vectoriels réels. Une application $t : V \longrightarrow W$ est une transformation linéaire si

1. Pour tous $x, y \in V$, $t(x+y) = t(x) + t(y)$;
2. Pour tous $x \in V$ et $r \in \mathbb{R}$, $t(rx) = rt(x)$.

Dans le cas présent, plaçons-nous dans un plan à deux dimensions muni de la base orthonormée usuelle $(\vec{e_1}, \vec{e_2})$. Soit la transformation

$$t : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

telle que

$$t(\vec{e_1}) = a\vec{e_1} + b\vec{e_2} \quad \text{et} \quad t(\vec{e_2}) = c\vec{e_1} + d\vec{e_2}$$

pour des coefficients a, b, c, d réels.
L'image $\vec{x'} = x_1'\vec{e_1} + x_2'\vec{e_2}$ du vecteur $\vec{x} = x_1\vec{e_1} + x_2\vec{e_2}$ par la transformation linéaire t est décrite ci-dessous

$$\begin{aligned}
\vec{x'} &= t(\vec{x}) \\
&= t(x_1\vec{e_1} + x_2\vec{e_2}) \\
&= x_1 t(\vec{e_1}) + x_2 t(\vec{e_2}) \\
&= (x_1 a + x_2 c)\vec{e_1} + (x_1 b + x_2 d)\vec{e_2},
\end{aligned}$$

où la troisième égalité vient du fait que la transformation t est linéaire. Ceci peut également s'écrire sous la forme matricielle ci-dessous

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = t\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 a + x_2 c \\ x_1 b + x_2 d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

où l'opération de multiplication représente le produit matriciel classique. De plus, la matrice

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

est la matrice codant la transformation linéaire t.
Dans leur livre, Rosseel et Schneider se proposent ensuite de particulariser cette représentation matricielle de la transformation t aux rotations et aux homothéties de centre $O(0,0)$. De fait, toutes deux sont des transformations linéaires du plan.

Commençons par rappeler la proposition ci-dessous.

Proposition 1.3.10. *La matrice codant une rotation de centre* $(0,0)$ *et d'angle* $\theta \in [0, 2\pi[$ *peut être représentée sous la forme*

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

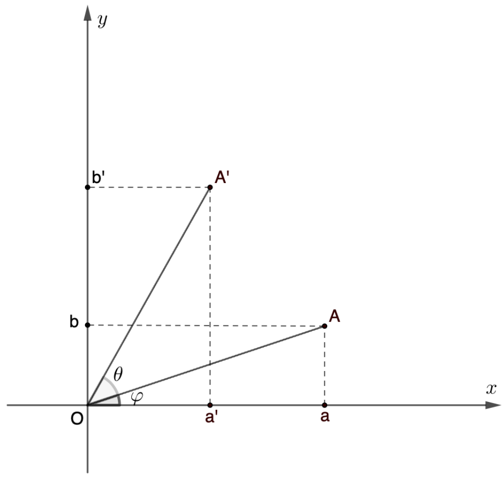
La matrice représentant une homothétie de centre $(0,0)$ *et de rapport* $\rho > 0$ *est de la forme*

$$\begin{pmatrix} \rho & 0 \\ 0 & \rho \end{pmatrix}$$

Démonstration. En ce qui concerne les homothéties, si t est une homothétie de centre $(0,0)$ et de rapport ρ, alors par définition le point du plan (x_1, x_2) sera envoyé sur le point $(\rho x_1, \rho x_2) = (x_1', x_2')$, donc

$$x_1'\vec{e_1} + x_2'\vec{e_2} = t(x_1\vec{e_1} + x_2\vec{e_2}) = \rho x_1\vec{e_1} + \rho x_2\vec{e_2},$$

d'où la forme matricielle souhaitée.
En ce qui concerne les rotations, considérons un point $A(a,b)$ dont l'image par la rotation de centre $(0,0)$ et d'angle θ est le point $A'(a',b')$. Par le choix d'une origine au repère orthonormé, le point O identifie le point A au vecteur $\overrightarrow{OA}$ et le point O identifie le point A' au vecteur $\overrightarrow{OA'}$. On désignera par a (resp. a', b, b') la mesure du segment $[Oa]$ (resp. $[Oa']$, $[Ob]$, $[Ob']$).



Dans le triangle OAa on a

$$\begin{cases} a = |OA| \cos(\varphi) \\ b = |OA| \sin(\varphi), \end{cases}$$

et dans le triangle $OA'b'$, on a

$$\begin{cases} a' &= |OA'| \cos(\varphi + \theta) \\ b' &= |OA'| \sin(\varphi + \theta). \end{cases}$$

En utilisant les formules de trigonométrie, le système ci-dessus peut se réécrire comme

$$\begin{cases} a' &= |OA|(\cos(\varphi)\cos(\theta) - \sin(\varphi)\sin(\theta)) \\ b' &= |OA'|(\sin(\varphi)\cos(\theta) + \cos(\varphi)\sin(\theta)). \end{cases}$$

Or, puisque $|OA'| = |OA|$, en utilisant le premier système il vient

$$\begin{cases} a' &= a\cos(\theta) - b\sin(\theta) \\ b' &= a\sin(\theta) + b\cos(\theta). \end{cases}$$

Ce dernier système d'équations peut se réécrire sous forme matricielle, nous obtenons alors l'écriture équivalente

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

d'où la conclusion. □

Remarquons que, comme explicité dans la section précédente, tout point P image du point $(1,0)$ par une rotation de centre $(0,0)$ et d'angle $\theta \in [0, 2\pi[$ et par une homothétie de rapport ρ peut être exprimé selon ses coordonnées polaires $(\rho\cos(\theta), \rho\sin(\theta))$ ou cartésiennes (a,b) où a, b sont réels.

Une similitude de centre $(0,0)$, d'angle $\theta \in [0, 2\pi[$ et de rapport $\rho > 0$ est la composée d'une rotation de centre $(0,0)$ et d'angle θ avec une homothétie de rapport ρ. Aussi, rappelons que, sous forme matricielle, composer deux transformations linéaires consiste à faire le produit de leurs matrices associées. Dès lors, la matrice codant une telle similitude prend la forme

$$\begin{pmatrix} \rho\cos(\theta) & -\rho\sin(\theta) \\ \rho\sin(\theta) & \rho\cos(\theta) \end{pmatrix}$$

si l'on utilise les coordonnées polaires, tandis que si les coordonnées cartésiennes sont privilégiées, la matrice aura la forme ci-dessous

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

En utilisant l'addition matricielle et la multiplication par un scalaire, les matrices ci-dessus peuvent se décomposer comme suit

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

ou

$$a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Par définition, nous remarquons que les matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

codent une rotation de centre $(0,0)$ et d'angle $\theta = 0$ et une rotation de centre $(0,0)$ et d'angle $\theta = \frac{\pi}{2}$ respectivement, ce qui nous conduit à la définition suivante.

Définition 1.3.11. On définit

$$i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{et} \quad 1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Il s'agit donc là de notations. Dès lors, grâce à ces notations, toute matrice

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

peut être exprimée comme $a + ib$, le produit d'une matrice par un scalaire étant commutatif.

Définition 1.3.12. Soient a et b deux nombres réels. Une expression de la forme

$$a + ib = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

est appelée nombre complexe.

Les définitions d'addition et de multiplication de nombres complexes ainsi que la condition particulière $i^2 = -1$ découlent immédiatement de la définition 1.3.12 et de la définition de la somme et du produit matriciel. En effet, soient $z = a + ib$ et $z' = a' + ib'$ deux nombres complexes. On a,

$$z + z' = \begin{pmatrix} a+a' & -b-b' \\ b+b' & a+a' \end{pmatrix} = (a+a') \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (b+b') \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (a+a') + i(b+b'), \quad (1.19)$$

$$z.z' = \begin{pmatrix} aa'-bb' & -ab'-ba' \\ ba'+ab' & -bb'+aa' \end{pmatrix} = (aa'-bb') \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (ab'+ba') \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = (aa'-bb') + i(ab'+ba'), \quad (1.20)$$

et

$$i^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = -1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = -1$$

Nous retrouvons donc les définitions usuelles pour la somme et le produit de deux nombres complexes.

Définition 1.3.13. Soient $z = a+ib$ et $z' = a'+ib'$ deux nombres complexes avec $a, a', b, b' \in \mathbb{R}$. La somme de z et z' est définie par

$$z + z' = (a + ib) + (a' + ib') = a + a' + i(b + b'). \quad (1.21)$$

La multiplication des deux non nombres complexes z et z' est définie par

$$z.z' = (a + ib)(a' + ib') = aa' - bb' + i(ab' + ba'). \quad (1.22)$$

La concordance entre les formules 1.19 et 1.21 est évidente, tout comme c'est le cas pour les formule 1.20 et 1.22.

Analyse didactique

Voici donc comment Maggy Schneider et Hilda Rosseel résument les propos de Lartiller en ce qui concerne l'introduction des nombres complexes par les matrices. Tentons d'y apporter un regard didactique.
Cette approche a l'avantage de pouvoir justifier explicitement les opérations d'addition et de multiplication des nombres complexes. De plus, les notations prises à la définition 1.3.11 ne sont pas totalement dénuées de sens. En effet, la notation 1 pour la matrice identité peut s'expliquer relativement aisément par ce qu'elle définit. Effectivement, rappelons qu'elle rend compte d'une rotation du point $(1, 0)$ de centre $O(0, 0)$ et d'angle nul. Ainsi, le point $(1, 0)$ est envoyé sur lui-même. Et il est commode d'identifier les points situés sur l'axe des abscisses par leur première coordonnées, dans ce cas-ci le point $(1, 0)$ sera identifié à 1. Nous pouvons aussi le comprendre parce que la matrice identité définit la rotation identité. Pour le choix de notation de la matrice

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

l'argument est quelque peu semblable. Cette matrice désigne, souvenons-nous, une rotation de centre $O(0, 0)$ et d'angle $\theta = \frac{\pi}{2}$ du point $(1, 0)$. Ainsi, en désignant par i cette matrice-là, on rejoindrait l'idée de Jean Robert Argand qui consistait à vouloir interpréter "$\sqrt{-1}$" comme une rotation de 90 degrés du point $(1, 0)$ dans le plan. Mais d'où lui vint cette idée ? Comme déjà dit dans la section 1.1, Argand se basait sur fait qu'appliquer deux telles rotations de centre $O(0, 0)$ consistait à appliquer une rotation de 180 degrés au point $(1, 0)$ qui serait alors envoyé sur le point $(-1, 0)$, qui rappelons-le est identifié au réel -1. Ainsi, n'effectuer qu'une seule rotation

de 90 degrés du point $(1, 0)$ impliquerait que ce dernier se trouve sur une droite verticale perpendiculaire à l'axe des abscisses (l'axe des réels) passant par l'origine du repère. Le point image correspondrait alors à la racine carrée du point $(-1, 0)$ autrement dit, il correspondrait à la notation ambigüe $\sqrt{-1}$. Cette dernière perdra son ambiguïté grâce à l'intervention d'Euler qui, en 1777, remplacera cette notation par i que nous utilisons désormais.
Toutefois, elle présente également des désavantages. Le premier est lié au nouveau référentiel. Effectivement, les matrices n'y figurent plus et dès lors, introduire les nombres complexes par la méthode proposée ici impliquerait un coût considérable au niveau du temps. Par ailleurs, il est nécessaire que l'interprétation matricielle des transformations linéaires soit également abordée. Les deux autrices ajoutent à cela le fait que la question du sens concernant les nombres complexes se reporterait alors sur les transformations linéaires. On aurait donc simplement déplacé le problème. Un autre obstacle est celui de l'appellation même de *nombre complexe* que l'on associe à une matrice. De fait, il s'agit là d'un obstacle d'apprentissage du fait que les élèves pourraient éprouver des difficultés à associer une matrice, constituées de 4 nombres, à un nombre. Ils peuvent être embourbés dans un concept en se mettant des limites que personne ne leur impose. Dès les balbutiements de leur apprentissage scolaire ils identifient un nombre à une grandeur, or une matrice ne peut pas être représentée comme une grandeur.

Chapitre 2

Les quaternions

2.1 Un peu d'histoire et première définition

Dans le deuxième chapitre de ce mémoire, nous avançons dans l'histoire des mathématiques, ou plutôt dans l'histoire d'une infime part des mathématiques. Nous présenterons une importante découverte, faite en 1843, basée sur les nombres complexes : les quaternions. Aussi, nous démontrerons que l'algèbre des quaternions est une algèbre à composition. Ce résultat sera d'une grande importance dans la suite de ce travail, puisqu'il confirmera en quelque sorte le théorème d'Hurwitz. Avant d'entrer dans l'étude, même partielle, des quaternions, il serait bon de retracer l'histoire de leur origine mais également celle du brillant mathématicien qui est à l'origine de leur découverte [1].

FIGURE 2.1 – William Rowan Hamilton (1805 - 1865)

Sir William Rowan Hamilton est un mathématicien irlandais né à Dublin en 1805. Dès son plus jeune âge, et grâce à l'aide de son oncle professeur, il maîtrise plusieurs langues. Rapidement, à l'âge de 12 ans, il fait la connaissance de Zerah Colburn, un enfant prodige américain capable de réaliser des calculs mentaux extraordinaires. L'intérêt porté par Hamilton aux mathématiques semble être apparu après une défaite contre Zerah lors d'une "compétition arithmétique" qui avait lieu à Dublin. Par la suite, il étudie divers travaux de Newton et de Laplace, l'orientant vers le domaine de la physique. À l'âge de 18 ans, il entre comme élève au Trinity College de Dublin où il fait de remarquables progrès.
En 1827, alors qu'il est toujours étudiant, il est nommé professeur d'astronomie du Trinity

1. Pour des informations plus complètes sur la biographie d'Hamilton, le lecteur est renvoyé à la référence [1]

College et il obtient la fonction prestigieuse de directeur de l'observatoire de Dunsink à Dublin. On lui accorde également le titre honorifique de "Royal Astronomer of Ireland". Toutefois, Hamilton est visiblement trop jeune pour accepter cette fonction prestigieuse, d'autant plus que son intérêt pour l'astronomie commence à diminuer au profit des mathématiques.
Les années 1830 sont un véritable tournant pour Hamilton en ce qui concerne son intérêt pour les mathématiques. En effet, après avoir introduit les nombres complexes comme couples de nombres réels, il voulut étendre la théorie valide pour des paires de nombres à des triplets de nombres réels. Véritablement obsédé par cela, ses enfants deviennent également préoccupés par les recherches de leur père. On connaît encore aujourd'hui la phrase désormais célèbre que lui lançait un de ses fils chaque matin :

"Well, Papa can you multiply triplets ?"

Et chaque matin il lui répondait, la mine contrite, que malheureusement il ne pouvait que les additionner et les soustraire.
En effet, dans la base canonique de $\mathbb{R}^3$ donnée par $e := (1,0,0), i := (0,1,0)$ et $j := (0,0,1)$, il considère l'expression $\alpha + \beta i + \gamma j$ où $i^2 = j^2 = -1$ et souhaite tout simplement multiplier de telles expressions. Il veut naturellement que le produit soit distributif et commutatif, tout comme c'est le cas pour les nombres complexes, de sorte que

$$(\alpha + \beta i + \gamma j)^2 = \alpha^2 - \beta^2 - \gamma^2 + 2i\alpha\beta + 2j\alpha\gamma + 2ij\beta\gamma. \tag{2.1}$$

Aussi, il souhaite que la norme d'un produit de deux éléments de la forme $\alpha + \beta i + \gamma j$ soit égale au produit des normes associées, où la norme est désignée par la longueur Euclidienne. En d'autres termes, Hamilton désire que

$$|(\alpha + \beta i + \gamma j)^2| = |(\alpha + \beta i + \gamma j)(\alpha + \beta i + \gamma j)| = |\alpha + \beta i + \gamma j||\alpha + \beta i + \gamma j|. \tag{2.2}$$

Autrement dit, il souhaite que

$$|(\alpha^2 - \beta^2 - \gamma^2) + 2\alpha\beta i + 2\alpha\gamma j + 2\beta\gamma ij| = (\alpha^2 + \beta^2 + \gamma^2)^2.$$

Or, il remarque que

$$(\alpha^2 - \beta^2 - \gamma^2)^2 + (2\alpha\beta)^2 + (2\alpha\gamma)^2 = (\alpha^2 + \beta^2 + \gamma^2)^2. \tag{2.3}$$

Ainsi, étant donné l'expression (2.3) et pour que l'égalité 2.2 soit vérifiée, il faut que le coefficient $2ij$ soit nul.
Toutefois, partiellement convaincu de ce résultat, il en vient à considérer l'idée que le terme en ij de l'expression (2.1) ne doit peut-être pas s'écrire sous la forme d'un double produit mais plutôt sous la forme d'une somme $ij + ji$ telle que $ij = -ji$ pour conserver l'égalité souhaitée 2.2. La loi de commutativité n'étant dès lors plus conservée. Il prend l'initiative de poser $ij = k$ et $ji = -k$, se laissant l'opportunité de chercher si la valeur de k est nulle ou non.
Une première révélation vient alors à lui, le problème de la multiplication de triplets de nombres réels n'est pas à considérer dans un espace à 3 dimensions, mais bien dans un espace à 4 dimensions. Parvenant à montrer que la loi d'associativité est toujours préservée pour la multiplication de triplets, Hamilton peut alors affirmer ceci

$$k^2 = (ij)(ij) = i(ji)j = -i(ij)j = -i^2j^2 = -1.$$

C'est lors d'une balade avec sa femme, Helen Maria Bayly, le 16 octobre 1843 sur le pont Broome à Dublin qu'une deuxième grande révélation émerge dans son esprit telle une étincelle. Les relations fondamentales reliant les éléments de la base canonique de $\mathbb{R}^3$ qu'il avait jusqu'alors utilisées n'étaient en réalité pas de simples relations, elles décrivaient ce qu'il décida d'appeler *les quaternions*. Dès lors, dans un acte que l'on pourrait qualifier d'euphorie provoquée par cette découverte et surtout par l'idée même d'avoir enfin résolu, à cet instant précis, un problème qui lui avait torturé l'esprit pendant des années, il grave dans la pierre du pont Broome la formule fondamentale des quaternions

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

Sir William Rowan Hamilton consacre tout le reste de sa vie à étudier les quaternions, s'efforçant de les faire accepter par le monde des mathématiques. À l'époque, et dans de nombreuses université de Dublin, les quaternions deviennent même une matière d'examen.
Le plus fabuleux n'est pas tant la découverte des quaternions mais la reconnaissance qu'ils ont eu par la suite. Leur découverte a permis d'acquérir une grande liberté lors de la construction des systèmes qualifiés d'hypercomplexes.
En 1853, Hamilton publie un livre intitulé "Lectures on Quaternions" mais n'étant pas convaincu de son ouvrage et bien décidé à fournir un livre de qualité permettant d'étudier les quaternions le plus adéquatement possible, il publie un second livre corrigé qu'il intitule "Elements of Quaternions". Finalement, après avoir lutté toute sa vie contre son alcoolisme sévère, il décède d'une attaque de goutte peu de temps après avoir été élu premier membre étranger de la "National Academy of Science of the USA".

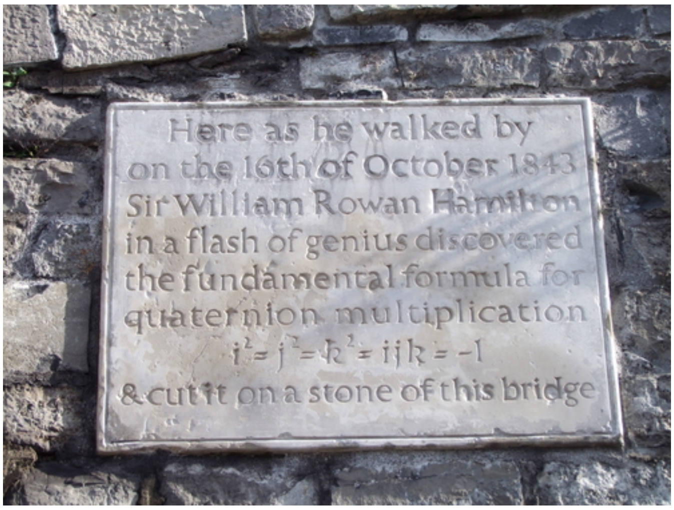


FIGURE 2.2 – Plaque commémorative pour la découverte de la formule de multiplication des quaternions par Hamilton sur le pont de Broome, Dublin.

Développons ici les conséquences de la formule fondamentale gravée par Hamilton dans la pierre du pont de Broome.

Proposition 2.1.1. *En faisant l'hypothèse que la multiplication est associative, la formule fondamentale des quaternions implique l'égalité $k = ij = -ji$.*

Démonstration. En premier lieu, on sait que $ijk = -1$. Dès lors, en multipliant à droite par k il vient, $(ijk)k = -k$ puisque 1 est l'élément neutre. Or, en utilisant l'associativité nous avons

$$(ijk)k = (ij)(kk) = (ij)k^2 = -ij,$$

ce qui nous donne $-ij = -k$ ou encore $ij = k$. Partant de cela il s'en suit

$$(ij)^2 = k^2 = -1$$

Or, par associativité on a $(ij)^2 = (ij)(ij) = i(ji)j$ donc

$$i(ji)j = -1$$

Dès lors, en multipliant à gauche et à droite par i et j respectivement nous avons les équivalences successives

$$\begin{aligned} & i(i(ji)j)j = -ij \\ \Leftrightarrow & (ii)(ji)(jj) = -ij \\ \Leftrightarrow & (-1)(ji)(-1) = -ij \\ \Leftrightarrow & ji = -ij, \end{aligned}$$

ce qui conclut la preuve. □

Dans le but de mieux comprendre le cheminement d'Hamilton, détaillons ici le résultat auquel il s'est heurté une bonne partie de sa vie. Ce résultat qui est également présenté à la référence [10].

Proposition 2.1.2. *Il n'existe pas de champ de dimension* 3 *qui soit une extension de* $\mathbb{R}$ *dont la base* $\{1, i, j\}$ *serait telle que* 1 *est l'élément neutre et telle que ses éléments vérifient la condition* $i^2 = j^2 = -1$.

Démonstration. Procédons par l'absurde et supposons qu'il existe un tel champ que nous noterons $\mathbb{T}$. Puisqu'il s'agit d'un champ, $\mathbb{T}$ est fermé pour la multiplication, autrement dit, le produit de deux éléments de $\mathbb{T}$ est encore un élément de $\mathbb{T}$. Montrons donc que le produit ij ne peut être une combinaison linéaire des éléments de la base. En effet, si $ij = a + bi + cj$ avec $a, b, c \in \mathbb{R}$, alors d'une part $i(ij) = -j$ par associativité et car $i^2 = -1$. Et d'autre d'autre part

$$i(ij) = i(a + bi + cj) = ai - b + cij = ai - b + c(a + bi + cj) = ca - b + (a + cb)i + c^2 j$$

par associativité et commutativité puisque $\mathbb{T}$ est un champ. Ainsi, sous cette condition nous avons

$$-j = ca - b + (a + cb)i + c^2 j$$

ce qui implique que $c^2 = -1$ ce qui est absurde étant donné que c est un nombre réel.
Dès lors, il n'existe pas un tel champ $\mathbb{T}$ de dimension 3 dont les éléments de la base ont les propriétés souhaitées. □

2.2 L'algèbre des quaternions : introduction classique et décomposition en partie réelle et vectorielle

Cette section consiste en la définition et l'élaboration de certaines propriétés des quaternions. Nous définirons un quaternions de trois façons différentes mais seules deux d'entre elles seront exploitées dans la présente section. Il sera également montré que l'ensemble des quaternions forme un corps, l'addition et la multiplication ayant toutes les propriétés adéquates pour qu'il le soit. Les définitions, propositions et autres théorèmes repris ci-dessous sont notamment tirés du livre de Ebbinghaus et al. intitulé *Numbers*, pour plus amples informations, le lecteur est invité à aller consulter la référence [15].

Tout comme il est d'usage de décomposer un nombre complexe dans la base $\{1, i\}$ de $\mathbb{C}$, comme espace vectoriel sur $\mathbb{R}$, nous utiliserons dans le travail la décomposition dans la base canonique $\{1, i, j, k\}$ de $\mathbb{R}^4$, et il sera sous-entendu, sous mention du contraire, que dans l'écriture $q = a + bi + cj + dk$, les nombres a, b, c, d sont réels.
Dans un premier temps, nous allons introduire les quaternions par leur table de multiplication. Pour ce faire, nous considérons donc la base $\mathcal{B}_{\mathbb{H}} = (1, i, j, k)$ où 1 est l'élément neutre. La table

de multiplication peut être déterminée grâce aux conditions imposées par Sir William Rowan Hamilton. Rappelons que les conditions imposées par Hamilton sont l'associativité de la multiplication ainsi que les quatre égalités $i^2 = j^2 = k^2 = ijk = -1$. Établissons donc la table de multiplication des quaternions.

Proposition 2.2.1. *La table de multiplication des quaternions est exprimée par le tableau à double entrée ci-dessous*

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Démonstration. Nous avons déjà démontré le fait que $ij = k$ à la Proposition 2.1.1. De plus, cette même proposition nous indique directement que $ji = -k$. Puisque l'on souhaite l'associativité de la multiplication, on doit obligatoirement avoir

$$ik = i(ij) = (ii)j = i^2 = -1.$$

De même,

$$(ik)k = i(kk) = ik^2 = -i$$

si nous voulons que la multiplication soit associative et que l'égalité $k^2 = -1$ soit vérifiée. Dès lors,

$$-i = (ik)k = -jk \quad \text{et} \quad i = jk$$

Ensuite, si l'on souhaite satisfaire à nouveau aux conditions exposées ci-dessus, il s'en suit

$$ki = (-ji)i = -j(ii) = -ji^2 = j,$$

et

$$kj = k(ki) = (kk)i = k^3 i = -i.$$

Et ainsi, la table de multiplication est complètement déterminée et représentée ci-dessus. □

L'algèbre réelle de dimension 4 construite de cette façon est l'algèbre des quaternions [2], notée $\mathbb{H}$ dont les éléments sont les quaternions. Ainsi, nous identifions $\mathbb{H}$ à $\mathbb{R}^4$.

Définition 2.2.2. L'ensemble des quaternions est l'ensemble

$$\mathbb{H} = \{q = a + bi + cj + dk | a, b, c, d \in \mathbb{R}\}$$

Une autre façon d'écrire les quaternions tout aussi connue car plus commode et moins fastidieuse, est d'exprimer un quaternion à partir de sa partie réelle et de sa partie imaginaire. C'est ce que nous développons ci-après.

Définition 2.2.3. On définit l'espace imaginaire de $\mathbb{H}$ comme

$$\begin{aligned} Im\mathbb{H} &= \mathbb{R}i + \mathbb{R}j + \mathbb{R}k \\ &= \{\beta i + \gamma j + \delta k : \beta, \gamma, \delta \in \mathbb{R}\}. \end{aligned}$$

2. où la notion "d'algèbre" désigne une structure munie d'une addition, d'un produit par un scalaire et d'une opération interne qui obéissent à diverses conditions spécifiées à la définition 2.3.1 de la prochaine section. Nous démontrerons plus loin dans la présente section l'affirmation faite ici.

Il s'agit d'un sous-espace vectoriel de $\mathbb{H}$ dont les éléments sont appelés *imaginaires purs*. L'espace des quaternions peut alors se décomposer en deux parties : une partie réelle et une partie imaginaire telles que

$$\mathbb{H} = \mathbb{R} \oplus Im\mathbb{H}.$$

C'est Hamilton qui, en 1846, utilisa pour la première fois le terme *vecteur* au sens moderne [3]. Ainsi, un quaternion imaginaire pur peut également être appelé *quaternion vecteur*. Ceci nous mène donc à la définition suivante.

Définition 2.2.4. Tout quaternion w peut s'exprimer de façon unique sous la forme

$$w = \alpha + v_w \quad (\alpha \in \mathbb{R} \text{ et } v_w \in Im\mathbb{H}), \tag{2.4}$$

où le terme α désigne la partie scalaire de w (ou encore la partie réelle de w), notée $\Re(w)$, et où le terme v_w est appelé partie vectorielle de w (ou encore partie imaginaire (pure) de w) et est noté $\Im(w)$.

Assurément, bien que le calcul vectoriel moderne soit l'oeuvre de Gibbs [4] et non celle d'Hamilton, il ne paraît pas totalement farfelu de vouloir introduire cette autre définition car, non seulement Hamilton est à l'origine de la notion moderne de vecteur, mais lui-même écrivait déjà un quaternion sous la forme 2.4. En effet, dans l'ouvrage *Elements of Quaternions* [16] écrit par Sir William Rowan Hamilton en personne et publié à titre posthume par son fils nous pouvons lire les propos suivants :

"It will be shown, at a larger stage, that there is an important sense in which we can conceive a scalar to be added to a vector; and that the sum so obtained, or the combination "Scalar Plus Vector" is a quaternion."

Remarque 2.2.5. Partant de cela, il est évident que $w \in Im\mathbb{H}$ si et seulement si $\alpha = 0$.

Avant de continuer dans l'introduction des quaternions et des différents résultats s'y apparentant, faisons un aparté sur une autre définition possible d'un quaternion. Même si nous ne développerons pas cette vision-là des quaternions dans la suite de cette section, il est bon de constater que l'ensemble des quaternions $\mathbb{H}$, qui rappelons-le est identifié à $\mathbb{R}^4$, peut-être identifié à $\mathbb{R}^2 \times \mathbb{R}^2$. La remarque ci-après vient alors naturellement.

Remarque 2.2.6. Une autre façon d'écrire un quaternion existe et nous la devons à Sir William Rowan Hamilton lui-même. Elle consiste à écrire un quaternion sous la forme d'un couple de deux nombres complexes. Pour arriver à un tel résultat il convient de considérer un quaternion $q = a + bi + cj + dk$ où a, b, c, d sont quatre nombres réels et de réexprimer le dernier élément de base k comme ij et ce, sans problème aucun puisque $ij = k$. Ainsi nous avons

$$q = a + bi + cj + dij = (a + bi) + (c + di)j,$$

où $a + bi$ et $c + di$ désignent deux nombres complexes. Notons-les x et y respectivement. Par conséquent, le quaternion q peut s'écrire sous la forme $q = x + yj$ ou encore sous la forme $q = (x, y)$ si on identifie $(1, 0) = 1$ et $(0, 1) = j$.

Cette observation étant faite, nous pouvons poursuivre l'introduction des quaternions. Mais avant d'entrer dans le vif du sujet, nous commençons par une petite propriété qui, bien que n'ayant pas de rôle dans la suite de ce mémoire, reste intéressante.

