RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

TEOREMA DE HOPF SOBRE ÁLGEBRAS DE DIVISÃO REAIS

HOPF THEOREM ABOUT REAL DIVISION ALGEBRAS

TEOREMA DE HOPF SOBRE ÁLGEBRAS DE DIVISIÓN REALES

Lia Nojosa Sena[1], Rubens Cainan Saboia Monteiro[1]

e473446
https://doi.org/10.47820/recima21.v4i7.3446
PUBLICADO: 07/2023

RESUMO
O presente artigo tem como objetivo apresentar uma demonstração para um importante resultado apresentado pelo matemático Hopf, em 1940, no qual é determinada a dimensão de uma álgebra de divisão sobre os reais.

PALAVRAS-CHAVE: Álgebras reais. Álgebras não associativas. Álgebras de divisão.

ABSTRACT
This article aims to present a demonstration for an important result presented by the mathematician Hopf, em 1940, in which the dimension of a division algebra over reals is determined.

KEYWORDS: *Real algebras. Non-associative algebras. Division algebras.*

RESUMEN
Este artículo tiene como objetivo una demonstración de un importante resultado presentado por el matemático Hopf, em 1940, en el que se determina la dimensión de un álgebra de división sobre reales.

PALABRAS CLAVE: *Álgebra reales. Álgebras no asociativas. Álgebras de división.*

INTRODUÇÃO

O presente artigo tem como objetivo apresentar uma demonstração para um importante resultado apresentado pelo matemático Hopf, em 1940, no qual é determinada a dimensão de uma álgebra de divisão sobre os reais. Seguindo Hopf, provaremos um teorema sobre aplicações ímpares de esferas, do qual o teorema sobre álgebras de divisão seguirá como corolário.

O matemático Gauss, em 1831, estava convencido que uma extensão dos números complexos que preservasse as propriedades básicas de um corpo era impossível, o que foi chamado de "sistema de números hipercomplexos".

No ano de 1843, o matemático Hamilton descobriu os números quatérnios, e pouco tempo depois, os matemáticos Graves e Cayley construíram os números octônios. Esses números hipercomplexos não são corpos – no caso dos quatérnios a lei da comutatividade é perdida e no caso dos octônios a lei da associatividade é abandonada – mas todo elemento não nulo possui inverso. A propriedade de divisão (esta propriedade dos números racionais foi considerada indispensável pelos criadores da teoria) pode ser realizada e sem ambiguidade.

Atualmente o sistema de números hipercomplexos são chamados de álgebras reais. Se a divisão pode ser realizada de forma inequívoca, chamaremos de álgebras de divisão.

[1] Mestre em Matemática pela Universidade Federal do Ceará.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Em 1867, o matemático Hankel publicou uma demonstração de que nenhum sistema de números hipercomplexos satisfaz todas as propriedades básicas de um corpo. Entretanto, em 1877, o matemático Frobenius conseguiu uma resposta mais concreta ao provar que as únicas álgebras de divisão (associativas) sobre os reais (a menos de isomorfismos) são o corpo dos números reais, o corpo dos números complexos e a álgebra dos quatérnios.

O problema para a álgebra não associativa (= associativas ou não) sobre os reais ainda perdurou, sendo estudado por um bom tempo. Hopf demonstrou, em 1940, que a dimensão de uma álgebra de divisão sobre os reais é uma potência de 2. Já a classificação final, feita em 1957 pelos matemáticos Bott, Milnor e Kervaire, mostrou que as álgebras de divisão sobre os reais são isomorfas a algumas das seguintes álgebras: ao corpo dos números reais, ao corpo dos números complexos, à álgebra dos quatérnios ou à álgebra dos octônios.

1 REFERENCIAL TEÓRICO

Nesta seção apresentaremos conceitos fundamentais para o entendimento e demonstração do Teorema de Hopf sobre álgebras de divisão reais.

Definição 1.1. Seja V um espaço vetorial sobre $\mathbb{R}$. Este espaço é chamado álgebra sobre $\mathbb{R}$ (ou $\mathbb{R}$-álgebra ou ainda álgebra real) se for possível definir sobre V uma operação binária que chamaremos de multiplicação,

$$V \times V \to V;$$

$$(x, y) \mapsto xy,$$

satisfazendo as duas leis distributivas:

$$(\alpha x + \beta y)z = \alpha(xz) + \beta(\alpha y);$$

$$x(\alpha y + \beta z) = \alpha(xy) + \beta(yz),$$

com $\alpha, \beta \in \mathbb{R}$ e $x,\ y,\ z \in V$. Em outras palavras, se a multiplicação for bilinear.

Em particular, as relações

$$\alpha(xy) = (\alpha x)y = x(\alpha y)$$

sempre serão válidas.

Se vale a lei associativa $x(yz) = (xy)z$, com $x,\ y,\ z \in V$, então a álgebra é chamada associativa. Se vale a lei comutativa $xy = yx$, com $x,\ y \in V$, então a álgebra é dita comutativa. Em geral, as $\mathbb{R}$-álgebras não são comutativas e nem associativas.

Um elemento $1 \in V$ é chamado de elemento identidade (ou elemento unidade) se $1x = x1 = x,\ \forall x \in V$. Quando V possui um elemento identidade, ela é chamada álgebra com identidade. Se a unidade $1 = 0$, então $x = 1x = 0x,\ \forall x \in V$, ou seja, $V = 0$.

Para distinguir álgebras definidas a partir do espaço vetorial V, o símbolo da multiplicação é muitas vezes indicado de modo explícito como parte da notação, de modo que escrevemos $\mathcal{A} := (V,\ .)$. A dimensão da álgebra $\mathcal{A}$ sobre $\mathbb{R}$, denotada por $dim\,\mathcal{A}$, é a dimensão do espaço vetorial V sobre $\mathbb{R}$, isto é, $dim\,\mathcal{A} = dim\,V$.

