UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL

$\mathbb{R}$-álgebras de dimensão finita

Sóstenes Souza de Oliveira

Orientador: Zaqueu Alves Ramos

São Cristóvão, 2017.

UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA
EM REDE NACIONAL

$\mathbb{R}$-álgebras de dimensão finita

Dissertação apresentada ao Departamento de Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Sóstenes Souza de Oliveira

Orientador: Zaqueu Alves Ramos

São Cristóvão, 2017.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Oliveira, Sóstenes Souza de
O48r $\mathbb{R}$-álgebras de dimensão finita / Sóstenes Souza de Oliveira ; orientador Zaqueu Alves Ramos. – São Cristóvão, 2017.
55 f.

Dissertação (mestrado em Matemática) – Universidade Federal de Sergipe, 2017.

1. Matemática. 2. Álgebra. 3. Quatérnios. I. Ramos, Zaqueu Alves, orient. II. Título.

CDU: 512

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

R-álgebras de dimensão finita

por

Sóstenes Souza de Oliveira

Aprovada pela Banca Examinadora:

Prof. Dr. Zaqueu Alves Ramos - UFS
Orientador

Prof. Dr. Danilo Dias da Silva- UFS
Primeiro Examinador

Prof. Dr. Marcelo Fernandes de Almeida
Segundo Examinador

São Cristóvão, 24 de março de 2017.

Agradecimentos

Primeiro a Deus, pelo dom da vida e sua misericórdia infinita.

Minha família, Priscila, Tafnes, Silas e Calebe meus irmãos. Em especial a Edileusa Josefa (Dyla), minha mãe, meu apoio e sustentação.

Ao professor Zaqueu A. Ramos, pela orientação.

Aos professores Danilo D. da Silva e Marcelo F. de Almeida, pela composição da banca.

Aos colegas de mestrado Canuto Ruan, Glauber Evangelista, Edson de Jesus, Deusdete Junior, Italo Guimarães, Wesley Sidnei, Marcone Augusto e Diego Alves pelo tempo de convívio de estudos e descontrações. Em especial, para Emanoel Lázaro, compartilhando todas etapas nesse mestrado.

Aos professores do DMA Almir Rogério, Evilson da Silva, André Dorea, Zaqueu Ramos, Debora Lopes, Kalasas Vasconcelos, Fábio dos Santos, Humberto Viglione, Danilo Dias, Marcelo Fernandes, Bruno Luis e especialmente Giovana Siracusa, pelos ensinamentos, compartilhando conhecimentos. Vocês são além de excelentes profissionais, pessoas maravilhosas.

À Giovana Siracusa, pelo carinho, pelos ensinamentos durante todo curso, sou muito grato a você.

Aos amigos de UNEB, Leniedson Guedes, Rosemar Almeida, Lúcio Flávio, Darlan Regis e Apio Rodrigo, pelos sábados e domingos de estudos, pelos churrascos, pelas viagens e pela amizade construida.

Aos amigos(as) de longa data, Marcos Sidnei, Rodrigo Ceará, Vanessa Santos e Itanajar Lopes.

À Vanessa Santos, pelas orações e conselhos.

À CAPES, pelo apoio financeiro. Enfim, a todos que me ajudaram e compartilharam experiências de estudos em busca do conhecimento.

Resumo

Nesse trabalho estudamos a noção de $\mathbb{R}$-álgebra. A grosso modo, elas são estruturas que generalizam algumas propriedades aritméticas do corpo dos números complexos. A flexibilidade nessa generalização é a não exigência de propriedades como comutatividade, associatividade e existência de elemento identidade. Focamos principalmente nas $\mathbb{R}$-álgebras de divisão de dimensão finita. Como é bem conhecido, módulo isomorfismos existem exatamente quatro dessas $\mathbb{R}$-álgebras. No desenvolvimento da dissertação discutiremos detalhadamente suas principais propriedades algébricas e geométricas.

Palavras Chave: $\mathbb{R}$-álgebras, $\mathbb{R}$-álgebras de divisão, $\mathbb{R}$-álgebras de Composição, Quatérnios, Octônios.

Abstract

In this work we study the notion of $\mathbb{R}$-algebra. Roughly, they are structures that generalize some arithmetic properties of the body of complex numbers. The flexibility in this generalization is the non-requirement of properties such as commutativity, associativity and identity element existence. We focus primarily on the finite dimensional division $\mathbb{R}$-algebras. As is well known, modulo isomorphisms exist exactly four of those $\mathbb{R}$-algebras. In the development of the dissertation we will discuss in detail its main algebraic and geometric properties.

Keywords: $\mathbb{R}$-algebras, $\mathbb{R}$-algebras of division, $\mathbb{R}$-algebra of composition, Quaternions, Octonions.

Lista de símbolos

Símbolo	**Descrição**
$M_n(\mathbb{R})$	espaço das matrizes quadradas de ordem n com entradas em $\mathbb{R}$
$M_n(\mathbb{C})$	espaço das matrizes quadradas de ordem n com entradas em $\mathbb{C}$
$\wedge$	produto vetorial
$\mathbb{R}[x_1, \ldots, x_n]$	anel de polinômios em n variáveis com coeficientes em $\mathbb{R}$
$\mathrm{End}_{\mathbb{R}}(V)$	espaço dos operadores lineares de V
$\mathbb{S}^n$	esfera n-dimensional
$\mathbb{H}$	álgebra dos quatérnios de Hamilton
$\mathbb{O}$	álgebra dos octônios de Cayley

Conteúdo

Introdução

A história da álgebra é dividida em dois períodos. O primeiro período (1700 a.C.-1700 d.C.), denominado de clássico, é caracterizado pelo fato de que os principais temas de estudo são as equações e as manipulações com expressões literais. Nessa fase da álgebra encontramos a criação gradativa dos símbolos e a resolução de equações quadráticas, cúbicas e de grau quatro. No decorrer desse período, a notação algébrica evolui da retórica (verbal) passando pela sincopada (palavras abreviadas) até a simbólica.

O segundo período (final do século XIX até os dias atuais), denominado moderno, é caracterizado pelo estudo das estruturas algébricas. O surgimento desse período é influenciado pela atmosfera da época, onde as palavras abstração e axiomática estavam em destaque. Um dos marcos cruciais para que a álgebra tomasse esse novo direcionamento é sem dúvidas a criação dos quatérnios de Hamilton.

Quando identificamos cada número complexo com um ponto do $\mathbb{R}^2$ é possível conferir a multiplicação entre números complexos interpretações geométricas bastante úteis. Por exemplo, rotações no plano podem ser entendidas como multiplicação por números complexos unitários. Assim, no final do século XIX, Hamilton investigava formas de definir uma multiplicação em $\mathbb{R}^3$ que pudesse ter propriedades algébricas e geométricas semelhantes as de $\mathbb{R}^2$ onde, a exemplo do caso planar, rotações espaciais também pudessem ser entendidas em termos dessa multiplicação. O resultado da investigação de Hamilton foi a criação de um sistema algébrico conhecido como quatérnios.

Inicialmente, os quatérnios de Hamilton ficaram conhecidos como números hipercomplexos. Uma peculiaridade dessa nova modalidade de números é que, diferente dos seus predecessores ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$), a multiplicação para estes não é comutativa. Esse trabalho pioneiro de Hamilton foi fundamental para que outros sistemas onde as regras aritméticas usuais são infringidas pudessem ser considerados. Um exemplo disso, foi a criação dos octônios de Cayley que, além da não comutatividade, também

falha para a propriedade associativa.

Modernamente, os quatérnios de Hamilton e os octônios de Cayley são exemplos da estrutura algébrica denominada de $\mathbb{R}$-álgebra. Nosso objetivo nesse trabalho é estudar esse tipo de estrutura, focando sobretudo nos exemplos de dimensão finita.

Esta dissertação está dividida em quatro capítulos. Na sequência descrevemos brevemente o que acontece em cada um deles.

O primeiro capítulo é dedicado a apresentação dos conceitos mais básicos em torno da noção de $\mathbb{R}$-álgebra tais como: dimensão, homomorfismo, isomorfismo, matriz de multiplicação, etc. São distribuídos ao longo do capítulo exemplos que ilustram cada um dos conceitos introduzidos.

No capítulo 2 especializamos a discussão para as álgebras de divisão e de composição. Discutimos a curiosa relação entre as álgebras de divisão e o problema das esferas paralelizáveis. Também fazemos uma demonstração, baseada em ferramentas básicas de álgebra linear, do belíssimo teorema de Hurwitz. Este teorema revela o quão restritiva é a hipótese de uma álgebra de dimensão finita ser de composição.

No capítulo 3 estudamos as propriedades básicas da célebre álgebra dos quatérnios de Hamilton. O destaque é para o fato de que esta é uma álgebra de divisão, de composição e não comutativa. Mostramos que esta álgebra pode ser apresentada em termos de matrizes ou através de um processo de "duplicação" da álgebra dos complexos. Encerramos este capítulo com o teorema de Frobenius, o qual permite concluir a unicidade da álgebra dos quatérnios módulo isomorfismos.

No quarto e último capítulo nos debruçamos sobre a álgebra dos octônios de Cayley. Apresentamos esta álgebra como uma "duplicação" dos quatérnios. Verificamos que ela é uma álgebra de divisão, de composição, não comutativa e não associativa. Apesar de falhar para a associatividade, mostraremos que a álgebra dos octônios é alternante, propriedade esta que pode ser notada como um enfraquecimento da associatividade.

Capítulo 1

Álgebras sobre $\mathbb{R}$

O objetivo deste capítulo é estabelecer a terminologia básica em torno da noção de $\mathbb{R}$-álgebra. Apresentamos também diversos exemplos que servem de suporte para melhor compreensão dos conceitos apresentados.

1.1 Noções básicas

Seja V um espaço vetorial sobre $\mathbb{R}$.

Definição 1.1.1. Uma *multiplicação* em V é uma operação $* : V \times V \to V$ com as seguintes propriedades:

(a) Para quaisquer $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ e $\alpha \in \mathbb{R}$, $(\alpha\mathbf{x} + \mathbf{y}) * \mathbf{z} = \alpha(\mathbf{x} * \mathbf{z}) + \mathbf{y} * \mathbf{z}$.

(b) Para quaisquer $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$ e $\alpha \in \mathbb{R}$, $\mathbf{x} * (\alpha\mathbf{y} + \mathbf{z}) = \alpha(\mathbf{x} * \mathbf{y}) + \mathbf{x} * \mathbf{z}$.

Obviamente, uma multiplicação em V é, em particular, uma aplicação bilinear.

Definição 1.1.2. Um espaço vetorial V sobre $\mathbb{R}$ equipado com uma multiplicação $*$ é chamado de *álgebra sobre* $\mathbb{R}$ (ou $\mathbb{R}$-álgebra).

Na sequência listamos alguns exemplos de álgebras sobre $\mathbb{R}$.

Exemplo 1.1.3. $\mathbb{R}$ e $\mathbb{C}$ equipados com suas operações usuais de multiplicação são álgebras sobre $\mathbb{R}$.

Exemplo 1.1.4. Seja $\mathbb{R}[x_1, \ldots, x_n]$ o espaço vetorial dos polinômios em n variáveis com coeficientes em $\mathbb{R}$. Este espaço vetorial munido da multiplicação usual de polinômios também é uma álgebra sobre $\mathbb{R}$.

Exemplo 1.1.5. Seja $M_n(\mathbb{R})$ o espaço vetorial das matrizes quadradas de ordem n. Este espaço vetorial munido da operação de multiplicação de matrizes é uma álgebra sobre $\mathbb{R}$.

Exemplo 1.1.6. Seja V um $\mathbb{R}$-espaço vetorial. Denotamos por $\mathrm{End}_{\mathbb{R}}(V)$ o espaço vatorial de todos os operadores lineares de V em V. Este espaço vetorial equipado com a operação de composição é uma $\mathbb{R}$-álgebra.

Exemplo 1.1.7. Dados vetores $\mathbf{u} = (u_1, u_2, u_3)$ e $\mathbf{v} = (v_1, v_2, v_3)$ do $\mathbb{R}^3$, o *produto vetorial* de $\mathbf{u}$ por $\mathbf{v}$, denotado $\mathbf{u} \wedge \mathbf{v}$, é dado pela seguinte igualdade:

$$\mathbf{u} \wedge \mathbf{v} = (u_2v_3 - u_3v_2, u_3v_1 - u_2v_3, u_1v_2 - u_2v_1). \tag{1.1}$$

É de fácil verificação que $\wedge : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ satisfaz as condições para ser uma multiplicação. Assim, $\mathbb{R}^3$ equipado com o produto vetorial é uma álgebra sobre $\mathbb{R}$. Além disso, o produto vetorial também satisfaz as seguintes condições

(a) Para quaisquer $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$, $\mathbf{u} \wedge \mathbf{v} = -\mathbf{v} \wedge \mathbf{u}$.

(d) Para quaisquer $\mathbf{u}, \mathbf{v} \in \mathbb{R}^3$, $\mathbf{u} \wedge \mathbf{v}$ é perpendicular $\mathbf{u}$ e a $\mathbf{v}$.

Definição 1.1.8. Seja $\mathcal{A} = (V, *)$ uma álgebra sobre $\mathbb{R}$. Dizemos que $\mathcal{A}$ é uma álgebra

(a) *comutativa* se $\mathbf{x} * \mathbf{y} = \mathbf{y} * \mathbf{x}$ para quaisquer $\mathbf{x}, \mathbf{y} \in V$.

(b) *associativa* se $\mathbf{x} * (\mathbf{y} * \mathbf{z}) = (\mathbf{x} * \mathbf{y}) * \mathbf{z}$ para quaisquer $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.

(c) *com identidade* se existe $\mathbf{e}$ tal que $\mathbf{x} * \mathbf{e} = \mathbf{e} * \mathbf{x} = \mathbf{x}$ para qualquer $\mathbf{x} \in V$.

Observação 1.1.9. Convém observar que $\mathbb{R}$-álgebras associativas são exemplos da estrutura de anel.

Nos exemplos 1.1.3, 1.1.4 figuram álgebras sobre $\mathbb{R}$ que são comutativas, associativas e com identidade. No exemplo 1.1.5 temos uma álgebra sobre $\mathbb{R}$ que é associativa, com identidade mas falha para a comutatividade sempre que $n \geq 2$. Com efeito, consideremos as seguintes as matrizes de ordem n:

$$A = \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right) \quad \text{e} \quad B = \left(\begin{array}{cc|ccc} 1 & 0 & 0 & \dots & 0 \\ 0 & 2 & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right)$$

Temos

$$A \cdot B = \left(\begin{array}{cc|ccc} 0 & 2 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right) \quad \text{e} \quad B \cdot A = \left(\begin{array}{cc|ccc} 0 & 1 & 0 & \dots & 0 \\ 2 & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array}\right)$$

Logo, $A \cdot B \neq B \cdot A$. Portanto, realmente $M_n(\mathbb{R})$ não pode ser uma álgebra comutativa se $n \geq 2$.

O Exemplo 1.1.7 ilustra uma $\mathbb{R}$-álgebra que não é comutativa, nem associativa e nem tem identidade. De fato:

(a) $(1,0,0) \wedge (0,1,0) = (0,0,1) \neq (0,0,-1) = (0,1,0) \wedge (1,0,0)$; logo, $(\mathbb{R}^3, \wedge)$ não é $\mathbb{R}$-álgebra comutativa.

(b) A identidade não existe por conta da propriedade (a) do Exemplo 1.1.7.

(c) $((1,0,0) \wedge (0,1,0)) \wedge (0,1,0) = (1,0,0) \neq (0,0,0) = (1,0,0) \wedge ((0,1,0) \wedge (0,1,0))$; logo, $(\mathbb{R}^3, \wedge)$ não é uma álgebra associativa.

Definição 1.1.10. Seja $\mathcal{A} = (V, *)$ uma álgebra sobre $\mathbb{R}$. A *dimensão da álgebra* $\mathcal{A}$ é a dimensão do espaço vetorial V.

Denotaremos a dimensão de uma $\mathbb{R}$-álgebra $\mathcal{A} = (V, *)$ por $\dim \mathcal{A}$.

Definição 1.1.11. Seja $\mathcal{A} = (V, *)$ uma $\mathbb{R}$-álgebra. Um subespaço U de $\mathcal{A}$ é chamado de *sub-álgebra* de $\mathcal{A}$ se ele é fechado para a multiplicação de $\mathcal{A}$, isto é, se $\mathbf{u}, \mathbf{v} \in U$, então $\mathbf{u} * \mathbf{v} \in U$.

Obviamente, subálgebras são, em particular, $\mathbb{R}$-álgebras.

Exemplo 1.1.12. Seja $U = \{A \in M_n(\mathbb{R}) \mid a_{ij} = 0 \text{ se } i \neq j\}$, isto é, o subespaço vetorial das matrizes diagonais. É imediato observar que esta é uma subálgebra de $M_n(\mathbb{R})$.

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

Definição 1.2.1. Sejam $\mathcal{A} = (V, *)$ e $\mathcal{A}' = (V', *)$ álgebras sobre $\mathbb{R}$. Um *homomorfismo* da $\mathbb{R}$-álgebra $\mathcal{A}$ para a $\mathbb{R}$-álgebra $\mathcal{A}'$ é uma transformação linear $\varphi : V \to V'$

tal que

$$\varphi(\mathbf{u} * \mathbf{v}) = \varphi(\mathbf{u}) *' \varphi(\mathbf{v})$$

para quaisquer $\mathbf{u}, \mathbf{v} \in V$.

Exemplo 1.2.2. Sejam $\mathcal{A} = (V, *)$ e $\mathcal{A}' = (V', *)$ álgebras sobre $\mathbb{R}$. A aplicação identicamente nula $\mathbb{N} : V \to V'$ dada por $\mathbb{N}(\mathbf{v}) = 0$ para cada $\mathbf{v} \in V$ é um homomorfismo da $\mathbb{R}$-álgebra $\mathcal{A}$ para a $\mathbb{R}$-álgebra $\mathcal{A}'$.

Exemplo 1.2.3. Seja $\mathcal{A} = (V, *)$ uma $\mathbb{R}$-álgebra. A aplicação identidade $\mathbf{1}_V : V \to V$, dada por $\mathbf{1}_V(\mathbf{v}) = \mathbf{v}$ para cada $\mathbf{v} \in V$, é um homomorfismo da $\mathbb{R}$-álgebra $\mathcal{A}$ nela própria.