3. Argand utilisait déjà implicitement le concept de vecteur dans sa représentation géométrique des nombres complexes tout comme Kepler qui l'utilisait sous la notion de rayon-vecteur. Pour plus amples informations, le lecteur est invité à consulter la référence [2]

4. Josiah Williard Gibbs (1839 – 1903) est un scientifique américain.

Proposition 2.2.7. *Soient $u, v \in Im\mathbb{H}$ (u, v sont deux quaternions purement imaginaires). Alors, $u^2 = -\omega$ où $\omega \in \mathbb{R}^+$ et $uv + vu \in \mathbb{R}$.*

Démonstration. Soient $\beta, \gamma, \delta \in \mathbb{R}$ tels que $u = \beta i + \gamma j + \delta k$. On trouve que

$$u^2 = -(\beta^2 + \gamma^2 + \delta^2) \in \mathbb{R}$$

en développant simplement le carré et étant donné que i, j et k anticommutent. Il est bien entendu évident que le facteur $\beta^2 + \gamma^2 + \delta^2$ est positif ou nul puisque chacun des termes qui le compose est un nombre réel positif ou nul. Or, u, v et $u + v \in Im\mathbb{H}$. Donc, puisque $uv + vu$ peut s'écrire comme

$$\begin{aligned} uv + vu &= u^2 + uv + vu + v^2 - u^2 - v^2 \\ &= (u + v)^2 - u^2 - v^2, \end{aligned}$$

il est évident qu'il appartient à l'ensemble des réels $\mathbb{R}$ puisque, par ce qui vient d'être fait dans la première partie de la démonstration, chacun de ses termes est un nombre appartenant lui-même aux réels. □

Afin de pouvoir analyser différents résultats par la suite, il est important de poser quelques définitions et propriétés élémentaires à propos des quaternions. Les quelques propositions qui suivent ne sont évidemment pas des plus intéressantes de par leur simplicité, mais elles sont faites uniquement dans le but de rendre ce mémoire complet.

Proposition 2.2.8. *Soient $w = a + bi + cj + dk = a + v_w$ et $w' = a' + b'i + c'j + d'k = a' + v_{w'}$ deux quaternions avec $a, a', b, b', c, c', d, d' \in \mathbb{R}$ et v_w (resp. $v_{w'}$) la partie vectorielle de w (resp. w'). On a l'égalité des deux quaternions si et seulement si*

$$\begin{cases} a &= a' \\ v_w &= v_{w'} \end{cases}$$

Démonstration. C'est immédiat par définition de l'égalité de deux vecteurs de $\mathbb{R}^4$. □

Définition 2.2.9. Soient a, b, c, d, a', b', c' et d' des réels tels que $w = a + bi + cj + dk$ et $w' = a' + b'i + c'j + d'k$ sont deux quaternions. La somme de w avec w' est le quaternion $w + w'$ défini comme

$$w + w' = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

Proposition 2.2.10. *Soient $w = a + v_w$ et $w' = a' + v_{w'}$ deux quaternions avec $a, a' \in \mathbb{R}$ et $v_w, v_{w'}$ les parties vectorielles de w et w' respectivement. La somme de w et w' est le quaternion $w + w'$ donné par*

$$w + w' = (a + a') + (v_w + v_{w'}).$$

Démonstration. En effet, en particulier v_w et $v_{w'}$ sont des quaternions, et si on considère que $v_w = bi + cj + dk$ et $v_{w'} = b'i + c'j + d'k$ avec $b, b', c, c', d, d' \in \mathbb{R}$ alors, par définition de la somme de deux quaternions, on a

$$v_w + v_{w'} = (b + b')i + (c + c')j + (d + d')k.$$

Aussi, avec les notations prises ici nous avons

$$w + w' = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

ce qui nous permet de dire que $w + w' = (a + a') + (v_w + v_{w'})$, ce que nous souhaitions. □

Proposition 2.2.11. *L'addition possède les propriétés suivantes :*

1. *Elle est associative : pour tous $w_1, w_2, w_3 \in \mathbb{H}$, $(w_1 + w_2) + w_3 = w_1 + (w_2 + w_3)$;*
2. *Elle est commutative : pour tous $w_1, w_2 \in \mathbb{H}$, $w_1 + w_2 = w_2 + w_1$;*
3. *Il existe un neutre $0 = 0 + 0i + 0j + 0k$: pour tout $w \in \mathbb{H}$, $w + 0 = 0 + w = w$;*
4. *Tout élément w admet un opposé noté $-w$: pour tout $w \in \mathbb{H}, \exists w' \in \mathbb{H}$, $w + w' = 0 = w' + w$.*

Démonstration. Soient $w_m = a_m + b_m i + c_m j + d_m k \in \mathbb{H}$ où $a_m, b_m, c_m, d_m \in \mathbb{R}$ pour $m \in \{1, 2, 3\}$. L'addition est associative. En effet, en utilisant la Définition 2.2.9, et puisque l'addition est associative sur $\mathbb{R}$ nous avons,

$$\begin{aligned}(w_1 + w_2) + w_3 &= ((a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k) + (a_3 + b_3 i + c_3 j + d_3 k)\\ &= ((a_1 + a_2) + a_3) + ((b_1 + b_2) + b_3)i + ((c_1 + c_2) + c_3)j + ((d_1 + d_2) + d_3)k\\ &= (a_1 + (a_2 + a_3)) + (b_1 + (b_2 + b_3))i + (c_1 + (c_2 + c_3))j + (d_1 + (d_2 + d_3))k\\ &= w_1 + (w_2 + w_3)\end{aligned}$$

Elle est commutative car

$$\begin{aligned}w_1 + w_2 &= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k\\ &= (a_2 + a_1) + (b_2 + b_1)i + (c_2 + c_1)j + (d_2 + d_1)k\\ &= w_2 + w_1\end{aligned}$$

puisque la somme sur $\mathbb{R}$ est commutative.
L'addition admet un neutre. En effet, considérons deux quaternions w_1 et w_2. On a $w_1 + w_2 = w_1$ si et seulement si

$$(a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k = a_1 + b_1 i + c_1 j + d_1 k$$

Etant donné la Définition 2.2.8, ceci est équivalent à

$$\left\{\begin{array}{rcl} a_1 + a_2 &=& a_1\\ b_1 + b_2 &=& b_1\\ c_1 + c_2 &=& c_1\\ d_1 + d_2 &=& d_1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} a_2 &=& 0\\ b_2 &=& 0\\ c_2 &=& 0\\ d_2 &=& 0 \end{array}\right.$$

puisque 0 est neutre pour l'addition sur $\mathbb{R}$. Bien entendu, le résultat est le même pour montrer que $w_2 + w_1 = w_1$.
Pour tout quaternion w_1, il existe un quaternion w_2 tel que $w_1 + w_2 = 0$. En effet,

$$w_1 + w_2 = 0 \Leftrightarrow (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k = 0 + 0i + 0j + 0k,$$

ce qui est équivalent à

$$\left\{\begin{array}{rcl} a_1 + a_2 &=& 0\\ b_1 + b_2 &=& 0\\ c_1 + c_2 &=& 0\\ d_1 + d_2 &=& 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} a_2 &=& -a_1\\ b_2 &=& -b_1\\ c_2 &=& -c_1\\ d_2 &=& -d_1 \end{array}\right.$$

étant donné que, sur $\mathbb{R}$, tout élément admet un opposé. □

Définition 2.2.12. Soient a, b, c, d, a', b', c' et d' des réels tels que $w = a + bi + cj + dk$ et $w' = a' + b'i + c'j + d'k$ sont deux quaternions. Le produit de w par w' est le quaternion ww' défini comme

$$ww' = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' + ca' + db' - bd')j + (ad' + da' + bc' - cb')k$$

Remarque 2.2.13. Dans le cas où nous considérerions qu'un quaternion est défini par un couple de nombres complexes, l'addition et la multiplication seraient définies comme suit,

$$q + p = (x, y) + (x', y') = (x + x', y + y'),$$

et

$$qp = (x, y)(x', y') = (xx' - \overline{y'}y, y\overline{x'} + y'x).$$

où $q = (x, y)$ et $p = (x', y')$ sont deux éléments de $\mathbb{H}$ et où l'application conjugaison présente ici est la conjugaison définie sur $\mathbb{C}$.

La définition 2.2.12 que nous venons de poser permet de rencontrer le souhait d'Hamilton, c'est-à-dire de faire en sorte que la multiplication soit associative et que la quadruple identité gravée dans le pont de Broome soit vérifiée. En effet, il suffirait de faire les calculs à la main pour s'en assurer mais ce serait long et fastidieux, c'est pourquoi nous introduisons une autre formule rendant compte du produit de deux quaternions. Ainsi, nous exprimons la multiplication de quaternions en fonction de deux opérations bien connues sur leurs parties imaginaires que sont le produit scalaire et le produit vectoriel.

Nous supposons qu'à ce stade le lecteur/la lectrice connaît les résultats s'apparentant aux produits scalaire et vectoriel canoniques de $\mathbb{R}^3$ et $\mathbb{R}^4$. Nous allons maintenant démontrer les propriétés pour la multiplication.

Proposition 2.2.14. *Soient $w = a + v_w$ et $w' = a' + v_{w'}$ deux quaternions avec a, a' les parties réelles et $v_w, v_{w'}$ les parties vectorielles de w et w' respectivement. Le produit de w avec w' est déterminé par l'expression*

$$ww' = (aa' - \langle v_w, v_{w'}\rangle) + (a'v_w + av_{w'} + v_w \wedge v_{w'})$$

avec le produit scalaire et le produit vectoriel usuels de $\mathbb{R}^3$ où on a supposé la base (i, j, k) orthonormée et positive.

Démonstration. Calculons le membre de droite. Ainsi, dans $\mathbb{R}^3$, déterminons les produits $a'v_w$, $av_{w'}$ ainsi que le produit scalaire et le produit vectoriel de v_w avec $v_{w'}$ où $v_w = bi + cj + dk$ et $v_{w'} = b'i + c'j + d'k$. On a

$$a'v_w = a'bi + a'cj + a'dk \quad \text{et} \quad av_{w'} = ab'i + ac'j + ad'k.$$

Ensuite, par définition du produit vectoriel, on a

$$v_w \wedge v_{w'} = (cd' - c'd)i + (b'd - bd')j + (bc' - b'c)k.$$

Et pour finir, le produit scalaire étant bilinéaire il vient

$$\begin{aligned}\langle v_w, v_{w'}\rangle &= \langle bi + cj + dk, b'i + c'j + d'k\rangle \\ &= bb'\langle i, i\rangle + bc'\langle i, j\rangle + bd'\langle i, k\rangle + cb'\langle j, i\rangle + cc'\langle j, j\rangle + cd'\langle j, k\rangle + db'\langle k, i\rangle \\ &\quad + dc'\langle k, j\rangle + dd'\langle k, k\rangle.\end{aligned}$$

La base $\mathcal{B}_{\mathbb{H}} = (i, j, k)$ étant orthonormée, les produits scalaires de deux éléments distincts de la base sont nuls. Dès lors, il nous reste

$$\langle v_w, v_{w'}\rangle = bb' + cc' + dd' \tag{2.5}$$

Finalement, en comparant le produit de w avec w' comme indiqué à la Définition 2.2.12 avec les calculs que nous avons obtenu, nous avons le résultat souhaité

$$ww' = (aa' - \langle v_w, v_{w'}\rangle) + (a'v_w + av_{w'} + v_w \wedge v_{w'}).$$

□

Il me parait utile d'énoncer et de développer la proposition suivante puisqu'elle met en évidence le produit scalaire et le produit vectoriel de quaternions imaginaires ainsi que les liens entre les deux. Par ailleurs, il y est fait mention de deux beaux résultats que sont l'identité de Grassmann et l'identité de Jacobi. De plus, cette proposition sera également utilisée dans la suite de ce mémoire. En vue de ne pas alourdir l'écriture dans cette proposition, nous noterons u (resp. v) les quaternions imaginaires purs v_u (resp. v_v).

Proposition 2.2.15. *Soient $u, v \in Im\mathbb{H}$ tels que $u = \beta i + \gamma j + \delta k$ et $v = \rho i + \sigma j + \tau k$. Alors*

- $uv = -(\beta\rho + \gamma\sigma + \delta\tau) + (\gamma\tau - \delta\sigma)i + (\delta\rho - \beta\tau)j + (\beta\sigma - \gamma\rho)k;$ (2.6)
- $uv = -\langle u, v\rangle + u \wedge v;$ (2.7)
- *L'application $(u, v) \mapsto u \wedge v$ est bilinéaire et antisymétrique, i.e. $u \wedge v = -v \wedge u$;* (2.8)
- $u \wedge v = \frac{1}{2}(uv - vu)$ *et* $\langle u, v\rangle = -\frac{1}{2}(uv + vu);$ (2.9)
- *Le produit vectoriel n'est pas associatif et $u \wedge (v \wedge w) = \frac{1}{2}(uvw - vwu)$;* (2.10)
- *L'identité de Grassmann : $u \wedge (v \wedge w) = \langle u, w\rangle v - \langle u, v\rangle w$;* (2.11)
- *L'identité de Jacobi : $u \wedge (v \wedge w) + v \wedge (w \wedge u) + w \wedge (u \wedge v) = 0$;* (2.12)

Démonstration. Le premier point est immédiat et à déjà été prouvé à la proposition 2.2.14. Le second point s'obtient en comparant 2.6 avec la somme $-\langle u, v\rangle + u \wedge v$ où les expressions détaillées de $-\langle u, v\rangle$ et $u \wedge v$ ont été exprimées à la proposition 2.2.14. Le résultat 2.8 de cette proposition est évident par définition du produit vectoriel. Montrons maintenant le quatrième point de cette proposition. Par 2.7, on sait

$$uv = -\langle u, v\rangle + u \wedge v \quad \text{et} \quad vu = -\langle v, u\rangle + v \wedge u$$

Or le produit scalaire est symétrique et le produit vectoriel est antisymétrique comme l'affirme 2.8, donc

$$vu = -\langle u, v\rangle - u \wedge v$$

Ainsi, $uv + vu = -2\langle u, v\rangle$ et $uv - vu = 2(u \wedge v)$, ce que nous souhaitions.
Passons désormais à la démonstration du cinquième point de cette proposition. En utilisant 2.7 il vient,

$$uvw = u(-\langle v, w\rangle + v \wedge w) = -\langle v, w\rangle u + u(v \wedge w)$$

et

$$vwu = (-\langle v, w\rangle + v \wedge w)u = -\langle v, w\rangle u + (v \wedge w)u.$$

Dès lors, par ce que nous venons d'établir et en utilisant la propriété 2.7 nous obtenons

$$\begin{aligned} uvw - vwu &= u(v \wedge w) - (v \wedge w)u \\ &= -\langle u, v \wedge w\rangle + u \wedge (v \wedge w) + \langle v \wedge w, u\rangle - (v \wedge w) \wedge u \\ &= 2u \wedge (v \wedge w). \end{aligned}$$

où la dernière égalité découle de la symétrie du produit scalaire et de l'antisymétrie du produit vectoriel. Démontrons l'identité de Grassmann. Pour ce faire, repartons de ce que nous venons de prouver ci-dessus. On a

$$\begin{aligned} u \wedge (v \wedge w) &= \frac{1}{2}(uvw - vwu) \\ &= \frac{1}{2}(uvw - vuw + vuw - vwu) \\ &= \frac{1}{2}((uv + vu)w - v(uw + wu)) \end{aligned}$$

Or, $uv + vu = -2\langle u, v\rangle$ et réciproquement, $uw + wu = -2\langle u, w\rangle$. Dès lors, il vient directement

$$u \wedge (v \wedge w) = -\langle u, v\rangle w + \langle u, w\rangle v$$

Pour montrer l'identité de Jacobi, il suffit de réécrire le membre de gauche en utilisant l'identité de Grassmann 2.11 que nous venons de démontrer. □

Proposition 2.2.16. *Soient u, v, w trois quaternions imaginaires purs. On a l'égalité*

$$\langle u \wedge v, w\rangle = \langle u, v \wedge w\rangle. \tag{2.13}$$

Démonstration. Dans cette démonstration, u, v, w sont trois quaternions imaginaires purs. Tout d'abord, nous avons

$$\begin{aligned} \langle u \wedge v, w\rangle &= \langle \frac{1}{2}(uv - vu), w\rangle \\ &= \frac{1}{2}(\langle uv, w\rangle - \langle vu, w\rangle) \\ &= -\frac{1}{4}(uvw + wuv - vuw - wvu), \end{aligned}$$

en utilisant l'expression du produit scalaire et du produit vectoriel donné par 2.9 à la proposition 2.2.15. Par le même argument, nous trouvons également

$$\begin{aligned} \langle u, v \wedge w\rangle &= \langle u, \frac{1}{2}(vw - wv)\rangle \\ &= \frac{1}{2}(\langle u, vw\rangle - \langle u, wv\rangle) \\ &= -\frac{1}{4}(uvw + vwu - uwv - wvu). \end{aligned}$$

Si nous parvenons à montrer que nous avons l'égalité $wuv - vuw = vwu - uwv$, alors nous aurons le résultat escompté 2.13. On a,

$$\begin{aligned} wuv - vuw - vwu + uwv &= 0 \\ \Leftrightarrow (wu + uw)v - v(uw + wu) &= 0 \\ \Leftrightarrow -2\langle w, u\rangle v + 2v\langle u, w\rangle &= 0. \end{aligned}$$

Or, puisque le produit scalaire de deux quaternions est symétrique et qu'il désigne un nombre réel, alors la dernière égalité est toujours vérifiée et nous pouvons conclure. □

Il convient également de remarquer que, puisque par définition du produit vectoriel $u \wedge v$ est orthogonal à u et à v, il s'en suit que $\langle u \wedge v, u\rangle = \langle u \wedge v, v\rangle = 0$.
Démontrons désormais les diverses propriétés prises par la multiplication. Non seulement intéressantes, celles-ci nous seront très utiles dans la suite de ce travail.

Proposition 2.2.17. *La multiplication possède les propriétés suivantes :*

1. *Elle est associative : pour tous $w_1, w_2, w_3 \in \mathbb{H}, (w_1w_2)w_3 = w_1(w_2w_3)$;*
2. *Elle n'est pas commutative : il existe $w_1, w_2 \in \mathbb{H}, w_1w_2 \neq w_2w_1$;*
3. *Le neutre pour l'addition est absorbant pour la multiplication : pour tout $w \in \mathbb{H}, w0 = 0 = 0w$;*
4. *Existence d'un neutre $1 = 1 + 0i + 0j + 0k$: pour tout $w \in \mathbb{H}, w1 = w = 1w$.*
5. *La multiplication distribue l'addition : pour tous $w_1, w_2, w_3 \in \mathbb{H}, w_1(w_2 + w_3) = w_1w_2 + w_1w_3$ et $(w_1 + w_2)w_3 = w_1w_3 + w_2w_3$.*

Démonstration. Dans cette démonstration, sauf mention explicite, nous considérons les octonions w_1, w_2, w_3 sous la forme $w_1 = a_1 + v_{w_1}, w_2 = a_2 + v_{w_2}, w_3 = a_3 + v_{w_3}$.
Commençons par prouver que la multiplication est associative, et pour ce faire montrons que $(w_1w_2)w_3 = w_1(w_2w_3)$. D'une part, en utilisant deux fois la proposition 2.2.14 on a

$$\begin{aligned}(w_1w_2)w_3 &= ((a_1a_2 - \langle v_{w_1}, v_{w_2}\rangle) + (a_2v_{w_1} + a_1v_{w_2} + v_{w_1} \wedge v_{w_2}))(a_3 + v_{w_3}) \\ &= ((a_1a_2 - \langle v_{w_1}, v_{w_2}\rangle)a_3 - \langle a_2v_{w_1} + a_1v_{w_2} + v_{w_1} \wedge v_{w_2}, v_{w_3}\rangle) \\ &\quad + (a_3(a_2v_{w_1} + a_1v_{w_2} + v_{w_1} \wedge v_{w_3}) + (a_1a_2 - \langle v_{w_1}, v_{w_2}\rangle)v_{w_3} \\ &\quad + (a_2v_{w_1} + a_1v_{w_2} + v_{w_1} \wedge v_{w_2}) \wedge v_{w_3}).\end{aligned}$$

Or, par définition du produit d'un quaternion par un scalaire tout en utilisant le fait que le produit vectoriel est linéaire et antisymétrique et que le produit scalaire est linéaire, il s'en suit

$$\begin{aligned}(w_1w_2)w_3 = a_1a_2a_3 &- \langle v_{w_1}, v_{w_2}\rangle a_3 - a_2\langle v_{w_1}, v_{w_3}\rangle - a_1\langle v_{w_2}, v_{w_3}\rangle - \langle v_{w_1} \wedge v_{w_2}, v_{w_3}\rangle \\ &+ a_3a_2v_{w_1} + a_3a_1v_{w_2} + a_3v_{w_1} \wedge v_{w_2} + a_1a_2v_{w_3} - \langle v_{w_1}, v_{w_2}\rangle v_{w_3} \\ &+ a_2v_{w_1} \wedge v_{w_3} + a_1v_{w_2} \wedge v_{w_3} - v_{w_3} \wedge (v_{w_1} \wedge v_{w_2}).\end{aligned}$$

D'autre part, en utilisant exactement le même raisonnement, on a

$$\begin{aligned}w_1(w_2w_3) &= (a_1 + v_{w_1})((a_2 + v_{w_2})(a_3 + v_{w_3})) \\ &= a_1a_2a_3 - a_1\langle v_{w_2}, v_{w_3}\rangle - a_3\langle v_{w_1}, v_{w_2}\rangle - a_2\langle v_{w_1}, v_{w_3}\rangle - \langle v_{w_1}, v_{w_2} \wedge v_{w_3}\rangle \\ &\quad + a_2a_3v_{w_1} - \langle v_{w_2}, v_{w_3}\rangle v_{w_1} + a_1a_3v_{w_2} + a_1a_2v_{w_3} + a_1v_{w_2} \wedge v_{w_3} \\ &\quad + a_3v_{w_1} \wedge v_{w_2} + a_2v_{w_1} \wedge v_{w_3} + v_{w_1} \wedge (v_{w_2} \wedge v_{w_3}).\end{aligned}$$

Ensuite, pour montrer l'égalité $(w_1w_2)w_3 = w_1(w_2w_3)$ nous devons nous assurer que

$$-\langle v_{w_1} \wedge v_{w_2}, v_{w_3}\rangle - \langle v_{w_1}, v_{w_2}\rangle v_{w_3} - v_{w_3} \wedge (v_{w_1} \wedge v_{w_2}) = -\langle v_{w_1}, v_{w_2} \wedge v_{w_3}\rangle - \langle v_{w_2}, v_{w_3}\rangle v_{w_1} + v_{w_1} \wedge (v_{w_2} \wedge v_{w_3}) \tag{2.14}$$

Toutefois, par la proposition précédente on sait que $\langle v_{w_1} \wedge v_{w_2}, v_{w_3}\rangle = \langle v_{w_1}, v_{w_2} \wedge v_{w_3}\rangle$. Ainsi, l'égalité 2.14 n'est vérifiée que si nous avons l'égalité suivante

$$-\langle v_{w_1}, v_{w_2}\rangle v_{w_3} - v_{w_3} \wedge (v_{w_1} \wedge v_{w_2}) = -\langle v_{w_2}, v_{w_3}\rangle v_{w_1} + v_{w_1} \wedge (v_{w_2} \wedge v_{w_3}). \tag{2.15}$$

Or, celle-ci est bien vérifiée. En effet, en utilisant l'identité de Jacobi, l'identité de Grassmann et puisque le produit scalaire est symétrique, le terme de gauche de l'égalité ci-dessus s'écrit successivement sous la forme

$$\begin{aligned}-\langle v_{w_1}, v_{w_2}\rangle v_{w_3} - v_{w_3} \wedge (v_{w_1} \wedge v_{w_2}) &= -\langle v_{w_1}, v_{w_2}\rangle v_{w_3} + v_{w_1} \wedge (v_{w_2} \wedge v_{w_3}) + v_{w_2} \wedge (v_{w_3} \wedge v_{w_1}) \\ &= -\langle v_{w_1}, v_{w_2}\rangle v_{w_3} + v_{w_1} \wedge (v_{w_2} \wedge v_{w_3}) + \langle v_{w_2}, v_{w_1}\rangle v_{w_3} - \langle v_{w_2}, v_{w_3}\rangle v_{w_1} \\ &= v_{w_1} \wedge (v_{w_2} \wedge v_{w_3}) - \langle v_{w_2}, v_{w_3}\rangle v_{w_1}.\end{aligned}$$

D'où l'égalité désirée.
Ensuite, la multiplication n'est pas commutative. En effet, considérons par exemple les quaternions $w_1 = 1 - i$ et $w_2 = 1 + (j - k)$. D'une part nous avons

$$w_1w_2 = (1 - i)(1 + j - k) = 1 + j - k - i - ij + ik = 1 + j - k - i - k - j = 1 - i - 2k,$$

et d'autre part,

$$w_2w_1 = (1 + j - k)(1 - i) = 1 - i + j - ji - k + ki = 1 - i + j + k - k + j = 1 - i + 2j.$$

Dès lors, on trouvons bien $w_1w_2 \neq w_2w_1$.
Montrons que $0 = 0 + 0i + 0j + 0k$ est absorbant pour la multiplication. Considérons $w = a + bi + cj + dk$, par définition on a

$$w0 = 0 + 0i + 0j + 0k = 0$$

étant donné que 0 est absorbant pour la multiplication sur $\mathbb{R}$. Le résultat est identique pour montrer que $0w = 0$.
Ensuite, montrons que $1 = 1 + 0i + 0j + 0k$ est neutre pour la multiplication. On a

$$\begin{aligned}
w1 &= (a1 - b0 - c0 - d0) + (a0 + b1 + c0 - d0)i + (a0 + c1 + d0 - b0)j + (a0 + d1 + b0 - c0)k \\
&= a + bi + cj + dk \\
&= w
\end{aligned}$$

où la deuxième égalité est justifiée par le fait que 0 soit absorbant pour la multiplication et neutre pour l'addition dans $\mathbb{R}$. Par le même développement on peut montrer que $1w = w$ de sorte que 1 est l'élément neutre pour la multiplication.
Pour finir, montrons que la multiplication distribue l'addition. On a

$$\begin{aligned}
w_1(w_2 + w_3) &= (a_1 + v_{w_1})((a_2 + a_3) + (v_{w_2} + v_{w_3})) \\
&= (a_1(a_2 + a_3) - \langle w_1, w_2 + w_3\rangle) + (a_2 + a_3)v_{w_1} + a_1(v_{w_2} + v_{w_3}) + v_{w_1} \wedge (v_{w_2} + v_{w_3}) \\
&= (a_1a_2 + a_1a_3 - \langle w_1, w_2\rangle - \langle w_1, w_3\rangle) + (a_2 + a_3)v_{w_1} + a_1(v_{w_2} + v_{w_3}) + v_{w_1} \wedge (v_{w_2} + v_{w_3}),
\end{aligned}$$

puisque le produit scalaire est bilinéaire. Le produit vectoriel étant distributif sur la somme, il vient finalement

$$\begin{aligned}
w_1(w_2 + w_3) &= a_1a_2 + a_1a_3 - \langle w_1, w_2\rangle - \langle w_1, w_3\rangle + a_2v_{w_1} + a_3v_{w_1} + a_1v_{w_2} + a_1v_{w_3} + v_{w_1} \wedge v_{w_2} \\
&\quad + v_{w_1} \wedge v_{w_3} \\
&= a_1a_2 - \langle w_1, w_2\rangle + a_2v_{w_1} + a_1v_{w_2} + v_{w_1} \wedge v_{w_2} + a_1a_3 - \langle w_1, w_3\rangle + a_3v_{w_1} + a_1v_{w_3} \\
&\quad + v_{w_1} \wedge v_{w_3} \\
&= w_1w_2 + w_1w_3.
\end{aligned}$$

Le résultat $(w_1 + w_2)w_3$ se démontre de façon équivalente. □

Proposition 2.2.18. *L'ensemble des quaternions $\mathbb{H}$ muni de l'addition et de la multiplication données aux définitions 2.2.9 et 2.2.12 (ou encore définies aux propositions 2.2.10 et 2.2.14) est une algèbre sur $\mathbb{R}$ au sens de la définition 2.3.1.*

Démonstration. Pour tous $x, y, z \in \mathbb{H}$, la proposition 2.2.17 indique que $(x + y)z = xz + yz$ et $x(y + z) = xy + xz$. Dès lors, il suffit de montrer que pour tous $\lambda, \mu \in \mathbb{R}$ et tous $x, y \in \mathbb{H}$ on a $(\lambda x)(\mu y) = \lambda\mu(xy)$. Autrement dit, nous devons prouver que tous les nombres réels commutent avec tous les quaternions. Supposons que $x = a + v_x$ et $y = b + v_y$ avec $a, b \in \mathbb{R}$ et rappelons que λ et μ sont deux quaternions particuliers. Par définition du produit de deux quaternions on a,

$$\lambda x = (\lambda + 0)(a + v_x) = \lambda a + \lambda v_x \quad \text{et} \quad \mu y = (\mu + 0)(b + v_y) = \mu b + \mu v_y.$$

Par conséquent,

$$\begin{aligned}
(\lambda x)(\mu y) &= (\lambda a + \lambda v_x)(\mu b + \mu v_y) \\
&= \lambda a\mu b - \langle\lambda v_x, \mu v_y\rangle + \mu b\lambda v_x + \lambda a\mu v_y \\
&= \lambda\mu ab - \lambda\mu\langle v_x, v_y\rangle + \lambda\mu bv_x + \lambda\mu av_y \\
&= \lambda\mu(ab - \langle v_x, v_y\rangle + bv_x + av_y) \\
&= \lambda\mu(xy),
\end{aligned}$$

ce que nous souhaitions. □

La proposition ci-dessus justifie donc les propos utilisés précédemment lorsqu'il était question de "l'algèbre des quaternions". Les propositions 2.2.11 et 2.2.17 nous permettent également d'en conclure que $\mathbb{H}$ est un anneau, nous verrons par la suite qu'il s'agit en réalité d'un corps. Pour ce faire, nous allons définir le conjugué d'un quaternion. Puisque Hamilton cherchait à avoir une propriété sur la norme, nous définissons aussi la norme d'un quaternion, qui n'est en réalité rien d'autre que la norme usuelle sur $\mathbb{R}^4$.

