Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas

Uma Introdução às Álgebras com Identidades Polinomiais

Trabalho de Conclusão de Curso

Ricardo David Morais da Silva

Florianópolis, 2013

Ricardo David Morais da Silva

Uma Introdução às Álgebras com Identidades Polinomiais

Trabalho de Conclusão de Curso apresentado ao Curso de Matemática do Departamento de Matemática do Centro de Ciências Físicas e Matemáticas da Universidade Federal de Santa Catarina para obtenção do grau de Licenciado em Matemática.

Orientadora:
Prof.ª Dr.ª Alda Dayana Mattos Mortari

Universidade Federal de Santa Catarina

Florianópolis

2013

Esta monografia foi julgada adequada como TRABALHO DE CONCLUSÃO DE CURSO no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº 32/CCM/2013.

Prof. Silvia Martini de Holanda Janesch
Coordenadora do Curso de Graduação em Matemática

Banca Examinadora:

Prof.ª Dr.ª Alda Dayana Mattos Mortari
Orientadora

Prof. Dr. Giuliano Boava

Prof.ª Ma. Carmem Suzane Comitre Gimenez

Índice

Introdução

O objetivo principal deste trabalho é definir e exemplificar álgebras e álgebras com identidades polinomiais. Uma álgebra consiste em um conjunto não vazio munido de três operações: soma, produto e produto por escalar, em que estas operações estão sujeitas a algumas regras. Se uma álgebra tem a propriedade de que existem polinômios, em um conjunto de variáveis, que se anulam quando avaliados em quaisquer elementos da álgebra, então estes polinômios são denominados identidades polinomiais para a álgebra em questão.

Apresentamos uma disposição geral de nosso trabalho. No primeiro capítulo, apresentamos um estudo preliminar para o entendimento das álgebras e das álgebras com identidades polinomiais. Nesse capítulo estudamos os principais conceitos, propriedades e resultados das estruturas e das subestruturas de: grupos, anéis e espaços vetoriais, afim de usá-los no capítulo 2. Entre os conceitos comentados estão os de grupos, anéis e espaços vetoriais quocientes, conceitos esses importantes para o entendimento do, não menos importante, teorema do homomorfismo, que apresentamos em cada estrutura uma versão do mesmo.

No segundo e último capítulo, definimos formalmente a estrutura de álgebra e estudamos algumas de suas subestruturas, como subálgebras e ideais de álgebras. Veremos que uma álgebra é uma estrutura que, com relação às operações de soma e produto, se comporta como um anel e com relação às operações de soma e produto por escalar, se comporta como um espaço vetorial. Um dos exemplos de álgebras é o conjunto dos polinômios em um conjunto de variáveis, com as operações usuais de polinômios que denotaremos por $\mathbb{K}\langle X\rangle$. Veremos também o teorema do homomorfismo para álgebras.

Também estudamos nesse último capítulo, as álgebras com identidades polinomiais que, como já dito, são polinômios que quando avaliados em quaisquer elementos da álgebra se anulam. Um dos exemplos de álgebras com identidades polinomais é a chamada álgebras de Grassmann. No conjunto dos polinômios iremos definir um polinômio chamado de comutador que será uma identidade polinomial para a álgebra de Grassmann. A partir do chamado polinômio standard, veremos que todas as álgebras finitas são álgebras com identidades polinomiais.

Mostraremos ainda, que o conjunto de todas as identidades polinomiais de uma álgebra $\mathcal{A}$, denotado por $\mathrm{T}(\mathcal{A})$, é um ideal da álgebra dos polinômios $\mathbb{K}\langle X\rangle$, que chamaremos de T-ideal de $\mathcal{A}$. Apresentamos um resultado que mostra que o T-ideal $\mathrm{T}(\mathcal{A})$ é finitamente gerado. Para finalizar apresentamos algumas perguntas a respeito dos T-ideais e veremos que existem perguntas que ainda não foram respondidas sobre os mesmos.

1 Estruturas Algébricas

Uma estrutura algébrica é formada por um conjunto não vazio, munido de uma ou mais operações, em que estas operações estão sujeitas a algumas regras. Dependendo da estrutura algébrica, algumas operações são entre elementos do conjunto principal e elementos de um conjunto externo, denominado conjunto de escalares. Nesse capítulo, estudaremos um pouco das estruturas algébricas como: **Grupos**, **Anéis** e **Espaços Vetoriais**, que são fundamentais para o entendimento das **Álgebras** e das **Álgebras com Identidades Polinomiais**, estruturas que definiremos no próximo capítulo.

1.1 Grupos

Em 1824 o matemático norueguês Niels Henrik Abel (1802-1829) provou que não há uma fórmula geral por radicais para resolver as equações polinomiais de graus maiores ou iguais a 5. Dessa maneira, surge uma questão: "Por que algumas equações algébricas com graus maiores ou iguais a 5 são solúveis por radicais e outras não?". A resposta para essa pergunta foi dada pelo matemático francês Evariste Galois (1811-1832). Galois associou a cada equação um grupo formado por permutações de suas raízes e condicionou a resolubilidade por radicais a uma propriedade desse grupo. Surge assim, a *teoria de Galois* que, grosso modo, procura descrever as simetrias das equações satisfeitas pelas soluções de uma equação polinomial; e essa é a origem histórica do conceito de grupos. Com o tempo, a ideia de grupos se mostrou um instrumento muito importante para a organização e o estudo de várias partes da matemática.

Definição 1.1. *Um* grupo *é um par ordenado* $(G, *)$*; em que* G *é um conjunto não vazio, munido de uma operação denotada por* $*$*, tal que para todo* $x, y, z \in G$*, as seguintes condições são satisfeitas:*

G1*:* $(x * y) * z = x * (y * z)$ *(associatividade);*

G2*: Existe um elemento* $e \in G$*, tal que* $e * x = x * e = x$ *(existência do elemento neutro);*

***G3**: Para cada elemento $x \in G$, existe $x' \in G$, tal que $x * x' = x' * x = e$ (existência do elemento simétrico).*

***Observação:** A operação $*$ é uma função do tipo:*

$$\begin{array}{rccc} * : & G \times G & \to & G \\ & (x, y) & \mapsto & x * y. \end{array}$$

Quando a operação do grupo é uma soma conhecida, dizemos que $(G, +)$ é um *grupo aditivo*. O mesmo acontece quando a operação é uma multiplicação conhecida, neste caso dizemos que $(G, \cdot)$ é um *grupo multiplicativo*. Quando ficar subentendida a existência da operação, vamos nos referir ao grupo $(G, *)$ simplesmente por *grupo G*.

Exemplo 1.2. *$(M_2(\mathbb{R}), +)$ é um grupo, em que a operação $+$ é a soma usual de matrizes.*

Obviamente, a operação $+$ é fechada em $M_2(\mathbb{R})$.

Sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ e $C = \begin{pmatrix} c_{11} & a_{12} \\ c_{21} & c_{22} \end{pmatrix} \in M_2(\mathbb{R})$ quaisquer.

Associatividade:

$$\begin{aligned} A + (B + C) &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \left[\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & a_{12} \\ c_{21} & c_{22} \end{pmatrix} \right] \\ &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} + c_{11} & b_{12} + c_{12} \\ b_{21} + c_{21} & b_{22} + c_{22} \end{pmatrix} \end{aligned}$$

$$\begin{aligned} &= \begin{pmatrix} a_{11} + (b_{11} + c_{11}) & a_{12} + (b_{12} + c_{12}) \\ a_{21} + (b_{21} + c_{21}) & a_{22} + (b_{22} + c_{22}) \end{pmatrix} \\ &= \begin{pmatrix} (a_{11} + b_{11}) + c_{11} & (a_{12} + b_{12}) + c_{12} \\ (a_{21} + b_{21}) + c_{21} & (a_{22} + b_{22}) + c_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix} + \begin{pmatrix} c_{11} & a_{12} \\ c_{21} & c_{22} \end{pmatrix} \\ &= \left[\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right] + \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} = (A + B) + C. \end{aligned}$$

Observe que nesta demonstração foi usada a associatividade da soma dos números reais.

Existência do elemento neutro: Considere a matriz nula $E = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$.

Assim temos:

$$A + E = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}+0 & a_{12}+0 \\ a_{21}+0 & a_{22}+0 \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A = \begin{pmatrix} 0+a_{11} & 0+a_{12} \\ 0+a_{21} & 0+a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = E + A.$$

Logo, E é o elemento neutro.

Existência do elemento simétrico: Seja $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R})$ qualquer e tome $A' = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$. Assim, temos

$$A + A' = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} = \begin{pmatrix} a_{11}-a_{11} & a_{12}-a_{12} \\ a_{21}-a_{21} & a_{22}-a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = E \quad \text{e}$$

$$A' + A = \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix} + \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} -a_{11}+a_{11} & -a_{12}+a_{12} \\ -a_{21}+a_{21} & -a_{22}+a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = E.$$

.

Portanto, A' é o simétrico de A.

Mostramos assim que $(M_2(\mathbb{R}), +)$ é um grupo.

Definição 1.3. *Seja $(G, *)$ um grupo. Dizemos que $(G, *)$ é um* grupo abeliano *quando a operação $*$ é comutativa, ou seja, para quaisquer $x, y \in G$ temos:*
***G4**: $x * y = y * x$ (comutatividade).*

Exemplo 1.4. *$(M_2(\mathbb{R}), +)$ é um grupo abeliano.*

De fato, já mostramos no exemplo anterior que $(M_2(\mathbb{R}), +)$ é um grupo. Resta mostrarmos que vale a comutatividade. Para tanto, sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ $\in M_2(\mathbb{R})$ quaisquer.

Comutatividade:

$$A+B=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}+\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}=\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$
$$=\begin{pmatrix} b_{11}+a_{11} & b_{12}+a_{12} \\ b_{21}+a_{21} & b_{22}+a_{22} \end{pmatrix}=\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}+\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=B+A.$$

Observe que nesta demonstração foi usada a comutatividade da soma dos números reais.

Portanto, $(M_2(\mathbb{R}),+)$ é um grupo abeliano.

A seguir, mostraremos um exemplo de grupo que será importante para o nosso último capítulo, mas antes, precisamos entender um conceito necessário para o nosso exemplo.

Seja X um conjunto não vazio. Uma função bijetora $f : X \longrightarrow X$ é denominada *permutação* de X. Sejam $k \in \mathbb{N}^*$ e X_k um conjunto qualquer com k elementos, por exemplo, $X_k = \{1, 2, \ldots, k\}$. Denote por S_k o conjunto de todas as permutações de X_k.

Seja $\sigma \in S_k$ qualquer. Denotaremos essa permutação por $\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_k \\ b_1 & b_2 & \ldots & b_k \end{pmatrix}$ tal que para todo $i \in \{1, 2, \ldots, k\}$, $a_i = i$ e $\sigma(a_i) = b_i$.

Para melhor entendermos, considere $X_3 = \{1, 2, 3\}$. Como exemplo, considere também uma permutação $\sigma \in S_3$ tal que, $\sigma(1) = 3$; $\sigma(2) = 1$ e $\sigma(3) = 2$. Portanto, pela notação que usaremos temos $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Perceba que não se trata de uma matriz, mas sim, de uma notação que representa a permutação $\sigma \in S_3$.

Exemplo 1.5. *$(S_k, \circ)$ é um grupo, em que $\circ$ é a operação composição de funções, definida por*

$$\begin{array}{rccc} \circ : & S_k \times S_k & \longrightarrow & S_k \\ & (f, g) & \longmapsto & f \circ g, \end{array}$$

em que, para todo $x \in X_k$, $(f \circ g)(x) = f(g(x))$.

Note que se $f, g \in S_k$, então $f \circ g \in S_k$, pois a composição de duas bijeções é uma bijeção.

Para mostrarmos que duas funções são iguais, devemos mostrar que a lei de formação é a mesma e, além disso, devemos mostrar que seus domínios e contradomínios são iguais. No nosso caso, todas as funções possuem o mesmo domínio e contradomínio, logo basta mostrarmos que elas têm a mesma lei de formação. Para tanto, sejam $f, g, h \in S_k$ e

$x \in X_k$ quaisquer.

Associatividade:
$[f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = [(f \circ g) \circ h](x)$.

Logo,

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Existência do elemento neutro: Para todo $g \in S_k$ e $x \in X_k$, tome $f_e \in S_k$ tal que $f_e(x) = x$. Assim,

$$(g \circ f_e)(x) = g(f_e(x)) = g(x) \quad \text{e}$$

$$(f_e \circ g)(x) = f_e(g(x)) = g(x).$$

Logo, f_e é o elemento neutro.

Existência do elemento simétrico:
Seja $f \in S_k$ qualquer. Como f é bijetora, existe a função inversa $f^{-1} \in S_k$ tal que para todo $x \in X_k$,

$$\left(f \circ f^{-1}\right)(x) = f_e(x) = \left(f^{-1} \circ f\right)(x).$$

Assim,

$$f \circ f^{-1} = f^{-1} \circ f = f_e$$

e, portanto, f^{-1} é o simétrico de f.

Mostramos assim que $(S_k, \circ)$ é um grupo.

Observação: O grupo S_k é chamado de *grupo de permutações* ou de *grupo simétrico* do conjunto X_k.

Definição 1.6. *Seja* $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ b_1 & b_2 & \dots & b_k \end{pmatrix} \in S_k$ *qualquer. O* sinal *de* σ *é o número real, denotado por* $(-1)^\sigma$ *e definido por:*

$$(-1)^\sigma = \prod \frac{a_i - a_j}{b_i - b_j},$$

em que o produto é estendido a todos os pares (i, j) *de índices tais que* $i > j$.

Exemplo 1.7. *O sinal de* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ *é*

$$(-1)^\sigma = \frac{2-1}{3-2} \cdot \frac{3-1}{1-2} \cdot \frac{3-2}{1-3} = 1 \cdot (-2) \cdot \frac{1}{-2} = 1$$

Observação: Não iremos provar aqui, mas o sinal de uma permutação é sempre 1 ou -1.

1.1.1 Subgrupos

Definição 1.8. *Sejam* $(G, *)$ *grupo e* $H \subseteq G$ *não vazio. Dizemos que* H *é um* subgrupo *de* G *se:*
(*i*) H *é fechado com relação à operação* $*$*, ou seja, se* $x, y \in H$ *tem-se* $x * y \in H$*;*
(*ii*) $(H, *)$ *é um grupo.*

Lema 1.9. *Sejam* $(G, *)$ *um grupo,* $(H, *)$ *um subgrupo de* $(G, *)$ *e* $y \in H$ *qualquer. Então o inverso de* y *em* H *é o mesmo inverso de* y *em* G *e o elemento neutro de* H *é o mesmo elemento neutro de* G*.*

Demonstração. Seja $y \in H$ qualquer e denote por y'' o inverso de y em H e por y' o inverso de y em G. Vamos mostrar que $y'' = y'$. Denote e_H o elemento neutro de H e e_G o elemento neutro de G. Então,

$$\begin{aligned} y * y'' = e_H &= e_H * e_G = e_H * (y * y') \\ &= (e_H * y) * y' = y * y' \\ &\Rightarrow y' * (y * y'') = y' * (y * y') \\ &\Rightarrow (y' * y) * y'' = (y'y)y' \\ &\Rightarrow e_G * y'' = e_G * y' \Rightarrow y'' = y'. \end{aligned} \tag{1.1}$$

Também,

$$e_H = y * y'' = y * y' = e_G \Rightarrow e_H = e_G,$$

já que $y'' = y'$. Concluímos assim a demonstração.

■

Proposição 1.10. *Sejam* $(G, *)$ *grupo e* $H \subseteq G$ *não vazio.* H *é subgrupo de* G *se, e somente se, para quaisquer* $x, y \in H$ *tem-se* $x * y' \in H$*, em que* y' *é o simétrico de* y*.*

Demonstração.
($\Longrightarrow$) Sejam $x, y \in H$ quaisquer. Como H é subgrupo de G, pelo lema 1.9 na página 8, temos: $y' \in H$ e como H é fechado com relação a $*$, temos que $x * y' \in H$.

($\Longleftarrow$) Temos agora como hipótese que para quaisquer $x, y \in H$ tem-se $x * y' \in H$, devemos mostrar que $(H, *)$ é um subgrupo de $(G, *)$. Para tanto, mostremos primeiro que H é fechado com relação à operação $*$. Note primeiro que se $x \in H$ temos que $x * x' = e \in H$, em que e é o elemento neutro de G, ou seja, mostramos assim que o elemento neutro de G está em H. Agora sejam $x, y \in H$ quaisquer. Sabendo que $e \in H$ e usando a nossa hipótese, temos que: $e * y' = y' \in H$ e assim temos: $x * (y')' = x * y \in H$. Logo, H é fechado com relação a operação $*$.

Mostremos agora que $(H, *)$ é um grupo.

Associatividade: Note que, $H \subseteq G$ e como $*$ é associativa em G, em particular $*$ é associativa em H (propriedade hereditária).

Existência do elemento neutro: Já mostramos que o elemento neutro de G está em H, ou seja, o elemento neutro de H é o mesmo de G.

Existência do elemento simétrico: Seja $x \in H$ qualquer, já mostramos que $x' \in H$, portanto, todo elemento de H tem simétrico.

■

Exemplo 1.11. *Considere o grupo aditivo $M_2(\mathbb{R})$. Vamos mostrar que o conjunto $sl_2(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ z & -x \end{pmatrix}; x, y, z \in \mathbb{R} \right\}$ é um subgrupo de $M_2(\mathbb{R})$.*

Primeiro note que $sl_2(\mathbb{R})$ não é vazio, pois $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in sl_2(\mathbb{R})$ e ainda $sl_2(\mathbb{R}) \subset M_2(\mathbb{R})$.

Sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & -b_{11} \end{pmatrix} \in sl_2(\mathbb{R})$ quaisquer. Assim temos,

$$A + (-B) = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & -a_{11} + b_{11} \end{pmatrix} = \begin{pmatrix} a_{11} - b_{11} & a_{12} - b_{12} \\ a_{21} - b_{21} & -(a_{11} - b_{11}) \end{pmatrix} \in sl_2(\mathbb{R}).$$

Portanto, pela proposição anterior, temos que $sl_2(\mathbb{R})$ é subgrupo de $M_2(\mathbb{R})$.

Na nossa próxima subseção, falaremos sobre homomorfismos de grupos, que nada mais é do que uma correspondência entre dois grupos, sujeita a algumas regras. Devido à importância de algumas correspondências específicas, que trataremos no decorrer desse trabalho, achamos necessário e útil uma visão geral sobre correspondências entre conjuntos.

Definição 1.12. *Sejam $\mathcal{V}$ e $\mathcal{W}$ conjuntos não vazios. Uma* aplicação *de $\mathcal{V}$ em $\mathcal{W}$ é uma função, ou seja, é uma relação pela qual a cada elemento de $\mathcal{V}$ está associado a um único elemento de $\mathcal{W}$. Se F indica essa relação e $v \in \mathcal{V}$ qualquer, então $F(v)$ indica o elemento associado a v e se denomina a* imagem *de v por F. Assim, definimos o* conjunto imagem *de F como*

$$\mathfrak{I}m(F) = \{F(v); v \in \mathcal{V}\}.$$

E ainda indicamos esta aplicação por

$$F : \mathcal{V} \longrightarrow \mathcal{W}.$$

Definição 1.13. *Uma aplicação $F : \mathcal{V} \longrightarrow \mathcal{W}$ é denominada* injetiva*, se para todos $v_1, v_2 \in \mathcal{V}$, tais que $F(v_1) = F(v_2)$ tem-se $v_1 = v_2$.*

Definição 1.14. *Uma aplicação $F : \mathcal{V} \longrightarrow \mathcal{W}$ é denominada* sobrejetiva*, se para todo $w \in \mathcal{W}$, existe $v \in \mathcal{V}$ tal que $F(v) = w$. Nesse caso, $\mathfrak{I}m(F) = \mathcal{W}$.*

Definição 1.15. *Uma aplicação $F : \mathcal{V} \longrightarrow \mathcal{W}$ é denominada* bijetiva *se F é injetiva e sobrejetiva.*

Exemplo 1.16. *A aplicação $F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, definida para todo $(x, y) \in \mathbb{R}^2$ por $F(x, y) = (x, -y)$ é bijetiva.*

De fato, mostremos que F é injetiva. Para tanto, sejam $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ tais que, $F(x_1, y_1) = F(x_2, y_2)$. Então temos,

$$(x_1, -y_1) = (x_2, -y_2) \Longrightarrow x_1 = x_2 \text{ e } y_1 = y_2.$$

Logo, $(x_1, y_1) = (x_2, y_2)$.

Agora dado $(x, y) \in \mathbb{R}^2$ qualquer, tome $(x, -y) \in \mathbb{R}^2$. Assim temos,

$$F(x, -y) = (x, -(-y)) = (x, y).$$

Logo, F é sobrejetiva.

Concluímos assim que F é bijetiva.

1.1.2 Homomorfismos de Grupos

Nessa subseção, estudaremos funções entre grupos. As funções de interesse aqui, são aquelas que preservam as operações dos grupos. Essas funções são chamadas de *homomorfismos* de grupos.

Definição 1.17. *Sejam $(G, *)$ e $(H, \cdot)$ grupos. Um* homomorfismo *de G em H é uma função $f : G \to H$ que satisfaz, para quaisquer $x, y \in G$,*

$$f(x * y) = f(x) \cdot f(y).$$

Exemplo 1.18. *Seja $(G, *)$ e $(H, \cdot)$ grupos. Considere a função $f : G \to H$, tal que, para todo $x \in G$ tem-se $f(x) = e_H$ em que, e_H é o elemento neutro de H. Vamos mostrar que f é um homomorfismo.*

De fato, sejam $x, y \in G$ quaisquer. Então temos:

$$f(x * y) = e_h = e_h \cdot e_h = f(x) \cdot f(y).$$

Observação: Esse homomorfismo é chamado de *homomorfismo nulo.*

Definição 1.19. *Um homomorfismo injetor é chamado de* monomorfismo. *Um homomorfismo sobrejetor é chamado de* epimorfismo. *Um homomorfismo bijetor é chamado de* isomorfismo. *Um homomorfismo $f : G \to G$ é chamado de* endomorfismo. *Um isomorfismo $f : G \to G$ é chamado de* automorfismo.

Definição 1.20. *Sejam G, J grupos. Se existe $f : G \longrightarrow J$ um isomorfismo de grupos, dizemos que G é* isomorfo *a J e denotamos por $G \simeq J$.*

Proposição 1.21. *Sejam G e J grupos, e_G e e_J seus respectivos elementos neutros e seja $f : G \longrightarrow J$ homomorfismo. Então $f(e_G) = e_J$ e para qualquer $x \in G$ tem-se $f(x^{-1}) = f(x)^{-1}$.*

Demonstração. Primeiro note que,

$$\begin{aligned} e_J f(e_G) = f(e_G) = f(e_G e_G) = f(e_G) f(e_G) \\ \Longrightarrow e_J f(e_G) = f(e_G) f(e_G) \\ \Longrightarrow e_J f(e_G) f(e_G)^{-1} = f(e_G) f(e_G) f(e_G)^{-1} \\ \Longrightarrow e_J = f(e_G). \end{aligned}$$

Agora seja $x \in G$ qualquer. Assim temos,

$$\begin{aligned} f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_J = f(x)f(x)^{-1} \\ \Longrightarrow f(x)f(x^{-1}) = f(x)f(x)^{-1} \\ \Longrightarrow -f(x)f(x)f(x^{-1}) = f(x)^{-1}f(x)f(x)^{-1} \\ \Longrightarrow f(x^{-1}) = f(x)^{-1}. \end{aligned}$$

Portanto, concluímos que $f(e_G) = e_J$ e $f(x^{-1}) = f(x)^{-1}$.

■

De agora em diante, denotaremos o elemento neutro de um grupo G por e_G, de um grupo J por e_J, ou seja, o índice do elemento neutro indica de qual grupo ele é.

Definição 1.22. *Seja $f : G \longrightarrow J$ um homomorfismo de grupos. O* núcleo *de f, denotado por $N(f)$ ou $ker(f)$, é o seguinte conjunto:*

$$N(f) = \{x \in G; f(x) = e_j\}.$$

Proposição 1.23. *Sejam G, J grupos quaisquer, H subgrupo de G e $f : G \longrightarrow J$ homomorfismo. Então $f(H) = \{f(x); x \in H\}$ é um subgrupo de J.*

Demonstração. Note que $0_G \in H$ pois H é subgrupo de G, então $f(0_G) = 0_J \in f(H)$ e assim $f(H)$ não é vazio.

Sejam $x, y \in f(H)$. Então existem $a, b \in H$ tais que $f(a) = x$ e $f(b) = y$. Assim

$$xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}).$$

Como $ab^{-1} \in H$ temos que $f(ab^{-1}) \in f(H)$. Desta forma, $xy^{-1} \in f(H)$ e pela proposição 1.10, temos que $f(H)$ é subgrupo de J.

■

Proposição 1.24. *Sejam G, J grupos quaisquer e $f : G \longrightarrow J$ homomorfismo. Então:*

(i) *$N(f)$ é um subgrupo de G;*

(ii) *$\Im m(f)$ é um subgrupo de J.*

Demonstração. **(i)** $N(f)$ é não vazio, pois como visto na proposição 1.21, $e_G \in N(f)$. Agora sejam $x, y \in N(f)$ quaisquer. Vamos mostrar que $xy^{-1} \in N(f)$. Note que,

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e_J e_J = e_J.$$

Logo, $xy^{-1} \in N(f)$ e pela proposição 1.10, temos que $N(f)$ é subgrupo de G.

(ii) Segue da proposição 1.23, pois $\mathfrak{I}m(f) = f(G)$.

■

Proposição 1.25. *Sejam G, J grupos e $f : G \longrightarrow J$ um homomorfismo. Então $N(f) = \{e_G\}$ se, e somente se, f é injetiva.*

Demonstração.

($\Longrightarrow$) Sejam $x, y \in J$, tais que, $f(x) = f(y)$. Então,

$$f(x)(f(y))^{-1} = e_J \Longrightarrow f(x)f(y^{-1}) = f(xy^{-1}) = e_J.$$

Logo, $xy^{-1} \in N(f)$ e como $N(f) = \{e_G\}$, temos

$$xy^{-1} = e_G \Longrightarrow x = y,$$

o que prova a injetividade de f.

($\Longleftarrow$) Seja $x \in N(f)$ qualquer. Então,

$$f(x) = e_J = f(e_G).$$

Como f é injetiva, temos que $x = e_G$. Assim,

$$N(f) \subseteq \{e_g\}.$$

Note que, $\{e_g\} \subseteq N(f)$, pois $f(e_g) = e_j$.

Concluímos assim que $N(f) = \{e_g\}$.

■

1.1.3 Classes Laterais, Subgrupos Normais e Grupos Quocientes

Considere $(G, *)$ um grupo qualquer e H um subgrupo qualquer de G. Para a demonstração das proposições dessa seção, usaremos a notação multiplicativa, por simplicidade. Então quando nos referirmos a G como grupo, usaremos xy ao invés de $x * y$, ou seja, fica subentendido que $x * y = xy$ e ainda o simétrico de x em G notaremos como x^{-1}.

Proposição 1.26. *Sejam G um grupo, H um subgrupo de G e $x, y \in G$ quaisquer. A relação*

$$yRx \iff x^{-1}y \in H$$

é uma relação de equivalência em G.

Demonstração.

(i) (Reflexiva) Seja $x \in G$ qualquer. Temos, $x^{-1}x = e \in H$, logo xRx.

(ii) (Simétrica) Sejam $x, y \in G$ quaisquer. Temos que,

$$yRx \implies x^{-1}y \in H \implies (x^{-1}y)^{-1} = y^{-1}x \in H \implies xRy.$$

(iii) (Transitiva) Sejam x, y e $z \in G$ quaisquer, tais que, yRx e xRz. Então, $x^{-1}y \in H$ e $z^{-1}x \in H$. Assim,

$$(z^{-1}x)(x^{-1}y) \in H \implies z^{-1}y \in H \implies yRz.$$

■

De maneira análoga, se G é um grupo e H um subgrupo de G, a relação

$$xR^*y \iff yx^{-1} \in H$$

é também uma relação de equivalência.

Perceba agora que,

$$yRx \iff x^{-1}y \in H \iff \exists h \in H, \quad \text{tal que}$$

$$x^{-1}y = h \iff y = xh \iff y \in xH = \{xh; h \in H\}.$$

A *classe de equivalência* de $x \in G$, definida pela relação R, é

$$\{y \in G; yRx\} = xH.$$

No caso em que a relação é $yR^*x \iff yx^{-1} \in H$, a *classe de equivalência* de $y \in G$ é

$$\{y \in G; yR^*x\} = Hx.$$

Isso motiva as seguintes definições:

Definição 1.27. *A classe de equivalência* $xH = \{xh; h \in H\}$ *é chamada* classe lateral de x à esquerda de H *em* G.