Definição 1.2. Uma álgebra $\mathcal{A} \neq 0$ sobre $\mathbb{R}$ é dita uma álgebra de divisão, se para quaisquer $a, b \in V$, com $a \neq 0$ as duas equações

$$ax = b,$$

$$ya = b$$

têm soluções únicas em $\mathcal{A}$. No caso em que a álgebra $\mathcal{A}$ é associativa, a condição para ser álgebra de divisão é que todo $a \neq 0$ tem inverso (único).

Definição 1.3. Um elemento x de uma álgebra $\mathcal{A}$ é dito divisor de zero em $\mathcal{A}$ se existe um elemento $y \neq 0$ em $\mathcal{A}$ tal que $xy = 0$ ou $yx = 0$. Uma álgebra $\mathcal{A}$ é chamada sem divisores de zero se esta não contém divisores de zero. Nesta, a equação é $xy = 0$, se, e somente, $x = 0$ ou $y = 0$.

Definição 1.4. Se $\mathcal{A} = (V,\ .)$ e $\mathcal{B} = (W,\ .)$ são duas álgebras quaisquer, uma função $\mathbb{R}$-linear bijetora $f: V \rightarrow W$ é dita um isomorfismo de $\mathbb{R}$-álgebras, se

$$f(xy) = f(x)f(y),$$

quaisquer que sejam $x, y \in V$.

Teorema 1.5. Seja $\mathcal{A}$ uma $\mathbb{R}$-álgebra de dimensão finita n, então as seguintes afirmações são equivalentes:

i. $\mathcal{A}$ é uma álgebra de divisão;
ii. $\mathcal{A}$ não possui divisores de zero.

Prova:

i) $\Rightarrow$ ii)

Seja $\mathcal{A}$ uma álgebra de divisão. Sejam $a, b \in \mathcal{A}$ e $a \neq 0$, então

$$ax = b \text{ e } ya = b$$

possuem únicas soluções. Suponha que $ab = 0$. Como $a \neq 0$, então $b = 0$, pois 0 é solução de

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$ax = 0$ e essas soluções são únicas por hipótese. Portanto, $\mathcal{A}$ não possui divisores de zero.

ii) ⇒ *i*)

Queremos mostrar que a equação

$$ax = b, \qquad (1.1.)$$

com $a \neq 0$, possui solução.

Seja

$$e_1, e_2, \ldots, e_n$$

uma base do espaço vetorial $\mathcal{A}$. Multiplicando cada elemento da base à esquerda por a, teremos:

$$ae_1, ae_2, \ldots, ae_n. \qquad (1.2.)$$

Provaremos que os vetores acima formam outra base de $\mathcal{A}$. Suponha que os vetores (1.2.) não são linearmente independentes, então existem $k_1, \ldots, k_n \in \mathbb{R}$ que não são todos nulos tais que

$$k_1ae_1 + k_2ae_2 + \cdots + k_nae_n = 0.$$

Assim,

$$ak_1e_1 + ak_2e_2 + \cdots + ak_ne_n =$$

$$a(k_1e_1 + k_2e_2 + \cdots + k_ne_n) = 0.$$

Como $a \neq 0$ e por hipótese $\mathcal{A}$ não possui divisores de zero, então

$$k_1e_1 + k_2e_2 + \cdots + k_ne_n = 0,$$

contradizendo o fato de que $e_1, e_2, \ldots, e_n$ formam uma base de $\mathcal{A}$. Assim, os valores de (1.2.) são linearmente independentes e, portanto, uma base de $\mathcal{A}$. Agora, escreva b como combinação dos elementos da nova base, ou seja,

$$j_1ae_1 + j_2ae_2 + \cdots + j_nae_n = b,$$

onde $j_1, \ldots, j_n \in \mathbb{R}$. Logo,

$$a(j_1e_1 + \cdots + j_ne_n) = b,$$

o que implica em $j_1e_1 + \cdots + j_ne_n$ ser uma solução de (1.1.). Agora mostraremos que essa solução é única.

Seja x' outra solução de (1.1.), ou seja, $ax' = b$. Logo,

$$ax = ax' \Rightarrow ax - ax' = 0$$

$$\Rightarrow a(x - x') = 0.$$

Como $\mathcal{A}$ não possui divisores de zero e $a \neq 0$, temos que

$$x - x' = 0 \Rightarrow x = x'.$$

Agora vamos mostrar que a equação

$$ya = b, \qquad (1.3.)$$

com $a \neq 0$, possui solução.

Novamente, seja

$$e_1, e_2, \dots, e_n$$

uma base do espaço vetorial $\mathcal{A}$. Multiplicando cada elemento da base à direita por a, teremos:

$$e_1 a, e_2 a, \dots, e_n a. \qquad (1.4.)$$

Provaremos que os vetores acima formam outra base de $\mathcal{A}$.

Suponha que os vetores de (1.4.) não são linearmente independentes, então existem $l_1, \dots, l_n \in \mathbb{R}$ que não são todos nulos tais que:

$$l_1 e_1 a + l_2 e_2 a + \cdots + l_n e_n a = 0.$$

Assim,

$$(l_1 e_1 + l_2 e_2 + \cdots + l_n e_n)a = 0.$$

Como $a \neq 0$ e, por hipótese, $\mathcal{A}$ não possui divisores de zero, então

$$l_1 e_1 + l_2 e_2 + \cdots + l_n e_n = 0,$$

contradizendo o fato de que $e_1, e_2, \dots, e_n$ são uma base de $\mathcal{A}$. Assim, os valores de (1.4.) são linearmente independentes e, portanto, uma base de $\mathcal{A}$. Agora, podemos escrever b como uma combinação dos elementos da nova base, isto é,

$$m_1 e_1 a + m_2 e_2 a + \cdots + m_n e_n a = b,$$

onde $m_1, m_2, \cdots, m_n \in \mathbb{R}$. Logo,

$$(m_1 e_1 + m_2 e_2 + \cdots + m_n e_n)a = b,$$

o que implica em $m_1 e_1 + m_2 e_2 + \cdots + m_n e_n$ ser uma outra solução de (1.3.). Agora, mostraremos

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

que essa solução é única.