Définition 2.2.19. Soient a, b, c, d des réels tels que $w = a + bi + cj + dk = a + v_w$ soit un quaternion. Le conjugué de w est le quaternion

$$\begin{aligned}\overline{w} &= a - bi - cj - dk \\ &= a - v_w.\end{aligned}$$

On définit la norme de w comme le nombre réel positif ou nul tel que

$$\begin{aligned}|w|^2 &= a^2 + b^2 + c^2 + d^2 \\ &= a^2 + \langle v_w, v_w \rangle.\end{aligned}$$

Proposition 2.2.20. *Pour tout quaternion $w = a + v_w$ on a $|w|^2 = w\bar{w} = \bar{w}w$.*

Démonstration. En effet,

$$\begin{aligned}w\bar{w} &= (a + v_w)(a - v_w) \\ &= aa - \langle v_w, -v_w \rangle + av_w - av_w + v_w \wedge v_w \\ &= a^2 + \langle v_w, v_w \rangle \\ &= |w|^2.\end{aligned}$$

Et par un procédé analogue on trouve également que $\bar{w}w = |w|^2$ d'où la conclusion. □

Remarque 2.2.21. Bien que la multiplication ne soit pas commutative, il est aisé de constater qu'elle l'est malgré tout dans le cas où on effectue le produit d'un quaternion avec son conjugué.

Remarque 2.2.22. Un quaternion w est nul si et seulement si sa norme $|w|$ est nulle.

Remarque 2.2.23. Si le quaternion w s'écrit comme le couple de nombres complexes (x, y) alors le conjugué de w est le quaternion $\bar{w} = (\bar{x}, -y)$, et la norme de w est le nombre réel positif ou nul $|w|$ tel que $|w|^2 = |x|^2 + |y|^2$.

Remarquons ensuite une petite propriété intéressante du produit scalaire canonique sur $\mathbb{R}^4$.

Proposition 2.2.24. *Soient x, y deux quaternions. Le produit scalaire de x avec y est égal à la partie réelle du produit de x par le conjugué de y. En d'autres termes,*

$$\langle x, y \rangle = \Re(x\bar{y}).$$

Démonstration. Considérons deux quaternions $x = x_1 + x_2 i + x_3 j + x_4 k = x_1 + v_x$ et $y = y_1 + y_2 i + y_3 j + y_4 k = y_1 + v_y$. On a

$$\begin{aligned}\Re(x\bar{y}) &= \Re((x_1 + v_x)(y_1 - v_y)) \\ &= \Re(x_1 y_1 + \langle v_x, v_y \rangle + y_1 v_x - x_1 v_y - v_x \wedge v_y) \\ &= x_1 y_1 + \langle v_x, v_y \rangle \\ &= x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \\ &= \langle x, y \rangle,\end{aligned}$$

où la quatrième et la cinquième égalité s'explique par définition du produit scalaire canonique sur $\mathbb{R}^3$ et $\mathbb{R}^4$ respectivement, d'où la conclusion. □

Proposition 2.2.25. *L'ensemble des réels $\mathbb{R}$ et l'espace imaginaire des quaternions $Im\mathbb{H}$ sont orthogonaux.*

Démonstration. Il suffit de montrer que le produit scalaire de tout élément de $\mathbb{R}$ avec tout élément de $Im\mathbb{H}$ est nul. Considérons donc $x \in \mathbb{R}$ et $v \in Im\mathbb{H}$ tels que $x = x + 0i + 0j + 0k$ et $v = 0 + bi + cj + dk$. Par la proposition 2.2.24 on a,

$$\begin{aligned}\langle x, v\rangle &= \Re(x\bar{v}) \\ &= \Re((x + 0i + 0j + 0k)(0 - bi - cj - dk)) \\ &= 0\end{aligned}$$

où la dernière égalité se justifie par calcul du produit de deux quaternions et par définition de la partie réelle. □

Grâce à cette proposition, nous pouvons réécrire le produit mixte de quaternions imaginaires purs sous une autre forme. C'est ce que nous développons dans la proposition ci-dessous.

Proposition 2.2.26. *Pour tous $u, v, w \in Im\mathbb{H}$, le produit mixte peut se réécrire comme*

$$\langle u \wedge v, w\rangle = \langle uv, w\rangle$$

Démonstration. En effet,

$$\begin{aligned}\langle uv, w\rangle &= \langle -\langle u, v\rangle + u \wedge v, w\rangle \\ &= \langle -\langle u, v\rangle, w\rangle + \langle u \wedge v, w\rangle \\ &= -\langle\langle u, v\rangle, w\rangle + \langle u \wedge v, w\rangle \\ &= \langle u \wedge v, w\rangle\end{aligned}$$

La dernière égalité est justifiée par la proposition 2.2.25 puisque $\langle u, v\rangle$ est un élément de $\mathbb{R}$ alors que w est un quaternion imaginaire pur. □

Proposition 2.2.27. *Soit w un quaternion. La partie réelle et la partie imaginaire de w sont respectivement exprimées par*

$$\Re(w) = \frac{w + \bar{w}}{2} \qquad \textit{et} \qquad \Im(w) = \frac{w - \bar{w}}{2}.$$

Démonstration. Soit $w = w_1 + v_w$ un quaternions avec w_1 sa partie réelle et v_w sa partie vectorielle. La démonstration se fait directement par définition de la somme de deux quaternions. En effet,

$$\frac{w + \bar{w}}{2} = \frac{(w_1 + v_w) + (w_1 - v_w)}{2} = w_1 = \Re(w),$$

et

$$\frac{w - \bar{w}}{2} = \frac{(w_1 + v_w) - (w_1 - v_w)}{2} = v_w = \Im(w).$$

□

Les propositions suivantes méritent également d'être démontrées car elles seront d'une grande utilité par la suite. En particulier, nous démontrerons que le conjugué d'un produit de quaternions n'est pas le produit des conjugués comme c'était le cas pour les nombres complexes.

Proposition 2.2.28. *Soient p et q deux quaternions. Les propriétés suivantes sont vérifiées :*

1. $\overline{p+q} = \bar{p} + \bar{q}$ *;*
2. $\bar{\bar{p}} = p$ *;*
3. $\overline{pq} = \bar{q}\bar{p}$ *;*
4. $\overline{rp} = r\bar{p} \quad (r \in \mathbb{R})$*.*

Démonstration. Supposons p et q donnés sous la forme $p = a + v_p$ et $q = a' + v_q$ où a et a' sont leur partie réelle et v_p, v_q leur partie imaginaire respectives.
Montrons le premier point. Par définition de la somme de deux quaternions, on a

$$\overline{p+q} = \overline{a + v_p + a' + v_q} = \overline{(a + a') + (v_p + v_q)}.$$

Dès lors, par définition du conjugué il vient,

$$\overline{p+q} = (a + a') - (v_p + v_q) = a + a' - v_p - v_q.$$

Puisque la somme des quaternions est commutative, on a finalement

$$\overline{p+q} = a - v_p + a' - v_q = \bar{p} + \bar{q}.$$

En appliquant successivement deux fois la définition du conjugué, nous trouvons le second point de cette proposition car

$$\bar{\bar{p}} = \overline{\overline{a + v_p}} = \overline{a - v_p} = a + v_p = p.$$

Le troisième point est quant à lui quelque peu plus subtile, détaillons-le également.
Par la proposition 2.2.14, on a $pq = (a + v_p)(a' + v_q) = (aa' - \langle v_p, v_q \rangle) + (a'v_p + av_q + v_p \wedge v_q)$. Donc,

$$\begin{aligned}
\overline{pq} &= \overline{(aa' - \langle v_p, v_q \rangle) + (a'v_p + av_q + v_p \wedge v_q)} \\
&= (aa' - \langle v_p, v_q \rangle) - a'v_p - av_q + \overline{v_p \wedge v_q} \\
&= (aa' - \langle v_p, v_q \rangle) - a'v_p - av_q + v_q \wedge v_p.
\end{aligned}$$

De plus,

$$\begin{aligned}
\bar{q}\bar{p} &= (a' - v_q)(a - v_p) \\
&= (a'a - \langle v_q, v_p \rangle) - a'v_p - av_q + v_q \wedge v_p,
\end{aligned}$$

d'où l'égalité souhaitée.
Quant au dernier point, il découle directement du troisième point et du fait que le nombre r est un nombre réel. En effet,

$$\overline{rp} = \bar{r}\bar{p} = r\bar{p}.$$

□

Nous arrivons désormais à un résultat qui, sans en avoir l'air, est très important. En effet, il s'agit là d'une condition qu'Hamilton cherchait à obtenir pour son algèbre des quaternions. Ainsi, tout comme pour les nombres complexes, la norme d'un produit de quaternions est égale au produit des normes desdits quaternions. Ce résultat est également intéressant du fait qu'il nous permet de dire que l'algèbre des quaternions est en réalité une algèbre à composition au sens de la définition 3.2.9 au chapitre suivant. La forme quadratique non-dégénérée associée étant, dans le cas présent, la norme sur $\mathbb{R}^4$ définie précédemment.

Proposition 2.2.29. *Soient p et q deux quaternions. On a $|pq| = |p||q|$.*

Démonstration. En utilisant la proposition sur la norme 2.2.20 ainsi que la proposition 2.2.28 et le fait que le multiplication soit associative, on a

$$|pq|^2 = pq\overline{pq} = pq\bar{q}\bar{p} = p|q|^2\bar{p} = |q|^2|p|^2 = |p|^2|q|^2.$$

Puisque la norme d'un quaternion est définie comme étant un nombre réel positif ou nul, il vient alors $|pq| = |p||q|$. □

Nous continuons alors avec une petite propriété qui lie la norme, le produit scalaire et la norme du produit vectoriel de deux quaternions imaginaires purs.

Proposition 2.2.30. *Si v_u, v_w sont deux quaternions imaginaires purs, alors l'égalité*

$$\langle v_u, v_w\rangle^2 + |v_u \wedge v_w|^2 = |v_u|^2|v_w|^2 \tag{2.16}$$

est vérifiée.

Démonstration. En utilisant 2.7 et par définition de la norme, on a

$$\begin{aligned}
|v_u \wedge v_w|^2 &= (v_uv_w + \langle v_u, v_w\rangle)\overline{(v_uv_w + \langle v_u, v_w\rangle)} \\
&= (v_uv_w + \langle v_u, v_w\rangle)(\overline{v_w}\,\overline{v_u} + \langle v_u, v_w\rangle) \\
&= \langle v_u, v_w\rangle\langle v_u, v_w\rangle - \langle v_uv_w, \overline{v_w}\,\overline{v_u}\rangle + \langle v_u, v_w\rangle v_uv_w + \langle v_u, v_w\rangle\overline{v_w}\,\overline{v_u} + (v_uv_w) \wedge (\overline{v_w}\,\overline{v_u}) \\
&= \langle v_u, v_w\rangle^2 - \langle v_uv_w, \overline{v_uv_w}\rangle + \langle v_u, v_w\rangle(v_uv_w + \overline{v_w}\,\overline{v_u}) + (v_uv_w) \wedge \overline{v_uv_w} \\
&= \langle v_u, v_w\rangle^2 + \langle v_uv_w, v_uv_w\rangle + \langle v_u, v_w\rangle(-2\langle v_u, v_w\rangle) - (v_uv_w) \wedge (v_uv_w) \\
&= -\langle v_u, v_w\rangle^2 + |v_u|^2|v_w|^2.
\end{aligned}$$

L'avant dernière égalité étant justifiée en utilisant à nouveau 2.7 et étant donné que $\overline{v_w} = -v_w$. Quant à la dernière égalité, elle découle de la proposition 2.2.29. Ceci nous permet alors de conclure puisque nous obtenons l'expression souhaitée

$$|v_u \wedge v_w|^2 + \langle v_u, v_w\rangle^2 = |v_u|^2\ |v_w|^2.$$

□

Le résultat suivant est également très intéressant puisqu'il nous permet de dire que $\mathbb{H}$ est un corps, on parlera donc du corps des quaternions. D'après ce que nous avons fait plus haut, on sait déjà que $\mathbb{H}$ est un anneau. Dès lors, il nous reste à montrer que tout quaternion non nul est inversible, et c'est ce que nous allons faire ci-dessous.

Proposition 2.2.31. *Si p est un quaternion non nul, alors p est inversible avec $p^{-1} = \dfrac{1}{|p|^2}\bar{p}$.*

Démonstration. Par la remarque 2.2.22, puisque p est un quaternion non nul alors sa norme n'est pas nulle. De plus, la proposition 2.2.20 nous indique que $|p|^2 = p\bar{p}$ donc en divisant les deux membres par $|p|^2$ nous obtenons

$$1 = \frac{1}{|p|^2}p\bar{p} = p\frac{1}{|p|^2}\bar{p}.$$

Il en résulte que p est inversible à droite avec $\frac{1}{|p|^2}\bar{p}$. De même, par la proposition 2.2.20 on sait que $|p|^2 = \bar{p}p$. Ainsi, en appliquant le même raisonnement que celui qui vient d'être fait, nous trouvons que p est aussi inversible à gauche avec $\frac{1}{|p|^2}\bar{p}$, de sorte qu'il est inversible avec $\frac{1}{|p|^2}\bar{p}$. □

En conséquence de cette proposition, nous avons les deux résultats suivants.

Corollaire 2.2.32. *Si p est un quaternion tel que $|p| = 1$, alors p est inversible avec $p^{-1} = \bar{p}$. Si p et q sont deux quaternions non nuls, alors pq est un quaternion non nul et $(pq)^{-1} = q^{-1}p^{-1}$.*

Démonstration. Le premier résultat est immédiat par la proposition précédente. Il nous reste alors à démontrer l'autre point de ce corollaire. Etant donné que p et q sont deux quaternions non nuls, alors leur norme respective est non nulle. Dès lors, en raison de la proposition 2.2.29, la norme du produit est également non nulle et la remarque 2.2.22 permet de conclure que pq est non nul. Notons son inverse $(pq)^{-1}$. Ainsi, $pq(pq)^{-1} = 1$, et en multipliant à gauche par $q^{-1}p^{-1}$ il vient,

$$q^{-1}p^{-1}pq(pq)^{-1} = q^{-1}p^{-1},$$

ce qui est équivalent à

$$(pq)^{-1} = q^{-1}p^{-1}$$

où l'équivalence s'explique par le fait que p et q sont non nuls et sont inversibles avec p^{-1} et q^{-1} respectivement. □

2.3 L'algèbre des quaternions : introduction matricielle $\mathcal{H}$

Cette section, comme son titre l'indique, aura pour objectif de présenter une seconde fois certains résultats à propos des quaternions mais d'une autre façon, selon une vision matricielle. À cela, cette approche nous permettra de démontrer que l'algèbre Hamiltonnienne est une algèbre à division associative. Pour ce faire, certaines définitions seront rappelées mais nous supposerons que les lecteurs de ce travail ont une bonne connaissance de l'algèbre des matrices et plus particulièrement de l'ensemble des matrices de dimension 2×2 à coefficients complexes $\mathbb{C}_2^2$. Nous supposerons également que les définitions de somme et produit de deux quaternions que l'on retrouve aux propositions 2.2.9 et 2.2.12 sont connues tout comme les définitions du conjugué et de la norme d'un quaternion ainsi que les propriétés apparentées.

Définition 2.3.1. Une algèbre sur un corps commutatif $\mathbb{K}$ est une structure $(A, +, \cdot, *)$ telle que $(A, +, \cdot)$ est un espace vectoriel sur $\mathbb{K}$ muni d'une opération binaire $* : A \times A \to A$ bilinéaire. Ainsi, pour tous $x, y, z \in A$ et tous $a, b \in \mathbb{K}$, les propriétés suivantes sont vérifiées

1. $(x + y) * z = x * z + y * z$;
2. $x * (y + z) = x * y + x * z$;
3. $(a.x) * (b.y) = (ab).(x * y)$.

L'opération binaire $*$ est appelée loi de composition interne.

Définition 2.3.2. Un sous-espace B de l'algèbre A est une sous-algèbre de A si, pour tous $x, y \in B$, $x * y \in B$.

Dans la suite, nous ne noterons plus l'opération binaire $*$, elle sera sous-entendue mais aucun symbole ne sera noté.

Définition 2.3.3. Une algèbre A non réduite à $\{0\}$ est une algèbre à division si, pour tout élément a et b de A avec a non nul, les deux équations $ax = b$ et $ya = b$ admettent une et une seule solution dans A.

La proposition suivante nous fournit un critère très utile concernant les algèbres à division.

Proposition 2.3.4. *Soit A une algèbre de dimension finie. Les assertions suivantes sont équivalentes :*

1) *A est une algèbre à division ;*
2) *A est intègre.*

Démonstration. La deuxième assertion implique la première. Considérons a un élément non nul de A et l'application $f : A \to A : x \mapsto ax$. Soient $x, y \in A$ tels que $ax = ay$. On a alors $a(x - y) = 0$, et étant donné que $a \neq 0$ et que l'algèbre A est intègre, il vient directement que $x = y$ et donc l'application est injective. Ensuite, puisque f est une application linéaire injective, de A dans lui-même et que l'algèbre A est de dimension finie, alors l'application est surjective et par conséquent elle est bijective. Dès lors, toute équation du type $ax = b$ admet une unique solution.
De manière similaire, si on considère l'application $g : A \to A : y \mapsto ya$ où a est un élément non nul de A alors, par un raisonnement analogue à celui fait précédemment, cette application est, elle aussi, bijective et par conséquent toute équation de la forme $ya = b$ admet une unique solution. Ainsi, par définition, A est une algèbre de division.
La première assertion implique la seconde. Supposons que A soit une algèbre à division. Alors, par définition, pour tous $a, b \in A$ avec $a \neq 0$, les deux équations $ax = b$ et $ya = b$ admettent une unique solution. C'est donc en particulier vrai pour $b = 0$ et par conséquent les équations $ax = 0$ et $ya = 0$ admettent une unique solution. Puisque 0 est solution, parce que le produit est bilinéaire, cela permet de conclure que x (resp. y) doit être nul et que A est sans diviseur de zéro, autrement dit A est intègre. □

Dans la suite de cette section, nous travaillerons avec un ensemble de matrices de dimension 2×2 à coefficients complexes présentant une certaine forme. L'ensemble de ces matrices, noté $\mathcal{H}$ est défini dans la définition ci-après.

Définition 2.3.5. On définit l'ensemble

$$\mathcal{H} = \left\{ \begin{pmatrix} w & -z \\ \bar{z} & \bar{w} \end{pmatrix} : w, z \in \mathbb{C} \right\}$$

qui est un sous-ensemble de $\mathcal{C}$, l'ensemble des matrices 2×2 à coefficients complexes défini via

$$\mathcal{C} = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{C} \right\} = \mathbb{C}^2_2.$$

Proposition 2.3.6. *$\mathcal{H}$ est une sous-algèbre de $\mathcal{C}$ munie du produit matriciel et vue comme une algèbre sur $\mathbb{R}$.*

Démonstration. Bien entendu $\mathcal{H}$ est un sous-espace vectoriel réel, il nous reste alors à montrer que $\mathcal{H}$ est stable par le produit. Soient $a, b \in \mathcal{H}$, et $x, y, u, v \in \mathbb{C}$ tels que

$$a = \begin{pmatrix} x & -y \\ \bar{y} & \bar{x} \end{pmatrix} \quad \text{et} \quad b = \begin{pmatrix} u & -v \\ \bar{v} & \bar{u} \end{pmatrix}.$$

on a

$$ab = \begin{pmatrix} xu - y\bar{v} & -xv - y\bar{u} \\ \bar{y}u + \bar{x}\bar{v} & -\bar{y}v + \bar{x}\bar{u} \end{pmatrix} \in \mathcal{H}$$

en effet, sur le champ des complexes on a $\overline{(xu - y\bar{v})} = \overline{xu} - \overline{y\bar{v}} = \bar{x}\bar{u} - \bar{y}v$ et $\overline{(xv + y\bar{u})} = \overline{xv} + \overline{y\bar{u}} = \bar{x}\bar{v} + \bar{y}u$.
Par conséquent, $\mathcal{H}$ est une sous-algèbre sur $\mathcal{C}$. Aussi, puisque le produit matriciel est une opération interne et que pour tous $a, b, c \in \mathcal{H}$ et tous $\lambda, \mu \in \mathbb{R}$ on a

$$(a + b)c = ac + bc \quad \text{et} \quad a(b + c) = ab + ac \quad \text{et} \quad (\lambda a)(\mu b) = (\lambda\mu)(ab),$$

par définition du produit matriciel, alors $\mathcal{H}$ est une algèbre sur $\mathbb{R}$. □

Remarque 2.3.7. L'ensemble $\mathcal{H}$ n'est évidemment pas un sous-espace vectoriel complexe. En effet, le produit d'une matrice X de $\mathcal{H}$ par un élément de $\mathbb{C}$ n'est pas nécessairement un élément de $\mathcal{H}$. Considérons par exemple le produit

$$iX = i\begin{pmatrix} x & -y \\ \bar{y} & \bar{x} \end{pmatrix},$$

avec $x = x_1 + ix_2$ et $y = y_1 + iy_2$. Après calculs il vient,

$$i\begin{pmatrix} x & -y \\ \bar{y} & \bar{x} \end{pmatrix} = \begin{pmatrix} ix_1 - x_2 & -iy_1 + y_2 \\ iy_1 + y_2 & ix_1 + x_2 \end{pmatrix}. \tag{2.17}$$

Or, étant donné que $\overline{ix_1 - x_2} \neq ix_1 + x_2$ et que $iy_1 + y_2 \neq \overline{iy_1 - y_2}$, on en conclut immédiatement que la matrice iX ci-dessus ne fait pas partie de l'ensemble $\mathcal{H}$.

Proposition 2.3.8. *L'application*

$$f : \mathbb{H} \longrightarrow \mathcal{H} : (\alpha, \beta, \gamma, \delta) \longmapsto \begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix}$$

est un isomorphisme sur une algèbre réelle où les égalités suivantes sont vérifiées

$$f(1) = f(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} := \mathbb{I} \qquad f(i) = f(e_2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} := I$$

$$f(j) = f(e_3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} := J \qquad f(k) = f(e_4) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} := K$$

Démonstration. Il suffit de montrer que l'application f est un homomorphisme bijectif.
Pour l'injectivité, considérons $\alpha, \alpha', \beta, \beta', \gamma, \gamma', \delta, \delta' \in \mathbb{R}$ et supposons

$$\begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix} = \begin{pmatrix} \alpha' + \beta' i & -\gamma' - \delta' i \\ \gamma' - \delta' i & \alpha' - \beta' i \end{pmatrix}$$

Ainsi, comme par définition deux matrices sont égales si et seulement si leurs coefficients sont égaux, il s'en suit immédiatement

$$\begin{cases} \alpha & = & \alpha' \\ \beta & = & \beta' \\ \gamma & = & \gamma' \\ \delta & = & \delta'. \end{cases}$$

Et donc finalement, $(\alpha, \beta, \gamma, \delta) = (\alpha', \beta', \gamma', \delta')$.
En ce qui concerne la surjectivité, il suffit de considérer les réels $\alpha, \beta, \gamma, \delta$ tel que nous disposons de la matrice

$$\begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix}.$$

La définition de l'application nous affirme que cette matrice est l'image par f d'un élément de l'algèbre des quaternions $(\alpha, \beta, \gamma, \delta)$.
L'application f est évidemment linéaire par définition de la somme matricielle et du produit d'un réel par une matrice. Finalement, il reste à montrer que f est un homomorphisme. Pour ce faire, puisque f est linéaire et puisque les produits dans $\mathbb{H}$ et $\mathcal{H}$ sont bilinéaires, il suffit de vérifier la condition sur les vecteurs de base, c'est-à-dire qu'il nous faut montrer

$$f(e_i)f(e_j) = f(e_ie_j) \quad \forall i, j \in \{1, 2, 3, 4\}. \tag{2.18}$$

Puisque $1 = e_1$ est neutre et puisque $f(e_1)$ l'est aussi, il reste alors 9 égalités à vérifier, à savoir

$$I^2 = -\mathbb{I}, \quad J^2 = -\mathbb{I}, \quad K^2 = -\mathbb{I}$$

$$IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J$$

Ces égalités se démontrent par simple calcul matriciel. $\square$

Remarque 2.3.9. L'expression de l'application f considérée à la proposition ci-dessus rend compte du fait que les éléments de $\mathbb{H}$ sont déterminés par deux nombres complexes, à savoir $\alpha + i\beta$ et $\gamma + i\delta$.

Proposition 2.3.10. *Toute matrice*

$$A = \begin{pmatrix} x & -y \\ \bar{y} & \bar{x} \end{pmatrix} \in \mathcal{H}$$

satisfait, sur $\mathbb{R}$, *l'équation quadratique*

$$A^2 - (\operatorname{Tr} A)A + (\det A)\mathbb{I} = 0$$

où $\operatorname{Tr} A = 2\Re(x)$ *et* $\det A = |x|^2 + |y|^2$. *De plus,* $\mathcal{H}$ *est une algèbre à division associative de dimension 4.*

Démonstration. Vérifier que l'équation quadratique est satisfaite pour chaque matrice $A \in \mathcal{H}$ se fait immédiatement. En effet,

$$P(\lambda) = \lambda^2 - (\operatorname{Tr} A)\lambda + (\det A)$$

désigne le polynôme caractéristique en λ de la matrice A. De plus, par le théorème de Cayley-Hamilton, on sait que la matrice A annule son polynôme caractérique, dès lors

$$A^2 - (\operatorname{Tr} A)A + (\det A)\mathbb{I} = 0,$$

et l'équation quadratique est satisfaite.

Pour continuer, $\mathcal{H}$ est évidemment de dimension 4 puisqu'une base de cet espace est donnée par l'ensemble

$$\mathcal{B}_{\mathcal{H}} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}.$$

Ensuite, $\mathcal{H}$ est associative puisque c'est une sous-algèbre. Et ainsi, il reste à montrer que $\mathcal{H}$ est une algèbre à division. Pour ce faire, puisque $\mathcal{H}$ est une algèbre sur $\mathbb{R}$ de dimension finie, il faut s'assurer qu'elle vérifie la proposition 2.3.4.

Considérons donc deux matrices A et B de $\mathcal{H}$ quelconques et supposons que $AB = 0$. Dès lors, $\det(AB) = 0$ ou encore $(\det A).(\det B) = 0$. En raison de l'expression des matrices A et B considérées, les déterminants $\det A$ et $\det B$ sont deux nombres réels positifs. Ainsi, la condition $(\det A).(\det B) = 0$ est équivalente à la condition $\det A = 0$ ou $\det B = 0$. En faisant l'hypothèse que $\det B \neq 0$, il nous reste

$$\det A = x\bar{x} + \bar{y}y = |x|^2 + |y|^2 = 0.$$

Ceci n'étant vrai que si $x = y = 0$, il en résulte que la matrice A doit être la matrice nulle. Un développement analogue peut être fait en supposant $\det A \neq 0$ et nous en conclurons que la matrice B est la matrice nulle. Par conséquent, on en conclut que si deux matrices $A, B \in \mathcal{H}$ sont telles que $AB = 0$, alors $A = 0$ ou $B = 0$. Cela traduit le fait que $\mathcal{H}$ est intègre et donc, par la proposition 2.3.4, $\mathcal{H}$ est une algèbre à division. $\square$

Nous en arrivons donc à l'objectif principal de cette section qui consiste à démontrer que l'algèbre des quaternions est une algèbre à division.

Théoreme 2.3.11. *L'algèbre Hamiltonienne* $\mathbb{H}$ *est une algèbre à division associative.*

Démonstration. En raison de la proposition 2.3.8, $\mathbb{H}$ et $\mathcal{H}$ sont isomorphes. De plus, $\mathcal{H}$ étant une algèbre à division associative, il en est de même pour $\mathbb{H}$, ce qui conclut la preuve. $\square$

Chapitre 3

Les octonions

3.1 Introduction aux octonions

Les octonions ne sont pas aussi connus que les quaternions car ils sont moins étudiés et utilisés. Mais malgré cela, ils possèdent des propriétés intéressantes et nous pouvons les relier à de nombreuses structures exceptionnelles en mathématiques telles que les groupes de Lie exceptionnels. À cela, s'ajoute un grand nombre d'applications en relativité et en logique quantique. Les octonions ont été découverts par *John T. Graves* en 1843 qui s'inspira de la découverte des quaternions par son ami Hamilton. À l'époque, Graves les appelait octaves. Ils ont été découverts indépendamment de Graves par *Arthur Cayley* qui publia le premier article sur le sujet en 1845 à peine quelques temps avant l'article publié par Graves sur le sujet. C'est pourquoi, les octonions sont parfois appelés octaves de Cayley ou algèbre de Cayley.
Nous venons d'aborder les complexes ainsi que les quaternions, deux algèbres réelles de dimension 2 et 4 respectivement. En particulier, nous avons introduit les quaternions par leur table de multiplication. Nous allons nous atteler à faire de même pour introduire les octonions. La plupart des propos développés ici sont principalement tirés, et parfois développés différemment, de l'ouvrage de Ebbinghaus intitulé *Numbers* ainsi que du livre *On quaternions and Octonions* de Conway que l'on retrouve aux références [15] et [13].

Avant tout, spécifions que dans ce mémoire, nous utiliserons la base canonique de $\mathbb{R}^8$

$$\mathcal{B}_{\mathbb{O}} = \{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$$

pour décomposer les octonions (avec 1 l'élément neutre), et il sera sous-entendu que dans l'écriture $w = w_0+w_1e_1+w_2e_2+w_3e_3+w_4e_4+w_5e_5+w_6e_6+w_7e_7$, les coefficients $w_i (i \in \{0, ..., 7\})$ sont des réels.
Ainsi, La multiplication des éléments de la base est décrite par la table de multiplication donnée ci-dessous :

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	e_2	$-e_4$	-1	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	e_3	$-e_7$	$-e_5$	-1	e_6	e_2	$-e_4$	e_1
e_4	e_4	e_2	$-e_1$	$-e_6$	-1	e_7	e_3	$-e_5$
e_5	e_5	$-e_6$	e_3	$-e_2$	$-e_7$	-1	e_1	e_4
e_6	e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	-1	e_2
e_7	e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	-1

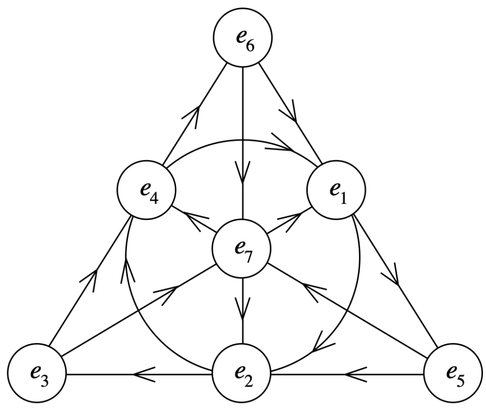
Cette table de multiplication, bien que difficile à comprendre et à retenir, nous apporte certains faits intéressants. En effet, elle nous dit que 1 est l'élément neutre pour la multiplication sur $\mathbb{O}$, mais aussi que $e_l^2 = -1,\ \forall l \in \{1, ..., 7\}$ et encore, que $e_l e_m = -e_m e_l,\ \forall l, m \in \{1, ..., 7\}(l \neq m)$, autrement dit que e_l et e_m anticommutent lorsque l et m sont différents. De plus, on constate que les indices suivent un certain cycle. En effet,

$$\text{si } e_l e_m = e_n \quad \text{alors} \quad e_{l+1} e_{m+i} = e_{n+1} \quad \text{mod } 7,$$

et

$$\text{si } e_l e_m = e_n \quad \text{alors} \quad e_{2l} e_{2m} = e_{2n}.$$

Ainsi, en considérant l'unique produit un peu particulier $e_1 e_2 = e_4$ ainsi que toutes ces constatations, nous pouvons sans problème aucun reconstruire la table ci-dessus. Toutefois, il existe un moyen plus aisé pour retenir les lois de multiplication de deux éléments de la base des octonions. Ce moyen mnémotechnique est représenté par la figure ci-dessous appelée plan de Fano.