Definição 1.28. *A classe de equivalência* $Hx = \{hx; h \in H\}$ *é chamada* classe lateral de x à direita de H *em* G.

Definição 1.29. *Um subgrupo* H *de um grupo* G *é chamado de* subgrupo normal *se, para todo* $x \in G$*, se verifica a igualdade*

$$xH = Hx.$$

Exemplo 1.30. *Seja* $f : G \longrightarrow J$ *homomorfismo de grupos. Vamos mostrar que* $N(f)$ *é um subgrupo normal de* G.

Já mostramos na proposição 1.24 na página 12 que $N(f)$ é um subgrupo de G, resta mostrarmos então, que para todo $x \in G$ tem-se $xH = Hx$, vamos mostrar por dupla inclusão.

Primeira inclusão $xN(f) \subseteq N(f)x$. Seja $y \in xN(f)$ qualquer. Então, existe $n \in N(f)$ tal que $y = xn$. Note que

$$y = xn = xnx^{-1}x.$$

Assim, temos

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = f(x)e_Jf(x)^{-1} = f(x)f(x)^{-1} = e_J.$$

Portanto, $xnx^{-1} \in N(f)$, logo existe $n_1 \in N(f)$ tal que, $xnx^{-1} = n_1$. Assim, temos

$$y = xnx^{-1}x = n_1x \in N(f)x.$$

ou seja, Concluímos assim que $xN(f) \subseteq N(f)x$.

De maneira análoga, demonstra-se que $N(f)x \subseteq xN(f)$.

Portanto, $xN(f) = N(f)x$.

Sejam G um grupo e $H \subseteq G$ um subgrupo normal de G. Sabemos que para $x, y \in G$

$$yRx \iff x^{-1}y \in H$$

é uma relação de equivalência em G. O conjunto

$$G/H = \{xH; x \in G\} = \{Hx; x \in G\}$$

é o conjunto das *classes de equivalência módulo* H.

Lema 1.31. *Sejam G um grupo, H um subgrupo de G e $x, y \in G$ quaisquer. Então:*

(i) $y \in xH \iff xH = yH$;

(ii) $y \in Hx \iff Hx = Hy$.

Demonstração.

(i) ($\Longrightarrow$) Como $y \in xH$, temos yRx, por simetria temos que xRy. Vamos mostrar que $xH \subseteq yH$. Se $z \in xH$, então zRx. Mas xRy logo, pela transitividade, temos zRy. Portanto, $z \in yH$.

$yH \subseteq xH$ é análogo.
($\Longleftarrow$) Como $y \in yH$ e $yH = xH$, então $y \in xH$.

(ii) É semelhante ao item (i), basta trocar a lateralidade.

■

Proposição 1.32. *Sejam G um grupo e H um subgrupo normal de G. Defina a seguinte operação*

$$\begin{array}{rccc} \cdot : & G/H \times G/H & \to & G/H \\ & (xH, yH) & \mapsto & xyH. \end{array}$$

Então $(G/H, \cdot)$ é um grupo.

Demonstração. Primeiramente, vamos mostrar que a operação está bem definida. Para tanto, sejam xH, yH, x_1H e $y_1H \in G/H$ tais que, $xH = x_1H$ e $yH = y_1H$. Vamos mostrar que $xyH = x_1y_1H$.

Como $xH = x_1H$ e $yH = y_1H$, pelo lema 1.31 temos que, $x_1 \in xH$ e $y_1 \in yH$, ou seja, existem $h_1, h_2 \in H$ tais que, $x_1 = xh_1$ e $y_1 = yh_2$. Assim,

$$x_1y_1 = (xh_1)(yh_2) = x(h_1y)h_2.$$

Note que, $h_1y \in Hy$ e como H é normal, temos que $Hy = yH$. Portanto, existe $h_3 \in H$ tal que, $h_1y = yh_3$. Assim,

$$x_1y_1 = x(h_1y)h_2 = x(yh_3)h_2 = xy(h_3h_2).$$

Como $h_3, h_2 \in H$ temos que $h_3h_2 \in H$, ou seja, existe $h \in H$ tal que, $h_3h_2 = h$. Portanto,

$$x_1y_1 = xy(h_3h_2) = xyh \in xyH.$$

Logo, pelo lema 1.31 na página 16, temos que $xyH = x_1y_1H$. Concluímos assim, que a operação está bem definida.

Provaremos agora os axiomas de grupos.

Associatividade: Sejam xH, yH e $zH \in G/H$ quaisquer. Assim,

$$(xH \cdot yH) \cdot zH = xyH \cdot zH = (xy)zH = x(yz)H = xH \cdot yzH = xH \cdot (yH \cdot zH).$$

Existência do elemento neutro: Considere $eH = H \in G/H$ e dado $xH \in G/H$ qualquer, temos:

$$eH \cdot xH = exH = xH \quad \text{e}$$

$$xH \cdot eH = xeH = xH.$$

Logo, eH é o elemento neutro de G/H.

Existência do elemento simétrico: Seja $xH \in G/H$ qualquer. Note que $x^{-1}H \in G/H$ e que

$$xH \cdot x^{-1}H = xx^{-1}H = eH \quad \text{e}$$

$$x^{-1}H \cdot xH = x^{-1}xH = eH.$$

Portanto, o simétrico de xH é $x^{-1}H$. Concluímos então, que $(G/H, \cdot)$ é um grupo.

■

1.1.4 Teorema do Homomorfismo para Grupos

Sejam G e J grupos. Dado $f : G \longrightarrow J$ um homomorfismo, podemos colocar a seguinte questão: como podemos construir um isomorfismo, apartir de f? Bom, sabemos que um isomorfismo é um homomorfismo injetor e sobrejetor. Podemos, tentar resolver essa questão por partes. Se pensarmos em construir um homomorfismo sobrejetor, podemos mudar o contradomínio de f, para $\mathfrak{Im}(f)$, o que resolve a sobrejetividade. Mas, e a injetividade? Uma motivação para a resposta seria o seguinte: Se, $x, y \in G$ são tais que $f(x) = f(y)$ então,

$$f(x) = f(y) \Longrightarrow f(x)f(y)^{-1} = e_J \Longrightarrow f(x)f(y^{-1}) = f(xy^{-1}) = e_J.$$

Isso significa que $xy^{-1} \in N(f)$, ou seja, x e y estão relacionados pela relação de equivalência módulo $N(f)$. Quando quocientamos G por $N(f)$, fazemos com que o elemento neutro de $G/N(f)$ seja a classe do $e_gN(f) = N(f)$. Isso nos dá, uma pista de que podemos trocar o domínio G de f por $G/N(f)$. Para ficar claro, vamos para o teorema que dá nome a essa subseção.

Teorema 1.33 (Teorema do homomorfismo para grupos)**.** *Sejam G, J grupos e ainda $f : G \longrightarrow J$ um homomorfismo. Então, a função*

$$\begin{array}{rccc} \varphi: & G/N(f) & \longrightarrow & \mathfrak{Im}(f) \\ & xN(f) & \longmapsto & f(x) \end{array}$$

é um isomorfismo.

Demonstração.

Vamos primeiro mostrar que φ está bem definida. Para tanto, sejam $xN(f)$, $yN(f) \in G/N(f)$ quaisquer, tais que $xN(f) = yN(f)$. Assim, yRx, ou seja, $x^{-1}y \in N(f)$. Note que, $\varphi(xN(f)) = f(x)$ e $\varphi(yN(f)) = f(y)$, então

$$\begin{aligned} \varphi(xN(f))\left(\varphi(yN(f))\right)^{-1} &= f(x)\left(f(y)\right)^{-1} \\ &= f(x)f(y^{-1}) \\ &= f(xy^{-1}) = e_J \\ &\Longrightarrow \varphi(xN(f)) = \varphi(yN(f)). \end{aligned}$$

Portanto, φ está bem definida.

Mostremos agora que φ é um homomorfismo. Sejam $xN(f)$ e $yN(f) \in G/N(f)$

quaisquer, assim

$$\varphi(xN(f)\cdot yN(f)) = \varphi(xyN(f)) = f(xy) = f(x)f(y) = \varphi(xN(f))\varphi(yN(f)).$$

Logo φ é um homomorfismo.

Mostremos que φ é injetiva. Seja $xN(f) \in N(\varphi)$ qualquer. Então

$$\varphi(xN(f)) = e_J \Longrightarrow f(x) = e_J.$$

Logo, $x \in N(f)$, assim

$$N(\varphi) = \{xN(f); x \in N(f)\} = \{N(f)\}.$$

Vimos na proposição 1.32 na página 16, que a classe $e_gN(f) = N(f)$ é o elemento neutro do grupo quociente $G/N(f)$. Logo, pela proposição 1.25 na página 16, temos que φ é injetiva.

Mostremos que φ é sobrejetiva. Seja $y \in \mathfrak{I}m(f)$ qualquer. Então existe $x \in G$ tal que, $f(x) = y$, logo existe $xN(f) \in G/N(f)$ tal que,

$$\varphi(xN(f)) = f(x) = y.$$

Portanto, φ é sobrejetiva.

Como φ é homomorfismo injetor e sobrejetor, temos que φ é um isomorfismo, ou seja, $G/N(f)$ é isomorfo a $\mathfrak{I}m(f)$, em notação fica, $G/N(f) \simeq \mathfrak{I}m(f)$. Concluímos assim, a demonstração.

■

Exemplo 1.34. *Seja G um grupo. Considere $H = \{e_g\}$, em que e_g é o elemento neutro de G. Então $G/\{e_g\} \simeq G$.*

Primeiro, note que H é um subgrupo normal de G, pois para cada $g \in G$ temos $gH = ge_g = e_gg = Hg$. Agora considere $f : G \longrightarrow G$ tal que, para todo $x \in G$ temos, $f(x) = x$, assim, para $x, y \in G$ quaisquer temos, $f(xy) = xy = f(x)f(y)$, ou seja, f é homomorfismo. Note agora que, $N(f) = \{e_g\}$ e $\mathfrak{I}m(f) = G$, segue então, do teorema do homomorfismo que $G/\{e_g\} \simeq G$.

1.2 Anéis

A definição formal de anel foi elaborada em 1914 pelo matemático alemão A. Fraenkel (1891-1965) . O conceito de anel foi fundamental para axiomatização da álgebra. Surgiu como consequência da sistematização de conjuntos numéricos, principalmente do conjunto dos números inteiros. O conceito de anel está intimamente relacionado com as seguintes questões: qual o conjunto mínimo das propriedades de adição e da multiplicação em $\mathbb{Z}$ é necessário para demonstrar as outras propriedades de $\mathbb{Z}$? Ou seja, quais propriedades as operações de um determinado conjunto tem que ter, para que possamos operar nesse conjunto de forma semelhante que operamos em $\mathbb{Z}$? As respostas para estas perguntas levaram aos seis axiomas de anel.

Definição 1.35. *Um* anel *é uma tripla ordenada* $(\mathcal{R}, +, *)$*, em que* $\mathcal{R}$ *é um conjunto não vazio, munido de uma operação denotada por* $+$ *(chamada de soma) e de uma operação denotada por* $*$ *(chamada de multiplicação), tais que para quaisquer* $x, y, z \in \mathcal{R}$*, as seguintes condições são satisfeitas:*

S: $(\mathcal{R}, +)$ *é um grupo abelino;*

P1: $(x * y) * z = x * (y * z)$ *(associatividade do produto);*

P2: $x * (y + z) = x * y + x * z$ *e* $(x + y) * z = x * z + y * z$ *(distributividade da soma com respeito ao produto).*

Definição 1.36. *Seja* $(\mathcal{R}, +, *)$ *um anel. Dizemos que:*

(i) $(\mathcal{R}, +, *)$ *é um* anel comutativo *se* $*$ *for comutativa, ou seja, para quaisquer* $x, y \in \mathcal{R}$ *temos* $x * y = y * x$*;*

(ii) $(\mathcal{R}, +, *)$ *é um* anel com unidade *se existe* $1_R \in \mathcal{R}$ *tal que, para todo* $x \in \mathcal{R}$ *temos* $1_R * x = x * 1_R = x$*;*

(iii) $a \in \mathcal{R}$ *e* $a \neq 0$ *é um* divisor de zero*, quando existe* $b \in \mathcal{R}$ *e* $b \neq 0$*, tal que,* $a * b = 0$*;*

(iv) $a \in \mathcal{R}$ *(um anel com unidade) e* $a \neq 0$ *é um* elemento inversível*, se existe* $b \in \mathcal{R}$ *e* $b \neq 0$*, tal que,* $a * b = b * a = 1_R$*.*

Definição 1.37. *Um anel* $(\mathcal{R}, +, *)$ *comutativo, com unidade e sem divisores de zero é chamado de* anel de integridade *ou* domínio de integridade*.*

Definição 1.38. *Um anel de integridade* $(\mathcal{R}, +, *)$ *em que todo elemento não nulo é inversível é chamado de* corpo*.*

Definição 1.39. *Seja* $\mathbb{K}$ *um corpo, dizemos que a* característica *de* $\mathbb{K}$ *é igual a* n *e denotamos por* $char\ \mathbb{K} = n$*, se* n *é o menor inteiro positivo, de forma que*

$$\underbrace{1+1+\ldots+1}_{n-vezes} = 0.$$

Quando não existe inteiro positivo tal que isso ocorra, dizemos que $char\ \mathbb{K} = 0$.

É possível mostrar que a característica de um corpo é sempre zero ou um número primo. Trabalharemos apenas com corpos de característica zero.

Exemplo 1.40. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ *e* $(\mathbb{C}, +, \cdot)$ *são corpos de característica zero com as operações usuais.*

Observação: Quando ficar subentendida a existência das operações, vamos nos referir ao anel $(\mathcal{R}, +, *)$ simplesmente por anel $\mathcal{R}$.

Exemplo 1.41. $(M_2(\mathbb{R}), +, \cdot)$ *com as operações usuais de soma e multiplicação de matrizes é um anel.*

Já vimos no exemplo 1.2 na página 4 que $(M_2(\mathbb{R}), +)$ é um grupo abeliano. Resta mostrarmos então que **P1** e **P2** são satisfeitas. Para tanto, sejam $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \in M_2(\mathbb{R})$ quaisquer.

P1 (*associatividade do produto*)

Temos que

$$A \cdot (B \cdot C) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \left[\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right]$$

$$= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \left[\begin{pmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{pmatrix} \right]$$

$$= \begin{pmatrix} a_1(b_1c_1 + b_2c_3) + a_2(b_3c_1 + b_4c_3) & a_1(b_1c_2 + b_2c_4) + a_2(b_3c_2 + b_4c_4) \\ a_3(b_1c_1 + b_2c_3) + a_4(b_3c_1 + b_4c_3) & a_3(b_1c_2 + b_2c_4) + a_4(b_3c_2 + b_4c_4) \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_4c_3 & a_1b_1c_2 + a_1b_2c_4 + a_2b_3c_2 + a_2b_4c_4 \\ a_3b_1c_1 + a_3b_2c_3 + a_4b_3c_1 + a_4b_4c_3 & a_3b_1c_2 + a_3b_2c_4 + a_4b_3c_2 + a_4b_4c_4 \end{pmatrix}. \quad (1.2)$$

Por outro lado,

$$(A \cdot B) \cdot C = \left[\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \right] \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$
$$= \left[\begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix} \right] \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$

$$= \begin{pmatrix} (a_1b_1 + a_2b_3)c_1 + (a_1b_2 + a_2b_4)c_3 & (a_1b_1 + a_2b_3)c_2 + (a_1b_2 + a_2b_4)c_4 \\ (a_3b_1 + a_4b_3)c_1 + (a_3b_2 + a_4b_4)c_3 & (a_3b_1 + a_4b_3)c_2 + (a_3b_2 + a_4b_4)c_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1c_1 + a_2b_3c_1 + a_1b_2c_3 + a_2b_4c_3 & a_1b_1c_2 + a_2b_3c_2 + a_1b_2c_4 + a_2b_4c_4 \\ a_3b_1c_1 + a_4b_3c_1 + a_3b_2c_3 + a_4b_4c_3 & a_3b_1c_2 + a_4b_3c_2 + a_3b_2c_4 + a_4b_4c_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_4c_3 & a_1b_1c_2 + a_1b_2c_4 + a_2b_3c_2 + a_2b_4c_4 \\ a_3b_1c_1 + a_3b_2c_3 + a_4b_3c_1 + a_4b_4c_3 & a_3b_1c_2 + a_3b_2c_4 + a_4b_3c_2 + a_4b_4c_4 \end{pmatrix}. \tag{1.3}$$

Note que (1.3)=(1.2).

Logo, $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ e portanto, a associatividade do produto é válida.

P2(*distributividade do produto com respeito a soma*):

$$A \cdot (B + C) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \left[\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} + \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right]$$
$$= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 + c_1 & b_2 + c_2 \\ b_3 + c_3 & b_4 + c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1(b_1 + c_1) + a_2(b_3 + c_3) & a_1(b_2 + c_2) + a_2(b_4 + c_4) \\ a_3(b_1 + c_1) + a_4(b_3 + c_3) & a_3(b_2 + c_2) + a_4(b_4 + c_4) \end{pmatrix}$$
$$= \begin{pmatrix} a_1b_1 + a_1c_1 + a_2b_3 + a_2c_3 & a_1b_2 + a_1c_2 + a_2b_4 + a_2c_4 \\ a_3b_1 + a_3c_1 + a_4b_3 + a_4c_3 & a_3b_2 + a_3c_2 + a_4b_4 + a_4c_4 \end{pmatrix}. \tag{1.4}$$

Por outro lado,

$$A \cdot B + A \cdot C = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} + \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix} + \begin{pmatrix} a_1c_1 + a_2c_3 & a_1c_2 + a_2c_4 \\ a_3c_1 + a_4c_3 & a_3c_2 + a_4c_4 \end{pmatrix}.$$

$$= \begin{pmatrix} a_1b_1 + a_2b_3 + a_1c_1 + a_2c_3 & a_1b_2 + a_2b_4 + a_1c_2 + a_2c_4 \\ a_3b_1 + a_4b_3 + a_3c_1 + a_4c_3 & a_3b_2 + a_4b_4 + a_3c_2 + a_4c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1b_1 + a_1c_1 + a_2b_3 + a_2c_3 & a_1b_2 + a_1c_2 + a_2b_4 + a_2c_4 \\ a_3b_1 + a_3c_1 + a_4b_3 + a_4c_3 & a_3b_2 + a_3c_2 + a_4b_4 + a_4c_4 \end{pmatrix} \quad (1.5)$$

Note que (1.5)=(1.4). Logo, $A \cdot (B + C) = A \cdot B + A \cdot C$.

Agora,

$$(A + B) \cdot C = \left[\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \right] \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$
$$= \begin{pmatrix} (a_1 + b_1)c_1 + (a_2 + b_2)c_3 & (a_1 + b_1)c_2 + (a_2 + b_2)c_4 \\ (a_3 + b_3)c_1 + (a_4 + b_4)c_3 & (a_3 + b_3)c_2 + (a_4 + b_4)c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1c_1 + b_1c_1 + a_2c_3 + b_2c_3 & a_1c_2 + b_1c_2 + a_2c_4 + b_2c_4 \\ a_3c_1 + b_3c_1 + a_4c_3 + b_4c_3 & a_3c_2 + b_3c_2 + a_4c_4 + b_4c_4 \end{pmatrix}. \quad (1.6)$$

Por outro lado,

$$(A \cdot C + B \cdot C) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \cdot \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1c_1 + a_2c_3 & a_1c_2 + a_2c_4 \\ a_3c_1 + a_4c_3 & a_3c_2 + a_4c_4 \end{pmatrix} + \begin{pmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1c_1 + a_2c_3 + b_1c_1 + b_2c_3 & a_1c_2 + a_2c_4 + b_1c_2 + b_2c_4 \\ a_3c_1 + a_4c_3 + b_3c_1 + b_4c_3 & a_3c_2 + a_4c_4 + b_3c_2 + b_4c_4 \end{pmatrix}$$
$$= \begin{pmatrix} a_1c_1 + b_1c_1 + a_2c_3 + b_2c_3 & a_1c_2 + b_1c_2 + a_2c_4 + b_2c_4 \\ a_3c_1 + b_3c_1 + a_4c_3 + b_4c_3 & a_3c_2 + b_3c_2 + a_4c_4 + b_4c_4 \end{pmatrix}. \quad (1.7)$$

Note que (1.6)=(1.7). Logo, $(A + B) \cdot C = A \cdot C + B \cdot C$.

Portanto, $(M_2(\mathbb{R}), +, \cdot)$ é um anel.

Exemplo 1.42. *Seja* $\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \longrightarrow \mathbb{R}; f \text{ é função}\}$. *Defina as seguintes operações:*

$$\begin{array}{rccc} + : & \mathcal{F}(\mathbb{R}) \times \mathcal{F}(\mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R}) \\ & (f, g) & \longmapsto & f + g, \end{array}$$

em que para todo $x \in \mathbb{R}$, $(f+g)(x) = f(x) + g(x)$ *e*

$$\begin{array}{rccc} \cdot : & \mathcal{F}(\mathbb{R}) \times \mathcal{F}(\mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R}) \\ & (f, g) & \longmapsto & f \cdot g, \end{array}$$

em que para todo $x \in \mathbb{R}$, $(f \cdot g)(x) = f(x) \cdot g(x)$.

$(\mathcal{F}(\mathbb{R}), +, \cdot)$ *é um anel comutativo com unidade.*

Associatividade da soma: Sejam f, g e $h \in \mathcal{F}(\mathbb{R})$ quaisquer. Então para todo $x \in \mathbb{R}$ temos,

$$\begin{aligned} ((f+g)+h)(x) &= (f+g)(x) + h(x) = f(x) + g(x) + h(x) \\ &= f(x) + (g+h)(x) = (f + (g+h))(x), \end{aligned}$$

já que a associatividade da soma em $\mathbb{R}$ é válida.

Logo, $(f+g)+h = f+(g+h)$.

Comutatividade da soma: Sejam $f, g \in \mathcal{F}(\mathbb{R})$ quaisquer. Então para todo $x \in \mathbb{R}$ temos:

$$(f+g)(x) = f(x) + g(x).$$

Devido à comutatividade da soma nos reais, temos

$$f(x) + g(x) = g(x) + f(x) = (g+f)(x).$$

Logo, $f + g = g + f$.

Existência do elemento neutro para soma: Seja $f \in \mathcal{F}(\mathbb{R})$ qualquer e considere $e_0 : \mathbb{R} \longrightarrow \mathbb{R}$ tal que, para todo $x \in \mathbb{R}$ temos $e_0(x) = 0$. Assim,

$$(e_0 + f)(x) = e_0(x) + f(x) = 0 + f(x) = f(x) \quad \text{e}$$

$$(f + e_0)(x) = f(x) + e_0(x) = f(x) + 0 = f(x).$$

Portanto, e_0 é o elemento neutro da soma em $\mathcal{F}(\mathbb{R})$.

Existência do lemento simétrico para soma: Seja $f \in \mathcal{F}(\mathbb{R})$ qualquer. Considere

$-f \in \mathcal{F}(\mathbb{R})$ tal que, para todo $x \in \mathbb{R}$ tem-se $(-f)(x) = -f(x)$, assim temos,

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = e_0(x) \quad \text{e}$$

$$(-f + f)(x) = (-f)(x) + f(x) = -f(x) + f(x) = 0 = e_0(x).$$

Portanto, $-f$ é o simétrico de f. Mostramos então que $(\mathcal{F}(\mathbb{R}), +)$ é um grupo abeliano.

Associatividade do produto: Sejam f, g e $h \in \mathcal{F}(\mathbb{R})$ quaisquer. Então para todo $x \in \mathbb{R}$, temos

$$\begin{aligned}((f \cdot g) \cdot h)(x) &= (f \cdot g)(x) \cdot h(x) = [f(x) \cdot g(x)] \cdot h(x) \\ &= f(x) \cdot [g(x) \cdot h(x)] = f(x) \cdot (g \cdot h)(x) = (f \cdot (g \cdot h))(x).\end{aligned}$$

Logo, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.

Comutatividade do produto: Sejam $f, g \in \mathcal{F}(\mathbb{R})$ quaisquer. Então para todo $x \in \mathbb{R}$ temos,

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Pela comutatividade do produto em $\mathbb{R}$ temos

$$f(x) \cdot g(x) = g(x) \cdot f(x) = (g \cdot f)(x).$$

Logo, $f \cdot g = g \cdot f$.

Distributividade(produto com respeito a soma): Sejam f, g e $h \in \mathcal{F}(\mathbb{R})$ quaisquer. Então para todo $x \in \mathbb{R}$ temos:

$$((f + g) \cdot h)(x) = (f + g)(x) \cdot h(x) = (f(x) + g(x)) \cdot h(x)$$

e pela distributividade nos reais temos,

$$(f(x) + g(x)) \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x) = (f \cdot h)(x) + (g \cdot h)(x) = (f \cdot h + g \cdot h)(x).$$

Por outro lado, pelo primeiro caso e pela comutatividade do produto, temos

$$(f + g) \cdot h = f \cdot h + g \cdot h \quad \text{e}$$

$$h \cdot (f + g) = h \cdot f + h \cdot g.$$

Existência do elemento neutro para o produto: Seja $f \in \mathcal{F}(\mathbb{R})$ qualquer e considere $e : \mathbb{R} \longrightarrow \mathbb{R}$ tal que, para todo $x \in \mathbb{R}$ temos $e(x) = 1$. Assim, temos

$$(e \cdot f)(x) = e(x) \cdot f(x) = 1 \cdot f(x) = f(x) \quad \text{e}$$

$$(f \cdot e)(x) = f(x) \cdot e(x) = f(x) \cdot 1 = f(x).$$

Logo, e é o elemento neutro do produto em $\mathcal{F}(\mathbb{R})$. Portanto, $(\mathcal{F}(\mathbb{R}), +, \cdot)$ é um anel comutativo com unidade.

Considere

$$f(x) = \begin{cases} 0, \text{ se } x > 0 \\ 1, \text{ se } x \leqslant 0 \end{cases} \quad \text{e } g(x) = \begin{cases} 1, \text{ se } x > 0 \\ 0, \text{ se } x \leqslant 0 \end{cases} .$$

Note que $f, g \in \mathcal{F}(\mathbb{R})$ e $f, g \neq e_0$, no entanto $f(x) \cdot g(x) = 0 = e_0(x)$, ou seja, $f \cdot g = e_0$. Portanto, $\mathcal{F}(\mathbb{R})$ tem divisores de zero. Assim, $\mathcal{F}(\mathbb{R})$ não é um anel de integridade e conseguentemente também não é um corpo.

1.2.1 Subanéis, Ideais e Anéis Quocientes

Definição 1.43. *Sejam $(\mathcal{R}, +, \cdot)$ um anel e $\mathcal{B} \subseteq \mathcal{R}$ não vazio. $\mathcal{B}$ é denominado* subanel *de $\mathcal{R}$ quando:*

(i) *as operações $+$ e $\cdot$ são fechadas em $\mathcal{B}$, ou seja, para todo $x, y \in \mathcal{B}$ tem-se $x + y \in \mathcal{B}$ e $x \cdot y \in \mathcal{B}$;*

(ii) *$(\mathcal{B}, +, \cdot)$ é um anel.*

Proposição 1.44. *Sejam $(\mathcal{R}, +, \cdot)$ um anel e $\mathcal{B} \subseteq \mathcal{R}$ não vazio. $\mathcal{B}$ é subanel de $\mathcal{R}$ se, e somente se, $(\mathcal{B}, +)$ é subgrupo de $(\mathcal{R}, +)$ e dados quaisquer $x, y \in \mathcal{B}$ tem-se $x \cdot y \in \mathcal{B}$.*

Demonstração.
($\Longrightarrow$) Como $\mathcal{B}$ é subanel, por definição $\mathcal{B}$ é anel, assim $(\mathcal{B}, +)$ é grupo e como $\mathcal{B} \subseteq \mathcal{R}$, temos que $(\mathcal{B}, +)$ é subgrupo de $(\mathcal{R}, +)$ e pelo fato de que $\mathcal{B}$ é anel, temos $x \cdot y \in \mathcal{B}$.

($\Longleftarrow$) Por hipótese, para quaisquer $x, y \in \mathcal{B}$ temos $x \cdot y \in \mathcal{B}$, logo a operação multiplicação é fechada em $\mathcal{B}$. Como $(\mathcal{B}, +)$ é subgrupo de $(\mathcal{R}, +)$ temos que $(\mathcal{B}, +)$ é grupo e portanto a operação soma também é fechada em $\mathcal{B}$.