Exemplo 1.2.4. Seja V um espaço vetorial sobre $\mathbb{R}$ de dimensão n. Fixado uma base B de V, denotaremos a representação matricial de um operador $T \in \mathrm{End}_{\mathbb{R}}(V)$ por $[T]_B$. Como aprendemos nos cursos de álgebra linear, a aplicação $[\quad]_B : \mathrm{End}_{\mathbb{R}}(V) \to M_n(\mathbb{R})$ é uma transformação linear que satisfaz

$$[T \circ S]_B = [T]_B [S]_B$$

para quaisquer $T, S \in \mathrm{End}_R(V)$. Assim, $[\quad]_B$ é um homomorfismo da $\mathbb{R}$-álgebra $\mathrm{End}_{\mathbb{R}}(V)$ para a $\mathbb{R}$-álgebra $M_n(\mathbb{R})$.

Definição 1.2.5. Sejam $\mathcal{A} = (V, *)$ e $\mathcal{A}' = (V', *)$ álgebras sobre $\mathbb{R}$. Um homomorfismo bijetor da $\mathbb{R}$-álgebra $\mathcal{A}$ para a $\mathbb{R}$-álgebra $\mathcal{A}'$ é chamado de *isomorfismo* de $\mathbb{R}$-álgebras.

Dizemos que uma $\mathbb{R}$-álgebra $\mathcal{A} = (V, *)$ é *isomorfa* a uma $\mathbb{R}$-álgebra $\mathcal{A}' = (V', *)$ se existe um isomorfismo de $\mathcal{A}$ para $\mathcal{A}'$. Usamos a notação $\mathcal{A} \simeq \mathcal{A}'$ para dizer que $\mathcal{A}$ é isomorfa a $\mathcal{A}'$.

Proposição 1.2.6. *Sejam $\mathcal{A} = (V, *)$ e $\mathcal{A}' = (V', *')$ álgebras sobre $\mathbb{R}$. Se φ é um isomorfismo de $\mathcal{A}$ para $\mathcal{A}'$ então φ^{-1} é um isomorfismo de $\mathcal{A}'$ para $\mathcal{A}$.*

Prova. Um fato bem conhecido da teoria de funções é que a função inversa de uma bijeção é também uma bijeção. Assim, para provar essa proposição é suficiente concluir que φ^{-1} é um homomorfismo de $\mathbb{R}$-álgebras. Para isso, consideremos $\mathbf{u}', \mathbf{v}' \in V'$. Como φ é uma bijeção, existem (únicos) $\mathbf{u}, \mathbf{v} \in V$ tais que $\varphi(\mathbf{u}) = \mathbf{u}'$ e $\varphi(\mathbf{v}) = \mathbf{v}'$

(equivalentemente, $\mathbf{u} = \varphi^{-1}(\mathbf{u}')$ e $\mathbf{v} = \varphi^{-1}(\mathbf{v}')$). Com isso, temos:

$$\begin{aligned}
\varphi^{-1}(\alpha\mathbf{u}' + \mathbf{v}') &= \varphi^{-1}(\alpha\varphi(\mathbf{u}) + \varphi(\mathbf{v})) \\
&= \varphi^{-1}(\varphi(\alpha\mathbf{u} + \mathbf{v})) \\
&= \varphi^{-1} \circ \varphi(\alpha\mathbf{u} + \mathbf{v}) \\
&= \alpha\mathbf{u} + \mathbf{v} \\
&= \alpha\varphi^{-1}(\mathbf{u}') + \varphi^{-1}(\mathbf{v}'),
\end{aligned}$$

para cada $\alpha \in \mathbb{R}$, e

$$\begin{aligned}
\varphi^{-1}(\mathbf{u}' *' \mathbf{v}') &= \varphi^{-1}(\varphi(\mathbf{u}) *' \varphi(\mathbf{v})) \\
&= \varphi^{-1}(\varphi(\mathbf{u} * \mathbf{v})) \\
&= \varphi^{-1} \circ \varphi(\mathbf{u} * \mathbf{v}) \\
&= \mathbf{u} * \mathbf{v} \\
&= \varphi^{-1}(\mathbf{u}') * \varphi^{-1}(\mathbf{v}'),
\end{aligned}$$

Portanto, segue das igualdades acima o resultado desejado. □

1.3 Matrizes de multiplicação de uma $\mathbb{R}$-álgebra

Seja $\mathcal{A} = (V, *)$ uma $\mathbb{R}$-álgebra de dimensão finita n. Suponhamos $B = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ uma base ordenada de V. Para cada $1 \leq p, q \leq n$, existem $\gamma_{pq}^1, \ldots, \gamma_{pq}^n \in \mathbb{R}$, unicamente determinados, tais que:

$$\mathbf{e}_p * \mathbf{e}_q = \sum_{i=1}^{n} \gamma_{p,q}^i \mathbf{e}_i. \tag{1.2}$$

Assim, para cada $1 \leq i \leq n$ podemos considerar a matriz

$$C^i = \begin{pmatrix} \gamma_{1,1}^i & \gamma_{1,2}^i & \cdots & \gamma_{1,n}^i \\ \gamma_{2,1}^i & \gamma_{2,2}^i & \cdots & \gamma_{2,n}^i \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{n,1}^i & \gamma_{n,2}^i & \cdots & \gamma_{n,n}^i \end{pmatrix}$$

Chamamos $C^1, \ldots, C^n$ *matrizes de multiplicação* da $\mathbb{R}$-álgebra $\mathcal{A}$ com respeito a base ordenada B.

Observamos que se $\mathbf{u} = \sum_{i=1}^{n} u_i \mathbf{e}_i$ e $\mathbf{v} = \sum_{i=1}^{n} v_i \mathbf{e}_i$ são vetores de V então

$$\begin{aligned} \mathbf{u} * \mathbf{v} &= \left(\sum_{p=1}^{n} u_p \mathbf{e}_p \right) * \left(\sum_{q=1}^{n} v_q \mathbf{e}_q \right) \\ &= \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q (\mathbf{e}_p * \mathbf{e}_q) \\ &= \sum_{i=1}^{n} \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma_{p,q}^{i} \mathbf{e}_i \\ &= \sum_{i=1}^{n} z_i \mathbf{e}_i \end{aligned} \tag{1.3}$$

onde

$$z_i = \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma_{p,q}^{i} = [\mathbf{u}]_B^t \cdot C^i \cdot [\mathbf{v}]_B \in \mathbb{R} \tag{1.4}$$

são as cordenadas de $\mathbf{u} * \mathbf{v} \in V$ com respeito a base ordenada B.

Estas igualdades nos mostram que a multiplicação fica completamente determinada pelas matrizes de multiplicação.

Exemplo 1.3.1. Consideremos a $\mathbb{R}$-álgebra dos complexos. Fixada a base ordenada $\{1, \mathbf{i}\}$, do espaço vetorial $\mathbb{C}$ sobre $\mathbb{R}$,temos:

$$1 \cdot 1 = \gamma_{11}^{1} 1 + \gamma_{11}^{2} \mathbf{i} = 1 \cdot 1 + 0 \cdot \mathbf{i},$$

$$1 \cdot \mathbf{i} = \gamma_{12}^{1} 1 + \gamma_{12}^{2} \mathbf{i} = 0 \cdot 1 + 1 \cdot \mathbf{i},$$

$$\mathbf{i} \cdot 1 = \gamma_{21}^{1} 1 + \gamma_{21}^{2} \mathbf{i} = 0 \cdot 1 + 1 \cdot \mathbf{i}$$

e

$$\mathbf{i} \cdot \mathbf{i} = \gamma_{22}^{1} 1 + \gamma_{22}^{2} \mathbf{i} = (-1) \cdot 1 + 0 \cdot \mathbf{i}$$

Com essas igualdades segue que as matrizes de multiplicação da $\mathbb{R}$-álgebra $\mathbb{C}$ são:

$$C^1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{e} \quad C^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Capítulo 2

$\mathbb{R}$-álgebras de divisão e de composição

Dada uma $\mathbb{R}$-álgebra $\mathcal{A} = (V, *)$, uma questão natural é saber sobre a existência de soluções para equações com os seguintes formatos

$$\mathbf{u} * \mathbf{x} = \mathbf{v} \quad \text{e} \quad \mathbf{y} * \mathbf{u} = \mathbf{v}.$$

Este tipo de questão leva à noção de $\mathbb{R}$-*álgebra de divisão*. Veremos no desenrolar desse capítulo que as hipóteses de uma $\mathbb{R}$-álgebra ser de divisão e de dimensão finita são bastante restritivas. Além disso, discutiremos as álgebras de composição que, como será notado, estão intimamente relacionadas às álgebras de divisão.

2.1 $\mathbb{R}$-álgebras de divisão

Definição 2.1.1. Uma $\mathbb{R}$-álgebra $\mathcal{A} = (V, *)$ é dita de *divisão* se para cada $\mathbf{u}, \mathbf{v} \in V$, $\mathbf{u} \neq 0$, as duas equações

$$\mathbf{u} * \mathbf{x} = \mathbf{v} \quad \text{e} \quad \mathbf{y} * \mathbf{u} = \mathbf{v}$$

têm únicas soluções em $\mathcal{A}$.

Exemplo 2.1.2. Por razões óbvias, toda extensão de corpos de $\mathbb{R}$ é uma $\mathbb{R}$-álgebra de divisão. Em particular, $\mathbb{R}$ e $\mathbb{C}$ são $\mathbb{R}$-álgebras de divisão.

Exemplo 2.1.3. Consideremos $\mathcal{A} = (\mathbb{R}^3, \wedge)$ a $\mathbb{R}$-álgebra definida no Exemplo 1.1.7. Esta não é uma $\mathbb{R}$-álgebra de divisão. Por exemplo, para $\mathbf{u} = (1, 0, 0)$ e $\mathbf{v} = (0, 0, 0)$ a equação

$$\mathbf{u} \wedge \mathbf{x} = \mathbf{v}$$

possui duas soluções distintas. De fato, $\mathbf{x} = \mathbf{u}$ e $\mathbf{x} = -\mathbf{u}$ são soluções da equação dada.

Proposição 2.1.4. *Seja $\mathcal{A} = (V, *)$ uma $\mathbb{R}$-álgebra de dimensão finita. As seguintes condições são equivalentes:*

(a) *$\mathcal{A}$ é uma $\mathbb{R}$-álgebra de divisão.*

(b) *Para cada $\mathbf{u} \in V$ não nulo as aplicações $f_{\mathbf{u}} : V \to V$ e $g_{\mathbf{u}} : V \to V$ dadas por $f_{\mathbf{u}}(\mathbf{x}) = \mathbf{u} * \mathbf{x}$ e $g_{\mathbf{u}}(\mathbf{x}) = \mathbf{x} * \mathbf{u}$, são isomorfismos.*

(c) *Para cada $\mathbf{u}, \mathbf{v} \in V$, $\mathbf{u} \neq 0$, as duas equações*

$$\mathbf{u} * \mathbf{x} = \mathbf{v} \quad e \quad \mathbf{y} * \mathbf{u} = \mathbf{v}$$

tem solução em $\mathcal{A}$.

Prova. (a) $\Rightarrow$ (b) Primeiro verificaremos que as aplicações $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são transformações lineares. De fato, dados $\mathbf{x}, \mathbf{y} \in V$ e $\alpha \in \mathbb{R}$, temos:

$$f_{\mathbf{u}}(\alpha\mathbf{x} + \mathbf{y}) = \mathbf{u} * (\alpha\mathbf{x} + \mathbf{y}) = \alpha(\mathbf{u} * \mathbf{x}) + (\mathbf{u} * \mathbf{y}) = \alpha f_{\mathbf{u}}(\mathbf{x}) + f_{\mathbf{u}}(\mathbf{y}).$$

Analogamente:

$$g_{\mathbf{u}}(\alpha\mathbf{x} + \mathbf{y}) = (\alpha\mathbf{x} + \mathbf{y}) * \mathbf{u} = \alpha(\mathbf{x} * \mathbf{u}) + (\mathbf{y} * \mathbf{u}) = \alpha g_{\mathbf{u}}(\mathbf{x}) + g_{\mathbf{u}}(\mathbf{y}).$$

Agora mostraremos que $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são injetivas. Com efeito, dados $\mathbf{v}_1, \mathbf{v}_2 \in V$, tais que $f_{\mathbf{u}}(\mathbf{v}_1) = f_{\mathbf{u}}(\mathbf{v}_2)$ segue que

$$\mathbf{u} * \mathbf{v}_1 = \mathbf{u} * \mathbf{v}_2.$$

Como $\mathcal{A}$ uma $\mathbb{R}$-álgebra de divisão, segue da unicidade das soluções que $\mathbf{v}_1 = \mathbf{v}_2$. O mesmo argumento se aplica para $g_{\mathbf{u}}$. Portanto, como $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são transformações lineares injetoras de um espaço vetorial de dimensão finita nele próprio, segue que $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são isomorfismos.

(b) $\Rightarrow$ (a) Sejam $\mathbf{u}, \mathbf{v} \in V$. Como $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são isomorfismos, em particular elas são aplicações sobrejetoras e injetoras. Assim, a existência fica garantida pela sobrejetividade e a unicidade pela injetividade.

(b) $\Rightarrow$ (c) Como $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são isomorfismos, em particular elas sao aplicações sobrejetoras. Assim, a existência fica garantida pela sobrejetividade.

(c)⇒(b) Suponha que as equações

$$\mathbf{u} * \mathbf{x} = \mathbf{v} \quad \text{e} \quad \mathbf{y} * \mathbf{u} = \mathbf{v}$$

têm solução em $\mathcal{A}$. Como verificado antes, $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$, são transformações lineares. Note que $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são sobrejetoras pois, para cada $\mathbf{v} \in V$, as equações

$$\mathbf{u} * \mathbf{x} = \mathbf{v} \quad e \quad \mathbf{y} * \mathbf{u} = \mathbf{v}$$

têm soluções. Como $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são transformações lineares sobrejetoras de um espaço vetorial de dimensão finita nele próprio segue que $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são isomorfismos. □

2.2 Álgebras de divisão e campos de vetores sobre a esfera

Nesse capítulo faremos uso de algumas noções e resultados relativos às variedades diferenciáveis. Para não distanciarmos do nosso foco, não nos ocuparemos em definir os objetos nem em demonstrar os resultados concernentes às variedades diferenciáveis. Citamos [2] como referência para essa parte.

Seja M uma variedade diferenciável de dimensão n. A cada ponto $\mathbf{x} \in M$ está associado um espaço vetorial n-dimensional $T_{\mathbf{x}}M$, chamado *espaço tangente* a M no ponto $\mathbf{x}$. Uma função ω que associa cada ponto $\mathbf{x} \in M$ a um vetor $\omega(\mathbf{x}) \in T_{\mathbf{x}}M$ é chamada *campo de vetores* sobre M. Dado um campo de vetores ω sobre M, dizemos que um ponto $\mathbf{x} \in M$ é um *ponto de singularidade* do campo ω se $\omega(\mathbf{x}) = 0$. O seguinte resultado caracteriza quando uma variedade diferenciável M admite um campo de vetores contínuo sem singularidades:

Teorema 2.2.1 (Hopf, 1926)**.** *Uma variedade diferenciável M admite um campo de vetores contínuo sem singularidades se, e somente se, a característica de Euler-Poincaré de M é zero.*

Um exemplo importante de variedade diferenciável é a *esfera n-dimensional*:

$$\mathbb{S}^n = \{\mathbf{x} \in \mathbb{R}^{n+1} \mid \| \mathbf{x} \| = 1\}. \tag{2.1}$$

É provado que a característica de Euler-Poincaré de $\mathbb{S}^n$ é 2 se n é par e 0 se n é

ímpar. Assim, a esfera $\mathbb{S}^n$ admite um campo de vetores contínuo sem singularidades se, e somente se, n é ímpar.

Seja k um inteiro não negativo. Um *k-campo contínuo* sobre M é uma k-upla $\omega_1, \ldots, \omega_k$ de campos contínuos sobre M tal que para cada $\mathbf{x} \in M$, os vetores $\omega_1(\mathbf{x}), \ldots, \omega_k(\mathbf{x}) \in T_{\mathbf{x}}M$ são linearmente independentes. O maior inteiro para o qual existe um k-campo contínuo sobre M é denotado por $\mathrm{Span}(M)$. Claramente, $0 \leq \mathrm{Span}(M) \leq \dim M = n$. Dizemos que M é uma variedade *paralelizável* se $\mathrm{Span}(M) = n$.

Nosso objetivo é discutir a relação entre as noções de esfera paralelizável e álgebra de divisão. Para isso, convém fixarmos alguns resultados que serão úteis para essa discussão.

Teorema 2.2.2. *Sejam X e Y espaços topológicos tais que X é compacto e Y é de Hausdorff. Se $f : X \to Y$ é uma bijeção contínua então f é um homeomorfismo.*

Prova. Ver [4, Chapter 3]. □

Observação 2.2.3. A esfera $\mathbb{S}^n$ é um exemplo de espaço topológico que é compacto e de Hausdorff. Assim, uma bijeção contínua $f : \mathbb{S}^n \to \mathbb{S}^n$ é um homeomorfismo.

Observação 2.2.4. No caso particular da esfera $\mathbb{S}^n$ temos a seguinte descrição para o espaço tangente a $\mathbb{S}^n$ no ponto $\mathbf{x} \in \mathbb{S}^n$:

$$T_{\mathbf{x}}\mathbb{S}^n = \{\mathbf{y} \in \mathbb{R}^{n+1} \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0\}.$$

Teorema 2.2.5. *Seja n um inteiro positivo. Suponha que $\mathbb{R}^{n+1}$ admite uma multiplicação $*$ tal que $(\mathbb{R}^{n+1}, *)$ é uma $\mathbb{R}$-álgebra de divisão. Então a esfera $\mathbb{S}^n$ é paralelizável.*

Prova. Seja $\{\mathbf{e}_1, \ldots, \mathbf{e}_{n+1}\}$ a base canônica de $\mathbb{R}^{n+1}$. Suponha $\mathbf{x} \in \mathbb{S}^n$. Como $(\mathbb{R}^{n+1}, *)$ é uma álgebra de divisão e $\mathbf{x} \neq 0$, segue que a aplicação $f_{\mathbf{x}} : \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$ (ver Proposição 2.1.4) é um isomorfismo. Em particular, $f_{\mathbf{x}}$ transforma base em base. Assim, $\{\mathbf{x} * \mathbf{e}_1, \ldots, \mathbf{x} * \mathbf{e}_{n+1}\}$ é uma base de $\mathbb{R}^{n+1}$. Observem que, para cada $1 \leq i \leq n+1$, as coordenadas de $\mathbf{x} * \mathbf{e}_i$ são expressões lineares das coordenadas de $\mathbf{x}$. Assim, a função $\mathbf{x} \mapsto \mathbf{x} * \mathbf{e}_i$ é contínua. Assim, ao ortonormalizarmos $\{\mathbf{x} * \mathbf{e}_1, \ldots, \mathbf{x} * \mathbf{e}_{n+1}\}$, por Gram-Schmidt, obtemos uma base $\{\nu_1(\mathbf{x}), \ldots, \nu_{n+1}(\mathbf{x})\}$ de $\mathbb{R}^{n+1}$ tal que cada ν_i depende continuamente de $\mathbf{x}$ (pois cada vetor em $\{\nu_1(\mathbf{x}), \ldots, \nu_{n+1}(x)\}$ é resultado de operações como soma, divisão produto interno dos elementos de $\{\mathbf{x}*\mathbf{e}_1, \ldots, \mathbf{x}*\mathbf{e}_{n+1}\}$). Notemos que no processo de ortonormalização de Gram-Schmidt, $\nu_1(\mathbf{x}) = \frac{\mathbf{x}*\mathbf{e}_1}{\|\mathbf{x}*\mathbf{e}_1\|}$.