Seja y' outra solução de (1.3.), ou seja, $y'a = b$. Logo,

$$ya = y'a \Rightarrow ya - y'a = 0$$
$$\Rightarrow (y - y')a = 0.$$

Como $\mathcal{A}$ não possui divisores de zero e $a \neq 0$, temos que:

$$y - y' = 0 \Rightarrow y = y'.$$

Para demonstrar que (1.2.) e (1.4.) são bases, usamos o seguinte teorema de Álgebra Linear: seja V um espaço vetorial de dimensão n. Se os vetores $v_1, \cdots, v_p$ são linearmente independentes, então $p \leq n$. Se $p = n$, então os vetores formam uma base de V.

Portanto, $\mathcal{A}$ é uma álgebra de divisão. ■

Agora mostraremos que $\mathbb{R}^n$ com o produto induzido por uma álgebra $\mathcal{A}$ é uma álgebra de divisão. Seja $\mathcal{A}$ uma álgebra de divisão de dimensão n sobre $\mathbb{R}$. Em particular, $\mathcal{A}$ é um espaço vetorial sobre $\mathbb{R}$. Logo, sejam $B = \{v_1, \ldots, v_n\}$ uma base de $\mathcal{A}$ sobre $\mathbb{R}$ e uma aplicação $\Phi_B: \mathcal{A} \to \mathbb{R}^n$ dada por:

$$\phi_B(v) = \phi_B(\alpha_1 v_1 + \cdots + \alpha_n v_n) := (\alpha_1, \ldots, \alpha_n),$$

onde $v = \alpha_1 v_1 + \cdots + \alpha_n v_n \in \mathcal{A}$, com $\alpha_i \in \mathbb{R}$, $\forall i \in \{1, \ldots, n\}$. Esta aplicação está bem definida, pois qualquer elemento arbitrário v de $\mathcal{A}$ poderá ser escrito como combinação linear dos elementos da base e assim, por definição, existe $\phi_B(v)$, para todo $v \in \mathcal{A}$, e temos também que para cada $v \in \mathcal{A}$, existe um único $\phi_B(v)$ em $\mathbb{R}^n$.

Da Álgebra Linear, sabemos que a escolha de uma base do espaço vetorial $\mathcal{A}$ sobre $\mathbb{R}$ estabelece um isomorfismo (de espaços vetoriais) entre $\mathcal{A}$ e $\mathbb{R}^n$. De fato,

1. ϕ_B é linear:

Prova:

i. Sejam $v, w \in \mathcal{A}$ tais que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ e $w = \beta_1 v_1 + \cdots + \beta_n v_n$, com $\alpha_i, \beta_i \in \mathbb{R}$, onde $i \in \{1, \cdots, n\}$. Então:

$$\varphi_B(v + w) = \varphi_B(\alpha_1 v_1 + \cdots + \alpha_n v_n + \beta_1 v_1 + \cdots + \beta_n v_n)$$
$$= \varphi_B\big((\alpha_1 + \beta_1)v_1 + \cdots + (\alpha_n + \beta_n)v_n\big)$$

$$= (\alpha_1 + \beta_1, \cdots, \alpha_n + \beta_n)$$

$$= (\alpha_1, \cdots, \alpha_n) + (\beta_1, \cdots, \beta_n)$$

$$= \varphi_B(v) + \varphi_B(w).$$

ii. Sejam $\alpha \in \mathbb{R}$ e $w \in \mathcal{A}$ tal que $w = \beta_1 v_1 + \cdots + \beta_n v_n$, com $\beta_i \in \mathbb{R}$ onde $i \in \{1, \ldots, n\}$. Logo:

$$\varphi_B(\alpha w) = \varphi_B\big(\alpha(\beta_1 v_1 + \cdots + \beta_n v_n)\big)$$

$$= \varphi_B(\alpha\beta_1 v_1 + \cdots + \alpha\beta_n v_n)$$

$$= (\alpha\beta_1, \cdots, \alpha\beta_n)$$

$$= \alpha(\beta_1, \cdots, \beta_n)$$

$$= \alpha\varphi_B(w).\blacksquare$$

2. ϕ_B é bijetora.

Prova:

Sejam $v, w \in \mathcal{A}$ tais que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$, $w = \beta_1 v_1 + \cdots + \beta_n v_n$, com $\alpha_i, \beta_i \in \mathbb{R}$, onde $i \in \{1, \ldots, n\}$. Temos que:

$$\varphi_B(v) = \varphi_B(w);$$

$$\varphi_B(\alpha_1 v_1 + \cdots + \alpha_n v_n) = \varphi_B(\beta_1 v_1 + \cdots + \beta_n v_n);$$

$$(\alpha_1, \cdots, \alpha_n) = (\beta_1, \cdots, \beta_n) \Leftrightarrow \alpha_1 = \beta_1, \cdots, \alpha_n = \beta_n,$$

o que implica que $\alpha_1 v_1 + \cdots + \alpha_n v_n = \beta_1 v_1 + \cdots + \beta_n v_n$. Logo, ϕ_B é injetora.

Para mostrar que ϕ_B é sobrejetora, usaremos o seguinte teorema da Álgebra Linear:

Sejam E, F espaços vetoriais de mesma dimensão finita n. Uma transformação linear $A: E \to F$ é injetiva se, e somente se, é sobrejetiva e, portanto, um isomorfismo.