Resta mostrarmos então, que **P1** e **P2** são satisfeitas. Para tanto, sejam x, y e $z \in \mathcal{B}$ quaisquer, como $\mathcal{B} \subseteq \mathcal{R}$ então x, y e $z \in \mathcal{R}$ logo, pela associatividade do produto em $\mathcal{R}$, temos que

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z,$$

o que mostra a associatividade do produto em $\mathcal{B}$. O mesmo ocorre com a distributividade. Portanto $(\mathcal{B}, +, \cdot)$ é anel. Concluímos assim que $\mathcal{B}$ é subanel de $\mathcal{R}$.

■

Exemplo 1.45. *Considere $\mathcal{F}(\mathbb{R})$ definido no exemplo 1.42, na página 23. Seja $\mathcal{B} = \{f \in \mathcal{F}(\mathbb{R}); f(1) = 0\}$, então $\mathcal{B}$ é subanel de $\mathcal{F}(\mathbb{R})$.*

De fato, note que $\mathcal{B}$ não é vazio, pois a função $g : \mathbb{R} \longrightarrow \mathbb{R}$, definida como $g(x) = x - 1$ pertence a $\mathcal{B}$.

Agora sejam $f, g \in \mathcal{B}$ quaisquer. Então temos,

$$(f - g)(1) = f(1) - g(1) = 0 - 0 = 0,$$

ou seja, $f - g \in \mathcal{B}$ logo, pela proposição 1.10 na página 8, $(\mathcal{B}, +)$ é subgrupo de $(\mathcal{F}(\mathbb{R}), +)$. Também,

$$(f \cdot g)(1) = f(1) \cdot g(1) = 0 \cdot 0 = 0$$

assim, $f \cdot g \in \mathcal{B}$. Então, pela proposição anterior, temos que $\mathcal{B}$ é subanel de $\mathcal{F}(\mathbb{R})$.

Definição 1.46. *Seja $(\mathcal{R}, +, \cdot)$ um anel e $\mathcal{I} \subseteq \mathcal{R}$ não vazio. $\mathcal{I}$ é denominado um* ideal à esquerda *de $\mathcal{R}$ quando:*

(i) *Para quaisquer $x, y \in \mathcal{I}$ tem-se $x - y \in \mathcal{I}$;*

(ii) *Para todo $x \in \mathcal{I}$ e para todo $y \in \mathcal{R}$ tem-se $y \cdot x \in \mathcal{I}$.*

Definição 1.47. *Seja $(\mathcal{R}, +, \cdot)$ um anel e $\mathcal{I} \subseteq \mathcal{R}$ não vazio. $\mathcal{I}$ é denominado um* ideal à direita *de $\mathcal{R}$ quando:*

(i) *Para todo $x, y \in \mathcal{I}$ tem-se $x - y \in \mathcal{I}$;*

(ii) *Para todo $x \in \mathcal{I}$ e para todo $y \in \mathcal{R}$ tem-se $x \cdot y \in \mathcal{I}$.*

Definição 1.48. *Seja $(\mathcal{R}, +, \cdot)$ um anel e $\mathcal{I} \subseteq \mathcal{R}$ não vazio. $\mathcal{I}$ é denominado um* ideal *de $\mathcal{R}$ ou um* ideal bilateral *de $\mathcal{R}$ quando $\mathcal{I}$ é um ideal à direita e à esquerda de $\mathcal{R}$.*

Proposição 1.49. *$\mathcal{I}$ é um subanel de $\mathcal{R}$.*

Demonstração. De fato, a condição (i) garante que $(\mathcal{I}, +)$ é um subgrupo de $(\mathcal{R}, +)$ e a condição (ii) garante o fechamento da multiplicação. Assim pela proposição 1.44 na página 26, temos que $\mathcal{I}$ é um subanel de $\mathcal{R}$.

■

Exemplo 1.50. *Sejam $\mathcal{R}$ anel e $a \in \mathcal{R}$ fixo, qualquer. Então,*

$$\mathcal{I} = \{x \in \mathcal{R}; xa = 0_R\}$$

é um ideal à esquerda de $\mathcal{R}$.

De fato, note que $\mathcal{I}$ não é vazio pois $0_R \in \mathcal{I}$.

(i) Sejam $x, y \in \mathcal{I}$ quaisquer, então $xa = 0_R$ e $ya = 0_R$. Assim,

$$(x - y)a = xa - ya = 0_R - 0_R = 0_R.$$

Portanto, $x - y \in \mathcal{I}$.

(ii) Sejam $x \in \mathcal{I}$ e $y \in \mathcal{R}$ quaisquer. Assim,

$$(yx)a = y(xa) = y0_R = 0_R.$$

Portano, $yx \in \mathcal{I}$. Logo, $\mathcal{I}$ é um ideal à esquerda de $\mathcal{R}$.

De maneira análoga mostra-se que $\mathcal{I}^* = \{x \in \mathcal{R}; ax = 0_R\}$ é um ideal à direira de $\mathcal{R}$.

Exemplo 1.51. *Sejam $\mathcal{R} = \{f : [a, b] \longrightarrow \mathbb{R}; f$ é função$\}$ e $\mathcal{S} \subseteq [a, b]$. Vamos mostrar que o conjunto*

$$\mathcal{I} = \{f \in \mathcal{R}; \forall x \in \mathcal{S}, f(x) = 0\}$$

é um ideal de $\mathcal{R}$.

De fato, note que $\mathcal{I}$ não é vazio, pois para todo $x \in \mathcal{R}$ considere $e(x) = 0$ em que $e(x)$ é o elemento neutro (soma) de $\mathcal{R}$, em particular, temos que, para todo $x \in \mathcal{S}$ $e(x) = 0$, assim $e(x) \in \mathcal{I}$.

(i) Sejam $f, g \in \mathcal{I}$ quaisquer. Então para todo $x \in \mathcal{S}$ temos $f(x) = 0$ e $g(x) = 0$. Assim, para todo $x \in \mathcal{S}$ temos,

$$(f - g)(x) = f(x) - g(x) = 0 - 0 = 0.$$

Portanto, $f - g \in \mathcal{I}$.

(ii) Sejam $f \in \mathcal{I}$ e $g \in \mathcal{R}$ quaisquer. Então, para todo $x \in \mathcal{S}$ temos,

$$(g \cdot f)(x) = g(x) \cdot f(x) = g(x) \cdot 0 = 0.$$

Portanto, $g \cdot f \in \mathcal{I}$ e, assim, $\mathcal{I}$ é um ideal à esquerda de $\mathcal{R}$.

Agora, para todo $x \in \mathcal{S}$ temos,

$$(f \cdot g)(x) = f(x) \cdot g(x) = 0 \cdot g(x) = 0.$$

Portanto, $g \cdot f \in \mathcal{I}$ e assim $\mathcal{I}$ é um ideal à direita de $\mathcal{R}$.

Logo, $\mathcal{I}$ é um ideal de $\mathcal{R}$.

Vimos na seção de grupos que para G um grupo e $H \subseteq G$ um subgrupo de G as relações

$$yRx \iff x^{-1}y \in H \quad \text{e}$$

$$yR^*x \iff yx^{-1} \in H$$

são relações de equivalência. Vimos também, que essas relações, determinam classes de equivalências e as chamamos de *classes de equivalência módulo H*. Agora, novamente de maneira natural, vamos definir uma relação de equivalência determinada por um *ideal* de um anel. Seja $\mathcal{R}$ um anel qualquer e $\mathcal{I}$ um ideal de $\mathcal{R}$. Assim, o ideal $\mathcal{I}$ define no anel $\mathcal{R}$ a relação

$$y \equiv x \ (mod \ \ \mathcal{I}) \iff y - x \in \mathcal{I}.$$

Quando $y - x \in \mathcal{I}$, dizemos que y é *congruente* a x módulo $\mathcal{I}$ ou y está relacionado com x módulo $\mathcal{I}$. Vale salientar que a relação

$$y \equiv x \ (mod \ \ \mathcal{I}) \iff y - x \in \mathcal{I}$$

é uma relação de equivalência, pois $(\mathcal{I}, +)$ é subgrupo de $(\mathcal{R}, +)$.

Considere $\mathcal{R}$ um anel e $\mathcal{I}$ um ideal de $\mathcal{R}$. Já mostramos na proposição 1.49 na página 28 que $\mathcal{I}$ é um subanel de $\mathcal{R}$. Portanto $(\mathcal{I}, +)$ é um subgrupo de $(\mathcal{R}, +)$. Não é difícil mostrar que se $(\mathcal{R}, +)$ é abeliano, todos os seus subgrupos são normais. Assim temos que $\mathcal{I}$ é subgrupo normal de $(\mathcal{R}, +)$.

Com essas informações, faz sentido considerarmos o grupo quociente $\mathcal{R}/\mathcal{I}$ em que, sua operação é a operação de classes, definida na seção de grupos. Para lembramos, se

$x+\mathcal{I}, y+\mathcal{I} \in \mathcal{R}/\mathcal{I}$, operamos os elementos da seguinte forma:

$$(x+\mathcal{I})+(y+\mathcal{I}) = (x+y)+\mathcal{I}.$$

Também, o elemento neutro de $\mathcal{R}/\mathcal{I}$ é a classe $0+\mathcal{I}$ e o oposto da classe $x+\mathcal{I}$ é a classe $(-x)+\mathcal{I}$. A seguir, mostraremos que o grupo $(\mathcal{R}/\mathcal{I},+)$ torna-se um anel, com a escolha apropriada de uma operação de multiplicação.

Proposição 1.52. *Seja $\mathcal{I}$ um ideal de um anel $\mathcal{R}$. Considere $(\mathcal{I},+)$ como subgrupo normal de $(\mathcal{R},+)$, então o grupo quociente $\mathcal{R}/\mathcal{I}$ é um anel, com a seguinte operação de multiplicação:*

$$\begin{array}{rccc} \cdot: & \mathcal{R}/\mathcal{I}\times\mathcal{R}/\mathcal{I} & \longrightarrow & \mathcal{R}/\mathcal{I} \\ & (x+\mathcal{I}, y+\mathcal{I}) & \longmapsto & (x+\mathcal{I})\cdot(y+\mathcal{I}), \end{array}$$

em que para quaisquer $x+\mathcal{I}, y+\mathcal{I} \in \mathcal{R}/\mathcal{I}$ tem-se $(x+\mathcal{I})\cdot(y+\mathcal{I}) = xy+\mathcal{I}$.

Demonstração. Primeiramente, vamos mostrar que a operação multiplicação está bem definida. Para tanto, sejam $x+\mathcal{I},\ y+\mathcal{I},\ z+\mathcal{I}$ e $h+\mathcal{I} \in \mathcal{R}/\mathcal{I}$ tais que $x+\mathcal{I} = y+\mathcal{I}$ e $z+\mathcal{I} = h+\mathcal{I}$, mostremos que $xz+\mathcal{I} = yh+\mathcal{I}$.

Como $x+\mathcal{I} = y+\mathcal{I}$, temos que $x-y \in \mathcal{I}$, de maneira análoga, temos que $z-h \in \mathcal{I}$. Como $\mathcal{I}$ é um ideal de $\mathcal{R}$ temos que, $(x-y)z \in \mathcal{I}$ e $y(z-h) \in \mathcal{I}$. Assim,

$$[(x-y)z + y(z-h)] = xz - yz + yz - yh = xz - yz \in \mathcal{I},$$

ou seja, xz e yh estão relacionados e portanto, estão na mesma classe de equivalência. Assim, $xz+\mathcal{I} = yh+\mathcal{I}$ e a operação multiplicação está bem definida.

Vamos mostrar agora as propriedades da multiplicação, necessárias para que $\mathcal{R}/\mathcal{I}$ seja um anel.

(Associatividade): Sejam $x+\mathcal{I}, y+\mathcal{I}$ e $z+\mathcal{I} \in \mathcal{R}/\mathcal{I}$ quaisquer. Assim, temos

$$(x+\mathcal{I})\cdot[(y+\mathcal{I})\cdot(z+\mathcal{I})] = (x+\mathcal{I})\cdot[yz+\mathcal{I}] = x(yz)+\mathcal{I}.$$

Por outro lado, pela associatividade em $\mathcal{R}$ temos,

$$x(yz)+\mathcal{I} = (xy)z+\mathcal{I} = [(xy)+\mathcal{I}]\cdot(z+\mathcal{I}) = [(x+\mathcal{I})\cdot(y+\mathcal{I})]\cdot(z+\mathcal{I}).$$

Portanto,

$$(x+\mathcal{I})\cdot[(y+\mathcal{I})\cdot(z+\mathcal{I})] = [(x+\mathcal{I})\cdot(y+\mathcal{I})]\cdot(z+\mathcal{I}).$$

(Distributividade): Sejam $x+\mathcal{I}, y+\mathcal{I}$ e $z+\mathcal{I} \in \mathcal{R}/\mathcal{I}$ quaisquer. Assim temos,

$$\begin{aligned}(x+\mathcal{I})\cdot[(y+\mathcal{I})+(z+\mathcal{I})] &= (x+\mathcal{I})\cdot[(y+z)+\mathcal{I}] = (x(y+z))+\mathcal{I} \\ &= (xy+xz)+\mathcal{I} = (xy+\mathcal{I})+(xz+\mathcal{I}) \\ &= (x+\mathcal{I})\cdot(y+\mathcal{I})+(x+\mathcal{I})\cdot(z+\mathcal{I}).\end{aligned}$$

Por outro lado,

$$\begin{aligned}[(x+\mathcal{I})+(y+\mathcal{I})]\cdot(z+\mathcal{I}) &= [(x+y)+\mathcal{I}]\cdot(z+\mathcal{I}) = (x+y)z+\mathcal{I} \\ &= (xz+yz)+\mathcal{I} = (xz+\mathcal{I})+(yz+\mathcal{I}) \\ &= (x+\mathcal{I})\cdot(z+\mathcal{I})+(y+\mathcal{I})\cdot(z+\mathcal{I}).\end{aligned}$$

Portanto, $(\mathcal{R}/\mathcal{I}, +, \cdot)$ é um anel.

■

Definição 1.53. *Sejam $\mathcal{R}$ um anel e $\mathcal{I} \subseteq \mathcal{R}$ um ideal. O anel $(\mathcal{R}/\mathcal{I}, +, \cdot)$ é denominado* anel quociente *de $\mathcal{R}$ por $\mathcal{I}$.*

1.2.2 Homomorfirmos de Anéis

Assim como em grupos, agora vamos estudar funções entre anéis. Da mesma forma, as funções de interesse aqui são aquelas que preservam as operações de anéis, essas funções são chamadas de *homomorfismos de anéis.*

Definição 1.54. *Sejam $(\mathcal{R}, +, \cdot)$ e $(\mathcal{B}, \triangle, *)$ anéis. Uma função $f : \mathcal{R} \longrightarrow \mathcal{B}$ é denominado um* homomorfismo de anéis *quando, para todos $x, y \in \mathcal{R}$ tem-se:*

(i) $f(x+y) = f(x) \triangle f(y)$;

(ii) $f(x \cdot y) = f(x) * f(y)$.

Observação: Quando estamos estudando homomorfismos entre anéis é comum denotarnos as operações dos anéis pelos mesmos símbolos. Assim $(\mathcal{R}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ têm símbolos iguais, mas apesar disso, designam operações diferentes em $\mathcal{R}$ e $\mathcal{B}$.

Definição 1.55. *Um homomorfismo injetor é chamado de* monomorfismo. *Um homomorfismo sobrejetor é chamado de* epimorfismo. *Um homomorfismo bijetor é chamado*

de isomorfismo. *Um homomorfismo $f : \mathcal{R} \to \mathcal{R}$ é chamado de* endomorfismo. *Um isomorfismo $f : \mathcal{R} \to \mathcal{R}$ é chamado de* automorfismo.

Definição 1.56. *Sejam $\mathcal{R}$ e $\mathcal{B}$ anéis. Se existe $f : \mathcal{R} \longrightarrow \mathcal{B}$ um isomorfismo, dizemos que $\mathcal{R}$ e $\mathcal{B}$ são* isomorfos *e denotamos por $\mathcal{R} \simeq \mathcal{B}$.*

Exemplo 1.57. *Seja $\mathcal{I}$ um ideal de $\mathcal{R}$. A função $f : \mathcal{R} \longrightarrow \mathcal{R}/\mathcal{I}$, tal que, para todo $x \in \mathcal{R}$ tem-se $f(x) = x + \mathcal{I}$ é um homomorfismo, chamado de* homomorfismo canônico.

De fato, sejam $x, y \in \mathcal{R}$ quaisquer. Assim:

$$f(x+y) = (x+y) + \mathcal{I} = (x + \mathcal{I}) + (y + \mathcal{I}) = f(x) + f(y) \quad \text{e}$$

$$f(x \cdot y) = (x \cdot y) + \mathcal{I} = (x + \mathcal{I}) \cdot (y + \mathcal{I}) = f(x) \cdot f(y).$$

Exemplo 1.58. *Considere $\mathbb{R}$ e $M_2(\mathbb{R})$ como anéis com suas operações usuais. Seja $f : \mathbb{R} \longrightarrow M_2(\mathbb{R})$ uma função, tal que, para todo $x \in \mathbb{R}$ tem-se $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ vamos mostrar que f é um homomorfismo de anéis.*

Sejam $x, y \in \mathbb{R}$ quaisquer. Assim temos:

(i) $f(x+y) = \begin{pmatrix} x+y & 0 \\ 0 & x+y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x) + f(y).$

(ii) $f(xy) = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \cdot \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x) \cdot f(y).$

Portanto, f é um homomorfismo.

Proposição 1.59. *Sejam $(\mathcal{R}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ anéis e $f : \mathcal{R} \longrightarrow \mathcal{B}$ um epimorfismo, então:*

(i) *Se $\mathcal{R}$ tem unidade, então $\mathcal{B}$ tem unidade e $f(1_R) = 1_B$;*

(ii) *Se $\mathcal{R}$ tem unidade e $x \in \mathcal{R}$ é inversível em $\mathcal{R}$, então $f(x)$ é inversível em $\mathcal{B}$ e $f(x)^{-1} = f(x^{-1})$.*

Demonstração.

(i) Seja $y \in \mathcal{B}$ qualquer. Como f é sobrejetiva, existe $x \in \mathcal{R}$ tal que $f(x) = y$. Assim,

$$y \cdot f(1_R) = f(x) \cdot f(1_R) = f(x \cdot 1_R) = f(x) = y \quad \text{e}$$

$$f(1_R) \cdot y = f(1_R) \cdot f(x) = f(1_R \cdot x) = f(x) = y.$$

Portanto, $f(1_R) = 1_B$.

(ii) Seja $x \in \mathcal{R}$ tal que x é inversível. Assim temos,

$$f(x^{-1}) \cdot f(x) = f(x^{-1} \cdot x) = f(1_R) = 1_B \quad \text{e}$$

$$f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1_R) = 1_B.$$

Logo, $f(x^{-1})$ é o inverso de $f(x)$, ou seja, $f(x^{-1}) = f(x)^{-1}$.

■

Definição 1.60. *Seja $f : \mathcal{R} \longrightarrow \mathcal{B}$ um homomorfismo de anéis. O* núcleo *de f, denotado por $N(f)$ ou $ker(f)$, é o conjunto:*

$$N(f) = \{x \in \mathcal{R}; f(x) = 0_B\}.$$

Proposição 1.61. *Sejam $(\mathcal{R}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ anéis e $f : \mathcal{R} \longrightarrow \mathcal{B}$ um homomorfismo. Então, $\mathfrak{I}m(f)$ é um subanel de $\mathcal{B}$.*

Demonstração. Primeiro, note que $(\mathcal{R}, +)$ e $(\mathcal{B}, +)$ são grupos e que f também é um homomorfismo de grupos, então pela proposição 1.23(ii) na página 12, $(\mathfrak{I}m(f), +)$ é subgrupo de $(\mathcal{B}, +)$. Agora sejam $y_1, y_2 \in \mathfrak{I}m(f)$ quaisquer. Então, existem $x_1, x_2 \in \mathcal{R}$, tais que $f(x_1) = y_1$ e $f(x_2) = y_2$. Assim,

$$y_1 \cdot y_2 = f(x_1) \cdot f(x_2) = f(x_1 \cdot x_2).$$

Logo, $y_1 \cdot y_2 \in \mathfrak{I}m(f)$, já que $x_1 \cdot x_2 \in \mathcal{R}$. Portanto, pela proposição 1.44 na página 26, temos que $\mathfrak{I}m(f)$ é subanel de $\mathcal{B}$.

■

Proposição 1.62. *Sejam $(\mathcal{R}, +, \cdot)$ e $(\mathcal{B}, +, \cdot)$ anéis e $f : \mathcal{R} \longrightarrow \mathcal{B}$ um homomorfismo. Então $N(f)$ é um ideal de $\mathcal{R}$.*

Demonstração. Note que pelo que já argumentamos na proposição anterior, temos que $(\mathcal{R}, +)$ e $(\mathcal{B}, +)$ são grupos e que f é um homomorfismo de grupos, então novamente pela proposição 1.23(i), temos que $(N(f), +)$ é subgrupo de $(\mathcal{R}, +)$. Agora sejam $x, y \in N(f)$ quaisquer. Assim,

$$f(x \cdot y) = f(x) \cdot f(y) = 0_B \cdot 0_B = 0_B.$$

Logo, $x \cdot y \in N(f)$. Portanto, pela proposição 1.44 que $N(f)$ é subanel de $\mathcal{R}$.

Agora, sejam $x \in N(f)$ e $y \in \mathcal{R}$ quaisquer. Assim,

$$f(y \cdot x) = f(y) \cdot f(x) = f(y)0_B = 0_B,$$

já que, $x \in N(f)$. Logo, $y \cdot x \in N(f)$ e, assim, $N(f)$ é ideal à esquerda de $\mathcal{R}$

Da mesma forma, temos

$$f(x \cdot y) = f(x) \cdot f(y) = 0_B \cdot f(y) = 0_B.$$

Logo, $x \cdot y \in N(f)$ e, assim, $N(f)$ é um ideal à direta de $\mathcal{R}$.

Portanto, $N(f)$ é um ideal de $\mathcal{R}$.

■

1.2.3 Teorema do Homomorfismo para Anéis

Na seção de Grupos, demonstramos um teorema de fundamental importância para Álgebra, que é o teorema do homomorfismo para grupos. Esse teorema é uma ferramenta matemática muito importante, pois é usada para a produção de isomorfismos, tanto entre grupos, quanto entre anéis, como vamos ver agora.

Teorema 1.63 (Teorema do homomorfismo para anéis)**.** *Sejam $\mathcal{R}, \mathcal{B}$ anéis, e $f : \mathcal{R} \longrightarrow \mathcal{B}$ um homomorfismo. Então a função*

$$\begin{array}{rccc} \varphi: & \mathcal{R}/N(f) & \longrightarrow & \mathfrak{I}m(f) \\ & x + N(f) & \longmapsto & f(x) \end{array}$$

é um isomorfismo.

Demonstração. Já mostramos no teorema 1.33 na página 18, que φ está bem definida, que φ é injetiva e sobrejetiva e que ainda preserva a primeira operação. Desta forma, resta apenas mostrar que φ preserva a segunda operação, ou seja, preserva a operação multiplicação de classes. Sejam $x + N(f), y + N(f) \in \mathcal{R}/N(f)$ quaisquer. Assim,

$$\begin{aligned} \varphi((x + N(f)) \cdot (y + N(f))) &= \varphi(xy + N(f)) \\ &= f(xy) = f(x)f(y) \\ &= \varphi(x + N(f))\varphi(y + N(f)). \end{aligned}$$

Portanto, concluímos que φ é um isomorfismo. ■

Exemplo 1.64. *Considere o conjunto* $\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \longrightarrow \mathbb{R}; f \text{ é função}\}$. *Esse conjunto com as operações*

$$(f+g)(x) = f(x) + g(x) \quad e$$

$$(fg)(x) = f(x)g(x)$$

é um anel (ver exemplo 1.42 na página 23).

Seja $f \in \mathcal{F}(\mathbb{R})$ qualquer. Defina $\psi : \mathcal{F}(\mathbb{R}) \longrightarrow \mathbb{R}$ por $\psi(f) = f(0)$. Vamos mostrar que ψ é um epimorfismo.

Primeiro note que, para quaisquer $f, g \in \mathcal{F}(\mathbb{R})$ temos

$$\psi(f+g) = (f+g)(0) = f(0) + g(0) = \psi(f) + \psi(g) \quad \text{e}$$

$$\psi(fg) = f(0)g(0) = \psi(f)\psi(g).$$

Portanto, ψ é um homomorfismo de anéis. Vamos mostrar agora que ψ é sobrejetiva, para tanto, tome $c \in \mathbb{R}$ qualquer e escolha em $\mathcal{F}(\mathbb{R})$ a função constante c, ou seja, para todo $x \in \mathbb{R}$ tem-se $f(x) = c$. Assim, $\psi(f) = f(0) = c$, logo ψ é sobrejetiva.

Vamos calcular $N(\psi)$. Seja $f \in N(\psi)$ qualquer. Então, $\psi(f) = f(0) = 0$.

Logo, $N(\psi) = \{f : \mathbb{R} \longrightarrow \mathbb{R}; f(0) = 0\}$, ou seja, o núcleo de ψ é formado pelas funções que se anulam em 0. Assim, pelo teorema do homomorfismo, temos que

$$\mathcal{F}(\mathbb{R})/N(\psi) \simeq \mathbb{R}$$

uma vez que $\mathfrak{I}m(\psi) = \mathbb{R}$.

1.3 Espaços Vetoriais

Quando estudamos a estrutura de anéis, verificamos que na definição está presente a estrutura de grupos. Agora, iremos estudar mais uma estrutura, em que está presente a estrutura de grupos. Isso reforça a importância dos grupos. Na seção de anéis demos a definição de corpo (ver definição 1.38 na página 20). Agora, vamos ver que podemos definir uma operação entre os elementos do conjunto e os elementos de um corpo, estes últimos chamados de escalares.

Definição 1.65. *Seja* $\mathbb{K}$ *um corpo. Um* espaço vetorial $(\mathcal{V}, +, \cdot)$ *sobre* $\mathbb{K}$ *é um conjunto não vazio* $\mathcal{V}$*, munido de uma operação denotada por* $+$ *(chamada de soma), e de uma operação entre os elementos de* $\mathbb{K}$ *e os elementos de* $\mathcal{V}$*, denotada por* $\cdot$ *(chamada de produto por escalar), tais que para todo* $x, y \in \mathcal{V}$ *e* $\alpha, \beta \in \mathbb{K}$*, as seguintes condições são satisfeitas:*

S: $(\mathcal{V}, +)$ *é um grupo abeliano;*

PE1: $\alpha \cdot (\beta \cdot x) = (\alpha\beta) \cdot x$*;*

PE2: $1 \cdot x = x$*, em que 1 é a unidade de* $\mathbb{K}$*;*

PE3: $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$*;*

PE4: $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$*.*

Mais uma vez por simplicidade diremos que $\mathcal{V}$ é um espaço vetorial sobre $\mathbb{K}$, em vez de $(\mathcal{V}, +, \cdot)$, ou seja, fica subentendida a existência das operações.

Definição 1.66. *Seja* $\mathcal{V}$ *um espaço vetorial sobre* $\mathbb{K}$*. Denominamos os elementos de* $\mathcal{V}$ *de* vetores *e o elemento neutro da soma em* $\mathcal{V}$*, denominamos de* vetor nulo *e o denotamos por* $\vec{0}$*.*

Exemplo 1.67. *Considere o conjunto* $M_2(\mathbb{R})$ *com a soma usual de matrizes.* $(M_2(\mathbb{R}), +, \cdot)$ *é um espaço vetorial sobre* $\mathbb{R}$*, em que a multiplicação por escalar para quaisquer* $\alpha \in \mathbb{R}$ *e* $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R})$ *é definida abaixo:*

$$\alpha \cdot A = \alpha \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix},$$

onde o produto αa_{ij} *é o produto em* $\mathbb{R}$*, em que,* $i, j \in \{1, 2\}$*.*

De fato, já mostramos no exemplo 1.2 na página 4, que $(M_2(\mathbb{R}), +)$ é um grupo abeliano. Resta mostrarmos as propriedades **PE1**, **PE2**, **PE3** e **PE4**. Para tanto, considere $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(\mathbb{R})$ e $\alpha, \beta \in \mathbb{R}$ quaisquer.