La plan de Fano est en réalité un cercle inscrit dans un triangle équilatéral. Chacun des trois côtés du triangle constitue un triplet (e_l, e_m, e_n) pour $l, m, n \in \{1, ..., 6\}$ de même que les trois hauteurs issues des trois sommets du triangle ainsi que le cercle inscrit passant par les pieds des trois hauteurs. Les triplets sur chacun des côtés du triangle ont le même sens. Ils peuvent être lus soit dans le sens horloger, soit dans le sens anti-horloger. Il en est de même pour le triplet situé sur le cercle. Et enfin, les triplets situés sur les trois hauteurs du triangle doivent être lus dans le même sens eux aussi. De bas en haut ou de haut en bas. Afin de guider le sens de lecture, des flèches sont apposées sur les segments de droite et sur le cercle. Soit (e_l, e_m, e_n) un triplet ordonné de point situés sur un des cotés du triangle, sur une des hauteurs ou sur le cercle avec l'ordre donné par la direction de la flèche. La multiplication se lit comme

$$e_l e_m = e_n \quad \text{et} \quad e_m e_l = -e_n,$$

avec des permutations circulaires qui conservent l'ordre des points

$$e_m e_n = e_l \quad \text{et} \quad e_n e_m = -e_l, \qquad e_n e_l = e_m \quad \text{et} \quad e_l e_n = -e_m.$$

Ainsi, nous avons par exemple $e_7 e_4 = e_5$ tandis que $e_6 e_5 = -e_1$ ce qui coïncide bien avec ce nous trouvons dans la table de multiplication. Des informations complémentaires sur le plan de Fano se trouvent dans l'article intitulé *The Eight Cayley-Dickson Doubling Products* [8].

Nous avons jusqu'alors parlé des octonions sans réellement les définir, en voici une définition.

Définition 3.1.1. L'ensemble des octonions est l'ensemble

$$\mathbb{O} = \{x = x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 + x_4 e_4 + x_5 e_5 + x_6 e_6 + x_7 e_7 | x_i \in \mathbb{R} \quad \forall i \in \{0, ..., 7\}\}.$$

Toutefois, il est assez courant dans la littérature de voir les octonions exprimés sous forme d'un couple de quaternions. Il est en effet parfois plus commode de travailler sous cette écriture puisqu'elle est plus compacte et qu'elle fait appel à la théorie des quaternions que nous connaissons désormais. En particulier, cette nouvelle écriture impose de renommer les éléments de la base en vue de les utiliser plus adéquatement. Ainsi, nous noterons

$$\begin{aligned} &1=(1,0), \quad e_1=(i,0), \quad e_2=(j,0), \quad e_4=(k,0), \\ &e_3=(0,1), \quad e_7=(0,i), \quad e_5=(0,j), \quad e_6=(0,-k). \end{aligned}$$

Cela étant, en définissant la somme de deux couples comme la somme composante à composante et le produit d'un couple par un scalaire comme le produit de chaque composante par ce scalaire, nous pouvons réécrire un octonion $x = a_0 1 + a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 + a_5 e_5 + a_6 e_6 + a_7 e_7$ sous la forme

$$\begin{aligned} x &= a_0(1,0) + a_1(i,0) + a_2(j,0) + a_3(0,1) + a_4(k,0) + a_5(0,j) + a_6(0,-k) + a_7(0,i) \\ &= (a_0 + a_1 i + a_2 j + a_4 k, a_3 + a_7 i + a_5 j - a_6 k) \\ &= (x_1, x_2) \end{aligned}$$

où $x_1 = a_0 + a_1 i + a_2 j + a_4 k$ et $x_2 = a_3 + a_7 i + a_5 j - a_6 k$ sont deux quaternions.
Ceci nous amène à la définition suivante.

Définition 3.1.2. En tant que $\mathbb{R}$-vectoriel, on définit $\mathbb{O}$ comme $\mathbb{O} = \mathbb{R}^4 \oplus \mathbb{R}^4$.

Les définitions qui suivent vont être exprimées sur base de cette deuxième définition. Bien entendu, elles peuvent se traduire en utilisant la première définition et les résultats s'y attenant seront équivalents.
Dans les définitions et propositions suivantes tout octonion x (resp. y, z) s'écrit comme un couple (x_1, x_2) (resp. (y_1, y_2) , (z_1, z_2)) avec $x_1, x_2 \in \mathbb{H}$ (resp. $y_1, y_2, z_1, z_2 \in \mathbb{H}$).

Définition 3.1.3. Soient $x = (x_1, x_2)$ et $y = (y_1, y_2)$ deux octonions. On a l'égalité des deux octonions si et seulement si on a l'égalité des quaternions respectifs. Autrement dit,

$$x = y \Leftrightarrow x_1 = y_1 \text{ et } x_2 = y_2.$$

Définition 3.1.4. Soient $x = (x_1, x_2)$ et $y = (y_1, y_2)$ deux octonions. La somme de x et de y est l'octonion $x + y$ défini par l'expression

$$x + y = (x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2).$$

Proposition 3.1.5. *L'addition possède les propriétés suivantes :*

1. *Elle est associative : pour tous* $x, y, z \in \mathbb{O}, (x + y) + z = x + (y + z)$ *;*
2. *Elle est commutative : pour tous* $x, y \in \mathbb{O}, x + y = y + x$ *;*
3. *Il existe un neutre* $0 = (0, 0)$ *: pour tout* $x \in \mathbb{O}, x + 0 = x = 0 + x$ *;*
4. *Tout élément* $x = (x_1, x_2)$ *admet un opposé noté* $-x$ *tel que* $-x = (-x_1, -x_2)$.

Démonstration. Considérons $x = (x_1, x_2), y = (y_1, y_2), z = (z_1, z_2)$ trois octonions. La démonstration des quatre points de cette proposition se fait immédiatement en se ramenant aux propriétés correspondantes pour les quaternions. □

Définition 3.1.6. Soient $x = (x_1, x_2)$ et $y = (y_1, y_2)$ deux octonions. Le produit de x par y est l'octonion xy défini par l'expression

$$xy = (x_1, x_2)(y_1, y_2) = (x_1 y_1 - \overline{y_2} x_2, x_2 \overline{y_1} + y_2 x_1)$$

où $\overline{y_1}$ et $\overline{y_2}$ désignent le conjugué des quaternions y_1 et y_2 respectivement.

Proposition 3.1.7. *La multiplication possède les propriétés suivantes :*

1) *Elle n'est ni associative ni commutative ;*
2) *Il existe un neutre* $1 = (1, 0)$ *: pour tout* $x \in \mathbb{O}, x\,1 = x = 1\,x$*,*
3) *Elle distribue l'addition : pour tous* $x, y, z \in \mathbb{O}, x(y + z) = xy + xz$*.*

Démonstration. Soit $x = (x_1, x_2), y = (y_1, y_2), z = (z_1, z_2) \in \mathbb{O}$.
La propriété 2) résulte d'un calcul simple en appliquant la définition. En effet,

$$1\,x = (1, 0)(x_1, x_2) = (1\,x_1 - \overline{x_2}\,0, 0\,\overline{x_1} + x_2\,1) = (x_1, x_2) = x.$$

Il en est de même pour montrer que $x\,1 = x$.
Afin de montrer que la multiplication n'est ni commutative, ni associative, considérons l'exemple où $x = (i, j), y = (1, k)$ et $z = (-k, 0)$. Nous avons d'une part

$$xy = (i\,1 - \bar{k}j, j\bar{1} + ki) = (i - i, j + j) = (0, 2j),$$

et d'autre part,

$$yx = (1i - \bar{j}k, k\bar{i} + j\,1) = (i + i, -j + j) = (2i, 0).$$

Par conséquent, $xy \neq yx$ et donc la multiplication n'est pas commutative. Ensuite, en appliquant deux fois la définition du produit de deux octonions, il vient d'une part

$$(xy)z = (0, 2j)(-k, 0) = (0(-k) - \bar{0}\,2j, 2j\,\overline{(-k)} + 0) = (0, 2i),$$

et, en tenant compte du fait que $yz = (1, k)(-k, 0) = (-k, -1)$, on a d'autre part

$$x(yz) = (i, j)(-k, -1) = (i(-k) - \overline{(-1)}\,j, j\,\overline{(-k)} + (-1)i) = (2j, 0).$$

On en conclut que $(xy)z \neq x(yz)$. En d'autres mots, la multiplication définie sur $\mathbb{O}$ n'est pas associative.
La démonstration du dernier point de l'énoncé se fait simplement en appliquant la définition de la somme et du produit de deux octonions. De fait, on a

$$\begin{aligned}
x(y + z) &= (x_1, x_2)(y_1 + z_1, y_2 + z_2) \\
&= (x_1(y_1 + z_1) - (\overline{y_2 + z_2})x_2\,,\ x_2(\overline{y_1 + z_1}) + (y_2 + z_2)x_1) \\
&= (x_1y_1 + x_1z_1 - \overline{y_2}x_2 - \overline{z_2}x_2\,,\ x_2\overline{y_1} + x_2\overline{z_1} + y_2x_1 + z_2x_1) \\
&= (x_1y_1 - \overline{y_2}x_2\,,\ x_2\overline{y_1} + y_2x_1) + (x_1z_1 - \overline{z_2}x_2\,,\ x_2\overline{z_1} + z_2x_1) \\
&= xy + xz.
\end{aligned}$$

□

La plupart des résultats valables pour les quaternions sont encore vérifiés pour les octonions. En effet, effectuer des calculs sur l'algèbre des octonions est équivalent à se ramener à des calculs, certes plus complexes, sur l'algèbre des quaternions étant donné la définition donnée en 3.1.2. Ainsi, nous pouvons définir, dans un premier temps, le conjugué d'un octonion et nous pouvons démontrer les propriétés associées. De plus, il est bon de remarquer que la définition du conjugué d'un octonion donnée ci-dessous fait écho à la remarque 2.2.23 où le conjugué d'un quaternion, écrit sous la forme d'un couple de nombres complexes, était défini.

Définition 3.1.8. Soit $x = (x_1, x_2)$ un octonion. Le conjugué de x est l'octonion

$$\bar{x} = (\overline{x_1}, -x_2).$$

Proposition 3.1.9. *Pour tous $x, y \in \mathbb{O}$ tels que $x = (x_1, x_2)$ et $y = (y_1, y_2)$, on a*

1) $\overline{x+y} = \bar{x} + \bar{y}$;
2) $\overline{xy} = \bar{y}\bar{x}$;
3) $\bar{\bar{x}} = x$;
4) $\overline{\alpha x} = \alpha \bar{x}, \alpha \in \mathbb{R}$.

Démonstration. Montrons le premier résultat. On a

$$\overline{x+y} = \overline{(x_1+y_1, x_2+y_2)} = (\overline{x_1+y_1}, -(x_2+y_2)) = (\overline{x_1}+\overline{y_1}, -x_2-y_2) = (\overline{x_1}, -x_2)+(\overline{y_1}, -y_2) = \bar{x}+\bar{y},$$

où la troisième égalité vient du fait que la propriété correspondante est vérifiée sur l'algèbre des quaternions. Pour le second résultat, notons tout d'abord que $\bar{x} = (\overline{x_1}, -x_2)$ et $\bar{y} = (\overline{y_1}, -y_2)$. D'une part, on a

$$\begin{aligned}
\bar{y}\bar{x} &= (\overline{y_1}, -y_2)(\overline{x_1}, -x_2) \\
&= (\overline{y_1}\,\overline{x_1} - (\overline{-x_2})(-y_2), -y_2\,\overline{\overline{x_1}} + (-x_2)\,\overline{y_1}) \\
&= (\overline{y_1}\,\overline{x_1} + (\overline{-x_2})y_2, -y_2\,x_1 - x_2\,\overline{y_1}) \\
&= (\overline{y_1}\,\overline{x_1} - \overline{x_2}\,y_2, -y_2\,x_1 - x_2\,\overline{y_1}).
\end{aligned}$$

Et d'autre part, nous avons

$$\begin{aligned}
\overline{xy} &= \overline{(x_1, x_2)(y_1, y_2)} \\
&= \overline{(x_1y_1 - \overline{y_2}x_2, x_2\overline{y_1} + y_2x_1)} \\
&= (\overline{x_1y_1 - \overline{y_2}x_2}, -(x_2\overline{y_1} + y_2x_1)) \\
&= (\overline{x_1y_1} - \overline{\overline{y_2}x_2}, -x_2\overline{y_1} - y_2x_1) \\
&= (\overline{y_1}\ \overline{x_1} - \overline{x_2}\ \overline{\overline{y_2}}, -x_2\overline{y_1} - y_2x_1) \\
&= (\overline{y_1}\ \overline{x_1} - \overline{x_2}y_2, -x_2\overline{y_1} - y_2x_1)
\end{aligned}$$

L'égalité $\overline{xy} = \bar{y}\bar{x}$ apparaît alors directement.
En ce qui concerne la démonstration du troisième résultat, on a directement

$$\bar{\bar{x}} = \overline{(\overline{x_1}, -x_2)} = (\overline{\overline{x_1}}, -(-x_2)) = (x_1, x_2),$$

puisque la propriété correspondante est vérifiée pour tout quaternion. Finalement, montrons le quatrième et dernier résultat de cette proposition. Pour tout nombre réel α on a successivement

$$\overline{\alpha x} = \overline{(\alpha x_1, \alpha x_2)} = (\overline{\alpha x_1}, -\alpha x_2) = (\alpha\overline{x_1}, -\alpha x_2) = \alpha(\overline{x_1}, -x_2) = \alpha\bar{x},$$

ce qui conclut la preuve. □

Proposition 3.1.10. *L'ensemble des octonions muni de l'addition et de la multiplication définies aux propositions 3.1.4 et 3.1.6 forme une algèbre sur $\mathbb{R}$.*

Démonstration. Nous avons déjà montré, à la proposition 3.1.7, que la multiplication distribue l'addition. Aussi, par définition, la multiplication sur $\mathbb{O}$ est une application interne. Ainsi, il nous reste montrer que pour tous $a, b \in \mathbb{R}$ et tous $x, y \in \mathbb{O}$ on a

$$(ax)(by) = (ab)(xy).$$

Autrement dit, montrons que tout nombre réel commute avec tout octonion. Tout d'abord, on a

$$ax = a(x_1, x_2) = (ax_1, ax_2) \quad \text{et} \quad by = b(y_1, y_2) = (by_1, by_2).$$

Dès lors,

$$\begin{aligned}(ax)(by) &= (ax_1by_1 - \overline{by_2}ax_2\,, ax_2\overline{by_1} + by_2ax_1)\\ &= (ax_1by_1 - b\overline{y_2}ax_2\,, ax_2b\overline{y_1} + by_2ax_1)\\ &= (abx_1y_1 - ab\overline{y_2}x_2\,, abx_2\overline{y_1} + aby_2x_1)\\ &= ab(x_1y_1 - \overline{y_2}x_2\,, x_2\overline{y_1} + y_2x_1)\\ &= ab(xy),\end{aligned}$$

ce que nous voulions, d'où la conclusion. □

Nous passons désormais à une autre définition très importante, la norme d'un octonion.

Définition 3.1.11. La norme de l'octonion $x = (x_1, x_2)$ est le nombre définit par

$$|x|^2 = |x_1|^2 + |x_2|^2.$$

Remarque 3.1.12. Dans la définition ci-dessus, la norme des quaternions x_1 et x_2 fait référence à la norme euclidienne sur $\mathbb{R}^4$, i.e. la norme définie par $|q|^2 = \langle q, q\rangle$ pour tout $q \in \mathbb{R}^4$, où le produit scalaire est le produit scalaire usuel sur $\mathbb{R}^4$ et où on a supposé que la base canonique de $\mathbb{R}^4$ était orthonormée positive.

Remarque 3.1.13. La norme d'un octonion est toujours un nombre réel positif puisque par définition c'est la somme de deux nombres réels positifs. En particulier, la norme d'un octonion est nulle si et seulement l'octonion est nul. Autrement dit, $|x| = 0 \Leftrightarrow x = 0$.

Proposition 3.1.14. *Soit $x = (x_1, x_2)$ un octonion. On a $|x|^2 = x\bar{x} = \bar{x}x$.*

Démonstration. En effet, il suffit de développer le produit de x avec son conjugué pour avoir

$$\begin{aligned}x\bar{x} &= (x_1, x_2)(\overline{x_1}, -x_2)\\ &= (x_1\overline{x_1} - (\overline{-x_2})x_2, x_2\overline{\overline{x_1}} + (-x_2)x_1)\\ &= (x_1\overline{x_1} + \overline{x_2}x_2, x_2x_1 - x_2x_1)\\ &= (|x_1|^2 + |x_2|^2, 0)\\ &= |x_1|^2 + |x_2|^2,\end{aligned}$$

où la dernière égalité vient du fait que l'on a identifié le couple $(1, 0)$ au premier élément de la base $\mathcal{B}_{\mathbb{O}}$ noté 1 qui est le neutre pour la multiplication. De même, le produit $\bar{x}x$ s'écrit comme

$$\begin{aligned}\bar{x}x &= (\overline{x_1}, -x_2)(x_1, x_2)\\ &= (\overline{x_1}x_1 - \overline{x_2}(-x_2), -x_2\overline{x_1} + x_2\overline{x_1})\\ &= (|x_1|^2 + |x_2|^2, 0)\\ &= |x_1|^2 + |x_2|^2,\end{aligned}$$

d'où la conclusion. □

Venons-en à un résultat qui fait écho au résultat espéré par Hamilton pour les quaternions, à savoir le fait que la norme d'un produit soit égale au produit des normes. Rappelons que pour le cas de l'algèbre des quaternions $\mathbb{H}$, nous l'avions démontré en utilisant l'associativité de la multiplication. Ici, il n'en est rien puisqu'en doublant la dimension de l'algèbre nous avons perdu cette propriété. Nous allons donc devoir procéder de façon différente dans la proposition suivante. Par ailleurs, nous supposerons que le lecteur/la lectrice de ce travail connait les propriétés associées à la norme euclidienne et au produit scalaire usuel définis sur $\mathbb{R}^4$.

Proposition 3.1.15. *Pour tous $x, y \in \mathbb{O}$, on a $|xy| = |x||y|$.*

Démonstration. Considérons deux quelconques octonions x et y définis par $x = (x_1, x_2)$ et $y = (y_1, y_2)$. En utilisant la définition de la norme d'un octonion 3.1.11, le carré du membre de droite de l'égalité souhaitée s'écrit sous la forme

$$|x|^2|y|^2 = (|x_1|^2 + |x_2|^2)(|y_1|^2 + |y_2|^2).$$

Aussi, après avoir calculé le produit xy, et en utilisant cette même définition 3.1.11, le carré du membre de gauche s'écrit

$$|xy|^2 = |x_1y_1 - \overline{y_2}x_2|^2 + |x_2\overline{y_1} + y_2x_1|^2.$$

Dès lors, nous devons montrer l'égalité

$$|x_1y_1 - \overline{y_2}x_2|^2 + |x_2\overline{y_1} + y_2x_1|^2 = (|x_1|^2 + |x_2|^2)(|y_1|^2 + |y_2|^2). \tag{3.1}$$

D'une part on a,

$$\begin{aligned}
|x_1y_1 - \overline{y_2}x_2|^2 + |x_2\overline{y_1} + y_2x_1|^2 &= \langle x_1y_1 - \overline{y_2}x_2, x_1y_1 - \overline{y_2}x_2\rangle + \langle x_2\overline{y_1} + y_2x_1, x_2\overline{y_1} + y_2x_1\rangle \\
&= |x_1y_1|^2 - 2\langle x_1y_1, \overline{y_2}x_2\rangle + |\overline{y_2}x_2|^2 + |x_2\overline{y_1}|^2 + 2\langle x_2\overline{y_1}, y_2x_1\rangle \\
&\quad + |y_2x_1|^2 \\
&= |x_1|^2|y_1|^2 - 2\langle x_1y_1, \overline{y_2}x_2\rangle + |y_2|^2|x_2|^2 + |x_2|^2|y_1|^2 \\
&\quad + 2\langle y_2x_1, x_2\overline{y_1}\rangle + |y_2|^2|x_1|^2,
\end{aligned}$$

puisque la propriété correspondante est vérifiée sur l'algèbre des quaternions $\mathbb{H}$ et étant donné que $|\bar{q}| = |q|$ pour tout quaternion q. Et d'autre part nous avons,

$$(|x_1|^2 + |x_2|^2)(|y_1|^2 + |y_2|^2) = |x_1|^2|y_1|^2 + |x_1|^2|y_2|^2 + |x_2|^2|y_1|^2 + |x_2|^2|y_2|^2.$$

Par conséquent, afin de montrer l'égalité 3.1, il suffit de montrer que

$$2\langle x_1y_1, \overline{y_2}x_2\rangle = 2\langle y_2x_1, x_2\overline{y_1}\rangle.$$

Puisque l'algèbre des octonions n'est pas de caractéristique égale à 2, cela revient à devoir montrer que

$$\langle x_1y_1, \overline{y_2}x_2\rangle = \langle y_2x_1, x_2\overline{y_1}\rangle.$$

Or, en utilisant la proposition 2.2.24 nous avons

$$\langle y_2x_1, x_2\overline{y_1}\rangle = \Re(y_2x_1\overline{x_2\overline{y_1}}) = \Re(y_2x_1y_1\overline{x_2}).$$

Par cette même proposition nous avons également

$$\langle x_1y_1, \overline{y_2}x_2\rangle = \Re(x_1y_1\overline{\overline{y_2}x_2}) = \Re(x_1y_1\overline{x_2}y_2).$$

Cependant, pour tous quaternions a et b, la partie réelle du produit ab est identique à la partie réelle du produit ba. Dans le cas présent il vient alors

$$\Re(x_1y_1\overline{x_2}y_2) = \Re(y_2x_1y_1\overline{x_2}),$$

d'où la conclusion. $\square$

Cette proposition nous permet d'en conclure que l'algèbre des octonions est une algèbre à composition, la définition d'une telle algèbre est donnée à la section suivante par la définition 3.2.9. La norme sur $\mathbb{O}$ est la forme quadratique non-dégénérée à considérer. De plus, comme nous le verrons plus tard, le théorème d'Hurwitz nous indique qu'il n'existe pas d'algèbre à composition de plus grande dimension.
Après avoir défini et montré différentes propriétés concernant le conjugué et la norme d'un octonion, nous continuons avec la notion d'inverse. Grâce à cette dernière nous serons en mesure de montrer que l'algèbre des octonions est également une algèbre à division.

Définition 3.1.16. Tout élément $x = (x_1, x_2) \in \mathbb{O} \setminus \{(0,0)\}$ admet un inverse, noté x^{-1}, satisfaisant $xx^{-1} = x^{-1}x = 1$.

Proposition 3.1.17. *Tout octonion non nul x admet un inverse dont l'expression est donnée par*

$$x^{-1} = \frac{\bar{x}}{|x|^2}.$$

Démonstration. La démonstration est semblable à celle faite pour le cas des quaternions, détaillons-la tout de même en quelques lignes.
Par définition, x admet un inverse noté x^{-1}. De plus, par la proposition 3.1.14 on sait que pour tout $x \in \mathbb{O}$, $x\bar{x} = \bar{x}x = |x|^2$. Puisque $x \neq 0$, alors $|x| \neq 0$ et dès lors diviser par $|x|^2$ a du sens. Ainsi, puisque tout nombre réel commute avec tout octonion ($\mathbb{O}$ est une algèbre), alors en divisant chacun des membres des deux équations

$$x\bar{x} = 1 \quad \text{et} \quad \bar{x}x = 1$$

par $|x|^2$ on peut montrer que x est inversible à droite et gauche respectivement par $\frac{\bar{x}}{|x|^2}$. On pose alors $x^{-1} = \frac{\bar{x}}{|x|^2}$. □

Comme nous venons de définir un inverse pour tout octonion non nul, une question légitime serait de se demander si ce dernier est unique. Et effectivement, c'est bel et bien le cas. Ainsi, nous allons montrer que, tout comme pour les nombres complexes et les quaternions, si un octonion possède un inverse, celui-ci est unique. Toutefois, nous ne pouvons désormais plus utiliser l'associativité pour la multiplication comme nous l'avions fait sur $\mathbb{H}$. C'est pourquoi, nous allons établir un résultat intermédiaire qui spécifie que l'associativité est toujours de mise dans certains cas particuliers. Ce lemme technique est énoncé et démontré ci-dessous.

Lemme 3.1.18. *Soit $x = (x_1, x_2) \in \mathbb{O} \setminus (0,0)$ et x^{-1} son inverse. Pour tout $y = (y_1, y_2) \in \mathbb{O}$, on a*

$$(yx)x^{-1} = y \quad \text{et} \quad x^{-1}(xy) = y.$$

Démonstration. Tout d'abord, par la proposition précédente et puisque $\mathbb{O}$ est une algèbre, on sait que

$$x^{-1} = \frac{\bar{x}}{|x|^2} = (\overline{x_1}, -x_2)\frac{1}{|x|^2}.$$

Dès lors, il nous suffit de calculer le produit $(yx)x^{-1}$. Ainsi, il vient

$$\begin{aligned}
(yx)x^{-1} &= (y_1x_1 - \overline{x_2}y_2, y_2\overline{x_1} + x_2y_1)(\overline{x_1}, -x_2)\frac{1}{|x|^2} \\
&= ((y_1x_1 - \overline{x_2}y_2)\overline{x_1} - (\overline{-x_2})(y_2\overline{x_1} + x_2y_1), (y_2\overline{x_1} + x_2y_1)\overline{\overline{x_1}} - x_2(y_1x_1 - \overline{x_2}y_2))\frac{1}{|x|^2} \\
&= (y_1x_1\overline{x_1} - \overline{x_2}y_2\overline{x_1} + \overline{x_2}y_2\overline{x_1} + \overline{x_2}x_2y_1, y_2\overline{x_1}x_1 + x_2y_1x_1 - x_2y_1x_1 + x_2\overline{x_2}y_2)\frac{1}{|x|^2} \\
&= (y_1|x_1|^2 + |x_2|^2y_1, y_2|x_1|^2 + |x_2|^2y_2)\frac{1}{|x|^2} \\
&= ((|x_1|^2 + |x_2|^2)y_1, (|x_1|^2 + |x_2|^2)y_2)\frac{1}{|x|^2} \\
&= (|x_1|^2 + |x_2|^2)(y_1, y_2)\frac{1}{|x|^2} \\
&= y.
\end{aligned}$$

De façon analogue, en considérant également la proposition 3.1.9 nous avons

$$\begin{aligned}
x^{-1}(xy) &= \frac{1}{|x|^2}(\overline{x_1}, -x_2)(x_1y_1 - \overline{y_2}x_2, x_2\overline{y_1} + y_2x_1) \\
&= \frac{1}{|x|^2}(\overline{x_1}(x_1y_1 - \overline{y_2}x_2) - (\overline{x_2\overline{y_1} + y_2x_1})(-x_2), -x_2(\overline{x_1y_1 - \overline{y_2}x_2}) + (x_2\overline{y_1} + y_2x_1)\overline{x_1}) \\
&= \frac{1}{|x|^2}(|x_1|^2y_1 - \overline{x_1}\,\overline{y_2}x_2 + y_1|x_2|^2 + \overline{x_1}\,\overline{y_2}x_2, -x_2\overline{y_1}\,\overline{x_1} + |x_2|^2y_2 + x_2\overline{y_1}\,\overline{x_1} + y_2|x_1|^2) \\
&= \frac{1}{|x|^2}((|x_1|^2 + |x_2|^2)y_1, (|x_1|^2 + |x_2|^2)y_2) \\
&= \frac{1}{|x|^2}(|x_1|^2 + |x_2|^2)(y_1, y_2) \\
&= y.
\end{aligned}$$

□

Proposition 3.1.19. *Si x est un octonion non nul, alors il admet un inverse et celui-ci est unique.*

Démonstration. Procédons par l'absurde. Considérons $x \in \mathbb{O}$ et supposons qu'il admette deux inverses $y, z \in \mathbb{O}$. Par la proposition précédente, puisque z est inverse de x, on a

$$(yx)z = y.$$

Or, y est également inverse de x, dès lors on a

$$(yx)z = 1z = z.$$

En conclusion, on a $y = z$ d'où l'unicité de l'inverse. □

Nous pouvons alors naturellement démontrer le résultat suivant.

