X Bienal de Matemática 2024
Universidade Federal de São Carlos - UFSCar
29 de julho a 02 de agosto de 2024

Álgebras com divisão sobre os Reais e o Teorema de Frobenius [1]

Bussola, Pedro Augusto [2];Gonçalves, Dimas José (orientador) [3]

Resumo: *Neste trabalho será apresentado o Teorema de Frobenius. Mais especificamente, será mostrado que toda álgebra com divisão associativa de dimensão finita sobre o corpo dos Reais é isomorfa aos Reais ou Complexos ou Quatérnions.*

Palavras-chave: *Teorema de Frobenius, álgebras com divisão sobre os Reais.*

1. Introdução

O assunto a ser tratado neste trabalho está inserido dentro da área de álgebra, ou mais especificamente, dentro da teoria de anéis associativos. As álgebras com divisão de dimensão finita são objetos simples e reúnem os aspectos e propriedades mais favoráveis dentro da teoria. Como muitas vezes acontece, os objetos mais simples não são os mais fáceis de estudar, e os temas clássicos não são menos profundos que os modernos.

Duas álgebras com divisão sobre $\mathbb{R}$ são bem conhecidas desde o ensino básico: $\mathbb{R}$ e $\mathbb{C}$. Uma outra álgebra não tão conhecida é a dos quatérnions, denotada por $\mathbb{H}$. Essa foi descoberta pelo matemático Hamilton durante a tentativa de extensão de $\mathbb{C}$, e trata-se da primeira álgebra com divisão sobre $\mathbb{R}$ não comutativa.

Podemos nos perguntar: além das 3 álgebras citadas, existe outra álgebra com divisão associativa de dimensão finita sobre $\mathbb{R}$? A resposta será dada neste trabalho.

2. Pré-Requisito

Um espaço vetorial $(A, +, \cdot)$ sobre um corpo $\mathbb{F}$ é uma álgebra sobre $\mathbb{F}$ se existe uma operação binária $* : A \times A \to A$, chamada multiplicação, que satisfaz

$$(x+y)*z = x*z+y*z, \ z*(x+y) = z*x+z*y \ \text{ e}$$

$$\lambda \cdot (x*y) = (\lambda \cdot x)*y = x*(\lambda \cdot y)$$

para todos $x, y, z \in A$ e $\lambda \in \mathbb{F}$. Com a condição

$$x*(y*z) = (x*y)*z$$

para todos $x, y, z \in A$, dizemos que A é uma álgebra associativa.

Por exemplo, $\mathbb{R}$, $\mathbb{C}$ e $M_n(\mathbb{R})$ com as operações usuais de soma, produto por escalar e multiplicação são álgebras associativas sobre $\mathbb{R}$. Porém $\mathbb{R}$ e $\mathbb{C}$ têm uma propriedade a mais, que definimos a seguir.

Uma álgebra A sobre um corpo $\mathbb{F}$ é chamada de álgebra com divisão se:

(a) A tem um elemento, denotado por 1, com a propriedade

$$1*x = x = x*1 \text{ para todo } x \in A,$$

(b) todo $x \in A$ tem um elemento, denotado por x^{-1}, tal que

$$x*x^{-1} = 1 = x^{-1}*x.$$

Sejam A e A' álgebras sobre um corpo $\mathbb{F}$. Uma função $\phi : A \to A'$ é chamada homomorfismo de álgebras se satisfaz as seguintes propriedades:

$$\phi(x+y) = \phi(x)+\phi(y), \quad \phi(\lambda x) = \lambda\phi(x) \ \text{ e } \ \phi(x*y) = \phi(x)*\phi(y)$$

para todo $x, y \in A$ e $\lambda \in \mathbb{F}$. Um homomorfismo bijetivo é chamado de isomorfismo.

3. Resultados obtidos

Assumimos que D é uma álgebra associativa com divisão de dimensão finita n sobre $\mathbb{R}$. Encontraremos todos os n possíveis para os quais tal álgebra existe e, além disso, todas as multiplicações possíveis que transformam um espaço vetorial real de dimensão finita em uma álgebra com divisão.

Lema 4.1 *Para todo $x \in D$, existe $\lambda \in \mathbb{R}$ tal que $x^2 + \lambda x \in \mathbb{R}$.*

A parte imaginária de $\mathbb{C}$ é o subespaço vetorial $\mathbb{R}i$, pode ser descrito como o conjunto de todos os $z \in \mathbb{C}$ tal que z^2 é um número real não positivo. Uma generalização para qualquer D consta no lema abaixo.

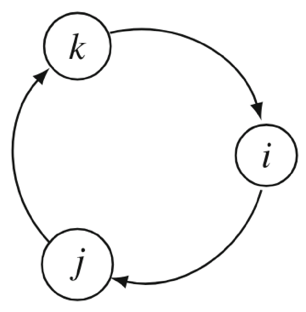
Lema 4.2 *O conjunto $V = \{v \in D| \ v^2 \in \mathbb{R}$ e $v^2 \leq 0\}$ é um subespaço vetorial de D. Além disso, $D = \mathbb{R} \oplus V$.*

Definimos $u \circ v := uv + vu$ para $u, v \in V$. Como $u \circ v = (u+v)^2 - u^2 - v^2$, segue do Lema 4.2 que $u \circ v \in \mathbb{R}$. Se $v \neq 0$, então $v \circ v = 2v^2 \neq 0$. A partir dessa nova operação definimos o seguinte produto interno $\langle \ , \ \rangle$ em V: $(u, v) \mapsto \langle u, v\rangle = -\frac{1}{2}\, u \circ v$.

