RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

TEOREMAS DE FROBENIUS E HURWITZ SOBRE ÁLGEBRAS DE DIVISÃO REAIS

FROBENIUS AND HURWITZ THEOREMS ABOUT REAL DIVISION ALGEBRAS

TEOREMAS DE FROBENIUS Y HURWITZ SOBRE ÁLGEBRAS DE DIVISIÓN REALES

Lia Nojosa Sena[1], Rubens Cainan Saboia Monteiro[2], Maria Madalena de Queiroz Alves[3]

e473594
https://doi.org/10.47820/recima21.v4i7.3594

PUBLICADO: 07/2023

RESUMO

Este trabalho tem como objetivo apresentar uma proximidade entre as álgebras dos complexos $\mathbb{C}$, dos quaternios $\mathbb{H}$ e dos octônios $\mathbb{O}$ com a álgebra dos reais $\mathbb{R}$. Para tanto, descreveremos ferramentas para as demonstrações dos teoremas de Frobenius e Hurwitz, onde o primeiro diz que as álgebras $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ são as únicas álgebras de divisão sobre os reais onde a multiplicação é associativa (tais álgebras são chamadas associativas) e o segundo afirma que as álgebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ e $\mathbb{O}$ são as únicas álgebras de divisão com elemento identidade nas quais é possível definir uma norma compatível com a multiplicação.

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

ABSTRACT

This work aims to present a proximity between the algebras of the complexes $\mathbb{C}$, of the quaternions $\mathbb{H}$, of the octonions $\mathbb{O}$ with the algebra of reals $\mathbb{R}$. To do so, we will describe tools for the demonstrations of the theorems of Frobenius and Hurwitz, where the first one says that the algebras $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{H}$ are the only divisions algebras over the reals where multiplications is associative (such as algebras are called associative) and the second states that algebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$ are the only ones division algebras with identity element in which it is possible to define a norm compatible with the multiplication.

KEYWORDS: *Real algebras. Associative algebras. Division algebras.*

RESUMEN

Este trabajo tiene como objetivo presentar una proximidad entre las álgebras de los complejos $\mathbb{C}$, de los cuaterniones $\mathbb{H}$ y octoniones $\mathbb{O}$ con el álgebra de reales $\mathbb{R}$. Para ello, describiremos herramientas para las demonstraciones de los teoremas de Frobenius y Hurwitz, donde el primero dice que las álgebras $\mathbb{R}$, $\mathbb{C}$ y $\mathbb{H}$ son las únicas álgebras de división sobre los reales donde la multiplicación es asociativa (como álgebras se denominan asociativas) y la segunda establece que las álgebras $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ y $\mathbb{O}$ son las únicas álgebras de división con elemento identidad en las que es posible definir una norma compatible con la multiplicacion.

PALABRAS CLAVE*: Álgebra reales. Álgebras asociativas. Álgebras de división.*

[1] Mestra em Matemática pela Universidade Federal do Ceará.
[2] Mestre em Matemática pela Universidade Federal do Ceará.
[3] Graduada no bacharelado em ciência da computação no Instituto Federal de Educação, Ciência e Tecnologia do Ceará, campus Tianguá.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

INTRODUÇÃO

Os quatro exemplos clássicos de álgebras de divisão são os reais $\mathbb{R}$, os complexos $\mathbb{C}$, os quatérnios $\mathbb{H}$ e os octônios $\mathbb{O}$. Em comparação com outras álgebras, as álgebras dos complexos, dos quatérnios e dos octônios são as mais próximas da álgebra dos reais, isto é, as que compartilham com a álgebra dos números reais o maior número de propriedades algébricas. Exemplos dessa proximidade são:

1. As álgebras $\mathbb{R}, \mathbb{C}$ e $\mathbb{H}$ são as únicas álgebras de divisão sobre os reais onde a multiplicação é associativa (tais álgebras são chamadas associativas). A versão mais precisa desta proposição é conhecida como Teorema de Frobenius.
2. As álgebras $\mathbb{R}, \mathbb{C}, \mathbb{H}$ e $\mathbb{O}$ são as únicas álgebras de divisão com elemento identidade nas quais é possível definir uma norma compatível com a multiplicação. Essa é a essência do teorema de Hurwitz.

1 REFERENCIAL TEÓRICO

A seguir, algumas definições e resultados importantes para o desenvolvimento desse trabalho.

Definição 1.1. Seja V um espaço vetorial sobre $\mathbb{R}$. Este espaço é chamado álgebra sobre $\mathbb{R}$ (ou $\mathbb{R}$-álgebra, ou 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

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

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

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

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

são sempre 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 $1x = x1 =$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

x, $\forall x \in V$. Neste caso, V é chamada álgebra com unidade. Se a unidade $1 = 0$, então $x = 1x = 0x = 0$ para todo $x \in V$, isto é, $V = 0$.

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, assim, escrevemos $\mathcal{A} := (V, \cdot)$. 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, $dim\ \mathcal{A} = dim\ V$.

Assim, uma álgebra $\mathcal{A}$ n-dimensional sobre $\mathbb{R}$ consiste em todas as combinações lineares

$$x = \sum_{i=1}^{n} \alpha_i \epsilon_i$$

de n elementos básicos $\epsilon_1, \cdots, \epsilon_n$ com eficientes α_i em $\mathbb{R}$.

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 $\mathcal{A}$.

Definição 1.3**.** Uma álgebra real $\mathcal{A}$ é normada se podemos definir um produto escalar de modo que tenhamos a identidade

$$(ab, ab) = (a, a)(b, b). \qquad (1.1.)$$

Exibiremos, a seguir, alguns exemplos de álgebras de divisão.

1. O corpo dos números reais é uma $\mathbb{R}$-álgebra de dimensão 1, com elemento identidade e sem divisores de zero. Essa álgebra é comutativa, associativa e com divisão.
2. O corpo $\mathbb{C}$ dos números complexos é uma álgebra real. A dimensão dessa álgebra, isto é, a dimensão de $\mathbb{C}$ como espaço vetorial sobre $\mathbb{R}$, é igual a 2. Temos que $B = (1, i)$, onde $i^2 = -1$, é uma base de $\mathbb{C}$ sobre $\mathbb{R}$. Dado $z \in \mathbb{C}$, existem $a, b \in \mathbb{R}$ tais que $z = a + bi$. Chamamos a de parte real e b de parte imaginária de z. Se $z = a + bi$ e $w = c + di$ são números complexos, então $z + w = (a + c) + (b + d)i$ e $zw = (ac - bd) + (bc - ad)i$. Essa multiplicação é comutativa e associativa, o que torna $\mathbb{C}$ uma álgebra que é comutativa e associativa. O número complexo $z = a - bi$ é chamado conjugado de z. O

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

número real não negativo $|z| = \sqrt{z\bar{z}} = \sqrt{a^2 + b^2}$ é chamado de módulo de z. Além disso, $z = 0$ se e somente se $|z| = 0$. Se $|z| \neq 0$, então $\frac{\bar{z}}{|z|^2}$ satisfaz $zw = wz = 1$. Assim, $\mathbb{C}$ é uma álgebra de divisão.

3. O conjunto dos quatérnios $\mathbb{H}$ é composto por números da forma $a_1 + a_2 i + a_3 j + a_4 k$, com $a_l \in \mathbb{R}$ tal que $a_l \in \{1, \cdots, 4\}$. A regra de adição é dada por $(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$. Para determinar a regra da multiplicação é suficiente atribuir valores aos produtos dos números $i,\ j,\ k$ dados por:

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

$$ij = k \quad ji = -k;$$

$$jk = i \quad kj = -i;$$

$$ki = j \quad ik = -j.$$

A álgebra dos quatérnios $\mathbb{H}$ é uma álgebra sobre os reais de dimensão quatro não comutativa, associativa e de divisão.