Afirmação: *A função $\nu_1 : \mathbb{S}^n \to \mathbb{S}^n$ é uma bijeção.*

Suponhamos $\mathbf{x}_1, \mathbf{x}_2$ tais que $\nu(\mathbf{x}_1) = \nu_1(\mathbf{x}_2)$. Então

$$\frac{\mathbf{x}_1 * \mathbf{e}_1}{\| \mathbf{x}_1 * \mathbf{e}_1 \|} = \frac{\mathbf{x}_2 * \mathbf{e}_1}{\| \mathbf{x}_2 * \mathbf{e}_1 \|}.$$

Como $(\mathbb{R}^{n+1}, *)$ é álgebra de divisão segue que

$$\frac{\mathbf{x}_1}{\| \mathbf{x}_1 * \mathbf{e}_1 \|} = \frac{\mathbf{x}_2}{\| \mathbf{x}_2 * \mathbf{e}_1 \|} \tag{2.2}$$

Passando o módulo nos dois lados dessa igualdade vem

$$\frac{\| \mathbf{x}_1 \|}{\| \mathbf{x}_1 * \mathbf{e}_1 \|} = \frac{\| \mathbf{x}_2 \|}{\| \mathbf{x}_2 * \mathbf{e}_1 \|}.$$

Mas, como $\| \mathbf{x}_1 \| = \| \mathbf{x}_2 \| = 1$, segue que

$$\| \mathbf{x}_1 * \mathbf{e}_1 \| = \| \mathbf{x}_2 * \mathbf{e}_1 \| .$$

Assim, de (2.2) obtemos $\mathbf{x}_1 = \mathbf{x}_2$. Logo ν_1 é injetora.

Agora consideremos $\mathbf{y} \in \mathbb{S}^n$. Pelo fato de $(\mathbb{R}^{n+1}, *)$ ser álgebra de divisão, existe $\mathbf{v} \in \mathbb{R}^{n+1}$ tal que $\mathbf{v} * \mathbf{e}_1 = \mathbf{y}$. Para $\mathbf{x} = \frac{\mathbf{v}}{\|\mathbf{v}\|} \in \mathbb{S}^n$ temos

$$\frac{\mathbf{x} * \mathbf{e}_1}{\| \mathbf{x} * \mathbf{e}_1 \|} = \mathbf{y},$$

ou seja, $\nu_1(\mathbf{x}) = \mathbf{y}$. Logo, ν_1 é sobrejetora.

Portanto, como ν_1 é injetora e sobrejetora a afirmação segue.

Esta afirmação combinada com o fato de que ν_1 é contínua nos dão, pela Observação 2.2.3, que ν_1^{-1} é contínua. Consideremos agora as funções

$$\omega_2 := \nu_2 \circ \nu_1^{-1}, \ldots, \omega_{n+1} := \nu_{n+1} \circ \nu_1^{-1}.$$

Como cada ω_i é composição de funções contínuas, então ω_i é contínua. Pelo que vimos anteriormente, para cada $\mathbf{y} \in \mathbb{S}^n$, $\{\mathbf{y}, \omega_2(\mathbf{y}), \ldots, \omega_{n+1}\}$ é base ortonormal de $\mathbb{R}^{n+1}$. Assim, $\langle \omega_i(\mathbf{y}), \mathbf{y} \rangle = 0$ para cada $2 \leq i \leq n+1$, ou seja, $\omega_2(\mathbf{y}), \ldots, \omega_{n+1}(\mathbf{y}) \in T_{\mathbf{y}}\mathbb{S}^n$. Logo, $\omega_2, \ldots, \omega_{n+1}$ é um n-campo contínuo sobre a esfera $\mathbb{S}^n$. Portanto, $\mathbb{S}^n$ é paralelizável. □

Usando métodos de topologia algébrica, Bott e Milnor e, independentemente,

Kervaire obtiveram o seguinte resultado que nos mostra o quão restritiva é a hipótese de uma álgebra de dimensão finita ser de divisão.

Teorema 2.2.6 (**Bott-Milnor, Kervaire 1958).** *Se* $\mathbb{S}^n$ *é paralelizável então* $n =$ 1, 3 *ou* 7. *Em particular, se* $\mathcal{A}$ *é uma álgebra de divisão de dimensão* n *então* $n =$ 1, 2, 4 *ou* 8.

Como visto acima, para $n = 1$ ou 2 existem álgebras de divisão com essas dimensões, de fato, $\mathbb{R}$ e $\mathbb{C}$. A pergunta que subsiste é se existem álgebras de divisão de dimensão 4 e 8. Nos capítulos 3 e 4 desse trabalho mostraremos que a resposta é afirmativa.

2.3 $\mathbb{R}$-álgebras de composição

Definição 2.3.1. Sejam $\mathcal{A} = (V, *)$ uma $\mathbb{R}$-álgebra e $\langle\ ,\ \rangle$ um produto interno sobre V com norma associada $\|\ \|$. Se

$$\| \mathbf{u} * \mathbf{v} \| = \| \mathbf{u} \| \cdot \| \mathbf{v} \| \tag{2.3}$$

para cada $\mathbf{u}, \mathbf{v} \in V$, a álgebra $\mathcal{A}$ é dita $\mathbb{R}$-*álgebra de composição* com respeito ao produto interno $\langle\ ,\ \rangle$ (ou ao módulo $\|\ \|$).

Exemplo 2.3.2. Por razões bem conhecidas sabemos, que $\mathbb{R}$ é uma $\mathbb{R}$-álgebra de composicão.

Exemplo 2.3.3. Como sabemos, a $\mathbb{R}$-álgebra dos complexos é comutativa, associativa, tem identidade e satisfaz as seguintes propriedades:

(A) $\| z \|^2 = z\overline{z}$, para cada $z \in \mathbb{C}$.

(B) $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$, para quaisquer $z_1,\ z_2 \in \mathbb{C}$ (onde $\overline{z}$ significa o conjugado complexo de z).

De posse dessas propriedades temos:

$$\| z_1 z_2 \|^2 = (z_1 z_2)(\overline{z_1 z_2}) = (z_1 \overline{z_1})(z_2 \overline{z_2}) = \| z_1 \|^2 \| z_2 \|^2 .$$

Logo,

$$\| z_1 z_2 \| = \| z_1 \| \cdot \| z_2 \| .$$

Assim, $\mathbb{C}$ é uma $\mathbb{R}$- álgebra de composição.

Proposição 2.3.4. *Se $\mathcal{A} = (V, *, \langle\ ,\ \rangle)$ é uma $\mathbb{R}$-álgebra de composição de dimensão finita então $\mathcal{A}$ é uma $\mathbb{R}$-álgebra de divisão.*

Prova. Seja $\mathbf{u}$ um elemento não nulo de V. Consideremos $f_{\mathbf{u}}, g_{\mathbf{u}} : V \to V$ as aplicações definidas na Proposição 2.1.4. Por essa mesma proposição, para provar o desejado é suficiente mostrar que $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são funções injetoras. Assim, consideremos $\mathbf{v}_1 \in \ker f_{\mathbf{u}}$ e $\mathbf{v}_2 \in \ker g_{\mathbf{u}}$. Então:

$$\| \mathbf{u} * \mathbf{v}_1 \| = 0 \quad \text{e} \quad \| \mathbf{v}_1 * \mathbf{u} \| = 0.$$

Dessas igualdades e da hipótese que $\mathcal{A}$ é uma álgebra de composição segue

$$\| \mathbf{u} \| \cdot \| \mathbf{v}_1 \| = 0 \quad \text{e} \quad \| \mathbf{v}_2 \| \cdot \| \mathbf{u} \| = 0.$$

Como $\| \mathbf{u} \| \neq 0$, pois $\mathbf{u} \neq 0$, segue que $\| \mathbf{v}_1 \| = \| \mathbf{v}_2 \| = 0$ ou, equivalentemente, $\mathbf{v}_1 = \mathbf{v}_2 = \mathbf{0}$. Assim, $\ker f_{\mathbf{u}} = \ker g_{\mathbf{u}} = \{\mathbf{0}\}$, ou seja, $f_{\mathbf{u}}$ e $g_{\mathbf{u}}$ são injetoras como queríamos provar. □

Problema 2.3.5. *Para quais valores de $n \geq 1$ existem $\mathbb{R}$-álgebras de composição $\mathcal{A} = (V, *, \langle\ ,\ \rangle)$ de dimensão n?*

O teorema abaixo apresenta uma forma equivalente de estudar o problema acima

Teorema 2.3.6. *Seja n um inteiro positivo. As seguintes condições são equivalentes:*

(a) *Existe uma $\mathbb{R}$-álgebra de composição de dimensão n.*

(b) *Existem $\gamma_{p,q}^{i} \in \mathbb{R}$, com $1 \leq i, p, q \leq n$, tais que para $u_1, \ldots, u_n$ e $v_1, \ldots, v_n$ números reais arbitrários e*

$$z_i = \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma_{p,q}^{i} \in \mathbb{R}$$

temos

$$(u_1^2 + \ldots + u_n^2)(v_1^2 + \ldots + v_n^2) = (z_1^2 + \ldots + z_n^2) \tag{2.4}$$

Prova. (a) $\Rightarrow$ (b) Suponha que exista uma $\mathbb{R}$-álgebra $\mathcal{A}$ de composição de dimensão n. Seja $B = \{\mathbf{e}_1, ..., \mathbf{e}_n\}$ uma base ortonormal de V. Dados números reais $u_1, .., u_n$ e $v_1, ..., v_n$, consideremos os seguintes vetores de V:

$$\mathbf{u} = \sum_{i=1}^{n} u_i \mathbf{e}_i \quad \text{e} \quad \mathbf{v} = \sum_{i=1}^{n} v_i \mathbf{e}_i.$$

Pela igualdade (1.3), temos:

$$\mathbf{u} * \mathbf{v} = \sum_{i=1}^{n} z_i \mathbf{e}_i,$$

onde $z_i = \sum_{p=1}^{n}\sum_{q=1}^{n} u_p v_q \gamma_{p,q}^{i} \in \mathbb{R}$. Disso segue que

$$\| \mathbf{u} * \mathbf{v} \|^2 = z_1^2 + \cdots + z_n^2 \tag{2.5}$$

Por outro lado

$$\| \mathbf{u} \|^2 \cdot \| \mathbf{v} \|^2 \;\; = \;\; (u_1^2 + \cdots + u_n^2)(v_1^2 + \cdots + v_n^2) \tag{2.6}$$

Como $\| \mathbf{u} * \mathbf{v} \| = \| \mathbf{u} \| \cdot \| \mathbf{v} \|$, segue de (2.5) e (2.6) que

$$(u_1^2 + \cdots + u_n^2)(v_1^2 + \cdots + v_n^2) = (z_1^2 + \cdots + z_n^2)$$

como queríamos provar.

(b) $\Rightarrow$(a) Defina $V = \mathbb{R}^n$ e $* : V \times V \to V$ da seguinte maneira: dados $\mathbf{u} = (u_1, ..., u_n)$ e $\mathbf{v} = (v_1, ..., v_n)$ faremos

$$\mathbf{u} * \mathbf{v} = \sum_{i=1}^{n} z_i \mathbf{e}_i,$$

onde $\{\mathbf{e}_1, ..., \mathbf{e}_n\}$ é uma base canônica de $\mathbb{R}^n$ e $z_i = \sum_{p=1}^{n}\sum_{q=1}^{n} u_p v_q \gamma_{p,q}^{i} \in \mathbb{R}$. Mostraremos que $\mathcal{A} = (V, *)$ definida dessa maneira é uma $\mathbb{R}$-álgebra de composição. Notemos que:

$$\| \mathbf{u} * \mathbf{v} \| = z_1^2 + \cdots + z_n^2 \tag{2.7}$$

Por outro lado:

$$\| \mathbf{u} \| \cdot \| \mathbf{v} \| = (u_1^2 + \cdots + u_n^2)(v_1^2 + \cdots + v_n^2) \tag{2.8}$$

Como por hipótese

$$(u_1^2 + \cdots + u_n^2)(v_1^2 + \cdots + v_n^2) = z_1^2 + \cdots + z_n^2,$$

segue de (2.7) e (2.8) que

$$\| \mathbf{u} * \mathbf{v} \| = \| \mathbf{u} \| \cdot \| \mathbf{v} \|$$

como queríamos provar. □

A relação (2.4) é chamada *identidade sobre soma de quadrados.*

O resto dessa seção será dedicado a responder o Problema 2.3.5. Para esse propósito convém considerarmos o seguinte lema:

Lema 2.3.7. *Seja* $\{B_1, \ldots, B_{n-1}\}$ *um conjunto de matrizes anti-simétricas de ordem* $n \times n$ *tal que*

$$B_i^2 = -I \quad 1 \leq i \leq n-1$$

e

$$B_i B_j = -B_j B_i$$

para cada $i \neq j$. *Suponhamos*

$$\mathcal{B} = \{B_{i_1} B_{i_2} \cdots B_{i_r} \,|\, 1 \leq i_1, \ldots, i_r \leq n-1 \text{ e } r \geq 1\}.$$

Então:

(a) n *é um número par.*

(b) *Se* $\mathcal{B}$ *é linearmente dependente então* 4 *divide* n.

(c) $\mathcal{B}$ *contém pelo menos* 2^{n-2} *elementos que são linearmente independentes.*

Prova. (a) Como $B_i = -B_i^t$ então $\det(B_i) = (-1)^n \det(B_i)$. Mas B_i é invertível, logo $\det(B_i) \neq 0$. Assim, $1 = (-1)^n$. Dessa igualdade segue que n é par.

(b) Pelas propriedades das B_i's os elementos do conjunto $\mathcal{B}$ são da forma

$$\pm B_1^{e_1} \cdots B_{n-1}^{e_{n-1}}, \;\; e_i = 0 \text{ ou } 1$$

que correspondem a 2^{n-1} produtos. Vejamos quais dessas matrizes são simétricas e quais são anti-simétricas. Para isso, consideremos

$$M = B_{i_1} B_{i_2} \cdots B_{i_r}, \quad r \leq n-1, \; i_1 < i_2 < \ldots < i_r. \tag{2.9}$$

Então:

$$\begin{aligned} M^t &= (B_{i_1}B_{i_2}\cdots B_{i_r})^t = B_{i_r}^t B_{i_{r-1}}^t \cdots B_{i_1}^t \\ &= (-1)^r B_{i_r}B_{i_{r-1}}\cdots B_{i_1} \\ &= (-1)^{r+(r-1)} B_{i_1}B_{i_r}\cdots B_{i_2} \\ &\vdots \\ &= (-1)^{r+(r-1)+(r-2)+\cdots+2+1} B_{i_1}B_{i_2}\cdots B_{i_r} \\ &= (-1)^{r(r+1)/2} M \end{aligned}$$

Desse modo, M é simétrica se, e somente se, r ou $(r+1)$ é divisível por 4.

Suponhamos $k > 0$ sendo a menor cardinalidade de um conjunto linearmente dependente de $\mathcal{B}$. Assim, digamos que $\{M_1, \ldots, M_k\}$ é um subconjunto linearmente dependente de $\mathcal{B}$. Então existe uma combinação linear

$$\alpha_1 M_1 + \cdots + \alpha_k M_k = 0 \tag{2.10}$$

onde $\alpha_i \neq 0$ para qualquer $1 \leq i \leq k$ e qualquer subconjunto próprio de $\{M_1, \ldots, M_k\}$ é linearmente independente (de fato, se existisse uma combinação não trivial dos M_i's com um coeficiente nulo encontraríamos um conjunto linearmente dependente com cardinalidade menor que k, o que seria um absurdo). Assim, como o espaço das matrizes simétricas tem interseção nula com o espaço das matrizes anti-simétricas, segue que todas as matrizes do conjunto $\{M_1, \ldots, M_k\}$ são simétricas ou todas são anti-simétricas.

Observamos que a relação (2.10) pode ser suposta da forma

$$I = \alpha_1 M_1 + \cdots + \alpha_{k-1} M_{k-1} \tag{2.11}$$

com cada M_i sendo uma matriz simétrica (basta multiplicar (2.10) por $\alpha^{-1}M_1^{-1}$).

Digamos que, na escrita de (2.9), M_1 envolva o menor número de fatores r. Suponhamos por um momento que $r < n-1$. Se $r+1$ é divisível por 4 e

$$M_1 = B_{i_1}B_{i_2}\cdots B_{i_r}$$

então podemos escolher $j \neq i_1, \ldots, i_r$ tal que ao multiplicarmos (2.11) por B_j obtemos:

$$B_j = \alpha_1 M_1 B_j + \cdots + \alpha_{k-1} M_{k-1} B_j \tag{2.12}$$

onde B_j é anti-simétrica e $M_1 B_j$ é simétrica. Mas isso é uma contradição. Por outro lado, se r é divisível por 4 então ao multiplicarmos (2.11) por B_{i_1} obtemos:

$$B_{i_1} = \alpha_1 M_1 B_{i_1} + \cdots + \alpha_{k-1} M_{k-1} B_{i_1} \tag{2.13}$$

onde B_{i_1} é anti-simétrica e $M_1 B_{i_1}$ é simétrica. Assim, devemos ter $r = n - 1$. Logo, a relação (2.11) deve ser da forma

$$I = \alpha B_1 B_2 \cdots B_{n-1}$$

Assim, $n - 1$ é divisível por 4 ou n é divisível por 4. Como n é par, segue que n é divisível por 4.

(c) Se n é par mas não divisível por 4 então, pela contra-positiva do item anterior, todas as matrizes de $\mathcal{B}$ são linearmente independentes. Logo, o resultado segue nesse caso.