Proposition 3.1.20. *L'algèbre des octonions $\mathbb{O}$ est une algèbre à division.*

Démonstration. Par la proposition 2.3.4, montrer que $\mathbb{O}$ est une algèbre à division est équivalent à montrer qu'elle est intègre. C'est ce que nous allons faire. Soient $x = (x_1, x_2), y = (y_1, y_2)$ deux octonions. Montrons que si le produit de x par y est nul alors cela implique que x ou y est nul. Ainsi, en utilisant la définition 3.1.6 nous avons

$$\begin{aligned} xy = 0 &\Leftrightarrow (x_1, x_2)(y_1, y_2) = (0, 0) \\ &\Leftrightarrow (x_1 y_1 - \overline{y_2} x_2, x_2 \overline{y_1} + y_2 x_1) = (0, 0), \end{aligned}$$

ce qui est équivalent, par la définition 3.1.3, au système ci-dessous

$$\left\{ \begin{array}{lcl} x_1 y_1 - \overline{y_2} x_2 & = & 0 \\ x_2 \overline{y_1} + y_2 x_1 & = & 0. \end{array} \right. \tag{3.2}$$

Supposons désormais que $x = (x_1, x_2)$ n'est pas l'octonion nul. Il nous faut donc montrer que $y = (y_1, y_2)$ est nul, autrement dit que $y_1 = y_2 = 0$. Dès lors, trois cas possibles s'offrent à nous. Premier cas, si $x_1 \neq 0$ et $x_2 = 0$. Dans ce cas, le système ci-dessus se réécrit de la façon suivante :

$$\left\{ \begin{array}{lcl} x_1 y_1 & = & 0 \\ y_2 x_1 & = & 0 \end{array} \right. \quad \Leftrightarrow \quad \left\{ \begin{array}{lcl} y_1 & = & 0 \\ y_2 & = & 0 \end{array} \right.$$

où l'équivalence vient bien entendu du fait que x_1 est non nul et que l'algèbre $\mathbb{H}$ est une algèbre à division, donc intègre.
Le second cas est du même ordre. Si $x_2 \neq 0$ et $x_1 = 0$, alors dans ce cas, le système se réécrit comme

$$\left\{ \begin{array}{rcl} -\overline{y_2} x_2 & = & 0 \\ x_2 \overline{y_1} & = & 0 \end{array} \right. \quad \Leftrightarrow \quad \left\{ \begin{array}{lcl} \overline{y_2} & = & 0 \\ \overline{y_1} & = & 0 \end{array} \right. \quad \Leftrightarrow \quad \left\{ \begin{array}{lcl} y_2 & = & 0 \\ y_1 & = & 0 \end{array} \right.$$

où nous avons à nouveau utilisé le fait que $\mathbb{H}$ soit une algèbre à division.
La dernière possibilité correspond au cas où l'on suppose x_1 et x_2 non nuls. Dans le cas présent, le système considéré est inchangé. Avant tout, remarquons que puisque x_1 est non nul, il possède un inverse noté x^{-1}. Par conséquent, le système 3.2 est équivalent au système

$$\left\{ \begin{array}{l} y_1 = x_1^{-1} \overline{y_2} x_2 \qquad (3.3) \\ x_2 \overline{y_1} + y_2 x_1 = 0 \qquad (3.4) \end{array} \right.$$

Or, il est à souligner que la proposition 2.2.31 nous permet de réécrire x_1^{-1} comme

$$x_1^{-1} = \frac{\overline{x_1}}{|x_1|^2}$$

Ensuite, il nous est possible de donner l'expression du conjugué de y_1 en procédant successivement comme suit

$$\overline{y_1} = \overline{\frac{\overline{x_1}}{|x_1|^2} (\overline{y_2} x_2)} = \overline{\overline{y_2} x_2} \, \overline{\frac{\overline{x_1}}{|x_1|^2}} = \overline{\overline{y_2} x_2} \, \frac{\overline{\overline{x_1}}}{|x_1|^2} = \overline{x_2} y_2 \frac{x_1}{|x_1|^2}.$$

En effet, nous avons utilisé le dernier point de la proposition 2.2.28 pour justifier la troisième égalité en utilisant le fait que $|x_1|^2$ est un nombre réel, et nous justifions les égalités deux et quatre par les deuxième et troisième points de cette même proposition 2.2.28. De là, l'équation 3.4 se réécrit

$$|x_2|^2 y_2 x_1 \frac{1}{|x_1|^2} + y_2 x_1 = 0.$$

En mettant tous les termes de cette équation au même dénominateur puis en simplifiant, il vient directement

$$|x_2|^2 y_2 x_1 + |x_1|^2 y_2 x_1 = 0.$$

Ainsi, il s'en suit les équivalences suivantes :

$$\begin{aligned}
& |x_2|^2 y_2 x_1 + |x_1|^2 y_2 x_1 = 0 \\
\Leftrightarrow\ & (|x_2|^2 + |x_1|^2) y_2 x_1 = 0 \\
\Leftrightarrow\ & y_2\, x_1 = 0 \\
\Leftrightarrow\ & y_2 = 0
\end{aligned}$$

En effet, la première équivalence a lieu par définition même d'une algèbre qui est en particulier un espace vectoriel. Comme $|x_2|^2 + |x_1|^2$ est un réel non nul, il possède un inverse. Et enfin, la troisième et dernière équivalence se justifie par le fait que $\mathbb{H}$ soit une algèbre à division et que x_1 soit non nul.
Pour finir, si on insère le résultat obtenu dans l'équation 3.3, on trouve immédiatement $y_1 = 0$. Finalement, nous obtenons le résultat escompté

$$y = (y_1, y_2) = (0, 0),$$

il en résulte alors que l'algèbre $\mathbb{O}$ est une algèbre à division. $\square$

Comme nous l'avons montré précédemment, la multiplication sur $\mathbb{O}$ n'est ni commutative, ni associative. Nous avons donc perdu la propriété d'associativité en passant de l'algèbre des quaternions à l'algèbre des octonions. Toutefois, nous allons démontrer dans la proposition ci-dessous qu'elle possède une propriété un peu plus faible que l'associativité : l'alternativité. [1]

Définition 3.1.21. Une algèbre A est alternative à droite (resp. à gauche) si la multiplication définie sur cette algèbre est alternative à droite (resp. à gauche). Et, la multiplication est

1. alternative à droite si pour tous $x, y \in A$, on a $(yx)x = y(xx)$,
2. alternative à gauche si pour tous $x, y \in A$, on a $(xx)y = x(xy)$.

En particulier, une algèbre est dite alternative si elle est alternative à droite et à gauche.

Remarque 3.1.22. Evidemment, il est utile de remarquer que toute algèbre associative est alternative.

Proposition 3.1.23. *L'algèbre des octonions $\mathbb{O}$ est alternative.*

Démonstration. Soient $x = (x_1, x_2)$ et $y = (y_1, y_2)$ deux octonions. Montrons que la multiplication est alternative à droite. D'une part on a

$$\begin{aligned}
y(xx) &= (y_1, y_2)(x_1 x_1 - \overline{x_2} x_2\,,\ x_2 \overline{x_1} + x_2 x_1) \\
&= (y_1(x_1^2 - \overline{x_2} x_2) - (\overline{x_2 \overline{x_1} + x_2 x_1}) y_2\,,\ y_2(\overline{x_1 x_1 - \overline{x_2} x_2}) + (x_2 \overline{x_1} + x_2 x_1) y_1) \\
&= (y_1 x_1^2 - y_1 |x_2|^2 - (x_1 \overline{x_2} + \overline{x_1}\, \overline{x_2}) y_2\,,\ y_2(\overline{x_1}^2 - \overline{x_2} x_2) + x_2 \overline{x_1} y_1 + x_2 x_1 y_1) \\
&= (y_1 x_1^2 - y_1 |x_2|^2 - x_1 \overline{x_2} y_2 - \overline{x_1}\, \overline{x_2} y_2\,,\ y_2 \overline{x_1}^2 - y_2 |x_2|^2 + x_2 \overline{x_1} y_1 + x_2 x_1 y_1).
\end{aligned}$$

Et d'autre part, on a

$$\begin{aligned}
(yx)x &= (y_1 x_1 - \overline{x_2} y_2\,,\ y_2 \overline{x_1} + x_2 y_1)(x_1, x_2) \\
&= ((y_1 x_1 - \overline{x_2} y_2) x_1 - \overline{x_2}(y_2 \overline{x_1} + x_2 y_1)\,,\ (y_2 \overline{x_1} + x_2 y_1) \overline{x_1} + x_2(y_1 x_1 - \overline{x_2} y_2)) \\
&= (y_1 x_1^2 - \overline{x_2} y_2 x_1 - \overline{x_2} y_2 \overline{x_1} - |x_2|^2 y_1\,,\ y_2 \overline{x_1}^2 + x_2 y_1 \overline{x_1} + x_2 y_1 x_1 - |x_2|^2 y_2)
\end{aligned}$$

1. La définition et l'énoncé des résultats relatifs à l'alternativité d'une algèbre sont notamment disponibles aux références [3], [15] et [13].

Afin d'avoir l'égalité désirée, il faut montrer deux égalités :

$$-x_1\overline{x_2}y_2 - \overline{x_1}\,\overline{x_2}y_2 = -\overline{x_2}y_2x_1 - \overline{x_2}y_2\overline{x_1} \tag{3.5}$$

et

$$x_2\overline{x_1}y_1 + x_2x_1y_1 = x_2y_1\overline{x_1} + x_2y_1x_1 \tag{3.6}$$

Montrons l'égalité 3.5. Puisque $x_1, y_1, y_2 \in \mathbb{H}$ et que la la multiplication distribue l'addition sur l'algèbre des quaternions, nous avons

$$-x_1\overline{x_2}y_2 - \overline{x_1}\,\overline{x_2}y_2 = -(x_1 + \overline{x_1})\overline{x_2}y_2$$

Or, par la définition 2.2.27, on sait que $x_1 + \overline{x_1} = 2\Re(x_1)$ et qu'il s'agit d'un nombre réel. Ainsi on a successivement

$$\begin{aligned}
-(x_1 + \overline{x_1})\overline{x_2}y_2 &= -2\Re(x_1)\overline{x_2}y_2 \\
&= -\overline{x_2}y_2\,2\Re(x_1) \\
&= -\overline{x_2}y_2(x_1 + \overline{x_1}) \\
&= -\overline{x_2}y_2x_1 - \overline{x_2}y_2\overline{x_1},
\end{aligned}$$

et la première des deux égalités est démontrée. En ce qui concerne l'égalité 3.6, les calculs sont analogues. Dès lors, nous avons

$$\begin{aligned}
x_2\overline{x_1}y_1 + x_2x_1y_1 &= x_2(\overline{x_1}y_1 + x_1y_1) \\
&= x_2(\overline{x_1} + x_1)y_1 \\
&= x_2 2\Re(x_1)y_1 \\
&= x_2y_1 2\Re(x_1) \\
&= x_2y_1(\overline{x_1} + x_1) \\
&= x_2y_1\overline{x_1} + x_2y_1x_1,
\end{aligned}$$

ce qui prouve la seconde égalité. Dès lors, il vient bel et bien

$$y(xx) = (yx)x \quad \text{pour tous } x, y \in \mathbb{O}.$$

Montrons maintenant que la multiplication est alternative à gauche. La démonstration est analogue à celle que nous venons de faire, c'est pourquoi je propose d'en démontrer les grandes lignes. Nous avons les égalités

$$(xx)y = (x_1^2y_1 - |x_2|^2y_1 - \overline{y_2}x_2\overline{x_1} - \overline{y_2}x_2x_1\,,\ x_2\overline{x_1}\,\overline{y_1} + x_2x_1\overline{y_1} + y_2x_1^2 - y_2|x_2|^2)$$

et

$$x(xy) = (x_1^2y_1 - x_1\overline{y_2}x_2 - y_1|x_2|^2 - \overline{x_1}\,\overline{y_2}x_2\,,\ x_2\overline{y_1}\,\overline{x_1} - |x_2|^2y_2 + x_2\overline{y_1}x_1 + y_2x_1^2)$$

Dès lors, nous avons l'égalité souhaitée puisque nous avons

$$-\overline{y_2}x_2\overline{x_1} - \overline{y_2}x_2x_1 = -\overline{y_2}x_2(\overline{x_1} + x_1) = -(x_1 + \overline{x_1})\overline{y_2}x_2 = -x_1\overline{y_2}x_2 - \overline{x_1}\,\overline{y_2}x_2,$$

et

$$x_2\overline{x_1}\,\overline{y_1} + x_2x_1\overline{y_1} = x_2(\overline{x_1} + x_1)\overline{y_1} = x_2\overline{y_1}(\overline{x_1} + x_1) = x_2\overline{y_1}\,\overline{x_1} + x_2\overline{y_1}x_1.$$

Puisque la multiplication est alternative à droite et à gauche, elle est alternative et nous en concluons que l'algèbre $\mathbb{O}$ est alternative. $\square$

Grâce à ce résultat, nous sommes en mesure de dire que l'algèbre des octonions $\mathbb{O}$ est une algèbre alternative à division. Nous allons maintenant nous atteler à démontrer que l'algèbre $\mathbb{O}$ vérifie les trois identités de Moufang [2]. Pour ce faire, commençons par une définition et par la démonstration de plusieurs résultats intermédiaires.

Définition 3.1.24. Soit A une algèbre et x, y, z trois de ses éléments. Les identités de Moufang sont données par

1) $(zxz)y = z(x(zy))$;
2) $y(zxz) = ((yz)x)z$;
3) $(zy)(xz) = z(yx)z$.

Proposition 3.1.25. *Soit A une algèbre alternative. L'associateur défini par*

$$[\cdot,\cdot,\cdot] : A \times A \times A \to A : (x, y, z) \mapsto (xy)z - x(yz)$$

est une opération trilinéaire et antisymétrique. Par ailleurs, il vérifie les égalités $[x, x, y] = 0$ et $[y, x, x] = 0$ pour tous $x, y \in A$.

Démonstration. Considérons x, y, z, u quatre éléments de l'algèbre A. Dans un premier temps, en raison de l'alternativité à gauche et à droite de l'algèbre, il vient directement

$$[x, x, y] = (xx)y - x(xy) = 0 \quad \text{et} \quad [y, x, x] = (yx)x - y(xx) = 0.$$

Montrons désormais que l'opération est trilinéaire. Pour cela, nous allons montrer $[x, \alpha u + \beta y, z] = \alpha[x, u, z] + \beta[x, y, z]$ pour tous $\alpha, \beta \in \mathbb{R}$. Les deux autres possibilités se démontrent pareillement. On a

$$\begin{aligned}\alpha[x, u, z] + \beta[x, y, z] &= \alpha((xu)z - x(uz)) + \beta((xy)z - x(yz)) \\ &= \alpha(xu)z - \alpha x(uz) + \beta(xy)z - \beta x(yz) \\ &= (x\alpha u)z - x(\alpha uz) + (x\beta y)z - x(\beta yz),\end{aligned}$$

où nous avons utilisé le fait que A soit une algèbre et α, β deux nombres réels. De plus, en raison du fait que A soit une algèbre, on sait que la multiplication distribue l'addition. Ainsi, il vient

$$\begin{aligned}(x\alpha u)z - x(\alpha uz) + (x\beta y)z - x(\beta yz) &= ((x\alpha u) + (x\beta y))z - x((\alpha uz) + (\beta yz)) \\ &= (x(\alpha u + \beta y))z - x((\alpha u + \beta y)z) \\ &= [x, \alpha u + \beta y, z],\end{aligned}$$

ce que nous souhaitions.
Finalement, prouver l'antisymétrie se fait aisément en utilisant les deux résultats que nous venons à l'instant de démontrer. En effet, on a

$$[x, y, z] + [y, x, z] = [(x + y), (y + x), z] = [(x + y), (x + y), z] = 0,$$

et

$$[x, y, z] + [x, z, y] = [x, (y + z), (z + y)] = [x, (y + z), (y + z)] = 0.$$

La conjonction de ces deux petits résultats nous permet d'en conclure que l'associateur est antisymétrique puisque deux transpositions associées (12) et (23) engendrent S_3, le groupe des permutations de trois éléments. □

2. Ruth Moufang (1905 - 1977) est une mathématicienne allemande spécialisée dans la géométrie projective. En 1946, elle devient la première professeure titulaire allemande en mathématiques quelques années après que Hitler lui ait refusé l'accès à un poste d'enseignant d'université en raison de sa condition de femme.

Proposition 3.1.26. *Toute algèbre alternative A est flexible. Autrement dit, pour tous $x, y \in A$, on a $(xy)x = x(yx)$.*

Démonstration. Considérons l'associateur défini à la proposition précédente. Dans ce cas, on a

$$[x, y, x] = (xy)x - x(yx).$$

Si nous parvenons à montrer que $[x, y, x]$ est nul, nous aurons directement le résultat escompté. En utilisant la trilinéarité de l'associateur et l'alternativité de l'algèbre, nous avons

$$\begin{aligned} [x, y, x] &= [x, x, x] + [x, y, x] + [y, x, x] + [y, y, x] \\ &= [(x + y), (x + y), x] \\ &= 0. \end{aligned}$$

D'où la conclusion. $\square$

Théoreme 3.1.27. *Toute algèbre alternative A vérifie les identités de Moufang.*

1) $(zxz)y = z(x(zy))$,
2) $y(zxz) = ((yz)x)z$,
3) $(zy)(xz) = z(yx)z$,

pour tous $x, y, z \in A$.

Démonstration. Afin de démontrer la première identité, remarquons que

$$(zxz)y - z(x(zy)) = [zx, z, y] + [z, x, zy]$$

En effet,

$$[zx, z, y] + [z, x, zy] = ((zx)z)y - (zx)(zy) + (zx)(zy) - z(x(zy)) = (zxz)y - z(x(zy))$$

en considérant que $zxz = (zx)z$ puisque, par la proposition précédente, $(zx)z = z(xz)$, autrement dit la façon de poser les parenthèses importe peu.
Dès lors, en utilisant l'antisymétrie de l'associateur nous avons

$$\begin{aligned} (zxz)y - z(x(zy)) &= -[z, zx, y] - [z, zy, x] \\ &= -(z(zx))y + z((zx)y) - (z(zy))x + z((zy)x) \\ &= -(z^2x)y + z((zx)y) - (z^2y)x + z((zy)x) \end{aligned}$$

où la dernière égalité est justifiée en utilisant l'alternativité à gauche de A. Nous continuons en utilisant l'artifice de calcul suivant

$$\begin{aligned} (zxz)y - z(x(zy)) &= -(z^2x)y + z^2(xy) - z^2(xy) + z((zx)y) - (z^2y)x + z^2(yx) - z^2(yx) + z((zy)x) \\ &= -[z^2, x, y] - z^2(xy) + z((zx)y) - [z^2, y, x] - z^2(yx) + z((zy)x). \end{aligned}$$

Comme la multiplication distribue l'addition sur l'algèbre et parce que l'associateur est antisymétrique on a,

$$\begin{aligned} (zxz)y - z(x(zy)) &= -[z^2, x, y] - z^2(xy) - [z^2, y, x] - z^2(yx) + z((zx)y + (zy)x) \\ &= -z^2(xy) - z^2(yx) + z((zx)y + (zy)x) \\ &= z(-z(xy) - z(yx) + (zx)y + (zy)x) \\ &= z([z, x, y] + [z, y, x]) \\ &= 0. \end{aligned}$$

Ainsi, $(zxz)y = z(x(zy))$ et la première égalité est démontrée.
De même, toute algèbre alternative vérifie la seconde égalité. La démonstration de ce résultat est semblable à ce que nous venons de faire, c'est pourquoi on ne détaillera ici que les grandes étapes sans en justifier les différentes égalités. Ainsi, on a

$$\begin{aligned}((yz)x)z - y(zxz) &= [y,z,xz] + [yz,x,z]\\ &= -[y,xz,z] - [x,yz,z]\\ &= -(y(xz))z + y(xz^2) - (x(yz))z + x(yz^2)\\ &= -(y(xz))z + y(xz^2) - (yx)z^2 + (yx)z^2 - (x(yz))z + x(yz^2) - (xy)z^2 + (xy)z^2\\ &= -(y(xz))z - [y,x,z^2] + (yx)z^2 - (x(yz))z - [x,y,z^2] + (xy)z^2\\ &= (-y(xz) + (yx)z - x(yz) + (xy)z)z\\ &= 0.\end{aligned}$$

Par conséquent, $((yz)x)z = y(zxz)$ et la deuxième égalité vient d'être démontrée.
Il nous reste désormais à démontrer la dernière égalité de Moufang. Pour démontrer cette troisième égalité, nous allons utiliser la première égalité. Remarquons que

$$(zy)(xz) - z(yx)z = [z,y,xz] + z(y(xz) - (yx)z).$$

Etant donné que l'associateur est antisymétrique, nous avons

$$\begin{aligned}(zy)(xz) - z(yx)z &= -[z,xz,y] + z(y(xz) - (yx)z)\\ &= -[z,xz,y] - z[y,x,z].\end{aligned}$$

En utilisant ensuite la définition de l'associateur et puisque l'algèbre est flexible, il vient

$$\begin{aligned}(zy)(xz) - z(yx)z &= -(z(xz))y + z((xz)y) - z[y,x,z]\\ &= -(zxz)y + z((xz)y) - z[y,x,z].\end{aligned}$$

Ensuite, grâce à la première égalité de Moufang et par distributivité de la multiplication sur l'addition, la dernière égalité ci-dessus se réécrit successivement comme

$$\begin{aligned}(zy)(xz) - z(yx)z &= -z(x(zy)) + z((xz)y) - z[y,x,z]\\ &= -z(x(zy) - (xz)y + [y,x,z])\\ &= -z(-[x,z,y] + [y,x,z])\\ &= 0\end{aligned}$$

où l'antisymétrie a été appliquée deux fois pour justifier la dernière égalité. Nous avons donc $(zy)(xz) = z(xy)z$, ce qui conclut la troisième et dernière égalité de Moufang. □

Théoreme 3.1.28. *L'algèbre des octonions $\mathbb{O}$ vérifie les trois identités de Moufang.*

Démonstration. L'algèbre $\mathbb{O}$ étant une algèbre alternative, le résultat est immédiat par le théorème 3.1.27. □

3.2 Doublement de Dickson - Théorème de Hurwitz

Cette section sera consacrée à la démonstration du théorème d'Hurwitz qui affirme que les réels $\mathbb{R}$, les complexes $\mathbb{C}$, les quaternions $\mathbb{H}$ et les octonions $\mathbb{O}$ sont les seules algèbres à composition. Pour ce faire, nous aurons besoin d'introduire une formule, appelée formule de Dickson, que nous développons dans la première partie de cette section. Les résultats développés ici sont tirés du livre de Conway et Smith intitulé *On Quaternions and Octonions : their geometry, arithmetic and symmetry* que l'on retrouve à la référence [13].

3.2.1 Règle du doublement de Dickson

Comme nous l'avons vu dans les chapitres et sections précédents, tout nombre complexe z peut s'écrire comme un couple de nombres réels (a, b) dont la multiplication et l'opération conjugué sont données ci-dessous

$$\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C} : ((a, b), (a', b')) \mapsto (aa' - bb', ab' + a'b),$$

et

$$^{-} : \mathbb{C} \to \mathbb{C} : (a, b) \mapsto (a, -b).$$

De même, au chapitre 2, nous avons vu que tout quaternion q pouvait s'écrire comme un couple de nombres complexes (q_1, q_2) dont la multiplication et l'opération conjugué sont données par les expressions

$$\cdot : \mathbb{H} \times \mathbb{H} \to \mathbb{H} : ((q_1, q_2), (q_1', q_2')) \mapsto (q_1 q_1' - \overline{q_2'} q_2, q_2 \overline{q_1'} + q_2' q_1),$$

et

$$^{-} : \mathbb{H} \to \mathbb{H} : (q_1, q_2) \mapsto (\overline{q_1}, -q_2).$$

Finalement, nous avons montré, au début de ce chapitre, que tout octonion x pouvait s'écrire comme un couple de quaternions (x_1, x_2). Dans ce cas, nous avons également définit la multiplication comme l'opération

$$\cdot : \mathbb{O} \times \mathbb{O} \to \mathbb{O} : ((x_1, x_2), (y_1, y_2)) \mapsto (x_1 y_1 - \overline{y_2} x_2, x_2 \overline{y_1} + y_2 x_1),$$

et l'opération conjugué a quant à elle été définie par

$$^{-} : \mathbb{O} \to \mathbb{O} : (x_1, x_2) \mapsto (\overline{x_1}, -x_2).$$

On constate donc bien des correspondances entre les différentes formules de multiplication et celles donnant l'opération conjugué. Nous allons montrer qu'elles obéissent à la formule de doublement de Dickson.
La construction de Cayley-Dickson est un processus qui, comme indiqué dans l'article de Laurent La Fuente-Gravy intitulé *Le Théorème d'Hurwitz*, permet d'obtenir une formule qui, à partir d'un produit sur un espace vectoriel $(A, \cdot)$, fournit un produit sur $A \times A$. Dans ce but, A doit être muni d'une conjugaison que l'on note

$$^{-} : A \to A : a \mapsto \bar{a}$$

et qui vérifie $\bar{\bar{a}} = a$ et $\overline{ab} = \bar{b}\bar{a}$ pour tous $a, b \in A$, et $(A, \cdot, ^{-})$ désignera un espace vectoriel muni d'un produit et d'une conjugaison. La définition suivante suit immédiatement.

Définition 3.2.1. Le double de Dickson de $(A, \cdot, ^{-})$ est l'espace vectoriel $A \times A$ muni du produit

$$(a, b) \cdot (c, d) = (ac - d\bar{b}, cb + \bar{a}d) \quad \forall (a, b), (c, d) \in A \times A,$$

et d'une conjugaison définie comme

$$\overline{(a, b)} = (\bar{a}, -b) \quad \forall (a, b) \in A \times A.$$

Avant d'entrer dans le vif du sujet, il est bon de rappeler certaines définitions d'algèbre bilinéaire qui seront utiles par la suite dans cette section. S'ils le souhaitent, les lecteurs peuvent consulter les références [9] et [14] afin d'obtenir plus amples informations sur cette matière.

Définition 3.2.2. Soit E un espace vectoriel. Une forme bilinéaire sur $\mathbb{R}$ est une application $B : E \times E \to \mathbb{R}$ telle que pour tous $x, y, z \in E$ et $\lambda \in \mathbb{R}$, les conditions

1. $B(\lambda x + y, z) = \lambda B(x, z) + B(y, z)$,
2. $B(x, \lambda y + z) = \lambda B(x, y) + B(x, z)$,

sont vérifiées.

Définition 3.2.3. Une forme bilinéaire $B : E \times E \to \mathbb{R}$ est symétrique si pour tous $x, y \in E$, on a $B(x, y) = B(y, x)$.

Définition 3.2.4. Soit $B : E \times E \to \mathbb{R}$ une forme bilinéaire avec E un espace vectoriel. Le noyau d'une forme bilinéaire est défini par

$$\ker(B) = \{y \in E | \forall x \in E, B(x, y) = 0\}.$$

Une forme bilinéaire est dite non dégénérée si son noyau est restreint au vecteur nul. En d'autres termes, $\ker(B) = \{0\}$.

Définition 3.2.5. Soit $B : E \times E \to \mathbb{R}$ une forme bilinéaire symétrique où E est un espace vectoriel. L'application $Q : E \to \mathbb{R}$ donnée par

$$Q(x) = B(x, x)$$

pour tout $x \in E$, est la forme quadratique associée à la forme bilinéaire B.

Remarque 3.2.6. Cette définition nous indique directement que $Q(ax) = a^2 Q(x)$ pour tout $a \in \mathbb{R}$ et tout $x \in E$. En effet, par bilinéarité de B on a

$$Q(ax) = B(ax, ax) = aaB(x, x) = a^2 Q(x).$$

Proposition 3.2.7. *Soit $Q : E \to \mathbb{R}$ la forme quadratique associée à la forme bilinéaire symétrique $B : E \times E \to \mathbb{R}$. Pour tous $x, y \in E$ on a l'égalité*

$$B(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)).$$

Démonstration. En effet, par définition d'une forme quadratique Q on a, pour tous $x, y \in E$

$$Q(x + y) - Q(x) - Q(y) = B(x, x) + 2B(x, y) + B(y, y) - B(x, x) - B(y, y) = 2B(x, y)$$

étant donné que la forme B associée à Q est bilinéaire et symétrique. □

Définition 3.2.8. Soit A une algèbre de dimension finie. Une forme quadratique $Q : A \to \mathbb{R}$ est non dégénérée si la forme bilinéaire symétrique associée $B : A \times A \to \mathbb{R}$ est non dégénérée.

Définition 3.2.9. Une algèbre à composition sur le champ des réels $\mathbb{R}$ est une algèbre A sur $\mathbb{R}$ où

1) A admet une forme quadratique non dégénérée $Q : A \to \mathbb{R}$;
2) Q respecte la loi de composition, c'est-à-dire

$$\forall x, y \in A, \quad Q(xy) = Q(x)Q(y),$$

ou encore

$$\forall x, y \in A, \quad B(xy, xy) = B(x, x)B(y, y). \tag{3.7}$$

Les définitions exposées précédemment ainsi que la proposition 3.2.7 ne représentent pas uniquement de simples rappels d'algèbre bilinéaire. Effectivement, ces notions et résultats seront fréquemment utilisés dans la fin de ce chapitre.
Dans un premier temps, nous démontrons le résultat ci-dessous qui est très intéressant puisqu'il lie les notions d'algèbre à composition et d'algèbre à division.

Proposition 3.2.10. *Une algèbre A à composition est une algèbre à division si la forme quadratique Q associée à l'algèbre satisfait la condition*

$$Q(x) = 0 \quad \Rightarrow \quad x = 0 \quad \forall x \in A. \tag{3.8}$$

Démonstration. Dans un premier temps, montrons que $Q(0) = 0$. Cela nous aidera en effet dans la suite de la preuve. Par définition,

$$Q(0) = B(0,0) = \frac{1}{2}(Q(0+0) - Q(0) - Q(0)) = -\frac{1}{2}Q(0),$$

et donc

$$\frac{3}{2}Q(0) = 0 \Leftrightarrow Q(0) = 0.$$

Montrons désormais que l'algèbre est à division. Supposons que la condition 3.8 soit vérifiée. Nous supposons également que $xy = 0$ et nous allons montrer que $x = 0$ ou $y = 0$. Si on prend la forme quadratique Q du produit xy, il vient

$$Q(xy) = Q(0) = 0,$$

puisque xy est supposé nul et en considérant le résultat intermédiaire démontré plus haut. Etant donné que l'algèbre est à composition, cela est équivalent à

$$Q(x)Q(y) = 0. \tag{3.9}$$

Or, $Q(x)$ et $Q(y)$ sont deux nombres réels. Ainsi, puisque le champ des réels est intègre, il s'en suit que la condition 3.9 est équivalente à la condition

$$Q(x) = 0 \quad \text{ou} \quad Q(y) = 0,$$

ou encore à la condition

$$x = 0 \quad \text{ou} \quad y = 0,$$

par la condition 3.8. Dès lors, ce résultat nous indique que l'algèbre A est intègre et donc à division en utilisant la proposition 2.3.4. □

Afin de pouvoir démontrer le théorème d'Hurwitz, certains résultats intermédiaires sont nécessaires. Nous allons donc, dans un premier temps, nous intéresser à la démonstration des résultats en question. Sauf mention explicite, dans les propriétés ci-dessous, A désigne une algèbre à composition avec une unité, notée 1, munie d'une forme quadratique non dégénérée Q associée à la forme bilinéaire symétrique B.

Proposition 3.2.11 (Scaling law)**.** *Pour tous $x, y, z \in A$, les égalités*

$$B(xy, xz) = Q(x)B(y,z) = B(x,x)B(y,z) \quad \text{et} \quad B(xz, yz) = B(x,y)Q(z) = B(x,y)B(z,z)$$

sont vérifiées.