Suponhamos que $\mathcal{A}$ tenha identidade e que seja 1 uma identidade desta álgebra. Todo elemento a pode ser unicamente representado como soma de dois termos no qual um seja proporcional a 1 e o outro ortogonal a 1. O fato citado acima pode ser visto de um modo mais geral: seja i um vetor não nulo. Todo vetor a pode ser decomposto como soma de dois vetores no qual um é proporcional a i e o outro ortogonal a i:

$$a = ki + u,\ u \perp i.$$

De fato, para demostrar a afirmação acima, devemos mostrar a existência de um número k tal que o vetor $u = a - ki$ é ortogonal a i, isto é, tal que

$$(a - ki, i) = 0.$$

Equivalentemente,

$$(a, i) = k(i, i).$$

Então

$$k = \frac{(a,i)}{(i,i)}.$$

Note que $i \neq 0$, de modo que $(i, i) \neq 0$.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Temos que

$$a = k1 + a',$$

onde k é um número real e $a' \perp 1$. Introduziremos nesta álgebra uma operação de conjugação cujo efeito sobre um elemento a é dado por

$$\overline{a} = k1 - a'.$$

Em particular, se a é proporcional a 1, então $\overline{a} = a$, e se a é ortogonal a 1, então $\overline{a} = -a$. Claramente,

$$\overline{\overline{a}} = a$$

e

$$\overline{a + b} = \overline{a} + \overline{b}.$$

Definição 1.4**.** Um subespaço vetorial real $\mathcal{P}$ de uma $\mathbb{R}$-álgebra $\mathcal{A}$ é chamado $\mathbb{R}$-subálgebra de $\mathcal{A}$ se $xy \in \mathcal{P}$ para todos $x,\ y \in \mathcal{P}$.

Definição 1.5**.** Se $\mathcal{A} = (V, .)$ e $\mathcal{B} = (W, .)$ são duas álgebras quaisquer, uma função $\mathbb{R}$-linear bijetora $f: V \to W$ é dita um isomorfismo de $\mathbb{R}$-álgebras se

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

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

Se $\mathcal{A}$ é uma subálgebra com identidade e, então $f: \mathbb{R} \to \mathcal{A}$ dada por $\alpha = \alpha e$ é monomórfica, isto é, um homomorfismo injetor. Em particular, toda álgebra real com elemento identidade de dimensão 1 é isomorfa a $\mathbb{R}$ (exceto quando f é nula).

1.1 PROCESSO DE DUPLICAÇÃO

Descreveremos aqui um processo que permite a construção dos octônios através dos quatérnios como um caminho natural. Mostraremos que este processo de duplicação do qual serão obtidos os octônios é o resultado de uma" duplicação" dos quatérnios. Este processo de duplicação poderá, não somente ser usado para obter os octônios dos quatérnios, como também os quatérnios dos complexos e os complexos dos números reais. Usando o fato de que $ij = k$, podemos escrever qualquer quatérnio

$$q = a_0 + a_1 i + a_2 j + a_3 k$$

na forma

$$q = (a_0 + a_1 i) + (a_2 j + a_3 i)j,$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

ou

$$q = z_1 + z_2 j,$$

com $z_1 = a_0 + a_1 i$ e $z_2 = a_2 + a_3 i$.

Com essa nova forma de escrever os quatérnios, consideremos a multiplicação. Tome o quatérnio r, dado por

$$r = w_1 + w_2 j,$$

e considere o produto

$$\begin{aligned} qr &= (z_1 + z_2 j)(w_1 + w_2 j) \\ &= z_1 w_1 + z_1(w_2 j) + (z_2 j) w_1 + (z_2 j) w_2 j \\ &= z_1 w_1 + z_1 w_2 j + z_2 j w_1 + z_2 j w_2 j. \end{aligned} \qquad (1.1.1.)$$

Os parênteses podem ser retirados, pois a álgebra dos quatérnios é associativa. Como $ij = -ji$,

temos $(a_0 + a_1 i)j = a_0 j + a_1 ij = a_0 j - a_1 ji = j(a_0 - a_1 i)$, isto é,

$$z_1 j = j\overline{z_1}.$$

Temos que dois elementos z e w da forma $a + bi$ comutam, *i.e.*,

$$zw = wz.$$

Com estas propriedades em mente, reescrevemos o segundo termo do lado direito de (1.1.1.) como $z_1 w_2 j = w_2 z_1 j$, o terceiro termo sendo $z_2 j w_1 = z_2 \overline{w_1} j$, e o quarto $z_2 j w_2 j = z_2 \overline{w_1} jj = z_2 \overline{w_2} j^2 = -z_2 \overline{w_2}$. Segue que

$$\begin{aligned} qr &= z_1 w_1 + w_2 z_1 j + z_2 \overline{w_1} j - z_2 \overline{w_2} \\ &= (z_1 w_1 - z_2 \overline{w_2}) + (w_2 z_1 + z_2 \overline{w_1}) j. \end{aligned} \qquad (1.1.2.)$$

Um ponto importante sobre a representação dos quatérnios na forma $q = z_1 + z_2 j$, isto é, quando $i^2 = -1$, todos os quatérnios da forma $a + bi$ podem ser vistos como números complexos.

Definimos os quatérnios como expressões da forma $z_1 + z_2 j$, quando z_1 e z_2 são números complexos e j é um símbolo, que são multiplicados conforme (1.1.2.). Seja $\mathcal{U}$ uma álgebra com elementos da forma

$$u = a_0 + a_1 i_1 + a_2 i_2 + \cdots + a_n i_n,$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

com adição e multiplicação definidas. O elemento

$$\overline{u} = a_0 - a_1 i_1 - a_2 i_2 - \cdots - a_n i_n$$

sendo o conjugado de u.

Agora definimos $\mathcal{U}^{(2)}$, a $\mathcal{U}$ duplicada, uma álgebra com dimensão $2n$ cujos elementos são expressões da forma

$$u_1 + u_2 e, \qquad (1.1.3.)$$

com u_1 e u_2 elementos arbitrários em $\mathcal{U}$ e e um novo símbolo. Os elementos de $\mathcal{U}^{(2)}$ são adicionados de acordo com a regra

$$(u_1 + u_2 e) + (v_1 + v_2 e) = (u_1 + v_1) + (u_2 + v_2)e \qquad (1.1.4.)$$

e a multiplicação é dada por

$$(u_1 + u_2 e)(v_1 + v_2 e) = (u_1 v_1 - \overline{v_2} u_2) + (v_2 u_1 + u_2 \overline{v_1})e, \qquad (1.1.5.)$$

a barra denota conjugação em $\mathcal{U}$. A forma usual de um elemento em $\mathcal{U}^{(2)}$ é

$$a_0 + a_1 i_1 + \cdots + a_n i_n + a_{n+1} i_{n+1} + \cdots + a_{2n+1} i_{2n+1}, \qquad (1.1.6.)$$

sendo os pares de elementos u_1 e u_2 em $\mathcal{U}$ dados por $u_1 = a_0 + a_1 i_1 + \cdots + a_n i_n$ e $u_2 = a_{n+1} i_{n+1} + \cdots + a_{2n+1} i_{2n+1}$, assim, os elementos de (1.1.3) podem ser considerados como uma forma de escrever simplificada de (1.1.6). Além disso, as definições da adição e da multiplicação em (1.1.4.) e (1.1.5.) são mais curtas e mais claras do que uma definição em termos de uma tabela de multiplicação. Claro que a tabela da multiplicação para as "unidades imaginárias" $i_1, i_2, \cdots, i_{2n+1}$ poderá ser obtida de (1.1.5.). Agora que definimos o processo de duplicação, é fácil ver que no começo dessa sessão nós obtivemos os octônios a partir da duplicação dos quatérnios.