PE1 $\alpha \cdot (\beta \cdot A) = \alpha \cdot \left(\beta \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \right) = \alpha \cdot \begin{pmatrix} \beta a_{11} & \beta a_{12} \\ \beta a_{21} & \beta a_{22} \end{pmatrix}$

$$= \begin{pmatrix} \alpha(\beta a_{11}) & \alpha(\beta a_{12}) \\ \alpha(\beta a_{21}) & \alpha(\beta a_{22}) \end{pmatrix} = \begin{pmatrix} (\alpha\beta)a_{11} & (\alpha\beta)a_{12} \\ (\alpha\beta)a_{21} & (\alpha\beta)a_{22} \end{pmatrix} = (\alpha\beta) \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = (\alpha\beta) \cdot A.$$

PE2 $1 \cdot A = 1 \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1a_{11} & 1a_{12} \\ 1a_{21} & 1a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = A.$

PE3 $(\alpha + \beta) \cdot A = (\alpha + \beta) \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} (\alpha+\beta)a_{11} & (\alpha+\beta)a_{12} \\ (\alpha+\beta)a_{21} & (\alpha+\beta)a_{22} \end{pmatrix}$

$$= \begin{pmatrix} \alpha a_{11} + \beta a_{11} & \alpha a_{12} + \beta a_{12} \\ \alpha a_{21} + \beta a_{21} & \alpha a_{22} + \beta a_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix} + \begin{pmatrix} \beta a_{11} & \beta a_{12} \\ \beta a_{21} & \beta a_{22} \end{pmatrix}$$

$$= \alpha \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \beta \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \alpha \cdot A + \beta \cdot A.$$

PE4 $\alpha \cdot (A + B) = \alpha \cdot \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) = \alpha \cdot \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$

$$= \begin{pmatrix} \alpha(a_{11} + b_{11}) & \alpha(a_{12} + b_{12}) \\ \alpha(a_{21} + b_{21}) & \alpha(a_{22} + b_{22}) \end{pmatrix} = \begin{pmatrix} \alpha a_{11} + \alpha b_{11} & \alpha a_{12} + \alpha b_{12} \\ \alpha a_{21} + \alpha b_{21} & \alpha a_{22} + \alpha b_{22} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix} + \begin{pmatrix} \alpha b_{11} & \alpha b_{12} \\ \alpha b_{21} & \alpha b_{22} \end{pmatrix} = \alpha \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \alpha \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \alpha \cdot A + \alpha \cdot B.$$

Portanto, $(M_2(\mathbb{R}), +, \cdot)$ é um espaço vetorial sobre $\mathbb{R}$.

Na verdade, de forma análoga, mostra-se que $(M_n(\mathbb{R}), +, \cdot)$ é um espaço vetorial sobre $\mathbb{R}$, para $n \in \mathbb{N},\ n \geq 2$. Mais ainda, mostra-se que $(M_{n\times m}(\mathbb{R}), +, \cdot)$ é um espaço vetorial sobre $\mathbb{R}$, para $m, n \in \mathbb{N},\ m, n \geq 2$.

Exemplo 1.68. *Seja* $\mathbb{K}^n = \{(x_1, x_2, \ldots, x_n); x_1, \ldots, x_n \in \mathbb{K}\}$. *Sejam* $X = (x_1, x_2, \ldots, x_n)$ *e* $Y = (y_1, y_2, \ldots, y_n)$ *elementos de* $\mathbb{K}^n$. *Chamamos* $x_1, x_2, \ldots, x_n$ *de* coordenadas *de* X. *Definimos*

$$X + Y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

Se $\alpha \in \mathbb{K}$, *definimos*

$$\alpha X = (\alpha x_1, \ldots, \alpha x_n).$$

Pode-se mostrar, que $\mathbb{K}^n$ *com as operações definidas anteriormente, é um espaço vetorial sobre* $\mathbb{K}$.

Exemplo 1.69. *Considere o conjunto* $\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \longrightarrow \mathbb{R}; f \text{ é função}\}$. *Mostramos no exemplo 1.42 na página 23, que* $(\mathcal{F}(\mathbb{R}), +)$ *é um grupo abeliano. Mostremos agora que* $(\mathcal{F}(\mathbb{R}), +, \cdot)$ *é um espaço vetorial sobre* $\mathbb{R}$, *em que o produto por escalar* $\cdot$ *é definido, para todo* $\alpha, x \in \mathbb{R}$ *e* $f \in \mathcal{F}(\mathbb{R})$, *como* $(\alpha \cdot f)(x) = \alpha f(x)$.

De fato, sejam $\alpha, \beta, x \in \mathbb{R}$ e $f, g \in \mathcal{F}(\mathbb{R})$ quaisquer. Assim temos:

PE1 $\alpha \cdot (\beta \cdot f)(x) = \alpha \cdot (\beta f(x)) = (\alpha\beta)f(x) = ((\alpha\beta) \cdot f)(x)$.

Logo, $\alpha \cdot (\beta \cdot f) = (\alpha\beta) \cdot f$.

PE2 $(1 \cdot f)(x) = 1f(x) = f(x)$. Logo, $(1 \cdot f) = f$.

PE3 $((\alpha + \beta) \cdot f)(x) = (\alpha + \beta)f(x) = \alpha f(x) + \beta f(x) = (\alpha \cdot f)(x) + (\beta \cdot f)(x)$.

Logo, $(\alpha + \beta) \cdot f = \alpha \cdot f + \beta \cdot f$.

PE4
$$\begin{aligned}(\alpha \cdot (f + g))(x) &= \alpha(f + g)(x) = \alpha(f(x) + g(x)) \\ &= \alpha f(x) + \alpha g(x) = (\alpha \cdot f)(x) + (\alpha \cdot g)(x).\end{aligned}$$

Logo, $\alpha \cdot (f + g) = \alpha \cdot f + \alpha \cdot g$.

Mostramos assim, que $(\mathcal{F}(\mathbb{R}), +, \cdot)$ é um espaço vetorial sobre $\mathbb{R}$.

1.3.1 Subespaços Vetoriais, Base e Dimensão

Definição 1.70. *Seja $\mathcal{V}$ um espaço vetorial sobre $\mathbb{K}$. Um* subespaço vetorial *de $\mathcal{V}$ é um subconjunto não vazio $\mathcal{W} \subseteq \mathcal{V}$, tal que para todo $x, y \in \mathcal{W}$ e $\alpha \in \mathbb{K}$ tem-se:*

(i) $x + y \in \mathcal{W}$;

(ii) $\alpha \cdot x \in \mathcal{W}$.

Proposição 1.71. *Seja $(\mathcal{V}, +, \cdot)$ um espaço vetorial sobre $\mathbb{K}$. Se $\mathcal{W} \subseteq \mathcal{V}$ é um subespaço vetorial de $\mathcal{V}$, então $(\mathcal{W}, +, \cdot)$ é um espaço vetorial sobre $\mathbb{K}$.*

Demonstração. Primeiramente, por definição $\mathcal{W}$ é não vazio. Agora, pelo item (ii) da definição acima, tomando $\alpha = -1$, em que -1 é o oposto de 1(unidade em $\mathbb{K}$). Temos

$$0y = (1 - 1)y = 1y - 1y = y - 1y = \vec{0} = y - y,$$

em que $-y$ é o oposto de y. Assim,

$$y - 1y = y - y \Longrightarrow -1y = -y.$$

Portanto, para todo $y \in \mathcal{W}$ temos que $-1y = -y \in \mathcal{W}$, assim pelo item (i) temos $x - y \in \mathcal{W}$. Portanto, pela proposição 1.10 na página 8, temos que $(\mathcal{W}, +)$ é um subgrupo abeliano de $(\mathcal{V}, +)$, uma vez que $(\mathcal{V}, +)$ é abeliano.

Sejam $x, y \in \mathcal{W}$ e $\alpha, \beta \in \mathbb{K}$ quaisquer. Assim temos:

PE1 é válida por (iii) e pelo fato de que $\mathcal{W}$ é um subconjunto de $\mathcal{V}$.

PE2 é válida pelo fato de que $\mathcal{W}$ é um subconjunto de $\mathcal{V}$.

PE3 é válida por (iii) e pelo fato de que $\mathcal{W}$ é um subconjunto de $\mathcal{V}$.

PE4 é válida por (ii) e por (iii) e pelo fato de que $\mathcal{W}$ é um subconjunto de $\mathcal{V}$.

Portanto, $(\mathcal{W}, +, \cdot)$ é um espaço vetorial sobre $\mathbb{K}$.

■

Exemplo 1.72. *O conjunto* $sl_2(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ z & -x \end{pmatrix}; x, y, z \in \mathbb{R} \right\}$, *é um subespaço vetorial de* $M_2(\mathbb{R})$.

De fato, já mostramos no exemplo 1.11 na página 9 que $sl_2(\mathbb{R}) \subset M_2(\mathbb{R})$ e que a soma é fechada em $sl_2(\mathbb{R})$. Agora sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix} \in sl_2(\mathbb{R})$ e $\alpha \in \mathbb{R}$ quaisquer. Assim,

$$\alpha \cdot A = \alpha \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha(-a_{11}) \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & -\alpha a_{11} \end{pmatrix} \in sl_2(\mathbb{R}).$$

Logo, $sl_2(\mathbb{R})$ é subespaço vetorial de $M_2(\mathbb{R})$ e, portanto, é também um espaço vetorial sobre $\mathbb{R}$.

Definição 1.73. *Sejam* $\mathcal{V}$ *um espaço vetorial qualquer sobre* $\mathbb{K}$ *e* $b_1, b_2, \ldots, b_n$ *elementos de* $\mathcal{V}$. *Sejam* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *elementos de* $\mathbb{K}$. *Uma expressão do tipo:*

$$\alpha_1 b_1 + \cdots + \alpha_n b_n$$

é denominada uma combinação linear *de* $b_1, \cdots, b_n$.

Definição 1.74. *Sejam* $\mathcal{V}$ *um espaço vetorial sobre* $\mathbb{K}$ *e* $b_1, b_2, \ldots, b_n$ *elementos de* $\mathcal{V}$. *O conjunto*

$$\mathcal{W} = \{\alpha_1 b_1 + \cdots + \alpha_n b_n;\ \alpha_1, \ldots, \alpha_n \in \mathbb{K}\}$$

é denominado conjunto gerado *por* $b_1, \cdots, b_n$ *e o conjunto*

$$\mathcal{S} = \{b_1, b_2, \ldots, b_n\}$$

é denominado conjunto gerador. *Nesse caso, dizemos que* $\mathcal{S}$ *gera o conjunto* $\mathcal{W}$ *ou que* $\mathcal{W}$ *é gerado por* $\mathcal{S}$.

Não é difícil mostrar que $\mathcal{W}$ é um subespaço vetorial de $\mathcal{V}$.

Definição 1.75. *Sejam $\mathcal{V}$ um espaço vetorial qualquer sobre $\mathbb{K}$ e $b_1, b_2, \ldots, b_n$ elementos de $\mathcal{V}$. Diremos que $b_1, b_2, \ldots, b_n$ são* linearmente dependentes *sobre $\mathbb{K}$, se existem $\alpha_1, \alpha_2, \ldots, \alpha_n$ em $\mathbb{K}$, nem todos nulos, tais que:*

$$\alpha_1 b_1 + \cdots + \alpha_n b_n = \vec{0}.$$

Se não existem tais números, dizemos que $b_1, b_2, \ldots, b_n$ são linearmente independentes*, ou seja, se $\alpha_1, \alpha_2, \ldots, \alpha_n$ são tais que*

$$\alpha_1 b_1 + \cdots + \alpha_n b_n = \vec{0}$$

então, para todo $i = \{1, 2, \ldots, n\}$, tem-se $\alpha_i = 0$.

Já mostramos no exemplo 1.69 na página 37, que $\mathcal{F}(\mathbb{R})$ é um espaço vetorial sobre $\mathbb{R}$. Não provaremos isso aqui, mas o subconjunto $\mathcal{V}$ de $\mathcal{F}(\mathbb{R})$ formado por todas as funções contínuas de $\mathbb{R}$ em $\mathbb{R}$ é um subespaço vetorial de $\mathcal{F}(\mathbb{R})$. Assim como o subconjunto $\mathcal{W}$ de $\mathcal{V}$ formado por todas as funções diferenciáveis é um subespaço vetorial de $\mathcal{V}$, uma vez que toda função diferenciável é contínua.

Exemplo 1.76. *Considere as funções $f(x) = e^x$ e $g(x) = e^{2x}$ ambas são elementos de $\mathcal{W}$, ou seja, são diferenciáveis. Vamos mostrar que estas funções são linearmente independentes.*

De fato, suponha que existam $\alpha, \beta \in \mathbb{R}$ tais que:

$$\alpha e^x + \beta e^{2x} = 0$$

Derivando com relação a x temos:

$$\alpha e^x + 2\beta e^{2x} = 0$$

Subtraindo a primeira da segunda temos $\beta e^{2x} = 0$, assim, $\beta = 0$ e da primeira relação segue que $\alpha e^x = 0$, logo $\alpha = 0$ e portanto, e^x e e^{2x} são linearmente independentes.

Definição 1.77. *Uma* base *de um espaço vetorial $\mathcal{V}$ sobre $\mathbb{K}$ é um conjunto $\mathcal{B} \subseteq \mathcal{V}$ linearmente independente que gera $\mathcal{V}$.*

Não iremos provar aqui, mas todo espaço vetorial admite uma base, não necessariamente finita. É possível mostrar que duas bases quaisquer de um espaço vetorial têm a

mesma quantidade de elementos. Estes fatos motivam nossas próximas definições.

Definição 1.78. *Sejam $\mathcal{V}$ um espaço vetorial sobre $\mathbb{K}$ e $\mathcal{B} \subseteq \mathcal{V}$ uma base para $\mathcal{V}$. Denominamos* dimensão *de $\mathcal{V}$ a quantidade de elementos que formam a base $\mathcal{B}$.*

Definição 1.79. *Diz-se que o espaço vetorial $\mathcal{V}$ tem dimesão finita se admite uma base $\mathcal{B} = \{b_1, \ldots, b_n\}$ com um número finito n de elementos. Nesse caso, denotamos a dimensão do espaço vetorial $\mathcal{V}$ por $dim\mathcal{V} = n$.*

Definição 1.80. *Diz-se que o espaço vetorial $\mathcal{V}$ tem dimesão infinita e denotamos por $dim\mathcal{V} = \infty$ quando ele não tem dimensão finita, ou seja, quando nenhum subconjunto finito de $\mathcal{V}$ é uma base.*

Exemplo 1.81. *Vamos determinar uma base e a dimensão do espaço vetorial $M_2(\mathbb{R})$.*

Seja $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(\mathbb{R})$ qualquer. Temos

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + a_{12}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a_{21}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + a_{22}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

ou seja, os vetores:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ e } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

geram os elementos de $M_2(\mathbb{R})$. Além disso, se

$$\alpha\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \beta\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \gamma\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + \lambda\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

então $\alpha = \beta = \gamma = \lambda = 0$ e logo os vetores são linearmente independentes, portanto, o conjunto

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

é uma base para $M_2(\mathbb{R})$ e $dimM_2(\mathbb{R}) = 4$.

A base determinada de $M_2(\mathbb{R})$ a cima é a chamada base canônica. Para representarmos os elementos da base canônica, usamos a seguinte notação:

$$e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

ou seja, e_{12} indica que o número 1 se encontra na primeira linha e segunda coluna, os

outros elementos da matriz são nulos. De maneira genérica, o conjunto $\{e_{ij}\}$ tal que, $i, j \in \{1, 2, \ldots, n\}$ constitui uma base para $M_n(\mathbb{R})$ e ainda $dim M_n(\mathbb{R}) = n^2$.

Exemplo 1.82. *Consideremos o subespaço vetorial $sl_2(\mathbb{R})$ de $M_2(\mathbb{R})$. Vamos encontrar uma base para $sl_2(\mathbb{R})$ e calcular a dimensão desse espaço vetorial.*

Note que se $A \in sl_2(\mathbb{R})$ é qualquer, então A é da forma

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix}$$

e perceba que

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix} = a_{11} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + a_{12} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + a_{21} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

ou seja, os vetores

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ e } \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

geram os elementos de $sl_2(\mathbb{R})$.

Resta mostrarmos que esses vetores são linearmente independentes. Para tanto, considere $\alpha, \beta, \gamma \in \mathbb{R}$ tais que,

$$\alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Assim,

$$\alpha \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

logo $\alpha = \beta = \gamma = 0$. Portanto, o conjunto

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}$$

é uma base para $sl_2(\mathbb{R})$ e sua dimensão é exatamente o número de vetores que forma a base, ou seja, $dim\, sl_2(\mathbb{R}) = 3$.

Definição 1.83. *Sejam $\mathcal{V}$ um espaço vetorial sobre $\mathbb{K}$ e $\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_k$ subespaços ve-*

toriais de $\mathcal{V}$. Definimos a soma dos subespaços vetoriais $\mathcal{W}_1, \mathcal{W}_2, \ldots, \mathcal{W}_k$ por

$$\sum_{i=1}^{k} \mathcal{W}_i = \mathcal{W}_1 + \mathcal{W}_2 + \ldots + \mathcal{W}_k = \{x_1 + \ldots + x_k;\ x_i \in \mathcal{W}_i\}.$$

Definição 1.84. *Sejam $\mathcal{V}$ um espaço vetorial sobre $\mathbb{K}$ e $\mathcal{W}_1, \mathcal{W}_2$ dois subespaços de $\mathcal{V}$, tais que $\mathcal{V} = \mathcal{W}_1 + \mathcal{W}_2$. Dizemos que $\mathcal{V} = \mathcal{W}_1 + \mathcal{W}_2$ é a* soma direta *dos subespaços $\mathcal{W}_1, \mathcal{W}_2$ se $\mathcal{W}_1 \cap \mathcal{W}_2 = \{\vec{0}\}$. Nesse caso, denotamos*

$$\mathcal{V} = \mathcal{W}_1 \oplus \mathcal{W}_2.$$

É possível mostrar que se $\mathcal{V} = \mathcal{W}_1 \oplus \mathcal{W}_2$, então todo $x \in \mathcal{V}$ se escreve de forma única como $x = w_1 + w_2$, em que $w_1 \in \mathcal{W}_1$ e $w_2 \in \mathcal{W}_2$.

Não provaremos, aqui, a nossa próxima proposição a prova pode ser encontrada em [6], página 36.

Proposição 1.85. *Sejam $\mathcal{V}$ um espaço vetorial de dimensão finita sobre $\mathbb{K}$ e $\mathcal{W}_1, \mathcal{W}_2$ dois subespaços de $\mathcal{V}$, tais que $\mathcal{V} = \mathcal{W}_1 \oplus \mathcal{W}_2$. Então,*

$$dim(\mathcal{V}) = dim(\mathcal{W}_1) + dim(\mathcal{W}_2).$$

1.3.2 Transformações Lineares

Nessa subseção, estudaremos um pouco sobre aplicações entre espaços vetoriais. Mais especificamente, estamos interessados em aplicações que têm algumas propriedades importantes. Estamos falando, das transformações lineares, um caso particular de aplicações.

Na definição abaixo, por simplicidade, vamos usar os mesmos símbolos denotando as operações de $+$ (soma) e $\cdot$ (produto por escalar), tanto em $\mathcal{V}$, quanto em $\mathcal{W}$. O leitor deve estar atento que apesar da notação estes símbolos denotam operações em espaços diferentes.

Definição 1.86. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$. Uma* transformação linear

$$F : \mathcal{V} \longrightarrow \mathcal{W}$$

é uma aplicação que satisfaz as seguintes propriedades:

(i) *Para quaisquer $x, y \in \mathcal{V}$ tem-se $F(x + y) = F(x) + F(y)$;*

(ii) *Para quaisquer $x \in \mathcal{V}$ e $\alpha \in \mathbb{K}$ tem-se $F(\alpha \cdot x) = \alpha \cdot F(x)$.*

Exemplo 1.87. *Seja P uma matriz inversível em $M_n(\mathbb{R})$. Para todo $A \in M_n(\mathbb{R})$ defina $F : M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$ por $F(A) = P^{-1}AP$. Vamos mostrar que F é uma transformação linear.*

De fato, sejam $A, B \in M_n(\mathbb{R})$ e $\alpha \in \mathbb{R}$ quaisquer. Assim

$F(A+B) = P^{-1}(A+B)P = P^{-1}AP + P^{-1}BP = F(A) + F(B)$ e

$F(\alpha A) = P^{-1}(\alpha A)P = \alpha(P^{-1}AP) = \alpha F(A)$.

Nesse exemplo, é usado o produto usual de matrizes que é associativo e o produto por escalar usual de matrizes.

Vimos um exemplo não trivial de transformações lineares, mas será que, dados quaisquer dois espaços vetoriais, sempre existe uma transformação linear entre eles? O nosso próximo exemplo mostrará que sim.

Exemplo 1.88 (Transformação linear nula)**.** *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$. Considere $F : \mathcal{V} \longrightarrow \mathcal{W}$, tal que para todo $x \in \mathcal{V}$ tem-se $F(x) = \vec{0}_w$ em que, $\vec{0}_w$ é o elemento neutro da soma em $\mathcal{W}$. Então F é uma transformação linear.*

De fato, sejam $x, y \in \mathcal{V}$ e $\alpha \in \mathbb{K}$ quaisquer. Como $\mathcal{V}$ é espaço vetorial, então $x+y \in \mathcal{V}$ e $\alpha x \in \mathcal{V}$. Assim,

$$F(x+y) = \vec{0}_w = \vec{0}_w + \vec{0}_w = F(x) + F(y) \quad \text{e}$$

$$F(\alpha x) = \vec{0}_w = \alpha\vec{0}_w = \alpha F(x).$$

Logo, F é uma transformação linear.

Exemplo 1.89 (Transformação linear identidade)**.** *Seja $\mathcal{V}$ um espaço vetorial sobre $\mathbb{K}$. Considere $F : \mathcal{V} \longrightarrow \mathcal{V}$, tal que para todo $x \in \mathcal{V}$ tem-se $F(x) = x$. Então F é uma transformação linear.*

De fato, sejam $x, y \in \mathcal{V}$ e $\alpha \in \mathbb{K}$ quaisquer. Como $\mathcal{V}$ é espaço vetorial, então $x+y \in \mathcal{V}$ e $\alpha x \in \mathcal{V}$. Assim,

$$F(x+y) = x + y = F(x) + F(y) \quad \text{e}$$

$$F(\alpha x) = \alpha x = \alpha F(x).$$

Logo, F é uma transformação linear.

Definição 1.90. *Sejam $\mathcal{V}$, $\mathcal{W}$ espaços vetoriais e $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação*

linear. O núcleo *de F, denotado por $N(F)$ ou $ker(F)$, é o conjunto:*

$$N(F) = \left\{ x \in \mathcal{V}; f(x) = \vec{0}_w \right\}.$$

Proposição 1.91. *Sejam $\mathcal{V}$, $\mathcal{W}$ espaços vetoriais e $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação linear. Considere $\vec{0}_v$, $\vec{0}_w$ os vetores nulos, respectivamente de $\mathcal{V}$ e $\mathcal{W}$, e $-x$ o simétrico de $x \in \mathcal{V}$. Então:*

(i) $F(\vec{0}_v) = \vec{0}_w$*;*

(ii) $F(-x) = -F(x)$*, em que $-F(x)$ é o simétrico de $F(x)$ em $\mathcal{W}$.*

Demonstração. (i) De fato, temos,

$$F(\vec{0}_v) + \vec{0}_w = F(\vec{0}_v) = F(\vec{0}_v + \vec{0}_v) = F(\vec{0}_v) + F(\vec{0}_v),$$

operando com o simétrico de $F(\vec{0}_v)$ temos,

$$-F(\vec{0}_v) + F(\vec{0}_v) + \vec{0}_w = -F(\vec{0}_v) + F(\vec{0}_v) + F(\vec{0}_v).$$

Assim, $F(\vec{0}_v) = \vec{0}_w$.

(ii) Por (i) temos que, $\vec{0}_w = F(\vec{0}_v)$. Assim,

$$F(x) - F(x) = \vec{0}_w = F(\vec{0}_v) = F(x - x) = F(x) + F(-x),$$

ou seja,

$$F(x) - F(x) = F(x) + F(-x),$$

operando com o simétrico de $F(x)$ em ambos os lados, temos

$$-F(x) + F(x) - F(x) = -F(x) + F(x) + F(-x).$$

Portanto, $-F(x) = F(-x)$.

Concluímos assim nossa demonstração.

■

Proposição 1.92. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$. Seja $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação linear. Então $N(F)$ é um subespaço vetorial de $\mathcal{V}$.*

Demonstração. De fato, sejam $x, y \in N(F)$ e $\alpha \in \mathbb{K}$ quaisquer. Já mostramos na proposição anterior, que $F(\vec{0}_v) = \vec{0}_w$, assim, $\vec{0}_v \in N(F)$. Agora,

$$F(x+y) = F(x) + F(y) = \vec{0}_w + \vec{0}_w = \vec{0}_w.$$

Logo, $x + y \in N(F)$. Também,

$$F(\alpha x) = \alpha F(x) = \alpha \vec{0}_w = \vec{0}_w.$$

Logo, $\alpha x \in N(F)$. Portanto, pela definição 1.70 na página 38, temos que $N(F)$ é um subespaço vetorial de $\mathcal{V}$.

■

Proposição 1.93. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$. Seja $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação linear. Então $\mathfrak{I}m(F)$ é um subespaço vetorial de $\mathcal{W}$.*

Demonstração. Primeiro note que, pela proposição 1.91 na página 45, temos $F(\vec{0}_v) = \vec{0}_w$ ou seja, $\vec{0}_w \in \mathfrak{I}m(F)$. Agora sejam $y_1, y_2 \in \mathfrak{I}m(F)$ e $\alpha \in \mathbb{K}$ quaisquer, então existem $x_1, x_2 \in \mathcal{V}$ tais que, $F(x_1) = y_1$ e $F(x_2) = y_2$. Assim, temos

$$y_1 + y_2 = F(x_1) + F(x_2) = F(x_1 + x_2).$$

Logo, $y_1 + y_2 \in \mathfrak{I}m(F)$.

Agora, temos

$$\alpha y_1 = \alpha F(x_1) = F(\alpha x_1).$$

Logo, $\alpha y_1 \in \mathfrak{I}m(F)$.

Portanto, pela definição 1.70 na página 38, temos que $\mathfrak{I}m(F)$ é um subespaço vetorial de $\mathcal{W}$.

■

Proposição 1.94. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$ e F, T transformações lineares de $\mathcal{V}$ em $\mathcal{W}$. Defina, para todo $x \in \mathcal{V}$ e $\alpha \in \mathbb{K}$ a soma:*

$$(F+T)(x) = F(x) + T(x).$$

E o produto por escalar:

$$(\alpha \cdot F)(x) = \alpha F(x).$$

Então, $F+T$ e $\alpha \cdot F$ são transformações lineares de $\mathcal{V}$ em $\mathcal{W}$.

Demonstração. Sejam $x, y \in \mathcal{V}$ e $\alpha, \beta \in \mathbb{K}$ quaisquer. Assim,

$$(F+T)(x+y) = F(x+y) + T(x+y) = F(x) + F(y) + T(x) + T(y).$$

Como $(\mathcal{W}, +)$ é um grupo abeliano, temos que

$$F(x) + F(y) + T(x) + T(y) = F(x) + T(x) + F(y) + T(y) = (F+T)(x) + (F+T)(y),$$

ou seja,

$$(F+T)(x+y) = (F+T)(x) + (F+T)(y).$$

Agora temos,

$$(F+T)(\alpha x) = F(\alpha x) + T(\alpha x) = \alpha F(x) + \alpha T(x),$$

pois F e T são lineares. Assim,

$$\alpha F(x) + \alpha T(x) = \alpha(F(x) + T(x)) = \alpha(F+T)(x),$$

ou seja,

$$(F+T)(\alpha x) = \alpha(F+T)(x).$$

Portanto, $F+T$ é transformação linear.

Agora,

$$\begin{aligned}(\alpha \cdot F)(x+y) &= \alpha F(x+y) = \alpha(F(x) + F(y)) \\ &= \alpha F(x) + \alpha F(y) = (\alpha \cdot F)(x) + (\alpha \cdot F)(y) \quad \text{e}\end{aligned}$$

$$(\alpha \cdot F)(\beta x) = \alpha F(\beta x) = \alpha\beta F(x),$$

pois F é linear. Assim,

$$\alpha\beta F(x) = \beta(\alpha F(x)) = \beta(\alpha \cdot F)(x).$$

Portanto, $\alpha \cdot F$ é transformação linear.

Concluímos assim, a demonstração.

