Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Curso de Bacharelado em Matemática

Os Quatérnios

Jafé Silvestre de Morais

João Pessoa – PB
Outubro de 2024

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Curso de Bacharelado em Matemática

Os Quatérnios

por

Jafé Silvestre de Morais

sob a orientação do

Prof. Dr. Napoleón Caro Tuesta

João Pessoa – PB
Outubro de 2024

Catalogação na publicação
Seção de Catalogação e Classificação

M827q Morais, Jafe Silvestre de.
Os Quatérnios / Jafe Silvestre de Morais. - João Pessoa, 2024.
36 p. : il.

Orientação: Napoleón Caro Tuesta.
TCC (Curso de Licenciatura em Matemática) - UFPB/CCEN.

1. álgebras com divisão. 2. Quatérnios. 3. Teorema de Frobenius. I. Tuesta, Napoleón Caro. II. Título.

UFPB/CCEN CDU 51(043.2)

Elaborado por Josélia Maria Oliveira da Silva - CRB-15/113

FOLHA DE APROVAÇÃO

JAFÉ SILVESTRE DE MORAIS

Os Quatérnios

Trabalho de conclusão de curso apresentado ao Curso de Bacharelado em Matemática, do Departamento de Matemática, do Centro de Ciências Exatas e da Natureza, da Universidade Federal da Paraíba, como requisito para obtenção do título de Bacharel em Matemática.

Aprovado em 29 de outubro de 2024.

Banca Examinadora

Documento assinado digitalmente
gov.br
NAPOLEON CARO TUESTA
Data: 22/11/2024 13:20:11-0300
Verifique em https://validar.iti.gov.br

Prof. NAPOLEON CARO TUESTA
Orientador
(UFPB/CCEN/Departamento de Matemática)

Documento assinado digitalmente
gov.br
JACQUELINE FABIOLA ROJAS ARANCIBIA
Data: 24/11/2024 09:03:08-0300
Verifique em https://validar.iti.gov.br

Profª. JACQUELINE FABIOLA ROJAS ARANCIBIA
Membro Interno
(UFPB/CCEN/Departamento de Matemática)

Documento assinado digitalmente
gov.br
WALLACE MANGUEIRA DE SOUSA
Data: 22/11/2024 20:36:27-0300
Verifique em https://validar.iti.gov.br

Prof. WALLACE MANGUEIRA DE SOUSA
Membro Interno
(UFPB/CCEN/Departamento de Matemática)

Agradecimentos

Gostaria de agradecer primeiramente, todo meu agradecimento ao professor Napoleón Caro Tuesta que aceitou o desafio de me orientar. Obrigado por sempre mostrar os melhores caminhos e me incentivar, permitindo que eu alcançasse esta etapa tão importante na minha carreira. Agradeço aos membros da banca, Professor Dr Wallace e Professora Dra Jaqueline Rojas por aceitarem o convite. Agradeço pelo tempo dedicado e contribuições que, sem dúvida, enriquecerão ainda mais este trabalho. Muito obrigado por contribuírem para este momento tão importante da minha trajetória. Agradeço em especial a Aline Lourenço, que me incentivou a retomar e concluir o curso, e esteve ao meu lado nessa longa caminhada. Obrigado pelo total suporte e incentivo para que eu não desistisse no meio do caminho, e sim alcançasse este objetivo até o fim. Ao finalizar o curso, jamais imaginei que encontraria pessoas que seriam tão importantes no meu caminho, ajudando e me incentivando em cada etapa. Vocês têm uma participação fundamental em tudo isso. Por isso, meu agradecimento especial vai para Eduardo, Maria Eduarda, João, Francisco Inácio. Meu muito obrigado a todos por tudo. Agradeço imensamente ao meu amigo e professor Joémerson Maia, por ter dedicado seu tempo e atenção às minhas dúvidas. Muito obrigado pelo grande suporte oferecido ao longo dessa jornada. Agradeço também aos meus amigos de longa data, os raízes dos *"fídemangabeira"* que sempre me incentivaram e me deram suporte para não desistir. Por fim, agradeço a todos e a todas que me acompanharam nessa caminhada de conclusão do curso, aos que me apoiaram e torceram pelo meu sucesso, toda minha gratidão e mais sinceros, muito obrigado.

Dedico este trabalho, ao meu grande amigo, Tálito Borges, in memoriam. Enquanto neste plano sempre me deu suporte, apoio e incentivo. A você meu grande amigo, muito obrigado por tudo.

Resumo

Neste trabalho descrevemos a construção da álgebra dos quatérnios $\mathbb{H}$, sob duas perspectivas diferentes. A primeira segue as ideias do próprio Hamilton, quém introduziu os quatérnios em 1843, e a segunda, como uma subálgebra de certas matrizes complexas. Estudamos as propriedades fundamentais de $\mathbb{H}$, tanto algébricas quanto geométricas. Em particular provamos que $\mathbb{H}$ é uma álgebra real associativa com divisão de dimensão 4. Nosso estudo culmina apresentando uma prova detalhada do famoso Teorema de Frobenius que caracteriza as álgebras com divisão de dimensão finita sobre os reais. De acordo com dito teorema, cada tal álgebra é isomorfa a uma das seguintes álgebras:

(i) $\mathbb{R}$, a álgebra dos números reais;

(ii) $\mathbb{C}$, a álgebra dos números complexos;

(iii) $\mathbb{H}$, a álgebra dos quatérnios.

Palavras-chave: álgebras com divisão, quatérnios, Teorema de Frobenius

Abstract

In this work we describe the construction of the quaternions algebra $\mathbb{H}$, from two different perspectives. The first follows the ideas of Hamilton himself, who introduced quaternions in 1843, and the second, as a subalgebra of certain complex matrices. We study the fundamental properties of $\mathbb{H}$, both algebraic and geometric. In particular we prove that $\mathbb{H}$ is an associative division algebra of dimension 4 over $\mathbb{R}$. Our study culminates by presenting a detailed proof of the famous Frobenius's Theorem, which characterizes finite dimensional associative division algebras over $\mathbb{R}$. According to said theorem, each such algebra is isomorphic to one of the following algebras:

(i) $\mathbb{R}$, the algebra of real numbers;

(ii) $\mathbb{C}$, the algebra of complex numbers;

(iii) $\mathbb{H}$, the algebra of quaternions.

Keywords: division algebras, quaternions, Frobenius's theorem

Sumário

Introdução

Quatérnions são uma extensão dos números complexos. Os quatérnions foram descritos pela primeira vez pelo matemático irlandês Sir William Rowan Hamilton em 1843 e aplicados ao estudo da mecânica no espaço tridimensional. A álgebra dos quatérnios é frequentemente denotada por $\mathbb{H}$ (em homenagem a Hamilton). Quatérnios não formam um corpo, pois a multiplicação em $\mathbb{H}$ não é, em geral, comutativa.

Figura 1: Sir William Rowan Hamilton

Em 16 de outubro de 1843, Hamilton teve uma inspiração durante uma caminhada ao longo do Canal Real de Dublin. Ele ficou tão entusiasmado que, usando um canivete, talhou a descoberta na Ponte Broome. O grafite, que se tornou famoso na história da matemática, continha esta equação:

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

Embora pareça simples, ela foi responsável por transformar a maneira como os matemáticos representam informações e simplificou diversas aplicações técnicas, que vão desde o cálculo de forças na engenharia até o funcionamento de máquinas de ressonância magnética, turbinas eólicas e a programação de robôs. Assim, a álgebra dos quatérnios, a primeira álgebra associativa não-comutativa com divisão, subitamente nasceu e abriu as portas da álgebra abstrata.

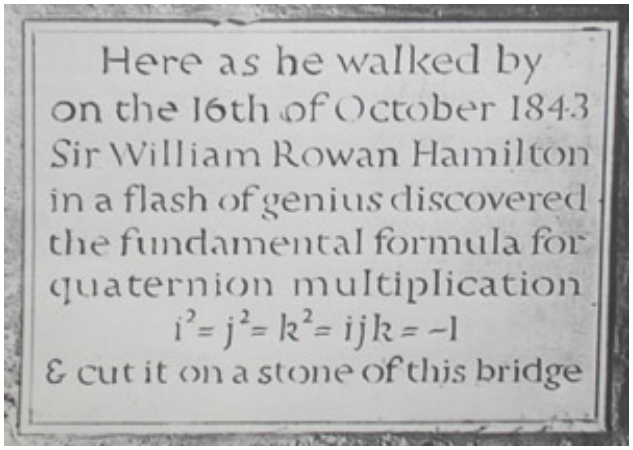


Figura 2: Placa em homenagem a Hamilton

O objetivo principal deste trabalho é estudar a construção e as propriedades fundamentais dos quatérnios. Com esse propósito dividimos a monografia em 4 capítulos.

No primeiro capítulo introduzimos as noções básicas da teoria de álgebras sobre o corpo dos números reais, com especial ênfase nas álgebras de divisão.

O capítulo 2 destina-se a descrever a construção da álgebra dos quatérnios $\mathbb{H}$, sob duas perspectivas diferentes. A primeira segue as ideias do próprio Hamilton e a segunda, como uma subálgebra de certas matrizes complexas. Estudamos neste mesmo capítulo as propriedades fundamentais de $\mathbb{H}$, tanto algébricas quanto geométricas. Em particular provamos que $\mathbb{H}$ é uma álgebra associativa com divisão de dimensão 4 sobre $\mathbb{R}$.

O terceiro capítulo estabelece uma conexão de $\mathbb{H}$ com alguns grupos topológicos. Em particular obtemos uma representação paramétrica da esfera compacta tridimensional $\mathbb{S}^3$.

Finalmente, apresentamos no capítulo 4 uma prova detalhada de um famoso teorema devido ao grande matemático alemão Ferdinand Georg Frobenius, demostrado em 1877 . Segundo tal teorema, toda álgebra associativa com divisão e de dimensão finita sobre os reais é isomorfa a uma das seguintes álgebras:

(i) $\mathbb{R}$, a álgebra dos números reais;

(ii) $\mathbb{C}$, a álgebra dos números complexos;

(iii) $\mathbb{H}$, a álgebra dos quatérnios.