1.2 SISTEMA DE NÚMEROS COMPLEXOS MAIS GERAIS

Definição: seja uma equação quadrática arbitrária e seu discriminante dadas por

$$x^2 + px + q = 0, \qquad (1.2.1.)$$

$$\Delta = p^2 - 4q. \qquad (1.2.2.)$$

Consideremos uma extensão do conjunto dos números reais $\mathbb{R}$ com um novo símbolo E que satisfaz a equação (1.2.1.) independentemente do sinal do discriminante (1.2.2.). O conjunto de todas as possíveis combinações lineares

$$a + bE, \text{ com } a,\ b \in \mathbb{R}$$

será chamado de sistema de números complexos mais gerais. A adição e a multiplicação são dadas

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

por:

$$(a + bE) + (c + dE) = (a + c) + (b + d)E$$

e

$$(a + bE)(c + dE) = ac + adE + bcE + bdE^2$$

$$= (ac - qbd) + (ad + bc - pbd)E, \qquad (1.2.3.)$$

sendo $E^2 = -pE - q$, no qual E é alguma raiz de (1.2.1.).

O fato de que (1.2.3.) contém dois números reais arbitrários p e q indica que encontraremos uma infinidade de sistemas de números. Mostraremos que cada um dos sistemas pode ser reduzido a um dos três casos:

1. Números $a + bE$, com $E^2 = -1$ (os números complexos);
2. Números $a + bE$, com $E^2 = 0$ (os números duais);
3. Números $a + bE$, com $E^2 = 1$ (os números duplos).

Prova:

Caso 1: $\Delta = p^2 - 4q < 0.$

Entre os números da forma $a + bE$ existem os números $i = \alpha + \beta E$ tais que $i^2 = -1$. De fato, sejam $\alpha = \frac{p}{-\Delta^{\frac{1}{2}}}$ e $\beta = \frac{2}{-\Delta^{\frac{1}{2}}}$. Logo,

$$\left(\frac{p}{-\Delta^{\frac{1}{2}}} + \frac{2}{-\Delta^{\frac{1}{2}}}E\right)^2$$

$$= \frac{p^2 + 4pE + 4E^2}{-\Delta}$$

$$= \frac{p^2 + 4pE + 4(-pE - q)}{-\Delta}$$

$$= \frac{p^2 + 4pE - 4pE - 4q}{-\Delta}$$

$$= \frac{\Delta}{-\Delta} = -1,$$

quando $E = \alpha_1 + \beta_1 i$, com $\alpha_1 = \frac{-p}{2}$ e $\beta_1 = \frac{-\Delta^{\frac{1}{2}}}{2}$. Segue que todo número $a + bE$ pode ser identificado a um número complexo qualquer, da forma

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$a + bE = a + b\left(\frac{-p}{2} + \frac{\left(-\Delta^{\frac{1}{2}}\right)}{2}i\right)$$

$$= \left(a - \frac{bp}{2}\right) + \frac{1}{2}\left(-\Delta^{\frac{1}{2}}\right)bi.$$

Caso 2: $\Delta = p^2 - 4q = 0.$

Similarmente, entre os números da forma $a + bE$ existem números $\varepsilon = \alpha + \beta E$ tais que $\varepsilon^2 = 0$; é possível, por exemplo, colocar $\varepsilon = \frac{p}{2} + E$ tal que

$$\varepsilon^2 = \left(\frac{p}{2} + E\right)^2$$

$$= \frac{p^2}{4} + pE + E^2$$

$$= \frac{p^2}{4} + pE - pE - q$$

$$= \frac{p^2 - 4q}{4} = 0,$$

já que $p^2 - 4q = 0$, por hipótese. Assim, o sistema de números $a + bE$ sempre poderá ser reduzido aos chamados números duais

$$a + bE, \text{ com } a,\ b \in \mathbb{R},\ \varepsilon^2 = 0,$$

quando $E = a_1 + b_1\varepsilon$, com $a_1 = -\frac{p}{2}$ e $b_1 = 1$. Segue que todo número $a + bE$ pode ser identificado com um número dual qualquer

$$a + bE = a + b\left(-\frac{p}{2} + 1\varepsilon\right)$$

$$= \left(a + -\frac{p}{2}b\right) + b\varepsilon.$$

Caso 3: $\Delta = p^2 - 4q > 0.$

Existem números da forma $e = a + bE$ tais que $e^2 = 1$. De fato, ponha $e = \frac{p}{\Delta^{\frac{1}{2}}} + \frac{2}{\Delta^{\frac{1}{2}}}E$ tal que

$$e^2 = \left(\frac{p}{\Delta^{\frac{1}{2}}} + \frac{2}{\Delta^{\frac{1}{2}}}E\right)^2$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$= \frac{p^2 + 4pE + 4E^2}{\Delta}$$

$$= \frac{p^2 + 4pE + 4(-pE - q)}{\Delta}$$

$$= \frac{p^2 + 4pE - 4pE - 4q}{\Delta}$$

$$= \frac{\Delta}{\Delta} = 1.$$

Isso nos permite reduzir nosso sistema de números complexos mais gerais aos chamados números duplos:

$$a + be, \text{ com } a,\ b \in \mathbb{R},\ e^2 = 1,$$

quando $E = c_1 + d_1 e$, com $c_1 = \frac{-p}{2}$ e $d_1 = \frac{\Delta^{\frac{1}{2}}}{2}$. Segue que todo número $a + bE$ pode ser identificado com um número duplo qualquer

$$a + bE = a + b\left(\frac{-p}{2} + \frac{\Delta^{\frac{1}{2}}}{2}e\right)$$

$$= \left(a - b\frac{p}{2}\right) + \left(b\frac{\Delta^{\frac{1}{2}}}{2}\right)e.$$

2 RESULTADOS

Nesta seção apresentaremos as demonstrações dos teoremas de Frobenius e Hurwitz. Seja $\mathcal{A}$ uma álgebra de divisão associativa sobre os reais. As seguintes afirmações são válidas para $\mathcal{A}$:

Afirmação 2.1. A álgebra $\mathcal{A}$ tem uma identidade.

Prova:

Seja a um elemento não nulo da álgebra $\mathcal{A}$. Considere a equação

$$xa = a.$$

Como $\mathcal{A}$ é uma álgebra de divisão, a equação acima possui uma única solução e, isto é, $ea = a$. Multiplicando esta equação à esquerda por b obtemos $b(ea) = ba$, como a álgebra $\mathcal{A}$ é associativa, então $(be)a = ba$. Temos também que a equação $xa = ba$ possui uma única solução, logo

$$be = b.$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Agora considere equação

$$ax = a.$$

De maneira análoga, como $\mathcal{A}$ é uma álgebra de divisão, a equação acima possui uma única solução e, isto é, $ae = a$. Multiplicando esta equação à direita por c obtemos $(ae)c = ac$, como a álgebra $\mathcal{A}$ é associativa então $a(ec) = ac$. Temos também que a equação $ax = ac$ possui uma única solução, logo

$$ec = c.$$

Já que b e c são elementos arbitrários, as equações $be = b$ e $ec = c$ mostram que e é elemento identidade de $\mathcal{A}$. Usualmente, denotamos este elemento por 1.

Afirmação 2.2**.** Se um elemento $a \in \mathcal{A}$ não é proporcional a 1, então o conjunto de elementos C_α da forma

$$\alpha 1 + \beta a$$

forma uma subálgebra isomorfa a álgebra dos números complexos.