Démonstration. Considérons $x, y, z \in A$, par la proposition 3.2.7 nous avons

$$\begin{aligned}
B(xy, xz) &= \frac{1}{2}(Q(xy + xz) - Q(xy) - Q(xz)) \\
&= \frac{1}{2}(Q(x(y + z)) - Q(xy) - Q(xz)) \\
&= \frac{1}{2}(Q(x)Q(y + z) - Q(x)Q(y) - Q(x)Q(z)) \\
&= \frac{1}{2}Q(x)(Q(y + z) - Q(y) - Q(z)) \\
&= Q(x)B(y, z) \\
&= B(x, x)B(y, z),
\end{aligned}$$

où nous avons utilisé le fait que la multiplication distribue l'addition sur l'algèbre A et que la forme quadratique Q respecte la loi de composition.
Pour les mêmes raisons, et par un développement similaire nous avons

$$B(xz, yz) = \frac{1}{2}(Q((x + y)z) - Q(xz) - Q(yz)) = B(x, y)B(z, z).$$

□

Proposition 3.2.12 (Exchange law)**.** *Pour tous $u, x, y, z \in A$, on a*

$$B(xy, uz) = 2B(x, u)B(y, z) - B(xz, uy).$$

Démonstration. En utilisant la proposition 3.2.11, on a

$$B((x + u)y, (x + u)z) = B(x + u, x + u)B(y, z).$$

Or, B est bilinéaire et symétrique donc

$$\begin{aligned}
B((x + u)y, (x + u)z) &= (B(x, x) + 2B(x, u) + B(u, u))B(y, z) \\
&= B(x, x)B(y, z) + 2B(x, u)B(y, z) + B(u, u)B(y, z).
\end{aligned}$$

De plus, sachant que A est une algèbre, la multiplication est distributive sur l'addition, et puisque B est bilinéaire, il vient respectivement

$$\begin{aligned}
B((x + u)y, (x + u)z) &= B(xy + uy, xz + uz) \\
&= B(xy, xz) + B(xy, uz) + B(uy, xz) + B(uy, uz).
\end{aligned}$$

Ensuite, en utilisant la proposition précédente, cette dernière égalité peut se réécrire comme

$$B((x + u)y, (x + u)z) = B(x, x)B(y, z) + B(xy, uz) + B(uy, xz) + B(u, u)B(y, z).$$

Finalement, après simplification de certains termes et en réarrangeant les termes restants il vient,

$$B(xy, uz) = 2B(x, u)B(y, z) - B(uy, xz)$$

ce qui peut se réécrire comme

$$B(xy, uz) = 2B(x, u)B(y, z) - B(xz, uy)$$

puisque la forme bilinéaire B est symétrique. □

Afin de pouvoir établir d'autres résultats nécessaires à la preuve du théorème d'Hurwitz, la définition suivante s'impose.

Définition 3.2.13. Pour tout $x \in A$, le conjugué de x est défini par

$$\bar{x} = 2B(x, 1) - x. \tag{3.10}$$

Remarque 3.2.14. Cette dernière définition n'est pas dénuée de sens. En effet, sur $\mathbb{R}$, nous avons $\bar{x} = x$, et pour les algèbres $\mathbb{C}, \mathbb{H}$ et $\mathbb{O}$ cette définition coïncide avec celle qui a été proposée dans chacun des cas.

Proposition 3.2.15 (Braid law)**.** *Pour tous $x, y, z \in A$, on a*

$$B(xy, z) = B(y, \bar{x}z) \quad \textit{et} \quad B(xy, z) = B(x, z\bar{y}).$$

Démonstration. En utilisant la proposition 3.2.12 nous avons

$$B(xy, z) = B(xy, 1z) = 2B(x, 1)B(y, z) - B(xz, 1y) = 2B(x, 1)B(y, z) - B(xz, y).$$

Puisque B est symétrique, c'est équivalent à

$$B(xy, z) = 2B(x, 1)B(y, z) - B(y, xz).$$

Or, le coefficient $B(x, 1)$ est réel, ainsi étant donné que B est une application bilinéaire, on a

$$\begin{aligned} B(xy, z) &= B(y, 2B(x, 1)z) - B(y, xz) \\ &= B(y, 2B(x, 1)z - xz) \\ &= B(y, (2B(x, 1) - x)z) \\ &= B(y, \bar{x}z), \end{aligned}$$

où l'avant dernière égalité se justifie par le fait que le produit distribue la somme sur l'algèbre considérée A.
De même, par un raisonnement équivalent on a,

$$\begin{aligned} B(xy, z) &= B(xy, z1) \\ &= 2B(x, z)B(y, 1) - B(x, zy) \\ &= B(x, z(2B(y, 1))) - B(x, zy) \\ &= B(x, z(2B(y, 1) - y)) \\ &= B(x, z\bar{y}). \end{aligned}$$

□

Proposition 3.2.16 (Double conjugué)**.** *Pour tous $x \in A$, on a $\bar{\bar{x}} = x$.*

Démonstration. Puisque B est non-dégénérée, il suffit de montrer que pour tout $t \in A$, l'égalité $B(x, t) = B(\bar{\bar{x}}, t)$ est vérifiée. Pour tout $t \in A$, en utilisant la proposition 3.2.15 on a,

$$B(x, t) = B(x\,1, t) = B(1, \bar{x}t)$$

puisque 1 est l'élément neutre sur l'algèbre. Par symétrie de B, on a également

$$B(x, t) = B(\bar{x}t, 1).$$

En appliquant une seconde la proposition 3.2.15 et par symétrie de B il vient,

$$B(x, t) = B(t, \bar{\bar{x}}1) = B(\bar{\bar{x}}1, t).$$

Nous obtenons alors immédiatement le résultat souhaité étant donné que 1 est l'unité de A. Ainsi,

$$B(x, t) = B(\bar{\bar{x}}, t) \qquad \forall t \in A,$$

et le résultat est démontré. □

Proposition 3.2.17 (Conjugué du produit)**.** *Pour tous $x, y \in A$ on a, $\overline{xy} = \bar{y}\bar{x}$.*

Démonstration. Montrons que pour tout $t \in A$, on a $B(\overline{xy}, t) = B(\bar{y}\bar{x}, t)$.
La démonstration de ce résultat découle d'une succession d'applications de la proposition 3.2.15 et de la proposition 3.2.16. Ainsi, nous avons

$$B(\bar{y}\bar{x}, t) = B(\bar{x}, \bar{\bar{y}}t) = B(\bar{x}, yt) = B(\bar{x}, y\bar{\bar{t}}) = B(\bar{x}\bar{t}, y) = B(\bar{t}, xy).$$

Or,

$$B(\bar{t}, xy) = B(\bar{t}, (xy)1) = B(\bar{t}, (\overline{\overline{xy}})1).$$

Et finalement,

$$B(\bar{t}, (\overline{\overline{xy}})1) = B((\overline{xy})\bar{t}, 1) = B(\overline{xy}, 1\bar{\bar{t}}) = B(\overline{xy}, 1t) = B(\overline{xy}, t).$$

On conclut encore par la non-dégénérescence de B. □

On va désormais s'intéresser aux lois de doublement, nous rapprochant de plus en plus de notre but qui est, rappelons-le, de démontrer le théorème d'Hurwitz à la section prochaine. Pour ce faire, nous considérons la situation dans laquelle H est une sous-algèbre de A de dimension n ($n \in \mathbb{N}_0$) contenant 1 et sur laquelle la forme quadratique de A est non dégénérée. Considérons également un vecteur unitaire i orthogonal à H. Ainsi, 1 et i sont orthogonaux au sens de B. Autrement dit,

$$B(1, i) = 0,$$

et en particulier $B(h, i) = 0$ pour tout élément h de la sous-algèbre H.
Certains faits peuvent directement être établis, reprenons-les dans les deux lemmes suivants.

Lemme 3.2.18. *Dans la situation ci-dessus, on a $\bar{i} = -i$.*

Démonstration. Il suffit d'utiliser l'identité 3.10. En effet, nous avons

$$\bar{i} = 2B(i, 1) - i = -i,$$

étant donné que $1 \in H$ et que i est un vecteur orthogonal à H. □

Lemme 3.2.19. *Pour tous $x, y, z \in H$, on a*

1. $B(ix, yz) = -B(iz, yx)$
2. $B(xi, yz) = -B(xz, yi)$
3. $B(xy, iz) = -B(xz, iy)$
4. $B(xy, zi) = -B(xi, zy)$

Démonstration. Dans chacun des cas, il s'agit d'une simple application de la proposition 3.2.12. Démontrons le premier point, les trois autres se démontrent de façon similaire. On a

$$B(ix, yz) = 2B(i, y)B(x, z) - B(iz, yx) = -B(iz, yx),$$

où la dernière égalité se justifie par le fait que $y \in H$ et i est orthogonal à H. □

Proposition 3.2.20 (Produit scalaire)**.** *Pour tous $a, b, c, d \in H$, l'identité*

$$B(a + ib, c + id) = B(a, c) + B(b, d)$$

est toujours vérifiée.

Démonstration. Remarquons tout d'abord que $B(i, i) = 1$ puisque i est un vecteur unitaire. Dès lors, en utilisant la bilinéarité de B et la proposition 3.2.11 il vient

$$\begin{aligned} B(a + ib, c + id) &= B(a, c) + B(a, id) + B(ib, c) + B(ib, id) \\ &= B(a, c) + B(a, id) + B(ib, c) + B(i, i)B(b, d) \\ &= B(a, c) + B(a, id) + B(ib, c) + B(b, d). \end{aligned}$$

Pour arriver au résultat escompté, nous devons montrer que $B(a, id) = 0$ et $B(ib, c) = 0$. Montrons que $B(a, id) = 0$. Par la proposition 3.2.15 et la proposition 3.2.16, on a

$$B(a, id) = B(a, i\bar{\bar{d}}) = B(a\bar{d}, i).$$

Or,

$$\bar{d} = 2B(d, 1) - d = 2B(d, 1)1 - d \in H$$

car $1, d \in H$, $B(d, 1) \in \mathbb{R}$ et H est une sous-algèbre donc stable pour la somme et le produit par un scalaire. De même, par définition d'une sous-algèbre, H est stable pour le produit, donc $a\bar{d} \in H$. Dès lors, $B(a\bar{d}, i) = 0$ ce qui implique que

$$B(a, id) = 0$$

Pour continuer, $B(ib, c) = 0$ est immédiat par ce que nous venons de faire puisque B est symétrique. Finalement, on trouve le résultat souhaité

$$B(a + ib, c + id) = B(a, c) + B(b, d).$$

□

Proposition 3.2.21 (Conjugaison)**.** *Pour tous $a, b \in H$, $\overline{a + ib} = \bar{a} - ib$ et en particulier $ib = -\overline{ib} = -\bar{b}\,\bar{i} = \bar{b}\,i$.*

Démonstration. Tout d'abord, on a

$$\begin{aligned} \overline{a + ib} &= 2B(a + ib, 1) - (a + ib) \\ &= 2(B(a, 1) + B(ib, 1)) - (a + ib) \\ &= 2B(a, 1) + 2B(ib, 1) - a - ib \\ &= 2B(a, 1) - a - ib \\ &= \bar{a} - ib, \end{aligned}$$

où l'égalité $B(ib, 1) = 0$ découle directement de la proposition précédente. Ensuite, d'une part en utilisant l'identité 3.10, on a

$$\overline{ib} = 2B(ib, 1) - ib = -ib$$

et d'autre part, en utilisant la proposition 3.2.17 on a $\overline{ib} = \bar{b}\,\bar{i}$. Finalement, le lemme 3.2.18 nous dit que $\bar{i} = -i$, ce qui nous permet d'obtenir l'égalité $-\bar{b}\,\bar{i} = \bar{b}i$. Ainsi, en considérant toutes les égalités que nous venons de démontrer, nous obtenons le résultat escompté. □

Proposition 3.2.22 (Product Doubling). *Pour tous $a, b, c, d \in H$, l'identité*

$$(a + ib)(c + id) = (ac - d\bar{b}) + i(cb + \bar{a}d)$$

est vérifiée.

Démonstration. Avant d'entrer dans le coeur de la preuve, rappelons que comme A est une algèbre, la multiplication distribue l'addition. Ainsi, on a

$$(a + ib)(c + id) = ac + a(id) + (ib)c + (ib)(id)$$

Pour montrer que $a(id) = i(\bar{a}d)$, il suffit de montrer que $B(a(id), t) = B(i(\bar{a}d), t)$ pour tout $t \in A$ et on concluera par la non-dégénérescence de B. Ainsi, pour tout $t \in A$, grâce à la proposition 3.2.15 et au lemme 3.2.19, on a

$$B(a(id), t) = B(id, \bar{a}t) = -B(it, \bar{a}d).$$

Nous continuons ensuite en utilisant la bilinéarité de B et le lemme 3.2.18, et nous avons

$$-B(it, \bar{a}d) = B(-it, \bar{a}d) = B(\bar{i}t, \bar{a}d).$$

Finalement, en utilisant une fois de plus les propriétés de cette section, nous obtenons

$$B(\bar{i}t, \bar{a}d) = B(t, i(\bar{a}d)) = B(i(\bar{a}d), t),$$

et en regroupant toutes les égalités on trouve le résultat souhaité. Pour continuer, $B((ib)c, t) = B(i(cb), t)$ pour tout $t \in A$. En effet, en utilisant les propositions 3.2.15 et 3.2.21 et le lemme 3.2.19, on a successivement

$$B((ib)c, t) = B(ib, t\bar{c}) = B(\bar{b}i, t\bar{c}) = -B(\bar{b}\bar{c}, ti).$$

Parce que $\bar{\bar{i}} = i$ et $\bar{i} = -i$, il s'en suit

$$-B(\bar{b}\bar{c}, ti) = -B(\bar{b}\bar{c}, t\bar{\bar{i}}) = B((\bar{b}\bar{c})i, t),$$

où pour arriver à la dernière égalité nous avons utilisé la proposition 3.2.15. La proposition 3.2.17 nous permet de continuer à développer, et nous obtenons

$$B((\bar{b}\bar{c})i, t) = B((\overline{cb})i, t).$$

Ainsi, en utilisant une dernière fois la proposition 3.2.21, on a

$$B((\overline{cb})i, t) = B(i(cb), t).$$

Par conséquent, $B((ib)c, t) = B(i(cb), t)$ pour tout $t \in A$, et on en conclut que $(ib)c = i(cb)$ par la non-dégénérescence de B.
Ensuite, montrons que $B((ib)(id), t) = B(-d\bar{b}, t)$ pour tout $t \in A$. Comme précédemment, il s'agit dans un premier temps d'utiliser les propositions 3.2.15, 3.2.21 ainsi que la bilinéarité de B pour réécrire $B((ib)(id), t)$ comme

$$B((ib)(id), t) = B(ib, t(\overline{id})) = B(ib, t(-\bar{d}i)) = -B(ib, t(\bar{d}i)).$$

La proposition 3.2.12 nous permet alors de continuer pour obtenir

$$-B(ib, t(\bar{d}i)) = -(2B(i, t)B(b, \bar{d}i) - B(i(\bar{d}i), tb)) = B(i(\bar{d}i), tb),$$

où cette dernière égalité est justifiée par le fait que $B(b, \bar{d}i) = B(db, i) = 0$ en utilisant la proposition 3.2.15 et le fait que H est une sous-algèbre donc stable pour le produit. Pour finir, en utilisant à nouveau les propositions précédentes de manière adéquate nous obtenons successivement

$$\begin{aligned} B(i(\bar{d}i), tb) &= B(i(id), tb) = B(id, \bar{i}(tb)) \\ &= -B(id, i(tb)) = -B(i,i)B(d, tb) \\ &= -B(d, tb) = -B(d, t\bar{\bar{b}}) \\ &= -B(d\bar{b}, t) = B(-d\bar{b}, t), \end{aligned}$$

où nous avons justifié la cinquième égalité par le fait que i soit un vecteur unitaire. Dès lors, $B((ib)(id), t) = B(-d\bar{b}, t)$ pour tout $t \in A$ comme souhaité.
Finalement, grâce à tout ce qui vient d'être démontré, nous obtenons

$$\begin{aligned} (a+ib)(c+id) &= ac + a(id) + (ib)c + (ib)(id) \\ &= ac + i(\bar{a}d) + i(cb) - d\bar{b} \\ &= (ac - d\bar{b}) + i(cb + \bar{a}d). \end{aligned}$$

□

3.2.2 Théorème d'Hurwitz

Nous venons de démontrer que si on dispose d'une algèbre à composition A avec unité contenant une sous-algèbre propre H alors elle contient également son double de Dickson $H \times H$. De plus, si A est de dimension finie alors, à un moment donné, le processus de doublement à partir de la plus petite sous-algèbre $\mathbb{R}$ sera contraint de s'arrêter. Dans cette section, nous montrerons que la propriété de doublement peut se répéter au plus trois fois pour arriver, in fine, à l'algèbre à composition des octonions. Et nous montrerons également le théorème d'Hurwitz qui stipule que les seules algèbres à compositions avec unité sont les algèbres $\mathbb{R}, \mathbb{C}, \mathbb{H}$ et $\mathbb{O}$. Dans la suite, sauf mention explicite, les algèbres considérées possèdent une unité que l'on notera 1.

Lemme 3.2.23. *L'algèbre $Z = Y + i_Z Y$ est une algèbre à composition si et seulement si Y est une algèbre à composition associative.*

Démonstration. L'algèbre $Y + i_Z Y$ est une algèbre à composition si et seulement si, pour tous $a, b, c, d \in Y$, l'égalité

$$B((a+i_Z b)(c+i_Z d), (a+i_Z b)(c+i_Z d)) = B(a+i_Z b, a+i_Z b)B(c+i_Z d, c+i_Z d)$$

est vérifiée. Or, en utilisant le produit défini à la proposition 3.2.22 on sait que

$$B((a+i_Z b)(c+i_Z d), (a+i_Z b)(c+i_Z d)) = B((ac-d\bar{b}) + i_Z(cb+\bar{a}d), (ac-d\bar{b}) + i_Z(cb+\bar{a}d)).$$

Ainsi, $Y + i_Z Y$ est une algèbre à composition si et seulement si, pour tous $a, b, c, d \in Y$ on a,

$$B((ac-d\bar{b})+i_Z(cb+\bar{a}d), (ac-d\bar{b})+i_Z(cb+\bar{a}d)) = B(a+i_Z b, a+i_Z b)B(c+i_Z d, c+i_Z d). \quad (3.11)$$

Détaillons désormais les deux membres de l'égalité 3.11. En ce qui concerne le membre de droite, que nous notons MD par soucis d'écriture, l'utilisation de la proposition 3.2.20 nous donne

$$\begin{aligned} MD &= (B(a,a) + B(b,b))(B(c,c) + B(d,d)) \\ &= B(a,a)B(c,c) + B(a,a)B(d,d) + B(b,b)B(c,c) + B(b,b)B(d,d). \end{aligned}$$

En ce qui concerne le membre de gauche, noté MG pour la même raison, si nous utilisons à nouveau la proposition 3.2.20 en plus de la bilinéarité et de la symétrie de B, il vient

$$\begin{aligned} MG &= B(ac - d\bar{b}, ac - d\bar{b}) + B(cb + \bar{a}d, cb + \bar{a}d) \\ &= B(ac, ac) - 2B(ac, d\bar{b}) + B(d\bar{b}, d\bar{b}) + B(cb, cb) + 2B(cb, \bar{a}d) + B(\bar{a}d, \bar{a}d) \\ &= B(a, a)B(c, c) - 2B(ac, d\bar{b}) + B(d, d)B(\bar{b}, \bar{b}) + B(c, c)B(b, b) + 2B(cb, \bar{a}d) + B(\bar{a}, \bar{a})B(d, d) \end{aligned}$$

où la dernière égalité découle du fait que Y est une algèbre de composition.
De plus, $B(\bar{x}, \bar{x}) = B(x, x)$ pour tout $x \in Y$. En effet,

$$B(\bar{x}, \bar{x}) = B(\bar{x}1, \bar{x}) = B(1, \bar{\bar{x}}\bar{x}) = B(1, x\bar{x}) = B(1x, x) = B(x, x).$$

Et ainsi, le membre de gauche de l'égalité 3.11 peut se réécrire sous la forme

$$MG = B(a, a)B(c, c) - 2B(ac, d\bar{b}) + B(d, d)B(b, b) + B(c, c)B(b, b) + 2B(cb, \bar{a}d) + B(a, a)B(d, d)$$

Finalement, si on égale les deux membres de l'égalité 3.11 et après suppression des termes semblables, il nous reste la succession d'équivalences suivantes : $Y + i_Z Y$ est une algèbre de composition si et seulement si, pour tous $a, b, c, d \in Y$,

$$\begin{aligned} & 0 = -2B(ac, d\bar{b}) + 2B(cb, \bar{a}d) \\ \Leftrightarrow\ & B(ac, d\bar{b}) = B(cb, \bar{a}d) \\ \Leftrightarrow\ & B((ac)b, d) = B(a(cb), d) \qquad \text{par la proposition 3.2.15} \\ \Leftrightarrow\ & (ac)b = a(cb) \quad \forall a, b, c \in Y, \end{aligned}$$

ce qui est donc équivalent à demander que Y soit une algèbre à composition associative. □

Lemme 3.2.24. *L'algèbre $Y = X + i_Y X$ est une algèbre à composition associative si et seulement si X est une algèbre à composition associative et commutative.*

Démonstration. L'algèbre $X + i_Y X$ est une algèbre à composition associative si et seulement si pour tous $a, b, c, d, e, f \in X$,

$$((a + i_Y b)(c + i_Y d))(e + i_Y f) = (a + i_Y b)((c + i_Y d)(e + i_Y f)) \tag{3.12}$$

Comme pour le lemme précédent, analysons séparément les deux membres de l'égalité 3.12. Le membre de gauche peut se réécrire sous la forme

$$\begin{aligned} ((a + i_Y b)(c + i_Y d))(e + i_Y f) &= ((ac - d\bar{b}) + i_Y(cb + \bar{a}d))(e + i_Y f) \\ &= (ac - d\bar{b})e - f\overline{(cb + \bar{a}d)} + i_Y(e(cb + \bar{a}d) + \overline{(ac - d\bar{b})}f) \\ &= (ac - d\bar{b})e - f(\bar{b}\bar{c} + \bar{d}a) + i_Y(e(cb + \bar{a}d) + (\bar{c}\,\bar{a} - b\bar{d})f) \\ &= (ac)e - (d\bar{b})e - f(\bar{b}\bar{c}) - f(\bar{d}a) + i_Y(e(cb) + e(\bar{a}d) + (\bar{c}\,\bar{a})f - (b\bar{d})f). \end{aligned}$$

Quant au membre de droite, il s'écrit comme

$$\begin{aligned} (a + i_Y b)((c + i_Y d)(e + i_Y f)) &= (a + i_Y b)((ce - f\bar{d}) + i_Y(ed + \bar{c}f)) \\ &= a(ce - f\bar{d}) - (ed + \bar{c}f)\bar{b} + i_Y((ce - f\bar{d})d + \bar{a}(ed + \bar{c}f)) \\ &= a(ce) - a(f\bar{d}) - (ed)\bar{b} - (\bar{c}f)\bar{b} + i_Y((ce)b - (f\bar{d})b + \bar{a}(ed) + \bar{a}(\bar{c}f)). \end{aligned}$$

Ainsi, l'égalité 3.12 est vérifiée si et seulement si, pour tous $a, b, c, d, e, f \in X$, on a

$$\begin{aligned} & (ac)e - (d\bar{b})e - f(\bar{b}\bar{c}) - f(\bar{d}a) + i_Y(e(cb) + e(\bar{a}d) + (\bar{c}\,\bar{a})f - (b\bar{d})f) \\ &\qquad = a(ce) - a(f\bar{d}) - (ed)\bar{b} - (\bar{c}f)\bar{b} + i_Y((ce)b - (f\bar{d})b + \bar{a}(ed) + \bar{a}(\bar{c}f)), \end{aligned}$$

ou encore

$$\left\{\begin{array}{rcl}(ac)e-(d\bar{b})e-f(\bar{b}\bar{c})-f(\bar{d}a) & = & a(ce)-a(f\bar{d})-(ed)\bar{b}-(\bar{c}f)\bar{b}\\ e(cb)+e(\bar{a}d)+(\bar{c}\,\bar{a})f-(b\bar{d})f & = & (ce)b-(f\bar{d})b+\bar{a}(ed)+\bar{a}(\bar{c}f).\end{array}\right. \tag{3.13}$$

Puisque ce système doit être vérifié pour tous $a, b, c, d, e, f \in X$, alors c'est en particulier vrai lorsque $d = f = 0$ et $b = 1$. Dans ce cas, le système devient

$$\left\{\begin{array}{rcl}(ac)e & = & a(ce)\\ ec & = & ce,\end{array}\right.$$

et on en tire que l'algèbre X doit être associative et commutative. Inversement, si X est une algèbre à composition associative et commutative, alors le système 3.13 est immédiatement vérifié. □

Lemme 3.2.25. *L'algèbre $X = W + i_X W$ est une algèbre à composition associative et commutative si et seulement si W est une algèbre à composition associative, commutative dont la conjugaison est triviale, c'est-à-dire $\bar{z} = z$ pour tout $z \in W$.*

Démonstration. L'algèbre $W+i_X W$ est une algèbre à composition commutative (et associative) si et seulement si pour tous $a, b, c, d \in W$

$$(a + i_X b)(c + i_X d) = (c + i_X d)(a + i_X b).$$

En utilisant le produit tel que défini à la proposition 3.2.22, cette condition est équivalente à demander que

$$(ac - d\bar{b}) + i_X(cb + \bar{a}d) = (ca - b\bar{d}) + i_X(ad + \bar{c}b)$$

ou encore, à ce que le système ci-dessous soit vérifié pour tous $a, b, c, d \in W$

$$\left\{\begin{array}{rcl}ac-d\bar{b} & = & ca-b\bar{d}\\ cb+\bar{a}d & = & ad+\bar{c}b.\end{array}\right. \tag{3.14}$$

Cela doit en particulier être vrai lorsque que nous supposons $b = 0$ et $d = 1$. Dans ce cas, le système considéré est ramené au système

$$\left\{\begin{array}{rcl}ac & = & ca\\ \bar{a} & = & a,\end{array}\right.$$

et on en tire que l'algèbre W est commutative et la conjugaison qui la muni est triviale. À l'inverse, si W est une algèbre commutative, associative et si la conjugaison dont elle est munie est triviale, le système 3.14 est automatiquement vérifié. □

Nous sommes maintenant en mesure de démontrer le théorème d'Hurwitz classique. Sa généralisation aux algèbres à composition quelconques suivra.

Théoreme 3.2.26 (Hurwitz)**.** *Si Z est une algèbre à composition avec unité, alors $Z = \mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$.*

Démonstration. Puisque Z est une algèbre à composition avec unité contenant $\mathbb{R}$, alors soit $Z = \mathbb{R}$, soit $\mathbb{R} \subset Z$. Si nous sommes dans le second cas alors Z contient son double de Dickson $\mathbb{R} + i_{\mathbb{C}}\,\mathbb{R} = \mathbb{C}$ qui est une algèbre à composition. A nouveau, soit $Z = \mathbb{C}$ soit $\mathbb{C} \subset Z$ et dans ce cas l'algèbre Z contient son double de Dickson $\mathbb{C} + i_{\mathbb{H}}\,\mathbb{C} = \mathbb{H}$ où, comme nous l'avons montré, $\mathbb{H}$ est une algèbre à composition. Une fois de plus, soit $Z = \mathbb{H}$, soit $\mathbb{H} \subset Z$ auquel cas l'algèbre à composition $\mathbb{H} + i_{\mathbb{O}}\,\mathbb{H} = \mathbb{O}$ est incluse dans Z. Finalement, il reste l'unique possibilité $Z = \mathbb{O}$ puisque le double de Dickson de l'algèbre des octonions n'est plus une algèbre à composition étant donné que la multiplication sur $\mathbb{O}$ n'est pas associative. En conclusion, $Z = \mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$. □

Le cas où Z ne possède pas d'unité demande une attention plus particulière et il nécessite notamment plusieurs résultats intermédiaires. Ainsi, dans la suite de cette section, nous supposerons, sauf mention contraire, que Z désigne une algèbre à composition quelconque sur $\mathbb{R}$, autrement dit qui n'est pas nécessairement munie d'une unité. Supposons également que Z admet la forme quadratique non-dégénérée Q, définie comme au début de ce chapitre.

Définition 3.2.27. Soit u un vecteur de norme 1 sur Z. On définit la multiplication à droite par u

$$a : Z \to Z : x \mapsto xu,$$

et la multiplication à gauche par u

$$b : Z \to Z : y \mapsto uy.$$

Proposition 3.2.28. *Les applications a et b sont des isométries linéaires.*

Démonstration. Le produit définit sur Z étant bilinéaire, les deux applications sont nécessairement linéaires. En effet, si on considère $x, y \in Z$ et $\lambda \in \mathbb{R}$ alors on a

$$a(\lambda x) = (\lambda x)u = \lambda(xu) = \lambda a(x) \quad \text{et} \quad a(x+y) = (x+y)u = xu + yu = a(x) + a(y).$$

Aussi, pour tous $x, y \in Z$ on a

$$Q(a(x)) = Q(xu) = Q(x)Q(u) = Q(x) \quad \text{et} \quad Q(b(y)) = Q(uy) = Q(u)Q(y) = Q(y).$$

Donc les applications a et b sont des isométries. □

Proposition 3.2.29. *Si les applications a et b préservent la forme quadratique Q au signe près, il en est de même pour la forme bilinéaire B associée à la forme quadratique.*

Démonstration. Par la proposition 3.2.7 on sait que pour tous $x, y \in Z$ on a

$$B(x, y) = \frac{Q(x+y) - Q(x) - Q(y)}{2}.$$

Si a est une application linéaire telle que $Q(a(x)) = \pm Q(x)$ pour tous $x \in Z$, alors

$$\begin{aligned}
B(a(x), a(y)) &= \frac{1}{2}(Q(a(x) + a(y)) - Q(a(x)) - Q(a(y))) \\
&= \frac{1}{2}(Q(a(x+y)) - Q(a(x)) - Q(a(y))) \\
&= \frac{1}{2}(\pm Q(x+y) \mp Q(x) \mp Q(y)) \\
&= \pm B(x, y).
\end{aligned}$$

De plus, si $B(a(x), a(y)) = 0$ pour tout $y \in Z$ alors, $B(x, y) = 0$ pour tout $y \in Z$ vu l'égalité ci-dessus. Nous pouvons procéder de façon similaire pour montrer que si $Q(b(y)) = \pm Q(y)$ pour tous $y \in Z$, alors $B(b(x), b(y)) = \pm B(x, y)$. □

Corollaire 3.2.30. *Les applications a et b sont des bijections.*

Démonstration. Montrons l'injectivité. Supposons que $a(x) = 0$ et montrons que $x = 0$. Nous ferons de même pour l'application b. Si $a(x) = 0$ alors, $B(a(x), a(y)) = 0$ pour tout $y \in Z$. Dès lors, puisque l'application a préserve la forme bilinéaire il s'en suit que $B(x, y) = 0$ pour tout $y \in Z$ ce qui implique finalement $x = 0$.
De même, si $b(y) = 0$ alors $B(b(x), b(y)) = 0$ pour tout $x \in Z$ ou encore $B(x, y) = 0$ pour tout $x \in Z$. En conséquence, $y = 0$. Nous en concluons donc que les deux applications considérées sont injectives. Aussi, puisque $Im(a) \subset Z$ et que $\dim(Im(a)) = \dim(Z)$ (par injectivité de a) alors l'application a est surjective. Il en est de même pour b. □

En vue de démontrer le théorème d'Hurwitz généralisé, c'est-à-dire lorsque l'algèbre Z est une algèbre à composition quelconque, nous avons besoin d'introduire une nouvelle opération. Suivant Conway, nous posons la définition suivante.

