UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
CAMPUS CHAPECÓ
CURSO DE MATEMÁTICA - LICENCIATURA

AUGUSTO MORLIN MORETTO

MÓDULOS E ÁLGEBRAS:
UM ESTUDO DE EXEMPLOS

CHAPECÓ
2022

AUGUSTO MORLIN MORETTO

MÓDULOS E ÁLGEBRAS:
UM ESTUDO DE EXEMPLOS

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática da Universidade Federal da Fronteira Sul (UFFS), como requisito para obtenção do título de licenciado em Matemática.

Orientador: Prof. Me. Antonio Marcos Correa Neri

CHAPECÓ

2022

Bibliotecas da Universidade Federal da Fronteira Sul - UFFS

Moretto, Augusto Morlin
Módulos e Álgebras: Um Estudo de Exemplos / Augusto Morlin Moretto. -- 2022.
51 f.

Orientador: mestre Antonio Marcos Correa Neri

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal da Fronteira Sul, Curso de Licenciatura em Matemática, Chapecó,SC, 2022.

1. Álgebras. 2. Módulo. 3. Anel. I. Neri, Antonio Marcos Correa, orient. II. Universidade Federal da Fronteira Sul. III. Título.

Elaborada pelo sistema de Geração Automática de Ficha de Identificação da Obra pela UFFS com os dados fornecidos pelo(a) autor(a).

AUGUSTO MORLIN MORETTO

MÓDULOS E ÁLGEBRAS:
UM ESTUDO DE EXEMPLOS

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura em Matemática da Universidade Federal da Fronteira Sul (UFFS), como requisito para obtenção do título de licenciado em Matemática.

Este trabalho foi defendido e aprovado pela banca em: 24/08/2022.

Prof. Me. Antonio Marcos Correa Neri - UFFS
Orientador

Profa. Dra. Janice Teresinha Reichert - UFFS
Avaliadora

Prof. Me. Edson Ribeiro dos Santos - UFFS
Avaliador

AGRADECIMENTOS

Agradeço a todas e a todos que de alguma forma me ajudaram a chegar até aqui.

RESUMO

O objetivo deste trabalho é apresentar a estrutura de *Álgebras* e alguns exemplos. Para a definição tornam-se necessários os conceitos de Anel, apresentado no primeiro Capítulo, e Módulos, no capítulo seguinte. Também são apresentados os conjuntos de *ideais* sobre anéis e *submódulos sobre módulos* e os conceitos de *conjunto quociente* e de *homomorfismo* de anéis e de módulos. Assim, obtém-se o conjunto necessário de premissa para apresentar a estrutura de *Álgebras* e alguns exemplos. Por fim, serão apresentados os conceitos de conjunto quociente e homomorfismo de Álgebras e demonstrado o resultado do *Teorema do Homomorfismo para Álgebras*.

Palavras-chave: Álgebra. Anel. Módulo.

ABSTRACT

The objective of this work is to present the structure of *Algebras* and some examples. For the definition, the concepts of Ring, presented in the first Chapter, and Modules, in the following chapter, become necessary. The sets of *ideals* over rings and *submodules over modules* and the concepts of *quotient set* and *homomorphism* of rings and modules are also presented. Thus, we obtain the necessary set of premises to present the structure of *Algebras* and some examples. Finally, the concepts of quotient set and homomorphism of Algebras will be presented and the result of the *Homomorphism Theorem for Algebras* will be demonstrated.

Keywords: Algebra. Ring. Module.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem por objetivo definir o que é uma *Álgebra* e apresentar alguns exemplos. Para a definição de álgebra são necessárias duas estruturas algébricas, que são os *anéis* e os *módulos* (em particular os *espaços vetoriais*). Um conhecimento prévio sobre grupos pode facilitar a leitura mas será feita uma pequena apresentação no Capítulo 1. A fundamentação teórica pode ser encontrada em (DOMINGUES H. H.; IEZZI, 2003). Ademais algumas definições sobre anéis e módulos podem ser estendidas para álgebras.

No Capítulo 2, define-se o que é um anel. A definição de anel parte de um conjunto dotado de duas operações. Além dessas também são apresentadas as definições sobre subanéis, ideais, anel quociente e homomorfismo de anéis. Será dado destaque aos resultados de anel quociente e homomorfismos de anéis, pois permitem a extensão do conceito para álgebras.