Prova:

Basta demonstrar que o elemento $a \in \mathcal{A}$ satisfaz uma equação quadrática

$$a^2 + sa + t1 = 0, \qquad (2.1.)$$

com discriminante negativo. De fato, (2.1) implica que $a^2 = -sa - t1$. Portanto, o conjunto dos elementos da forma $\alpha 1 + \beta\alpha$ é fechado para a multiplicação em $\mathcal{A}$. Logo, o conjunto C_a é uma subálgebra de $\mathcal{A}$ com dimensão 2. Como vimos na sessão (1.2), se $\Delta = s^2 - 4t < 0$, a subálgebra é isomorfa a álgebra dos números complexos. Seja n a dimensão da álgebra. Considere as $n + 1$ primeiras potências de a:

$$a^0 = 1, a^1, a^2, a^3, \cdots, a^n.$$

O sistema com $n + 1$ vetores é linearmente dependente, de modo que alguma potência deve ser combinação linear dos antecessores:

$$a^m = k_{m-1}a^{m-1} + \cdots + k_2a^2 + k_1a + k_0 1.$$

Em outras palavras, a é uma raiz da equação de grau m:

$$x^m - k_{m-1}x^{m-1} - \cdots - k_2a^2 - k_1a - k_0 1 = 0.$$

Considere em geral o polinômio de grau m:

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$P(x) = x^m - k_{m-1}x^{m-1} - \cdots - k_2x^2 - k_1x - k_0 1.$$

Tal polinômio pode ser escrito como um produto

$$P(x) = P_1(x)P_2(x)\cdots P_s(x) \qquad (2.2.)$$

de polinômios quadráticos lineares e irredutíveis (isto é, não é mais possível decompor cada $P_i(x)$, com $i \in \{1,2,\cdots,s\}$ em dois ou mais polinômios não constantes).

Para acompanhar o resto do argumento, devemos ter uma compreensão clara da igualdade (2.2.). Assim, cada um dos polinômios $P_1(x),\cdots,P_s(x)$ é uma soma de dois ou três termos:

$$x + t \text{ ou } x^2 + sx + t.$$

A igualdade (2.2.) afirma que, se multiplicarmos os polinômios $P_1(x),\cdots,P_s(x)$ usando a distribuição e a adição de polinômios, juntamente com o fato de que

$$x^k.x^l = x^{k+l},$$

reduzimos termos semelhantes e então encontramos $P(x)$. Lembre-se que a regra para trabalhar com as potências de a é a mesma para as potências dos desconhecidos x, ou seja,

$$a^k.a^l = a^{k+l},$$

pois $\mathcal{A}$ é uma álgebra associativa. Segue que, ao substituímos a por x na igualdade (2.2.), obtemos

$$P(a) = P_1(a)P_2(a)\cdots P_s(a).$$

Quando $P(a) = 0$ temos

$$P_1(a)P_2(a)\cdots P_s(a) = 0. \qquad (2.3.)$$

Agora usaremos o fato de $\mathcal{A}$ ser uma álgebra de divisão. Isto implica que o produto dos elementos sendo zero, pelo menos um deles é zero (sejam $u,\ v \in \mathcal{A}$, com $u \neq 0$ tais que $uv = 0$. Seja a equação $ux = 0$. Como $\mathcal{A}$ é uma álgebra de divisão, as equações $uv = 0$ e $ux = 0$ possuem as mesmas soluções, logo, $x = v = 0$). Aplicando a (2.3.), pelo menos para algum i vale

$$P_i(a) = 0,$$

isto é, o elemento a satisfaz uma equação linear ou quadrática. Se a satisfazer uma equação linear

$$a + t1 = 0,$$

então contrariamos a hipótese de a não ser proporcional a 1. Logo, a satisfaz uma equação quadrática irredutível (2.1.). Quando o polinômio $P_i(x)$ é irredutível, o discriminante é negativo (isto decorre do

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Teorema Fundamental da Álgebra, ou seja, todo polinômio com coeficientes complexos possui alguma raiz complexa).

Afirmação 2.3. Se dois elementos $a_1,\ a_2 \in \mathcal{A}$ não pertencem à mesma subálgebra C_a, então o conjunto Q_{a_1,a_2}de elementos da forma

$$\alpha 1 + \beta a_1 + \gamma a_2 + \delta a_1 a_2$$

é uma subálgebra isomorfa à álgebra dos quatérnios.

Para demonstrar essa afirmação, mostraremos que, se b_1 e b_2 são dois elementos cujos quadrados são -1, então

$$b_1 b_2 + b_2 b_1 = \lambda 1,$$

com λ sendo um número real.

Prova:

Na subálgebra C_{a_1}, escolhemos um elemento b_1 tal que $b_1^2 = -1$ (b_1 é a unidade imaginária da álgebra complexa C_{a_1}). Similarmente, na subálgebra C_{a_2}, escolhemos um elemento b_2 tal que $b_2^2 = -1$. Quando $b_1,\ b_2$ diferem, respectivamente, de $a_1,\ a_2$ por múltiplos de 1, segue que o conjunto dos elementos da forma $\alpha 1 + \beta a_1 + \gamma a_2 + \delta a_1 a_2$ coincide com o conjunto de elementos da forma $\alpha' 1 + \beta' a_1 + \gamma' a_2 + \delta' a_1 a_2$, isto é, Q_{a_1,a_2} coincide com Q_{b_1,b_2}. Além disso, se

$$e_1 = b_1,\ e_2 = k_1 b_1 + k_2 b_2 \text{ e } k_2 \neq 0,$$

então Q_{e_1,e_2} coincide com $Q_{b_1,\,b_2}$ e assim com Q_{a_1,a_2}. De fato, seja o conjunto dos elementos da forma $\alpha'' 1 + \beta'' e_1 + \gamma'' e_2 + \delta'' e_1 e_2$, o que implica que

$$\alpha'' 1 + \beta''(b_1) + \gamma''(k_1 b_1 + k_2 b_2) + \delta''(k_1 b_1 + k_2 b_2)$$

$$\Leftrightarrow \alpha'' 1 + (\beta'' + \gamma'' k_1 + \delta'' b_1 k_1) b_1 + (\gamma'' k_2) b_2 + (\delta'' k_2) b_1 b_2.$$

Mostraremos que é possível escolher números k_1 e k_2 de modo que

$$e_1^2 = -1,\ e_2^2 = -1 \text{ e } (e_1 e_2)^2 = -1. \qquad (2.4.)$$

A primeira das igualdades em (2.4.) vale para $k_1,\ k_2$ arbitrários. Por um lado, temos que

$$(b_1 + b_2)^2 = (b_1 + b_2)(b_1 + b_2) = b_1^2 + b_2^2 + (b_1 b_2 + b_2 b_1) = -2.1 + (b_1 b_2 + b_2 b_1),$$

e por outro lado, o quadrado de $b_1 + b_2$ pode ser escrito como uma combinação linear de 1 e $b_1 + b_2$:

$$(b_1 + b_2)^2 = p1 + q(b_1 + b_2).$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Portanto,

$$-2.1 + (b_1b_2 + b_2b_1) = p1 + q(b_1 + b_2) \Leftrightarrow b_1b_2 + b_2b_1 = 2.1 + p1 + q(b_1 + b_2).$$