■

Exemplo 1.95. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$. Consideremos o conjunto de todas as transformações lineares de $\mathcal{V}$ em $\mathcal{W}$ e denotemos esse conjunto por $\mathcal{L}(\mathcal{V},\mathcal{W})$. Defina, para quaisquer $F,T \in \mathcal{L}(\mathcal{V},\mathcal{W})$ e $\alpha \in \mathbb{K}$ as seguintes operações:*

$$\begin{array}{rccc} + : & \mathcal{L}(\mathcal{V},\mathcal{W}) \times \mathcal{L}(\mathcal{V},\mathcal{W}) & \longrightarrow & \mathcal{L}(\mathcal{V},\mathcal{W}) \\ & (F,T) & \longmapsto & F+T, \end{array}$$

em que $(F+T)(x) = F(x)+T(x)$ e

$$\begin{array}{rccc} \cdot : & \mathbb{K} \times \mathcal{L}(\mathcal{V},\mathcal{W}) & \longrightarrow & \mathcal{L}(\mathcal{V},\mathcal{W}) \\ & (\alpha,F) & \longmapsto & \alpha \cdot F, \end{array}$$

em que $(\alpha \cdot F)(x) = \alpha F(x)$. Então $(\mathcal{L}(\mathcal{V},\mathcal{W}),+,\cdot)$ é um espaço vetorial sobre $\mathbb{K}$. Note que a soma em $F+T$ é a soma definida em $\mathcal{L}(\mathcal{V},\mathcal{W})$ e a soma em $F(x)+T(x)$ é a soma em $\mathcal{W}$, também o produto por escalar em $\alpha \cdot F$ é o produto definido em $\mathcal{L}(\mathcal{V},\mathcal{W})$ e o produto por escalar em $\alpha F(x)$ é o produto em $\mathcal{W}$.

Demonstração. Primeiramente, $\mathcal{L}(\mathcal{V},\mathcal{W})$ não é vazio, pois a transformação nula (ver exemplo 1.88 na página 44) pertence a $\mathcal{L}(\mathcal{V},\mathcal{W})$. Note que as operações acima são fechadas, devido à proposição anterior.

Vamos mostrar que $\mathcal{L}(\mathcal{V},\mathcal{W})$ é um grupo abeliano. Para tanto, sejam $F,T,S \in \mathcal{L}(\mathcal{V},\mathcal{W})$ e $x \in \mathcal{V}$ quaisquer. Assim temos:

Associatividade: $(F+(T+S))(x) = F(x)+(T+S)(x) = F(x)+(T(x)+S(x))$. Pela associatividade em $\mathcal{W}$ temos
$F(x)+(T(x)+S(x)) = (F(x)+T(x))+S(x) = (F+T)(x)+S(x) = ((F+T)+S)(x)$.

Logo, $F+(T+S) = (F+T)+S$.

Comutatividade: $(F+T)(x) = F(x)+T(x)$. Pela comutatividade em $\mathcal{W}$ temos,
$F(x)+T(x) = T(x)+F(x) = (T+F)(x)$.

Logo, $F+T = T+F$.

Existência do elemento neutro: Considere, para todo $x \in \mathcal{V}$, $T_e(x) = \vec{0}_w$. Assim,

$$(F+T_e)(x) = F(x)+T_e(x) = T_e(x)+F(x) = \vec{0}_w + F(x) = F(x).$$

Portanto, $F+T_e = T_e+F = F$.

Existência do elemento simétrico: Considere $-F(x)$ o simétrico de $F(x)$ em $\mathcal{W}$ e defina

$$\begin{array}{rccc} -F: & \mathcal{V} & \longrightarrow & \mathcal{W} \\ & x & \longmapsto & -F(x). \end{array}$$

Assim,

$$(F+(-F))(x) = F(x)+(-F(x)) = F(x)-F(x) = \vec{0}_w = T_e(x) \quad \text{e}$$

$$((-F)+F)(x) = (-F(x))+F(x) = -F(x)+F(x) = \vec{0}_w = T_e(x).$$

Logo, $F+(-F) = T_e$ e $(-F)+F = T_e$, portanto $-F$ é o simétrico de F.

Mostramos assim que $(\mathcal{L}(\mathcal{V},\mathcal{W}),+)$ é um grupo abeliano. Resta mostrarmos então as propriedades **PE1**, **PE2**, **PE3** e **PE4** de espaço vetorial. Para tanto, sejam F, $T \in \mathcal{L}(\mathcal{V},\mathcal{W})$, $x \in \mathcal{V}$ e $\alpha, \beta \in \mathbb{K}$ quaisquer. Assim,

PE1: $(\alpha \cdot (\beta \cdot F))(x) = \alpha(\beta \cdot F)(x) = \alpha(\beta F(x))$. Como $F(x) \in \mathcal{W}$ que, por sua vez é um espaço vetorial, temos

$$\alpha(\beta F(x)) = (\alpha\beta)F(x) = ((\alpha\beta)\cdot F)(x).$$

Logo, $\alpha \cdot (\beta \cdot F) = (\alpha\beta)\cdot F$.

PE2: $(1 \cdot F)(x) = 1F(x)$. Novamente, como $F(x) \in \mathcal{W}$ que, por sua vez, é um espaço vetorial, temos $1F(x) = F(x)$, em que 1 é a unidade de $\mathbb{K}$.

Logo, $1 \cdot F = F$.

PE3: $((\alpha+\beta)\cdot F)(x) = (\alpha+\beta)F(x) = \alpha F(x) + \beta F(x) = (\alpha \cdot F)(x) + (\beta \cdot F)(x)$.

Logo, $(\alpha+\beta)\cdot F = \alpha \cdot F + \beta \cdot F$.

PE4: $(\alpha \cdot (F+T))(x) = \alpha((F+T)(x)) = \alpha(F(x)+T(x)) = \alpha F(x) + \alpha T(x)$
$=(\alpha \cdot F)(x) + (\alpha \cdot T)(x)$.

Logo, $\alpha \cdot (F+T) = \alpha \cdot F + \alpha \cdot T$.

Portanto, mostramos que $(\mathcal{L}(\mathcal{V},\mathcal{W}),+,\cdot)$ é um espaço vetorial sobre $\mathbb{K}$.

■

Exemplo 1.96. *Sejam $\mathcal{V}$ e $\mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$. Vimos no exemplo anterior que $\mathcal{L}(\mathcal{V},\mathcal{W})$ é um espaço vetorial sobre $\mathbb{K}$, em partircular, se tomarmos $\mathcal{V}=\mathcal{W}$ temos também que $\mathcal{L}(\mathcal{V},\mathcal{V})$ é um espaço vetorial sobre $\mathbb{K}$. Neste caso, denotamos $\mathcal{L}(\mathcal{V},\mathcal{V})$ por $End\,(\mathcal{V})$.*

1.3.3 Teorema do Homomorfismo para Espaços Vetorias

Seja $\mathcal{V}$ um espaço vetorial sobre $\mathbb{K}$ e $\mathcal{W}\subseteq\mathcal{V}$ um subespaço vetorial de $\mathcal{V}$. Assim, como em grupos e anéis, podemos agora, em espaços vetoriais, definir de maneira natural, uma relação de equivalência que determinará classes de equivalência apartir de $\mathcal{W}$. A ideia é definir espaços vetoriais quocientes e mostrar assim, que o teorema do homomorfismo é válido também para espaços vetoriais.

Definição 1.97. *Sejam $\mathcal{V}$ um espaço vetorial qualquer sobre $\mathbb{K}$ e $\mathcal{W}$ um subespaço vetorial de $\mathcal{V}$. Dados $x,y\in\mathcal{V}$, dizemos que y é* congruente *a x módulo $\mathcal{W}$ ou y está relacionado com x módulo $\mathcal{W}$, quando $y-x\in\mathcal{W}$ e denotamos por*

$$y\equiv x\ (mod\ \ \mathcal{W})\Longleftrightarrow y-x\in\mathcal{W}.$$

Vale salientar que esta é uma relação de equivalência. De maneira natural e semelhante, como em grupos e anéis, denotaremos a classe de $x\in\mathcal{V}$ por

$$x+\mathcal{W}=\{x+w;w\in\mathcal{W}\}.$$

Seja $(\mathcal{V},+,\cdot)$ um espaço vetorial qualquer sobre $\mathbb{K}$ e $\mathcal{W}$ um subespaço vetorial de $\mathcal{V}$. Por definição, $(\mathcal{V},+)$ é um grupo abeliano e como $\mathcal{W}\subseteq\mathcal{V}$ temos que, $(\mathcal{W},+)$ é subgrupo de $(\mathcal{V},+)$. Como $(\mathcal{V},+)$ é abeliano, temos que $(\mathcal{W},+)$ é subgrupo normal de $\mathcal{V}$. Com essas informações podemos considerar o grupo quociente $\mathcal{V}/\mathcal{W}$, lembrando que, os elementos desse grupo são as classes de equivalência denotadas por

$$x+\mathcal{W}=\{x+w;w\in\mathcal{W}\}.$$

Dessa forma,

$$\mathcal{V}/\mathcal{W}=\{x+\mathcal{W};x\in\mathcal{V}\}.$$

Sejam $x+\mathcal{W}, y+\mathcal{W} \in \mathcal{V}/\mathcal{W}$, operamos duas classes da seguinte forma

$$(x+\mathcal{W})+(y+\mathcal{W}) = (x+y)+\mathcal{W}.$$

Note que o elemento neutro de $\mathcal{V}/\mathcal{W}$ é a classe $\vec{0}_v + \mathcal{W} = \mathcal{W}$ e o simétrico da classe $x+\mathcal{W}$ é a classe $(-x)+\mathcal{W}$.

Iremos mostrar a seguir, que o grupo $(\mathcal{V}/\mathcal{W}, +)$ torna-se um espaço vetorial com uma multiplicação por escalar apropriada.

Proposição 1.98. *Seja $(\mathcal{V}, +, \cdot)$ um espaço vetorial qualquer sobre $\mathbb{K}$ e $\mathcal{W}$ um subespaço vetorial de $\mathcal{V}$. Considere $(\mathcal{W}, +)$ como subgrupo normal de $(\mathcal{V}, +)$, então $(\mathcal{V}/\mathcal{W}, +, \cdot)$ é um espaço vetorial sobre $\mathbb{K}$, com a seguinte multiplicação por escalar*

$$\begin{array}{rccc} \cdot : & \mathbb{K}\times\mathcal{V}/\mathcal{W} & \longrightarrow & \mathcal{V}/\mathcal{W} \\ & (\alpha, x+\mathcal{W}) & \longmapsto & \alpha\cdot(x+\mathcal{W}), \end{array}$$

em que $\alpha\cdot(x+\mathcal{W}) = \alpha x + \mathcal{W}$.

Demonstração. Primeiro, vamos mostrar que a multiplicação por escalar, definida acima, está bem definida. Para tanto, sejam $x+\mathcal{W}, y+\mathcal{W} \in \mathcal{V}/\mathcal{W}$ e $\alpha \in \mathbb{K}$ tal que $x+\mathcal{W} = y+\mathcal{W}$. Vamos mostrar que $\alpha x + \mathcal{W} = \alpha y + \mathcal{W}$. Como $x+\mathcal{W} = y+\mathcal{W}$ temos que $x-y \in \mathcal{W}$, assim

$$\alpha(x-y) = \alpha x - \alpha y \in \mathcal{W},$$

pois as operações de soma e produto por escalar são fechadas em $\mathcal{W}$.

Portanto, αx e αy estão relacionados pela relação de equivalência módulo $\mathcal{W}$, logo eles estão na mesma classe, ou seja, $\alpha x + \mathcal{W} = \alpha y + \mathcal{W}$.

Vamos mostrar agora, as propriedades de produto por escalar, necessárias para que $(\mathcal{V}/\mathcal{W}, +, \cdot)$ seja um espaço vetorial sobre $\mathbb{K}$. Para tanto, sejam $x+\mathcal{W}, y+\mathcal{W} \in \mathcal{V}/\mathcal{W}$ e $\alpha, \beta \in \mathbb{K}$ quaisquer. Assim temos,

PE1: $\alpha\cdot[\beta\cdot(x+\mathcal{W})] = \alpha\cdot(\beta x+\mathcal{W}) = \alpha(\beta x)+\mathcal{W} = (\alpha\beta)x+\mathcal{W} = (\alpha\beta)\cdot(x+\mathcal{W})$;

PE2: Considere $1 \in \mathbb{K}$ a unidade de $\mathbb{K}$, assim $1\cdot(x+\mathcal{W}) = 1x+\mathcal{W} = x+\mathcal{W}$;

PE3:

$$(\alpha+\beta)\cdot(x+\mathcal{W}) = (\alpha+\beta)x+\mathcal{W} = (\alpha x+\beta x)+\mathcal{W}$$

$$= (\alpha x + \mathcal{W}) + (\beta x + \mathcal{W})$$
$$= \alpha \cdot (x + \mathcal{W}) + \beta \cdot (x + \mathcal{W});$$

PE4: $\alpha \cdot [(x + \mathcal{W}) + (y + \mathcal{W})] = \alpha \cdot [(x + y) + \mathcal{W}] = \alpha(x + y) + \mathcal{W}$
$$= (\alpha x + \alpha y) + \mathcal{W} = (\alpha x + \mathcal{W}) + (\alpha y + \mathcal{W})$$
$$= \alpha \cdot (x + \mathcal{W}) + \alpha \cdot (y + \mathcal{W}).$$

Concluímos assim, que $(\mathcal{V}/\mathcal{W}, +, \cdot)$ é um espaço vetorial sobre $\mathbb{K}$.

■

Definição 1.99. *O espaço vetorial* $(\mathcal{V}/\mathcal{W}, +, \cdot)$ *é denominado* espaço vetorial quociente.

Não iremos provar aqui, mas se dois espaços vetoriais $\mathcal{V}$ e $\mathcal{W}$ são isomorfos, ou seja, se existe $F : \mathcal{V} \longrightarrow \mathcal{W}$ um isomorfismo, então $dim\mathcal{V} = dim\mathcal{W}$.

Proposição 1.100. *Sejam* $\mathcal{V}$ *um espaço vetorial de dimensão finita sobre* $\mathbb{K}$ *e* $\mathcal{W}, \mathcal{S}$ *dois subespaços de* $\mathcal{V}$*, tais que* $\mathcal{V} = \mathcal{W} \oplus \mathcal{S}$ *(ver definição 1.84 na página 43). A aplicação*

$$\begin{array}{rccc} F: & \mathcal{S} & \longrightarrow & \mathcal{V}/\mathcal{W} \\ & x & \longmapsto & x + \mathcal{W}. \end{array}$$

é uma transformação linear bijetiva, ou seja, é um isomorfismo. Além disso, se $\mathcal{V}$ *tem dimensão finita, então* $\mathcal{V}/\mathcal{W}$ *tem dimensão finita e*

$$dim\mathcal{V}/\mathcal{W} = dim\mathcal{V} - dim\mathcal{W}.$$

Demonstração. Primeiramente, vamos mostrar que F é uma transformação linear. Para tanto, sejam $x, y \in \mathcal{S}$ e $\alpha \in \mathbb{K}$ quaisquer. Assim temos,

$$F(x + y) = (x + y) + \mathcal{W} = (x + \mathcal{W}) + (y + \mathcal{W}) = F(x) + F(y).$$

Também,

$$F(\alpha x) = \alpha x + \mathcal{W} = \alpha \cdot (x + \mathcal{W}) = \alpha \cdot F(x).$$

Portanto, F é transformação linear.

Vamos mostrar agora, que F é injetiva. Para tanto, seja $x \in N(F)$ qualquer, assim temos

$$F(x) = x + \mathcal{W} = \vec{0}_v + \mathcal{W} = \mathcal{W},$$

já que, $\mathcal{W}$ é o elemento neutro de $\mathcal{V}/\mathcal{W}$. Assim, por definição de relação de congruência módulo $\mathcal{W}$, temos que, $x - \vec{0}_v = x \in \mathcal{W}$. Assim, $x \in \mathcal{W} \cap \mathcal{S}$ e como

$$\mathcal{V} = \mathcal{W} \oplus \mathcal{S},$$

temos que $\mathcal{W} \cap \mathcal{S} = \{\vec{0}_v\}$, logo $x = \vec{0}_v$.

Portanto, pela proposição 1.25 na página 13, temos que, F é injetiva. Mostremos agora, que F é sobrejetiva. Seja $x + \mathcal{W} \in \mathcal{V}/\mathcal{W}$ qualquer, assim $x \in \mathcal{V}$ como $\mathcal{V} = \mathcal{W} \oplus \mathcal{S}$, existem $w \in \mathcal{W}$ e $s \in \mathcal{S}$ tais que, $x = w + s$, assim $x - s \in \mathcal{W}$, ou seja, x é congruente a s módulo $\mathcal{W}$, logo

$$x + \mathcal{W} = s + \mathcal{W} = F(s).$$

Portanto, F é sobrejetiva.

Concluímos assim, que F é isomorfismo, ou seja, $\mathcal{S}$ é isomorfo a $\mathcal{V}/\mathcal{W}$. Como $\mathcal{S}$ é isomorfo a $\mathcal{V}/\mathcal{W}$ e $\mathcal{V} = \mathcal{W} \oplus \mathcal{S}$, temos

$$dim\mathcal{V}/\mathcal{W} = dim\mathcal{S}.$$

Portanto, pela proposição 1.85 na página 43, temos que,

$$dim\mathcal{V} = dim\mathcal{W} + dim\mathcal{V}/\mathcal{W},$$

ou seja,

$$dim\mathcal{V}/\mathcal{W} = dim\mathcal{V} - dim\mathcal{W}.$$

Donde segue a última afirmação.

■

Sejam $\mathcal{V}$ um espaço vetorial de dimensão finita n e $\mathcal{B}^* = \{b_1, \ldots, b_k\} \subset \mathcal{V}$ um subconjunto linearmente independente de $\mathcal{V}$, com $k < n$ (logo, $\mathcal{B}^*$ não é uma base para $\mathcal{V}$). É possível mostrar que o subespaço gerado por $\mathcal{B}^*$ tem dimensão finita k. Um fato importante em espaços vetoriais é que é possível completarmos o subconjunto $\mathcal{B}^*$ a fim obter uma base para $\mathcal{V}$. Ou seja, podemos completar $\mathcal{B}^*$ com os vetores $b_{k+1}, \ldots, b_n$ que serão linearmente independentes entre si e entre os vetores de $\mathcal{B}^*$, formando assim uma base $\mathcal{B} = \{b_1, \ldots, b_k, b_{k+1}, \ldots, b_n\}$ para $\mathcal{V}$. Também, se $\mathcal{W}_1$ é o subespaço gerado por $\mathcal{B}^*$ e $\mathcal{W}_2$ é o subespaço gerado por $b_{k+1}, \ldots, b_n$, teremos que $\mathcal{V} = \mathcal{W}_1 \oplus \mathcal{W}_2$.

Exemplo 1.101. *Sejam $\mathcal{V}$, $\mathcal{W}$ espaços vetoriais e $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação*

linear. Vimos na proposição 1.92 na página 45, que $N(F)$ é um subespaço vetorial de $\mathcal{V}$. Seja $\mathcal{B} = \{b_1, \ldots, b_k\}$ uma base para $N(F)$. Como vimos podemos completar $\mathcal{B}$ a obter uma base para $\mathcal{V}$. Sejam $b_{k+1}, \ldots, b_n$ os vetores que faltam para completarmos a base de $\mathcal{V}$. Assim, se $\mathcal{S}$ é o subespaço gerado por $b_{k+1}, \ldots, b_n$, temos que $\mathcal{V} = N(F) \oplus \mathcal{S}$.

Teorema 1.102 (Teorema do homomorfismo para espaços vetoriais)**.** *Sejam $\mathcal{V}, \mathcal{W}$ espaços vetoriais sobre $\mathbb{K}$ e $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação linear. Então, a aplicação*

$$\begin{array}{rccc} \varphi: & \mathcal{V}/N(F) & \longrightarrow & \mathfrak{I}m(F) \\ & x + N(F) & \longmapsto & F(x) \end{array}$$

é um isomorfismo.

Demonstração. Pelo teorema do homomorfismo para grupos temos que φ é uma bijeção e que φ preserva a operação soma. Resta mostrar que φ preserva a operação produto por escalar. Para tanto, sejam $x + N(F) \in \mathcal{V}/N(F)$ e $\alpha \in \mathbb{K}$ quaisquer. Assim, temos

$$\varphi[\alpha \cdot (x + N(F))] = \varphi(\alpha x + N(F)) = F(\alpha x) = \alpha F(x) = \alpha\varphi(x + N(F)).$$

Logo, φ é transformação linear bijetiva. Portanto, temos que φ é um isomorfismo, ou seja, $\mathcal{V}/N(F)$ é isomorfo à $\mathfrak{I}m(F)$, em notação fica, $\mathcal{V}/N(F) \simeq \mathfrak{I}m(F)$. Concluímos assim, a demonstração.

■

Corolário 1.103 (Teorema da dimensão)**.** *Sejam $\mathcal{V}, \mathcal{W}$ espaços vetoriais de dimensão finita sobre $\mathbb{K}$ e $F : \mathcal{V} \longrightarrow \mathcal{W}$ uma transformação linear. Então,*
$dim\mathcal{V} = dimN(F) + dim\mathfrak{I}m(F)$

Demonstração. De fato, pelo teorema anterior, temos que, $\mathcal{V}/N(F)$ e $\mathfrak{I}m(F)$ são isomorfos e portanto,

$$dim\, \mathcal{V}/N(F) = dim\, \mathfrak{I}m(F).$$

Por outro lado, pela proposição 1.100 na página 52 e pelo exemplo 1.101 na página 53, temos

$$dim\, \mathcal{V}/N(F) = dim\, \mathcal{V} - dimN(F).$$

Assim temos,

$$dim\, \mathfrak{I}m(F) = dim\, \mathcal{V}/N(F) = dim\mathcal{V} - dimN(F).$$

Portanto,

$$dim\mathcal{V} = dimN(F) + dim\mathfrak{I}m(F).$$

■

2 Álgebras

2.1 Definição e Exemplos

Neste capítulo, vamos definir a estrutura algébrica mais importante desse trabalho. A ideia é capturar informações obtidas no capítulo 1 e usá-las agora para definir a estrutura algébrica que será chamada de **Álgebra**. Como veremos a seguir na definição formal, uma álgebra é um conjunto não vazio munido de três operações, soma, produto e produto por escalar, que se comporta bem com relação a estas operações. Ainda neste capítulo, estudaremos álgebras com identidades polinomiais, que como veremos no decorrer do capítulo, essas identidades são polinômios, que se anulam quando avaliados em quaisquer elementos da álgebra.

Definição 2.1. *Seja* $\mathbb{K}$ *um corpo. Uma* álgebra *sobre* $\mathbb{K}$ *é uma quádrupla ordenada* $(\mathcal{A}, +, *, \cdot)$*, em que* $\mathcal{A}$ *é um conjunto não vazio, munido de uma operação denotada por* $+$ *(chamada de soma), de uma operação denotada por* $*$ *(chamada de produto) e de uma operação entre os elementos de* $\mathbb{K}$ *e os elementos de* $\mathcal{A}$*, denotada por* $\cdot$ *(chamada de produtos por escalar), tais que para todo* $x, y \in \mathcal{A}$*,* $\alpha \in \mathbb{K}$*, as seguintes condições são satisfeitas:*

A1: $(\mathcal{A}, +, *)$ *é um anel;*

A2: $(\mathcal{A}, +, \cdot)$ *é um espaço vetorial sobre* $\mathbb{K}$*;*

A3: $(\alpha \cdot x) * y = x * (\alpha \cdot y) = \alpha \cdot (x * y)$.

Seja $(\mathcal{A}, +, *, \cdot)$ uma álgebra sobre $\mathbb{K}$. Quando não houver possibilidade de dúvidas, diremos apenas que $\mathcal{A}$ é uma $\mathbb{K}$-álgebra, ou seja, ficam sobentendidas as operações. Também, quando não houver dúvidas com relação ao corpo que estamos trabalhando, diremos apenas que $\mathcal{A}$ é uma álgebra.

Exemplo 2.2. *O conjunto $M_2(\mathbb{R})$ com as operações de soma, produto e produto por escalar usuais é uma $\mathbb{R}$-álgebra.*

De fato, já mostramos no exemplo 1.41 na página 21 que $M_2(\mathbb{R})$ é um anel, com as operações usuais de matrizes. Também, mostramos no exemplo 1.67 na página 36 que $M_2(\mathbb{R})$ é um espaço vetorial. Resta então, mostrarmos que vale a condição **A3** da definição de álgebra. Para tanto, sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(\mathbb{R})$ e $\alpha \in \mathbb{R}$ quaisquer. Assim, temos

$$\begin{aligned}(\alpha A) \cdot B = \alpha \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} &= \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ \alpha a_{21} & \alpha a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ &= \begin{pmatrix} \alpha a_{11} b_{11} + \alpha a_{12} b_{21} & \alpha a_{11} b_{12} + \alpha a_{12} b_{22} \\ \alpha a_{21} b_{11} + \alpha a_{22} b_{21} & \alpha a_{21} b_{12} + \alpha a_{22} b_{22} \end{pmatrix} \\ &= \alpha \begin{pmatrix} a_{11} b_{11} + a_{12} b_{21} & a_{11} b_{12} + a_{12} b_{22} \\ a_{21} b_{11} + a_{22} b_{21} & a_{21} b_{12} + a_{22} b_{22} \end{pmatrix} \\ &= \alpha \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) = \alpha(A \cdot B).\end{aligned}$$

Logo, $(\alpha A) \cdot B = \alpha(A \cdot B)$. Note agora que

$$\begin{aligned}A \cdot (\alpha B) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \left(\cdot \alpha \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} \alpha b_{11} & \alpha b_{12} \\ \alpha b_{21} & \alpha b_{22} \end{pmatrix} \\ &= \begin{pmatrix} a_{11} \alpha b_{11} + a_{12} \alpha b_{21} & a_{11} \alpha b_{12} + a_{12} \alpha b_{22} \\ a_{21} \alpha b_{11} + a_{22} \alpha b_{21} & a_{21} \alpha b_{12} + a_{22} \alpha b_{22} \end{pmatrix} \\ &= \begin{pmatrix} \alpha(a_{11} b_{11}) + \alpha(a_{12} b_{21}) & \alpha(a_{11} b_{12}) + \alpha(a_{12} b_{22}) \\ \alpha(a_{12} b_{11}) + \alpha(a_{22} b_{21}) & \alpha(a_{21} b_{12}) + \alpha(a_{22} b_{22}) \end{pmatrix} \\ &= \alpha \begin{pmatrix} a_{11} b_{11} + a_{12} b_{21} & a_{11} b_{12} + a_{12} b_{22} \\ a_{12} b_{11} + a_{22} b_{21} & a_{21} b_{12} + a_{22} b_{22} \end{pmatrix} \\ &= \alpha \left(\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \right) = \alpha(A \cdot B).\end{aligned}$$

Logo, temos $(\alpha A) \cdot B = \alpha(A \cdot B) = A \cdot (\alpha B)$. Concluímos assim, que a condição **A3** é satisfeita.

Portanto, $M_2(\mathbb{R})$ é uma álgebra.

Exemplo 2.3. *Considere o conjunto* $sl_2(\mathbb{R}) = \left\{ \begin{pmatrix} x & y \\ z & -x \end{pmatrix}; x, y, z \in \mathbb{R} \right\}$. *Dadas duas matrizes* A, $B \in sl_2(\mathbb{R})$ *quaisquer, defina o produto*

$$\begin{array}{rccc} [\cdot,\cdot]: & sl_2(\mathbb{R}) \times sl_2(\mathbb{R}) & \longrightarrow & sl_2(\mathbb{R}) \\ & (A, B) & \longmapsto & [A, B], \end{array}$$

em que $[A, B] = AB - BA$ *e* AB *é o produto usual de matrizes. Considerando* $+$ *(soma usual de matrizes),* $\cdot$ *(produto escalar usual) e* $[\cdot,\cdot]$ *(produto definido acima). Vamos verificar se* $(sl_2(\mathbb{R}), +, [\cdot,\cdot], \cdot)$ *é uma álgebra.*

Já mostramos no exemplo 1.72 na página 39 que $sl_2(\mathbb{R})$ é um espaço vetorial sobre $\mathbb{R}$. Portanto, basta mostrarmos que $(sl_2(\mathbb{R}), +, [\cdot,\cdot])$ é um anel e que vale **A3**. Vamos primeiro, mostrar que a operação $[\cdot,\cdot]$ é fechada em $sl_2(\mathbb{R})$. Para tanto, sejam $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & -a_1 \end{pmatrix}, B = \begin{pmatrix} b_1 & b_2 \\ b_3 & -b_1 \end{pmatrix} \in sl_2(\mathbb{R})$ quaisquer. Assim, temos

$$\begin{aligned} [A, B] = AB - BA &= \begin{pmatrix} a_1 & a_2 \\ a_3 & -a_1 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & -b_1 \end{pmatrix} - \begin{pmatrix} b_1 & b_2 \\ b_3 & -b_1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ a_3 & -a_1 \end{pmatrix} \\ &= \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 - a_2b_1 \\ a_3b_1 - a_1b_3 & a_3b_2 + a_1b_1 \end{pmatrix} - \begin{pmatrix} b_1a_1 + b_2a_3 & b_1a_2 - b_2a_1 \\ b_3a_1 - b_1a_3 & b_3a_2 + b_1a_1 \end{pmatrix} \\ &= \begin{pmatrix} a_1b_1 + a_2b_3 - b_1a_1 - b_2a_3 & a_1b_2 - a_2b_1 - b_1a_2 + b_2a_1 \\ a_3b_1 - a_1b_3 - b_3a_1 + b_1a_3 & a_3b_2 + a_1b_1 - b_3a_2 - b_1a_1 \end{pmatrix} \\ &= \begin{pmatrix} a_2b_3 - b_2a_3 & 2a_1b_2 - 2a_2b_1 \\ 2a_3b_1 - 2a_1b_3 & -a_2b_3 + a_3b_2 \end{pmatrix} \\ &= \begin{pmatrix} a_2b_3 - b_2a_3 & 2a_1b_2 - 2a_2b_1 \\ 2a_3b_1 - 2a_1b_3 & -(a_2b_3 - b_2a_3) \end{pmatrix} \in sl_2(\mathbb{R}). \end{aligned}$$

Logo, a operação $[\cdot,\cdot]$ é fechada em $sl_2(\mathbb{R})$.