Assim, φ_B é injetora, e como $dim\,\mathcal{A} = dim\,\mathbb{R}^n$, então φ_B é sobrejetora. Logo, φ_B é bijetora.■

Portanto, temos um isomorfismo entre os espaços vetoriais $\mathcal{A}$ e $\mathbb{R}^n$. O isomorfismo ϕ_B permite transferir a operação " $\cdot$ ", definida em $\cdot : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$, para o $\mathbb{R}^n$ do seguinte modo:

$$(\alpha_1, \ldots, \alpha_n) \cdot (\beta_1, \ldots, \beta_n) = \phi_B\big(\phi_B^{-1}(\alpha_1, \ldots, \alpha_n) \cdot \phi_B^{-1}(\beta_1, \ldots, \beta_n)\big), \qquad (1.5.)$$

onde no lado esquerdo de (1.5.) a multiplicação é em $\mathbb{R}^n$ e do lado direito a multiplicação é em $\mathcal{A}$.

Afirmação: Com a operação dada por (1.5.), $\mathbb{R}^n$ é uma álgebra sobre os reais.

Prova:

Sejam $a, b, c \in \mathbb{R}^n$ e $\alpha, \beta \in \mathbb{R}$, onde $a = (\alpha_1, \dots, \alpha_n)$, $b = (\beta_1, \dots, \beta_n)$ e $c = (\gamma_1, \dots, \gamma_n)$. Então

$$a(\alpha b + \beta c) = (\alpha_1, \cdots, \alpha_n) \cdot \big(\alpha(\beta_1, \cdots, \beta_n) + \beta(\gamma_1, \cdots, \gamma_n)\big)$$

$$= \phi_B\left(\phi_B^{-1}(\alpha_1, \cdots, \alpha_n) \cdot \phi_B^{-1}\big(\alpha(\beta_1, \cdots, \beta_n) + \beta(\gamma_1, \cdots, \gamma_n)\big)\right)$$

$$= \phi_B\left(\alpha\big(\phi_B^{-1}(\alpha_1, \cdots, \alpha_n) \cdot \phi_B^{-1}(\beta_1, \cdots, \beta_n)\big) + \beta\big(\phi_B^{-1}(\alpha_1, \cdots, \alpha_n) \cdot \phi_B^{-1}(\gamma_1, \cdots, \gamma_n)\big)\right)$$

$$= \alpha\left((\alpha_1, \cdots, \alpha_n) \cdot (\beta_1, \cdots, \beta_n)\right) + \beta\big((\alpha_1, \cdots, \alpha_n) \cdot (\gamma_1, \cdots, \gamma_n)\big)$$

$$= \alpha(ab) + \beta(ac);$$

e

$$(\alpha a + \beta b)c = \big(\alpha(\alpha_1, \cdots, \alpha_n) + \beta(\beta_1, \cdots, \beta_n)\big) \cdot (\gamma_1, \cdots, \gamma_n)$$

$$= \phi_B\left(\phi_B^{-1}\big(\alpha(\alpha_1, \cdots, \alpha_n) + \beta(\beta_1, \cdots, \beta_n)\big) \cdot \phi_B^{-1}(\gamma_1, \cdots, \gamma_n)\right)$$

$$= \phi_B\left(\alpha\big(\phi_B^{-1}(\alpha_1, \cdots, \alpha_n) \cdot \phi_B^{-1}(\gamma_1, \cdots, \gamma_n)\big) + \beta\big(\phi_B^{-1}(\beta_1, \cdots, \beta_n) \cdot \phi_B^{-1}(\gamma_1, \cdots, \gamma_n)\big)\right)$$

$$= \alpha\big((\alpha_1, \cdots, \alpha_n) \cdot (\gamma_1, \cdots, \gamma_n)\big) + \beta\big((\beta_1, \cdots, \beta_n) \cdot (\gamma_1, \cdots, \gamma_n)\big)$$

$$= \alpha(ac) + \beta(bc).$$

Logo, $\mathbb{R}^n$ com a operação de (1.5.) torna-se uma álgebra sobre os reais. ■

Para que ϕ_B seja um isomorfismo de álgebras, teremos que demonstrar $\phi_B(v \cdot w) = \phi_B(v) \cdot \phi_B(w)$, para quaisquer $v, w \in \mathcal{A}$. Sejam $v, w \in \mathcal{A}$ tais que $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ e $w = \beta_1 v_1 + \cdots + \beta_n v_n$, com $\alpha_i, \beta_i \in \mathbb{R}$, onde $i \in \{1, \cdots, n\}$.

Assim,

$$\phi_B(v) \cdot \phi_B(w) = \phi_B(\alpha_1 v_1 + \cdots + \alpha_n v_n) \cdot \phi_B(\beta_1 v_1 + \cdots + \beta_n v_n)$$

$$= (\alpha_1, \cdots, \alpha_n) \cdot (\beta_1, \cdots, \beta_n)$$

$$= \phi_B\big(\phi_B^{-1}(\alpha_1, \cdots, \alpha_n) \cdot \phi_B^{-1}(\beta_1, \cdots, \beta_n)\big)$$

$$= \phi_B\left((\alpha_1 v_1 + \cdots + \alpha_n v_n) \cdot (\beta_1 v_1 + \cdots + \beta_n v_n)\right)$$

$$= \phi_B(v \cdot w).$$

Como $\mathcal{A}$ é uma álgebra de divisão, temos que $\mathbb{R}^n$ com o produto induzido pelo de $\mathcal{A}$, também será uma álgebra de divisão. De fato, dados $a, b \in \mathbb{R}^n$, $a \neq 0$, $\mathbb{R}^n$ será uma álgebra de divisão se as duas equações

$$ax = b$$

e

$$ya = b$$

possuírem únicas soluções, ou seja,

$$ax = b \Longrightarrow \phi_B\left(\phi_B^{-1}(a) \cdot \phi_B^{-1}(x)\right) = b$$

$$\Longrightarrow \phi_B^{-1}(a) \cdot \phi_B^{-1}(x) = \phi_B^{-1}(b).$$

e

$$ya = b \Rightarrow \phi_B\left(\phi_B^{-1}(y) \cdot \phi_B^{-1}(a)\right) = b$$

$$\Rightarrow \phi_B^{-1}(y) \cdot \phi_B^{-1}(a) = \phi_B^{-1}(b).$$

Como $\mathcal{A}$ é uma álgebra de divisão, existem únicos $u, v \in \mathcal{A}$ tais que:

$$\phi_B^{-1}(a) \cdot u = \phi_B^{-1}(b) \text{ e } v \cdot \phi_B^{-1}(a) = \phi_B^{-1}(b).$$

Afirmação 1: $\phi_B(u)$ é solução única de $ax = u$.