Agora suponhamos que n é divisível por 4. Afirmamos que a coleção dos elementos de $\mathcal{B}$ que envolvem no máximo $\frac{1}{2}(n-2)$ fatores é linearmente independente. Com efeito, se ocorresse o contrário poderíamos construir uma combinação linear dos elementos dessa coleção como em (2.10). Assim, seria possível obter uma relação como em (2.11), onde cada M_i tem no máximo $n - 2$ fatores. Mas isso é um absurdo pois, como provado no item anterior, uma relação como em (2.11) deve ser da forma (2.13). Mas a cardinalidade dessa coleção é:

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \cdots + \binom{n-1}{\frac{1}{2}(n-2)} = 2^{n-2}.$$

Assim, temos o desejado. □

Corolário 2.3.8. *Seja n um número inteiro maior ou igual a 2. Se existem $n - 1$ matrizes $B_1, \ldots, B_n \in M_n(\mathbb{R})$ satisfazendo as hipóteses do lema anterior então $n =$ 2, 4 ou 8.*

Prova. Como observado no inicio da prova do Lema anterior, n deve ser um número par. Também segue do Lema acima que podemos construir um subconjunto de 2^{n-2} matrizes que são linearmente independentes. Assim,

$$2^{n-2} \leq \dim M_n(\mathbb{R}) = n^2.$$

Mas essa desigualdade é falsa para $n \geq 9$. Esse fato combinado com a observação de que n é par implica em $n = 2,\ 4,\ 6$ ou 8. Analisamos agora o caso em que $n = 6$. Como 4 não divide 6 segue da prova do Lema acima que as 2^5 matrizes de $\mathcal{B}$ são linearmente independentes. Dentre estas temos as matrizes:

$$B_1, \ldots, B_5$$

$$B_1B_2,\ B_1B_3,\ B_1B_4,\ B_1B_5,\ B_2B_3,\ B_2B_4,\ B_2B_5, B_3B_4, B_3B_5, B_4B_5$$

$$B_1B_2B_3B_4B_5$$

que correspondem a 16 matrizes anti-simétricas. Mas, a dimensão do espaco das matrizes anti-simétricas de ordem 6×6 é

$$1 + 2 + \cdots + 5 = 15.$$

Logo, n não pode ser 6. Portanto, temos a conclusão desejada. □

Teorema 2.3.9 (Hurwitz, 1898)**.** *Seja n um inteiro positivo. Se existe álgebra de composição de dimensão n então $n = 1, 2, 4,$ ou 8.*

Prova. Suponhamos $n \geq 2$. Devemos mostrar que $n = 2,\ 4,$ ou 8. Para isso, devido o corolário anterior, basta exibirmos matrizes $B_1, \ldots, B_{n-1}$ que satisfaçam as hipóteses do Lema 2.3.7.

Pelo Teorema 2.3.6 existem $\gamma^i_{p,q} \in \mathbb{R}$, com $1 \leq i, p, q \leq n$, tais que para $u_1, \ldots, u_n$ e $v_1, \ldots, v_n$ números reais arbitrários e

$$z_i = \sum_{p=1}^{n} \sum_{q=1}^{n} u_p v_q \gamma^i_{p,q} \in \mathbb{R}$$

temos

$$(u_1^2 + \ldots + u_n^2)(v_1^2 + \ldots + v_n^2) = (z_1^2 + \ldots + z_n^2). \tag{2.14}$$

Para cada $1 \leq i, j \leq n$, definimos

$$\alpha_{ij} = \sum_{p=1}^{n} \gamma^i_{pj} u_p.$$

Com isso, temos:

$$(u_1^2+\cdots+u_n^2)(v_1^2+\cdots+v_n^2)=\left(\sum_{j=1}^{n}\alpha_{1j}v_j\right)^2+\cdots+\left(\sum_{j=1}^{n}\alpha_{nj}v_j\right)^2 \tag{2.15}$$

Para cada $1\leq j\leq n$, fazendo $v_j=1$ e os demais v_i's iguais a zero obtemos o seguinte sistema:

$$\begin{cases} u_1^2+\cdots+u_n^2 & = & \alpha_{11}^2+\cdots+\alpha_{n1}^2 \\ \cdots\cdots\cdots\cdots & \cdots & \cdots\cdots\cdots\cdots \\ u_1^2+\cdots+u_n^2 & = & \alpha_{1n}^2+\cdots+\alpha_{nn}^2 \end{cases} \tag{2.16}$$

Ao expandirmos o lado esquerdo de (2.15) obtemos:

$$(u_1^2+\cdots+u_n^2)(v_1^2+\cdots+v_n^2)=\left(\sum_{i=1}^{n}\alpha_{i1}^2\right)v_1^2+\cdots+\left(\sum_{i=1}^{n}\alpha_{in}^2\right)v_n^2+$$

$$+2\sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha_{1i}\alpha_{1j}+\cdots+\alpha_{ni}\alpha_{nj})v_iv_j \tag{2.17}$$

Assim, substituindo as igualdades de (2.16) em (2.17) obtemos

$$(u_1^2+\cdots+u_n^2)(v_1^2+\cdots+v_n^2)=(u_1^2+\cdots+u_n^2)(v_1^2+\cdots+v_n^2)+$$

$$+2\sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha_{1i}\alpha_{1j}+\cdots+\alpha_{ni}\alpha_{nj})v_iv_j. \tag{2.18}$$

Logo,

$$2\sum_{i=1}^{n}\sum_{j=1}^{n}(\alpha_{1i}\alpha_{1j}+\cdots+\alpha_{ni}\alpha_{nj})v_iv_j=0 \tag{2.19}$$

Agora, fazendo $v_i=v_j=1$ e os demais iguais a zero obtemos:

$$2(\alpha_{1i}\alpha_{1j}+\cdots+\alpha_{ni}\alpha_{nj})=0 \tag{2.20}$$

para cada $1\leq i,j\leq n$.

Reunindo as equações de (2.16) e (2.20) obtemos

$$A^t \cdot A = \left(\sum_{i=1}^{n} u_i^2 \right) I \tag{2.21}$$

onde A é a matriz $n \times n$ com entradas α_{ij} e I é a matriz identidade de ordem n.

Podemos escrever a matriz A da seguinte maneira:

$$A = u_1 A_1 + \cdots + u_n A_n \tag{2.22}$$

onde

$$A_i = \begin{pmatrix} \gamma_{p1}^1 & \cdots & \gamma_{pn}^1 \\ \vdots & \ddots & \vdots \\ \gamma_{p1}^n & \cdots & \gamma_{pn}^n \end{pmatrix}$$

para cada $1 \leq p \leq n$.

Substituindo essa expressão de A em (2.21) obtemos:

$$(u_1 A_1^t + \cdots + u_n A_n^t)(u_1 A_1 + \cdots + u_n A_n) = \left(\sum_{i=1}^{n} u_i^2 \right) I \tag{2.23}$$

Fazendo $u_i = 1$ e os demais iguais a zero temos

$$A_i^t \cdot A_i = I \tag{2.24}$$

para cada $1 \leq i \leq n$.

Definimos $B_i = A_n^t A_i$ para cada $1 \leq i \leq n-1$. Então:

$$(u_1 A_1^t + \cdots + u_n A_n^t)(A_n^t A_n)(u_1 A_1 + \cdots + u_n A_n) = \left(\sum_{i=1}^{n} u_i^2 \right) I \tag{2.25}$$

e daí vem

$$(u_1 B_1^t + \cdots + u_{n-1} B_{n-1}^t + u_n I)(u_1 B_1 + \cdots + u_{n-1} B_{n-1} + u_n I) = \left(\sum_{i=1}^{n} u_i^2 \right) I \tag{2.26}$$

Fazendo $u_i = 1$ e os demais iguais a zero obtemos

$$B_i^t B_i = I \tag{2.27}$$

para cada $1 \leq i \leq n-1$.

Por outro lado, fazendo em (2.26) $u_i = u_j = 1$, para $i \neq j$, e os demais iguais a zero temos:

$$B_i^t B_j + B_j^t B_i = 0 \tag{2.28}$$

para cada $1 \leq i, j \leq n-1$.

Finalmente, fazendo $u_i = u_n = 1$ em (2.26) obtemos

$$B_i^t + B_i = 0 \tag{2.29}$$

para cada $1 \leq i \leq n-1$.

Portanto, de (2.27), (2.28) e (2.29) segue o resultado desejado. □

Capítulo 3

Álgebra dos Quatérnios

Nesse capítulo estudaremos uma das principais $\mathbb{R}$-álgebras de dimensão finita, a saber, a *álgebra dos quatérnios*. A descoberta desse importante objeto matemático é atribuída ao matemático irlandês Sir Willian Rowan Hamilton (1843), quando este investigava sistemas matemáticos que pudessem generalizar as propriedades geométricas/algébricas dos números complexos. Mostraremos aqui que esta é uma $\mathbb{R}$-álgebra associativa, não comutativa, com identidade, de divisão e de composição e que, a menos de isomorfismos, ela é a única $\mathbb{R}$-álgebra com estas propriedades. Também discutiremos como esta $\mathbb{R}$-álgebra pode ser representada matricialmente.

3.1 Definição e propriedades básicas

Fixaremos as seguintes notações para os vetores da base canônica de $\mathbb{R}^4$:

$$\mathbf{1} := (1,0,0,0), \quad \mathbf{i} := (0,1,0,0), \quad \mathbf{j} := (0,0,1,0) \quad \text{e} \quad \mathbf{k} := (0,0,0,1)$$

Assim, cada vetor $\mathbf{u} = (u_1, u_2, u_3, u_4) \in \mathbb{R}^4$ pode ser escrito de forma única da seguinte maneira:

$$\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}$$

Definimos uma multiplicação $\cdot : \mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}^4$ da seguinte maneira: dados $\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}$ e $\mathbf{v} = v_1\mathbf{1} + v_2\mathbf{i} + v_3\mathbf{j} + v_4\mathbf{k}$ temos:

$$\begin{aligned}\mathbf{u}\cdot\mathbf{v} := {} & (u_1v_1 - u_2v_2 - u_3v_3 - u_4v_4)\mathbf{1} + (u_1v_2 + u_2v_1 + u_3v_4 - u_4v_3)\mathbf{i} \\ & +(u_1v_3 + u_3v_1 + u_4v_2 - u_2v_4)\mathbf{j} + (u_1v_4 + u_2v_3 + u_4v_1 - u_3v_2)\mathbf{k} \qquad (3.1)\end{aligned}$$

Definição 3.1.1. A $\mathbb{R}$-álgebra formado pelo o espaço vetorial $\mathbb{R}^4$ e a operação de multiplicação acima é chamada de *álgebra dos quatérnios* ou *álgebra de Hamilton*.

Utilizaremos a notação $\mathbb{H}$ para representar a álgebra dos quatérnios. Cada elemento de $\mathbb{H}$ será chamado de *quatérnio*.

Podemos observar diretamente de (3.1) as seguintes igualdades:

$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j} \quad \text{e} \quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}. \tag{3.2}$$

Também segue de (3.1) que

$$\mathbf{1} \cdot \mathbf{u} = \mathbf{u} \cdot \mathbf{1} = \mathbf{u} \tag{3.3}$$

para cada $\mathbf{u} \in \mathbb{R}^4$. Assim, de (3.2) segue que $\mathbb{H}$ não é uma $\mathbb{R}$-álgebra comutativa e de (3.3) segue que $\mathbb{H}$ é uma $\mathbb{R}$-álgebra com identidade.

Definição 3.1.2. Seja $\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}$ um quatérnio. O *conjugado* de $\mathbf{u}$, denotado por $\overline{\mathbf{u}}$, é o quatérnio $\overline{\mathbf{u}} := u_1\mathbf{1} - u_2\mathbf{i} - u_3\mathbf{j} - u_4\mathbf{k}$.

Com a definição do conjugado podemos verificar as seguintes propriedades:

Proposição 3.1.3. *Sejam* $\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}$ *e* $\mathbf{v} = v_1 + u_2\mathbf{i} + u_3\mathbf{j} + v_4\mathbf{k} \in \mathbb{H}$ *e* $\alpha \in \mathbb{R}$. *Então:*

(a) $\mathbf{u} \cdot \overline{\mathbf{u}} = \overline{\mathbf{u}} \cdot \mathbf{u} = (u_1^2 + u_2^2 + u_3^2 + u_4^2)\mathbf{1}$

(b) $\overline{\overline{\mathbf{u}}} = \mathbf{u}$.

(c) $\overline{\mathbf{u} \cdot \mathbf{v}} = \overline{\mathbf{v}} \cdot \overline{\mathbf{u}}$

(d) $\overline{\alpha\mathbf{u} + \mathbf{v}} = \alpha\overline{\mathbf{u}} + \overline{\mathbf{v}}$.

Prova. (a) Utilizando (3.1) temos:

$$\mathbf{u}\cdot\overline{\mathbf{u}} = (u_1^2+u_2^2+u_3^2+u_4^2)\mathbf{1}+(-u_1u_2+u_2u_1-u_3u_4+u_4v_3)\mathbf{i}+(-u_1u_3+u_3u_1-u_4u_2+u_2u_4)\mathbf{j}$$

$$+(-u_1u_4 - u_2u_3 + u_4u_1 + u_3u_2)\mathbf{k} = (u_1^2 + u_2^2 + u_3^2 + u_4^2)\mathbf{1}$$

(b) Temos:

$$\begin{aligned} \overline{\overline{\mathbf{u}}} &= \overline{u_1\mathbf{1} - u_2\mathbf{i} - u_3\mathbf{j} - u_4\mathbf{k}} \\ &= u_1\mathbf{1} - (-u_2)\mathbf{i} - (-u_3)\mathbf{j} - (-u_4)\mathbf{k} \\ &= u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k} = \mathbf{u} \end{aligned}$$

(c) Por um lado temos:

$$\overline{\mathbf{u}\cdot\mathbf{v}} = (u_1v_1 - u_2v_2 - u_3v_3 - u_4v_4)\mathbf{1} - (u_1v_2 + u_2v_1 + u_3v_4 - u_4v_3)\mathbf{i} -$$

$$-(u_1v_3 + u_3v_1 + u_4v_2 - u_2v_4)\mathbf{j} - (u_1v_4 + u_2v_3 + u_4v_1 - u_3v_2)\mathbf{k} \tag{3.4}$$

Por outro lado,

$$\begin{aligned}
\overline{\mathbf{v}}\cdot\overline{\mathbf{u}} &= (v_1u_1 - (-v_2)(-u_2) - (-v_3)(-u_3) - (-v_4)(-u_4))\mathbf{1} + \\
&(v_1(-u_2) + (-v_2)u_1 + (-v_3)(-u_4) - (-v_4)(-u_3))\mathbf{i} \\
&+(v_1(-u_3) + (-v_3)u_1 + (-v_4)(-u_2) - (-v_2)(-u_4))\mathbf{j} + \\
&(v_1(-u_4) + (-v_2)(-u_3) + (-v_4)u_1 - (-v_3)(-u_2))\mathbf{k} \\
&= (v_1u_1 - v_2u_2 - v_3u_3 - v_4u_4)\mathbf{1} - (u_1v_2 + u_2v_1 + u_3v_4 - u_4v_3)\mathbf{i} - \\
&-(u_1v_3 + u_3v_1 + u_4v_2 - u_2v_4)\mathbf{j} - (u_1v_4 + u_2v_3 + u_4v_1 - u_3v_2)\mathbf{k}
\end{aligned} \tag{3.5}$$

De (3.4) e (3.5) segue que $\overline{\mathbf{u}\cdot\mathbf{v}} = \overline{\mathbf{v}}\cdot\overline{\mathbf{u}}$ como desejado.
(d) Temos:

$$\begin{aligned}
\overline{\alpha\mathbf{u}+\mathbf{v}} &= \overline{(\alpha u_1 + v_1)\mathbf{1} + (\alpha u_2 + v_2)\mathbf{i} + (\alpha u_3 + v_3)\mathbf{j} + (\alpha u_4 + v_4)\mathbf{k}} \\
&= (\alpha u_1 + v_1)\mathbf{1} - (\alpha u_2 + v_2)\mathbf{i} - (\alpha u_3 + v_3)\mathbf{j} - (u_4 + v_4)\mathbf{k} \\
&= \alpha(u_1\mathbf{1} - u_2\mathbf{i} - u_3\mathbf{j} - u_4\mathbf{k}) + (v_1\mathbf{1} - v_2\mathbf{i} - v_3\mathbf{j} - v_4\mathbf{k}) \\
&= \alpha\overline{\mathbf{u}} + \overline{\mathbf{v}}.
\end{aligned}$$

□

Proposição 3.1.4. *Todo elemento não nulo de $\mathbb{H}$ tem inverso multiplicativo.*

Prova. Seja $\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k} \in \mathbb{H} \setminus \{0\}$. Pela Proposição 3.1.3(a) temos

$$\mathbf{u}\cdot\overline{\mathbf{u}} = \overline{\mathbf{u}}\cdot\mathbf{u} = (u_1^2 + u_2^2 + u_3^2 + u_4^2)\mathbf{1} \tag{3.6}$$

Como $\mathbf{u} \neq 0$, então $u_1^2 + u_2^2 + u_3^2 + u_4^2 \neq 0$. Desse modo, multiplicando (3.6) por $(u_1^2 + u_2^2 + u_3^2 + u_4^2)^{-1}$ vem

$$\mathbf{u}\cdot\frac{\overline{\mathbf{u}}}{u_1^2 + u_2^2 + u_3^2 + u_4^2} = \frac{\overline{\mathbf{u}}}{u_1^2 + u_2^2 + u_3^2 + u_4^2}\cdot\mathbf{u} = \mathbf{1} \tag{3.7}$$

Portanto, $\mathbf{u}$ é invertível. □

3.2 Representação matricial

Seja $M_2(\mathbb{C})$ o $\mathbb{R}$-espaço vetorial de todas as matrizes quadradas de ordem 2 com entradas nos complexos $\mathbb{C}$. A multiplicação usual em $M_2(\mathbb{C})$ lhe confere estrutura de $\mathbb{R}$-álgebra. De fato, podemos verificar sem dificuldades que esta é uma $\mathbb{R}$-álgebra de dimensão 8. Consideramos o seguinte subconjunto de $M_2(\mathbb{C})$:

$$\mathcal{H} := \left\{ \begin{pmatrix} \mathbf{w} & -\mathbf{z} \\ \overline{\mathbf{z}} & \overline{\mathbf{w}} \end{pmatrix} \mid \mathbf{w}, \mathbf{z} \in \mathbb{C} \right\}. \tag{3.8}$$

Proposição 3.2.1. *O subconjunto $\mathcal{H}$ é uma subálgebra de $M_2(\mathbb{C})$.*

Prova. Primeiro verificaremos que $\mathcal{H}$ é subespaço vetorial de $M_2(\mathbb{C})$.