Logo,

$$b_1b_2 + b_2b_1 = (2 + p).1 + q(b_1 + b_2). \qquad (2.5.)$$

Similarmente,

$$(b_1 + 2b_2)^2 = (b_1 + 2b_2)(b_1 + 2b_2) = b_1^2 + 4b_2^2 + 2(b_1b_2 + b_2b_1)$$
$$= -5.1 + 2(b_1b_2 + b_2b_1)$$

e

$$(b_1 + 2b_2)^2 = p'1 + q'(b_1 + 2b_2).$$

Assim,

$$-5.1 + 2(b_1b_2 + b_2b_1) = p'1 + q'(b_1 + 2b_2) \Leftrightarrow 2(b_1b_2 + b_2b_1)$$
$$= -5.1 + p'1 + q'(b_1 + 2b_2),$$

o que implica que

$$b_1b_2 + b_2b_1 = \frac{1}{2}(5 + p').1 + \frac{1}{2}q'(b_1 + 2b_2).$$

Supondo que $q \neq 0$ e igualando as duas expressões podemos deduzir que b_1 difere de b_2 por um múltiplo de 1, isto é, $b_2 \in C_{b_1}$. Mas isso está descartado por suposição, assim, $q = 0$ e a igualdade (2.5.) implica que

$$b_1b_2 + b_2b_1 + \lambda.1, \qquad (2.6.)$$

onde $\lambda = 2 + p$. Em outras palavras, se b_1 e b_2 são dois elementos cujos quadrados são -1, então teremos (2.6.) em mãos.

Agora é fácil determinar os elementos requeridos e_1 e e_2. Para isto, considere o elemento $c = \lambda b_1 + 2b_2$, onde λ tem o mesmo valor que em (2.5). Seja

$$c^2 = (\lambda b_1 + 2b_2)(\lambda b_1 + 2b_2)$$

$$= \lambda^2 b_1^2 + 4b_2^2 + 2\lambda(b_1b_2 + b_2b_1)$$

$$= -\lambda^2.1 - 4.1 + 2\lambda(b_1b_2 + b_2b_1)$$

$$= -\lambda^2.1 - 4.1 + 2\lambda^2.1$$

$$= (\lambda^2 - 4).1, \qquad (2.7.)$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

significando que $\lambda^2 - 4 < 0$. Se tivéssemos $p = \lambda^2 - 4 \geq 0$, então $c^2 = p1$, implicando que $\left(c - \sqrt{p}.1\right)\left(c + \sqrt{p}.1\right) = 0$, isto é, que $c = \sqrt{p}.1$ e $c = -\sqrt{p}.1$. Mas isto é impossível, pois b_1 e b_2 não pertencem a mesma subálgebra complexa.

Ponha $e_2 = \frac{1}{\sqrt{4-\lambda^2}}c$. Logo,

$$e_2^2 = \frac{c^2}{4-\lambda^2}$$

$$= \frac{\lambda^2 - 4}{4-\lambda^2} = -1.$$

Então (2.7.) implica que $e_2^2 = -1$, a segunda igualdade em (2.4.). Provamos a terceira igualdade notando que

$$e_1e_2 + e_2e_1 = 0. \qquad (2.8.)$$

De fato,

$$e_1e_2 + e_2e_1 = b_1\left(\frac{1}{\sqrt{4-\lambda^2}}\right)(\lambda b_1 + 2b_2) + \left(\frac{1}{\sqrt{4-\lambda^2}}\right)(\lambda b_1 + 2b_2)b_1$$

$$= \frac{\lambda b_1^2 + 2b_1b_2 + \lambda b_1^2 + 2b_2b_1}{\sqrt{4-\lambda^2}}$$

$$= \frac{\lambda(b_1^2 + b_1^2) + 2(b_1b_2 + b_2b_1)}{\sqrt{4-\lambda^2}}$$

$$= \frac{-2\lambda.1 + 2\lambda.1}{\sqrt{4-\lambda^2}} = 0.$$

Usando (2.8.), obtemos

$$(e_1e_2)^2 = (e_1e_2)(e_1e_2) = (e_1e_2)(-e_2e_1) = -(e_1e_2^2)e_1 = e_1^2 = -1. \qquad (2.9.)$$

Isto estabelece a terceira igualdade em (2.4.).

Agora mostraremos que o conjunto dos elementos Q_{e_1,e_2} da forma

$$\alpha_1 + \beta e_1 + \gamma e_2 + \delta e_1e_2$$

(que, como já mencionado anteriormente, coincide com Q_{a_1,a_2}) é uma subálgebra da álgebra $\mathcal{A}$.

Para isto é suficiente mostrar que o produto de dois dos quatro elementos

$$1,\ e_1,\ e_2,\ e_1e_2 \qquad (2.10.)$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

é uma combinação linear destes elementos. Para tanto, devemos verificar os produtos

$$e_1(e_1e_2),\ (e_1e_2)e_1,\ e_2(e_1e_2),\ (e_1e_2)e_2.$$

Temos que

$$e_1(e_1e_2) = (e_1e_1)e_2 = e_1^2e_2 = -e_2$$

$$(e_1e_2)e_1 = (-e_2e_1)e_1 = -e_2(e_1e_1) = -e_2e_1^2 = e_2$$

$$e_2(e_1e_2) = e_2(-e_2e_1) = -(e_2e_2)e_1 = -e_2^2e_1 = e_1$$

$$(e_1e_2)e_2 = e_1(e_2e_2) = e_1e_2^2 = -e_1. \qquad (2.11.)$$

Isto completa a prova de que Q_{a_1,a_2} é uma subálgebra.

Agora devemos mostrar que esta subálgebra é isomorfa a álgebra dos quatérnios. Primeiro, mostraremos que os elementos de (2.10.) formam uma base da subálgebra em questão e, em segundo, que a tabela da multiplicação desta base é a mesma tabela da multiplicação para a base $1, i, j, k$ da álgebra dos quatérnios. Por enquanto, sabemos que todo elemento de Q_{a_1,a_2} é uma combinação linear dos elementos de (2.10.). Para mostrar que esses elementos formam uma base, devemos mostrar que eles são linearmente independentes ou que nenhum desses elementos é combinação linear dos antecessores. O elemento e_2 não é uma combinação linear de 1 e e_1, isto decorre do fato de que e_1 e e_2 não pertencem a mesma subálgebra C_α. Assim, temos que mostrar que e_1e_2 não é uma combinação linear de 1, e_1 e e_2, isto é, que não podemos ter

$$e_1e_2 = pe_2 + qe_1 + r1. \qquad (2.12)$$

Suponha que a igualdade acima ocorra. Então p e q são diferentes de 0. De fato, se, digamos, $p = 0$, então multiplicando (2.12.) por e_1 pela esquerda, obtemos $-e_2 = -q.1 + re_1$, encontramos um absurdo, já que e_2 não pode ser combinação linear de e_1 e 1, como já comentado anteriormente. Multiplicando (2.12.) pela esquerda por e_1, obtemos

$$-e_2 = pe_1e_2 - q + re_1,$$

ou

$$e_1e_2 = -\frac{1}{p}e_2 - \frac{r}{p}e_1 + \frac{q}{p}.1.$$

A diferença das duas expressões para e_1e_2 é dada por

$$\left(p + \frac{1}{p}\right)e_2 + \left(q + \frac{r}{p}\right)e_1 + \left(r - \frac{q}{p}\right).1 = 0.$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

O coeficiente de e_2 deve ser o 0, pois de outra forma e_2 seria uma combinação linear de 1 e e_1. Logo,

$$p + \frac{1}{p} = 0 \Leftrightarrow p^2 + 1 = 0,$$

absurdo, pois é impossível encontrar um p real satisfazendo a última igualdade dada.

Portanto, demonstramos que os elementos $1,\ e_1,\ e_2,\ e_3$, com $e_3 = e_1e_2$ formam uma base para a álgebra $Q_{e_1,\,e_2}$.