Prova:

De fato, temos:

$$a \cdot \phi_B(u) = \phi_B\left(\phi_B^{-1}(a) \cdot \phi_B^{-1}\left(\phi_B(u)\right)\right)$$

$$= \phi_B(\phi_B^{-1}(a) \cdot u)$$

$$= \phi_B\left(\phi_B^{-1}(b)\right) = b.$$

Suponha que $\phi_B(u')$ seja outra solução para $ax = b$, então

$$a \cdot \phi_B(u') = b.$$

Como $\mathcal{A}$ é uma álgebra de divisão, existe $u' \in \mathcal{A}$ tal que $\phi_B^{-1}(a) \cdot u' = \phi_B^{-1}(b)$. Logo, $u = u'$.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Se $\phi_B(u) \neq \phi_B(u')$, então $u \neq u'$, pois ϕ_B é injetiva, o que é uma contradição. Concluímos então que $\phi_B(u) = \phi_B(u')$.■

Afirmação 2: $\phi_B(v)$ é solução única de $ya = b$.

Prova:

De fato, temos que:

$$\begin{aligned}\phi_B(v)\cdot y &= \phi_B\left(\phi_B^{-1}(\phi_B(v))\cdot\phi_B^{-1}(y)\right)\\ &= \phi_B(v\cdot\phi_B^{-1}(y))\\ &= \phi_B(\phi_B^{-1}(y))\\ &= y.\end{aligned}$$

Suponha que $\phi_B(v')$ seja outra solução para $ya = b$, então:

$$\phi_B(v')\cdot a = b.$$

Como $\mathcal{A}$ é uma álgebra de divisão, existe $v' \in \mathcal{A}$ tal que $v'\phi_B^{-1}(a) = \phi_B^{-1}(b)$. Logo, $v = v'$. Se $\phi_B^{-1}(v) \neq \phi_B^{-1}(v')$, então $v \neq v'$, pois ϕ_B é injetiva, o que é uma contradição. Assim, $\phi_B(v) = \phi_B(v')$.■

Portanto, $\mathbb{R}^n$ com o produto induzido de $\mathcal{A}$ torna-se uma álgebra de divisão, e pelo Teorema 1.5., não possui divisores de zero.

Seja $S^{n-1} = \{x \in R^n; ||x|| = 1\}$ uma esfera unitária e f uma função definida como segue:

$$f: S^{n-1}\times S^{n-1} \longrightarrow S^{n-1};$$

$$(v,w) \mapsto v\cdot w.$$

Se $v, w \in S^{n-1}$, então $v \neq 0$ e $w \neq 0$.

Se $a, b \in \mathbb{R}^n$ e $ab = 0$, então $a = 0$ ou $b = 0$.

Portanto, $f: S^{n-1}\times S^{n-1} \to \mathbb{R}^n$ nunca assume o valor 0. É possível, então, definir $g: S^{n-1}\times S^{n-1} \longrightarrow S^{n-1}$

dada por

$$g(v,w) := \frac{f(v,w)}{||f(v,w)||}.$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Sobre g podemos afirmar:

(1) $g(-v,w) = g(v,-w) = -g(v,w).$

De fato,

$$\begin{aligned} g(-v,w) &= \frac{f(-v,w)}{||f(-v,w)||} \\ &= \frac{-v \cdot w}{||-v \cdot w||} \\ &= \frac{-(v \cdot w)}{||v \cdot w||} \\ &= -\frac{f(v,w)}{||f(v,w)||} \\ &= -g(v,w) \end{aligned}$$

e

$$\begin{aligned} g(v,-w) &= \frac{f(v,-w)}{||f(v,-w)||} \\ &= \frac{v(-w)}{||v(-w)||} \\ &= \frac{-(vw)}{vw} \\ &= -\frac{f(v,w)}{||f(v,w)||} \\ &= -g(v,w). \end{aligned}$$

Dizemos que g é uma aplicação ímpar.

(2) g é contínua.

Escolha em $S^{n-1} \times S^{n-1}$ a norma do máximo:

$$||(u,v)||_M = MAX\{||u||, ||v||\}; \forall (u,v) \in S^{n-1} \times S^{n-1}.$$

Vamos, primeiro, mostrar que f é contínua. Para isso, dado $\epsilon > 0$, devemos exibir $\delta > 0$ tal que, se $||(u,v) - (u_0,v_0)||_M < \delta$, então, $||f(u,v) - f(u_0,v_0)|| < \epsilon$. Observe que

$$||f(u,v) - f(u_0,v_0)|| < \epsilon \Leftrightarrow$$

$$\Leftrightarrow ||u \cdot v - u_0 \cdot v_0|| < \epsilon \Leftrightarrow$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$\Leftrightarrow ||u \cdot v - u_0 \cdot v + u_0 \cdot v - u_0 \cdot v_0|| < \epsilon \Leftrightarrow$$

$$\Leftrightarrow ||u - u_0|| \cdot ||v|| + ||u_0|| \cdot ||v - v_0|| < \epsilon. \qquad (1.6.)$$

Assim, devemos demonstrar (1.6.). Agora,

$$||u - u_0|| < ||(u, v) - (u_0, v_0)||_M < \delta \qquad (1.7.)$$

$$||v- v_0|| < ||(u, v) - (u_0, v_0)||_M < \delta \qquad (1.8.)$$

Pela Desigualdade Triangular,

$$||v|| = ||v- v_0 + v_0|| \leq ||v- v_0|| + ||v_0||. \qquad (1.9.)$$

Escolha $\left\{1, \frac{\epsilon}{2||u_0||}, \frac{\epsilon}{2(1+||v_0||)}\right\}$. Seja $\delta \leq 1$, então, por (1.8.), temos que $||v - v_0|| < \delta \leq 1$. Por (1.9.), temos que $||v|| \leq ||v - v_0|| + ||v_0|| < 1 + ||v_0||$.