Fazendo $\mathbf{z} = \mathbf{w} = 0$, temos

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{w} & -\mathbf{z} \\ \overline{\mathbf{z}} & \overline{\mathbf{w}} \end{pmatrix};$$

logo, a matriz nula pertence a $\mathcal{H}$. Por outro lado, dados $\alpha \in \mathbb{R}$ e

$$\begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix}, \quad \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix}$$

elementos de $\mathcal{H}$, temos:

$$\alpha \begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix} + \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix} = \begin{pmatrix} (\alpha\mathbf{w}_1 + \mathbf{w}_2) & -(\alpha\mathbf{z}_1 + \mathbf{z}_2) \\ \overline{(\alpha\mathbf{z}_1 + \mathbf{z}_2)} & \overline{(\alpha\mathbf{w}_1 + \mathbf{w}_2)} \end{pmatrix}$$

Assim, dessa igualdade segue que

$$\alpha \begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix} + \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix}$$

é elemento de $\mathcal{H}$. Portanto, $\mathcal{H}$ é subespaço vetorial de $M_2(\mathbb{C})$.

Agora mostraremos que $\mathcal{H}$ é fechado para a multiplicação. Dados

$$\begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix}, \quad \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix}$$

elementos de $\mathcal{H}$, temos:

$$\begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix} = \begin{pmatrix} \mathbf{w}_1 \cdot \mathbf{w}_2 - \mathbf{z}_1 \cdot \overline{\mathbf{z}_2} & -\mathbf{w}_1 \cdot \mathbf{z}_2 - \mathbf{z}_1 \cdot \overline{\mathbf{w}_2} \\ \overline{\mathbf{z}_1} \cdot \mathbf{w}_2 + \overline{\mathbf{w}_1} \cdot \overline{\mathbf{z}_2} & -\overline{\mathbf{z}_1} \cdot \mathbf{z}_2 + \overline{\mathbf{w}_1} \cdot \overline{\mathbf{w}_2} \end{pmatrix}$$
$$= \begin{pmatrix} \mathbf{w}_1 \cdot \mathbf{w}_2 - \mathbf{z}_1 \cdot \overline{\mathbf{z}_2} & -(\mathbf{w}_1 \cdot \mathbf{z}_2 + \mathbf{z}_1 \cdot \overline{\mathbf{w}_2}) \\ \overline{\mathbf{w}_1 \cdot \mathbf{z}_2 + \mathbf{z}_1 \cdot \overline{\mathbf{w}_2}} & \overline{\mathbf{w}_1 \cdot \mathbf{w}_2 - \mathbf{z}_1 \cdot \overline{\mathbf{z}_2}} \end{pmatrix}.$$

Dessa última igualdade segue que o produto

$$\begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix}$$

pertence a $\mathcal{H}$ como queríamos provar. □

Observação 3.2.2. Como é bem conhecido, $M_2(\mathbb{C})$ é uma $\mathbb{R}$-álgebra associativa. Assim, em particular, $\mathcal{H}$ também é associativa.

Proposição 3.2.3. *As matrizes*

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}, \quad J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ e } K := \begin{pmatrix} 0 & -\mathbf{i} \\ -\mathbf{i} & 0 \end{pmatrix}$$

formam uma base de $\mathcal{H}$. Em particular, $\mathcal{H}$ é uma $\mathbb{R}$-álgebra com identidade e de dimensão 4.

Prova. Seja

$$\begin{pmatrix} \mathbf{w} & -\mathbf{z} \\ \overline{\mathbf{z}} & \overline{\mathbf{w}} \end{pmatrix}$$

um elemento arbitrário de $\mathcal{H}$. Escrevendo $\mathbf{w} = a + b\mathbf{i}$ e $\mathbf{z} = c + d\mathbf{i}$ temos

$$\begin{pmatrix} \mathbf{w} & -\mathbf{z} \\ \overline{\mathbf{z}} & \overline{\mathbf{w}} \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix} + c \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & -\mathbf{i} \\ -\mathbf{i} & 0 \end{pmatrix}$$
$$= aE + bI + cJ + dK$$

Dessa igualdade segue que E, I, J e K formam um conjunto gerador de $\mathcal{H}$.

Agora suponhamos

$$aE + bI + cJ + dK = 0$$

Então:

$$\begin{pmatrix} a+b\mathbf{i} & -(c+d\mathbf{i}) \\ c-d\mathbf{i} & a-b \end{pmatrix} = \begin{pmatrix} a+b\mathbf{i} & -(c+d\mathbf{i}) \\ \overline{c+d\mathbf{i}} & \overline{a+b\mathbf{i}} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Logo, $a+b\mathbf{i} = c+d\mathbf{i} = 0$, ou seja, $a = b = c = d = 0$.

Portanto, como $\{E, I, J, K\}$ é um conjunto gerador e linearmente independente de $\mathcal{H}$ segue que ele é uma base. A segunda parte do teorema é consequência imediata da primeira. □

Observação 3.2.4. Cálculos diretos nos dão as seguintes igualdades

$$I \cdot J = -J \cdot I = K,\ J \cdot K = -K \cdot J = I,\ K \cdot I = -I \cdot K = J \quad \text{e} \quad I^2 = J^2 = K^2 = -E \tag{3.9}$$

Teorema 3.2.5. *O mapa*

$$F : \mathbb{H} \to \mathcal{H}, \qquad \alpha\mathbf{1} + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \mapsto \alpha E + \beta I + \gamma J + \delta K$$

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

$$F(\mathbf{1}) = E,\ F(\mathbf{i}) = I,\ F(\mathbf{j}) = J,\ \textit{e}\ F(\mathbf{k}) = K$$

Prova. Sejam $\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}$ e $\mathbf{v} = v_1\mathbf{1} + v_2\mathbf{i} + v_3\mathbf{j} + v_4\mathbf{k}$ elementos de $\mathbb{H}$ e $\alpha \in \mathbb{R}$. Então:

$$\begin{aligned} F(\alpha\mathbf{u} + \mathbf{v}) &= F((\alpha u_1 + v_2)\mathbf{1} + (\alpha u_2 + v_2)\mathbf{i} + (\alpha u_3 + v_3)\mathbf{j} + (\alpha u_4 + v_4)\mathbf{k}) \\ &= (\alpha u_1 + v_2)E + (\alpha u_2 + v_2)I + (\alpha u_3 + v_3)J + (\alpha u_4 + v_4)K \\ &= \alpha(u_1E + u_2I + u_3J + u_4K) + (v_1E + v_2I + v_3J + v_4K) \\ &= \alpha F(\mathbf{u}) + F(\mathbf{v}) \end{aligned} \tag{3.10}$$

Logo, F é de fato uma transformação linear. Além disso, ela é uma bijeção pois envia base em base. Assim, resta provar que F preserva a multiplicação. Para isso,

consideremos $\mathbf{u}$ e $\mathbf{v}$ elementos de $\mathbb{H}$ como antes. Então:

$$\begin{aligned}
F(\mathbf{u})\cdot F(\mathbf{v}) &= (u_1E+u_2I+u_3J+u_4K)(v_1E+v_2I+v_3J+v_4K)\\
&= u_1v_1E+(u_1v_2+u_2v_1)I+(u_1v_3+u_3v_1)J+\\
&\quad (u_1v_4+u_4v_1)K+u_2v_2I^2+u_2v_3IJ+u_2v_4IK+\\
&\quad u_3v_2JI+u_3v_3J^2+u_3v_4JK+u_4v_2KI+u_4v_3KJ+u_4v_4K^2\\
&= u_1v_1E+(u_1v_2+u_2v_1)I+(u_1v_3+u_3v_1)J+\\
&\quad (u_1v_4+u_4v_1)K-u_2v_2E+u_2v_3K-u_2v_4J\\
&\quad -u_3v_2K-u_3v_3E+u_3v_4I+u_4v_2J-u_4v_3I-u_4v_4E\\
&= (u_1v_1-u_2v_2-u_3v_3-u_4v_4)E+(u_1v_1+u_2v_1+u_3v_4-u_4v_3)I+\\
&\quad (u_1v_3-u_2v_4+u_3v_1+u_4v_2)J+(u_1v_4++u_2v_3-u_3v_2+u_4v_1)K\\
&= F((u_1v_1-u_2v_2-u_3v_3-u_4v_4)\mathbf{1}+(u_1v_1+u_2v_1+u_3v_4-u_4v_3)\mathbf{i}+\\
&\quad (u_1v_3-u_2v_4+u_3v_1+u_4v_2)\mathbf{j}+(u_1v_4++u_2v_3-u_3v_2+u_4v_1)\mathbf{k})\\
&= F(\mathbf{u}\cdot\mathbf{v}). \qquad (3.11)
\end{aligned}$$

Portanto, F é um isomorfismo de $\mathbb{R}$-álgebras. □

Corolário 3.2.6. *A álgebra dos quatérnios é associativa.*

Prova. De acordo com a Observação 3.2.2, $\mathcal{H}$ é uma $\mathbb{R}$-álgebra associativa. Assim, pelo isomorfismo $\mathbb{H}\simeq\mathcal{H}$ provado no teorema anterior segue o resultado desejado. □

Proposição 3.2.7. *A álgebra dos quatérnios $\mathbb{H}$ é uma $\mathbb{R}$-álgebra de composição com respeito a norma euclidiana, ou seja, para cada $\mathbf{u},\mathbf{v}\in\mathbb{H}$,*

$$\| \mathbf{u}\cdot\mathbf{v} \| = \| \mathbf{u} \| \cdot \| \mathbf{v} \| .$$

Em particular $\mathbb{H}$ é uma álgebra de divisão.

Prova. Sejam $\mathbf{u},\mathbf{v}\in\mathbb{H}$. Pelo item (c) da Proposição 3.1.3 temos

$$\overline{\mathbf{u}\cdot\mathbf{v}} = \overline{\mathbf{v}}\cdot\overline{\mathbf{u}} \qquad (3.12)$$

Assim,

$$\begin{aligned} \| \mathbf{u}\cdot\mathbf{v} \|^2 \mathbf{1} &= (\mathbf{uv})\overline{\mathbf{u}\cdot\mathbf{v}} && (3.13)\\ &= (\mathbf{uv})\cdot(\overline{\mathbf{v}}\cdot\overline{\mathbf{u}}) && (3.14)\\ &= \mathbf{u}(\mathbf{v}\overline{\mathbf{v}})\overline{\mathbf{u}} && (3.15)\\ &= \| \mathbf{v} \| \mathbf{u}\overline{\mathbf{u}} && (3.16)\\ &= \| \mathbf{u} \|^2 \cdot \| \mathbf{v} \|^2 \mathbf{1} && (3.17) \end{aligned}$$

onde as igualdades (3.13), (3.16) e (3.17) seguem da Proposição 3.1.3 (a), (3.14) segue de (3.12) e (3.15) segue da propriedade associativa de $\mathbb{H}$. Finalmente, de (3.17) concluímos

$$\| \mathbf{u}\cdot\mathbf{v} \| = \| \mathbf{u} \| \cdot \| \mathbf{v} \|$$

como desejávamos. □

A álgebra $\mathbb{C}$ surge a partir da álgebra $\mathbb{R}$ quando, no produto cartesiano $\mathbb{R}\times\mathbb{R}$ introduzimos uma multiplicação definida por

$$(a_1,a_2)(b_1,b_2) = (a_1b_1 - b_2a_2, a_2b_1 + b_2a_1), \quad a_1,a_2,b_1,b_2 \in \mathbb{R}.$$

Nosso próximo resultado mostrará que a álgebra dos quatérnios pode ser obtida da álgebra dos complexos por meio de um processo de duplicação análogo.

Teorema 3.2.8. *Seja $\cdot$ uma multiplicação em $\mathbb{C}\times\mathbb{C}$ definida pela seguinte igualdade:*

$$(\mathbf{w}_1,\mathbf{z}_1)\cdot(\mathbf{w}_2,\mathbf{z}_2) = (\mathbf{w}_1\mathbf{w}_2 - \overline{\mathbf{z}}_2\mathbf{z}_1, \mathbf{z}_1\overline{\mathbf{w}}_2 + \mathbf{z}_2\mathbf{w}_1) \tag{3.18}$$

para cada $\mathbf{w}_1,\mathbf{w}_2,\mathbf{z}_1,\mathbf{z}_2 \in \mathbb{C}$. Então a aplicação

$$\varphi : \mathbb{C}\times\mathbb{C} \to \mathcal{H}, \quad (\mathbf{w},\mathbf{z}) \mapsto \begin{pmatrix} \mathbf{w} & -\mathbf{z} \\ \overline{\mathbf{z}} & \overline{\mathbf{w}} \end{pmatrix}$$

é um isomorfismo de $\mathbb{R}$-álgebras. Em particular, $\mathbb{C}\times\mathbb{C}$ com esta multiplicação é uma $\mathbb{R}$-álgebra isomorfa a $\mathbb{H}$.

Prova. Dados $(\mathbf{w}_1, \mathbf{z}_1),\ (\mathbf{w}_2, \mathbf{z}_2) \in \mathbb{C} \times \mathbb{C}$ e $\alpha \in \mathbb{R}$ temos

$$\begin{aligned}
\varphi(\alpha(\mathbf{w}_1, \mathbf{z}_1) + (\mathbf{w}_2, \mathbf{z}_2)) &= \varphi(\alpha\mathbf{w}_1 + \mathbf{w}_2, \alpha\mathbf{z}_1 + \mathbf{z}_2) \\
&= \begin{pmatrix} \alpha\mathbf{w}_1 + \mathbf{w}_2 & -(\alpha\mathbf{z}_1 + \mathbf{z}_2) \\ \overline{\alpha\mathbf{z}_1 + \mathbf{z}_2} & \overline{\alpha\mathbf{w}_1 + \mathbf{w}_2} \end{pmatrix} \\
&= \begin{pmatrix} \alpha\mathbf{w}_1 + \mathbf{w}_2 & -\alpha\mathbf{z}_1 - \mathbf{z}_2) \\ \alpha\overline{\mathbf{z}_1} + \overline{\mathbf{z}_2} & \alpha\overline{\mathbf{w}_1} + \overline{\mathbf{w}_2} \end{pmatrix} \\
&= \alpha \begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}_1} & \overline{\mathbf{w}_1} \end{pmatrix} + \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}_2} & \overline{\mathbf{w}_2} \end{pmatrix} \\
&= \alpha\varphi(\mathbf{w}_1, \mathbf{z}_1) + \varphi(\mathbf{w}_2, \mathbf{z}_2). \qquad (3.19)
\end{aligned}$$

Logo, φ é transformação linear.

Também temos

$$\varphi(\mathbf{w}, \mathbf{z}) = \begin{pmatrix} \mathbf{w} & -\mathbf{z} \\ \overline{\mathbf{z}} & \overline{\mathbf{w}} \end{pmatrix} = 0$$

se, e somente se, $\mathbf{w} = \mathbf{z} = 0$. Assim, φ é uma transformação linear injetora. Como $\dim(\mathbb{C} \times \mathbb{C}) = \dim(\mathcal{H})$ segue que φ é um isomorfismo linear.

Finalmente, mostraremos que φ preserva multiplicação. Para isso, suponhamos $(\mathbf{w}_1, \mathbf{z}_1),\ (\mathbf{w}_2, \mathbf{z}_2) \in \mathbb{C} \times \mathbb{C}$. Então:

$$\begin{aligned}
\varphi((\mathbf{w}_1, \mathbf{z}_1) \cdot (\mathbf{w}_2, \mathbf{z}_2)) &= \varphi(\mathbf{w}_1\mathbf{w}_2 - \overline{\mathbf{z}}_2\mathbf{z}_1, \mathbf{z}_1\overline{\mathbf{w}}_2 + \mathbf{z}_2\mathbf{w}_1) \\
&= \begin{pmatrix} \mathbf{w}_1\mathbf{w}_2 - \overline{\mathbf{z}}_2\mathbf{z}_1 & -\mathbf{z}_1\overline{\mathbf{w}}_2 - \mathbf{z}_2\mathbf{w}_1 \\ \overline{\mathbf{z}_1}\mathbf{w}_2 + \overline{\mathbf{z}}_2\overline{\mathbf{w}_1} & \overline{\mathbf{w}_1} \cdot \overline{\mathbf{w}_2} - \mathbf{z}_2\overline{\mathbf{z}_1} \end{pmatrix} \\
&= \begin{pmatrix} \mathbf{w}_1 & -\mathbf{z}_1 \\ \overline{\mathbf{z}}_1 & \overline{\mathbf{w}}_1 \end{pmatrix} \cdot \begin{pmatrix} \mathbf{w}_2 & -\mathbf{z}_2 \\ \overline{\mathbf{z}}_2 & \overline{\mathbf{w}}_2 \end{pmatrix} \\
&= \varphi(\mathbf{w}_1, \mathbf{z}_1) \cdot \varphi(\mathbf{w}_2, \mathbf{z}_2)
\end{aligned}$$

Portanto, φ é um isomorfismo de $\mathbb{R}$-álgebras. □

3.3 O teorema de Frobenius

Em toda esta seção $\mathbb{K}$ denotará uma $\mathbb{R}$-álgebra associativa e com identidade $\mathbf{1}$.

Definição 3.3.1. Três elementos $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{K}$ formam um *tripla Hamiltoniana* se

satisfazem as nove condições de Hamilton, i.e., a tabela de multiplicação para estes elementos é:

$\cdot$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$
$\mathbf{u}$	$-\mathbf{1}$	$\mathbf{w}$	$-\mathbf{v}$
$\mathbf{v}$	$-\mathbf{w}$	$-\mathbf{1}$	$\mathbf{u}$
$\mathbf{w}$	$\mathbf{v}$	$-\mathbf{u}$	$-\mathbf{1}$

Observação 3.3.2. O subespaço vetorial de $\mathbb{K}$ gerado por $\mathbf{1}$ é uma $\mathbb{R}$-subálgebra isomorfa a $\mathbb{R}$. Em virtude disso, abusaremos da notação e identificaremos $\mathbb{R}$ como uma subálgebra de $\mathbb{K}$.

Definimos o seguinte subconjunto de $\mathbb{K}$.

$$\mathrm{Im}(\mathbb{K}) = \{\mathbf{v} \in \mathbb{K} \mid \mathbf{v}^2 \in \mathbb{R} \text{ e } \mathbf{v} \notin \mathbb{R} \setminus \{0\}\}. \tag{3.20}$$

Chamaremos $\mathrm{Im}(\mathbb{K})$ de *parte imaginária de* $\mathbb{K}$. Claramente,

$$\mathbb{R} \cap \mathrm{Im}(\mathbb{K}) = \{0\} \tag{3.21}$$

e se $\mathbf{v} \in \mathrm{Im}(\mathbb{K})$, então $\alpha\mathbf{v} \in \mathrm{Im}(\mathbb{K})$ para cada $\alpha \in \mathbb{R}$. A terminologia é baseada na observação que no caso $\mathbb{K} = \mathbb{C}$ ou $\mathbb{H}$, existe um espaço de vetores *imaginários*, no sentido que se $\mathbf{v} \notin \mathbb{R}$, então $\mathbf{v}^2 \in \mathbb{R}$.