No Capítulo 3, está o que se define por módulo. Trazendo a estrutura do que é um módulo e alguns exemplos. Trata-se ainda de definir sub-módulos e homomorfismos de módulos que merecem destaque pelo mesmo motivo que os conceitos de ideais e homomorfismos de anéis.

Após apresentados os conceitos de anéis e módulos torna-se possível definir as Álgebras. É o que será feito no Capítulo 4, bem como serão apresentados alguns exemplos e proposições sobre álgebras.

2 PRELIMINARES

A construção de estruturas importantes como as de *módulos* podem ser dados aproveitando os conceitos de *grupo* e *subgrupo*. Entende-se que seja pertinente a apresentação que segue.

2.1 GRUPOS

Definição 2.1.1. *Seja G um conjunto dotado de uma operação da forma*

$$\cdot : G \times G \longrightarrow G$$

$$(a, b) \mapsto a \cdot b.$$

O conjunto será chamado de Grupo caso se verifique:

i) A associatividade, ou seja, para todos $g, h, i \in G$, vale $(g \cdot h) \cdot i = g \cdot (h \cdot i)$.

ii) A existência de um elemento neutro, ou seja, existe $h \in G$ tal que $g \cdot h = g$, geralmente denotado por e_G.

iii) A existência de oposto, ou seja, para todo $g \in G$ existe $h \in G$ tal que $g \cdot h = e_G$. Neste caso h é denotado por g^{-1}.

Nos casos em que a operação $\cdot$ é comutativa, ou seja, para quaisquer $g, h \in G$ vale $g \cdot h = h \cdot g$, o grupo G é dito *grupo abeliano*.

Definição 2.1.2. *Sejam G um grupo e $H \subset G$. Chama-se H de subgrupo de G caso H seja grupo para a operação de G.*

Exemplo 2.1.1. *Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são grupos considerando a operação de adição da forma usual.*

Exemplo 2.1.2. *$\mathbb{Q}^*$ e $\mathbb{R}^*$ são grupo com a multiplicação usual.*

3 ANÉIS

Os anéis são estruturas algébricas importantes, sendo o conceito de *anel* conhecido e utilizado na teoria de números algébricos por Richard Dedekind e Leopolde Kroneker (1823 - 1891) mas com o nome de *ordem*. Em 1897 o termo *anel* foi introduzido por David Hilbert (1862 - 1943), ainda no contexto da teoria dos números algébricos. A primeira definição abstrata surgiu apenas em 1914 por Abraham A. Fraenkel (1891 - 1965) em um artigo ilustrando a abrangência do conceito dando alguns exemplos. Uma outra definição abstrata também foi feita pelo matemático japonês Masazo Sono em um artigo de 1917, sendo a dele a definição de anel utilizada atualmente. A seguir define-se o que é um *anel* e algumas de suas propriedades.

3.1 ANÉIS

Definição 3.1.1. *Seja um conjunto não vazio A dotado de duas operações:*

$$+ : A \times A \longrightarrow A$$

$$(a, b) \mapsto a + b$$

$$\cdot : A \times A \longrightarrow A$$

$$(a, b) \mapsto a \cdot b$$

chamadas respectivamente de adição e multiplicação. O conjunto A é um anel caso se verifique:

i) A associatividade na adição, ou seja, para todos $a, b, c \in A$, vale $(a+b)+c = a+(b+c)$.

ii) A comutatividade na adição, ou seja, para todos $a, b \in A$, vale $a + b = b + a$.

iii) A existência de um elemento neutro na adição, ou seja, existe $b \in A$ tal que $a+b = a$ para todo $a \in M$. Este b é geralmente denotado por 0_A. Pode-se referir a 0_A como elemento nulo ou ainda zero de A.

iv) A existência de oposto na adição, ou seja, para todo $a \in A$ existe $b \in A$ tal que $a + b = 0_A$. Neste caso b é denotado por $-a$.

v) A associatividade na multiplicação, ou seja, para todos $a, b, c \in A$ é verdadeiro que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

vi) A distributividade da multiplicação em relação a adição, ou seja, dados $a, b, c \in A$ vale a expressão $a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$.