Définition 3.2.31. On note α l'application a^{-1} et β l'application b^{-1}. On définit sur Z la multiplication $\star$ définie par

$$\star : Z \times Z \to Z : (x, y) \mapsto x \star y = \alpha(x)\beta(y).$$

Cette définition nous amène à la proposition suivante

Proposition 3.2.32. *Si* $(Z, \cdot, Q)$ *est une algèbre à composition, alors* $(Z, \star, Q)$ *est une algèbre à composition avec unité.*

Démonstration. Considérons $x, y, z \in Z$ et $\lambda, \mu \in \mathbb{R}$. On a

$$(x + y) \star z = \alpha(x + y)\beta(z) = (\alpha(x) + \alpha(y))\beta(z) = \alpha(x)\beta(z) + \alpha(y)\beta(z) = x \star z + y \star z,$$

puisque α et β sont linéaires. Pour les mêmes raisons, on a

$$x \star (y + z) = \alpha(x)\beta(y + z) = \alpha(x)(\beta(y) + \beta(z)) = \alpha(x)\beta(y) + \alpha(x)\beta(z) = x \star y + x \star z.$$

Finalement, puisque

$$(\lambda x) \star (\mu y) = \alpha(\lambda x)\beta(\mu y) = (\lambda\alpha(x))(\mu\beta(y)) = \lambda\mu(\alpha(x)\beta(y)) = \lambda\mu(x \star y),$$

on en conclut que $(Z, \star, Q)$ est une algèbre. Ensuite, montrons que l'algèbre est à composition. Tout d'abord, montrons que les applications α et β préservent la forme quadratique Q. Pour tout $x \in Z$, on a

$$Q(\alpha(a(x)) = Q(x) = Q(a(x))$$

étant donné que α est l'application inverse de a et que a préserve la forme quadratique. Ainsi α préserve la forme quadratique. Par un raisonnement similaire, on montre que β est une application qui préserve la forme quadratique. Ainsi, nous avons

$$Q(x \star y) = Q(\alpha(x)\beta(y)) = Q(\alpha(x))Q(\beta(y)) = Q(x)Q(y),$$

et ainsi la loi de composition est satisfaite. Finalement, montrons que l'algèbre à composition ainsi obtenue possède une unité donnée par u^2. D'une part on a,

$$u^2 \star b(y) = (uu) \star b(y) = \alpha(uu)\beta(b(y)) = \alpha(a(u))\beta(b(y)) = uy = b(y),$$

ce qui implique que u^2 est une unité à gauche puisque b est surjectif. Et d'autre part, on a

$$a(x) \star u^2 = a(x) \star (uu) = \alpha(a(x))\beta(b(u)) = xu = a(x),$$

et comme a est une application surjective alors cela implique que u^2 est une unité à droite. Finalement, u^2 est une unité, d'où la conclusion. $\square$

Afin de pouvoir démontrer le théorème d'Hurwitz dans le cas général, nous avons besoin d'introduire la notion d'isotopie. Les définitions suivantes sont issues de l'article intitulé *Central Isotopes of* $(-1, 1)$-*Algebras* que l'on retrouve à la référence [20].

Définition 3.2.33. Deux algèbres A et B sont dites isotopes s'il existe un triplet d'isomorphismes linéaires $(\alpha, \beta, \gamma) : A \to B$ tel que

$$\alpha(x)\beta(y) = \gamma(xy)$$

pour tous $x, y \in A$. Dans ce cas, on dit que le triplet (α, β, γ) est une isotopie.

Remarque 3.2.34. L'isotopie est une notion plus large que la notion d'isomorphisme. Il s'agit d'une relation.

Définition 3.2.35. Soient $\alpha, \beta : A \to A$ deux applications linéaires inversibles. On définit l'algèbre $A_\star = (A, +, \star)$ avec le produit

$$x \star y = \alpha(x)\beta(y),$$

où le produit $\alpha(x)\beta(y)$ désigne le produit sur A. Alors, on dit que $A_\star$ est l'isotope principal de A.

Théoreme 3.2.36 (Hurwitz généralisé)**.** *Si A est une algèbre à composition quelconque, alors A est isotope à $\mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$.*

Démonstration. La preuve découle de la proposition 3.2.32 ainsi que des définitions ci-dessus. Effectivement, étant donné une algèbre à composition quelconque A, on définit une algèbre à composition avec unité $A_\star = (A, \star, Q)$. De plus, par la définition 3.2.35, on sait que $A_\star$ est l'isotope principal de A donc en particulier A et $A_\star$ sont isotopes. Or, par le théorème d'Hurwitz 3.2.26 on sait que $A_\star$ est l'une des quatre algèbres à composition $\mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$. Par conséquent, l'algèbre à composition quelconque A est une algèbre isotope à $\mathbb{R}, \mathbb{C}, \mathbb{H}$ ou $\mathbb{O}$, d'où la conclusion. $\square$

Chapitre 4

Pour aller plus loin : aspect géométrique des algèbres $\mathbb{R}, \mathbb{C}, \mathbb{H}$ et $\mathbb{O}$

Dans le présent chapitre nous reprenons des résultats du livre *On Quaternions and Octonions* de Conway et de l'écrit de Taylor intitulé *The octonions*. Pour les lecteurs intéressés par le sujet, les bibliographies complètes sont disponibles aux références [13] et [23] respectivement.

4.1 Groupes d'isométries

Dans cette section, nous montrons comment les nombres complexes et les quaternions permettent de décrire les isométries en dimension $2, 3$ et 4. Avant cela, rappelons la définition des isométries et les premières propriétés.

Définition 4.1.1. Une application linéaire A sur $\mathbb{R}^n$ est une isométrie si elle préserve la norme, c'est-à-dire si

$$|Ax| = |x|$$

pour tout $x \in \mathbb{R}^n$.

Ici, la norme est la norme standard de $\mathbb{R}^n$, qui est associée au produit scalaire standard. La formule de polarisation classique

$$\langle x, y \rangle = \frac{|x+y|^2 - |x|^2 - |y|^2}{2}$$

ou encore la formule

$$\langle x, y \rangle = \frac{|x+y|^2 - |x-y|^2}{4}$$

montrent que toute isométrie préserve le produit scalaire. En effet, une application linéaire A est une isométrie si et seulement si

$$\langle Ax, Ay \rangle = \langle x, y \rangle.$$

Parmi les isométries, on compte les symétries orthogonales par rapport à des hyperplans (vectoriels).

Définition 4.1.2. Si N est un vecteur non nul, que l'on peut supposer normé, alors l'hyperplan normal à N est

$$\pi = \{x \in \mathbb{R}^n : \langle N, x \rangle = 0\}.$$

Tout vecteur $x \in \mathbb{R}^n$ se décompose de manière unique en

$$x = x_\pi + x_N,$$

où $x_\pi \in \pi$ et $x_N \in \rangle N \langle$. Alors, on dit que x_π est la projection orthogonale de x sur π et on note $p_\pi(x)$. Enfin, le symétrique de x par rapport à π est $s_\pi(x) = 2p_\pi(x) - x$.

Il est aisé de calculer $p_\pi(x)$ et $s_\pi(x)$ en utilisant le produit scalaire.

Proposition 4.1.3. *On a*

$$p_\pi(x) = x - \frac{\langle x, N\rangle}{|N|^2}N \qquad et \qquad s_\pi(x) = x - 2\frac{\langle x, N\rangle}{|N|^2}N$$

pour tout $x \in \mathbb{R}^n$.

Démonstration. On a évidemment

$$x = x - \frac{\langle x, N\rangle}{|N|^2}N + \frac{\langle x, N\rangle}{|N|^2}N,$$

où le dernier terme est multiple de N.
Il nous reste à montrer que le terme $x - \frac{\langle x,N\rangle}{|N|^2}N$ appartient à π, c'est à dire qu'il est orthogonal à N. Mais, par linéarité on a

$$\langle x - \frac{\langle x, N\rangle}{|N|^2}N, N\rangle = \langle x, N\rangle - \frac{\langle x, N\rangle}{|N|^2}|N|^2 = 0,$$

ce qui suffit. Enfin, on calcule $s_\pi(x)$. On a

$$s_\pi(x) = 2p_\pi(x) - x = 2x - 2\frac{\langle x, N\rangle}{|N|^2}N - x = x - 2\frac{\langle x, N\rangle}{|N|^2}N,$$

ce qui termine la preuve. □

Montrons maintenant la propriété fondamentale des symétries.

Proposition 4.1.4. *Pour tout hyperplan π, l'application s_π est une isométrie.*

Démonstration. Montrons en premier lieu que s_π est linéaire. Puisque $s_\pi = 2p_\pi - Id$ où l'application identité Id est linéaire, il suffit de montrer que p_π est linéaire. Mais c'est le cas car pour tous $x, x' \in \mathbb{R}^n$ et tout $\lambda \in \mathbb{R}$ on a

$$p_\pi(x + x') = (x + x') - \frac{\langle x + x', N\rangle}{|N|^2}N = x + x' - \frac{\langle x, N\rangle + \langle x', N\rangle}{|N|^2}N = p_\pi(x) + p_\pi(x'),$$

et

$$p_\pi(\lambda x) = (\lambda x) - \frac{\langle \lambda x, N\rangle}{|N|^2}N = \lambda(x - \frac{\langle x, N\rangle}{|N|^2}N) = \lambda p_\pi(x).$$

Il nous faut désormais montrer que s_π préserve la norme, autrement dit que $|s_\pi(x)| = |x|$ pour tout $x \in \mathbb{R}^n$. Pour ce faire, notons que pour tout $x \in \mathbb{R}^n$, on a

$$x = p_\pi(x) + \frac{\langle x, N\rangle}{|N|^2}N$$

et

$$s_\pi(x) = p_\pi(x) - \frac{\langle x, N\rangle}{|N|^2}N$$

où dans chacun des cas les deux termes sont orthogonaux. On a donc

$$|x|^2 = |p_\pi(x)|^2 + \frac{|\langle x, N\rangle|}{|N|^2}|N| = |s_\pi(x)|^2,$$

d'où la conclusion. □

Nous allons désormais démontrer que ces symétries forment les blocs de base du groupe des isométries. Le résultat principal repose sur le lemme suivant.

Lemme 4.1.5. *Si α est une isométrie qui fixe les éléments d'un sous-espace vectoriel V et si $\alpha(u) \neq u$, il existe une symétrie orthogonale s telle que $s \circ \alpha$ fixe les éléments de $V \oplus \rangle u \langle$.*

Démonstration. Soit $N = \alpha(u) - u$. Notons s la symétrie par rapport au plan π orthogonal à N. Si $x \in V$, alors

$$\langle N, x \rangle = \langle \alpha(u) - u, x \rangle = \langle \alpha(u), x \rangle - \langle u, x \rangle.$$

Or, puisque α fixe les éléments de V, alors $\alpha(x) = x$ et on a

$$\langle N, x \rangle = \langle \alpha(u), \alpha(x) \rangle - \langle u, x \rangle = 0$$

car α est une isométrie donc elle préserve le produit scalaire.
Alors, pour $x \in V$, étant donné la proposition 4.1.3 et puisque $\langle N, x \rangle = 0$, on a $s(x) = x$ donc $s \circ \alpha(x) = x$ puisque α fixe les éléments de V. Par conséquent, $s \circ \alpha$ fixe les éléments de V.
Montrons que $s \circ \alpha$ fixe également les éléments de $\rangle u \langle$. On a

$$s \circ \alpha(u) = \alpha(u) - 2\frac{\langle \alpha(u), \alpha(u) - u \rangle}{|\alpha(u) - u|^2}(\alpha(u) - u).$$

Or, on a

$$\begin{aligned}
\langle \alpha(u), \alpha(u) - u \rangle &= \langle \alpha(u), \alpha(u) \rangle - \langle \alpha(u), u \rangle \\
&= \langle u, u \rangle - \langle \alpha(u), u \rangle \\
&= \langle u - \alpha(u), u \rangle \\
&= \langle u, u - \alpha(u) \rangle \\
&= \langle -u, \alpha(u) - u \rangle.
\end{aligned}$$

Donc

$$\begin{aligned}
2\langle \alpha(u), \alpha(u) - u \rangle &= \langle \alpha(u), \alpha(u) - u \rangle + \langle \alpha(u), \alpha(u) - u \rangle \\
&= \langle \alpha(u), \alpha(u) - u \rangle + \langle -u, \alpha(u) - u \rangle \\
&= \langle \alpha(u) - u, \alpha(u) - u \rangle,
\end{aligned}$$

et finalement

$$s \circ \alpha(u) = \alpha(u) - \frac{\langle \alpha(u) - u, \alpha(u) - u \rangle}{|\alpha(u) - u|^2}(\alpha(u) - u) = \alpha(u) - (\alpha(u) - u) = u,$$

ce qui permet de dire que les $s \circ \alpha$ préserve les éléments de $V \oplus \rangle u \langle$ comme souhaité. □

On peut maintenant démontrer le résultat fondamental.

Théoreme 4.1.6. *Si $f : \mathbb{R}^n \to \mathbb{R}^n$ est une isométrie qui fixe les points d'un sous-espace vectoriel de dimension k, alors f est le produit d'au plus $n - k$ symétries par rapport à des hyperplans.*

Démonstration. En appliquant au plus $n - k$ fois le lemme précédent, on obtient des symétries $\sigma_1, ..., \sigma_{n-k}$ telles que $g = \sigma_{n-k} \circ ... \circ \sigma_1 \circ f$ fixe les éléments d'un sous-espace de dimension n. Comme g fixe tous les points de l'espace, alors g est l'identité, et

$$f = \sigma_1 \circ ... \circ \sigma_{n-k},$$

ce qui suffit pour conclure cette preuve. □

Rappelons que le déterminant d'une application linéaire sur $\mathbb{R}^n$ est le déterminant de sa représentation dans toute base, et celui-ci est indépendant de la base. On appelle application positive (resp. négative) une application dont le déterminant est positif (resp. négatif). On continue en rappelant la définition suivante.

Définition 4.1.7. Le groupe des isométries de $\mathbb{R}^n$ est noté $O(n)$. Le sous-groupe des isométries positives est noté $SO(n)$.

Définition 4.1.8. On appelle rotation toute isométrie positive. Dans $\mathbb{R}^n$, on appelle rotation simple toute rotation qui fixe les éléments d'un sous-espace de dimension $n-2$ (au moins).

En dimension 2, toutes les rotations sont simples par définition. En dimension 3, c'est en fait un théorème, qui peut se montrer facilement à l'aide de l'algèbre linéaire, mais que nous allons montrer à l'aide du résultat précédent.

Lemme 4.1.9. *La composée de deux symétries orthogonales par rapport à des hyperplans est une rotation simple.*

Démonstration. Considérons les symétries orthogonales s_1 et s_2 par rapport à π_1 et π_2 respectivement. Alors l'application $s_2 \circ s_1$ est une isométrie car c'est une composée de symétries. Elle est positive car s_1 et s_2 sont négatives. Enfin, elle fixe les éléments de $\pi_1 \cap \pi_2$ puisque, par définition d'une symétrie orthogonale, s_1 fixe les éléments de π_1 et s_2 fixes ceux de π_2. Mais, si on note n la dimension de l'espace, on a

$$\dim(\pi_1 \cap \pi_2) = \dim(\pi_1) + \dim(\pi_2) - \dim(\pi_1 + \pi_2) \geqslant \dim(\pi_1) + \dim(\pi_2) - n \geqslant n - 2,$$

étant donné que $\dim(\pi_1) = \dim(\pi_2) = n - 1$ et que $\dim(\pi_1 + \pi_2) \leq n$. Donc $s_2 \circ s_1$ est une isométrie positive qui fixe tous les éléments d'un sous-espace de dimension supérieure ou égale à $n - 2$. Il s'agit donc, par définition, d'une rotation simple. □

Le théorème 4.1.6 admet donc le corollaire suivant.

Corollaire 4.1.10. *Dans $\mathbb{R}^3$, toutes les rotations sont simples. De manière générale, le groupe $SO(n)$ est engendré par les rotations simples.*

Démonstration. Nous avons montré que tout élément de $SO(3)$ est le produit d'au plus trois symétries orthogonales. Or, $SO(3)$ est le sous-groupe des isométries positives de $\mathbb{R}^3$, ainsi étant donné qu'une symétrie orthogonale est une isométrie négative, $SO(3)$ ne peut être ni un produit à un facteur, ni à trois facteurs. Cela ne peut donc être que le produit de deux symétries orthogonales, et on conclut par le lemme 4.1.9. Le cas général se traite de la même façon : tout élément A de $SO(n)$ est une composée de symétries orthogonales. Le nombre de facteurs doit être pair, et en groupant les symétries par deux, on obtient des rotations simples, donc A est un produit de rotations simples. □

4.1.1 Isométries en dimension 2

Nous pouvons utiliser le théorème 4.1.6 ainsi que les nombres complexes pour décrire les isométries de $\mathbb{R}^2$. Cela peut également se faire à la main, sans aucune théorie. C'est cela que nous ferons ici.
Pour tout $z \in \mathbb{C}$, notons L_z la multiplication à gauche par z. Il s'agit d'une application $\mathbb{R}$-linéaire sur $\mathbb{C}$, identifié à $\mathbb{R}^2$. Cela donne des exemples d'isométries.

Définition 4.1.11. L'opération de conjugaison définie sur les complexes est l'opération $K_\mathbb{C} : \mathbb{C} \to \mathbb{C} : z \mapsto \bar{z}$.

Proposition 4.1.12. *Pour tout $u \in \mathbb{C}$ tel que $|u| = 1$, L_u est une isométrie positive. De même, la conjugaison $K_{\mathbb{C}}$ est une isométrie négative.*

Démonstration. Pour tout $z \in \mathbb{C}$, on a

$$|L_u z| = |uz| = |u||z| = |z|$$

puisque u est de norme égale à 1, ce qui nous permet de dire que L_u est une isométrie. On a aussi, sous l'hypothèse que $u = a + ib$,

$$|\bar{u}| = |a - ib| = \sqrt{a^2 + b^2} = |u|.$$

Dans la base $(1, i)$ de $\mathbb{C}$, l'application L_u se représente par la matrice

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

et elle est à déterminant positif. Il s'agit donc bien d'une application positive. Enfin, dans cette base, l'application K se représente par

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

et le déterminant de cette matrice est négatif. □

Remarquons que la conjugaison est une symétrie orthogonale par rapport à l'axe réel. En effet, si $z = a + ib \in \mathbb{C}$, alors la projection de z sur $\mathbb{R}$ est a et le symétrique est $2a - z = a - ib$. Passons maintenant à la caractérisation des isométries de $\mathbb{R}^2$, à l'aide des nombres complexes.

Théoreme 4.1.13. *Toute isométrie de $\mathbb{R}^2$ s'écrit de manière unique L_u ou $L_u \circ K_{\mathbb{C}}$, où u est un nombre complexe de module égal à* 1.

Démonstration. Démontrons en premier lieu l'unicité. Il y a alors trois cas à considérer.
Pour le premier cas, supposons que $L_u = L_{u'}$. Dans ce cas, on a en particulier $L_u(1) = L_{u'}(1)$ et donc $u1 = u'1$ par définition de L_u et $L_{u'}$. On en conclut donc que $u = u'$.
Pour le second cas, supposons que $L_u \circ K_{\mathbb{C}} = L_{u'} \circ K_{\mathbb{C}}$. On a alors $L_u(K_{\mathbb{C}}(1)) = L_{u'}(K_{\mathbb{C}}(1))$ ou encore $L_u(1) = L_{u'}(1)$ étant donné que le $K_{\mathbb{C}}(1) = 1$. On conclut alors que $u = u'$ comme pour le cas précédent.
Pour le dernier cas, supposons désormais que $L_u = L_{u'} \circ K_{\mathbb{C}}$. De la même façon que précédemment, nous trouvons que $u = u'$. Or, dans ce cas on a $L_u = L_u \circ K_{\mathbb{C}}$ et donc en particulier $L_u(i) = L_u \circ K_{\mathbb{C}}(i) = L_u(-i) = -L_u(i)$ puisque la multiplication à gauche est une application linéaire. Ainsi, cela nous donne $ui = 0$, et donc $u = 0$ ce qui contredit l'hypothèse. Ce troisième cas est donc impossible d'où l'unicité.
Démontrons ensuite l'existence. Si I est une isométrie et si nous définissons $u = I(1)$, alors u est de norme 1 et l'isométrie $L_{u^{-1}} \circ I = L_{\bar{u}} \circ I$ fixe 1. En effet, on a

$$L_{u^{-1}} \circ I(1) = L_{u^{-1}}(I(1)) = L_{u^{-1}} u = u^{-1} u = 1.$$

Si elle fixe i, c'est l'identité puisqu'elle fixe les deux éléments de la base standard de $\mathbb{C}$. Donc $L_{u^{-1}} \circ I = id$ ou encore $I = L_u$. En revanche, si elle ne fixe pas le nombre complexe i, alors puisque $L_{u^{-1}} \circ I$ est une isométrie, on a

$$|L_{u^{-1}} \circ I(i)| = |i| = 1 \quad \text{ et } \quad \langle L_{u^{-1}} \circ I(i), L_{u^{-1}} \circ I(1) \rangle = \langle i, 1 \rangle = 0.$$

Donc, soit on a $L_{u^{-1}} \circ I(i) = i$, soit on a $L_{u^{-1}} \circ I(i) = -i$, mais comme par hypothèse, la symétrie ne fixe pas i alors nous sommes dans le second cas. Puisque $K_{\mathbb{C}} \circ L_{u^{-1}} \circ I$ fixe 1 et i, alors $K_{\mathbb{C}} \circ L_{u^{-1}} \circ I = id$, et par conséquent $I = L_u \circ K_{\mathbb{C}}$ d'où la conclusion. □

Le théorème 4.1.6 admet l'interprétation suivante, qui caractérise les groupes orthogonaux.

Proposition 4.1.14. *Le groupe $SO(2)$ est isomorphe au groupe S^1 des nombres complexes de module 1. Le groupe $O(2)$ est l'union disjointe de deux copies de $SO(2)$.*

Démonstration. On peut vérifier que l'application qui à tout $u \in S^1$ associe L_u est un isomorphisme de groupes. L'assertion sur $O(2)$ découle directement du théorème 4.1.13. En effet, ce théorème et la définition 4.1.7 nous indiquent que $O(2) = \{L_u : u \in S^1\} \cup \{K_{\mathbb{C}} \circ L_u : u \in S^1\}$. Or, ces deux ensembles sont en bijection avec le groupe S^1 qui est lui-même isomorphe au groupe $SO(2)$. Ainsi, $O(2)$ est bel et bien une union disjointe de deux copies de $SO(2)$. □

4.1.2 Isométries en dimension 3

Passons maintenant à la caractérisation des rotations de $\mathbb{R}^3$ à l'aide des quaternions. Pour obtenir des isométries, on pense naturellement à généraliser ce qui a été fait dans les nombres complexes, en utilisant la multiplication. Ici, on a même le choix, puisqu'on peut multiplier à gauche ou à droite.

Proposition 4.1.15. *Pour tous quaternions non nuls q_1 et q_2, l'application*

$$C_{q_1,q_2} : \mathbb{H} \to \mathbb{H} : q \mapsto q_1 q q_2$$

est une similitude de $\mathbb{H}$ de rapport $|q_1q_2|$. En particulier c'est une isométrie si $|q_1q_2| = 1$.

Démonstration. L'application est linéaire, puisque le produit des quaternions est bilinéaire. Ensuite, il suffit juste de remarquer que l'on a $|q_1qq_2| = |q||q_1q_2|$, et le résultat suit. □

Cependant, même si cette proposition permet d'obtenir beaucoup de rotations, elles n'ont pas de raison de stabiliser un sous-espace de dimension 3, et donc de définir des rotations d'un espace de dimension 3. Si une isométrie stabilise un sous-espace de dimension 3, le complément orthogonal de ce sous-espace est un espace propre. Il est donc naturel de demander qu'une rotation fixe un élément de $\mathbb{H}$ (à un multiple près). On choisit de demander que la rotation fixe l'élément $1 \in \mathbb{H}$ à un multiple près. Mais si on veut que la restriction de cette rotation au sous espace orthogonal à 1 soit une rotation, il faut que l'image de 1 soit 1. C'est le choix le plus simple, et ce n'est pas une restriction. On a alors le résultat suivant.

Proposition 4.1.16. *La rotation C_{q_1,q_2} fixe 1 si et seulement si $q_2 = q_1^{-1}$. Pour tout quaternion non nul $q = a + v_q$, l'application $C_{q,q^{-1}}$ définit une rotation de $Im(\mathbb{H})$, qui fixe v_q.*

Démonstration. La première partie est directe : on a $C_{q_1,q_2}(1) = 1$ si et seulement si $q_1q_2 = 1$. Dans ce cas, puisque $C_{q,q^{-1}}$ fixe 1, elle stabilise son complément orthogonal $Im(\mathbb{H})$. En effet, pour ce faire, il faut montrer que si $u \in Im(\mathbb{H})$, alors $C_{qq^{-1}}(u) \in Im(\mathbb{H})$. Or, comme $u \in Im(\mathbb{H})$ alors $\langle 1, u\rangle = 0$ et comme $C_{qq^{-1}}$ est une isométrie, elle préserve le produit scalaire. Ainsi, on a

$$0 = \langle 1, u\rangle = \langle C_{qq^{-1}}(1), C_{qq^{-1}}(u)\rangle = \langle 1, C_{qq^{-1}}(u)\rangle,$$

et donc $C_{qq^{-1}}(u) \in Im(\mathbb{H})$.
Sa restriction à ce sous espace est encore une isométrie positive. De plus, on sait que q commute avec q et $\overline{q}$, donc il commute avec v_q et on a

$$C_{q,q^{-1}}(v_q) = qv_qq^{-1} = v_qqq^{-1} = v_q.$$

□

Simplifions quelque peu les notations.

Définition 4.1.17. Pour tout quaternion non nul q, on note simplement C_q l'application $C_{q,q^{-1}}$. On note de la même façon la restriction à $Im(\mathbb{H})$. On note encore C l'application qui à tout quaternion non nul associe l'isométrie C_q de $Im(\mathbb{H})$.

L'application C définie ci-dessus a les propriétés qui nous intéressent. Dans la proposition suivante, nous identifions l'ensemble des isométries positives de $Im(\mathbb{H})$ à $SO(3)$.

Proposition 4.1.18. *L'application C définit un homomorphisme surjectif de $\mathbb{H} \setminus \{0\}$ dans $SO(3)$. Son noyau est $\mathbb{R}_0$.*

Démonstration. Pour la première assertion, on note que $C(1) = C_1$ est la transformation identique, et que

$$C_{q_1} \circ C_{q_2}(x) = q_1(q_2 x q_2^{-1})q_1^{-1} = (q_1 q_2)x(q_1 q_2)^{-1} = C_{q_1 q_2}(x),$$

pour tout $x \in Im(\mathbb{H})$.

Passons maintenant à la surjectivité. Soit I un élément de $SO(3)$. Nous avons démontré au corollaire 4.1.10 que I admet un vecteur propre u (non nul) et de valeur propre 1, que l'on peut supposer normé. Soit v un vecteur normé orthogonal à u et $w = u \wedge v$ (donc normé lui aussi). Puisque I est une isométrie dont u est un vecteur propre, elle stabilise le sous-espace orthogonal à u, c'est-à-dire l'enveloppe linéaire de v et w. Puisque v est un vecteur normé, $I(v)$ l'est aussi. En effet, cela découle du fait que I soit une isométrie, on a alors $|I(v)| = |v| = 1$. Ainsi, il existe $\theta \in \mathbb{R}$ tel que

$$I(v) = \cos(\theta)v + \sin(\theta)w.$$

La relation $w = u \wedge v$ implique alors $I(w) = I(u) \wedge I(v)$ (car I est une isométrie positive, donc elle préserve le produit vectoriel). On a donc

$$I(w) = u \wedge (\cos(\theta)v + \sin(\theta)w) = \cos(\theta)w - \sin(\theta)v,$$

où on a utilisé la formule du double produit vectoriel à la dernière égalité.

Il est clair que I est complètement déterminé par les images de u, v, w. Puisque u est fixe, vu la proposition 4.1.16, il est naturel d'analyser les transformations C_q pour $q = a + u$, où a est réel, ou plus généralement pour $q = ra + ru = a' + ru$ où r est réel, puisque les rotations associées à q ou à un multiple sont égales. Pour simplifier le calcul, on peut même considérer q normé, c'est-à-dire de la forme

$$q = \cos(\alpha) + \sin(\alpha)u \tag{4.1}$$

pour $\alpha \in \mathbb{R}$. On va dès à présent montrer que toute isométrie positive s'écrit comme C_q, donc C_q est une application surjective. Selon les conditions dans lesquelles nous nous trouvons, nous avons déjà démontré l'égalité $C_q(u) = u = I(u)$ (cf. 4.1.16). Il reste à calculer $C_q(v)$ et $C_q(w)$. On calcule $C_q(v)$ en tenant compte du fait que le produit est bilinéaire et on a

$$\begin{aligned} C_q(v) &= (\cos(\alpha) + \sin(\alpha)u)v(\cos(\alpha) - \sin(\alpha)u) \\ &= \cos^2(\alpha)v + \cos(\alpha)\sin(\alpha)(uv - vu) - \sin^2(\alpha)uvu. \end{aligned}$$

On sait par la proposition 2.2.15 que w vaut $\frac{1}{2}(uv - vu)$, et que, puisque u et v sont orthogonaux, on a $uv = u \wedge v = w$. Pour la même raison et en utilisant la formule du double produit vectoriel on a $wu = w \wedge u = v$. Nous obtenons donc

$$C_q(v) = \cos(2\alpha)v + \sin(2\alpha)w.$$

En choisissant $\alpha = \frac{\theta}{2}$, on obtient $C_q(v) = I(v)$. Dans ce cas, puisque I et C_q préservent le produit vectoriel, on a aussi $C_q(w) = I(w)$, donc $I = C_q$.