Proposição 3.3.3. *São verdadeiras as seguintes afirmações:*

(a) *Se* $\mathbf{u}, \mathbf{v} \in \mathrm{Im}(\mathbb{K})$ *são linearmente independentes, então* $\mathbf{1}, \mathbf{u}$ *e* $\mathbf{v}$ *são linearmente independentes.*

(b) *Se* $\mathbf{u}, \mathbf{v}, \mathbf{u}+\mathbf{v} \in \mathrm{Im}(\mathbb{K})$*, então*

$$\mathbf{u} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{u} \in \mathbb{R}. \tag{3.22}$$

(c) *Se* $\mathbb{K}$ *não tem divisores de zero, então para cada elemento* $\mathbf{v} \in \mathrm{Im}(\mathbb{K})$ *temos* $\mathbf{v}^2 = -\omega$ *com* $\omega > 0$*. Em particular, se* $\mathrm{Im}(\mathbb{K}) \neq \emptyset$ *então existe* $\mathbf{u} \in \mathrm{Im}(\mathbb{K})$ *tal que* $\mathbf{u}^2 = -1$*.*

(d) *Se* $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{K}$ *é uma tripla Hamiltoniana, então a transformação linear de*

$$\varphi : \mathbb{H} \to \mathbb{K}$$

definido por $\varphi(\mathbf{1}) = \mathbf{1}$, $\varphi(\mathbf{i}) = \mathbf{u}$, $\varphi(\mathbf{j}) = \mathbf{v}$, $\varphi(\mathbf{k}) = \mathbf{w}$ *é injetora e o subespaço* $\langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$ *está contido em* $\mathrm{Im}(\mathbb{K})$.

Prova. (a) Suponhamos que $\mathbf{v} = \alpha + \beta\mathbf{u}$, com $\alpha, \beta \in \mathbb{R}$. Teremos

$$2\alpha\beta\mathbf{u} = \mathbf{v}^2 - \alpha^2 - \beta^2\mathbf{u}^2 \in \mathbb{R}.$$

Portanto, $\alpha\beta = 0$, pois $\mathbf{u} \in \mathrm{Im}(\mathbb{K})$. Pela hipótese, $\alpha \neq 0$ pois $\mathbf{u}$ e $\mathbf{v}$ são linearmente independentes. Assim, $\beta = 0$. Isso por sua vez implica que $\mathbf{v} \notin \mathrm{Im}(\mathbb{K})$. Mas isso é um absurdo. Portanto (a) está provada.

(b) Segue observando-se que

$$\mathbf{u} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{u} = (\mathbf{u} + \mathbf{v})^2 - \mathbf{u}^2 - \mathbf{v}^2 \in \mathbb{R}.$$

(c) Seja $\mathbf{v} \in \mathrm{Im}(\mathbb{K})$. Por definição $\mathbf{v}^2 = \alpha$ com $\alpha \in \mathbb{R}$. Se $\alpha \geq 0$, então $\alpha = \beta^2$, para um $\beta \in \mathbb{R}$. Assim,

$$(\mathbf{v} - \beta) \cdot (\mathbf{v} + \beta) = \mathbf{v}^2 - \alpha = 0.$$

Disso segue $\mathbf{v} = \beta$ ou $\mathbf{v} = -\beta$ e $\mathbf{v}$ não pertenceria a $\mathrm{Im}(\mathbb{K})$ o que é um absurdo. Logo, $\alpha = -\omega$ com $\omega > 0$ e $\omega = \gamma^2$. O elemento $\mathbf{u} = \gamma^{-1}v$ é tal que $\mathbf{u}^2 = -1$.

(d) A injetividade de φ é equivalente a mostrar que $\mathbf{1}$, $\mathbf{u}$, $\mathbf{v}$ e $\mathbf{w}$ são linearmente independentes em $\mathbb{K}$. Os vetores $\mathbf{u}$ e $\mathbf{v}$ são linearmente independentes porque se $\mathbf{v}$ fosse múltiplo escalar de $\mathbf{u}$, teríamos $\mathbf{w} = \mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u} = -\mathbf{w}$ e portanto $\mathbf{w} = 0$, contradizendo $\mathbf{w}^2 = -1 \neq 0$. O item (a) mostra que $\mathbf{1}, \mathbf{u}$ e $\mathbf{v}$ são linearmente independentes. Se $\mathbf{w} \in \langle \mathbf{1}, \mathbf{u}, \mathbf{v} \rangle$, existiriam únicos $\alpha, \beta, \gamma \in \mathbb{R}$ tais que

$$\mathbf{w} = \alpha\mathbf{u} + \beta\mathbf{v} + \gamma. \tag{3.23}$$

Multiplicando essa relação por u, teremos

$$-\mathbf{v} = -\alpha + \beta\mathbf{w} + \gamma\mathbf{u} \Rightarrow \mathbf{w} = -\frac{\gamma}{\beta}\mathbf{u} - \frac{1}{\beta}\mathbf{v} + \frac{\alpha}{\beta}. \tag{3.24}$$

Assim, (3.23) e (3.24) implicaria, pela unicidade das constantes, que $\beta^2 = -1$. Mas isso é um absurdo. Logo, $\mathbf{1}, \mathbf{u}, \mathbf{v}, \mathbf{w}$ são linearmente independentes. Por fim

temos que $\langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$ está contido em $\mathrm{Im}(\mathbb{K})$. De fato, notemos que:

$$\begin{aligned}(\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w})(\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w}) &= -\alpha^2 - \beta^2 - \gamma^2 + \alpha\beta(\mathbf{uv} + \mathbf{vu}) \\ &+ \alpha\gamma(\mathbf{wu} + \mathbf{uw}) + \beta\gamma(\mathbf{vw} + \mathbf{wv}) \\ &= (\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w})^2 \in \mathbb{R}\end{aligned}$$

e que $\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w} \notin \mathbb{R} - \{0\}$ (pois caso contrário, teremos $\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w} = a \in \mathbb{R}$). Dai $\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w} - a = 0$. Aplicando φ em ambos os membros:

$$\varphi(\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w} - a) = \varphi(0) = 0,$$

ou equivalentemente,

$$\alpha\mathbf{u} + \beta\mathbf{v} + \gamma\mathbf{w} - a \in \ker\varphi = \{\,0\}$$

Mas isso é um absurdo. □

A noção de tripla de Hamilton deve sua importância ao seguinte resultado de existência.

Proposição 3.3.4. *Seja $U \subseteq \mathrm{Im}(\mathbb{K})$ um subespaço de dimensão dois de $\mathbb{K}$. Para cada elemento $\mathbf{u} \in U$ tal que $\mathbf{u}^2 = -\mathbf{1}$, existe $\mathbf{v} \in U$ tal que $\mathbf{u}, \mathbf{v}$ e $\mathbf{u} \cdot \mathbf{v}$ formam uma tripla Hamiltoniana em $\mathbb{K}$.*

Prova. Pela Proposição 3.3.3 (b), existe $\mathbf{v}' \in U$ tal que $\mathbf{u} \cdot \mathbf{v}' + \mathbf{v}' \cdot \mathbf{u} = \beta \in \mathbb{R}$. Definimos agora $\mathbf{v}'' = \mathbf{v}' + \frac{\beta}{2}\mathbf{u}$. Obviamente, $\mathbf{v}'' \in U \subset \mathrm{Im}(\mathbb{K})$. Além disso,

$$\begin{aligned}\mathbf{u} \cdot \mathbf{v}'' + \mathbf{v}'' \cdot \mathbf{u} &= \mathbf{u} \cdot (\mathbf{v}' + \frac{\beta}{2}\mathbf{u}) + (\mathbf{v}' + \frac{\beta}{2}\mathbf{u}) \cdot \mathbf{u} \\ &= \frac{\beta}{2}\mathbf{u}^2 + \mathbf{u} \cdot \mathbf{v}' + \frac{\beta}{2}\mathbf{u}^2 + \mathbf{v}' \cdot \mathbf{u} \\ &= \beta\mathbf{u}^2 + \mathbf{u} \cdot \mathbf{v}' + v' \cdot \mathbf{u} \\ &= -\beta + \beta \\ &= 0\end{aligned}$$

Pela prova da Proposição 3.3.3 (c), existe um múltiplo $\mathbf{v} = \gamma\mathbf{v}''$, com $\gamma \in \mathbb{R}$, tal que $\mathbf{v}^2 = -1$. Uma conta direta nos mostra que $\mathbf{v}$ também satisfaz a relação $\mathbf{u} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{u} = 0$.

Assim,

$$\mathbf{u}^2 = \mathbf{v}^2 = -1 \quad \text{e} \quad \mathbf{u} \cdot \mathbf{v} = -\mathbf{v} \cdot \mathbf{u}.$$

Para concluirmos o desejado resta provar que para $\mathbf{w} = \mathbf{u} \cdot \mathbf{v}$ temos

$$\mathbf{w}^2 = -1 \quad \text{e}$$

(as demais identidades seguem de $\mathbf{u}^2 = \mathbf{v}^2 = -1$, $\mathbf{wu} = \mathbf{u} \cdot \mathbf{v}$, e $\mathbf{u} \cdot \mathbf{v} = -\mathbf{v} \cdot \mathbf{u}$). Ora,

$$\mathbf{v} \cdot \mathbf{w}^2 = (\mathbf{v} \cdot \mathbf{w}) \cdot \mathbf{w} = -(\mathbf{v}^2 \cdot \mathbf{u}) \cdot \mathbf{w} = -\mathbf{v}.$$

Assim, deduzimos

$$\mathbf{v}(\mathbf{w}^2 + 1) = 0.$$

Portanto, $\mathbf{w}^2 = -1$, já que $\mathbb{K}$ não tem divisores de zero. □

Necessitaremos mais adiante da seguinte definição:

Definição 3.3.5. Dizemos que $\mathbb{K}$ é uma $\mathbb{R}$-álgebra *quadrática* se para cada $\mathbf{u} \in \mathbb{K}$, existem $\alpha, \beta \in \mathbb{R}$ tais que $\mathbf{u}^2 = \alpha\mathbf{u} + \beta$.

Exemplo 3.3.6. A extensão $\mathbb{H}$ é quadrática. De fato, para cada $\mathbf{u} = a + bi + cj + dk$, temos $\mathbf{u}^2 = 2a\mathbf{u} - (a^2 + b^2 + c^2 + d^2)$. Em particular, como $\mathbb{C} \subset \mathbb{H}$, também temos que $\mathbb{C}$ é quadrática.

O seguinte resultado de Frobenius mostra a importância da noção de elemento imaginário.

Teorema 3.3.7 (Lema de Frobenius). *Seja $\mathbb{K}$ uma $\mathbb{R}$-álgebra quadrática. Então* $\mathrm{Im}(\mathbb{K})$ *é um subespaço vetorial de $\mathbb{K}$ e*

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

Prova. Sejam $\mathbf{u}, \mathbf{v} \in \mathrm{Im}(\mathbb{K})$. É suficiente mostrar que $\mathbf{u} + \mathbf{v} \in \mathrm{Im}(\mathbb{K})$, pois $\alpha\mathbf{u} \in \mathrm{Im}(\mathbb{K})$ para cada $\mathbf{u} \in \mathrm{Im}(\mathbb{K})$ e para cada $\alpha \in \mathbb{R}$ como já observado acima. Se $\mathbf{u}$ e $\mathbf{v}$ são linearmente dependentes, teremos $\mathbf{v} = \alpha\mathbf{u}$ e $\mathbf{u} + \mathbf{v} = (1 + \alpha)\mathbf{u} \in \mathrm{Im}(\mathbb{K})$. Assim, suponhamos $\mathbf{u}$ e $\mathbf{v}$ linearmente independentes. Como $\mathbb{K}$ é quadrática,

$$(\mathbf{u} + \mathbf{v})^2 = \alpha_1 + \beta_1(\mathbf{u} + \mathbf{v}), \quad (\mathbf{u} - \mathbf{v})^2 = \alpha_2 + \beta_2(\mathbf{u} - \mathbf{v}),$$

para certos $\alpha_1, \beta_1, \alpha_2, \beta_2 \in \mathbb{R}$. Isso implica que

$$(\beta_1 + \beta_2)\mathbf{u} + (\beta_1 - \beta_2)\mathbf{v} = 2\mathbf{u}^2 + 2\mathbf{v}^2 - (\alpha_1 + \alpha_2) \in \mathbb{R}.$$

A Proposição 3.3.3 garante que $\beta_1+\beta_2 = \beta_1-\beta_2 = 0$, i.e. $\beta_1 = \beta_2 = 0$ e $(\mathbf{u}+\mathbf{v})^2 = \alpha_1$. Novamente pela Proposição 3.3.3 $\mathbf{u}+\mathbf{v} \notin \mathbb{R}$ e portanto $\mathbf{u}+\mathbf{v} \in \mathrm{Im}(\mathbb{K})$.

Seja $\mathbf{v} \in \mathbb{K}\backslash\mathbb{R}$. Por hipótese $\mathbf{v}^2 = \alpha+\beta\mathbf{v}$ e portanto $(\mathbf{v}-\beta/2)^2 = (\alpha+\beta^2/4)$. Como $\mathbf{v}-\beta/2 \notin \mathbb{R}$ então $\mathbf{v}-\beta/2 \in \mathrm{Im}(\mathbb{K})$, i.e., $\mathbb{K} = \mathbb{R}+\mathrm{Im}(\mathbb{K})$ e portanto $\mathbb{K} = \mathbb{R} \oplus \mathrm{Im}(\mathbb{K})$. □

Podemos finalmente provar o resultado principal dessa seção.

Teorema 3.3.8 (**Frobenius, 1877**). *Seja $\mathbb{K}$ uma $\mathbb{R}$-álgebra quadrática e sem divisores de zero. Então, a menos de isomorfismos, $\mathbb{K}$ é uma das seguintes $\mathbb{R}$-álgebras: $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. Em particular, uma extensão quadrática sem divisores de zero e não comutativa deve ser isomorfa a $\mathbb{H}$.*

Prova. Seja $n \geq 1$ a dimensão vetorial de $\mathbb{K}$. Se $n = 1$, é imediato deduzir que o homomorfismo $\varphi : \mathbb{K} \to \mathbb{R}$ definido por $\varphi(1) = 1$ é um isomorfismo de $\mathbb{K}$ em $\mathbb{R}$.

Seja $n = 2$. Pelo Lema de Frobenius temos $\mathrm{Im}(\mathbb{K}) \neq \emptyset$ e portanto existe $\mathbf{u} \in \mathbb{K}$ tal que $\mathbf{u}^2 = -1$. Seja $\varphi : \mathbb{C} \to \mathbb{K}$ a transformação linear definida por $\varphi(1) = 1$ e $\varphi(i) = \mathbf{u}$. Esta transformação é injetora pois 1 e $\mathbf{u}$ são linearmente independentes. Sendo $n = 2$, φ é um isomorfismo e linear. Para mostrar que é isomorfismo de $\mathbb{R}$-álgebras basta mostrar que $\varphi(\mathbf{u} \cdot \mathbf{u}') = \varphi(\mathbf{u}) \cdot \varphi(\mathbf{u}')$ o que é imediato.

Seja $n \geq 3$. Pelo Teorema 3.3.7, $\mathbb{K} = \mathbb{R} \oplus \mathrm{Im}(\mathbb{K})$. Assim, $\dim(\mathrm{Im}(\mathbb{K})) \geq 2$. Dessa forma, pela Proposição 3.3.4, $\mathbb{K}$ contém uma tripla Hamiltoniana $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathrm{Im}(\mathbb{K})$ (em particular, $\dim(\mathrm{Im}(\mathbb{K})) \geq 3$). Mostraremos agora que $\mathrm{Im}(\mathbb{K}) = \langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$. Para isso, suponhamos $\mathbf{x} \in \mathrm{Im}(\mathbb{K})$ arbitrário. Pela Proposição 3.3.3, existem $\alpha, \beta, \gamma \in \mathbb{R}$ tais que

$$\mathbf{x} \cdot \mathbf{u} + \mathbf{u} \cdot \mathbf{x} = \alpha, \quad \mathbf{x} \cdot \mathbf{v} + \mathbf{v} \cdot \mathbf{x} = \beta, \quad \mathbf{x} \cdot \mathbf{w} + \mathbf{w} \cdot \mathbf{x} = \gamma. \tag{3.25}$$

Multiplicando à direita a primeira equação por $\mathbf{v}$ e multiplicando à esquerda a segunda equação por $\mathbf{u}$, deduzimos

$$\mathbf{x} \cdot \mathbf{w} + (\mathbf{u} \cdot \mathbf{x}) \cdot \mathbf{v} = \alpha\mathbf{v}, \quad \mathbf{u} \cdot (\mathbf{x} \cdot \mathbf{v}) + \mathbf{w} \cdot \mathbf{x} = \beta\mathbf{u}$$

e portanto

$$\mathbf{x} \cdot \mathbf{w} - \mathbf{w} \cdot \mathbf{x} = \alpha\mathbf{v} - \beta\mathbf{u}.$$

A última equação combinada com a terceira em (3.25) fornece

$$2\mathbf{x} \cdot \mathbf{w} \in \langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$$

e enfim $-2\mathbf{x} = \mathbf{x} \cdot \mathbf{w}^2 \in \langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$, i.e. $\mathrm{Im}(\mathbb{K}) = \langle \mathbf{u}, \mathbf{v}, \mathbf{w} \rangle$. Assim, $\dim \mathbb{K} = 4$ e a transformação linear $\varphi : \mathbb{H} \to \mathbb{K}$ tal que $\varphi(\mathbf{1}) = \mathbf{1}$, $\varphi(\mathbf{i}) = \mathbf{u}$, $\varphi(\mathbf{j}) = v$ e $\varphi(\mathbf{k}) = \mathbf{w}$ é um isomorfismo de $\mathbb{R}$-álgebras. □

Capítulo 4

Álgebra dos Octônios

Nesse capítulo estudamos a álgebra dos octônios de Cayley. Assim como ocorre com os quatérnios, veremos que a álgebra dos octônios é de divisão, de composição e não comutativa. A novidade nesse caso é que ela não é associativa. De acordo com relatos históricos, a álgebra dos octônios foi descoberta dois meses após os quatérnios por John T. Graves. Todavia, a descoberta de Graves só foi publicada 5 anos depois (1848). Em 1845, Cayley redescobre a álgebra dos quatérnios e a publica no apêndice de um trabalho sobre funções elíticas. Daí em diante esta álgebra passa a ser chamada de álgebra dos octônios de Cayley.