Capítulo 1

$\mathbb{R}$-álgebras com divisão

Neste primeiro capítulo vamos nos familiarizar com os conceitos básicos da teoria de álgebras sobre o corpo dos números reais, com especial ênfase nas álgebras de divisão. Como é tradicional, o corpo dos números reais e o corpo dos números complexos serão denotados por $\mathbb{R}$ e $\mathbb{C}$, respectivamente.

1.1 $\mathbb{R}$-álgebras

Definição 1.1. Uma $\mathbb{R}$-*álgebra* é um espaço vetorial real A equipado com uma aplicação $\mathbb{R}$-bilinear

$$\varphi : A \times A \longrightarrow A$$

chamada *multiplicação*.

Para um par ordenado $(x, y) \in A \times A$, é usual escrever $x \cdot y$ no lugar de $\varphi(x, y)$. Nestos termos, a bilinearidade de φ significa que, para todo $\alpha, \beta \in \mathbb{R}$ e para todo $x, y, z \in A$, valem as seguintes identidades:

- $(\alpha x + \beta y) \cdot z = \alpha(x \cdot z) + \beta(y \cdot z)$,
- $x \cdot (\alpha y + \beta z) = \alpha(x \cdot y) + \beta(x \cdot z)$.

Tais relações são conhecidas como *propriedades distributivas.* Em particular cumpre-se que,

- $\alpha(x \cdot y) = (\alpha x) \cdot y = x \cdot (\alpha y)$, para todo $\alpha \in \mathbb{R}$ e para todo $x, y \in A$.

Definição 1.2. Seja A uma $\mathbb{R}$-álgebra.

(i) Se $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ para todo $x, y, z \in A$, dizemos que A é uma *álgebra associativa*.

(ii) A é chamada *álgebra comutativa*, se $x \cdot y = y \cdot x$ para todo $x, y \in A$.

(iii) Um elemento $e \in A$ é chamado *elemento identidade* de A, se $e \cdot x = x \cdot e = x$ para todo $x \in A$.

(iv) Um elemento x de uma álgebra A é um *divisor de zero* se existe um elemento $y \neq 0$ em A tal que $x \cdot y = 0$ ou $y \cdot x = 0$. Dizemos que A é uma *álgebra sem divisores de zero*, se não possui divisores de zero diferentes de $0 \in A$.

(v) A dimensão de A como espaço vetorial sobre $\mathbb{R}$ é chamada *dimensão da álgebra* A.

1.2 Exemplos de $\mathbb{R}$-álgebras

(1) Os corpos dos números reais $\mathbb{R}$ e dos números complexos $\mathbb{C}$ são $\mathbb{R}$-álgebras comutativas e associativas de dimensões 1 e 2, respectivamente, cada uma com elemento identidade e sem divisores de zero.

(2) O $\mathbb{R}$-espaço vetorial $Mat(n, \mathbb{R})$ das matrizes reais de ordem $n \times n$ é uma $\mathbb{R}$-álgebra associativa com elemento identidade de dimensão n^2 com respeito à multiplicação de matrizes.

(3) O $\mathbb{R}$-espaço vetorial $Mat(n, \mathbb{C})$ das matrizes complexas de ordem $n \times n$ é uma $\mathbb{R}$-álgebra associativa com elemento identidade de dimensão $2n^2$ com respeito à multiplição de matrizes.

Note que se $n \geq 2$, então $Mat(n, \mathbb{R})$ e $Mat(n, \mathbb{C})$ são álgebras não comutativas.

(4) Sejam $u = (a_1, a_2, a_3), v = (b_1, b_2, b_3)$ vetores de $\mathbb{R}^3$. Definimos o *produto vetorial* de u e v por:

$$u \times v := (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1) \in \mathbb{R}^3.$$

Então, $\mathbb{R}^3$ com sua estrutura vetorial canônica juntamente com o produto vetorial $\times$ é uma $\mathbb{R}$-álgebra associativa e anticomutativa (isto é, $v \times u = -u \times v$) de dimensão 3.

(5) Seja $n \geq 2$. O $\mathbb{R}$-espaço vetorial $Sim(n, \mathbb{R})$ das matrizes simétricas reais de ordem $n \times n$ é, com respeito ao *produto simétrico* de matrizes,

$$(A, B) \mapsto \frac{1}{2}(AB + BA),$$

uma álgebra comutativa não associativa.

(6) Todo $\mathbb{R}$-espaço vetorial $V \neq 0$ pode ser munido de uma estrutura de $\mathbb{R}$-álgebra comutativa, associativa e com elemento identidade. Para isto, fixemos um vetor $0 \neq e \in V$ e escolhamos um somando direto U do subespaço $\mathbb{R}e$ gerado por e. Sejam $x = \alpha_1 e + u_1$, $y = \alpha_2 e + u_2$ dois vetores arbitrários de $V = \mathbb{R}e \oplus U$. Definimos uma multiplicação em V por:

$$x \cdot y := (\alpha_1\alpha_2)e + (\alpha_1 u_2 + \alpha_2 u_1).$$

Note que e é o elemento identidade. Além disso, cumpre-se $u \cdot v = 0$ para todo $u, v \in U$. Isto implica que todo elemento de U é um divisor de zero.

(7) Sejam A_1 ,..., A_n álgebras sobre $\mathbb{R}$ e seja $A := A_1 \oplus \cdots \oplus A_n$, a soma direta dos espaços vetoriais $A_1, ..., A_s$. Em A definimos um produto pela seguinte regra:

$$x \cdot y = x_1 y_1 + \cdots + x_s y_s,$$

onde $x = x_1 + \cdots + x_s$, $y = y_1 + \cdots + y_s$ com cada $x_i, y_i \in A_i$. A álgebra A obtida dessa maneira é chamada *álgebra soma direta* de $A_1, ..., A_n$. Se todas as álgebras $A_1, ...A_n$ são comutativas (respectivamente associativas), então A também é comutativa (respectivamente associativa). No caso que $n \geq 2$, A sempre tem divisores de zero. Se cada álgebra A_i possui um elemento identidade e_i, A também possui um elemento identidade, a saber, $e := e_1 + \cdots + e_n$.

1.3 Subálgebras

Definição 1.3. Sejam A $\mathbb{R}$-álgebra e B um subconjunto de A. Dizemos que B é uma *subálgebra* de A, se são satisfeitas as seguintes condições:

(i) B é um subespaço vetorial de A,

(ii) B é fechado com relação a multiplicação, isto é, $x \cdot y \in B$ para todo $x, y \in B$.

Obviamente toda subálgebra de uma álgebra também é uma álgebra.

Exemplo 1.1. O conjunto

$$B = \left\{ \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{R} \right\}$$

é uma $\mathbb{R}$-subálgebra de $Mat(2, \mathbb{R})$.

Exemplo 1.2. Os subespaços de matrizes triangulares superiores que formam, em cada caso, $\mathbb{R}$-subálgebras de $Mat(2, \mathbb{R})$ e $Mat(2, \mathbb{C})$ de dimensões $\frac{1}{2}n(n+1)$ e $n(n+1)$, respectivamente.

Exemplo 1.3. Seja $B = \{A \in Mat(\mathbb{R}) \mid a_{ij} = 0 \text{ se } i \neq j\}$ o subespaço das matrizes diagonais. Não é dificil ver que B é uma subálgebra de $Mat\mathbb{R}$ de dimensão n.

1.4 Homomorfismos de $\mathbb{R}$-álgebras

Definição 1.4. Sejam A e B duas $\mathbb{R}$-álgebras. Um *homomorfismo* entre A e B é uma aplicação $\mathbb{R}$-linear $\varphi : A \longrightarrow B$ tal que $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ para todo $x, y \in A$.

Um homomorfismo de $\mathbb{R}$-álgebras $\varphi : A \longrightarrow B$ é um *isomorfismo*, se φ é uma bijeção. Dizemos que A e B são *álgebras isomorfas*, caso existir um isomorfismo entre elas. Neste caso escreveremos $A \cong B$.

Lema 1.4.1. Suponhamos que $\varphi : A \longrightarrow B$ é um isomorfismo de $\mathbb{R}$-álgebras. Então a aplicação inversa $\varphi^{-1} : B \longrightarrow A$ é um homomorfismo de $\mathbb{R}$-álgebras.

Demonstração. Sejam $\alpha \in \mathbb{R}$ e $x', y' \in B$. Como φ é uma bijeção, existem $x, y \in A$ tais que $\varphi(x) = x'$ e $\varphi(y) = y'$. Logo, temos que

$$\begin{aligned}\varphi^{-1}(\alpha x' - y') &= \varphi^{-1}((\alpha\varphi(x) + \varphi(y)) \\ &= \varphi^{-1}(\varphi(\alpha x + y)) \\ &= \varphi^{-1} \circ \varphi(\alpha x + y) \\ &= (\alpha x + y) \\ &= \alpha\varphi^{-1}(x') + \varphi^{-1}(y')\end{aligned}$$

Além disso,

$$\begin{aligned}\varphi^{-1}(x' \cdot y') &= \varphi^{-1}(\varphi(x) \cdot \varphi(y)) \\ &= \varphi^{-1}(\varphi(x \cdot y)) \\ &= \varphi^{-1} \circ \varphi(x \cdot y) \\ &= x \cdot y \\ &= \varphi^{-1}(x) \cdot \varphi^{-1}(y)\end{aligned}$$

Isto mostra que φ^{-1} é um homomorfismo de $\mathbb{R}$-álgebras.