Calculons maintenant le noyau de C. On sait déjà que si q est un réel non nul, alors C_q est l'identité. Il reste à montrer la réciproque. Sans perte de généralité, on peut supposer que q est normé, et qu'il n'est pas réel, sinon il n'y a rien à démontrer. Alors il s'écrit comme en 4.1. Le calcul de $C_q(v)$ ci-dessus impose $\sin(2\alpha) = 0$ et $\cos(2\alpha) = 1$, puisque $C_q(v) = v$ étant donné que C_q est l'identité. On a donc $2\alpha = 2k\pi$ ($k \in \mathbb{Z}$). Et ainsi, $\alpha = k\pi$ et $q = \cos(\alpha)+\sin(\alpha)u = \cos(\alpha)$ est réel, une absurdité puisqu'il a été supposé qu'il n'était pas réel. Par conséquent, q doit être un réel non nul. □

On applique alors le premier théorème d'isomorphie qui, rappelons-le, s'énonce comme suit.

Théoreme 4.1.19 (Premier théorème d'isomorphie)**.** *Si f est un homomorphisme de G dans G', où G et G' sont deux groupes, alors f induit un isomorphisme de $G/\ker(f)$ dans $Im(f)$.*

Proposition 4.1.20. *Les groupes $\mathbb{H} \setminus \{0\}/\mathbb{R}_0$ et $SO(3)$ sont isomorphes.*

Démonstration. C'est une application directe du premier théorème d'isomorphie pour les groupes. □

On peut encore obtenir un résultat similaire pour la sphère unité de $\mathbb{H}$. Nous notons cette sphère S^3. On a le résultat suivant.

Proposition 4.1.21. *La sphère S^3 est un sous-groupe de $\mathbb{H} \setminus \{0\}$.*

Démonstration. On sait que $S^3 = \{q \in \mathbb{H} : |q| = 1\}$. Dès lors, les trois conditions qui font de S^3 un sous-groupe sont vérifiées.
Tout d'abord, 1 appartient à S^3. Ensuite, si $q_1, q_2 \in S^3$ alors le produit q_1q_2 est un quaternion et il vérifie

$$|q_1q_2| = |q_1||q_2| = 1$$

puisque $\mathbb{H}$ est une algèbre à composition. Enfin, si q est normé, alors $q^{-1} = \overline{q}$ est aussi normé, donc on a $q^{-1} \in S^3$ d'où la conclusion. □

Les résultats ci-dessus s'adaptent directement, puisque l'application C a la propriété $C(\lambda q) = C(q)$, pour tout $\lambda \in \mathbb{R}_0$ et tout $q \in \mathbb{H} \setminus \{0\}$. Effectivement, pour tout x on a

$$C_{\lambda q}(x) = (\lambda q)x(\lambda q)^{-1} = \lambda q x q^{-1}\lambda^{-1} = \lambda\lambda^{-1}qxq^{-1} = qxq^{-1} = C_q(x).$$

Introduisons une dernière définition.

Définition 4.1.22. Nous notons C' la restriction de C à S^3.

Nous avons alors le résultat suivant.

Proposition 4.1.23. *L'application C' définit un homomorphisme surjectif de S^3 dans $SO(3)$. Son noyau est $\{-1; 1\}$. En conséquence, les groupes $S^3/\{-1; 1\}$ et $SO(3)$ sont isomorphes.*

Terminons cette section sur les rotations en dimension 3 en donnant une autre version de S^3. Nous avons déjà rencontré un isomorphisme entre les quaternions et une sous-algèbre de matrices. Rappelons la définition suivante.

Définition 4.1.24. Le groupe $U(n)$ est l'ensemble des matrices U carrées à coefficients complexes, telles que U^*U est l'identité. Le groupe $SU(n)$ est l'intersection de $U(n)$ avec l'ensemble des matrices de déterminant 1.

Il est assez simple de décrire $SU(2)$.

Proposition 4.1.25. *Le groupe $SU(2)$ est*

$$\left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} : \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

Démonstration. Considérons une matrice quelconque à coefficients complexes

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

Par définition, les colonnes doivent être normées pour le produit scalaire de $\mathbb{C}^2$. On a donc

$$|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1 \tag{4.2}$$

et

$$a\overline{c} + b\overline{d} = 0. \tag{4.3}$$

La condition 4.3 donne l'existence de $k \in \mathbb{C}$ tel que $(\overline{c}, \overline{d}) = k(-b, a)$, ou $(c, d) = k'(-\overline{b}, \overline{a})$. La condition 4.2 donne $|k'| = 1$, mais puisque le déterminant est égal à 1, on a $1 = ad - bc = k'(|a|^2 + |b|^2)$, donc $k = 1$. Ainsi, la matrice considérée plus haut prend la forme souhaitée

$$\begin{pmatrix} a & -\overline{b} \\ b & \bar{a} \end{pmatrix}.$$

□

Nous avons déjà rencontré une version matricielle de $\mathbb{H}$. Nous utilisons (presque) la même construction pour définir un isomorphisme entre S^3 et $SU(2)$.

Proposition 4.1.26. *L'application*

$$f : S^3 \to SU(2) : (z_1, z_2) \mapsto \begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix}$$

est un isomorphisme de groupes.

Enfin, terminons cette section sur les groupes d'isométries en dimension 3 par une description de $O(3)$.

Proposition 4.1.27. *Le groupe $O(3)$ est, en tant qu'ensemble, l'union de deux copies de $SO(3)$.*

Démonstration. Il suffit de remarquer que si I est une isométrie de $O(3)$, alors est positive ou négative et donc soit I appartient à $SO(3)$ dans le cas où elle est positive, soit $-I$ appartient à $SO(3)$ dans le cas où l'isométrie serait négative. □

4.1.3 Isométries en dimension 4

Passons maintenant à la description des isométries en dimension 4. Nous avons déjà remarqué que dans $\mathbb{H}$, l'application qui à tout quaternion q associe $q_1 q q_2$ est une isométrie si et seulement si $|q_1||q_2| = 1$. L'application transforme donc q en $\frac{q_1}{|q_1|} q \frac{q_2}{|q_2|}$, et il suffit donc de la considérer pour des quaternions unitaires. Nous savons également que la conjugaison qui applique q sur $\overline{q}$ est une isométrie (négative). En composant, on obtient alors les isométries qui à q associent $\frac{q_1}{|q_1|} \overline{q} \frac{q_2}{|q_2|}$. Nous allons démontrer qu'il n'y en a pas d'autre. Plus précisément, on introduit la proposition suivante.

Proposition 4.1.28. *L'application*

$$f : S^3 \times S^3 \to SO(4) : (l, r) \mapsto M_{l,r} : M_{l,r}(q) = lqr^{-1}$$

est un homomorphisme surjectif. Son noyau est $\{(1, 1), (-1, -1)\}$*. Plus généralement, toute isométrie de* $\mathbb{H}$ *est de la forme* $M_{l,r}$ *ou* $M_{l,r} \circ K_{\mathbb{H}}$*, où* $K_{\mathbb{H}}$ *est la conjugaison des quaternions.*

Avant de proposer la preuve de cette proposition, démontrons deux lemmes techniques.

Lemme 4.1.29. *Pour tout quaternion unitaire* q*, les quaternions* q, iq, jq, kq *forment une base orthonormée de* $\mathbb{H}$*.*

Démonstration. Il suffit de noter que $(1, i, j, k)$ est une base orthonormée par définition, et que la multiplication à droite par q est une isométrie. En effet, si on pose $R_q(x)$ la multiplication à droite de x par q, alors R_q est linéaire et pour tout $x \in \mathbb{H}$ on a $|R_q(x)| = |xq| = |x||q| = |x|$ puisque l'algèbre des quaternions est à composition et que q est unitaire. □

Lemme 4.1.30. *Pour tout quaternion unitaire* q*, l'application*

$$M_q : \mathbb{H} \to \mathbb{H} : x \mapsto -q\overline{x}q$$

est la symétrie orthogonale par rapport au plan orthogonal à q*.*

Démonstration. L'application M_q est linéaire puisque le produit sur $\mathbb{H}$ est bilinéaire. Il suffit de montrer que l'image de q est $-q$, et que le plan orthogonal à q est fixé par cette application, autrement dit que M_q fixe tous les éléments du plan orthogonal à q. On calcule $M_q(q) = -q\overline{q}q = -q$, puisque q est unitaire. Le plan orthogonal à q est l'enveloppe linéaire de iq, jq et kq. Nous calculons

$$M_q(uq) = -q\overline{uq}q = -q\overline{q}\,\overline{u}q = -\overline{u}q.$$

Donc M_q fixe les éléments iq, jq et kq, et par linéarité elle fixe tous les éléments du plan, d'où la conclusion. □

Passons maintenant à la preuve du résultat attendu.

Preuve de la proposition 4.1.28. Pour tous quaternions unitaires, l'application $M_{l,r}$ est une isométrie. En effet, $M_{l,r}$ est linéaire puisque le produit sur $\mathbb{H}$ est bilinéaire et on a

$$|M_{l,r}(q)| = |lqr^{-1}| = |l||q||r^{-1}| = |l||q||\bar{r}| = |q|.$$

Montrons que toutes les isométries s'écrivent $M_{l,r}$ ou $M_{l,r} \circ K_{\mathbb{H}}$. Nous savons par le théorème 4.1.6 que toute isométrie est une composée de symétries orthogonales par rapport à des hyperplans. Par le lemme 4.1.30, toutes ces isométries (ces symétries) sont de la forme M_q où q est un quaternion unitaire. Toute isométrie I s'écrit donc $M_{q_n} \circ \cdots \circ M_{q_1}$ pour des quaternions $q_1, \ldots, q_n$ unitaires. On a donc deux cas

1. Si n est pair, alors $M_{q_n} \circ \cdots \circ M_{q_1}(x) = q_n \ldots q_1 x q_1 \ldots q_n$;
2. Si n est impair, alors $M_{q_n} \circ \cdots \circ M_{q_1}(x) = -q_n \ldots q_1 \overline{x} q_1 \ldots q_n$;

Puisque $q_n \ldots q_1$ est unitaire, le premier cas correspond à l'isométrie $M_{l,r}$ tandis que le second cas correspond à l'isométrie $M_{l,r} \circ K_{\mathbb{H}}$. On a donc le résultat annoncé. De plus, puisque les applications M_q sont des symétries orthogonales (donc de déterminant -1), on constate que les éléments de $SO(4)$ correspondent au premier cas, car $M_{q_n} \circ ... \circ M_{q_1}$ n'est une isométrie positive que lorsque n est pair, tandis que les isométries négatives correspondent au deuxième cas. Ainsi, toute isométrie positive s'écrit sous la forme $M_{l,r}$ ce qui nous permet de dire que l'application f est surjective. On montre directement que f est un homomorphisme : d'une part

$$f((l,r).(l',r')) = f(ll',rr') = M_{ll',rr'},$$

et d'autre part pour tout x on a

$$M_{ll',rr'}(x) = ll'x(rr')^{-1} = ll'xr'^{-1}r^{-1} = M_{l,r} \circ M_{l',r'}(x) = f(l,r)f(l'r')(x).$$

On en tire l'égalité espérée, $f((l,r)(l',r')) = f(l,r)f(l',r')$. Montrons désormais que le noyau de l'application est $\{(-1,-1),(1,1)\}$. Rappelons que $\ker(f) = \{(l,r) \in S^3 \times S^3 : f(l,r) = Id\}$. Si $f(l,r)$ est l'application identité, alors elle fixe 1, et on a

$$f(l,r)(1) = 1 \Leftrightarrow l1r^{-1} = 1 \Leftrightarrow l = r.$$

On est alors dans les conditions de la proposition 4.1.18 et on trouve que $l = r$ appartient à $\mathbb{R}_0$. Mais l est unitaire, donc on a $l = \pm 1$. □

Le théorème d'isomorphie pour les groupes donne alors le résultat suivant, où on a posé $1 = (1,1)$ et $-1 = (-1,-1)$.

Proposition 4.1.31. *Le groupe $SO(4)$ est isomorphe à $S^3 \times S^3/\{-1,1\}$, ou à $SU(2) \times SU(2)/\{-1,1\}$.*

4.2 Groupes d'automorphismes

Nous allons maintenant faire apparaître des groupes comme groupes d'automorphismes des algèbres que nous avons définies. Comme nous l'avons dis au début de ce chapitre, nous utilisons principalement la référence [23] à laquelle nous apportons des développements complémentaires et/ou supplémentaires. Commençons directement avec une définition.

Définition 4.2.1. Soit $\mathcal{A}$ une algèbre (sur $\mathbb{R}$). Un automorphisme de $\mathcal{A}$ est une application linéaire inversible $A : \mathcal{A} \to \mathcal{A}$ telle que

$$A(xy) = A(x)A(y) \quad \forall x, y \in \mathcal{A}.$$

On note $Aut(\mathcal{A})$ l'ensemble des automorphismes de $\mathcal{A}$.

L'ensemble des automorphismes d'une algèbre a une structure naturelle.

Proposition 4.2.2. *L'ensemble $Aut(\mathcal{A})$ est un sous-groupe de $GL(\mathcal{A})$.*

Démonstration. Tout d'abord, il est clair que l'identité est un automorphisme. Ensuite, étant donné que si A et B sont deux automorphismes alors $A \circ B$ est une application linéaire qui vérifie

$$A \circ B(xy) = A(B(xy)) = A(B(x)B(y)) = A(B(x))A(B(y)) \quad \forall x, y \in \mathcal{A},$$

on en tire que la composée de deux automorphismes est un automorphisme. Aussi, remarquons que A est injectif puisque si $A(x) = A(y)$ alors comme A est inversible, on a $x = A^{-1}(A(x)) = A^{-1}(A(y)) = y$. Finalement, si A est un automorphisme, alors A^{-1} l'est aussi si, par définition, on a

$$A^{-1}(xy) = A^{-1}(x)A^{-1}(y), \quad \forall x, y \in \mathcal{A}.$$

Puisque A est injectif, cette relation est équivalente à

$$A(A^{-1}(xy)) = A(A^{-1}(x)A^{-1}(y)), \quad \forall x, y \in \mathcal{A}.$$

Cette dernière relation est vraie puisque A est un automorphisme. □

Dans la suite, sauf mention du contraire nous étudions les automorphismes des algèbres à composition $\mathcal{A} = \mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$. On donne également des informations pertinentes sur les automorphismes de l'algèbre à composition $\mathcal{A} = \mathbb{O}$, mais nous n'irons pas jusqu'au bout de la description puisque cela sortirait du cadre fixé par ce mémoire. En effet, l'étude des groupes de Lie serait nécessaire si nous souhaitions montrer que le groupe des automorphismes de l'algèbre des octonions $Aut(\mathbb{O})$ est le plus petit groupe de Lie réel exceptionnel G_2. Le résultat suivant permet directement de traiter le cas de $\mathbb{R}$.

Proposition 4.2.3. *Tout automorphisme d'une algèbre à composition avec unité fixe l'unité.*

Démonstration. Si l'unité est 1, et si A est un automorphisme alors, on a

$$A(1) = A(1.1) = A(1)A(1).$$

Puisque A est inversible, on a $A(1) \neq 0$, alors $A(1)$ est inversible et on a $A(1) = 1$. □

En corollaire, on traite le cas de $\mathbb{R}$.

Corollaire 4.2.4. *Le groupe $Aut(\mathbb{R})$ est réduit à l'identité.*

Démonstration. Pour tout $x \in \mathbb{R}$ et tout automorphisme A, on a par linéarité $A(x) = A(x\,1) = xA(1)$. On conclut alors que $A(x) = x\,1 = x$, donc A est l'identité. □

La proposition 4.2.3 permet aussi de caractériser les automorphismes de $\mathbb{C}$.

Proposition 4.2.5. *Le groupe des automorphismes de $\mathbb{C}$ est $\{\mathrm{Id}, K_{\mathbb{C}}\}$, où $K_{\mathbb{C}}$ est la conjugaison sur $\mathbb{C}$.*

Démonstration. Si A est un automorphisme, on a $A(1) = 1$. Mais on a aussi $A(i)^2 = A(i^2) = A(-1) = -1$ par linéarité de A. Donc $A(i) = i$ ou $A(i) = -i$. Dans le premier cas, A est l'identité, et dans le deuxième c'est la conjugaison. □

Dans la suite, nous continuons principalement avec $\mathcal{A} = \mathbb{H}$ ou $\mathbb{O}$. Nous donnons cependant des résultats de manière générale, quand cela a une utilité propre. Dans chacune des algèbres considérées, on a une décomposition $\mathcal{A} = \mathbb{R}1 \oplus Im(\mathcal{A})$. Dans toutes ces algèbres, on a la caractérisation suivante des éléments réels ou purement imaginaires.

Lemme 4.2.6. *Si $\mathcal{A} \in \{\mathbb{C}, \mathbb{H}, \mathbb{O}\}$, pour tout $u \in \mathcal{A}$, on a $u \in Im(\mathcal{A}) \cup \mathbb{R}1$ si et seulement si u^2 est réel. Plus précisément, on a $u \in Im(\mathcal{A})$ si et seulement si u^2 est réel négatif.*

Démonstration. Dans le cas de $\mathbb{C}$, si $u = a + ib$, où a et b sont réels, alors $u^2 = a^2 - b^2 + 2iab$. Donc u^2 est réel si et seulement si $a = 0$ ou $b = 0$. On constate aussi que si u est réel, alors $u^2 = a^2$ est positif, et que si u est imaginaire, alors $u^2 = -b^2$ est négatif, ce qui règle le cas particulier.
Dans le cas de $\mathbb{H}$, on utilise l'approche vectorielle : si $u = a + v_u$, alors on a

$$u^2 = a^2 - |v_u|^2 + 2av_u + v_u \wedge v_u = a^2 - |v_u|^2 + 2av_u.$$

On constate que u^2 est réel si $a = 0$ ou $v_u = 0$. Ici aussi, si u est réel, alors $u^2 = a^2$ est positif, et si u est imaginaire, alors $a = 0$ et $u^2 = -|v_u|^2$ est négatif.
Enfin, dans le cas de $\mathbb{O}$, on utilise la définition 3.1.6 pour $u = (u_1, u_2)$. On obtient

$$u^2 = (u_1^2 - |u_2|^2, u_2(u_1 + \overline{u_1})).$$

Donc u^2 est réel si et seulement si u_1^2 est réel et $u_2(u_1 + \overline{u_1}) = 0$. Mais u_1^2 est réel si et seulement si u_1 est réel ou imaginaire pur. Si u_1 est réel, la deuxième condition donne $2u_2u_1 = 0$, donc

$u_1 = 0$, ce qui implique que u est dans $Im(\mathbb{O})$, ou $u_2 = 0$, qui implique que u est réel puisque u_1 l'est. Si u_1 est imaginaire pur, alors u l'est aussi. Réciproquement, si u est réel, on a $u_2 = 0$ et u_1 est un quaternion réel, donc $u^2 = u_1^2$ est un réel positif, et si u est imaginaire, alors u_1 est imaginaire, donc $u_1 + \overline{u_1}$ est nul, et u_1^2 est réel négatif par le cas précédent, donc u est réel négatif.

□

Remarque 4.2.7. La proposition précédente peut encore être précisée : pour $u \in Im(\mathcal{A})$, on a u^2 négatif, donc $u^2 = -|u^2| = -|u|^2$.

Cette proposition permet de déduire une propriété pour les automorphismes.

Proposition 4.2.8. *Tout automorphisme A de $\mathcal{A}$ stabilise $Im(\mathcal{A})$. De plus, pour tout $u \in \mathcal{A}$, on a $\overline{A(u)} = A(\overline{u})$.*

Démonstration. On souhaite montrer que pour tout $u \in Im(\mathcal{A})$, on a $A(u) \in Im(\mathcal{A})$. Soit $u \in Im(\mathcal{A})$. On a $u^2 = -|u|^2 1$, donc

$$A(u).A(u) = A(u^2) = -|u|^2 A(1) = -|u|^2$$

Donc le carré de $A(u)$ est réel négatif, et $A(u)$ appartient à $Im(\mathcal{A})$, par le lemme 4.2.6.
On en déduit la propriété sur le conjugué. Puisque tout élément de $\mathcal{A}$ se décompose comme une somme d'un multiple de 1 et d'un élément de $Im(\mathcal{A})$, et que A est linéaire, il suffit de vérifier la propriété pour les mutliples de 1 et les éléments de $Im(\mathcal{A})$. Mais pour u réel, c'est-à-dire multiple de 1, on a $\overline{u} = u$ et $A(u) = A(u\,1) = uA(1) = u\,1 = u$ par linéarité de A et par la proposition 4.2.3 . Dès lors $\overline{A(u)} = A(u)$, puisque $A(u)$ est réel. Pour $u \in Im(\mathcal{A})$, on a $\overline{u} = -u$ et $\overline{A(u)} = -A(u)$, puisque $A(u)$ appartient à $Im(\mathcal{A})$ par stabilité. □

En corollaire, on obtient le résultat suivant, qui lie automorphismes et isométries.

Proposition 4.2.9. *Tout automorphisme de $\mathcal{A}$ est une isométrie de $\mathcal{A}$.*

Démonstration. Soit A un automorphisme. On a

$$|A(u)|^2 = A(u)\overline{A(u)} = A(u)A(\overline{u}) = A(u\overline{u}) = |u|^2 A(1) = |u|^2,$$

pour tout $u \in \mathcal{A}$. □

Cette proposition permet de déterminer les automorphismes de l'algèbre des quaternions.

Proposition 4.2.10. *On a $Aut(\mathbb{H}) = \{C_q : q \in q \in \mathbb{H}\}$, donc $Aut(\mathbb{H})$ est isomorphe à $SO(3)$.*

Démonstration. Par les propositions 4.2.9 et 4.2.3, nous savons que si A est un automorphisme de $\mathbb{H}$, alors A est une isométrie de $\mathbb{H}$, qui fixe 1. Elle est donc définie par sa restriction à $Im(\mathbb{H})$ qui, par les propositions 4.1.16 et 4.1.27, s'écrit C_q ou $-C_q$, pour un quaternion q, que l'on peut supposer unitaire. Il est facile de vérifier que C_q définit un automorphisme :

$$C_q(uv) = q(uv)q^{-1} = quq^{-1}qvq^{-1} = C_q(u)C_q(v), \quad \forall u, v \in \mathbb{H}.$$

Par contre, pour la même raison $-C_q$ ne définit pas un automorphisme. □

Nous pourrions désormais passer à la détermination des automorphismes de l'algèbre des octonions. Toutefois, comme il a été dit plus haut dans cette section, cela ne sera pas fait entièrement, les résultats ci-dessous en sont une amorce.

Proposition 4.2.11. *Soit $A \in Aut(\mathbb{O})$, définissons*

$$x_1 = A(e_1), \quad x_2 = A(e_2) \quad \text{et} \quad x_3 = A(e_3).$$

Alors on a les propriétés suivantes pour x_1, x_2, x_3 :

1) *Ils appartiennent à $Im(\mathbb{O})$,*
2) *Ils sont normés et orthogonaux deux à deux,*
3) *On a $\langle x_1x_2, x_3\rangle = 0$.*

Démonstration. On sait que A est une isométrie (car c'est un automorphisme) et qu'elle fixe 1. On a

$$\langle 1, x_l\rangle = \langle A(1), A(e_l)\rangle = \langle 1, e_l\rangle = 0$$

pour $l \in \{1, 2, 3\}$, ce qui nous permet de dire que les éléments x_l sont orthogonaux à 1, ils sont donc imaginaires. On obtient de la même façon les deuxième et troisième propriétés à partir des relations

$$\langle e_i, e_j\rangle = \delta_{ij} \quad \text{et} \quad \langle e_1e_2, e_3\rangle = 0$$

sachant que $A(e_1e_2) = A(e_1)A(e_2) = x_1x_2$. □

Passons maintenant à la réciproque de cette proposition.

Proposition 4.2.12. *Pour tout triplets (x_1, x_2, x_3) satisfaisant les trois propriétés de la proposition précédente, il existe un unique automorphisme A tel que*

$$A(e_1) = x_1, \quad A(e_2) = x_2 \quad \text{et} \quad A(e_3) = x_3. \tag{4.4}$$

Démonstration. Dans un premier, montrons l'unicité d'un tel automorphisme. Si A est un automorphisme satisfaisant les conditions 4.4, il satisfait aussi

$$A(1) = 1 \tag{4.5}$$

puisque A est un automorphisme, mais également

$$A(e_4) = A(e_1e_2) = A(e_1)A(e_2) = x_1x_2, \tag{4.6}$$

$$A(e_5) = A(e_2e_3) = A(e_2)A(e_3) = x_2x_3, \tag{4.7}$$

$$A(e_6) = A(e_3e_4) = A(e_3)A(e_4) = x_3(x_1x_2), \tag{4.8}$$

$$A(e_7) = A(e_1e_3) = A(e_1)A(e_3) = x_1x_3. \tag{4.9}$$

Ainsi, la condition 4.4 détermine l'image de A sur tous les vecteurs de base $\{1, e_1, \ldots, e_7\}$. Et comme A est linéaire alors il est univoquement déterminé par 4.4 puisque ces trois égalités impliquent les conditions 4.6 , 4.7, 4.8 et 4.9.
Passons à l'existence. On définit A par les relations 4.4−4.9 et on l'étend linéairement. Un calcul élémentaire mais fastidieux permet alors de démontrer que A préserve le produit, c'est-à-dire que

$$A(e_i)A(e_j) = A(e_ie_j) \qquad \forall i, j \in \{1, \ldots, 7\}.$$

□

Il vient alors le corollaire suivant, qui est également le dernier résultat que nous montrerons dans ce mémoire, qui nous permet de faire un lien supplémentaire avec le groupe de Lie exceptionnel G_2 : $Aut(\mathbb{O})$ et G_2 ont même dimension.

Corollaire 4.2.13. *Le groupe* $Aut(\mathbb{O})$ *est paramétré (de manière bijective) par les triplets* (x_1, x_2, x_3) *satisfaisant les trois conditions de la proposition 4.2.11. En particulier, il est de dimension* 14.

Démonstration. La paramétrisation de $Aut(\mathbb{O})$ par les triplets résulte des deux propositions précédentes. L'ensemble de ces triplets constitue une variété de dimension 14. En effet, les trois conditions de la proposition 4.2.11 sont équivalentes au fait que x_1 soit sur la sphère unité de $Im(\mathbb{O})$ qui est de dimension 6. L'élément x_2 appartient à l'intersection de cette sphère et de l'hyperplan orthogonal à x_1, qui est de dimension 5 et x_3 est à l'intersection de la sphère et du sous-espace orthogonal à x_1, x_2 et x_1x_2, qui est de dimension 3. $\square$

Bibliographie

[1] Disponible via l'URL <https://mathshistory.st-andrews.ac.uk/Biographies/Hamilton/>.

[2] Disponible via l'URL <http://serge.mehl.free.fr/chrono/Hamilton.html>.

[3] Disponible via l'URL <https://en.wikipedia.org/wiki/Alternative_algebra>.

[4] Disponible via l'URL <https://fr.wikipedia.org/wiki/Ruth_Moufang>.

[5] Disponible via l'URL <https://fr.wikipedia.org/wiki/Méthode_de_Ferrari>.

[6] Programme d'études : Mathématiques de base, 2014. Administration générale de l'Enseignement. Service général de l'Enseignement organisé par la Fédération Wallonie-Bruxelles.

[7] ARTIGUE, Michèle et André DELEDICQ. *Quatre étapes dans l'histoire des nombres complexes : " quelques commentaires épistémologiques et didactiques. "*. Université PARIS VII - Denis Diderot : Institut de recherche pour l'enseignement des mathématiques (IREM), Février 1992. ISBN 2-86612-108-2.

[8] BALES, John W. The Eight Cayley-Dickson Doubling Products. *Advances in applied Clifford algebra*. 2016, 26(2), p. 529–551. Springer International Publishing.

[9] BESSIERES, Laurent. *Algèbre bilinéaire et géométrie.* Institut de Mathématiques de Bordeaux, avril 2017.

[10] BUCHMANN, Amy. A Brief History of Quaternions and the theory of Holomorphic Functions of Quaternionic Variables. march 2009. Departement of Mathematics and Computer Sciences, Schmid College of Science, Chapman University, Orange. Disponible via l'URL <https://arxiv.org/pdf/1111.6088.pdf>.

[11] BÄCHTOLD, Manuel et Thomas HAUSBERGER. Les nombres complexes : entre mathématiques, physique et philosophie. la réforme des programmes des lycée : et alors ? mai 2013, pages 78–88. hal-00879219.

[12] CONSTANTIN, TZANAKIS. *Rotations, nombres complexes et quaternions.* Département d'éducation, Université de Crète, 74100 Rethymnon, Crète, Grèce.

[13] CONWAY, John H. et Derek A. SMITH. *On Quaternions and Octonions : their geometry, arithmetic and symmetry.* Natick, Mass : AK Peters, 2003. xii, 159 p. ISBN 1568811349.

[14] COUDENE, Yves. *Algèbre linéaire et bilinéaire I.* Sorbonne Université, septembre 2020. Version 2.

[15] EBBINGHAUS, et al. *Numbers.* New York : Springer-Verlag, 1991. (Graduate texts in mathematics ; 123). xviii, 391 p. ISBN 0387974970.

[16] HAMILTON, William Rowan. *Element of Quaternions Part 1.* Cambridge : Cambridge University Press, 2009. (Cambridge Library Collection - Mathematics). ISBN 1-108-00900-X.

[17] LA FUENTE-GRAVY, Laurent. Le théorème de Hurwitz. *Note de la quatrième BSSM.* 2011, p. 158–164. Disponible via l'URL <https://bssm.ulb.ac.be/data/books/Bssm-2011-Laurent-La-Fuente-Gravy.pdf>.

[18] MATHONET, Pierre. *Mathématiques Elémentaires*. Université de Liège. Note de cours pour la première année d'études de bachelier en Sciences Mathématiques. Année académique 2019-2020.

[19] NAHIN, Paul J. *An Imaginary tale : The story of* $\sqrt{-1}$. Princeton, New Jersey : Princeton University Press, 2010. (Princeton Science Library). xxiv, 267 p. ISBN 978-0-691-16924-8.

[20] PCHELINTSEV, S.V. Central isotopes of (-1,1)-algebras. *Siberian mathematical journal.* 2021, 62(4), p. 678–690. Moscou. Pleiades Publishing.

[21] ROSSEEL, Hilda et Maggy SCHNEIDER. *Ces nombres qu'on dit imaginaires sont-il vraiment des nombres ?* Liège : Les éd. de l'Université de Liège, 2011. (Si les mathématiques m'étaient contées). ISBN 9782874561412.

[22] ROSSEEL, Hilda et Maggy SCHNEIDER. *Les nombres complexes comme modèles algébriques de similitudes directes : avec ou sans matrices ?* Société Belge des Professeurs de Mathématiques d'Expression Française (SBPMef), 2013.

[23] TAYLOR, Michael. The octonions. Disponible via l'URL <`https://mtaylor.web.unc.edu/wp-content/uploads/sites/16915/2018/04/octon.pdf`>.