4.1 Definição e propriedades básicas

O produto cartesiano $\mathbb{H} \times \mathbb{H}$ tem estrutura natural de $\mathbb{R}$-espaço vetorial onde as operações de adição e multiplicação por escalar são dadas pelas seguintes igualdades:

$$(\mathbf{u}_1, \mathbf{v}_1) + (\mathbf{u}_2, \mathbf{v}_2) := (\mathbf{u}_1 + \mathbf{u}_2, \mathbf{v}_1 + \mathbf{v}_2) \tag{4.1}$$

para quaisquer $(\mathbf{u}_1, \mathbf{v}_1)$, $(\mathbf{u}_2, \mathbf{v}_2) \in \mathbb{H}$, e

$$\alpha(\mathbf{u}, \mathbf{v}) := (\alpha\mathbf{u}, \alpha\mathbf{v}) \tag{4.2}$$

para quaiquer $(\mathbf{u}, \mathbf{v}) \in \mathbb{H}\times\mathbb{H}$ e $\alpha \in \mathbb{R}$. Pode-se verificar que $\mathbb{H}\times\mathbb{H}$ com estas operações é isomorfo, como $\mathbb{R}$-espaço vetorial, a $\mathbb{R}^8$.

Inspirado no processo de duplicação que permite obter os quatérnios a partir da $\mathbb{R}$-álgebra dos complexos, definimos uma operação em $\mathbb{H} \times \mathbb{H}$ através da seguinte

igualdade:

$$(\mathbf{u}_1, \mathbf{u}_2) \cdot (\mathbf{v}_1, \mathbf{v}_2) := (\mathbf{u}_1\mathbf{v}_1 - \overline{\mathbf{v}}_2\mathbf{u}_2, \mathbf{u}_2\overline{\mathbf{v}}_1 + \mathbf{v}_2\mathbf{u}_1). \tag{4.3}$$

para quaisquer $(\mathbf{u}_1, \mathbf{u}_2)$, $(\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{H} \times \mathbb{H}$. É imediata a verificação que esta operação é uma multiplicação em $\mathbb{H} \times \mathbb{H}$. Assim, $(\mathbb{H} \times \mathbb{H}, \cdot)$ é uma $\mathbb{R}$-álgebra de dimensão 8.

Definição 4.1.1. A $\mathbb{R}$-álgebra $(\mathbb{H} \times \mathbb{H}, \cdot)$ é chamada $\mathbb{R}$-*álgebra dos octônios de Cayley* e a denotamos por $\mathbb{O}$. Chamaremos os elementos de $\mathbb{O}$ de octônios.

Observação 4.1.2. A álgebra dos octônios satisfaz as seguintes propriedades:

(a) Para $(\mathbf{1}, 0) \in \mathbb{O}$ temos $(\mathbf{1}, 0) \cdot (\mathbf{u}_1, \mathbf{u}_2) = (\mathbf{u}_1, \mathbf{u}_2) \cdot (\mathbf{1}, 0) = (\mathbf{u}_1, \mathbf{u}_2)$ para qualquer $(\mathbf{u}_1, \mathbf{u}_2) \in \mathbb{O}$. Logo, $\mathbb{O}$ é uma álgebra com identidade.

(b) A aplicação $\iota : \mathbb{H} \to \mathbb{O}$, $\mathbf{u} \mapsto (\mathbf{u}, 0)$, é um homomorfismo injetor de $\mathbb{R}$-álgebras. A injetividade e a linearidade de ι é óbvia. Por outro lado, dados $\mathbf{u}, \mathbf{v} \in H$ temos $(\mathbf{u}, 0) \cdot (\mathbf{v}, 0) = (\mathbf{u} \cdot \mathbf{v} - \overline{0} \cdot 0, 0 \cdot \overline{\mathbf{v}} + 0 \cdot \mathbf{u}) = (\mathbf{u} \cdot \mathbf{v}, 0)$; logo, ι é realmente um homomorfismo injetor. Com isso, segue que existe uma cópia de $\mathbb{H}$ em $\mathbb{O}$ e, em particular, $\mathbb{O}$ não é uma $\mathbb{R}$-álgebra comutativa.

Utilizaremos as seguintes notações:

$$\mathbf{1} := (\mathbf{1}, 0), \quad \mathbf{i} := (\mathbf{i}, 0), \quad \mathbf{j} := (\mathbf{j}, 0), \quad \mathbf{k} := (\mathbf{k}, 0), \quad \text{e} \quad \mathbf{l} := (0, \mathbf{1})$$

Proposição 4.1.3. *O conjunto* $\mathcal{B} = \{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}, \mathbf{l}, \mathbf{il}, \mathbf{jl}, \mathbf{kl}\}$ *é uma base ordenada de* $\mathbb{O}$.

Prova. Segue da observação que $\mathcal{B}$ é imagem da base canônica de $\mathbb{R}^8$ pelo isomorfismo linear $\Psi : \mathbb{R}^8 \to \mathbb{O}$ dado por

$$\Psi(u_1, u_2, u_3, u_4, v_1, v_2, v_3, v_4) = (u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k}, v_1\mathbf{1} + v_2\mathbf{i} + v_3\mathbf{j} + v_4\mathbf{k})$$

□

Em virtude da proposição acima, cada elemento $\mathbf{w} \in \mathbb{O}$ pode ser escrito de forma única como

$$\mathbf{w} = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k} + w_5\mathbf{l} + w_6\mathbf{il} + w_7\mathbf{jl} + w_8\mathbf{kl} \tag{4.4}$$

onde $w_1, \ldots, w_8 \in \mathbb{R}$.

Observamos que

$$\mathbf{il} = (0, \mathbf{i}), \quad \mathbf{jl} = (0, \mathbf{j}) \quad \text{e} \quad \mathbf{kl} = (0, \mathbf{k}) \tag{4.5}$$

Assim como ocorre com os complexos e quatérnios, também podemos definir uma conjugação em $\mathbb{O}$.

Definição 4.1.4. Seja $\mathbf{w} = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k} + w_5\mathbf{l} + w_6\mathbf{il} + w_7\mathbf{jl} + w_8\mathbf{kl}$ um octônio. O *conjugado* de $\mathbf{w}$, denotado por $\overline{\mathbf{w}}$, é o octônio

$$\overline{\mathbf{w}} = w_1\mathbf{1} - w_2\mathbf{i} - w_3\mathbf{j} - w_4\mathbf{k} - w_5\mathbf{l} - w_6\mathbf{il} - w_7\mathbf{jl} - w_8\mathbf{kl}.$$

Notemos que $\mathbf{w} = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k} + w_5\mathbf{l} + w_6\mathbf{il} + w_7\mathbf{jl} + w_8\mathbf{kl}$ pode ser reescrito como

$$\mathbf{w} = (\mathbf{u}_1, \mathbf{u}_2)$$

onde

$$\mathbf{u}_1 = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k} \quad \text{e} \quad \mathbf{u}_2 = w_5\mathbf{1} + w_6\mathbf{i} + w_7\mathbf{j} + w_8\mathbf{k}$$

Assim,

$$\begin{aligned}
\overline{\mathbf{w}} &= w_1\mathbf{1} - w_2\mathbf{i} - w_3\mathbf{j} - w_4\mathbf{k} - w_5\mathbf{l} - w_6\mathbf{il} - w_7\mathbf{jl} - w_8\mathbf{kl} \\
&= (w_1\mathbf{1}, 0) - (w_2, 0) - (w_3\mathbf{j}, 0) - (w_4\mathbf{k}, 0) - (0, w_5\mathbf{1}) - (0, w_6\mathbf{i}) - (0, w_7\mathbf{j}) - (0, w_8\mathbf{k}) \\
&= (w_1 - w_2\mathbf{i} - w_3\mathbf{j} - w_4\mathbf{k}, -(w_5\mathbf{1} + w_6\mathbf{i} + w_7\mathbf{j} + w_8\mathbf{k}))
\end{aligned}$$

Logo, o conjugado de um octônio $\mathbf{w} = (\mathbf{u}_1, \mathbf{u}_2)$ pode ser escrito de forma compacta como

$$\overline{\mathbf{w}} = (\overline{\mathbf{u}}_1, -\mathbf{u}_2).$$

Proposição 4.1.5. *Sejam* $\mathbf{w} = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k} + w_5\mathbf{l} + w_6\mathbf{il} + w_7\mathbf{jl} + w_8\mathbf{kl}$, $\mathbf{w}' = w_1'\mathbf{1} + w_2'\mathbf{i} + w_3'\mathbf{j} + w_4'\mathbf{k} + w_5'\mathbf{l} + w_6'\mathbf{il} + w_7'\mathbf{jl} + w_8'\mathbf{kl}$ *octônios e* $\alpha \in \mathbb{R}$. *Então:*

(a) $\mathbf{w} \cdot \overline{\mathbf{w}} = \overline{\mathbf{w}} \cdot \mathbf{w} = (w_1^2 + w_2^2 + w_3^2 + w_4^2 + w_5^2 + w_6^2 + w_7^2 + w_8^2)\mathbf{1}$.

(b) $\overline{\overline{\mathbf{w}}} = \mathbf{w}$.

(c) $\overline{\mathbf{w} \cdot \mathbf{w}'} = \overline{\mathbf{w}'} \cdot \overline{\mathbf{w}}$.

(d) $\overline{\alpha\mathbf{w} + \mathbf{w}'} = \alpha\overline{\mathbf{w}} + \overline{\mathbf{w}'}$

Prova. Primeiro escrevemos $\mathbf{w} = (\mathbf{u}_1, \mathbf{u}_2)$ e $\mathbf{w}' = (\mathbf{u}'_1, \mathbf{u}'_2)$ como

$$\mathbf{u}_1 = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k}, \quad \mathbf{u}_2 = w_5\mathbf{1} + w_6\mathbf{i} + w_7\mathbf{j} + w_8\mathbf{k}$$

e

$$\mathbf{u}'_1 = w'_1\mathbf{1} + w'_2\mathbf{i} + w'_3\mathbf{j} + w'_4\mathbf{k}, \quad \mathbf{u}'_2 = w'_5\mathbf{1} + w'_6\mathbf{i} + w'_7\mathbf{j} + w'_8\mathbf{k}$$

temos:

(a) Segue das seguintes igualdades

$$\begin{aligned}
\mathbf{w} \cdot \overline{\mathbf{w}} &= (\mathbf{u}_1, \mathbf{u}_2) \cdot (\overline{\mathbf{u}}_1, -\mathbf{u}_2) \\
&= (\mathbf{u}_1 \cdot \overline{\mathbf{u}}_1 + \overline{\mathbf{u}}_2\mathbf{u}_2, \mathbf{u}_2\overline{\overline{\mathbf{u}}}_1 - \mathbf{u}_2\mathbf{u}_1) \\
&= ((w_1^2 + w_2^2 + w_3^2 + w_4^2 + w_5^2 + w_6^2 + w_7^2 + w_8^2)\mathbf{1}, \mathbf{u}_2\overline{\mathbf{u}}_1 - \mathbf{u}_2\mathbf{u}_1) \\
&= ((w_1^2 + w_2^2 + w_3^2 + w_4^2 + w_5^2 + w_6^2 + w_7^2 + w_8^2)\mathbf{1}, 0) \\
&= (w_1^2 + w_2^2 + w_3^2 + w_4^2 + w_5^2 + w_6^2 + w_7^2 + w_8^2)\mathbf{1}
\end{aligned}$$

(b) Para esse item temos

$$\overline{\overline{\mathbf{w}}} = \overline{(\overline{\mathbf{u}}_1, -\mathbf{u}_2)} = (\overline{\overline{\mathbf{u}}_1}, -(-\mathbf{u}_2)) = (\mathbf{u}_1, \mathbf{u}_2) = \mathbf{w}.$$

(c) Temos

$$\begin{aligned}
\overline{\mathbf{w} \cdot \mathbf{w}'} &= \overline{(\mathbf{u}_1\mathbf{u}'_1 - \overline{\mathbf{u}'}_2\mathbf{u}_2, \mathbf{u}_2\overline{\mathbf{u}'}_1 + \mathbf{u}'_2\mathbf{u}_1)} \\
&= (\overline{\mathbf{u}_1\mathbf{u}'_1 - \overline{\mathbf{u}'}_2\mathbf{u}_2}, -(\mathbf{u}_2\overline{\mathbf{u}'}_1 + \mathbf{u}'_2\mathbf{u}_1)) \\
&= (\overline{\mathbf{u}_1\mathbf{u}'_1} - \overline{\overline{\mathbf{u}'}_2\mathbf{u}_2}, -\mathbf{u}_2\overline{\mathbf{u}'}_1 - \mathbf{u}'_2\mathbf{u}_1) \\
&= (\overline{\mathbf{u}'_1} \cdot \overline{\mathbf{u}_1} - \overline{\mathbf{u}_2} \cdot \mathbf{u}'_2, -\mathbf{u}_2\overline{\mathbf{u}'}_1 - \mathbf{u}'_2\mathbf{u}_1) \\
&= \overline{\mathbf{w}'} \cdot \overline{\mathbf{w}}.
\end{aligned}$$

(d) Finalmente, para esse item temos:

$$\begin{aligned}
\overline{\alpha\mathbf{w} + \mathbf{w}'} &= \overline{(\alpha\mathbf{u}_1 + \mathbf{u}'_1, \alpha\mathbf{u}_2 + \mathbf{u}'_2)} \\
&= (\overline{\alpha\mathbf{u}_1 + \mathbf{u}'_1}, -(\alpha\mathbf{u}_2 + \mathbf{u}'_2)) \\
&= (\alpha\overline{\mathbf{u}_1} + \mathbf{u}'_1, -\alpha\mathbf{u}_2 - \mathbf{u}'_2) \\
&= \alpha\overline{\mathbf{w}} + \overline{\mathbf{w}'}
\end{aligned}$$

A exemplo de $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ também temos que $\mathbb{O}$ é uma álgebra de divisão

Proposição 4.1.6. *Todo elemento não nulo de $\mathbb{O}$ tem inverso multiplicativo.*

Prova. Seja $\mathbf{w} = w_1\mathbf{1} + w_2\mathbf{i} + w_3\mathbf{j} + w_4\mathbf{k} + w_5\mathbf{l} + w_6\mathbf{il} + w_7\mathbf{jl} + w_8\mathbf{kl} \in \mathbb{O} \setminus \{0\}$. Pela Proposição 4.1.5(a) temos

$$\mathbf{w} \cdot \overline{\mathbf{w}} = \overline{\mathbf{w}} \cdot \mathbf{w} = (w_1^2 + \cdots + w_8^2)\mathbf{1}. \tag{4.6}$$

Como $\mathbf{w} \neq 0$, então $w_1^2 + \cdots + w_8^2 \neq 0$. Desse modo, multiplicando a igualdade (4.6) por $(w_1^2 + \cdots + w_8^2)^{-1}$ vem

$$\mathbf{w} \cdot \frac{\overline{\mathbf{w}}}{w_1^2 + \cdots + w_8^2} = \frac{\overline{\mathbf{w}}}{w_1^2 + \cdots + w_8^2} \cdot \mathbf{w} = \mathbf{1} \tag{4.7}$$

Portanto, $\mathbf{w}$ é invertível. □

4.2 A álgebra dos octônios é alternante

Para os octônios $\mathbf{w}_1 = \mathbf{l}, \mathbf{w}_2 = \mathbf{il}$ e $\mathbf{w}_3 = \mathbf{jl}$ temos

$$\mathbf{w}_1 \cdot (\mathbf{w}_2 \cdot \mathbf{w}_3) = \mathbf{kl} \quad \text{e} \quad (\mathbf{w}_1 \cdot \mathbf{w}_2) \cdot \mathbf{w}_3 = -\mathbf{kl}. \tag{4.8}$$

Com estas igualdades observamos que a álgebra dos octônios, além de não comutativa, é não associativa.

A noção a seguir é um enfraquecimento da propriedade associativa.

Definição 4.2.1. Uma $\mathbb{R}$-álgebra $\mathcal{A}$ é *alternante* se para cada $\mathbf{x}, \mathbf{y} \in \mathcal{A}$,

$$\mathbf{x} \cdot (\mathbf{x} \cdot \mathbf{y}) = \mathbf{x}^2 \cdot \mathbf{y} \quad \text{e} \quad (\mathbf{x} \cdot \mathbf{y}) \cdot \mathbf{y} = \mathbf{x} \cdot \mathbf{y}^2. \tag{4.9}$$

Naturalmente, toda álgebra associativa é alternante.

O produto interno euclidiano em $\mathbb{R}^8$ induz um produto interno em $\mathbb{O}$ dado pela seguinte igualdade:

$$\langle (\mathbf{u}_1, \mathbf{u}_2), (\mathbf{v}_1, \mathbf{v}_2) \rangle := \langle \mathbf{u}_1, \mathbf{v}_1 \rangle + \langle \mathbf{u}_2, \mathbf{v}_2 \rangle$$

para quaisquer $(\mathbf{u}_1, \mathbf{u}_2), (\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{O}$.

Dado um quatérnio $\mathbf{u} = u_1\mathbf{1} + u_2\mathbf{i} + u_3\mathbf{j} + u_4\mathbf{k} \in \mathbb{H}$, definimos a *parte real* de $\mathbf{u}$ como sendo o número real $\mathrm{Re}(\mathbf{u}) = u_1$. Cálculos diretos nos dão:

$$\mathbf{u}^2 = 2\mathrm{Re}(\mathbf{u})\mathbf{u} - \langle \mathbf{u}, \mathbf{u}\rangle \mathbf{1} \quad \text{e} \quad 2\mathrm{Re}(\mathbf{u}) = \overline{\mathbf{u}} + \mathbf{u} \tag{4.10}$$

Para cada $\mathbf{w} = (\mathbf{u}_1, \mathbf{u}_2) \in \mathbb{O}$ definimos

$$\lambda(\mathbf{w}) = \mathrm{Re}(\mathbf{u}_1)$$

Notemos que se $\mathbf{w} = (\mathbf{u}_1, \mathbf{u}_2) \in \mathbb{O}$ então

$$\begin{aligned} \mathbf{w}^2 &= (\mathbf{u}_1^2 - \overline{\mathbf{u}_2}\mathbf{u}_2, \mathbf{u}_2(\overline{\mathbf{u}}_1 + \mathbf{u}_1)) \\ &= (2\mathrm{Re}(\mathbf{u}_1)\mathbf{u}_1 - \langle \mathbf{u}_1, \mathbf{u}_1\rangle \mathbf{1} - \langle \mathbf{u}_2, \mathbf{u}_2\rangle \mathbf{1}, 2\mathrm{Re}(\mathbf{u}_1)\mathbf{u}_2) \\ &= 2\mathrm{Re}(\mathbf{u}_1)(\mathbf{u}_1, \mathbf{u}_2) - ((\langle \mathbf{u}_1, \mathbf{u}_1\rangle + \langle \mathbf{u}_2, \mathbf{u}_2\rangle)\mathbf{1}, 0) \end{aligned}$$

Logo,

$$\mathbf{w}^2 = 2\lambda(\mathbf{w})\mathbf{w} - \langle \mathbf{w}, \mathbf{w}\rangle \mathbf{1}. \tag{4.11}$$

Outra identidade útil e facilmente verificada é

$$\mathbf{w} = 2\lambda(\mathbf{w})\mathbf{1} - \overline{\mathbf{w}} \tag{4.12}$$

Proposição 4.2.2. *Se* $\mathbf{w} = (\mathbf{u}_1, \mathbf{u}_2),\ \mathbf{w}' = (\mathbf{v}_1, \mathbf{v}_2)$ *são octônios então*

$$\mathbf{w} \cdot (\overline{\mathbf{w}}\mathbf{w}') = \langle \mathbf{w}, \mathbf{w}\rangle \mathbf{w}' = (\mathbf{w}\overline{\mathbf{w}}) \cdot \mathbf{w}'$$

Prova. A segunda igualdade segue diretamente da Proposição 4.1.5 (a). Assim, nos ocuparemos em demonstrar apenas a primeira igualdade.