Para evitar excessos a partir daqui será omitido em alguns casos o sinal da multiplicação, fazendo $a \cdot b = ab$.

O anel A pode ser representado assim: $(A, +, \cdot)$. É possível ainda que o anel seja um *anel comutativo*, isto é, $ab = ba$ para todos $a, b \in A$. Quando o anel A possui elemento neutro para a multiplicação, esse é chamado de *anel com unidade*, ou seja existe $b \in A$ para todo $a \in A$ tal que $ab = ba = a$, geralmente denotado por 1_A. Há exemplos de anéis comutativos com unidade $(\mathbb{Z}, +, \cdot)$, comutativos sem unidade ($\mathbb{Z} \times \{0\}$ com as operações induzidas de $\mathbb{Z}$) e anéis com unidade que não são comutativos (anéis de matrizes, como será visto posteriormente).

Definição 3.1.2. *Um elemento a do anel com unidade A é chamado inversível se existir $b \in A$ tal que $ab = 1_A$. b é denotado por a^{-1}.*

Caso o conjunto A seja um anel comutativo com unidade e todo elemento não nulo é inversível, ele é chamado de *corpo*. Implica dizer que se $\mathbb{K}$ é corpo, o conjunto $\mathbb{K}^*$ dos elementos diferentes de zero é um grupo abeliano em relação à multiplicação.

Perceba que dado um anel A, para qualquer $a \in A$ $0_A a = a0_A = 0_A$.

Exemplo 3.1.1. *Considerando as operações usuais, os conjuntos $\mathbb{Q}$ e $\mathbb{R}$ são corpos, porém o conjunto dos inteiros, $\mathbb{Z}$, é um exemplo de anel comutativo e com unidade que não é corpo, pois apenas 1 e -1 são seus elementos inversíveis.*

Exemplo 3.1.2. *O conjunto $M_n[\mathbb{K}]$ das matrizes quadradas de ordem n com coeficientes em $\mathbb{K}$, com as operações usuais é um anel não comutativo.*

Exemplo 3.1.3. *Se A é um anel, então o conjunto dos polinômios em A, $A[X]$ também é um anel.*

Os exemplos **3.1.3.** e **3.1.3.** serão abordados novamente no **Capítulo 4**.

Definição 3.1.3. *Seja A um anel e A' um subconjunto de A. A' é um subanel de A caso verifique:*

i) A' é fechado em relação as operações de A.

ii) A' é um anel em relação as operações induzidas por restrição das operações de A.

3.2 IDEAL

Do ponto de vista das estruturas algébricas, o conceito de subanel não é das entidades mais imprescindíveis. O conceito abaixo, de ideais, acaba sendo mais importante, pois permite a construção de estruturas mais abrangentes, como a de anéis quociente.

Definição 3.2.1. *Um subconjunto I de um anel A diz-se um ideal à esquerda de A se verifica:*

i) I é um subgrupo de A em relação à adição.

ii) $ai \in I$ para quaisquer $a \in A$ e $i \in I$.

De modo análogo define-se *ideal à direita*. Caso o ideal I seja ideal à esquerda e à direita de A, ele é chamado de *ideal bilateral*. Perceba que isto não significa que $ai = ia$, em geral. Caso A seja anel comutativo, então todos ideal é bilateral. A partir de agora será referido a *ideal à esquerda* por *ideal* apenas.

Exemplo 3.2.1. *Seja A um anel. $\{0_A\}$ e A são ideais de A, chamados de ideais triviais.*

Exemplo 3.2.2. *O conjunto $2\mathbb{Z} = \{2x | x \in \mathbb{Z}\}$ é um ideal, pois a soma de dois números pares é par e o produto de qualquer inteiro por um inteiro par é par.*

Exemplo 3.2.3. *Sejam I e J ideais de um anel A. O conjunto $I+J = \{i+j | i \in I, j \in J\}$ é um ideal.*

Para que $I+J$ seja um ideal, deve valer $(i+j)+(h+k) \in I+J$ com $i+j, h+k \in I+J$. De fato, $(i+j)+(h+k) = i+j+h+k = i+h+j+k = (i+h)+(j+k)$ com $i+h \in I$ e $j+k \in J$. Como a adição é comutativa conclui-se que $(i+h)+(j+k) = (i+j)+(h+k) \in I+J$.