Vamos mostrar agora que vale **A3**. Para tanto, sejam $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & -a_1 \end{pmatrix}$, $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & -b_1 \end{pmatrix} \in sl_2(\mathbb{R})$ e $\alpha \in \mathbb{R}$ quaisquer. Assim, temos

$$[\alpha A, B] = (\alpha A)B - B(\alpha A) = A(\alpha B) - (\alpha B)A = [A, \alpha B] \qquad \text{e}$$

$$[A, \alpha B] = A(\alpha B) - (\alpha B)A = \alpha(AB) - \alpha(BA) = \alpha(AB - BA) = \alpha[A, B].$$

Logo, $[\alpha A, B] = [A, \alpha B] = \alpha[A, B]$ e assim **A3** é satisfeita.

Vamos verificar agora se $(sl_2(\mathbb{R}), +, [\cdot, \cdot])$ é um anel.

Já sabemos que $(sl_2(\mathbb{R}), +, \cdot)$ é um espaço vetorial, logo $(sl_2(\mathbb{R}), +)$ é um grupo abeliano. Resta mostrarmos a associatividade do produto e a distributividade do produto com respeito a soma. Vamos mostrar primeiro a distributividade. Para tanto, sejam $A, B\ e\ C \in sl_2(\mathbb{R})$ quaisquer. Assim, temos

$$\begin{aligned}
[A, (B + C)] &= A(B + C) - (B + C)A \\
&= AB + AC - (BA + CA) \\
&= AB + AC - BA - CA \\
&= AB - BA + AC - CA \\
&= [A, B] + [A, C].
\end{aligned}$$

Também temos

$$\begin{aligned}
[(A + B), C] &= (A + B)C - C(A + B) \\
&= AC + BC - CA - CB \\
&= AC - CA + BC - CB \\
&= [A, C] + [B, C].
\end{aligned}$$

Portanto, a distributividade é satisfeita. Resta então, a associatividade do produto.

Considere as seguintes matrizes:

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\ \text{e}\ C = \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \in sl_2(\mathbb{R}).$$

Assim, temos

$$\begin{aligned}
[[A, B], C] = [A, B]C - C[A, B] &= (AB - BA)C - C(AB - BA) \\
&= ABC - BAC - CAB + CBA
\end{aligned}$$

$$
\begin{aligned}
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \\
&- \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 6 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 6 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 2 \\ 12 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ -6 & 0 \end{pmatrix}. \quad (2.1)
\end{aligned}
$$

Por outro lado,

$$
\begin{aligned}
[A,[B,C]] &= A[B,C] - [B,C]A \\
&= A(BC - CB) - (BC - CB)A \\
&= ABC - ACB - BCA + CBA \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \\
&- \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \\
&- \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 3 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 4 \\ 6 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 6 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}. \quad (2.2)
\end{aligned}
$$

Note que (2.1)$\neq$ (2.2). Logo, $[[A,B],C] \neq [A,[B,C]]$.

Portanto, a associatividade do produto não é satisfeita. Como não temos a associatividade do produto, por definição

$$(sl_2(\mathbb{R}), +, [\cdot,\cdot])$$

não é um anel. Isso mostra que

$$(sl_2(\mathbb{R}), +, [\cdot,\cdot], \cdot)$$

não é uma álgebra. Porém, quando não temos a associatividade do produto, mas todas as outras condições necessárias para que um conjunto seja uma álgebra, são satisfeitas, dizemos então que esse conjunto com suas operações definidas é uma *álgebra não associativa.*

Portanto, concluímos que $(sl_2(\mathbb{R}), +, [\cdot,\cdot], \cdot)$ é uma álgebra não associativa.

Definição 2.4. *Uma álgebra $\mathcal{A}$ é dita ser* comutativa*, se $\mathcal{A}$ é um anel comutativo, ou seja, se para todo $x, y \in \mathcal{A}$ tem-se:*

$$x * y = y * x.$$

Definição 2.5. *Uma álgebra $\mathcal{A}$ é dita* álgebra com unidade*, se $\mathcal{A}$ é um anel com unidade, ou seja, se existe $1 \in \mathcal{A}$, tal que, para todo $x \in \mathcal{A}$ tem-se:*

$$x * 1 = 1 * x = x.$$

Exemplo 2.6. *O conjunto $\mathcal{F}(\mathbb{R})$ visto nos exemplos 1.42 e 1.69 nas páginas 23 e 37 respectivamente, com suas operações definidas, para todo $f, g \in \mathcal{F}(\mathbb{R})$ e α, $x \in \mathbb{R}$ como:*

$$(f+g)(x) = f(x) + g(x);$$

$$(f \cdot g)(x) = f(x)g(x) \quad e$$

$$(\alpha f)(x) = \alpha f(x),$$

é uma álgebra comutativa com unidade.

De fato, já mostramos no exemplo 1.42 na página 23 que $(\mathcal{F}(\mathbb{R}), +, \cdot)$ é um anel comutativo com unidade. Mostramos também, no exemplo 1.69 na página 37 que $\mathcal{F}(\mathbb{R})$ é um espaço vetorial sobre $\mathbb{R}$. Resta então, mostrarmos a condição **A3** da definição de álgebra. Para tanto, sejam $f, g \in \mathcal{F}(\mathbb{R})$ e α, $x \in \mathbb{R}$ quaisquer. Assim temos

$$((\alpha f) \cdot g)(x) = (\alpha f)(x)g(x) = (\alpha f(x))g(x) = \alpha(f(x)g(x)) = \alpha(f \cdot g)(x).$$

Logo, $(\alpha f) \cdot g = \alpha(f \cdot g)$.

Agora, como $\alpha, f(x)$ e $g(x) \in \mathbb{R}$, temos que

$$\begin{aligned}\alpha(f(x)g(x)) &= (\alpha f(x))g(x) = (f(x)\alpha)g(x)\\ &= f(x)(\alpha g(x)) = (f \cdot (\alpha g))(x).\end{aligned}$$

Logo, $(\alpha f) \cdot g = f \cdot (\alpha g)$. Assim temos,

$$(\alpha f) \cdot g = \alpha(f \cdot g) = f \cdot (\alpha g).$$

Portanto, $\mathcal{F}(\mathbb{R})$ é uma álgebra comutativa com unidade.

Exemplo 2.7. *Já mostramos no exemplo 1.95 na página 47, que o conjunto $\mathcal{L}(\mathcal{V}, \mathcal{W})$ das transformações lineares com as operações:*

$$(F + T)(x) = F(x) + T(x) \quad e$$

$$(\alpha \cdot T)(x) = \alpha T(x),$$

é um espaço vetorial sobre $\mathbb{K}$. Vimos também no exemplo 1.96 na página 50, que $End(\mathcal{V})$ é também um espaço vetorial sobre $\mathbb{K}$. Defina agora, para todo $F, T \in End(\mathcal{V})$ e $x \in \mathcal{V}$ a operação produto

$$\begin{array}{rccc} \circ: & End(\mathcal{V}) \times End(\mathcal{V}) & \longrightarrow & End(\mathcal{V}) \\ & (F, T) & \longmapsto & F \circ T, \end{array}$$

em que $(F \circ T)(x) = F(T(x))$. Vamos mostrar que $(End(\mathcal{V}), +, \circ, \cdot)$ é uma álgebra associativa com unidade.

De fato, já mostramos no exemplo 1.96 que $(End(\mathcal{V}), +, \cdot)$ é um espaço vetorial sobre $\mathbb{K}$. Resta então, mostrarmos que $(End(\mathcal{V}), +, \circ)$ é um anel com unidade e que vale **A3**. Vamos mostrar primeiro que $(End(\mathcal{V}), +, \circ)$ é um anel com unidade. Para tanto, sejam $F, T, S \in End(\mathcal{V})$, $x, y \in \mathcal{V}$ e $\alpha \in \mathbb{K}$ quaisquer. Como $(End(\mathcal{V}), +, \cdot)$ é um espaço vetorial, temos que $(End(\mathcal{V}), +)$ é um grupo abeliano, assim só precisamos mostrar que a associatividade do produto e a distributividade do produto com respeito a soma são válidas. Mas antes, vamos mostrar que a operação $\circ$ é fechada em $End(\mathcal{V})$. De fato, temos que

$$(F \circ T)(x + y) = F(T(x + y)),$$

como T é linear, temos

$$F(T(x + y)) = F(T(x) + T(y))$$

e como F é linear, temos

$$F(T(x)+T(y)) = F(T(x)) + F(T(x)) = (F\circ T)(x) + (F\circ T)(x).$$

Portanto, $(F\circ T)(x+y) = (F\circ T)(x) + (F\circ T)(x)$.

Agora, temos também

$$(F\circ T)(\alpha x) = F(T(\alpha x)),$$

como T é linear, temos

$$F(T(\alpha x)) = F(\alpha T(x)),$$

como F é linear, temos

$$F(\alpha T(x)) = \alpha F(T(x)) = \alpha(F\circ T)(x).$$

Logo, $F\circ T$ é linear. Portanto, $F\circ T \in End\,(\mathcal{V})$ e a operação é fechada.

Mostremos agora, as propriedades necessárias de pruduto para que $(End\,(\mathcal{V}), +, \circ)$ seja um anel.

Associatividade do produto:

$$(F\circ(T\circ S))(x) = F((T\circ S)(x)) = F(T(S(x))). \tag{2.3}$$

Por outro lado, temos

$$((F\circ T)\circ S)(x) = (F\circ T)(S(x)) = F(T(S(x))). \tag{2.4}$$

De (2.3) e (2.4) temos que,

$$(F\circ(T\circ S))(x) = ((F\circ T)\circ S)(x).$$

Portanto, $F\circ(T\circ S) = (F\circ T)\circ S$.

Distributividade da soma com respeito ao produto:

$$(F\circ(T+S))(x) = F((T+S)(x)) = F(T(x)+S(x)).$$

Como F é transformação linear, temos

$$F(T(x)+S(x)) = F(T(x)) + F(S(x)) = (F\circ T)(x) + (F\circ S)(x).$$

Logo, $F\circ(T+S) = F\circ T + F\circ S$.

Também temos

$$((F+T)\circ S)(x) = (F+T)(S(x)) = F(S(x)) + T(S(x)) = (F\circ S)(x) + (T\circ S)(x).$$

Logo, $(F+T)\circ S = F\circ S + T\circ S$.

Assim temos

$$F\circ(T+S) = F\circ T + F\circ S \quad \text{e}$$

$$(F+T)\circ S = F\circ S + T\circ S.$$

Concluímos assim, que a distributividade é válida.

Existência do elemento neutro do produto: Considere para todo $x\in\mathcal{V}$, $T_1(x) = x$. Note que, pelo exemplo 1.89 na página 44, $T_1 \in End(\mathcal{V})$. Assim, temos

$$(F\circ T_1)(x) = F(T_1(x)) = F(x);$$

$$(T_1\circ F)(x) = T_1(F(x)) = F(x).$$

Segue que,

$$F\circ T_1 = T_1\circ F = F.$$

Portanto, T_1 é o elemento neutro do produto $\circ$.

Concluímos assim, que $(End(\mathcal{V}), +, \circ)$ é um anel com unidade.

Mostremos agora que vale **A3**.

$$\begin{aligned}((\alpha\cdot F)\circ T)(x) &= (\alpha\cdot F)(T(x)) = \alpha F(T(x))\\ &= \alpha((F\circ T)(x)) = (\alpha\cdot(F\circ T))(x).\end{aligned}$$

Logo, $(\alpha\cdot F)\circ T = \alpha\cdot(F\circ T)$.

Por outro lado, temos

$$\alpha F(T(x)) = F(\alpha T(x)) = F((\alpha\cdot T)(x)) = (F\circ(\alpha\cdot T))(x).$$

Logo, $(\alpha \cdot F) \circ T = \alpha \cdot (F \circ T) = F \circ (\alpha \cdot T)$.

Concluímos assim, que $(End\,(\mathcal{V}), +, \circ, \cdot)$ é uma álgebra associativa com unidade.

Exemplo 2.8. *Considere* $\mathbb{R}$ *com as operações usuais e* $A = \{a\}$ *um conjunto unitário qualquer. Considere o conjunto* $\mathcal{F} = \{f : A \longrightarrow \mathbb{R}; f$ *é função* $\}$*. Defina, Para quaisquer* $f, g \in \mathcal{F}$ *e* $\alpha \in \mathbb{R}$*, as seguintes operações em* $\mathcal{F}$*:*

$$\begin{array}{rccc} + : & \mathcal{F} \times \mathcal{F} & \longrightarrow & \mathcal{F} \\ & (f, g) & \longmapsto & f + g, \end{array}$$

em que $(f + g)(a) = f(a) + g(a)$*,*

$$\begin{array}{rccc} * : & \mathcal{F} \times \mathcal{F} & \longrightarrow & \mathcal{F} \\ & (f, g) & \longmapsto & f * g, \end{array}$$

em que $(f * g)(a) = f(a)g(a)$ *e*

$$\begin{array}{rccc} \cdot : & \mathbb{K} \times \mathcal{F} & \longrightarrow & \mathcal{F} \\ & (\alpha, g) & \longmapsto & \alpha \cdot g, \end{array}$$

em que $(\alpha \cdot f)(a) = \alpha f(a)$*. Note que, as operações no membro direito da igualdade anterior, são as operações em* $\mathbb{R}$ *e as operações no membro esquerdo, são as operações em* $\mathcal{F}$*. Vamos mostrar que* $(\mathcal{F}, +, *, \cdot)$ *é uma* $\mathbb{R}$*-álgebra com unidade.*

Primeiro, vamos mostrar que as operações são fechadas. De fato, sejam $f, g \in \mathcal{F}$ e $\alpha \in \mathbb{R}$ quaisquer. Assim, temos

$$(f + g)(a) = f(a) + g(a) \in \mathbb{R},$$

pois $f(a), g(a) \in \mathbb{R}$. Logo, $f + g \in \mathcal{F}$.

Também temos,

$$(f * g)(a) = f(a)g(a) \in \mathbb{R},$$

pois $f(a), g(a) \in \mathbb{R}$. Logo, $f * g \in \mathcal{F}$.

E ainda,

$$(\alpha \cdot f)(a) = \alpha f(a) \in \mathbb{R},$$

pois $\alpha, f(a) \in \mathbb{R}$. Logo, $\alpha \cdot f \in \mathcal{F}$.

Concluímos assim que as operações são fechadas. Vamos mostrar agora que $\mathcal{F}$ é uma $\mathbb{R}$-álgebra associativa com unidade. Primeiro, vamos verificar que $(\mathcal{F}, +, *)$ é um anel com unidade. De fato, vamos mostrar que os axiomas de anéis são válidos. Para tanto,

sejam $f, g \in \mathcal{F}$ e $\alpha \in \mathbb{R}$ quaisquer.

Associatividade da soma:

$$\begin{aligned}(f+(g+h))(a) &= f(a)+(g+h)(a)\\ &= f(a)+(g(a)+h(a))\\ &= (f(a)+g(a))+h(a)\\ &= (f+g)(a)+h(a)\\ &= ((f+g)+h)(a).\end{aligned}$$

Observe que usamos nessa demonstração a associatividade da soma em $\mathbb{R}$.

Logo, $f+(g+h) = (f+g)+h$.

Comutatividade da soma:

$$(f+g)(a) = f(a)+g(a) = g(a)+f(a) = (g+f)(a).$$

Observe que usamos nessa demonstração a comutatividade da soma em $\mathbb{R}$.

Logo, $f+g = g+f$.

Existência do elemento neutro da soma: Considere a função $f_0 : A \longrightarrow \mathbb{R}$, tal que, $f_0(a) = 0$. Assim temos,

$$(f_0+g)(a) = f_0(a)+g(a) = 0+g(a) = g(a);$$

$$(g+f_0)(a) = g(a)+f_0(a) = g(a)+0 = g(a).$$

Logo, $f_0+g = g+f_0 = g$. Portanto, f_0 é elemento neutro da soma.

Existência do elemento simétrico para soma: Considere $-f \in \mathcal{F}$ tal que, $(-f)(a) = -f(a)$. Assim temos,

$$(f+(-f))(a) = f(a)+(-f)(a) = f(a)-f(a) = 0 = f_0(a);$$

$$((-f)+f)(a) = (-f)(a)+f(a) = -f(a)+f(a) = 0 = f_0(a).$$

Logo, $f+(-f) = (-f)+f = f_0$. Portanto, $-f$ é o simétrico de f.

Mostramos assim que $(\mathcal{F}, +)$ é um grupo abeliano. Falta mostrarmos a associatividade do produto e a distributividade. Vamos a elas:

Associatividade do produto:

$$\begin{aligned}[f * (g * h)](a) &= f(a)(g * h)(a) \\ &= f(a)[g(a)h(a)] \\ &= [f(a)g(a)]h(a) \\ &= (f * g)(a)h(a) \\ &= [(f * g) * h](a).\end{aligned}$$

Observe que usamos nessa demonstração a associatividade do produto em $\mathbb{R}$.

Logo, $f * (g * h) = (f * g) * h$.

Distributividade da soma com respeito ao produto:

$$\begin{aligned}(f * (g + h))(a) &= f(a)(g + h)(a) \\ &= f(a)[g(a) + h(a)] \\ &= f(a)g(a) + f(a)h(a) \\ &= (f * g)(a) + (f * h)(a) \\ &= (f * g + f * h)(a).\end{aligned}$$

E ainda,

$$\begin{aligned}((f + g) * h)(a) &= (f + g)(a)h(a) \\ &= [f(a) + g(a)]h(a) \\ &= f(a)h(a) + g(a)h(a) \\ &= (f * h)(a) + (g * h)(a) \\ &= (f * h + g * h)(a).\end{aligned}$$

Observe que usamos nessa demonstração a distributividade da soma com respeito ao produto em $\mathbb{R}$.

Logo,

$$f * (g + h) = f * g + f * h \quad \text{e}$$

$$(f+g)*h = f*h + g*h.$$

Existência do elemento neutro do produto: Considere $f_1 \in \mathcal{F}$; $f_1(a) = 1$. Assim, temos

$$(f*f_1)(a) = f(a)f_1(a) = f(a)1 = f(a);$$

$$(f_1*f)(a) = f_1(a)f(a) = 1f(a) = f(a).$$

Logo, $f*f_1 = f_1*f = f$. Portanto, f_1 é o elemento neutro do produto.

Concluímos assim que $(\mathcal{F}, +, *)$ é um anel com unidade.

Vamos mostrar agora que $(\mathcal{F}, +, \cdot)$ é um espaço vetorial. Já mostramos que $(\mathcal{F}, +)$ é um grupo abeliano. Resta mostrarmos as propriedades **PE1**, **PE2**, **PE3** e **PE4** de espaços vetoriais, ver definição 1.65 na página 35. Para tanto, sejam $f, g \in \mathcal{F}$ e $\alpha, \beta \in \mathbb{R}$ quaisquer. Assim temos,

PE1: $(\alpha \cdot (\beta \cdot f))(a) = \alpha(\beta \cdot f)(a) = \alpha(\beta f(a)) = (\alpha\beta)f(a) = ((\alpha\beta) \cdot f)(a)$.

Logo, $\alpha \cdot (\beta \cdot f) = (\alpha\beta) \cdot f$.

PE2: $(1 \cdot f)(a) = 1f(a) = f(a)$. Logo, $(1 \cdot f) = f$.

PE3: $((\alpha+\beta) \cdot f)(a) = (\alpha+\beta)f(a) = \alpha f(a) + \beta f(a) = (\alpha \cdot f)(a) + (\beta \cdot f)(a)$.

Logo, $(\alpha+\beta) \cdot f = \alpha \cdot f + \beta \cdot f$.

PE4:

$$\begin{aligned}(\alpha \cdot (f+g))(a) &= \alpha(f+g)(a)\\ &= \alpha(f(a)+g(a))\\ &= \alpha f(a) + \alpha g(a)\\ &= (\alpha \cdot f)(a) + (\alpha \cdot g)(a)\\ &= (\alpha \cdot f + \alpha \cdot g)(a).\end{aligned}$$

Logo, $\alpha \cdot (f+g) = \alpha \cdot f + \alpha \cdot g$.

Concluímos assim que $(\mathcal{F}, +, \cdot)$ é um espaço vetorial sobre $\mathbb{R}$. Resta ainda, mostrarmos que vale a propriedade **A3** da definição de álgebras. Para tanto, sejam $f, g \in \mathcal{F}$ e $\alpha \in \mathbb{R}$

quaisquer. Assim, temos

$$((\alpha \cdot f) * g)(a) = (\alpha \cdot f)(a)g(a) = (\alpha f(a))g(a) = \alpha(f(a)g(a))$$
$$= \alpha(f * g)(a) = (\alpha \cdot (f * g))(a).$$

Logo, $(\alpha \cdot f) * g = \alpha \cdot (f * g)$.

E ainda, como $\alpha, f(a)$ e $g(a) \in \mathbb{R}$ temos que,

$$\alpha(f(a)g(a)) = (\alpha f(a))g(a) = (f(a)\alpha)g(a) = f(a)(\alpha g(a)) = (f * (\alpha \cdot g))(a).$$

Logo,

$$\alpha \cdot (f * g) = f * (\alpha \cdot g).$$

Assim temos,

$$\alpha \cdot (f * g) = (\alpha \cdot f) * g = f * (\alpha \cdot g).$$

Concluímos assim que $(\mathcal{F}, +, *, \cdot)$ é uma álgebra com unidade.

2.2 Subálgebras

Definição 2.9. *Uma* subálgebra *de uma álgebra $\mathcal{A}$ é um subconjunto não vazio $\mathcal{S}$ de $\mathcal{A}$ que é fechado em relação as três operações de $\mathcal{A}$, soma, produto e produto por escalar, ou seja, este subconjunto é ao mesmo tempo um subespaço vetorial e um subanel de $\mathcal{A}$.*

Exemplo 2.10. *O conjunto* $U_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} ;\ a, b, c \ \in \mathbb{R} \right\}$ *das matrizes triangulares superiores de ordem* 2 *com entradas em* $\mathbb{R}$ *é uma* $\mathbb{R}$*-subálgebra de* $M_2(\mathbb{R})$.

De fato, primeiro note que $U_2(\mathbb{R})$ não é vazio, pois $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in U_2(\mathbb{R})$. Vamos mostrar agora que $U_2(\mathbb{R})$ é um subespaço vetorial de $M_2(\mathbb{R})$. Para tanto, sejam $A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} \in U_2(\mathbb{R})$ e $\alpha \in \mathbb{K}$ quaisquer. Assim temos,

$$A + B = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ 0 & a_{22} + b_{22} \end{pmatrix} \in U_2(\mathbb{R}) \quad \text{e}$$

$$\alpha A = \alpha \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} \\ 0 & \alpha a_{22} \end{pmatrix} \in U_2(\mathbb{R}).$$

Portanto, pela definição 1.70 na página 38, temos que $U_2(\mathbb{R})$ é um subespaço vetorial de $M_2(\mathbb{R})$. Com isso, $U_2(\mathbb{R})$ é também um espaço vetorial, logo $(U_2(\mathbb{R}), +)$ é um grupo abeliano. Vamos mostrar agora que $U_2(\mathbb{R})$ é um subanel de $M_2(\mathbb{R})$. De fato, temos

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix} \in U_2(\mathbb{R}).$$

Portanto, pela proposição 1.44 na página 26 temos que $U_2(\mathbb{R})$ é um subanel de $M_2(\mathbb{R})$.

Concluímos assim que $U_2(\mathbb{R})$ é uma $\mathbb{R}$-subálgebra de $M_2(\mathbb{R})$.

Exemplo 2.11. *O conjunto* $\mathbb{R}[x]$ *dos polinômios*

$$f(x) = c_0 + c_1 x + \ldots + c_k x^k,$$

em que $c_i \in \mathbb{R}$ *para todo* $i \in \{1, 2, \ldots, k\}$ *e* k *é um inteiro não negativo é uma* $\mathbb{R}$*-subálgebra de* $\mathcal{F}(\mathbb{R})$.

De fato, primeiro note que $\mathbb{R}[x] \subset \mathcal{F}(\mathbb{R})$, pois todo polinômio é uma função. Também $\mathbb{R}[x]$ não é vazio, pois para todo $x \in \mathbb{R}$ se tomarmos $f(x) = 0$, ou seja, o polinômio nulo tem-se que $f \in \mathbb{R}[x]$. Vamos mostrar agora que $\mathbb{R}[x]$ é um subespaço vetorial de $\mathcal{F}(\mathbb{R})$. Para tanto, sejam $f, g \in \mathbb{R}[x]$ e $\alpha \in \mathbb{R}$ quaisquer. Assim, temos

$$f(x) = c_0 + c_1 x + \ldots + c_k x^k;\ c_i \in \mathbb{R},\ i \in \{1, 2, \ldots, k\} \quad \text{e}$$

$$g(x) = d_0 + d_1 x + \ldots + d_l x^l;\ d_j \in \mathbb{R},\ j \in \{1, 2, \ldots, l\},$$

em que k e l são inteiros não negativos. Suponha, sem perda de generalidade, que $l \leq k$. Assim temos,

$$\begin{aligned}(f+g)(x) = f(x) + g(x) &= c_0 + c_1 x + \ldots + c_k x^k + (d_0 + d_1 x + \ldots + d_l x^l) \\ &= (c_0 + d_0) + (c_1 + d_1)x + \ldots + (c_l + d_l)x^l + \ldots + c_k x^k \in \mathbb{R}[x].\end{aligned}$$

Também temos,

$$(\alpha f)(x) = \alpha f(x) = \alpha(c_0 + c_1 x + \ldots + c_k x^k) = \alpha c_0 + \alpha c_1 x + \ldots + \alpha c_k x^k \in \mathbb{R}[x].$$

Logo, pela definição 1.70 na página 38 temos que $\mathbb{R}[x]$ é um subespaço vetorial de

$\mathcal{F}(\mathbb{R})$. Assim, $\mathbb{R}[x]$ também é um espaço vetorial e $(\mathbb{R}[x], +)$ é um subgrupo abeliano de $(\mathcal{F}(\mathbb{R}), +)$. Agora temos,

$$\begin{aligned}(f \cdot g)(x) &= f(x) \cdot g(x) \\ &= (c_0 + c_1x + \ldots + c_kx^k) \cdot (d_0 + d_1x + \ldots + d_lx^l) \\ &= (c_0d_0 + c_0d_1x + \ldots + c_0d_lx^l) + (c_1d_0x + c_1d_1x^2 + \ldots + c_1d_lx^{l+1}) + \\ &+ \ldots + (c_kd_0x^k + c_kd_1x^{k+1} + \ldots + c_kd_lx^{l+k}) \\ &= \sum_{i=0}^{k}\sum_{j=0}^{l} c_id_jx^{i+j} \in \mathbb{R}[x].\end{aligned}$$

Portanto, pela proposição 1.44 na página 26 temos que $\mathbb{R}[x]$ é um subanel de $\mathcal{F}(\mathbb{R})$.

Portanto, concluímos que $\mathbb{R}[x]$ é uma subálgebra de $\mathcal{F}(\mathbb{R})$.

Pelo fato de $\mathbb{R}[x]$ ser uma subálgebra de $\mathcal{F}(\mathbb{R})$, temos que $\mathbb{R}[x]$ é também uma álgebra.