Lema 4.3 *Se $n > 2$, então existem $i, j, k \in D$ tais que*

$$\begin{aligned} i^2 = j^2 = k^2 = -1, \\ ij = -ji = k, \ ki = -ik = j, \ jk = -kj = i \end{aligned} \tag{1}$$

e $1, i, j, k$ são linearmente independentes. As relações em (1) podem ser representadas pelo diagrama



Demonstração: O Lema 4.2 mostra que V tem dimensão $n-1 > 1$. Portanto, podemos escolher $v, w \in V$ linearmente independentes. Defina $u := w - \frac{w \circ v}{v \circ v} v$ pelo processo de Gram–Schmidt. Observe que $u \neq 0$ e $u \circ v = 0$. Defina $i := \frac{u}{\sqrt{-u^2}}$, $j := \frac{v}{\sqrt{-v^2}}$ e $k := ij$. É fácil verificar que as relações em (1) são satisfeitas, das quais obtemos que

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$$

é um número real positivo para quaisquer $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$ que não sejam todos zero. Isso prova, em particular, que $1, i, j, k$ são linearmente independentes. $\square$

A notação padrão para esta álgebra com divisão real não comutativa de dimensão 4 é $\mathbb{H}$, em homenagem ao seu descobridor, o matemático irlandês W. R. Hamilton. Os elementos de $\mathbb{H}$ são chamados de quatérnions. Faremos apenas um passo da análise que $\mathbb{H}$ é uma álgebra com divisão: Defina o conjugado de $\mathbf{h} = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ em $\mathbb{H}$ por

$$\bar{\mathbf{h}} = a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}.$$

Se $\mathbf{h} \neq 0$, então $\mathbf{h}\bar{\mathbf{h}} (= \bar{\mathbf{h}}\mathbf{h})$ é um escalar não nulo como mostrado anteriormente. Portanto, $\mathbf{h}$ é invertível com inverso $\mathbf{h}^{-1} = \frac{\bar{\mathbf{h}}}{\mathbf{h}\bar{\mathbf{h}}}$. Assim, $\mathbb{H}$ é uma álgebra com divisão.

Teorema 4.1 *Se D é uma álgebra associativa com divisão de dimensão finita sobre $\mathbb{R}$, então D é isomorfa a $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$.*

Demonstração: Se $n = 1$, então $D \cong \mathbb{R}$. Se $n = 2$, então $V \neq 0$ pelo Lema 4.2, de modo que D contém um elemento i tal que $i^2 = -1$; mas então $D \cong \mathbb{C}$. Pelo Lema 4.3 sabemos que $n \neq 3$ e que $D \cong \mathbb{H}$ se $n = 4$.

Suponha $n > 4$. Sejam i, j, k os elementos do Lema 4.3. Como a dimensão de V é $n-1$, existe $v \in V$ tal que v, i, j, k são linearmente independentes. Utilizando o processo de Gram–Schmidt,

$$e := v + \frac{i \circ v}{2} i + \frac{j \circ v}{2} j + \frac{k \circ v}{2} k$$

é um elemento não nulo em V e satisfaz $i \circ e = j \circ e = k \circ e = 0$. No entanto, das duas primeiras identidades, concluímos $eij = -iej = ije$, o que contradiz a terceira identidade, pois $ij = k$. Assim, n só pode ser 1, 2 ou 4. $\square$

Agora podemos nos perguntar: Quais são todas as álgebras associativas com divisão de dimensão finita sobre o corpo dos complexos? O próximo resultado é a resposta para esta pergunta num contexto mais geral.

Teorema 4.2 *Se D é uma álgebra associativa com divisão de dimensão finita sobre um corpo algebricamente fechado $\mathbb{F}$, então $D = \mathbb{F}$.*

Demonstração: Seja $x \in D$, e $dim \ D = n$. Assim, tem-se que $A = \{1, x, \ldots x^n\}$ é linearmente dependente, visto que A tem $n+1$ elementos. Com efeito, existe $f(\omega) \in \mathbb{F}[\omega]$ não nula, com grau menor ou igual a n tal que $f(x) = 0$, assumindo que o coeficiente líder seja 1. Como $\mathbb{F}$ é algebricamente fechado, pode-se fatorar $f(\omega)$ da forma

$$f(\omega) = (\omega - \alpha_1) \ldots (\omega - \alpha_r)$$

com $\alpha_i \in \mathbb{F}$, $i \in \{1, \ldots, r\}$. Analogamente, $f(x) = (x - \alpha_1) \ldots (x - \alpha_r)$. Como $f(x) = 0$ e D é uma álgebra de divisão então $x - \alpha_i = 0$ para algum $i \in \{1, \ldots, r\}$. Portanto, $x = \alpha_i \in \mathbb{F}$. $\square$

4. Conclusão

No trabalho apresentado fornecemos uma base fundamental para o estudo das álgebras associativas. Primeiramente, são abordados os conceitos preliminares, incluindo definições e exemplos básicos que ilustram o conceito de álgebra. Em seguida, é apresentado o Teorema de Frobenius, um resultado crucial que classifica as álgebras associativas com divisão reais de dimensão finita. O teorema demonstra que tal álgebra é isomorfa a um dos três casos: os números reais $\mathbb{R}$, os números complexos $\mathbb{C}$, ou os quatérnions $\mathbb{H}$, respondendo assim a pergunta inicial.

Referências

[1] BRESAR, M. Introduction to Noncommutative Algebra. [S.l.]: Springer, 2014. (Universitext). ISBN 978-3-319-08692-7.

Apoio: FAPESP

[1] Este trabalho foi apoiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Processo 2023/10439-1.
[2] Universidade Federal de São Carlos. Este autor foi apoiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Processo 2023/10439-1.
[3] Universidade Federal de São Carlos.