□

Exemplo 1.4. A aplicação $f : \mathbb{C} \longrightarrow Mat(2, \mathbb{R})$ definida por

$$\varphi(\alpha + \beta i) = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$$

é um homomorfismo injetivo de $\mathbb{R}$-álgebras. Consequentemente, $\mathbb{C} \cong \text{Im}\varphi$. Isto significa que $\mathbb{C}$ pode ser identificado com uma subálgebra de matrizes de ordem 2 com coeficientes reais. Veremos, no próximo capítulo, um resultado semelhante para os quatérnios.

Exemplo 1.5. Seja A uma $\mathbb{R}$-álgebra com elemento identidade e. A aplicação $f : \mathbb{R} \longrightarrow A$ dada por $\alpha \longmapsto \alpha e$ é um homomorfismo injetivo de $\mathbb{R}$-álgebras. Isto implica que toda $\mathbb{R}$-álgebra com elemento identidade e dimensão 1 é isomorfa à álgebra dos números reais $\mathbb{R}$.

1.5 Construção de uma álgebra com a utilização das bases

Suponhamos que A é um espaço vetorial real n-dimensional. Existe um proceso simples que permite transformar A numa álgebra de dimensão n. Para isto escolhamos $e_1, e_2, ..., e_n$ una base de A. Suponhamos por um momento que A tem estrutura de álgebra real. Se

$x = \sum_{i=1}^{n} \alpha_i e_i$, $y = \sum_{i=1}^{n} \beta_i e_i$ são vetores arbitrários de A, então, para qualquer produto $(x, y) \longmapsto xy$, teríamos, em virtude da propriedade distributiva, que

$$xy = \sum_{i,j=1}^{n} (\alpha_i \beta_j) e_i e_j$$

Portanto, uma multiplicação em A estará completamente definida uma vez que os n^2 produtos individuais $e_i e_j$ tinham sido definidos. Os valores podem ser arbitrariamente escolhidos em A. Desta toda forma possível estrutural de $\mathbb{R}$-álgebra sobre A pode ser obtida.

A maioria destas álgebras não são de interesse, pois não apresentam propriedades especiais. Se desejamos construir álgebras com elemento identidade, então podemos postular convenientemente, que e_1 é o elemento identidade. Então,

$$e_1 e_i = e_i e = e_i, \quad \text{para todo} \quad i = 1, ..., n.$$

Porém os $(n-1)^2$ produtos restantes $e_i e_j$, $1 \leq i, j \leq n$ podem ser escolhidos livremente.

É possível provar que uma álgebra A é associativa se, e somente se, $(e_i e_j) e_k = e_i (e_j e_k)$, para todo $i, j, k = 1, ..., n$.

Analogamente, A é comutativa se, e somente se, $e_i e_j = e_j e_i$ para todo $i, j = 1, ..., n$.

Suponhamos que B é outra $\mathbb{R}$-álgebra. Pode ser demonstrado também, que uma aplicação $\mathbb{R}$-linear $f : A \longrightarrow B$ é um homomorfismo de $\mathbb{R}$-álgebras se, e somente se, $f(e_i e_j) = f(e_i) f(e_j)$ para todo $i, j = 1, ..., n$.

1.6 Álgebras de dimensão 1 e 2

Todo espaço vetorial V trivialmente tem estrutura de $\mathbb{R}$-álgebra se definimos como multiplicação a *aplicação nula*, isto é, $V \times V \longrightarrow V$, $(x, y) \longmapsto 0$. A seguir mostraremos que quando a dimensão da álgebra real é 1, este é o único caso patológica.

Teorema 1.6.1. Seja A uma $\mathbb{R}$-álgebra de dimensão 1 cuja multiplicação não é a aplicação nula, então A é isomorfa à álgebra dos números reais $\mathbb{R}$.

Demonstração. Em virtude do observado acima é suficiente provar que A possui um elemento identidade. É claro que $A = \mathbb{R}a$ para todo $0 \neq a \in A$. Fixemos um elemento $0 \neq a \in A$. Como a multiplicação é diferente da aplicação nula, existem $x, y \in A$ diferentes de zero tais que $x \cdot y \neq 0$. Por outro lado, $x = \alpha a, y = \beta a$ para alguns $\alpha, \beta \in \mathbb{R}$. Desde que $\alpha\beta a^2 = x \cdot y \neq 0$, temos que $a^2 \neq 0$ e portanto, $A = \mathbb{R}a^2$. Em consequência, existe $\gamma \in \mathbb{R}$ tal que $a = \gamma a^2$. Afirmamos que $e := \gamma a$ é o elemento identidade de A. De fato, dado $b \in A$, então existe $\lambda \in \mathbb{R}$ tal que $b = \lambda a$. Logo $be = (\lambda a)(\gamma a) = \lambda(\gamma a^2) = \lambda a = b$. Analogamente prova-se que $e \cdot b = b$. □

Vamos caracterizar agora as $\mathbb{R}$-álgebras com elemento identidade de dimensão 2.

Teorema 1.6.2. Toda $\mathbb{R}$-álgebra A de dimensão 2 com elemento identidade é comutativa e associativa. Mais ainda, existem três únicas possibilidades, mutuamente excludentes:

(i) A é isomorfa à álgebra dos *números duais*, isto é, aquela álgebra cujo espaço vetorial subjacente é $\mathbb{R}^2$ e que têm $(1,0)$ como elemento identidade e o elemento $\epsilon := (0,1)$ satisfazendo a equação $\epsilon^2 = 0$.

(ii) A é isomorfa à soma direta $\mathbb{R} \oplus \mathbb{R}$, isto é, aquela álgebra onde os elementos básicos $a = (1,0)$ e $b = (0,1)$ satisfazem as relações $a^2 = a$, $b^2 = b$ e $a \cdot b = 0$.

(iii) A é isomorfa à álgebra dos números complexos $\mathbb{C}$.

Demonstração. Suponhamos que $\{e, v\}$ é uma base de A de maneira que e é o elemento identidade de A. Então $v^2 = \alpha e + \beta v$, para alguns $\alpha, \beta \in \mathbb{R}$. Da última relação obtemos que $v^2 - \beta v = \alpha e$. Portanto, $(v - \frac{\beta}{2}e)^2 = (\alpha + \frac{\beta^2}{4})e$. De acordo com o sinal do número real $\alpha + \frac{\beta^2}{4}$, há três casos mutuamente exclusivos por analisar:

- Em primeiro lugar, suponhamos que $\alpha + \frac{\beta^2}{4} = 0$. Isto implica que $(v - \frac{\beta}{2}e)^2 = 0e$. Seja $u := v - \frac{\beta}{2}e$, então e, u é uma base de A onde e é o elemento identidade e u satisfaz a igualdade $u^2 = 0e$. Nesta situação, a aplicação $A \longrightarrow \mathbb{R}^2$ definida por $\alpha e + \beta u \longmapsto \alpha(1,0) + \beta(0,1) = (\alpha, \beta)$ é um isomorfismo de $\mathbb{R}$-álgebras. Consequentemente A é isomorfa à álgebra dos números duais descritos em (i).

- No caso que $\alpha + \frac{\beta^2}{4} > 0$, dito número pode ser representado como o quadrado de um número real $k > 0$, isto é, $\alpha + \frac{\beta^2}{4} = k^2$. Da última equação obtemos $(v - \frac{\beta}{2}e)^2 = k^2 e$ e portanto $(\frac{1}{k}v - \frac{\beta}{2k}e)^2 = 1e$. Então, se $u := \frac{1}{k}v - \frac{\beta}{2k}e$, os elementos e, u formam uma base de A, onde e é o elemento identidade e $u^2 = 1e$. Definindo $w := \frac{1}{2}(e + u), z := \frac{1}{2}(e - v)$, temos que $\{w, z\}$ é outra base de A tal que $w^2 = w, z^2 = z, w \cdot z = 0$. Consequentemente, a aplicação $A \longrightarrow \mathbb{R} \oplus \mathbb{R}$ dada por $\alpha w + \beta z \longmapsto \alpha a + \beta b$ define um isomorfismo de $\mathbb{R}$-álgebras. Isto mostra que A é isomorfa à soma direta descrita em (ii).

- Finalmente, se $\alpha + \frac{\beta^2}{4} < 0$, então existe $k > 0$ tal que $\alpha + \frac{\beta^2}{4} = -k^2$. Isto implica que $(\frac{1}{k}v - \frac{\beta}{2k}e)^2 = (-1)e$. Portanto se denotamos com $u := \frac{1}{k}v - \frac{\beta}{2k}e$, vemos que $\{e, u\}$ é uma base de A com e como elemento identidade de A e onde u satisfaz a relação $u^2 = (-1)e$. Agora é claro que a aplicação $A \longrightarrow \mathbb{C}$, $\alpha e + \beta u \longmapsto \alpha + \beta i$ é um isomorfismo de $\mathbb{R}$-álgebras.

□

1.7 Álgebras com divisão

Definição 1.5. Uma $\mathbb{R}$-álgebra $A \neq 0$ é uma *álgebra de divisão*, se para todo $a, b \in A, a \neq 0$, as duas equações

$$ax = b, \qquad ya = b$$

têm soluções únicas em A.

Exemplo 1.6. Os corpos $\mathbb{R}$ e $\mathbb{C}$ são álgebras de divisão associativas e comutativas de dimensão 1 e 2, respectivamente.

Exemplo 1.7. As álgebras $Mat(n, \mathbb{R})$ e $Mat(n, \mathbb{C})$ não são álgebras de divisão quando $n > 1$.

Exemplo 1.8. O $\mathbb{R}$-espaço vetorial $\mathbb{C}$ com a multiplicação dada por

$$(w, z) \in \mathbb{C} \times \mathbb{C} \longmapsto \overline{wz} \in \mathbb{C}$$

é uma álgebra de divisão 2-dimensional comutativa, associativa e sem elemento identidade.

Proposição 1. Seja A uma $\mathbb{R}$-álgebra de divisão associativa com identidade, então o conjunto $G := A \setminus \{0\}$ é um grupo com respeito à multiplicação em A. O elemento neutro de G é o elemento identidade de A.