Podemos generalizar o exemplo anterior e mostrar que o conjunto $\mathbb{K}[x]$ dos polinômios é uma $\mathbb{K}$-álgebra com a soma, produto e o produto por escalar usuais de polinômios em uma variável.

Exemplo 2.12. *$\mathbb{K}[x, y]$ é o conjunto dos polinômios comutativos nas variáveis x e y com coeficientes em $\mathbb{K}$. Um polinômio desse conjunto é da forma*

$$f(x, y) = c_{00} + c_{10}x + c_{01}y + \ldots + c_{kl}x^ky^l$$

com $c_{ij} \in \mathbb{K}$, para todo $i \in \{1, 2, \ldots, k\}$ e para todo $j \in \{1, 2, \ldots, l\}$, em que k e l são inteiros não negativos. Da mesma forma que $\mathbb{K}[x]$ é uma $\mathbb{K}$-álgebra, temos que $\mathbb{K}[x, y]$ também é uma $\mathbb{K}$-álgebra.

Exemplo 2.13. *Também é possível mostrar que o conjunto*

$$\mathcal{F}(\mathbb{R} \times \mathbb{R}) = \{f : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R};\ f \text{ é função}\},$$

com as operações de soma, produto e produto por escalar, definidas abaixo respectivamente para todo $f, g \in \mathcal{F}(\mathbb{R} \times \mathbb{R})$, x, y e $\alpha \in \mathbb{R}$ é uma $\mathbb{R}$-álgebra.

$$\begin{array}{rccc} + : & \mathcal{F}(\mathbb{R} \times \mathbb{R}) \times \mathcal{F}(\mathbb{R} \times \mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R} \times \mathbb{R}) \\ & (f, g) & \longmapsto & f + g, \end{array}$$

em que $(f+g)(x,y) = f(x,y) + g(x,y)$,

$$\begin{array}{rccc} * : & \mathcal{F}(\mathbb{R}\times\mathbb{R}) \times \mathcal{F}(\mathbb{R}\times\mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R}\times\mathbb{R}) \\ & (f,g) & \longmapsto & f*g, \end{array}$$

em que $(f*g)(x,y) = f(x,y)g(x,y)$ *e*

$$\begin{array}{rccc} \cdot : & \mathcal{F}(\mathbb{R}\times\mathbb{R}) \times \mathcal{F}(\mathbb{R}\times\mathbb{R}) & \longrightarrow & \mathcal{F}(\mathbb{R}\times\mathbb{R}) \\ & (f,g) & \longmapsto & f\cdot g, \end{array}$$

em que $(\alpha\cdot f)(x,y) = \alpha f(x,y)$. *Também, não é difícil mostrar que* $\mathbb{R}[x,y]$ *é uma subálgebra de* $\mathcal{F}(\mathbb{R}\times\mathbb{R})$.

Se considerarmos o conjunto dos polinômios sobre $\mathbb{K}$ nas variáveis x e y, de forma que $xy \neq yx$, ou seja, as variáveis são não comutativas e denotarmos esse conjunto por $\mathbb{K}\langle x,y\rangle$, ainda assim, $\mathbb{K}\langle x,y\rangle$ é uma $\mathbb{K}$-álgebra. Podemos ainda, definir de maneira análoga $\mathbb{K}\langle x_1, x_2 \ldots, x_k\rangle$ o conjunto dos polinômios não comutativos sobre $\mathbb{K}$ em um número finito de variáveis $x_1, x_2 \ldots, x_k$ e mostrar que $\mathbb{K}\langle x_1, x_2 \ldots, x_k\rangle$ é uma $\mathbb{K}$-álgebra.

Exemplo 2.14. *Seja* $X = \{x_1, x_2, \ldots\}$ *um conjunto infinito enumerável. O conjunto* $\mathbb{K}\langle X\rangle$ *é uma generalização do conjunto* $\mathbb{K}\langle x_1, x_2 \ldots, x_k\rangle$, *considerando dessa vez um conjunto infinito de variáveis. Esse conjunto com as operações usuais é uma* $\mathbb{K}$*-álgebra, chamada* álgebra associativa livre, livremente gerada por X. *Note que, apesar de* X *ser um conjunto infinito, os elementos de* $\mathbb{K}\langle X\rangle$ *são polinômios finitos.*

Definição 2.15. *Uma subálgebra* $\mathcal{I}$ *de* $\mathcal{A}$ *é chamada* um ideal à esquerda *de* $\mathcal{A}$ *se para quaisquer* $a \in \mathcal{A}$ *e* $i \in \mathcal{I}$, *tem-se* $a * i \in \mathcal{I}$. *É chamada um* ideal à direita *de* $\mathcal{A}$ *se para quaisquer* $a \in \mathcal{A}$ *e* $i \in \mathcal{I}$, *tem-se* $i * a \in \mathcal{I}$. *Se* $\mathcal{I}$ *é simultaneamente um ideal à esquerda e à direita, dizemos que* $\mathcal{I}$ *é um* ideal bilateral *de* $\mathcal{A}$ *ou simplesmente* ideal *de* $\mathcal{A}$.

Não é difícil mostrar que em uma álgebra comutativa todos os seus ideais são ideais bilaterais.

Sejam $\mathcal{A}$ uma álgebra com unidade e $\mathcal{S} = \{s_1, \ldots, s_m\} \subseteq \mathcal{A}$, em que $m \in \mathbb{N}^*$. Como construir um ideal que contenha $\mathcal{S}$? O ideal que estamos interessados aqui é o menor ideal de $\mathcal{A}$ que contém $\mathcal{S}$. Considere o conjunto

$$\mathfrak{I} = \{\mathcal{I} \subseteq \mathcal{A};\ \mathcal{I} \text{ é ideal e } \mathcal{S} \subseteq \mathcal{I}\}.$$

Note que $\mathfrak{I}$ não é vazio, pois $\mathcal{A} \in \mathfrak{I}$ e $\mathcal{S} \subseteq \mathcal{A}$. Não iremos provar aqui, mas

$$\bigcap_{\mathcal{I} \in \mathfrak{I}} \mathcal{I}$$

é um ideal de $\mathcal{A}$. Será que $\mathcal{S} \subseteq \bigcap_{\mathcal{I} \in \mathfrak{I}} \mathcal{I}$? A resposta é sim, pois para todo $\mathcal{I} \in \mathfrak{I}$, temos $\mathcal{S} \subseteq \mathcal{I}$. Claramente

$$\bigcap_{\mathcal{I} \in \mathfrak{I}} \mathcal{I}$$

é o menor ideal que contém $\mathcal{S}$.

Denotamos este ideal por $\langle \mathcal{S} \rangle$. É possível mostrar que $\langle \mathcal{S} \rangle$ é o conjunto de todas as somas finitas da forma

$$a_1 s_1 c_1 + a_2 s_2 c_2 + \ldots + a_m s_m c_m,$$

para todo $a_i,\ c_i \in \mathcal{A}$ e $s_i \in \mathcal{S}$, em que $i \in \{1, 2, \ldots, m\}$.

Definição 2.16. *Sejam $\mathcal{A}$ uma álgebra com unidade, $\mathcal{I} \subseteq \mathcal{A}$ um ideal de $\mathcal{A}$ e $\mathcal{S} \subseteq \mathcal{I}$ um subconjunto de $\mathcal{I}$. Dizemos que $\mathcal{I}$ é um* ideal gerado *por $\mathcal{S}$ se*

$$\mathcal{I} = \langle \mathcal{S} \rangle.$$

Se existe $\mathcal{S}$ finito tal que isso ocorra, dizemos que $\mathcal{I}$ é finitamente gerado.

2.3 Homomorfismos de Álgebras

Como vimos em grupos, um homomorfismo de grupos é uma função que preserva a operação do grupo em questão. Em anéis, um homomorfismo preserva as duas operações do anel. Em espaços vetoriais, uma transformação linear preserva as operações de soma e produto por escalar, embora não as chamamos de homomorfismos. Um homomorfismo de álgebras se comporta, com relação às operações de soma e produto, como um homomorfismo de anéis. Com relação às operações de soma e produto por escalar, como uma transformação linear. Ou seja, um homomorfismo de álgebras preserva as três operações: soma, produto e produto por escalar.

Na definição abaixo, por simplicidade, vamos usar os mesmos símbolos, denotando as operações de $+$ (soma), $*$ (produto) e $\cdot$ (produto por escalar), tanto em $\mathcal{A}_1$, quanto em $\mathcal{A}_2$. O leitor deve estar atento que apesar da notação estes símbolos denotam operações diferentes.

Definição 2.17. *Sejam $\mathcal{A}_1$ e $\mathcal{A}_2$ duas $\mathbb{K}$-álgebras. Dizemos que a função $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$*

é um homomorfismo *de álgebras se, para todo* $x, y \in \mathcal{A}_1$ *e* $\alpha \in \mathbb{K}$*, temos:*

(i) $\varphi(x+y) = \varphi(x) + \varphi(y)$;

(ii) $\varphi(x * y) = \varphi(x) * \varphi(y)$;

(iii) $\varphi(\alpha \cdot x) = \alpha \cdot \varphi(x)$.

Definição 2.18. *Um homomorfismo injetor é chamado de* monomorfismo*. Um homomorfismo sobrejetor é chamado de* epimorfismo*. Um homomorfismo bijetor é chamado de* isomorfismo*. Um homomorfismo* $f : \mathcal{A} \to \mathcal{A}$ *é chamado de* endomorfismo*. Um isomorfismo* $f : \mathcal{A} \to \mathcal{A}$ *é chamado de* automorfismo*.*

Definição 2.19. *Sejam* $\mathcal{A}_1, \mathcal{A}_2$ *álgebras. Se existe* $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ *um isomorfismo de álgebras, dizemos que* $\mathcal{A}_1$ *é* isomorfa *a* $\mathcal{A}_2$ *e denotamos por* $\mathcal{A}_1 \simeq \mathcal{A}_2$*.*

Definição 2.20. *Sejam* $\mathcal{A}_1, \mathcal{A}_2$ *álgebras,* 0_2 *o elemento neutro da soma em* $\mathcal{A}_2$ *e* $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ *um homomorfismo de álgebras. O* núcleo *de* φ *é o conjunto*

$$N(\varphi) = \{x \in \mathcal{A}_1; \varphi(x) = 0_2\}.$$

Exemplo 2.21. *Sabemos que* $(\mathcal{F}, +, *, \cdot)$ *é uma álgebra associativa com unidade, ver exemplo 2.8 na página 65. Defina,*

$$\begin{array}{rccc} \varphi: & \mathcal{F} & \longrightarrow & \mathbb{R} \\ & f & \longmapsto & f(a). \end{array}$$

Vamos mostrar que φ *é um isomorfismo, ou seja, que* $\mathcal{F}$ *é isomorfo a* $\mathbb{R}$*.*

De fato, sejam $f, g \in \mathcal{F}$ e $\alpha \in \mathbb{R}$ quaisquer. Assim temos,

$$\varphi(f+g) = (f+g)(a) = f(a) + g(a) = \varphi(f) + \varphi(g);$$

$$\varphi(f * g) = (f * g)(a) = f(a)g(a) = \varphi(f)\varphi(g);$$

$$\varphi(\alpha \cdot f) = (\alpha \cdot f)(a) = \alpha f(a) = \alpha\varphi(f).$$

Logo, φ é um homomorfismo de álgebras. Agora sejam $f, g \in \mathcal{F}$ tais que

$$\varphi(f) = \varphi(g).$$

Assim, temos que

$$\varphi(f) = \varphi(g) \Longrightarrow f(a) = g(a) \Longrightarrow f = g,$$

pois o domínio é unitário. Portanto, φ é injetiva, logo pela proposição 1.25 na página 13, temos que $N(\varphi) = \{f_0\}$, em que, f_0 é o elemento neutro da soma em $\mathcal{F}$.

Note também, que φ é sobrejetiva, pois se $x \in \mathbb{R}$ basta tomarmos $h : A \longrightarrow \mathbb{R}$ tal que, $h(a) = x$, ou seja, $h \in \mathcal{F}$, assim temos

$$\varphi(h) = h(a) = x.$$

Logo, φ é sobrejetiva. Portanto, φ é um homomorfismo injetor e sobrejetor.

Concluímos assim que φ é um isomorfismo, ou seja, $\mathcal{F} \simeq \mathbb{R}$.

Definimos no primeiro capítulo nas classes de grupos, anéis e espaços vetoriais, os conceitos de núcleo e imagem de um homomorfismo. Tais conceitos são de extrema importância, pois por exemplo os usamos no teorema do homomorfismo. Agora, na classe de álgebra esses conceitos aparecem novamente de maneira natural.

Proposição 2.22. *Sejam $\mathcal{A}_1, \mathcal{A}_2$ álgebras e $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ um homomorfismo de álgebras. O conjunto $\mathfrak{I}m(\varphi)$ é uma subálgebra de $\mathcal{A}_2$.*

Demonstração. De fato, considerando φ como uma transformação linear e a proposição 1.93 na página 46, temos que $\mathfrak{I}m(\varphi)$ é um subespaço vetorial de $\mathcal{A}_2$. Também, considerando φ como um homomorfismo de anéis, temos pela proposição 1.61 na página 33, que $\mathfrak{I}m(\varphi)$ é um subanel de $\mathcal{A}_2$.

Portanto, pela definição de subálgebra, concluímos que $\mathfrak{I}m(\varphi)$ é subálgebra de $\mathcal{A}_2$.

■

Proposição 2.23. *Sejam $\mathcal{A}_1, \mathcal{A}_2$ álgebras e $\varphi : \mathcal{A}_1 \longrightarrow \mathcal{A}_2$ um homomorfismo de álgebras. O conjunto $N(\varphi)$ é um ideal de $\mathcal{A}_2$.*

Demonstração. De fato, considerando φ como uma transformação linear e a proposição 1.92 na página 45, temos que $N(\varphi)$ é um subespaço vetorial de $\mathcal{A}_1$. Agora, considerando φ como um homomorfismo de anéis, temos pela proposição 1.62 na página 33, que $N(\varphi)$ é um ideal de anéis em $\mathcal{A}_1$. Pela definição de ideal de anéis, temos que $N(\varphi)$ é um subanel de $\mathcal{A}_1$.

Portanto, pela definição de subálgebra, concluímos que $N(\varphi)$ é subálgebra de $\mathcal{A}_1$. Como $N(\varphi)$ é subálgebra de $\mathcal{A}_1$ e pelo fato de $N(\varphi)$ ser um ideal bilateral de anéis, temos que $N(\varphi)$ também é um ideal bilateral de álgebras.

■

2.4 Teorema do Homomorfismo para Álgebras

Sejam $\mathcal{A}$ uma álgebra sobre $\mathbb{K}$ e $\mathcal{I} \subseteq \mathcal{A}$ um ideal de $\mathcal{A}$. Assim como em grupos, anéis e espaços vetoriais, podemos agora em álgebras definir de maneira natural uma relação de equivalência que determinará classes de equivalência apartir de $\mathcal{I}$. A ideia é definir álgebras quocientes e mostrar assim que o teorema do homomorfismo é válido também para álgebras.

Definição 2.24. *Sejam $\mathcal{A}$ uma álgebra sobre $\mathbb{K}$ e $\mathcal{I}$ um ideal de $\mathcal{A}$. Assim, dados $x, y \in \mathcal{A}$ dizemos que y é* congruente *a x módulo $\mathcal{I}$ ou y está relacionado com x módulo $\mathcal{I}$, quando $y - x \in \mathcal{I}$ e denotamos por*

$$y \equiv x \ (mod \ \mathcal{I}) \Longleftrightarrow y - x \in \mathcal{I}.$$

Vale salientar que a relação

$$y \equiv x \ (mod \ \mathcal{I}) \Longleftrightarrow y - x \in \mathcal{I},$$

é uma relação de equivalência. Também, já mostramos que a classe de $x \in \mathcal{A}$ é dada por

$$x + \mathcal{I} = \{x + i; \ i \in \mathcal{I}\}.$$

Sejam $\mathcal{A}$ uma álgebra sobre $\mathbb{K}$ e $\mathcal{I}$ um ideal de $\mathcal{A}$. Por definição de ideal, temos que $\mathcal{I}$ é uma subálgebra. Por definição de subálgebra, temos que $\mathcal{I}$ é um subespaço vetorial e um subanel de $\mathcal{A}$, mas $\mathcal{I}$ é mais que subanel de $\mathcal{A}$, é também um ideal de anel.

Com essas informações, podemos considerar o anel quociente $(\mathcal{A}/\mathcal{I}, +, *)$, com a soma e o produto de classes. Também, podemos considerar o espaço vetorial quociente $(\mathcal{A}/\mathcal{I}, +, \cdot)$, com soma e produto por escalar de classes.

Note que o elemento neutro da soma em $\mathcal{A}/\mathcal{I}$ é a classe $0_A + \mathcal{I} = \mathcal{I}$ e o simétrico da classe $x+\mathcal{I}$ é a classe $(-x)+\mathcal{I}$. Já mostramos que as operações de soma, produto e produto por escalar de classes estão bem definidas, ver as versões do teorema do homomorfismo para grupos, anéis e espaços vetoriais. Vamos mostrar agora, que $\mathcal{A}/\mathcal{I}$ com as operações de soma, produto e produto por escalar é também uma álgebra.

Proposição 2.25. *Sejam $(\mathcal{A}, +, *, \cdot)$ uma álgebra sobre $\mathbb{K}$ e $\mathcal{I}$ um ideal de $\mathcal{A}$. Considere $(\mathcal{I}, +, *)$ como ideal de $(\mathcal{A}, +, *)$ e $(\mathcal{I}, +, \cdot)$ como subespaço vetorial de $(\mathcal{A}, +, \cdot)$. Então*

$\mathcal{A}/\mathcal{I}$ é uma álgebra, com as operações de soma, produto e produto por escalar de classes, dadas por

$$(x+\mathcal{I})+(y+\mathcal{I})=(x+y)+\mathcal{I},$$

$$(x+\mathcal{I})*(y+\mathcal{I})=xy+\mathcal{I} \quad e$$

$$\alpha\cdot(x+\mathcal{I})=\alpha x+\mathcal{I}.$$

Demonstração. De fato, pelo que já comentamos acima, temos que $(\mathcal{A}/\mathcal{I},+,*)$ é um anel e $(\mathcal{A}/\mathcal{I},+,\cdot)$ é um espaço vetorial sobre $\mathbb{K}$. Resta mostrarmos que vale a condição **A3** da definição de álgebras. Para tanto, sejam $x+\mathcal{I}, y+\mathcal{I}\in\mathcal{A}/\mathcal{I}$ quaisquer. Assim, temos

$$\begin{aligned}[\alpha\cdot(x+\mathcal{I})]*(y+\mathcal{I}) &= (\alpha x+\mathcal{I})*(y+\mathcal{I})\\ &= (\alpha x)y+\mathcal{I}=x(\alpha y)+\mathcal{I}\\ &= (x+\mathcal{I})*((\alpha y)+\mathcal{I})\\ &= (x+\mathcal{I})*(\alpha\cdot(y+\mathcal{I})).\end{aligned}$$

Logo, $[\alpha\cdot(x+\mathcal{I})]*(y+\mathcal{I})=(x+\mathcal{I})*(\alpha\cdot(y+\mathcal{I}))$.

Também temos,

$$\begin{aligned}[\alpha\cdot(x+\mathcal{I})]*(y+\mathcal{I}) &= (\alpha x+\mathcal{I})*(y+\mathcal{I})\\ &= (\alpha x)y+\mathcal{I}=\alpha(xy)+\mathcal{I}\\ &= \alpha\cdot[(xy)+\mathcal{I}]\\ &= \alpha\cdot[(x+\mathcal{I})*(y+\mathcal{I})].\end{aligned}$$

Logo, $[\alpha\cdot(x+\mathcal{I})]*(y+\mathcal{I})=(x+\mathcal{I})*(\alpha\cdot(y+\mathcal{I}))=\alpha\cdot[(x+\mathcal{I})*(y+\mathcal{I})]$.

Portanto, a condição $A3$ da definição de álgebra é satisfeita.

Concluímos assim que $(\mathcal{A}/\mathcal{I},+,*,\cdot)$ é uma álgebra.

■

Definição 2.26. *A álgebra $(\mathcal{A}/\mathcal{I},+,*,\cdot)$ é denominada* álgebra quociente.

Teorema 2.27 (Teorema do homomorfismo para álgebras)**.** *Sejam $\mathcal{A}_1,\mathcal{A}_2$ álgebras sobre o corpo $\mathbb{K}$, e $f:\mathcal{A}_1\longrightarrow\mathcal{A}_2$ homomorfismo de álgebras. Então a função*

$$\begin{array}{rccc}\varphi: & \mathcal{A}_1/N(f) & \longrightarrow & \Im m(f)\\ & (x+N(f)) & \longmapsto & f(x)\end{array}$$

é um isomorfismo.

Demonstração. Já mostramos no teorema 1.63 na página 34 que φ está bem definida, que φ é injetiva, sobrejetiva e que ainda preserva a primeira e segunda operações de $\mathcal{A}_1/N(f)$. Também já mostramos no teorema 1.102 na página 54 que φ preserva a terceira operação de $\mathcal{A}_1/N(f)$. Segue da definição de homomorfismo de álgebras que φ é um homomorfismo de álgebras injetor e sobrejetor. Concluímos assim, que φ é um isomorfismo.

■

2.5 Álgebras com Identidades Polinomiais

Vamos estudar agora algumas álgebras com propriedades interessantes. Estamos falando de álgebras que quando avaliados seus elementos em um determinado polinômio especial, o mesmo se anula. Quando isto acontece, dizemos que esse polinômio é uma identidade polinomial para a álgebra em questão.

Definição 2.28. *Seja $\mathcal{A}$ uma $\mathbb{K}$-álgebra, dizemos que $f(x_1, \ldots, x_r) \in \mathbb{K}\langle X\rangle$ é uma* identidade polinomial *para $\mathcal{A}$, se para quaisquer $a_1, \ldots, a_r \in \mathcal{A}$,*

$$f(a_1, \ldots, a_r) = 0.$$

Lembrando que $X = \{x_1, x_2, \ldots\}$ é um conjunto infinito enumerável e $\mathbb{K}\langle X\rangle$ é a álgebra de polinômios não comutativos.

Um exemplo trivial de identidade polinomial é o polinômio nulo, ou seja, $f(x) \in \mathbb{K}\langle X\rangle$, tal que, para todo $x \in X$ tem-se $f(x) = 0$. Neste caso, $f(x)$ é identidade polinomial para qualquer álgebra.

Definição 2.29. *Uma $\mathbb{K}$-álgebra $\mathcal{A}$ é denominada uma* álgebra com identidade polinomial*, ou uma* PI-álgebra*, se $\mathcal{A}$ satisfaz alguma identidade polinomial não trivial.*

Exemplo 2.30. *Seja $\mathcal{A}$ uma álgebra comutativa, então $f(x_1, x_2) = x_1x_2 - x_2x_1$ é uma identidade polinomial de $\mathcal{A}$.*

Definição 2.31. *Seja $\mathcal{A}$ uma álgebra, a aplicação $[\cdot, \cdot] : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$, definida para quaisquer $a, b \in \mathcal{A}$ por*

$$[a, b] = ab - ba,$$

é denominada comutador*.*

Note que se $\mathcal{A}$ é uma álgebra comutativa, então o comutador de quaisquer dois elementos de $\mathcal{A}$ é igual a zero.

Proposição 2.32. *Seja $\mathcal{A}$ uma álgebra. Então o comutador $[\cdot,\cdot] : \mathcal{A} \times \mathcal{A} \longrightarrow \mathcal{A}$ é uma aplicação bilinear, ou seja, para quaisquer $a, b, c \in \mathcal{A}$ e $\alpha, \beta \in \mathbb{K}$, temos que:*

(i) $[\alpha a + \beta b, c] = \alpha[a, c] + \beta[b, c]$;

(ii) $[a, \alpha b + \beta c] = \alpha[a, b] + \beta[a, c]$.

Demonstração. Sejam $a, b, c \in \mathcal{A}$ e $\alpha, \beta \in \mathbb{K}$ quaisquer. Assim, temos

$$\begin{aligned}[\alpha a + \beta b, c] &= (\alpha a + \beta b)c - c(\alpha a + \beta b) = \alpha ac + \beta bc - c\alpha a - c\beta b \\ &= \alpha ac + \beta bc - \alpha ca - \beta cb = (\alpha ac - \alpha ca) + (\beta bc - \beta cb) \\ &= \alpha(ac - ca) + \beta(bc - cb) = \alpha[a, c] + \beta[b, c].\end{aligned}$$

Também,

$$\begin{aligned}[a, \alpha b + \beta c] &= a(\alpha b + \beta c) - (\alpha b + \beta c)a = a\alpha b + a\beta c - \alpha ba - \beta ca \\ &= \alpha ab + \beta ac - \alpha ba - \beta ca = (\alpha ab - \alpha ba) + (\beta ac - \beta ca) \\ &= \alpha(ab - ba) + \beta(ac - ca) = \alpha[a, b] + \beta[a, c].\end{aligned}$$

Portanto,

$$[\alpha a + \beta b, c] = \alpha[a, c] + \beta[b, c] \quad \text{e}$$

$$[a, \alpha b + \beta c] = \alpha[a, b] + \beta[a, c].$$

■

Já estamos mais preparados para entendermos nosso próximo exemplo. A ideia é construir uma álgebra apartir de uma lista de símbolos, chamados de geradores, sujeitos a algumas relações. Por exemplo, considere o conjunto de símbolos $X = \{x_1, x_2, \ldots, x_n\}$, em que $n \in \mathbb{N}^*$. Os elementos de X serão considerados como letras de um alfabeto e com este alfabeto, construíremos uma lista com todas as palavras finitas formadas com estas letras. Deste modo, temos um novo conjunto que denotaremos por $\widetilde{\mathcal{A}}$. Note que, os elementos de $\widetilde{\mathcal{A}}$ são palavras finitas, formadas apartir dos símbolos $x_1, x_2, \ldots, x_n$. Consideramos também como um elemento de $\widetilde{\mathcal{A}}$ a palavra vazia, ou seja, aquela em que não figura nenhum dos símbolos $x_1, x_2, \ldots, x_n$.

Podemos agora, definir um produto em $\widetilde{\mathcal{A}}$, este produto é dado pela concatenação entre quaisquer dois elementos de $\widetilde{\mathcal{A}}$, ou seja, o produto é definido simplesmente colocando um elemento ao lado do outro. Claramente, tal procedimento é associativo. Feito isso, construimos o espaço vetorial gerado por $\widetilde{\mathcal{A}}$ sobre um corpo $\mathbb{K}$ e o denotamos por $\mathcal{A}$, dessa forma, impondo a condição de que vale a distributividade da soma com respeito ao produto, teremos assim uma álgebra. Essa álgebra é chamada de *álgebra dada por geradores e relações*. No nosso próximo exemplo, iremos estudar o caso particular em que o conjunto de geradores possui apenas três elementos e é imposta uma relação na construção da álgebra.

Exemplo 2.33. *Seja $\mathcal{V}_3$ um espaço vetorial de dimensão 3, com base $\{e_1, e_2, e_3\}$. A* álgebra de Grassmann *denotada por $E(\mathcal{V}_3)$, é a álgebra gerada por $\{e_1, e_2, e_3\}$, satisfazendo para todo i, $j \in \{1, 2, 3\}$ a relação*

$$e_i e_j = -e_j e_i. \tag{2.5}$$

Vamos mostrar que $E(\mathcal{V}_3)$ satisfaz a seguinte identidade:

$$[[x_1, x_2], x_3]. \tag{2.6}$$

Primeiramente, vamos encontrar um conjunto de geradores que gere $E(\mathcal{V}_3)$ como um espaço vetorial. Primeiro, vamos mostrar que os produtos possíveis terão, no máximo, comprimento igual a três. Note que, para qualquer $i \in \{1, 2, 3\}$ tem-se

$$e_i e_i = -e_i e_i \Longrightarrow e_i e_i + e_i e_i = 0 \Longrightarrow 2e_i^2 = 0 \Longrightarrow e_i^2 = 0.$$

Agora sejam i, j, k e $l \in \{1, 2, 3\}$ quaisquer. Assim, existem pelo menos dois índices iguais. Suponha, sem perda de generalidade, que $i = j$, desta forma temos

$$e_i e_j e_k e_l = e_i e_i e_k e_l = e_i^2 e_k e_l = 0,$$

se $i = k$ temos

$$e_i e_j e_k e_l = e_i e_j e_i e_l = -e_i e_i e_j e_l = -e_i^2 e_j e_l = 0,$$

se $i = l$ temos

$$e_i e_j e_k e_l = e_i e_j e_k e_i = -e_i e_j e_i e_k = e_i e_i e_j e_k = e_i^2 e_j e_k = 0,$$

pois $e_i^2 = 0$. Logo, os produtos possíveis têm comprimento no máximo 3. Isso quer dizer que, se tivermos um produto com 4 ou mais elementos, esse produto será igual a zero.