Temos

$$\begin{aligned} \overline{\mathbf{w}}\mathbf{w}' &= (\overline{\mathbf{u}}_1, -\mathbf{u}_2) \cdot (\mathbf{v}_1, \mathbf{v}_2) \\ &= (\overline{\mathbf{u}}_1\mathbf{v}_1 + \overline{\mathbf{v}}_2\mathbf{u}_2, -\mathbf{u}_2\overline{\mathbf{v}}_1 + \mathbf{v}_2\overline{\mathbf{u}}_1). \end{aligned}$$

Como H é associativa,

$$\begin{aligned}
\mathbf{w}(\overline{\mathbf{w}}\mathbf{w}') &= (\mathbf{u}_1[\overline{\mathbf{u}}_1\mathbf{v}_1 + \overline{\mathbf{v}}_2\mathbf{u}_2] - [-\mathbf{v}_1\overline{\mathbf{u}}_2 + \mathbf{u}_1\overline{\mathbf{v}}_2]\mathbf{u}_2, \mathbf{u}_2[\overline{\mathbf{v}}_1\mathbf{u}_1 + \overline{\mathbf{u}}_2\mathbf{v}_2] + [-\mathbf{u}_2\overline{\mathbf{v}}_1 + \mathbf{v}_2\overline{\mathbf{u}}_1]\mathbf{u}_1) \\
&= (\mathbf{u}_1\overline{\mathbf{u}}_1\mathbf{v}_1 + \mathbf{v}_1\overline{\mathbf{u}}_2\mathbf{u}_2, \mathbf{u}_2\overline{\mathbf{u}}_2\mathbf{v}_2 + \mathbf{v}_2\overline{\mathbf{u}}_1\mathbf{u}_1) \\
&= ((\langle \mathbf{u}_1, \mathbf{u}_1\rangle + \langle \mathbf{u}_2, \mathbf{u}_2\rangle)\mathbf{v}_1, (\langle \mathbf{u}_1, \mathbf{u}_1\rangle + \langle \mathbf{u}_2, \mathbf{u}_2\rangle)\mathbf{v}_2) \qquad (4.13) \\
&= \langle \mathbf{w}, \mathbf{w}\rangle(\mathbf{v}_1, \mathbf{v}_2) \\
&= \langle \mathbf{w}, \mathbf{w}\rangle\mathbf{w}'. \qquad (4.14)
\end{aligned}$$

□

Teorema 4.2.3. *A álgebra dos octônios é alternante.*

Prova. Sejam $\mathbf{x}, \mathbf{y} \in \mathbb{O}$. Por (4.12) e (4.11) temos

$$\overline{\mathbf{x}} = 2\lambda(\mathbf{x})\mathbf{1} - \mathbf{x} \quad \text{e} \quad \langle \mathbf{x}, \mathbf{x}\rangle\mathbf{1} = 2\lambda(\mathbf{x})\mathbf{x} - \mathbf{x}^2$$

Dessas igualdades e da Proposição 4.2.2 vem

$$\mathbf{x}(2\lambda(\mathbf{x})\mathbf{y} - \mathbf{x}\mathbf{y}) = (2\lambda(\mathbf{x})\mathbf{x} - \mathbf{x}^2)\mathbf{y} \qquad (4.15)$$

Desenvolvendo os dois lados dessa igualdade e efetuando cancelamentos obtemos

$$\mathbf{x}(\mathbf{x}\mathbf{y}) = \mathbf{x}^2\mathbf{y} \qquad (4.16)$$

Aplicando conjugação nos dois lados desse igualdade obtemos:

$$(\overline{\mathbf{y}} \cdot \overline{\mathbf{x}})\overline{\mathbf{x}} = \overline{\mathbf{y}} \cdot \overline{\mathbf{x}}^2 \qquad (4.17)$$

Como essa igualdade é verdadeira para qualquer $\mathbf{x}, \mathbf{y} \in \mathbb{O}$ também temos

$$(\mathbf{y}\mathbf{x})\mathbf{x} = \mathbf{y}\mathbf{x}^2 \qquad (4.18)$$

Portanto, de (4.16) e (4.18) segue a conclusão desejada. □

4.3 A álgebra dos octônios é de composição

Dados $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{O}$, segue de (4.11) que

$$(\mathbf{w}_1 + \mathbf{w}_2)^2 = 2\lambda(\mathbf{w}_1 + \mathbf{w}_2)(\mathbf{w}_1 + \mathbf{w}_2) - \langle \mathbf{w}_1 + \mathbf{w}_2, \mathbf{w}_1 + \mathbf{w}_2 \rangle \mathbf{1}$$

Desenvolvendo os dois lados dessa igualdade e efetuando cancelamentos obtemos

$$\mathbf{w}_1\mathbf{w}_2 + \mathbf{w}_2\mathbf{w}_1 = 2\lambda(\mathbf{w}_1)\mathbf{w}_2 + 2\lambda(\mathbf{w}_2)\mathbf{w}_1 - 2\langle \mathbf{w}_1, \mathbf{w}_2 \rangle \mathbf{1} \tag{4.19}$$

Aplicando λ em ambos os lados dessa igualdade vem:

$$\lambda(\mathbf{w}_1\mathbf{w}_2 + \mathbf{w}_2\mathbf{w}_1) = 4\lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) - 2\langle \mathbf{w}_1, \mathbf{w}_2 \rangle \tag{4.20}$$

Finalmente, dessa expressão obtemos

$$\langle \mathbf{w}_1, \mathbf{w}_2 \rangle = 2\lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) - \frac{1}{2}\lambda(\mathbf{w}_1\mathbf{w}_2 + \mathbf{w}_2\mathbf{w}_1) \tag{4.21}$$

Lema 4.3.1. *Sejam* $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3 \in \mathbb{O}$. *Então:*

(a) *Se* $\lambda(\mathbf{w}_1) = \lambda(\mathbf{w}_2) = 0$ *então* $\langle \mathbf{w}_1, \mathbf{w}_2\mathbf{w}_1 \rangle = 0$ *e* $\lambda(\mathbf{w}_1\mathbf{w}_2) = \lambda(\mathbf{w}_2\mathbf{w}_1)$.

(b) *Se* $\lambda(\mathbf{w}_1) = \lambda(\mathbf{w}_2) = \lambda(\mathbf{w}_3) = 0$ *então* $\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3 \rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2 \rangle = 0$.

Prova. (a) Por (4.19) temos

$$\mathbf{w}_1(\mathbf{w}_2\mathbf{w}_1) + (\mathbf{w}_2\mathbf{w}_1)\mathbf{w}_1 = 2\lambda(\mathbf{w}_1)\mathbf{w}_2\mathbf{w}_1 + 2\lambda(\mathbf{w}_2\mathbf{w}_1)\mathbf{w}_1 - 2(\mathbf{w}_1, \mathbf{w}_2\mathbf{w}_1)\mathbf{1}$$

e

$$(\mathbf{w}_1\mathbf{w}_2)\mathbf{w}_1 + (\mathbf{w}_2\mathbf{w}_1)\mathbf{w}_1 = -2\langle \mathbf{w}_1, \mathbf{w}_2 \rangle \mathbf{w}_1 \tag{4.22}$$

Subtraindo essas equações membro a membro e usando o fato que $\mathbb{O}$ é álgebra alternante obtemos:

$$0 = 2(\lambda(\mathbf{w}_2\mathbf{w}_1) + \langle \mathbf{w}_1, \mathbf{w}_2 \rangle)\mathbf{w}_1 - 2(\mathbf{w}_1, \mathbf{w}_2\mathbf{w}_1)\mathbf{1} \tag{4.23}$$

Assim, $(\mathbf{w}_1, \mathbf{w}_2\mathbf{w}_1) = 0$ e $\lambda(\mathbf{w}_2\mathbf{w}_1) + \langle \mathbf{w}_1, \mathbf{w}_2 \rangle = 0$. Dessas igualdades temos as conclusões desejadas.

(b) Temos $\lambda(\mathbf{w}_2 + \mathbf{w}_3) = \lambda(\mathbf{w}_1) = 0$. Assim, pelo item anterior

$$\langle \mathbf{w}_1(\mathbf{w}_2 + \mathbf{w}_3), \mathbf{w}_2 + \mathbf{w}_3 \rangle = 0;$$

logo,

$$\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_2\rangle + \langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_3\rangle = 0.$$

Mas $\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_2\rangle = \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_3\rangle = 0$, também pelo item anterior. Assim,

$$\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle = 0$$

como desejávamos. □

Proposição 4.3.2. *Sejam* $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3 \in \mathbb{O}$. *Então:*

(a) $\langle \mathbf{w}_1, \mathbf{w}_2\rangle = 2\lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) - \lambda(\mathbf{w}_1\mathbf{w}_2)$

(b) $\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle = 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle$

Prova. Escrevamos $\mathbf{w}_1 = \lambda(\mathbf{w}_1)\mathbf{1} + \mathbf{w}_1'$, $\mathbf{w}_2 = \lambda(\mathbf{w}_2)\mathbf{1} + \mathbf{w}_2'$ e $\mathbf{w}_3 = \lambda(\mathbf{w}_3)\mathbf{1} + \mathbf{w}_3'$.

(a) Temos

$$\begin{aligned}
\lambda(\mathbf{w}_1\mathbf{w}_2) &= \lambda(\lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2)\mathbf{1} + \lambda(\mathbf{w}_1)\mathbf{w}_2 + \lambda(\mathbf{w}_2)\mathbf{w}_1 + \mathbf{w}_1'\mathbf{w}_2') \\
&= \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) + \lambda(\mathbf{w}_1'\mathbf{w}_2') \\
&= \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2) + \lambda(\mathbf{w}_2'\mathbf{w}_1') \\
&= \lambda(\mathbf{w}_2\mathbf{w}_1)
\end{aligned}$$

onde da segunda igualdade para a terceira utilizamos o Lema 4.3.1 (a). Assim, como $\lambda(\mathbf{w}_1\mathbf{w}_2) = \lambda(\mathbf{w}_2\mathbf{w}_1)$, segue de (4.21) a igualdade desejada.

(b) Temos,

$$\begin{aligned}
\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle &= \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3) + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2)\langle \mathbf{1}, \mathbf{w}_3'\rangle + \\
&\quad + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_3)\langle \mathbf{w}_2', \mathbf{1}\rangle + \lambda(\mathbf{w}_1)\langle \mathbf{w}_2', \mathbf{w}_3'\rangle + \\
&\quad + \lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3)\langle \mathbf{w}_1', \mathbf{1}\rangle + \lambda(\mathbf{w}_2)\langle \mathbf{w}_1', \mathbf{w}_3'\rangle + \\
&\quad + \lambda(\mathbf{w}_3)\langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{1}\rangle + \langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{w}_3'\rangle \qquad (4.24)
\end{aligned}$$

e

$$\begin{aligned}\langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle &= \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3) + \lambda(\mathbf{w}_1)\lambda(\mathbf{w}_3)\langle \mathbf{1}, \mathbf{w}_2'\rangle + \\ &+\lambda(\mathbf{w}_1)\lambda(\mathbf{w}_2)\langle \mathbf{w}_3', \mathbf{1}\rangle + \lambda(\mathbf{w}_1)\langle \mathbf{w}_3', \mathbf{w}_2'\rangle + \\ &+\lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3)\langle \mathbf{w}_1', \mathbf{1}\rangle + \lambda(\mathbf{w}_3)\langle \mathbf{w}_1', \mathbf{w}_2'\rangle + \\ &+\lambda(\mathbf{w}_2)\langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{1}\rangle + \langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{w}_2'\rangle \end{aligned} \tag{4.25}$$

Mas $\langle \mathbf{1}, \mathbf{w}_3'\rangle = \langle \mathbf{w}_1', \mathbf{1}\rangle = \langle \mathbf{w}_2', \mathbf{1}\rangle = 0$. Logo,

$$\begin{aligned}\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle &= \lambda(\mathbf{w}_1)[\lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3) + \langle \mathbf{w}_2', \mathbf{w}_3'\rangle] + \lambda(\mathbf{w}_2)\langle \mathbf{w}_1', \mathbf{w}_3'\rangle + \\ &+\lambda(\mathbf{w}_3)\langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{1}\rangle + \langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{w}_3'\rangle\end{aligned}$$

e

$$\begin{aligned}\langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle &= \lambda(\mathbf{w}_1)[\lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3) + \langle \mathbf{w}_3', \mathbf{w}_2'\rangle] + \lambda(\mathbf{w}_3)\langle \mathbf{w}_1', \mathbf{w}_2'\rangle + \\ &+\lambda(\mathbf{w}_2)\langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{1}\rangle + \langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{w}_2'\rangle\end{aligned}$$

Como $\langle \mathbf{w}_2, \mathbf{w}_3\rangle = \lambda(\mathbf{w}_2)\lambda(\mathbf{w}_3) + \langle \mathbf{w}_3', \mathbf{w}_2'\rangle$ então

$$\begin{aligned}\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle &= \lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle + \lambda(\mathbf{w}_2)\langle \mathbf{w}_1', \mathbf{w}_3'\rangle + \lambda(\mathbf{w}_3)\langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{1}\rangle + \langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{w}_3'\rangle \\ &= \lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle - \lambda(\mathbf{w}_2)\lambda(\mathbf{w}_1'\mathbf{w}_3') + \lambda(\mathbf{w}_3)\lambda(\mathbf{w}_1'\mathbf{w}_2') + \langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{w}_3'\rangle\end{aligned}$$

e

$$\begin{aligned}\langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle &= \lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle + \lambda(\mathbf{w}_3)\langle \mathbf{w}_1', \mathbf{w}_2'\rangle + \lambda(\mathbf{w}_2)\langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{1}\rangle + \langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{w}_2'\rangle \\ &= \lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle - \lambda(\mathbf{w}_3)\lambda(\mathbf{w}_1'\mathbf{w}_2') + \lambda(\mathbf{w}_2)\lambda(\mathbf{w}_1'\mathbf{w}_3') + \langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{w}_2'\rangle\end{aligned}$$

Dessa maneira

$$\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle = 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle + \langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{w}_3'\rangle + \langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{w}_2'\rangle$$

Mas pelo Lema 4.3.1 (b), $\langle \mathbf{w}_1'\mathbf{w}_2', \mathbf{w}_3'\rangle + \langle \mathbf{w}_1'\mathbf{w}_3', \mathbf{w}_2'\rangle = 0$. Logo,

$$\langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_3\rangle + \langle \mathbf{w}_1\mathbf{w}_3, \mathbf{w}_2\rangle = 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_3\rangle$$

como desejado. □

Teorema 4.3.3. *A álgebra dos octônios é de composição. Em particular, $\mathbb{O}$ é uma álgebra de divisão.*

Prova. Sejam $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{O}$. Por 4.3.2 (b) temos

$$\langle \mathbf{w}_1(\mathbf{w}_1\mathbf{w}_2), \mathbf{w}_2\rangle + \langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_1\mathbf{w}_2\rangle = 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2.\mathbf{w}_1\mathbf{w}_2\rangle.$$

Equivalentemente,

$$\begin{aligned} \langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_1\mathbf{w}_2\rangle &= 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_1\mathbf{w}_2\rangle - \langle \mathbf{w}_1 \cdot (\mathbf{w}_1\mathbf{w}_2), \mathbf{w}_2\rangle \\ &= 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_1\mathbf{w}_2\rangle - \langle \mathbf{w}_1^2\mathbf{w}_2, \mathbf{w}_2\rangle \end{aligned} \tag{4.26}$$

Por (4.11), $\mathbf{w}_1^2 = 2\lambda(\mathbf{w}_1)\mathbf{w}_1 - \langle \mathbf{w}_1, \mathbf{w}_1\rangle\mathbf{1}$. Assim,

$$\begin{aligned} \langle \mathbf{w}_1\mathbf{w}_2, \mathbf{w}_1\mathbf{w}_2\rangle &= 2\lambda(\mathbf{w}_1)\langle \mathbf{w}_2, \mathbf{w}_1\mathbf{w}_2\rangle - \langle (2\lambda(\mathbf{w}_1)\mathbf{w}_1 - \langle \mathbf{w}_1, \mathbf{w}_1\rangle\mathbf{1})\mathbf{w}_2, \mathbf{w}_2\rangle \\ &= \langle \mathbf{w}_1, \mathbf{w}_1\rangle\langle \mathbf{w}_2, \mathbf{w}_2\rangle. \end{aligned} \tag{4.27}$$

Logo,

$$\| \mathbf{w}_1 \cdot \mathbf{w}_2 \|^2 = \| \mathbf{w}_1 \|^2 \cdot \| \mathbf{w}_2 \|^2$$

Portanto,

$$\| \mathbf{w}_1 \cdot \mathbf{w}_2 \| = \| \mathbf{w}_1 \| \cdot \| \mathbf{w}_2 \|$$

e isso conclui a demonstração. □

Bibliografia

[1] EBBINGHAUS, H. D.; HERMES, H.; HIRZEBRUCH, F.; KOECHER, M.; MAINZER, K.; NEUKIRCH, J.; PRESTEL, A.; REMMERT,R., *Numbers*, Graduate Texts in Mathematics, Springer, 1991.

[2] CARMO, Manfredo Perdigão do, *Geometria Riemanniana*, 2a Edição, 1988.

[3] CURTIS, Charles W., *Linear algebra: an introductory approach*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1984.

[4] MUNKRES, James R., *Topology*, 2nd Edition, Pearson, 2000.