Demonstração. Primeiro notemos que a multiplicação é fechada (e associativa) em G. Por outro lado, desde que em G toda equação $ax = b$ e $ya = b$ possui solução única, G é de fato um grupo.

□

É claro que toda álgebra de divisão é uma álgebra sem divisores de zero. Com relação a recíproca temos o seguinte critério:

Proposição 2. Seja A uma $\mathbb{R}$-álgebra de dimensão finita. As seguintes afirmações são equivalentes:

i) A é uma álgebra de divisão.

ii) A é uma álgebra sem divisores de zero.

Demonstração. Só falta mostrar que $ii) \Rightarrow i)$. Com efeito, seja $0 \neq a \in A$, a aplicação $\mathbb{R}$-linear $A \to A$ definida por $x \mapsto ax$ é injetiva. Mais ainda, como $dim(A)$ é finita, é bijetiva. Portanto, toda equação $ax = b$ tem uma única solução. De modo análogo, se consideramos a aplicação $\mathbb{R}$-linear $A \to A$ dada por $x \mapsto xa$, vemos que toda equação $ya = b$ tem uma única solução. □

Não é trivial dar um exemplo de uma $\mathbb{R}$-álgebra de divisão associativa de dimensão finita diferente de $\mathbb{R}$ e de $\mathbb{C}$. O primeiro exemplo é a *álgebra dos quaternios de Hamilton* que estudaremos no próximo capítulo.

Capítulo 2

Os Quatérnios

Os quatérnios foram descobertos pelo matemático irlandês William Rowan Hamilton com objetivo de mostrar a construção de uma álgebra de dimensão 4. Desde então, o conjunto formado por tais números é denotado por $\mathbb{H}$.

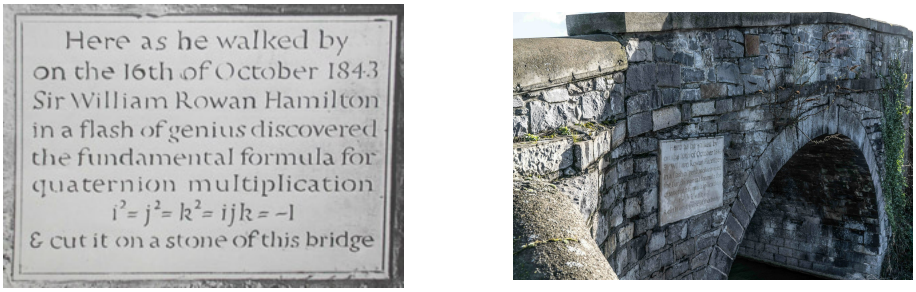


Figura 2.1: Placa e a Ponte Broome.

Em 16 de outubro de 1843, Hamilton teve uma inspiração durante uma caminhada ao longo do Canal Real de Dublin, na Irlanda. Ele ficou tão entusiasmado que, usando um canivete, talhou a descoberta na Ponte Broome.

2.1 Os quatérnios de Hamilton

No $\mathbb{R}$-espaço vetorial 4-dimensional $\mathbb{R}^4$ escolhemos a base canônica

$$e_1 = (1,0,0,0), e_2 = (0,1,0,0), e_3 = (0,0,1,0), e_4 = (0,0,0,1).$$

Vimos na última seção do capítulo anterior que uma estrutura de álgebra sobre $\mathbb{R}^4$ fica bem definida, se explicitarmos os 16 produtos e_ie_j, $1 \leq i,j \leq 4$. Primeiro escolhemos e_1 como o elemento identidade e os 9 produtos restantes e_ie_j são definidos usando as chamadas *relações de Hamilton*:

$$\begin{cases} e_2 \cdot e_2 := -e_1 & e_2 \cdot e_3 := e_4 & e_2 \cdot e_4 := -e_3 \\ e_3 \cdot e_2 := -e_4 & e_3 \cdot e_3 := -e_1 & e_3 \cdot e_4 := e_2 \\ e_4 \cdot e_2 := e_3 & e_4 \cdot e_3 := -e_2 & e_4 \cdot e_4 := -e_1 \end{cases}$$

A $\mathbb{R}$-álgebra de dimensão 4 construída de esta forma é chamada *álgebra dos quatérnios* e é denotada por $\mathbb{H}$. Os elementos de $\mathbb{H}$ são tradicionalmente chamados *quatérnios de Hamilton*.

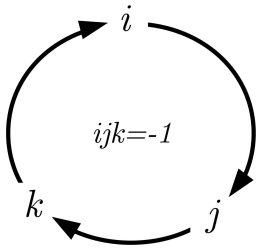
Desde que, $e_2 \cdot e_3 \neq e_3 \cdot e_2$, logo segue que $\mathbb{H}$ é uma álgebra não comutativa.

A validez das 27 equações $e_i(e_je_k) = (e_ie_j)e_k, 2 \leq i,j,k \leq 4$ pode ser verificada diretamente a partir das relações de Hamilton. Em consequência $\mathbb{H}$ é uma álgebra associativa.

Usualmente os vetores básicos e_1, e_2, e_3, e_4 são denotados por $1, i, j, k$, respectivamente. Portanto:

$$i^2 = j^2 = k^2 = i \cdot j \cdot k = -1, \ i \cdot j = -j \cdot i = k.$$

Notemos que os outros produtos derivam-se dos anteriores por um intercâmbio cíclico de i, j, k.



Usando a propriedade distributiva obtemos a *regra do produto* em $\mathbb{H}$:

$$(\alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k) \cdot (\alpha_2 e + \beta_2 i + \gamma_2 j + \delta_2 k) = (\alpha_1\alpha_2 - \beta_1\beta_2 - \gamma_1\gamma_2 - \delta_1\delta_2)e +$$

$$(\alpha_1\beta_2 + \alpha_2\beta_1 + \gamma_1\delta_2 - \gamma_2\delta_1)i + (\alpha_1\gamma_2 - \beta_1\delta_2 + \gamma_1\alpha_2 + \delta_1\beta_2)j + (\alpha_1\delta_2 + \beta_1\gamma_2 - \gamma_1\beta_2 + \delta_1\alpha_2)k.$$

2.2 A álgebra das matrizes $\mathcal{H}$

O conjunto das matrizes $\mathcal{C} = \left\{ \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} : \alpha, \beta \in \mathbb{R} \right\}$ é uma $\mathbb{R}$-subálgebra de $Mat(2, \mathbb{R})$ e a aplicação $\alpha + \beta i \longmapsto \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ é um isomorfismo de $\mathbb{R}$-álgebras $\mathbb{C} \longrightarrow \mathcal{C}$. Isto permite ver a álgebra dos números complexos como uma álgebra de matrizes. Em analogia com isto, veremos a seguir, que existe um isomorfismo de álgebras entre $\mathbb{H}$ e uma certa álgebra de matrizes. Para isto, consideremos agora o conjunto de matrizes complexas de ordem 2×2

$$\mathcal{H} = \left\{ \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix} : z, w \in \mathbb{C} \right\} \subset Mat(2, \mathbb{C}).$$

Proposição 3. $\mathcal{H}$ é uma $\mathbb{R}$-subálgebra de $Mat(2, \mathbb{C})$, com elemento identidade $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Além disso, toda matriz $A = \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix} \in \mathcal{H}$ safistaz a equação quadrática

$$A^2 - \mathrm{tr}(A)A + \det(A)E = 0,$$

onde $\mathrm{tr}(A) = 2Re(z)$ é o traço da matriz A e $\det(A) = \mid z \mid^2 + \mid w \mid^2$ seu determinante.

Mais ainda, $\mathcal{H}$ é uma $\mathbb{R}$-álgebra de divisão associativa de dimensão 4.

Demonstração. Não é difícil ver que $\mathcal{H}$ é um $\mathbb{R}$-subespaço vetorial de $Mat(2, \mathbb{C})$ de dimensão 4, fechado para a multiplicação de matrizes. A equação matricial pode ser verificada fazendo uso do Teorema de Cayley-Hamilton. A álgebra $\mathcal{H}$ é associativa pois $Mat(2, \mathbb{C})$ é associativa. Para provar que $\mathcal{H}$ é de divisão bastará ver que é uma álgebra sem divisores de zero (veja Proposição 2). De fato, sejam $A, B \in \mathcal{H}$ tais que $AB = 0$. Então $\det(AB) = 0$, logo $\det(A) = 0$ ou $\det(B) = 0$. Como $\det \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix} = \mid z \mid^2 + \mid w \mid^2$ se anula somente para $z = w = 0$, concluimos que $A = 0$ ou $B = 0$. □

Proposição 4. A aplicação $F : \mathbb{H} \longrightarrow \mathcal{H}$ definida por

$$(\alpha, \beta, \gamma, \delta) \longmapsto \begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix},$$

é um isomorfismo de $\mathbb{R}$-álgebras.

Demonstração. É claro que a aplicação F é um isomorfismo $\mathbb{R}$-linear. De acordo com a seção 1.5 bastará verificar que $F(e_i e_j) = F(e_i)F(e_j)$ para $i, j = 1, ..., 4$. Para isto, consideremos as matrizes $E := F(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I := F(e_2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J := F(e_3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

e $K := F(e_4) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ que são as imágenes via F de e_1, e_2, e_3, e_4 respectivamente, satisfacem as mesmas relações de multiplicação que e_1, e_2, e_3, e_4. As relações $I^2 = J^2 = -E, IJ = -JI = K$ são verificadas diretamente e as outras relações podem ser derivadas da propriedade associativa, por exemplo, $K^2 = (IJ)(-JI) = -IJ^2I = I^2 = -E$. □

Combinando a Proposição 3 com a Proposição 4 temos o seguinte resultado.

Teorema 2.2.1. A álgebra dos quatérnios de Hamilton $\mathbb{H}$ é uma $\mathbb{R}$-álgebra de divisão associativa de dimensão 4.