Também é necessário que dado $a \in A$, a multiplicação $a(i+j) \in I+J$. Basta ver que $a(i+j) = ai + aj$ e por I e J serem ideais, vem que $ai \in I$ e $aj \in J$ de modo que $a(i+j) \in I+J$.

3.3 ANEL QUOCIENTE

A partir de um *ideal bilateral* $I \subset A$, pode-se construir outro anel, chamado *anel quociente* de A módulo I. Este importante anel está fortemente associado com muitos teoremas de estrutura, que não serão apresentados. Entretanto, o *teorema do homomorfismo* é base para tais teoremas e será demonstrado em sua versão para álgebras.

Sejam A um anel e I um ideal bilateral. Define-se em A a seguinte relação: dados $a, b \in A$, "aRb se e somente se $a - b \in I$". Verifica-se que a relação é de equivalência, pois é *reflexiva*: dado $a \in A$, aRa, pois $a - a \in I$ visto que $a - a = 0_A$ e $0_A \in I$; é *simétrica*, pois dados $a, b \in A$ caso aRb, então $a - b \in I$. Como I é subgrupo fechado para a adição, $b - a \in I$ e então bRa; e é *transitiva*, pois dados $a, b, c \in I$ se aRb e bRc sabe-se que $a - b,\ b - c \in I$. Como I é subgrupo aditivo. $(a - b) + (b - c) = a - c \in I$ e aRc.

Definição 3.3.1. *O conjunto*

$$a + I = \{a + i \mid i \in I\}$$

será chamado de classe de equivalência em a.

O nome se justifica pela proposição abaixo.

Proposição 3.3.1. *São equivalentes, para todos $a, b \in A$:*

i) aRb.

ii) $a + I = b + I$.

iii) $a - b \in I$.

Demonstração. i) $\iff$ *iii)* pela definição da relação. *iii)* $\Rightarrow$ *ii)* Agora, se $a - b \in I$, então fazendo $ia - b$, tem-se $a = b + i$ e portanto $a \in b + I$. Isto garante que se $x \in a + I$ então $x = a + j$ com $j \in I$. Daí $x = a + j = b + i + j = b + h$ com $h \in I$. Daí $x \in b + I$ e $a + I \subset b + I$. De maneira análoga, prova-se que $b + I \subset a + I$. *ii)* $\Rightarrow$ *iii)* Suponha que $a + I = b + I$, então $a = b + i$ para algum $i \in I$. Logo $a - b = i \in I$.

□

O conjunto $A/I = \{a + I | a \in A\}$ é chamado *anel quociente de A módulo I.*

Para o conjunto A/I é possível definir duas operações:

$$(a + I) + (b + I) = (a + b) + I$$

$$(a + I) \cdot (b + I) = (a \cdot b) + I,$$

denominadas por adição e multiplicação, respectivamente.

É necessário que as operações estejam bem definidas para garantir que caso escolhidos $a + I = a' + I$ e $b + I = b' + I$, com $a \neq a'$ e $b \neq b'$ tanto adição quanto multiplicação garantam que

$$(a + b) + I = (a' + b') + I$$

e

$$(ab) + I = (a'b') + I.$$

Assim, tomam-se $a + I = a' + I$ e $b + I = b' + I$. Sabe-se que $a - a' \in I$ e $b - b' \in I$. Logo para adição vale $(a-a')+(b-b') \in I$. Então $(a+b)-(a'+b') \in I$ e $(a+b)+I = (a'+b')+I$ de modo que a adição está bem definida. Para a multiplicação consideram-se $(a-a')b \in I$ e $a'(b - b') \in I$. Ainda $(a - a')b + a'(b - b') \in I$, então $ab - a'b + a'b - a'b' \in I$. Logo $(ab - a'b') \in I$ e $(ab) + I = (a'b') + I$ e a multiplicação também está bem definida. Se $a, b, c \in A$, então são verdadeiras as seguintes propriedades:

i) A associatividade para a adição:

$$\begin{aligned}((a + I) + (b + I)) + (c + I) &= ((a + b) + I) + (c + I) \\ &= ((a + b) + c) + I \\ &= (a + (b + c)) + I \\ &= (a + I) + ((b + c) + I) \\ &= (a + I) + ((b + I) + (c + I)).\end{aligned}$$

ii) A comutatividade para a adição:

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I \\ &= (b+a)+I \\ &= (b+I)+(a+I).\end{aligned}$$

iii) A existência de neutro na adição: seja 0_A o neutro em A. Percebe-se que

$$\begin{aligned}(a+I)+(0_A+I) &= (a+0_A)+I \\ &= a+I.\end{aligned}$$

Assim $0_A + I$ é o neutro para a adição em A/I.

iv) A existência de oposto na adição: seja $-a$ o oposto de a em A. Tome $(-a)+I$ em A/I.

$$\begin{aligned}(a+I)+((-a)+I) &= (a+(-a))+I \\ &= 0_A+I.\end{aligned}$$

E $(-a)+I$ é o oposto de $a+I$ em A/I.

v) A associatividade na multiplicação:

$$\begin{aligned}((a+I)(b+I))(c+I) &= ((ab)+I)(c+I) \\ &= ((ab)c)+I \\ &= (a(bc))+I \\ &= (a+I)((b+I)(c+I)).\end{aligned}$$

vi) A distributividade da multiplicação em relação a adição:

$$\begin{aligned}(a+I)((b+I)+(c+I)) &= (a+I)((b+c)+I) \\ &= (a(b+c))+I \\ &= (ab+ac)+I \\ &= ((ab)+I)+((ac)+I) \\ &= (a+I)(b+I)+(a+I)(c+I)\end{aligned}$$

e

$$\begin{aligned}((a+I)+(b+I))(c+I) &= ((a+b)+I)(c+I)\\ &= ((a+b)c)+I\\ &= (ac+bc)+I\\ &= ((ac)+I)+((b\ c)+I)\\ &= (a+I)(c+I)+(b+I)(c+I).\end{aligned}$$

Ainda, se A é comutativo, então A/I também é. De fato, $(a+I)(b+I) = (ab)+I = (ba)+I = (b+I)(a+I)$. Se A é anel com unidade, então A/I também tem unidade. De fato, seja 1_A a unidade em A. Toma-se 1_A+I em A/I e $(a+I)(1_A+I) = (a1_A)+I = a+I$.

3.4 HOMOMORFISMO DE ANÉIS

Depois de conhecer as estruturas e propriedades que um anel carrega, é importante entender como dois anéis diferentes se relacionam. O conceito de homomorfismo garante que comparações possam ser feitas sem que as estruturas sejam comprometidas. Também é a partir de homomorfismos que se pode construir ideais bastante importantes: os núcleos de homomorfismos, no teorema do homomorfismo.

Definição 3.4.1. *Sejam A e A' dois anéis. Uma função $\varphi : A \longrightarrow A'$ diz-se um homomorfismo de anéis se valem:*

i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

ii) $\varphi(ab) = \varphi(a)\varphi(b)$

para todos $a, b \in A$.

Definição 3.4.2. *Quando um homomorfismo de anéis é sobrejetor, diz-se um epimorfismo. Quando um homomorfismo de anéis é injetor, diz-se um monomorfismo. Quando um homomorfismo é injetor e sobrejetor, diz-se um isomorfismo. Se $\varphi : A \longrightarrow A'$ é um isomorfismo, por definição A e A' são chamados de isomorfos e notados por $A \cong A'$.*

Caso o homomorfismo φ seja de A em A, chama-se um *endomorfismo*. Caso o endomorfismo seja bijetor (injetor e sobrejetor), então chama-se de *automorfismo*.

Definição 3.4.3. *Seja $\varphi : A \longrightarrow A'$ um homomorfismo de anéis. Chama-se imagem de φ ao conjunto*

$$Im(\varphi) = \{f(a) \in A' \mid a \in A\}.$$

Definição 3.4.4. *Seja $\varphi : A \longrightarrow A'$ um homomorfismo de anéis. Chama-se núcleo ou kernel de φ ao conjunto*

$$Ker(\varphi) = \{a \in A | \varphi(a) = 0_{A'}\}.$$

Teorema 3.4.1. *$Ker(\varphi)$ é ideal bilateral de A.*

Demonstração. Sejam $a, b \in Ker(\varphi)$. Te-se que: $\varphi(a+b) = \varphi(a) + \varphi(b) = 0_{A'} + 0_{A'} = 0_{A'}$ de modo que $a+b \in Ker(\varphi)$. Ainda, seja $a' \in A$. $\varphi(a'a) = \varphi(a')\varphi(a) = \varphi(a')0_{A'} = 0_{A'}$. Logo $a'a \in Ker(\varphi)$. De modo análogo prova-se para *ideal à direita*. Assim as condições para ser um *ideal bilateral* de A foram satisfeitas.