Neste ponto, demonstrar o isomorfismo da subálgebra Q_{e_1,e_2}e a álgebra dos quatérnios $\mathbb{H}$, requer que mostremos que a tabela da multiplicação para a álgebra Q_{e_1,e_2} com a base

$$1,\ e_1,\ e_2,\ e_3$$

seja a mesma tabela de multiplicação para a álgebra dos quatérnios $\mathbb{H}$ com a base

$$1,\ i,\ j,\ k,$$

mas isto segue diretamente das relações (2.4.), (2.8), (2.11).

Um dos problemas clássicos da teoria das álgebras é o da determinação de todas as álgebras de divisão. Um resultado obtido recentemente é no sentido de que a dimensão de tal álgebra só poderá ser 1, 2, 4 ou 8.

Esse problema torna-se mais simples se impusermos alguma condição adicional à álgebra, como no resultado clássico, obtido em 1878 pelo matemático alemão Ferdinand Georg Frobenius (1849 - 1917), em que a condição adicional sobre a álgebra é que ela seja associativa.

Teorema 2.4. (Teorema de Frobenius - 1878). Toda álgebra de divisão associativa é isomorfa a uma das seguintes álgebras:

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

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

(iii) A álgebra $\mathbb{Q}$ dos números quatérnios.

Prova:

Seja $\mathcal{A}$ uma álgebra de divisão associativa. Pela Afirmação 2.1., a álgebra $\mathcal{A}$ tem identidade. Os elementos da forma $k1$ formam uma subálgebra $\mathcal{R}$ isomorfa a álgebra dos números reais. Se $\mathcal{R} \subsetneq \mathcal{A}$, então pela Afirmação 2.2., $\mathcal{A}$ contém uma subálgebra C_a isomorfa aos números complexos. Se $C_a \subsetneq \mathcal{A}$, pela Afirmação 2.3., $\mathcal{A}$ contém uma subálgebra $Q_{a,\,b}$ isomorfa a álgebra dos quatérnios. Se $Q_{a,b} = \mathcal{A}$, não temos mais nada o que fazer. Suponha $Q_{a,b} \subsetneq \mathcal{A}$, então $\mathcal{A}$ contém um elemento c

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

que não está em $Q_{a,\,b}$, mostraremos que $\mathcal{A}$ não será uma álgebra de divisão, entrando em contradição com a hipótese do Teorema 2.4.

Na álgebra dos quatérnios $Q_{a,b}$, escolhemos uma base $1, i, j, k$ com a tabela da multiplicação

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

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

e considere c como $p1 + qe$, com $e^2 = -1$ (e é uma "unidade imaginária" da álgebra complexa C_c).

Usando a associatividade de $\mathcal{A}$ e a relação (2.6.), reescreveremos ie. Assim,

$$ie = (jk)e = j(ke) = j(-ek + \lambda' 1) = j(-ek) + j\lambda' = -(je)k + \lambda' j = -(-ej + \lambda'' 1)k + \lambda' j = (ej)k - \lambda'' k + \lambda' j = e(jk) - \lambda'' k + \lambda' j = ei - \lambda'' k + \lambda' j.$$

e assim,

$$ie - ei = -\lambda'' k + \lambda' j.$$

Por (2.6.) também temos que

$$ie - ei = \lambda''' 1.$$

Adicionando as duas últimas igualdades acima obtemos $ie = \frac{1}{2}(\lambda''' 1 + \lambda' j - \lambda'' k)$, logo, é um elemento da álgebra $Q_{a,b}$. Então, também o é $ic = i(p1 + qe)$. Se c' é um elemento de $Q_{a,b}$, então o produto ic' também é elemento de $Q_{a,b}$. Mas isto é impossível, pois $\mathcal{A}$ é uma álgebra de divisão (a equação $ix = c$, com c não sendo de $Q_{a,\,b}$). Isto contradiz o Teorema de Frobenius. Aqui encerramos a demonstração.

Seja $\mathcal{A}$ uma álgebra de divisão normada com uma identidade e seja $\mathcal{U}$ uma subálgebra contendo 1 e diferente de $\mathcal{A}$.

Lema 2.5**.** A seguinte identidade vale em qualquer álgebra normada:

$$(a_1 b_1, a_2 b_2) + (a_1 b_2, a_2 b_1) = 2(a_1, a_2)(b_1, b_2). \qquad (2.13.)$$

Note que esta identidade conecta os quatro elementos $a_1,\ a_2,\ b_1,\ b_2$ da álgebra $\mathcal{A}$.

Prova:

No lugar de a para a identidade fundamental (1.1.), coloque $a_1 + a_2$. Temos que

$$\big((a_1 + a_2)b, (a_1 + a_2)b\big) = (a_1 + a_2, a_1 + a_2)(b, b)$$

ou, desenvolvendo, temos:

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$(a_1b + a_2b, a_1b + a_2b) = \big((a_1, a_1) + (a_2, a_2)\big)(b, b)$$

$$(a_1b + a_2b, a_1b) + (a_1b + a_2b, a_2b) = \big((a_1 + a_2, a_1) + (a_1 + a_2, a_2)\big)(b, b)$$

$$(a_1b, a_1b) + (a_2b, a_1b) + (a_1b, a_2b) + (a_2b, a_2b) = \big((a_1, a_1) + (a_2, a_1) + (a_1, a_2) + (a_2, a_2)\big)(b, b)$$

Ou seja,

$$(a_1b, a_1b) + (a_2b, a_2b) + 2(a_1b, a_2b) = (a_1, a_1)(b, b) + (a_2, a_2)(b, b) + 2(a_1, a_2)(b, b).$$

Pela identidade fundamental, o primeiro e segundo termos da esquerda da última igualdade acima são iguais, respectivamente, ao primeiro e segundo termos da direita. Assim,

$$(a_1b, a_2b) = (a_1, a_2)(b, b). \qquad (2.14.)$$

Para conseguirmos o resultado requerido, ponha $b_1 + b_2$ no lugar de b em (2.14.). Então teremos

$$\big(a_1(b_1 + b_2), a_2(b_1 + b_2)\big) = (a_1b_1 + a_1b_2, a_2b_1 + a_2b_2) = (a_1, a_2)(b_1 + b_2, b_1 + b_2)$$

ou

$$(a_1b_1, a_2b_1) + (a_1b_2, a_2b_2) + (a_1b_1, a_2b_2) + (a_1b_2, a_2b_1) = (a_1, a_2)(b_1, b_1) + (a_1, a_2)(b_2, b_2) + 2(a_1, a_2)(b_1, b_2)$$

Por (2.14.), a primeira e a segunda parcela são iguais do lado esquerdo, respectivamente, a primeira e a segunda do lado direito. Cancelando, obtemos a identidade (2.13.).

Lema 2.6. A seguinte identidade vale em qualquer álgebra normada com identidade

$$(ab)\overline{b} = (b, b)a. \qquad (2.15.)$$

Em outras palavras, o elemento $(a, b)\overline{b}$ é sempre proporcional a a e o coeficiente de proporcionalidade é (b, b).