O conjunto $\mathcal{H} \setminus \{0\}$ é um grupo com respeito à multiplicação em virtude da Proposição 1. Mais ainda, quando usando as relações que aparecem na prova da Proposição 4, é possível demonstrar que o conjunto $\{E, -E, I, -I, J, -J, K, -K\}$ é um subgrupo de $\mathcal{H}\setminus\{0\}$ de ordem 8, onde cada um dos elementos diferentes de E tem ordem 4. Tal grupo é conhecido como *grupo (finito) dos quatérnios*. Este grupo é um exemplo de que um grupo não Abeliano com a propriedade que todo subgrupo é *normal*.

2.3 O Espaço Imaginário $\mathrm{Im}(\mathbb{H})$

Consideremos a base usual e, i, j, k de $\mathbb{H}$. O $\mathbb{R}$-subespaço vetorial

$$\mathrm{Im}(\mathbb{H}) := \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

gerado pelos vetores i, j, k, é chamado, em analogia com os números complexos, *espaço imaginário de* $\mathbb{H}$.

É claro que $\mathbb{H}$ é a soma direta dos subespaços $\mathbb{R}e$ e $\mathrm{Im}(\mathbb{H})$, isto é,

$$\mathbb{H} = \mathbb{R}e \oplus \mathrm{Im}(\mathbb{H}).$$

Observemos que a definição do espaço imaginário $\mathrm{Im}(\mathbb{H})$, aparentemente depende da base e, i, j, k. Mostremos que não é o caso. Para isto, notemos que um quatérnio $x = \alpha e + \beta i + \gamma j + \delta k$ satisfaz, em virtude da Proposição 3 e da Proposição 4, a equação quadrática

$$x^2 = 2\alpha x - (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)e.$$

Desde que $x \in \mathrm{Im}(\mathbb{H})$, se e somente se, $\alpha = 0$, obtemos uma caracterização do espaço $\mathrm{Im}(\mathbb{H})$, com representação livre de bases,

$$\mathrm{Im}(\mathbb{H}) = \left\{x \in \mathbb{H} : x^2 \in \mathbb{R}e \ , \ x \notin \mathbb{R}e \setminus \{0\}\right\}.$$

Proposição 5. Sejam $u, v \in \mathrm{Im}(\mathbb{H})$. Então,

$$u^2 = -\lambda e \ \text{ para algum } \ \lambda \in \mathbb{R}, \ \lambda \geq 0, u \cdot v + v \cdot u \in \mathbb{R}e.$$

Demonstração. Se $u = \beta i + \gamma j + \delta k$, então $u^2 = -(\beta^2 + \gamma^2 + \delta^2) \cdot e$, com $(\beta^2 + \gamma^2 + \delta^2) \geq 0$. Como $u, v,\ u + v \in \mathrm{Im}(\mathbb{H})$. Pelo anterior, $u^2, v^2, (u+v)^2 \in \mathbb{R}e$. Portanto, $u \cdot v + v \cdot u = (u+v)^2 - u^2 - v^2 \in \mathbb{R}e$. □

Em particular, para todo $u \in \mathrm{Im}(\mathbb{H}), u \neq 0$, existe um escalar $\rho = \sqrt{(\lambda)^{-1}}$ tal que $(\rho u)^2 = -e$ (tal processo é chamado *normalização*).

Em vista que $\mathbb{H} = \mathbb{R}e \oplus \mathrm{Im}(\mathbb{H})$, todo quatérnio x pode ser escrito de maneira única como

$$x = \alpha e + u, \quad \text{onde} \quad \alpha \in \mathbb{R} \quad \text{e} \quad u \in \mathrm{Im}(\mathbb{H}).$$

Nesta expressão, αe é chamada *parte escalar* ou *parte real* de x. Entanto que, u é conhecida como *parte vetorial* ou *parte imaginaria* de x. Todo elemento de $\mathrm{Im}(\mathbb{H})$ é conhecido como *vector*.

2.4 Relação do produto de quatérnios com o produto vetorial e com produto escalar

Para quatérnios imaginários ou vetores $u = \beta i + \gamma j + \delta k, v = \rho i + \sigma j + \tau k$, temos que

$$u \cdot v = -(\beta\rho + \gamma\sigma + \delta\tau)e + (\gamma\tau - \delta\sigma)i + (\delta\rho - \beta\tau)j + (\beta\sigma - \gamma\rho)k.$$

Vemos que, a parte escalar do produto em $\mathbb{H}$ é o inverso aditivo do *produto escalar euclideano* $\langle u, v\rangle$ dos vetores $u = (\beta, \gamma, \delta)$ e $v = (\rho, \sigma, \tau) \in \mathbb{R}^3$. A parte vetorial de $u \cdot v$ coincide com o *produto vetorial* $u \times v$ desses vetores. Obtemos assim a fórmula estética:

$$v \cdot u = -\langle u, v\rangle e + v \times u = -\langle u, v\rangle e - u \times v, \qquad u, v, u \times v \in \mathrm{Im}(\mathbb{H}). \tag{2.1}$$

Note que a aplicação $(u, v) \longmapsto u \times v$ é bilinear e anticomutativa, isto é,

$$v \times u = -u \times v, \qquad u, v \in \mathrm{Im}(\mathbb{H}). \tag{2.2}$$

Da equação (2.2)obtemos, usando a equação (2.1), as seguintes igualdades:

$$u \times v = \frac{1}{2}(u \cdot v - v \cdot u), \quad u \times v - u \cdot v = -\frac{1}{2}uv - \frac{1}{2}vu - uv, \quad u, v \in \mathrm{Im}(\mathbb{H}). \tag{2.3}$$

O produto vetorial não é associativo. Para provar esta afirmação, vamos verificar a validade da seguinte fórmula:

$$u \times (v \times w) = \frac{1}{2}(u \cdot v \cdot w - v \cdot w \cdot u). \tag{2.4}$$

Com efeito, desde que $u \cdot v \cdot w = -\langle v, w\rangle u + u(v \times w)$ e $v \cdot w \cdot u = -\langle v, w\rangle u + (v \times w)u$, pela equação (2.1), a identidade (2.4) segue, se observamos que $u \cdot (v \times w) - (v \times w) \cdot u = 2u \times (v \times w)$.

Como substituta, em alguma medida, da propriedade associativa temos a

$$u \cdot v \cdot w = u \cdot [-\langle v, w\rangle + v \times u] = -\langle v, w\rangle u + u \cdot (v \times w)$$

$$v \cdot w \cdot u = u \cdot [-\langle v, w\rangle \cdot u + v \times u] \cdot = -\langle v, w\rangle u + u \cdot (v \times w) \cdot u$$

$$\begin{aligned} \rightarrow u \cdot v \cdot w - v \cdot w \cdot u &= u \cdot (v \times w) + u \cdot (v \times w) \cdot u \\ &= 2u \times (v \times w) \end{aligned}$$

Proposição 6. (*Identidade de Grassmann*): Sejam $u, v, w \in Im(\mathbb{H})$. Então

$$u \times (v \times w) = \langle u, w\rangle v - \langle u, v\rangle w.$$

Demonstração. Esta identidade pode ser deduzida de (2.4) com ajuda de (2.3), desde que

$$u \cdot v \cdot w - v \cdot w \cdot u = (u \cdot v + v \cdot u) \cdot w - v \cdot (u \cdot w + w \cdot u) = -2\langle u, v\rangle w + 2\langle u, w\rangle v.$$

□

Se introduzimos ciclicamente u, v, w na Identidade de Grassmann, obtemos a

Proposição 7. (Identidade de Jacobi): Sejam $u, v, w \in Im(\mathbb{H})$. Então

$$u \times (v \times w) + v \times (w \times u) + w \times (u \times v) = 0.$$

Definindo uma álgebra de Lie temos que

Definição 2.1. Álgebra de Lie Consiste de um espaço vetorial $\eth$ munido de um produto (colchete ou comutador).

$$[,] : \eth \times \eth$$

com as seguintes propriedades

1. é bilinear,
2. anti-simétrico, isto é, $[X, X] = 0$ para todo $X \in \eth$ (o que implica $[X, Y] = -[Y, X]$, para todo $X, Y \in$e é equivalente ao corpo de escalares não é de característica doi) e
3. satisfaz a identidade de Jacobi, isto é, para todo $X, Y, Z \in \eth$,

$$[X, [Y, Z]] = [[X, Y], Z] + [Y[X, Z]]$$

Esta identidade juntamente com (2.3) demonstram que o espaço real $\mathbb{R}^3 \simeq \mathrm{Im}(\mathbb{H})$ equipado com o produto vetorial, é uma álgebra de Lie.

Segue-se diretamente da equação 2.1 e da regra do produto a seguinte identidade

$$| \langle u, v \rangle |^2 + | u \times v |^2 = | u |^2 | v |^2. \tag{2.5}$$

Notemos que de 2.5 podemos deduzir diretamente a famosa *Desigualdade de Cauchy-Schwarz*. Com efeito, se escrevemos $\langle u, v \rangle = | u || v | \cos(\varphi)$, para algum $\varphi \in [0, \pi]$, obtemos

$$| u \times v | = | u || v | \sin(\varphi).$$

Portanto $| u \times v |$ é a área do paralelogramo gerado pelos vetores u e v.

O *triplo produto escalar* de três vetores $u, v, w \in Im(\mathbb{H})$ é o número real $\langle u \times v, w \rangle$. Como $\mathbb{R}e$ e $Im(\mathbb{H})$ são ortogonais, se segue de (1) que

$$\langle u \times v, w \rangle = \langle uv, w \rangle, \qquad u, v, w \in Im(\mathbb{H})$$

Da definição de produto vetorial, não é difícil ver que $\langle u \times v, u \rangle = 0$. Portanto $\langle (u+v) \times w, u+v \rangle = 0$, logo $\langle u \times w, v \rangle + \langle v \times w, u \rangle = 0$ e em consequência temos a seguinte regra:

Proposição 8. (Regra do Intercambio) : Sejam $u, v, w \in Im(\mathbb{H})$. Então

$$\langle u \times v, w \rangle = \langle v \times w, u \rangle = \langle w \times u, v \rangle.$$

□

Agora é claro que a aplicação $(u, v, w) \mapsto \langle u \times v, w \rangle$ é uma aplicação 3-linear alternada do espaço $\mathrm{Im}(\mathbb{H})$ sobre $\mathbb{R}$. Portanto trata-se de uma função determinante.