Voltando a (1.6.) e usando (1.7.), (1.8.) e (1.9.), temos:

$$||u - u_0|| \cdot ||v|| + ||u_0|| \cdot ||v - v_0|| < ||u - u_0|| \cdot (1 + ||v_0||) + ||u_0|| \cdot ||v - v_0||$$

$$< \delta \cdot (1 + ||v_0||) + ||u_0|| \cdot \delta$$

$$\leq \frac{\epsilon}{2(1 + ||v_0||)} \cdot (1 + ||v_0||) + ||u_0|| \frac{\epsilon}{2||u_0||}$$

$$= \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Isso mostra que f é contínua. Como a norma $|| \ ||: \mathbb{R}^n \to \mathbb{R}$ é uma função contínua e a composta de funções contínuas é também contínua, temos que $||f(u, v)||$ é contínua. Uma vez que $||f(u, v)|| \neq 0, \forall (u, v) \in S^{n-1} \times S^{n-1}$,temos que $g(u, v) = \frac{f(u,v)}{||f(u,v)||}$ é contínua.

A estratégia para a demonstração do Teorema de Hopf sobre Álgebras de Divisão Reais é dada a seguir:

Teorema 1.6. Se existe uma aplicação contínua ímpar em $S^{n-1} \times S^{n-1}$,então n é uma potência de 2.

Corolário 1.7. (Teorema de Hopf): A dimensão de uma álgebra de divisão sobre os reais é uma potência de 2.

Uma vez demonstrado o teorema, a demonstração do corolário seguirá o raciocínio exposto acima.

Dada uma aplicação contínua ímpar $g: S^{n-1} \times S^{n-1} \to S^{n-1}$, a função

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$G: \mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \longrightarrow \mathbb{P}^{n-1}$$

dada por $G(\overline{u}, \overline{v}) = \overline{g(u,v)}$ é chamada função induzida por g. Como g é ímpar, G está bem definida ($\mathbb{P}^{n-1} = S^{n-1}/\sim = \{\overline{x};\ x \in S^{n-1}, \overline{x} = \{x, -x\}\}$), pois não depende da escolha de $\overline{u}$ e $\overline{v}$.

A demonstração do Teorema 1.6 fará uso de técnicas de Topologia Algébrica sobre o corpo $\mathbb{F}_2 = \{0,1\}$, no qual será aplicada à função G. Será necessário trabalhar com os espaços projetivos, pois a homologia de esferas é muito simples para fornecer quaisquer resultados.

2 RESULTADOS

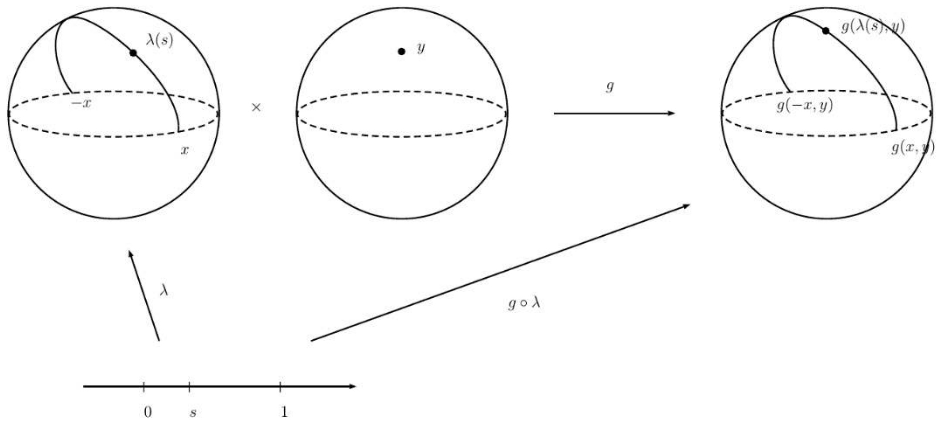
Nesta seção demonstraremos o Teorema 1.6. Já vimos que existe a função contínua $G: \mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$. Temos que $[x \times \mathbb{P}^1]$ e $[\mathbb{P}^1 \times y]$ formam uma base de $H_1(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$, pois $H_1(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$ é isomorfo ao espaço vetorial sobre o corpo $\mathbb{F}_2 = \{0,1\}$, quando $\mathbb{P}^1$ é um subespaço projetivo unidimensional de $\mathbb{P}^{n-1}$. Temos também que G induz um homomorfismo de grupos $G_*: H_q(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}) \to H_q(\mathbb{P}^{n-1})$.

Afirmação 1: $G_*([\mathbb{P}^1 \times y]) = G_*([x \times \mathbb{P}^1]) = [\mathbb{P}^1]$, onde $G_*([\mathbb{P}^1 \times y])$ é um elemento não nulo de $H_1(\mathbb{P}^{n-1})$.