Prova:

Primeiro notemos que, para provar a identidade (2.15.), é suficiente considerar o caso em que $b \perp 1$. De fato, seja b' um elemento da álgebra $\mathcal{A}$. Se representarmos

$$b' = k1 + b,$$

com $b \perp 1$, então $\overline{b} = -b$, e

$$(ab')\overline{b'} = \big(a(k1 + b)\big)(k1 - b) = k^2a - (ab)b = k^2a + (ab)\overline{b}.$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Se assumirmos a fórmula (2.15.) para o vetor b, então teremos

$$(ab')\overline{b'} = k^2a + (b,b)a = [k^2 + (b,b)]a = (b',b')a,$$

isto é, a fórmula (2.15.) para o vetor b'. Observe que a igualdade $b' = k1 + b$ implica que $(b',b') = (k1 + b, k1 + b) = k^2\,(1,1) + 2k(1,b) + (b,b)$. Temos que $2k(1,b) = 0$ e $(1,1) = 1$. Assim, provaremos a identidade (2.15.) se assumirmos que $b \perp 1$ (ou, equivalentemente, $\overline{b} = -b$). Também escreveremos λ para (b,b).

Considere o elemento

$$c = (ab)\overline{b} - \lambda a.$$

Mostraremos que $c = 0$ ou, equivalentemente, que

$$(c,c) = 0.$$

em vista das propriedades de produto escalar, temos

$$(c,c) = \Big((ab)\overline{b} - \lambda a, (ab)\overline{b} - \lambda a\Big) = \Big((ab)\overline{b}, (ab)\overline{b}\Big) + \lambda^2(a,a) - 2\lambda\Big((ab)\overline{b}, a\Big). \qquad (2.16.)$$

O lado direito é uma soma com três termos. Usando a igualdade fundamental (1.1.), simplificamos a primeira parcela

$$\Big((ab)\overline{b}, (ab)\overline{b}\Big) = (ab, ab)\big(\overline{b},\ \overline{b}\big)$$

$$= (a,a)(b,b)(-b,-b)$$

$$= (a,a)(b,b)^2$$

$$= \lambda^2(a,a).$$

Para simplificarmos a terceira parcela, usaremos a identidade (2.13.). Primeiro escreva como

$$(a_1b_1, a_2b_2) = 2(a_1,a_2)(b_1,b_2) - (a_1b_2, a_2b_1).$$

Nesta última identidade, coloque $a_1 = ab,\ b_1 = \overline{b},\ a_2 = a,\ b_2 = 1$, logo,

$$\Big((ab)\overline{b},\ a\Big) = 2(ab,\ a)\big(\overline{b},\ 1\big) - \big(ab,\ a\overline{b}\big).$$

Quando $b \perp 1$, a primeira soma é igual a 0, e a segunda é

$$-\big(ab, a\overline{b}\big) = (ab, ab) = (a,a)(b,b) = \lambda(a,a).$$

assim,

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

$$\big((ab)\overline{b}, a\big) = \lambda(a, a).$$

Agora, reescrevemos (2.16.):

$$(c, c) = \lambda^2(a, a) + \lambda^2(a, a) - 2\lambda^2(a, a) = 0,$$

que é o que desejávamos provar.

Uma consequência do Lema 2.6. é que podemos deduzir uma identidade a partir de (2.15.) muito importante para o que segue. Se no lugar de b em (2.15.) colocarmos $b = x + y$, obtemos

$$\big(a(x + y)\big)(\overline{x} + \overline{y}) = (x + y, x + y)a,$$

ou,

$$(ax)\overline{x} + (ay)\overline{y} + (ax)\overline{y} + (ay)\overline{x} = (x, x)a + (y, y)a + 2(x, y)a.$$

Em vista da identidade (2.15.) a primeira e segunda soma do lado esquerdo são iguais, respectivamente, a primeira e a segunda soma do lado direito. Portanto,

$$(ax)\overline{y} + (ay)\overline{x} = 2(x, y)a. \qquad (2.17.)$$

Esta é a igualdade que gostaríamos de estabelecer.

Afirmação 2.7**.** Existe um vetor unitário e que é ortogonal a $\mathcal{U}$, isto é, $(e, u) = 0$, para todo $u \in \mathcal{U}$. A representação dos elementos de $\mathcal{U} + \mathcal{U}e$ na forma

$$u_1 + u_2 e \qquad (2.18.)$$

é única, com $u_1,\ u_2 \in \mathcal{U}$.

Prova:

Lembremos que $\mathcal{U}$ é uma subálgebra da álgebra $\mathcal{A}$ contendo 1 e que não coincide com $\mathcal{A}$, e e é um vetor unitário ortogonal a $\mathcal{U}$. Primeiro, demonstraremos que os subespaços $\mathcal{U}$ e $\mathcal{U}e$ são ortogonais, isto é, $u_1 \perp u_2 e$ para quaisquer dois elementos $u_1,\ u_2 \in \mathcal{U}$. Usando o Lema 2.5., se colocarmos em (2.13.) $a_1 = u_1,\ b_1 = u_2,\ a_2 = e,\ b_2 = 1$, teremos

$$(u_1 u_2, e) + (u_1, u_2 e) = 2(u_1, e)(u_2, 1).$$

Agora, tenha em mente que $\mathcal{U}$ é uma subálgebra, de modo que $u_1 u_2 \in \mathcal{U}$. Mas então $u_1 \perp e,\ u_1 u_2 \perp e$. Segue que

$$(u_1, u_2 e) = 0,$$

isto é, $u_1 \perp u_2 e$. Isto significa que $\mathcal{U}$ e $\mathcal{U}e$ são ortogonais.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Agora, suponha que

$$u_1 + u_2 e = u_1' + u_2' e.$$

Então,

$$u_1 - u_1' = (u_2' + u_2)e.$$

Isto significa que $v = u_1 - u_1'$ está no subespaço $\mathcal{U}$ e $\mathcal{U}e$. Como estes subespaços são ortogonais, segue que $(v, v) = 0$ e, portanto, $v = 0$. Isto implica que $u_1 - u_1' = 0$ e $(u_2' - u_2)e = 0$. Na identidade (1.1.), quando $ab = 0$ temos que $a = 0$ ou $b = 0$. No nosso caso, $(u_2' - u_2)e = 0$ e $e \neq 0$ implica que $(u_2' - u_2) = 0$. Logo, $u_1 = u_1'$ e $u_2 = u_2'$.

Afirmação 2.8. O produto de dois elementos da forma (2.18.) é dado por

$$(u_1 + u_2 e)(v_1 + v_2 e) = (u_1 v_1 - \overline{v_2} u_2) + (v_2 u_1 + u_2 \overline{v_1})e. \qquad (2.19.)$$

Na expressão (2.19.), o termo $\overline{a}$ é definido, para um dado $a \in \mathcal{A}$, da seguinte maneira: $a \in \mathcal{A}$ pode ser escrito de modo único como $a = k1 + a'$, onde 1 é a unidade de $\mathcal{A}$ e a' é ortogonal a 1. O conjugado de a é dado por $\overline{a} = k1 - a'$. A subálgebra $\mathcal{U} + \mathcal{U}e$ é isomorfa a álgebra duplicada $\mathcal{U}$.

Prova:

Devemos mostrar que se u e v são elementos da subálgebra $\mathcal{U}$, então

$$(ue)v = (u\overline{v})e, \qquad (2.20.)$$

$$u(ve) = (vu)e, \qquad (2.21.)$$

$$(ue)(ve) = -\overline{v}\, u, \qquad (2.22.)$$

Com estas relações comprovadas, podemos provar facilmente (2.19.). Seja

$$(u_1 + u_2 e)(v_1 + v_2 e) = u_1 v_1 + u_1(v_2 e) + (u_2 e)v_1 + (u_2 e)(v_2 e)$$

Se transformamos os últimos três termos da direita da igualdade acima de acordo com as fórmulas (2.20.), (2.21.), (2.22.), então obtemos a igualdade

$$(u_1 + u_2 e)(v_1 + v_2 e) = (u_1 v_1 - \overline{v_2} u_2) + (v_2 u_1 + u_2 \overline{v_1})e,$$

isto é, a fórmula (2.19.). Para provar (2.20.), (2.21.) e (2.22.), usaremos a identidade (2.17.),

$$(ax)\overline{y} + (ay)\overline{x} = 2(x, y)a.$$

Se supusermos as identidades

$$a = u,\ x = e,\ y = \overline{u},$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

e tivermos em mente que $\overline{u} \perp e$, então teremos

$$(ue)v + (u\overline{v})\overline{e} = 2(e, \overline{v})u = 0.$$

Quando $\overline{e} = -e$ (para $e \perp 1$), obtemos a fórmula (2.20.).