2.5 O centro de $\mathbb{H}$.

Seja A um $\mathbb{R}$-álgebra. O conjunto

$$Z(A) = \{z \in A : zx = xz \ \ para \ \ todo \ \ x \in A\}$$

é chamado *Centro de A*. Se A é associativa, então $Z(A)$ é uma subálgebra de A; por outro lado, $Z(A) = A$ se, e somente se A é comutativa. No caso que A tenha elemento identidade e vale a inclusão $\mathbb{R}e \subseteq A$. O caso extremo, $\mathbb{R}e = A$ também pode acontecer.

Proposição 9. O centro de $\mathbb{H}$ é $\mathbb{R}e$.

Demonstração. Seja $z \in Z(\mathbb{H})$. Suponhamos que $z = \alpha e + \beta i + \gamma j + \delta k$. Da igualdade $z \cdot i = i \cdot z$, obtemos $-\beta + \alpha i + \delta j - \gamma k = -\beta i + \alpha i - \delta j + \gamma k$, portanto $\delta = \gamma = 0$. Logo $z = \alpha e + \beta i$. Da equação $z \cdot j = j \cdot z$, temos que $\alpha j + \beta k = \alpha j - \beta k$. Isto implica que $\beta = 0$. □

O fato que $\mathbb{H}$ não é comutativa traz consigo muitas consequencias inusuais. Uma delas é que polinômios podem ter máis raízes que seu grau. Por exemplo o polinômio quadrático $X^2 + e$ tem como zeros todos os quatérnios vetoriales $u = \beta i + \gamma j + \delta k$ tais que $(\beta^2 + \gamma^2 + \delta^2) = 1$. Estes quatérnios representam a esfera 2-dimensional $\mathbb{S}^2$ em $\mathbb{R}^3$.

Por outro lado, a não comutatividade de $\mathbb{H}$ faz que a definição usual de determinantes falhe. Por exemplo,

$$det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc \qquad \text{ou} \qquad det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - cb$$

não são definições adequadas, pois no primeiro caso

$$det \begin{pmatrix} i & j \\ i & j \end{pmatrix} = i \cdot j - j \cdot i = 2k \neq 0$$

e no segundo caso

$$\begin{pmatrix} i & i \\ j & j \end{pmatrix} = i \cdot j - j \cdot i = 2k \neq 0$$

Assim, o "determinante"seria diferente de zero, mesmo que no primeiro caso a matriz tem duas colunas iguais, enquanto no segundo caso, duas linhas iguais.

A não comutatividade de $\mathbb{H}$ também é o motivo pelo qual $\mathbb{H}$ possui muitos $\mathbb{R}$-automorfismos. De fato, para cada $0 \neq a \in \mathbb{H}$,

$$h_a : \mathbb{H} \longrightarrow \mathbb{H}, x \longmapsto axa^{-1}$$

é um automorfismo de $\mathbb{H}$.

2.6 $\mathbb{H}$ como um espaço vetorial Euclidiano.

Seja V um $\mathbb{R}$-espaço vetorial. Lembremos que uma forma bilinear $V \times V \to \mathbb{R}, (x, y) \mapsto \langle x, y \rangle$ é um **Produto Interno** se é simétrica e definida positiva, isto é,

$$\langle x, y \rangle = \langle y, x \rangle \qquad \text{e} \qquad \langle x, x \rangle > 0 \ \text{ para } x \neq 0.$$

O par $(V, \langle\ ,\ \rangle)$ é chamado **Espaço Euclidiano**. O número $\mid x \mid := \sqrt{\langle x, x \rangle} \geq 0$ é a **norma de** x. Dois vetores $x, y \in V$ são ditos **ortogonais** se $\langle x, y \rangle = 0$.

Para elementos $x = \alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k, y = \alpha_2 e + \beta_2 i + \gamma_2 j + \delta_2 k \in \mathbb{H}$, a aplicação

$$\langle x, y \rangle = \alpha_1 \alpha_2 + \beta_1 \beta_2 + \gamma_1 \gamma_2 + \delta_1 \delta_2 \in \mathbb{R}.$$

define um produto interno sobre $\mathbb{H}$, o qual é denominado **Produto Interno Canónico.**

Neste caso, a norma de $x \in \mathbb{H}$ é dada por

$$| x |^2 := \langle x, x \rangle = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

Notemos que os vetores básicos e, i, j, k formam uma base ortonormal de $\mathbb{H}$.

Como $\mathbb{H} = \mathbb{R}e \oplus \mathrm{Im}(\mathbb{H})$, todo quatérnio x possui uma única representação (livre de bases) $x = \alpha e + u$, onde $\alpha \in \mathbb{R}$ e $u \in \mathrm{Im}(\mathbb{H})$. Em analogia com a conjugação nos números complexos em $\mathbb{C}$ definimos a $\mathbb{R}$**-conjugação linear** como a aplicação

$$\mathbb{H} \to \mathbb{H}, \quad x \mapsto \bar{x} := \alpha e - u.$$

Segue diretamente da definição as seguintes igualdades.

$$\bar{\bar{x}} = x, \qquad \mathrm{Im}(\mathbb{H}) = \{x \in \mathbb{H} : \bar{x} = -x\}$$

Mais ainda,

$$| \bar{x} | = | x | \quad \text{para todo} \quad x \in \mathbb{H}.$$

Por outro lado, a aplicação $(x, y) \mapsto \overline{xy} - \bar{y}\bar{x}, \;\; x, y \in \mathbb{H}$ é bilinear e para cada par de elementos básicos e, i, j, k de $\mathbb{H}$ se anula, em consequência trata-se da aplicação nula. Portanto,

$$\overline{xy} = \bar{y}\bar{x}, \qquad x, y \in \mathbb{H}.$$

Em analogia com a aplicação parte real nos complexos $\mathbb{C}$, introduzimos a $\mathbb{R}$**-forma linear**

$$\mathrm{Re} : \mathbb{H} \longrightarrow \mathbb{R}, \quad x = \alpha e + u \longmapsto \mathrm{Re}(x) := \alpha.$$

Claramente Re é caracterizada pelas seguintes propriedades:

$$\mathrm{Re}(e) = 1, \qquad \ker(\mathrm{Re}) = \mathrm{Im}(\mathbb{H}).$$

Também segue da definição que

$$x + \bar{x} = 2\mathrm{Re}(x)e \;\; , \;\; \mathrm{Re}(\bar{x}) = \mathrm{Re}(x).$$

A equação quadrátrica estabelecida na Proposição 3 pode ser reescrita como

$$x^2 - 2\mathrm{Re}(x) + | x |^2 e = 0.$$

Desde que a aplicação bilinear $(x, y) \in \mathbb{H} \times \mathbb{H} \longmapsto \mathrm{Re}(xy) - \mathrm{Re}(yx) \in \mathbb{R}$ se anula para cada par de elementos básicos e, i, j, k de $\mathbb{H}$, deduzimos que

$$\mathrm{Re}(x \cdot y) = \mathrm{Re}(y \cdot x).$$

De forma explícita, se $x = \alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k$ e $y = \alpha_2 e + \beta_2 i + \gamma_2 j + \delta_2 k$, são dois quatérnios, então

$$\mathrm{Re}(x \cdot y) = \alpha_1\alpha_2 - \beta_1\beta_2 - \gamma_1\gamma_2 - \delta_1\delta_2.$$

A forma bilinear $\mathrm{Re}(x \cdot y)$ origina a **métrica de Lorentz de $\mathbb{R}^4$.**

As regras

$$\overline{x \cdot y} = \bar{y} \cdot \bar{x} \quad \text{e} \quad \mathrm{Re}(x \cdot y) = \mathrm{Re}(y \cdot x)$$

são mais fáceis de entender se fizermos uso do isomorfismo introduzido na Proposição 3, ou seja,

$$F : \mathbb{H} \longrightarrow \mathbb{H}$$

$x = (\alpha, \beta, \gamma, \delta) \longmapsto \begin{pmatrix} z & -w \\ \bar{w} & \bar{z} \end{pmatrix}$, onde $z := \alpha + \beta i$ e $w := \gamma + \delta i \in \mathbb{C}$, e trabalhamos na álgebra das matrizes $\mathcal{H}$. Se A^t é a transposta da matriz A, temos que

$$F(\bar{x}) = \overline{F(x)^t}, \qquad \mathrm{Re}(x) = \frac{1}{2}\mathrm{Tr}(F(x)).$$

Logo

$$F(\overline{x \cdot y}) = \overline{F(xy)^t} = \overline{(F(x)F(y))^t} = \overline{F(y)^t F(x)^t} = \overline{F(y)^t} \ \ \overline{F(x)^t} = F(\bar{y})F(\bar{x}) = F(\bar{y}\bar{x}).$$

Portanto $\overline{x \cdot y} = \bar{y}\bar{x}$, pois F é injetiva.

Por outro lado, em vista que $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, obtemos que

$$\mathrm{Tr}(F(x \cdot y)) = \mathrm{Tr}(F(x) \cdot F(y)) = \mathrm{Tr}(F(y) \cdot F(x)) = \mathrm{Tr}(F(y \cdot x)),$$

e portanto,

$$\mathrm{Re}(x \cdot y) = \mathrm{Re}(y \cdot x).$$

Inicialmente introduzimos o produto interno canônico em termos da base e, i, j, k de $\mathbb{H}$. Porém, a seguir veremos uma forma de descrever o produto interno independente da base, usando a conjugação. Para isto note que

$$x\bar{x} = \bar{x}x = \langle x, x \rangle e.$$

Em particular,

$$x^{-1} = \mid x \mid^{-2} \bar{x} \quad \text{se} \quad x \neq 0.$$

Escrevendo $x + y$ no lugar de x na expressão de cima, obtemos uma fórmula que estabelece o produto interno em termos do produto de quatérnios.