Demonstração da Afirmação 1:

Seja w um caminho fechado em $\mathbb{P}^{n-1}$. Existe um caminho $\overline{w}$ em S^{n-1} que é transformado em w pela aplicação antípoda $\alpha: S^{n-1} \to \mathbb{P}^{n-1}$. O caminho w é fechado se $\overline{w}$ liga dois pontos antípodas. Neste caso, $[w] \neq 0$. Caso contrário, quando w não é fechado, $[w] = 0$. Agora, $\mathbb{P}^1 \times \{y\}$ é um caminho fechado $w \times \{y\}$ em $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$ e o caminho $\overline{w}$ é metade de um grande círculo, ligando dois pontos antípodas de S^{n-1}. Como g: $S^{n-1} \times S^{n-1} \to S^{n-1}$, que induz G, satisfaz $g(-x,y) = -g(x,y)$, a imagem $g \circ (\overline{w} \times \{y\})$ em S^{n-1} também liga dois pontos antípodas.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218



Fonte: Dados da pesquisa / Próprios autores (2023)

Aplicando $\alpha: S^{n-1} \to \mathbb{P}^{n-1}$, isto é, identificando pontos antípodas, o caminho $g \circ (\overline{w} \times y)$ é transformado em $G \circ (w \times y)$, que representa a classe de homologia de $G_*([\mathbb{P}^1 \times y])$, que é, portanto, diferente de zero. Como $H_1(\mathbb{P}^{n-1}) \cong \mathbb{F}_2 = 0{,}1$ e $G_*([\mathbb{P}^1 \times y]) \neq 0$, temos que $G_*([\mathbb{P}^1 \times \{y\}]) = 1 = [\mathbb{P}^1]$.

Temos que $\{x\} \times \mathbb{P}^1$ é um caminho fechado $\{x\} \times w$ em $\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}$ e o caminho $\overline{w}$ é também metade de um grande círculo, ligando dois pontos antípodas de S^{n-1}. Como $g: S^{n-1} \times S^{n-1} \to S^{n-1}$, que induz G, satisfaz $g(x, -y) = -g(x, y)$, a imagem $g \circ (\{x\} \times \overline{w})$ em S^{n-1} também liga dois pontos antípodas.

Aplicando $\alpha: S^{n-1} \to \mathbb{P}^{n-1}$, isto é, identificando pontos antípodas, o caminho $g \circ (x \times \overline{w})$ é transformado em $G \circ (x \times w)$, que representa a classe de homologia de $G_*([x \times \mathbb{P}^1])$, que é, portanto, diferente de zero. Como $H_1(\mathbb{P}^{n-1}) \cong \mathbb{F}_2 = 0{,}1$ e $G_*([x \times \mathbb{P}^1]) \neq 0$, temos que $G_*([\{x\} \times \mathbb{P}_1]) = 1 = [\mathbb{P}_1]$. Isso conclui a demonstração da Afirmação 1.■

Temos que:

$$H^*(\mathbb{P}^{n-1}) \cong \mathbb{F}_2[t]/(t^n);$$

$$H^*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}) \cong \mathbb{F}_2[u, v]/(u^n, v^n).$$

Afirmação 2: $G^*: H^*(\mathbb{P}^{n-1}) \to H^*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$ é dado por $G^*(t) = u + v$, onde t gera $H^1(\mathbb{P}^{n-1})$, isto é, $H^1(\mathbb{P}^{n-1}) = \{at; a \in \mathbb{F}_2\} = \{0, t\}$ e u e v são induzidas pelas projeções

$$\phi_1: \mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \longrightarrow \mathbb{P}^{n-1},$$

$$(x, y) \mapsto x;$$

e

$$\phi_2: \mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \longrightarrow \mathbb{P}^{n-1},$$

$$(x, y) \mapsto y;$$

ou seja,

$$\phi_1^*: H^*(\mathbb{P}^{n-1}) \to H^*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$$

$$\phi_1^*(t) = u;$$

$$\phi_2^*: H^*(\mathbb{P}^{n-1}) \to H^*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$$

$$\phi_2^*(t) = v,$$

onde u e v são funções, em última instância, de $\mathbb{F}_2$ em $\mathbb{F}_2$.

Demonstração da Afirmação 2:

Vamos assumir $n > 2$. Se $n > 2$, então $H_1(\mathbb{P}^{n-1}) \cong \mathbb{F}_2 = \{0,1\}$.

Seja $\lambda: [0,1] \to S^{n-1}$ um caminho ligando dois pontos antípodas de S^{n-1}, $\lambda(0) = -x$ e $\lambda(1) = x$. Então, para y fixado, o caminho $\psi: [0,1] \to S^{n-1}$, dado por $s \mapsto g(\lambda(s), y)$, liga $g(x, y)$ a $g(-x, y) = -g(x, y)$. De fato,

$$\psi(0) = g(\lambda(0), y) = g(-x, y) = -g(x, y);$$

$$\psi(1) = g(\lambda(1), y) = g(x, y).$$

Temos que $g: S^{n-1} \times S^{n-1} \to S^{n-1}$ induz $G: \mathbb{P}^{n-1} \times \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$, que passa a induzir um homomorfismo de grupos $G^*: H^*(\mathbb{P}^{n-1}) \to H^*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$. Assim,

$$< G^*(t), [\{x\} \times \mathbb{P}^1] >=< t, G_*([\{x\} \times \mathbb{P}^1]) >$$

$$=< t, G_*([\mathbb{P}^1]) >$$

$$= 1 \in \mathbb{F}^2.$$

A igualdade $< t, G_*([\{x\} \times \mathbb{P}^1]) >=< t, [\mathbb{P}^1] >$ segue pela Afirmação 1. Se tivéssemos $< t, [\mathbb{P}^1] >= 0$, então t seria uma função identicamente nula. Contradição pois t gera $H^1(\mathbb{P}^{n-1})$. Logo, vale $< t, [\mathbb{P}^1] >= 1$. Temos que $u, v: H_*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1}) \longrightarrow \mathbb{F}^2$. Logo,

$$u([\mathbb{P}^1], [\{y\}]) = u(1,0) = 1 =< u, [\mathbb{P}^1, \{y\}] >,$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$u([\{x\}],[\mathbb{P}^1]) = u(0,1) = 0 =< u,[\mathbb{P}^1,\{y\}] >;$$