Para provar (2.21), suponha em (2.17.) que

$$\alpha = 1,\ x = u,\ y = \overline{v}e.$$

Quando $\overline{ve} = -ve$ ($ve \perp \mathcal{U}$, isto é, $ve \perp 1$), segue que

$$u(ve) - (ve)\overline{u} = 0.$$

Usando (2.20.) obtemos

$$u(ve) = (ve)\overline{u} = (vu)e.$$

Para provarmos (2.22.) usaremos a seguinte observação: se $v = c$ e $v = d$, então $v = c + d$. Quando todo elemento v pode ser escrito como uma soma de dois termos no qual uma é proporcional a 1 e a outra é ortogonal a 1, para provar (2.22.) é suficiente considerarmos dois casos: quando $v = k1$ e $v \perp 1$. Se $v = k1$, então a fórmula (2.22.) torna-se

$$k(ue)e = -ku,$$

uma identidade cuja validade está implícita por (2.15.).

Agora suponha $v \perp 1$ (de modo que $\overline{v} = -v$). Se em (2.17.) tivermos

$$a = u,\ x = e,\ y = -ku,$$

Então,

$$(ue)(ve) - \big(u(ve)\big)\overline{e} = -2(e, ve)u.$$

Pela identidade (2.14.), (e, ve) equivale a $(1, v)(e, e)$, isto é, 0. Portanto, por (2.21.), o segundo termo do lado esquerdo é igual a $-\big(u(ve)\big)\overline{e} = -vu = \overline{v}\,u$. Logo,

$$(ue)(ve) = -\overline{v}\,u,$$

como queríamos provar. Assim, provando (2.20.), (2.21.), (2.22.) demonstramos (2.19.).

Afirmação 2.9. Toda subálgebra contendo 1 e diferente de $\mathcal{A}$ é associativa.

Prova:

Usando (2.17.) e impondo que

$$a = ve,\ x = \overline{w},\ y = \overline{u}e,$$

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

temos que

$$\big((ve)\overline{w}\big)(-\overline{u}\,e) + \big((ve)(\overline{u}\,e)\big)w = 2(\overline{w},\overline{u}e)ve = 0,$$

pois $(\overline{w},\overline{u}e) = 0$. Usando (2.20.) e (2.22.) temos que

$$\big((vw)e\big)(-\overline{u}\,e) - (uv)w = 0,$$

$$u(vw) - (uv)w = 0.$$

Teorema 2.10. (Teorema de Hurwitz - 1896). Toda álgebra normada de divisão com identidade é isomorfa a uma das seguintes álgebras:

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

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

(iii) A álgebra $\mathbb{Q}$ dos números quatérnios;

(iv) A álgebra $\mathbb{O}$ dos números octônios.

Prova:

Seja $\mathcal{U}$ uma subálgebra da álgebra $\mathcal{A}$ contendo 1 e diferente de $\mathcal{A}$. Pela Afirmação 2.7., a representação do conjunto dos elementos na forma da identidade (2.18.) é única e pela Afirmação 2.8., este conjunto é fechado para a multiplicação, sendo assim uma subálgebra de $\mathcal{U}$, denotada por $\mathcal{U} + \mathcal{U}e$. O processo de construção da álgebra $\mathcal{U} + \mathcal{U}e$ a partir da álgebra $\mathcal{U}$ é chamado duplicação e a álgebra $\mathcal{U} + \mathcal{U}e$ é chamada $\mathcal{U}$ duplicada. Uma vez que contém um elemento de identidade 1, a álgebra $\mathcal{A}$ contém uma subálgebra de elementos da forma $k1$ que é isomorfa à álgebra de números reais e será denotada por $\mathcal{R}$. Se no argumento anterior substituímos $\mathcal{U}$ por $\mathcal{R}$, então e será um vetor unitário e ortogonal a 1. Pela fórmula (2.19.),

$$e^2 = (0 + 1e)(0 + 1e) = -1.$$

Isto implica que o quadrado de um vetor a a' ortogonal a 1 é $\lambda 1$, com $\lambda 1 \leq 0$. Por outro lado, se o quadrado de um elemento é $\lambda 1$ e $\lambda 1 \leq 0$, então este elemento é ortogonal a 1 (de fato, seja o quadrado de um elemento que não é ortogonal a 1, isto é, um elemento da forma $a = k1 + a'$, com $k \neq 0$ e a $a' \perp 1$ e $(k1 + a')(k1 + a') = k^2\,1 + a'^2 + 2ka' = k^2 1 + \mu 1 + 2ka'$. Se este elemento for proporcional a 1, então segue que $a' = 0$ e então $a = k1$. Mas o quadrado do último elemento não é igual a $\lambda 1$, com $\lambda \leq 0$).

Considere mais uma vez a subálgebra $\mathcal{R}$. Se $\mathcal{R} \neq \mathcal{A}$, então existe um vetor unitário e ortogonal a $\mathcal{R}$. Considere a subálgebra $\mathcal{C} = \mathcal{R} + \mathcal{R}e$. Como $\mathcal{C}$ é uma álgebra $\mathcal{R}$ duplicada, esta é isomorfa a álgebra dos números complexos. A partir do que foi dito sobre a conjugação da álgebra $\mathcal{A}$,

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

segue que para os elementos de $\mathcal{C}$ a conjugação coincide com a conjugação usual dos números complexos. Se a subálgebra $\mathcal{C}$ não coincidir com $\mathcal{A}$, então existe um vetor unitário e', ortogonal a $\mathcal{C}$. A subálgebra $\mathcal{Q} = \mathcal{C} + \mathcal{C}e'$, a duplicada de $\mathcal{C}$, é isomorfa à álgebra dos quatérnios. Nossa caracterização anterior da conjugação em $\mathcal{A}$ implica que os elementos de $\mathcal{Q}$ conjugados coincide com com a conjugação da álgebra dos quatérnios.

Se $\mathcal{Q} \neq \mathcal{A}$, escolhemos o vetor unitário ortogonal a $\mathcal{Q}$. A subálgebra $\mathcal{O} = \mathcal{Q} + \mathcal{Q}e''$, que é duplicada de $\mathcal{Q}$ e isomorfa à álgebra dos octônios. Esta álgebra deve coincidir com $\mathcal{A}$, pois, pela Afirmação 2.9., se não coincidisse, essa álgebra seria associativa, entrando em contradição com o fato de que a álgebra dos octônios não é associativa. Por sua vez, se a álgebra $\mathcal{A}$ não é isomorfa as álgebras $\mathcal{R}, \mathcal{C}, \mathcal{Q}$, então é isomorfa a álgebra $\mathcal{O}$, o que demonstra o Teorema de Hurwitz.

3 CONSIDERAÇÕES

Ao longo do desenvolvimento desse artigo foi possível compreender dois importantes resultados sobre álgebra de divisão reais associativas e também sobre álgebras de divisão normadas.

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.

KANTOR, I. L.; SOLODOVNIKOV, A. S. **Hypercomplex Numbers:** An elementary introduction to Algebras. New York: [s. n.], 1989.