Proposição 10. Sejam $x, y \in \mathbb{H}$, então

$$\langle x, y \rangle e = \frac{1}{2}(x \cdot \bar{y} + y \cdot \bar{x}).$$

Disto obtemos o seguinte critério
Critério de Ortogonalidade: $\langle x, y\rangle = 0 \Leftrightarrow x \cdot \bar{y} = -y \cdot \bar{x} \Leftrightarrow x\bar{y} \in Im(\mathbb{H})$.

Lembremos que o produto interno canônico em $\mathbb{C}$ está dado por

$$\mathbb{R}e(x \cdot \bar{y}).$$

Vejamos agora que o mesmo acontece em $\mathbb{H}$.

Proposição 11. Para $x, y \in \mathbb{H}$, vale a seguinte igualdade:

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

Em particular,

$$\langle x, e\rangle = \mathrm{Re}(x).$$

Demonstração. Sabemos que $\langle x, y\rangle e = \frac{1}{2}(x \cdot \bar{y} + y \cdot \bar{x})$. Mas $y\bar{x} = \overline{x\bar{y}}$, então

$$x \cdot \bar{y} + y \cdot \bar{x} = 2\mathrm{Re}(x \cdot \bar{y})e.$$

Isto mostra o desejado. □

Tal como acontece em $\mathbb{C}$, o produto interno em $\mathbb{H}$ se "comporta bem" com respeito ao produto.

Proposição 12 ((Regra do Produto)). Para $x, y \in \mathbb{H}$ vale a seguinte igualdade:

$$\mid x \cdot y \mid = \mid x \mid\mid y \mid .$$

Demonstração. Usando as regras anteriores e a propriedade associativa temos que

$$\mid x \cdot y \mid^2 e = \langle x{\cdot}y, x{\cdot}y\rangle e = \overline{x \cdot y}x{\cdot}ye = \bar{y}{\cdot}\bar{x}x{\cdot}ye = \bar{y}{\cdot}(\bar{x}{\cdot}x){\cdot}ye = \langle x, x\rangle\bar{y}{\cdot}ye = \langle x, x\rangle\langle y, y\rangle e = \mid x \mid^2 \mid y \mid^2 e.$$

□

Proposição 13 ((Identidade de Lagrange)). Para todo $\alpha_1, \beta_1, \gamma_1, \delta_1, \alpha_2, \beta_2, \gamma_2, \delta_2 \in \mathbb{R}$ se cumpre que:

$$\begin{gathered}(\alpha_1{}^2 + \beta_1{}^2 + \gamma_1{}^2 + \delta_1{}^2)(\alpha_2{}^2 + \beta_2{}^2 + \gamma_2{}^2 + \delta_2{}^2) = \\ (\alpha_1\alpha_2 - \beta_1\beta_2 - \gamma_1\gamma_2 - \delta_1\delta_2)^2(\alpha_1\beta_2 + \alpha_2\beta_1 + \gamma_1\delta_2 - \delta_1\gamma_2)^2 + \\ (\alpha_1\gamma_2 + \gamma_1\alpha_2 + \delta_1\beta_2 - \beta_1\delta_2)^2 + (\alpha_1\delta_2 + \delta_1\alpha_2 + \beta_1\gamma_2 - \gamma_1\beta_2)^2.\end{gathered}$$

Demonstração. Consideremos os quatérnios

$$x = \alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k \quad \text{e} \quad y = \alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k.$$

Então, usando a regra do produto (Proposição 12), temos que

$$\mid x \mid^2 \mid y \mid^2 = \mid x \cdot y \mid^2,$$

o que equivalente à identidade desejada. □

Proposição 14 (**(Identidade do triplo produto)**). Sejam $x, y \in \mathbb{H}$, então

$$y \cdot x \cdot y = 2\langle \bar{x}, y \rangle y - \langle y, y \rangle \bar{x}.$$

Demonstração. Sabemos pela Proposição 11 que $2\langle \bar{x}, y \rangle e = (\bar{x}\bar{y} + yx)$. Se multiplicamos à direita por y ambos os lados, obtemos o seguinte resultado

$$2\langle \bar{x}, y \rangle y = \bar{x} \cdot \bar{y} \cdot y + y \cdot x \cdot y = \bar{x}(\langle y, y \rangle e) + y \cdot x \cdot y = \langle y, y \rangle \bar{x} + y \cdot x \cdot y.$$

□

Capítulo 3

Algumas conexões de $\mathbb{H}$ com a geometria

3.1 O Grupo $\mathbb{S}^3$

Como consequência da regra do produto, demonstrada na Proposição 12, o conjunto

$$\mathbb{S}^3 := \{x \in \mathbb{H} : \ |x| = 1\}$$

formado por todos os quatérnios de comprimento 1 é um subgrupo do grupo multiplicativo $\mathbb{H}^* = \mathbb{H}\backslash\{0\}$.

Como e, i, j, k são elementos de $\mathbb{S}^3$, fica claro que o grupo $\mathbb{S}^3$ não é Abeliano.

Visto que $\mathbb{H} \cong \mathbb{R}^4$ como espaço topológico, o conjunto $\mathbb{S}^3$ é a esfera unitária compacta e tridimensional.

Proposição 15. Para todo $x \in \mathbb{S}^3$ existem elementos $u, v \in \mathbb{S}^3 \cap \text{Im}(\mathbb{H})$ tais que

$$x = u \cdot v \cdot u^{-1} \cdot v^{-1}.$$

Em consequência, $\mathbb{S}^3$ coincide com seu subgrupo comutador.

Demonstração. Dado $x \in \mathbb{S}$, escolha um elemento $y \in \mathbb{S}^3$ tal que $y^2 = x$. Suponhamos que $y = \alpha e + w$, onde $\alpha \in \mathbb{R}e$ e $w \in \text{Im}(\mathbb{H})$. Considere um vetor $u_1 \in \text{Im}(\mathbb{H})$ ortogonal a w com $|u_1| = 1$, então

$$u_1 \cdot y = \alpha u_1 + u_1 w = \alpha u_1 - \langle u_1, w_1 \rangle e + u_1 \times w = \alpha u_1 + u_1 \times w \in \text{Im}(\mathbb{H}).$$

Seja $v := u_1 y$, então $v \in Im(\mathbb{H})$. Mais ainda, se $u := u_1^{-1} = -u_1$, vamos obter que $y = u \cdot v$, com $u, v \in \text{Im}(\mathbb{H})$ e $|u| = |v| = 1$.

Portanto,

$$x = y^2 = u \cdot v \cdot u \cdot v = u \cdot v \cdot (-u) \cdot (-v) = u \cdot v \cdot u^{-1} \cdot v^{-1}.$$

Isto demonstra o resultado. □

Proposição 16. A aplicação $f : \mathbb{H}^* \longrightarrow \mathbb{R}_+ \times \mathbb{S}^3$ definida por $f(x) = (|x|, |x|^{-1}x)$ é um isomorfismo de grupos topológicos. Além disso, a aplicação $h : \mathbb{H}\backslash\{0\} \longrightarrow \mathbb{S}^3$ dada por $h(x) = x \cdot \overline{x}^{-1}$ é sobrejetiva.

Demonstração. Pela regra do produto podemos provar que f é um homomorfismo contínuo de grupos topológicos. Mais ainda, não é difícil verificar que $g : \mathbb{R}_+^x \times \mathbb{S}^3 \to \mathbb{S}^3$ dada por $g(t, y) = ty$ é a aplicação inversa de f.

Para provar a última parte note que para todo $x \neq 0 \in \mathbb{H}$,

$$x \mapsto x\overline{x}^{-1} = |x|^{-1}x^2 \in \mathbb{S}^3.$$

Isto prova que h está bem definida. Além disso, as igualdades

$$h\left(e + \frac{b}{1+\alpha}\right) = \alpha + b, \quad \text{se} \quad \alpha e + b \in \mathbb{S}^3\backslash\{-e\},\ \alpha \in \mathbb{R},\ b \in \mathrm{Im}(\mathbb{H}), \quad \text{e} \quad h(i) = e$$

mostram que h é sobrejetiva. □

Se $x = \beta + b$, onde $\beta \in \mathbb{R}$, $b \in \mathrm{Im}\mathbb{H}$, então $b^2 = -|b|^2$ e portanto, temos que

$$h(x) = \frac{\beta^2 - |b|^2}{\beta^2 + |b|^2}e + \frac{2\beta}{\beta^2 + |b|^2}b;$$

Assim foi possível obter uma **representação paramétrica** para o grupo $\mathbb{S}^3$:

$$\mathbb{S}^3 = \left\{ \frac{\beta^2 - |\ b\ |^2}{\beta^2 + |\ b\ |^2}e + \frac{2\beta}{\beta^2 + |\ b\ |^2}b : (\beta, b) \in (\mathbb{R} \times\ Im(\mathbb{H})) \setminus \{0\} \right\}$$

3.2 O grupo SU(2)

Lembremos agora que conjunto o $U(2, \mathbb{C}) := \left\{U \in GL(2, \mathbb{C}) : U\overline{U}^t = I\right\}$ formado por todas as matizes unitárias de ordem 2×2 é um subgrupo de $GL(2, \mathbb{C})$, o grupo formado por toda as matrizes invertíveis complexas de ordem 2×2. Desde que $\det(\overline{U}^t) = \overline{\det(U^t)}$, obtemos que $|\det(U)| = 1$ para cada $U \in U(2)$. O *subgrupo unitário especial* é o subgrupo normal de $U(2)$ onde é definido por

$$SU(2) = \{UU(2) : \det(U) = 1\}$$

Em termos da subálgebra $\mathcal{H}$ de $Mat(2,\mathbb{C})$ introduzido na Seção 2.1 temos a seguinte caracterização.