$$v([\mathbb{P}^1],[\{y\}]) = u(1,0) = 0 =< v,[\mathbb{P}^1,\{y\}] >,$$

$$u([\{x\}],[\mathbb{P}^1]) = u(0,1) = 1 =< v,[\mathbb{P}^1,\{y\}] >;$$

pois u e v são induzidas pelas projeções ϕ_1 e ϕ_2, respectivamente. Assim, temos que:

$$< u,[\mathbb{P}^1 \times \{y\}] >= 1,$$

$$< u,[\{x\} \times \mathbb{P}^1] >= 0;$$

$$< v,[\mathbb{P}^1 \times \{y\}] >= 0,$$

$$< v,[\{x\} \times \mathbb{P}^1] >= 1.$$

Logo:

$$< u+v,[\{x\} \times \mathbb{P}^1] > = < u,[\{x\} \times \mathbb{P}^1] > + < v,[\{x\} \times \mathbb{P}^1] > = 0+1,$$

e

$$< u+v,[\mathbb{P}^1 \times \{y\}] >=< u,[\mathbb{P}^1 \times \{y\}] > + < v,[\mathbb{P}^1 \times \{y\}] >= 1+0.$$

Temos que $[x \times \mathbb{P}^1]$ e $[\mathbb{P}^1 \times y] \in H_1(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$ são os geradores de $H_*(\mathbb{P}^{n-1} \times \mathbb{P}^{n-1})$. Dessa forma, $G_*(t)$ e $u+v$ coincidem nos geradores de $H_*(P^{n-1} \times P^{n-1})$, logo são iguais. Isso conclui a demonstração da segunda afirmação.■

Para $t^n = 0$, segue que

$$0 = \left(G^*(t)\right)^n = (u+v)^n.$$

Agora:

$$0 = (u+v)^n = \sum_{k=1}^{n} \binom{n}{k} u^k v^{n-k}.$$

Assim:

$$\sum_{k=1}^{n} \binom{n}{k} u^k v^{n-k} = 0 \Rightarrow$$

$$\Rightarrow \underbrace{u^n}_{=0} + \sum_{k=1}^{n-1} \binom{n}{k} u^k v^{n-k} + \underbrace{v^n}_{=0} \Rightarrow$$

$$\Rightarrow \sum_{k=1}^{n-1} \binom{n}{k} u^k v^{n-k} = 0 \text{ em } \mathbb{F}_2[u,v] \Rightarrow$$

$$\Rightarrow \binom{n}{k} = 0 \text{ em } \mathbb{F}_2, \forall k, 1 \leq k \leq n-1 \Rightarrow$$

$$\Rightarrow \binom{n}{k} \text{ é um inteiro par}, \forall k, 1 \leq k \leq n-1.$$

Se n não é uma potência de 2, então n é ímpar ou $n = 2^m \cdot q$, com q ímpar, $q > 1, m \geq 1$. Se n é ímpar, então $\binom{n}{n-1} = n$ é ímpar. Se $n = 2^m q$, com $m \geq 1$, devemos mostrar que existe k, $1 \leq k \leq n-1$, tal que $\binom{n}{k}$ é ímpar.

Afirmação *3*: $\binom{2^m q}{2^m}$ é ímpar.

Demonstração da Afirmação 3:

$$\binom{2^m q}{2^m} = \frac{2^m q(2^m q - 1)\ldots(2^m q - 2^m + 1)}{2^m q(2^m - 1)\ldots 3 \cdot 2 \cdot 1}$$

$$= \frac{\prod_{k=0}^{2^{m-1}}(2^{m-1} - k)}{\prod_{k=0}^{2^{m-1}}(k+1)} = \prod_{k=0}^{2^{m-1}} \frac{2^m q - k}{k+1}$$

$$= \frac{2^m q}{1} \cdot \frac{2^m q - 1}{2} \cdot \frac{2^m q - 2}{3} \ldots \frac{2^m q - 2^m + 2}{2^m - 1} \cdot \frac{2^m q - 2^m + 1}{2^m}$$

$$= \frac{2^m q}{2^m} \cdot \frac{2^m q - 1}{2^m - 1} \cdot \frac{2^m q - 2}{2^m - 2} \ldots \frac{2^m q - 2^m + 2}{2} \cdot \frac{2^m q - 2^m + 1}{1}$$

$$= q \cdot \frac{2^m q - 1}{2^m - 1} \cdot \frac{2^{m-1} q - 1}{2^{m-1} - 1} \ldots \frac{2^{m-1} q - 2^{m-1} + 1}{1} \cdot \frac{2^m q - 2^m + 1}{1}.$$

Essa última expressão é ímpar, pois todos os fatores que aparecem no numerador e no denominador são ímpares. Assim, pela contra positiva, como $\binom{n}{k}$ é um inteiro par, $\forall k$, $1 \leq k \leq n - 1$, então n é uma potência de 2.

3 CONSIDERAÇÕES

Ao longo do desenvolvimento desse artigo conseguimos compreender um importante resultado de classificação sobre álgebras de divisão reais. Para tanto, utilizamos de técnicas de homologia e cohomologia sobre o corpo $\mathbb{F}_2 = \{0,1\}$.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

REFERÊNCIAS

EBBINGHAUS, H. D.; HERMES, H.; HIRZEBRUCH, F.; KOECHER, M.; MAINZER, K.; NEUKIRCH, J.; PRESTEL, A.; REMMERT, R. **Graduate Texts in Mathematics, Readings in Mathematics:** numbers. New York: Springer, 1991.

FELZENSZWALB, B. **Álgebra de dimensão Finitas**. Rio de Janeiro*:* IMPA, 1979.

HATCHER, A. **Algebraic topology.** [*S. l.: s. n.*], 2001. Disponível em: AT.dvi (cornell.edu). Acesso em: 24 abr. 2023.