Agora, vamos listar todos os produtos possíveis de comprimento menor ou igual a 3.

Produtos com 2 elementos:

$$e_1e_2,\ e_1e_3,\ e_2e_1,\ e_2e_3,\ e_3e_1 \ \text{ e } \ e_3e_2.$$

De (2.5) temos que:

$$e_1e_2 = -e_2e_1,\ e_1e_3 = -e_3e_1,\ e_2e_3 = -e_3e_2.$$

Assim, os geradores formados por 2 elementos são: $e_1e_2,\ e_1e_3 \ \text{ e } \ e_2e_3$.

Produtos com 3 elementos:

$$e_1e_2e_3,\ e_1e_3e_2,\ e_2e_1e_3,\ e_2e_3e_1,\ e_3e_1e_2 \ \text{ e } \ e_3e_2e_1.$$

De (2.5) temos que:

$$e_1e_2e_3 = -e_2e_1e_3 = e_2e_3e_1 = -e_3e_2e_1 = e_3e_1e_2 = -e_1e_3e_2.$$

Neste caso, temos como gerador formado por três elementos apenas $e_1e_2e_3$.

Assim, o conjunto dos geradores de $E(V_3)$, como espaço vetorial, é o conjunto

$$\{e_1,\ e_2,\ e_3,\ e_1e_2,\ e_1e_3,\ e_2e_3,\ e_1e_2e_3\}. \tag{2.7}$$

Vamos mostrar agora, que $[[x_1, x_2], x_3]$ é uma identidade polinomial para $E(V_3)$. Para isso, precisamos mostrar que $[[x_1, x_2], x_3]$ se anula para quaisquer elementos de $E(\mathcal{V}_3)$. Um elemento arbitrário de $E(\mathcal{V}_3)$ é uma combinação linear dos elementos do conjunto (2.7).

Como todo elemento é uma combinação linear dos elementos do conjunto (2.7) e pelo fato do comutador ser bilinear, pois já provamos isso na proposição 2.32 na página 79, precisamos apenas verificar que $[[x_1, x_2], x_3]$ se anula para quaisquer três elementos do conjunto (2.7). Note que, pelo fato de $e_i^2 = 0$ e pela condição (2.5), podemos reduzir nosso trabalho, veja

$$e_1(e_1e_2) = e_1^2e_2 = 0$$
$$e_1(e_1e_3) = e_1^2e_3 = 0$$

$$e_2(e_1e_2) = e_2e_1e_2 = -e_2e_2e_1 = -e_2^2e_1 = 0$$
$$e_2(e_2e_3) = e_2^2e_3 = 0$$
$$e_3(e_2e_3) = e_3e_2e_3 = -e_3e_3e_2 = -e_3^2e_2 = 0.$$

Sabemos também, que um produto com comprimento maior que 3 é zero. Então, se algum elemento do conjunto (2.7) aparecer no comutador com outro elemento de comprimento 3, temos que algum e_i terá que se repetir e dessa forma o comutador é zero.

Dessa forma, só resta verificar que $[[x_1, x_2], x_3]$ se anulará para os elementos $e_1,\ e_2$ e e_3. Para tanto, sejam i, j e $k \in \{1, 2, 3\}$ quaisquer. Assim temos,

$$\begin{aligned}
[[e_i, e_j], e_k] &= [e_i, e_j]e_k - e_k[e_i, e_j] \\
&= (e_ie_j - e_je_i)e_k - e_k(e_ie_j - e_je_i) \\
&= e_ie_je_k - e_je_ie_k - e_ke_ie_j + e_ke_je_i \\
&= e_ie_je_k + e_ie_je_k + e_ie_ke_j - e_je_ke_i \\
&= 2e_ie_je_k - e_ie_je_k + e_je_ie_k \\
&= e_ie_je_k + e_je_ie_k = e_ie_je_k - e_ie_je_k = 0.
\end{aligned}$$

Logo, $[[x_1, x_2], x_3]$ se anulará para os elementos $e_1,\ e_2$ e e_3.

Portanto, concluímos assim que $[[x_1, x_2], x_3]$ é uma identidade polinomial para $E(\mathcal{V}_3)$. Logo, a álgebra de Grassmann $E(\mathcal{V}_3)$ é uma PI-álgebra.

Definição 2.34. *Seja $\mathcal{V}$ um espaço vetorial de dimensão infinita enumerável, com base denotada por $\{e_1, e_2, e_3, \ldots\}$. A* álgebra de Grassmann $E(\mathcal{V})$ *de $\mathcal{V}$, é a álgebra gerada por $\{e_i;\ i \in \mathbb{N}^*\}$, satisfazendo para todo $i, j \in \mathbb{N}^*$ a seguinte relação:*

$$e_ie_j = -e_je_i.$$

Observação: É possível mostrar que $[[x_1, x_2], x_3]$ é uma identidade polinomial para $E(\mathcal{V})$.

Vamos definir agora, um importante polinômio, e, em seguida, vamos ver que ele é identidade polinomial para uma classe de álgebras. Mas, para isso, temos que lembrar do grupo de permutações S_k visto no exemplo 1.5 na página 6, e da definição do sinal de uma permutação, denotado por $(-1)^\sigma$, visto na definição 1.6 na página 7. Observamos também que o sinal de uma permutação é sempre 1 ou -1.

Definição 2.35. *Seja $k \in \mathbb{N}^*$. O polinômio*

$$s_k(x_1, \ldots, x_k) = \sum_{\sigma \in S_k} (-1)^\sigma x_{\sigma(1)}, \ldots, x_{\sigma(k)},$$

em que $(-1)^\sigma$ é o sinal de σ, é denominado polinômio standard *de grau k.*

Proposição 2.36. *Seja $\mathcal{A}$ uma álgebra. Então*

$$\begin{array}{rccc} s_3: & \mathcal{A} \times \mathcal{A} \times \mathcal{A} & \longrightarrow & \mathcal{A} \\ & (a_1, a_2, a_3) & \longmapsto & s_3(a_1, a_2, a_3), \end{array}$$

em que para quaisquer a_1, a_2 e $a_3 \in \mathcal{A}$ tem-se

$$s_3(a_1, a_2, a_3) = a_1a_2a_3 - a_1a_3a_2 - a_2a_1a_3 + a_2a_3a_1 + a_3a_1a_2 - a_3a_2a_1,$$

é uma aplicação trilinear, ou seja, para quaisquer a_1, a_2, a_3 e $a_4 \in \mathcal{A}$ e $\alpha, \beta \in \mathbb{K}$ temos que:

(i) $s_3(\alpha a_1 + \beta a_2, a_3, a_4) = \alpha s_3(a_1, a_3, a_4) + \beta s_3(a_2, a_3, a_4)$;

(ii) $s_3(a_1, \alpha a_2 + \beta a_3, a_4) = \alpha s_3(a_1, a_2, a_4) + \beta s_3(a_1, a_3, a_4)$;

(iii) $s_3(a_1, a_2, \alpha a_3 + \beta a_4) = \alpha s_3(a_1, a_2, a_3) + \beta s_3(a_1, a_2, a_4)$.

Demonstração. Sejam a_1, a_2, a_3 e $a_4 \in \mathcal{A}$ e $\alpha, \beta \in \mathbb{K}$, quaisquer.

$$\begin{aligned} (i)\ s_3(\alpha a_1 + \beta a_2, a_3, a_4) &= (\alpha a_1 + \beta a_2)a_3a_4 - (\alpha a_1 + \beta a_2)a_4a_3 - a_3(\alpha a_1 + \beta a_2)a_4 \\ &\quad + a_3a_4(\alpha a_1 + \beta a_2) + a_4(\alpha a_1 + \beta a_2)a_3 - a_4a_3(\alpha a_1 + \beta a_2) \\ &= \alpha a_1a_3a_4 + \beta a_2a_3a_4 - \alpha a_1a_4a_3 - \beta a_2a_4a_3 - a_3\alpha a_1a_4 \\ &\quad - a_3\beta a_2a_4 + a_3a_4\alpha a_1 + a_3a_4\beta a_2 + a_4\alpha a_1a_3 + a_4\beta a_2a_3 \\ &\quad - a_4a_3\alpha a_1 - a_4a_3\beta a_2 \\ &= \alpha a_1a_3a_4 - \alpha a_1a_4a_3 - \alpha a_3a_1a_4 + \alpha a_3a_4a_1 + \alpha a_4a_1a_3 \\ &\quad - \alpha a_4a_3a_1 + \beta a_2a_3a_4 - \beta a_2a_4a_3 - \beta a_3a_2a_4 + \beta a_3a_4a_2 \\ &\quad + \beta a_4a_2a_3 - \beta a_4a_3a_2 \\ &= \alpha(a_1a_3a_4 - a_1a_4a_3 - a_3a_1a_4 + a_3a_4a_1 + a_4a_1a_3 - a_4a_3a_1) \\ &\quad + \beta(a_2a_3a_4 - a_2a_4a_3 - a_3a_2a_4 + a_3a_4a_2 + a_4a_2a_3 - a_4a_3a_2) \\ &= \alpha s_3(a_1, a_3, a_4) + \beta s_3(a_2, a_3, a_4). \end{aligned}$$

Os casos (ii) e (iii) são análogos.

Portanto, $s_3(a_1, a_2, a_3)$ é uma aplicação trilinear, ou seja, é linear em cada entrada.

■

Teorema 2.37. *Seja $\mathcal{A}$ uma álgebra de dimensão r, então s_{r+1} é uma identidade polinomial de $\mathcal{A}$.*

Demonstração.(parcial) Vamos verificar o caso particular em que $r = 2$. Sejam $\mathcal{A}$ uma álgebra de dimensão dois e $\{r_1, r_2\}$ uma base de $\mathcal{A}$. Note que, um elemento arbitrário $a \in \mathcal{A}$ pode ser expresso de maneira única como

$$a = \alpha r_1 + \beta r_2,$$

onde, $\alpha, \beta \in \mathbb{K}$. Já mostramos na proposição 2.36 na página 83, que s_3 é linear em cada entrada, ou seja, só precisamos verificar se s_3 se anula para os elementos da base. Note que, precisamos de três elementos para aplicar em s_3, e, só temos dois elementos distintos na base, ou seja, algum deles teremos que repetir. Sem perda de generalidade, considere r_1 o elemento que aparecerá repetido quando calcularmos s_3. Logo,

$$\begin{aligned} s_3(r_1, r_2, r_1) &= r_1r_2r_1 - r_1r_1r_2 - r_2r_1r_1 + r_2r_1r_1 + r_1r_1r_2 - r_1r_2r_1 \\ &= (r_1r_2r_1 - r_1r_2r_1) + (r_2r_1r_1 - r_2r_1r_1) + (r_1r_1r_2 - r_1r_1r_2) = 0. \end{aligned}$$

Também não é difícil mostrar que a ordem em que os elementos aparecem em s_3 não é relevante. Assim, concluímos que s_3 é uma identidade polinomial para $\mathcal{A}$.

■

Sabemos que a álgebra de matrizes $M_n(\mathbb{K})$ tem dimensão n^2. Como consequência do teorema anterior temos o seguinte resultado.

Corolário 2.38. *A álgebra de matrizes $M_n(\mathbb{K})$ satisfaz a identidade standard de grau $n^2 + 1$.*

Demonstração. De fato, como $M_n(\mathbb{K})$ tem dimensão n^2, pelo teorema anterior, temos que $M_n(\mathbb{K})$ satisfaz a identidade standard de grau $n^2 + 1$.

■

Em particular, s_5 é uma identidade polinomial para $M_2(\mathbb{K})$, pois $dim\ M_2(\mathbb{K}) = 4$.

Podemos concluir assim do teorema 2.37 que toda álgebra de dimensão finita é uma PI-álgebra.

Vimos que não é tão fácil mostrar que determinado polinômio é uma identidade polinomial para alguma álgebra. Nos nossos dois últimos exemplos, tivemos um pouco de trabalho, pois para que um polinômio seja uma identidade de uma álgebra ele tem que se anular para todos os elementos da álgebra. Para mostrar que um polinômio não é uma identidade polinomial para uma álgebra, basta encontrar elementos dessa álgebra, de modo que este polinômio não se anule neles.

Exemplo 2.39. *O polinômio standard de grau* 3 *não é uma identidade polinomial para* $M_2(\mathbb{K})$.

De fato, já comentamos no exemplo 1.81 na página 41, que os elementos da base canônica de $M_2(\mathbb{K})$, são as matrizes e_{ij}, em que $i, j \in \{1, 2\}$ e tais que, e_{ij} é a matriz em que o número 1 se encontra na i-ésima linha e na j-ésima coluna e o restante dos elementos são todos iguais a zero. Não é difícil mostrar que se e_{ij} e e_{kl} são matrizes da base canônica de $M_2(\mathbb{K})$, então

$$e_{ij}e_{kl} = \begin{cases} e_{il}, \text{ se } j = k \\ 0, \text{ se } j \neq k. \end{cases}$$

Agora considere as matrizes,

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \; e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Como

$$s_3(x_1, x_2, x_3) = x_1x_2x_3 - x_1x_3x_2 - x_2x_1x_3 + x_2x_3x_1 + x_3x_1x_2 - x_3x_2x_1,$$

então

$$\begin{aligned} s_3(e_{11}, e_{12}, e_{21}) &= e_{11}e_{12}e_{21} - e_{11}e_{21}e_{12} - e_{12}e_{11}e_{21} \\ &\quad + e_{12}e_{21}e_{11} + e_{21}e_{11}e_{12} - e_{21}e_{12}e_{11} \\ &= e_{12}e_{21} + e_{11}e_{11} + e_{21}e_{12} \\ &= e_{11} + e_{11} + e_{22} = 2e_{11} + e_{22} \\ &= \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Portanto, s_3 não é uma identidade polinomial para $M_2(\mathbb{K})$.

Já sabemos a definição de uma identidade polinomial e de uma PI-álgebra. Naturalmente, podemos perguntar: O conjunto de todas as identidades polinomiais de uma álgebra, possui alguma propriedade interessante? Veremos a seguir que a resposta é afirmativa. Mas antes, vamos definir e denotar este conjunto.

Definição 2.40. *Seja $\mathcal{A}$ uma álgebra, denotamos por $\mathrm{T}(\mathcal{A})$ o conjunto de todas as identidades polinomiais de $\mathcal{A}$, em que $\mathrm{T}(\mathcal{A}) \subset \mathbb{K}\langle X\rangle$.*

Note que $\mathrm{T}(\mathcal{A})$ não é vazio, pois o polinômio nulo é identidade polinomial para qualquer álgebra.

Exemplo 2.41. $[[x_1, x_2], x_3] \in \mathrm{T}(E(\mathcal{V}))$ *e* $s_5 \in \mathrm{T}(M_2(\mathbb{K}))$.

Perceba que $\mathrm{T}(\mathcal{A}) \subset \mathbb{K}\langle X\rangle$. Então, faz sentido perguntarmos se $\mathrm{T}(\mathcal{A})$ possui alguma estrutura, já que $\mathbb{K}\langle X\rangle$ é uma álgebra. Vamos ver isso na próxima proposição.

Proposição 2.42. *Seja $\mathcal{A}$ uma álgebra, então $\mathrm{T}(\mathcal{A})$ é um ideal de $\mathbb{K}\langle X\rangle$.*

Demonstração. Primeiramente, vamos mostrar que $\mathrm{T}(\mathcal{A})$ é uma subálgebra de $\mathbb{K}\langle X\rangle$. Para tanto, sejam $f, g \in \mathrm{T}(\mathcal{A})$, $a_1, \ldots, a_r \in \mathcal{A}$ e $\alpha \in \mathbb{K}$ quaisquer. Note que sem perda de generalidade, podemos considerar f e g nas mesmas variáveis, $x_{i_1}, x_{i_2}, \ldots, x_{i_r}$ tais que $i_1 < i_2 < \ldots < i_r$. Assim, temos

$$(f+g)(a_1, \ldots, a_r) = f(a_1, \ldots, a_r) + g(a_1, \ldots, a_r) = 0 + 0 = 0,$$

pois f, g são identidades polinomiais para $\mathcal{A}$. Logo, $f+g$ é uma identidade polinomial para $\mathcal{A}$, ou seja, $f+g \in \mathrm{T}(\mathcal{A})$. Também temos

$$(\alpha f)(a_1, \ldots, a_r) = \alpha f(a_1, \ldots, a_r) = \alpha 0 = 0.$$

Logo, $\alpha f \in \mathrm{T}(\mathcal{A})$.

Portanto, pela definição 1.70 na página 38, temos que $\mathrm{T}(\mathcal{A})$ é um subespaço vetorial de $\mathbb{K}\langle X\rangle$. Assim, $\mathrm{T}(\mathcal{A})$ também é um espaço vetorial e $(\mathrm{T}(\mathcal{A}), +)$ é um grupo abeliano e portanto, $(\mathrm{T}(\mathcal{A}), +)$ é subgrupo de $(\mathbb{K}\langle X\rangle, +)$. Agora temos

$$(f \cdot g)(a_1, \ldots, a_r) = f(a_1, \ldots, a_r) \cdot g(a_1, \ldots, a_r) = 0 \cdot 0 = 0.$$

Logo, $f \cdot g \in \mathrm{T}(\mathcal{A})$.

Portanto, pela proposição 1.44 na página 26, temos que $\mathrm{T}(\mathcal{A})$ é subanel de $\mathbb{K}\langle X\rangle$.

Concluímos assim, que $\mathrm{T}(\mathcal{A})$ é uma subálgebra de $\mathbb{K}\langle X\rangle$.

Vamos mostrar agora, que $\mathrm{T}(\mathcal{A})$ é um ideal de $\mathbb{K}\langle X\rangle$. Para tanto, sejam $f \in \mathrm{T}(\mathcal{A})$, $g \in \mathbb{K}\langle X\rangle$ e $a_1, \ldots, a_r \in \mathcal{A}$ quaisquer. Novamente, sem perda de generalidade, podemos considerar f e g nas mesmas variáveis, $x_{i_1}, x_{i_2}, \ldots, x_{i_r}$ tais que $i_1 < i_2 < \ldots < i_r$. Assim, temos

$$(f \cdot g)(a_1, \ldots, a_r) = f(a_1, \ldots, a_r) \cdot g(a_1, \ldots, a_r) = 0 \cdot g(a_1, \ldots, a_r) = 0;$$

$$(g \cdot f)(a_1, \ldots, a_r) = g(a_1, \ldots, a_r) \cdot f(a_1, \ldots, a_r) = g(a_1, \ldots, a_r) \cdot 0 = 0.$$

Logo, $f \cdot g$ e $g \cdot f \in \mathrm{T}(\mathcal{A})$.

Portanto, $\mathrm{T}(\mathcal{A})$ é um ideal de $\mathbb{K}\langle X\rangle$.

■

Definição 2.43. *Seja $\mathcal{A}$ uma álgebra, $\mathrm{T}(\mathcal{A})$ é denominado* T-ideal *de $\mathcal{A}$.*

Além de $\mathrm{T}(\mathcal{A})$ ser um ideal de $\mathcal{A}$, ele tem a propriedade de ser invariante por endomorfismos, ou seja, se $\varphi : \mathbb{K}\langle X\rangle \longrightarrow \mathbb{K}\langle X\rangle$ é um endomorfismo de álgebras, então

$$\varphi(\mathrm{T}(\mathcal{A})) \subset \mathrm{T}(\mathcal{A}).$$

Isso quer dizer que, dada uma identidade polinomial não importa o "nome das variáveis". Por exemplo, se $\mathcal{A}$ é uma álgebra comutativa, sabemos que

$$f(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1$$

é uma identidade polinomial para $\mathcal{A}$. Note que, se trocarmos x_1, x_2 por x_{21}, x_{15} o polinômio

$$f(x_{21}, x_{15}) = [x_{21}, x_{15}] = x_{21}x_{15} - x_{21}x_{15}$$

continua sendo uma identidade polinomial de $\mathcal{A}$. Mas ser invariante por endomorfismos é mais do que trocar variáveis, podemos também trocar uma variável por qualquer elemento de $\mathbb{K}\langle X\rangle$. Exemplificaremos mais uma vez com uma álgebra comutativa $\mathcal{A}$. Considere o polinômio

$$g(x_4, x_7, x_{13}, x_{21}) = [7x_4^3 + x_7^2x_{13}, x_{21}] = f(7x_4^3 + x_7^2x_{13}, x_{21}).$$

Vamos mostrar que g é uma identidade polinomial para $\mathcal{A}$. Para tanto, sejam a, b, c

e $d \in \mathcal{A}$ quaisquer. Assim temos

$$\begin{aligned} g(a,b,c,d) = [7a^3 + b^2c, d] &= (7a^3 + b^2c)d - d(7a^3 + b^2c) \\ &= (7a^3 + b^2c)d - (7a^3 + b^2c)d = 0, \end{aligned}$$

pois $\mathcal{A}$ é comutativa. Logo, g é também uma identidade polinomial de $\mathcal{A}$.

Concluindo, $\mathrm{T}(\mathcal{A})$ ser invariante por endomorfismos de $\mathbb{K}\langle X\rangle$ significa que para todo $f(x_1, \ldots, x_r) \in \mathrm{T}(\mathcal{A})$, podemos trocar qualquer x_i, $i \in \{1, \ldots, r\}$, por qualquer elemento de $\mathbb{K}\langle X\rangle$, e f, depois dessa alteração, continuará sendo uma identidade polinomial de $\mathcal{A}$.

Vimos na definição 2.16 na página 73, o conceito de ideal gerado por um conjunto de elementos, será que é possível encontrar geradores para os T-ideais? Mais ainda, será possível encontrar um conjunto finito de geradores? Este problema é conhecido como **Problema de Specht**. O mesmo foi resolvido por Kemer, quando a característica do corpo $\mathbb{K}$ é zero.

Definição 2.44. *Seja $\mathcal{S}$ um subconjunto de $\mathbb{K}\langle X\rangle$. Definimos o T-ideal gerado por $\mathcal{S}$, denotado por $\langle\mathcal{S}\rangle^T$, como sendo a intersecção de todos os T-ideais de $\mathbb{K}\langle X\rangle$ que contêm $\mathcal{S}$, ou seja,*

$$\langle\mathcal{S}\rangle^T = \bigcap_{\mathcal{I} \text{ é } T\text{-ideal},\ \mathcal{S}\subseteq\mathcal{I}} \mathcal{I}.$$

Teorema 2.45 (Kemer)**.** *Seja $\mathcal{A}$ uma álgebra sobre $\mathbb{K}$. Se $char(\mathbb{K}) = 0$, então o* T*-ideal $\mathrm{T}(\mathcal{A})$ é finitamente gerado.*

A prova do teorema 2.45 pode ser encontrada em [10].

Vamos ver agora, alguns exemplos de problemas na teoria de PI-álgebras.

Perguntas naturais:

• Dada uma álgebra, determinar se ela satisfaz alguma identidade polinomial.

• Sabendo que uma álgebra satisfaz uma identidade polinomial, determinar se seu T-ideal é finitamente gerado ou não.

• Sabendo que o T-ideal de uma álgebra é finitamente gerado, determinar seus geradores.

• Determinar um conjunto minimal de geradores, denominado *base*.

Veja dois resultados que determinam uma base para dois T-ideais.

Teorema 2.46. *Seja $E(\mathcal{V})$ a álgebra de Grassmann, então o* T*-ideal* $\mathrm{T}(E(\mathcal{V}))$ *é gerado como* T*-ideal por* $[x_1, x_2, x_3]$.

Teorema 2.47. *Se* $char(\mathbb{K}) \neq 2$*, então o* T*-ideal* $\mathrm{T}(M_2(\mathbb{K}))$ *é gerado como* T*-ideal por* $[[x_1, x_2]^2, x_3]$ *e* s_4.

As provas para os teoremas 2.46 e 2.47, podem ser encontradas em [11] e [12], respectivamente.

Apesar do resultado anterior, ainda não sabemos uma base, nem mesmo uma lista de geradores, para o T-ideal $\mathrm{T}(M_n(\mathbb{K}))$ em que $n \geq 3$.

Essa é uma das belezas da Matemática: problemas nem tão difíceis de entender, porém complicadíssimos de se resolver.

Considerações Finais

Antes de partirmos efetivamente para as considerações finais, gostaria de dizer que este trabalho possibilitou com que eu me aprofundasse um pouco mais nos conteúdos das disciplinas de Álgebra I e II, disciplinas que eu particularmente, penso ser umas das mais importantes do curso, pela generalidade que permite. Além disso, pude interligar conteúdos que são, aparentemente separados, como grupos, anéis e espaços vetoriais.

Entre os resultados apresentados neste trabalho, destaco a álgebra de Grassmann como uma PI-álgebra, tendo $[[x_1, x_2], x_3]$ como uma identidade polinomial e o teorema 2.37 na página 84, que surpreende pela generalidade, pois com ele concluímos que qualquer álgebra de dimensão finita é na verdade uma PI-álgebra, tendo o polinômio standard de grau k como identidade polinomial para qualquer álgebra de dimensão igual a $k-1$. Vimos que s_5 é uma identidade polinomial para $M_2(\mathbb{K})$, mas que s_3 não é identidade polinomial para $M_2(\mathbb{K})$, entre s_3 e s_5 passou, de certa forma despercebido, o s_4, uma pergunta natural seria: s_4 é identidade polinomial para $M_2(\mathbb{K})$? A resposta para essa pergunta é afirmativa e faz uso de um teorema conhecido como *O teorema de Amitsur-Levitzki*. Provado na década de 50, este teorema nos garante que s_{2n} é identidade polinomial para $M_n(\mathbb{K})$ e sua prova faz uso de propriedades do polinômio standard e da teoria de grafos, o que não compete a esse trabalho de caráter introdutório.

Pode-se dizer que ainda há um grande caminho a percorrer na teoria de álgebras com identidades polinomiais. Sabemos que $\mathrm{T}(M_2(\mathbb{K}))$ é gerado como T-ideal por $[[x_1, x_2]^2, x_3]$ e s_4, mas quais identidades polinomiais de $M_n(\mathbb{K})$ nos permitem reconstruir todas as outras? A resposta para essa pergunta ainda não se sabe. Dessa forma, fica evidenciado neste trabalho, uma das mais belas características da Matemática, que é a de fornecer problemas de fácil compreensão, mas de uma complexidade enorme para se provar.

Referências

[1] MATTOS, Alda Dayana; REIS, Júlio César; SOUZA, Manuela da Silva. Matrizes: Existem perguntas que ainda não sabemos responder? Uma introdução às Álgebras com Identidades polinomiais. II Colóquio de Matemática da região Centro-Oeste, Cuiabá, 2011.

[2] DOMINGUES, H. H; IEZZI, G. Álgebra Moderna, volume único, 4ª edição reformada, São Paulo, 2003.

[3] JANESCH, Oscar Ricardo; TANEJA, Inder Jeet. . Álgebra I. Florianópolis: UFSC/EAD, 2008. 217p.ISBN 9788599379486.

[4] JANESCH, Oscar Ricardo. Álgebra II. Florianópolis: UFSC/EAD, 2008. 216p. ISBN 9788599379561

[5] LANG, Serge. Estruturas algébricas. Rio de Janeiro: Ao Livro Técnico, 1972.

[6] LANG, Serge. Álgebra Linear, São Paulo: Ciência Moderna, 2003.

[7] CALLIOLI, C. A; DOMINGUES, H. H; COSTA, R. F., Álgebra Linear e Aplicações, 7. Ed., São Paulo: Atual, 1990.

[8] BIEZUNER, Rodney Josué. Álgebra Linear, primeiro semestre de 2006, Notas de Aula. Mimeografado.

[9] DE OLIVEIRA, M. M. Identidades de Álgebras de Matrizes e o Teorema de Amitsur-Levitzki. 2010. 93f. Dissertação (Mestrado em Matemática)- Centro de Ciências e Tecnologia, Universidade Federal de Campina Grande, Campina Grande. 2010.

[10] KEMER, A. Ideal of identities of associative algebras, Amer. Math. Soc. Transl. Ser. 87, 1991.

[11] COSTA, N. L. Identidades Polinomiais e Polinômios Centrais para Álgebras de Grassmann. 2012. 99f. Dissertação (Mestrado em Matemática)- Centro de Ciências e Tecnologia, Universidade Federal de Campina Grande, Campina Grande. 2012.

[12] DRENSKY, V. A minimal basis for the identities of a second-order matrix algebra over a field of characteristic 0, Algebra and Logic 12, 188-194 (1981).