[1]

Proposição 17. $SU(2) = \{A \in \mathcal{H} | \det A = 1\}$. Em particular $SU(2) \subset \mathcal{H}$. Mais ainda, o isomorfismo de $\mathbb{R}$-álgebras $F : \mathbb{H} \to \mathcal{H}$ aplica isomorficamente o grupo $\mathbb{S}^3$ no grupo $SU(2)$.

Demonstração. Seja $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SU(2)$, então $U^{-1} = \overline{U}^t = U = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$

Sendo $U^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, então $d = \overline{a}$, $c = -b$, o que implica que $U \in \mathcal{H}$.

Por outro lado temos que, seja $A \in \mathcal{H}$, tal que $\det(A) = 1$. A prova é direta logo que A satisfaz a equação $A\overline{A}^t = I$, e como consequência $A \in SU(2)$. Para a prova desta segunda equação, observamos que para todo $x \in \mathbb{H}$, $\det(F(x)) = |x|^2$, consequentemente,

$$F(\mathbb{S}^3) = \{A \in \mathcal{H} : \ \det A = 1\} = SU(2).$$

□

[1]Grupo Topológico: É um grupo cujo o conjunto subjacente está munido de uma topologia compatível com o produto no grupo no sentido em que

1. o produto $G \times G \longrightarrow G, p, (g,h) = gh$ é uma aplicação contínua, quando se considera $G \times G$ com topologia do produto
2. $\iota : G \longrightarrow G, \iota(g) = g^{-1}$, é contínua (e, portanto, um homeomorfismo, já que, $\iota - 1 = \iota$).

Capítulo 4

O Teorema de Frobenius

Neste capítulo final daremos uma demonstração explícita do celebrado Teorema de Frobenius, o qual caracteriza as álgebras de divisão associativa de dimensão finita sobre os números reais. Tal resultado foi provado pelo grande matemático alemão Ferdinand Georg Frobenius, em 1877.

4.1 O Teorema de Frobenius

Nesta seção, A denotará uma $\mathbb{R}$-álgebra associativa com divisão e com elemento neutro e cuja dimensão real é finita. É claro que a aplicação $\mathbb{R} \longrightarrow A,\ \alpha \longmapsto \alpha e$ é um homomorfismo injetivo de $\mathbb{R}$-álgebras que permite identificar $\mathbb{R}$ com uma subálgebra de A que denotaremos por $\mathcal{R}$. Vamos supor que $A \neq \mathcal{R}$. Seja b qualquer elemento de A tal que $b \notin \mathcal{R}$ e seja $\mathbb{R}\langle b\rangle$ o subespaço vetorial de A gerado por e e b, isto é,

$$\mathbb{R}\langle b\rangle := \{\alpha e + \beta b :\ \alpha, \beta \in \mathbb{R}\}\,.$$

Lema 4.1.1. Se $b \in A \setminus \mathbb{R}$. Então $\mathbb{R}\langle b\rangle$ é um subconjunto comutativo maximal de A, composto por todos os elementos de A que comutam com b. Mais ainda, $\mathbb{R}\langle d\rangle$ é um corpo isomorfo a $\mathbb{C}$.

Demonstração. Escolha um subespaço F de A que contém a $\mathbb{R}\langle d\rangle$ de dimensão maximal e que seja comutativo. Se $x \in A$ comuta com todo elemento de F, então $F + \mathbb{R}$ também é um subespaço comutativo de A. Portanto deve coincidir com F. Isto implica que $x \in F$, provando que F é um subconjunto comutativo maximal de A. Em particular, se $x0$ é um elemento de F com $x \neq 0$, então x^{-1} comuta com todo elemento y de F, pois a igualdade $x \cdot y = x \cdot y$ implica que $y \cdot x^{-1} = x^{-1} \cdot y$. Portanto $x^{-1} \in F$. Em consequência F é um corpo. Pelo Teorema de Hopf (veja [1]), F é um corpo isomorfo a $\mathbb{C}$. Em particular F têm dimensão real 2. Portanto $\mathbb{R}\langle b\rangle = F$. Finalmente, se $x \in A$ comuta com b, então x comuta com todo elemento de $\mathbb{R}\langle b\rangle = F$, consequentemente x pertence a $\mathbb{R}\langle b\rangle = F$. □

[1]

De acordo com o Lema 4.1.1, existe um elemento $i \in A$ tal que $i^2 = -1$, o qual permite-nos identificar $\mathbb{R}\langle i\rangle$ com $\mathbb{C}$. É claro agora que A também é $\mathbb{C}$-espaço vetorial onde o produto por um escalar é a multiplicação à esquerda em A.
Considere a aplicação $T : A \longrightarrow A$ definida por $T(x) = xi$. Note que T é $\mathbb{C}$-linear. Além disso, desde que $T^2 = -Id$, seus únicos possíveis autovalores são i e $-i$. Denotemos con A^+ e com A^- os $\mathbb{C}$-autoespaços correspondentes. Em outras palavras,

$$A^+ = \{x \in A : xi = ix\}, \quad A^- = \{x \in A : xi = -ix\}.$$

Lema 4.1.2. A álgebra A é a soma direta de A^+ e A^-, isto é,

$$A = A^+ \oplus A^-.$$

Demonstração. É claro que $A^+ \cap A^- = 0$. Por outro lado, se $x \in A$ então $x - i \cdot x \cdot i \in A^+$ e $x + i \cdot x \cdot i \in A^-$. Mais ainda, $x = \frac{1}{2}(x - i \cdot x \cdot i) + \frac{1}{2}(x + i \cdot x \cdot i)$, o que implica que $A = A^+ \oplus A^-$. □

De acordo com o Lema 4.1.1, A^+ é um corpo isomorfo a $\mathbb{C}$. Além disso, se $x, y \in A^-$, então $x \cdot y \in A^+$.
No caso que $A^- = 0$ temos que $A = A^+$. Portanto, nesta situação, A é isomorfo a $\mathbb{C}$. Suponhamos então $A^- \neq 0$. Provaremos que neste caso A é isomorfa à álgebra dos quatérnios $\mathbb{H}$.

Lema 4.1.3. Suponhamos que $A^- \neq 0$, então $\dim_{\mathbb{C}} A^- = 1$. Além disso, se $0 \neq c \in A^-$, então

$$c^2 \in \mathcal{R} \text{ e } c^2 < 0.$$

[1]Teorema de Hopf. Seja A uma $\mathbb{R}$- álgebra de divisão comutativa de dimensão finita. Então $Dim(A) \leq 2$.

Demonstração. Seja $c \in A^- \setminus \{0\}$. As aplicações : $A \longrightarrow A,\ x \longmapsto x \cdot c$ é um isomorfismo $\mathbb{C}$-linear, cuja inversa $S^{-1} : A \longrightarrow A$ é dada pela regra $S^{-1}(x) = xc^{-1}$ para todo $x \in A$. Note que $S(A^+) = A^-$, portanto $\dim_{\mathbb{C}} A^+ = dim_{\mathbb{C}} A^- = 1$. Por outro lado, graças ao Lema 4.1.1, $\mathbb{R}\langle c\rangle$ é um corpo isomorfo a $\mathbb{C}$ que contém a c^2. Mas $c \in A^-$, então $c^2 \in A^+ = \mathbb{R}\langle i\rangle$. Logo, $c^2 \in \mathbb{R}\langle i\rangle \cap \mathbb{R}\langle c\rangle = \mathbb{R}$. Si c^2 fosse identificado com um real positivo, c^2 teria duas raízes quadráticas em $\mathcal{R}$, e portanto três raízes quadráticas em $\mathbb{R}\langle c\rangle$, o que é impossível. Consequentemente, c^2 é identificado com um número negativo. □

Fixemos $0 \neq c \in A^-$. Pelo Lema 4.1.2, existe $k \in \mathbb{R}, k > 0$ tal que $c^2 = -k^2$ e portanto $(\frac{c}{k})^2 = -1$. Denotemos com j o elemento $\frac{c}{k}$, então $j \in A^-$ e $j^2 = -1$. Defina $k := i$, então

$$k \cdot i = (i \cdot j) \cdot i = i \cdot (j \cdot i) = i \cdot (-i \cdot j) = -i \cdot (i \cdot j) = -i \cdot k,$$

o que implica que $k \in A^-$. Desde que i, j é uma base de A^- e como $A = A^+ \oplus A^-$, então e, i, j, k formam uma base de A como $\mathbb{R}$-espaço vetorial. Como $j, k \in A^-$, eles anticomutam com i. Isto juntamente com as igualdades

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

demonstram que e, i, j, k satisfazem as relações estabelecidas para os quatérnios.

Combinando o Lema 4.1.1 com o Lema 4.1.2 e a última análise provam o seguinte resultado:

Teorema 4.1.4 (Teorema de Frobenius)**.** Seja A uma $\mathbb{R}$-álgebra associativa de divisão e dimensão finita. Então, existem três possibilidades:

(i) A é isomorfa à álgebra dos números reais $\mathbb{R}$

(ii) A é isomorfa à álgebra dos números complexos $\mathbb{C}$.

(iii) A é isomorfa à álgebra dos quatérnios $\mathbb{H}$.

Referências Bibliográficas

[1] Napoleón Caro Tuesta, *Álgebras reais com divisão*, livro em preparação.

[2] John Conway, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry* , CR Press, 2003.

[3] H. D. Ebbinghaus et al, *Numbers*, Springer Verlag, 1990.

[4] Claudio Gorodski, *Quatérnions e Rotações: uma Jornada pela Álgebra, Geometria e Topologia*, 2020.

[5] William Rowan Hamilton, *Elements of Quaternions*, Longmans, Green(London), 1866.