□

Exemplo 3.4.1. *Para o próximo resultado faz-se necessário a definição da seguinte função:*

$$j : A \longrightarrow A/I$$

$$a \mapsto a + I.$$

É fácil verificar que j é epimorfismo, com efeito, dados $a, b \in A$.

$$j(a+b) = (a+b) + I = (a+I) + (b+I) = j(a) + j(b)$$

$$j(ab) = (ab) + I = (a+I)(b+I) = j(a)j(b).$$

A função j é sobrejetora, pois dado $a + I \in A/I$ existe $a \in A$ tal que $j(a) = a + I$. Ainda verifica-se que $j(0) = I$ (o elemento nulo do anel quociente) e caso A seja anel com unidade, então $j(1)$ é a unidade de A/I. Chama-se o epimorfismo j de *projeção canônica* .

Teorema 3.4.2. *(Teorema do homomorfismo) Sejam A e A' anéis, $\varphi : A \to A'$ um homomorfismo, j a projeção canônica de A no quociente $A/Ker(\varphi)$ e i a inclusão de $Im(\varphi)$ em A' que também é homomorfismo. Existe uma única função*

$$\varphi^* : A/Ker(\varphi) \to Im(\varphi)$$

tal que:

i) $\varphi = i \circ \varphi^* \circ j$.

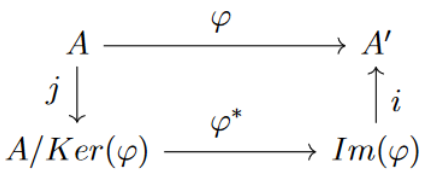
ii) φ^* é um isomorfismo.

A demonstração deste teorema, bem como a demonstração do seu equivalente para módulos, é muito semelhante à que será feita na seção sobre álgebras. Então, neste texto, decidiu-se fazer apenas aquela versão de demonstração.

O diagrama a seguir é uma representação das relações entre as funções.

Corolário: Se $\varphi : A \to A'$ é um epimorfismo de anéis, então $A/Ker(\varphi) \cong A'$. Basta perceber que se φ é sobrejetora, então $Im(\varphi) = A'$.

Figura 1 – Diagrama para o Teorema do Homomorfismo de Anéis.



Fonte: Elaborada pelo autor.

4 MÓDULOS

O conceito de *módulo* busca uma generalização da ideia de *espaço vetorial* ao considerar o *produto por escalar* em um *anel* ao invés de um *corpo*. Ao longo deste Capítulo, o anel R será sempre um anel com unidade (não necessariamente comutativo).

4.1 MÓDULOS

Definição 4.1.1. *Seja R um anel com unidade. Um grupo abeliano M é um R-módulo à esquerda caso seja dotado de uma multiplicação por escalar*

$$* : R \times M \longrightarrow M$$

$$(\alpha, m) \mapsto \alpha * m$$

tal que as seguintes propriedades sejam válidas:

Novamente $\alpha * m = \alpha m$.

i) $1_R m_1 = m_1$

ii) $(\alpha_1 \alpha_2) m_1 = \alpha_1 (\alpha_2 m_1)$

iii) $(\alpha_1 + \alpha_2) m_1 = \alpha_1 m_1 + \alpha_2 m_1$

iv) $\alpha_1 (m_1 + m_2) = \alpha_1 m_1 + \alpha_1 m_2$

para todos $\alpha_1, \alpha_2 \in R$ e $m_1, m_2 \in M$. De modo análogo define-se *módulo à direita*.

Neste trabalho serão considerados apenas os casos de *módulos à esquerda* de modo que a partir de agora o termo *módulo* se refere a um *módulo à esquerda*.

Nos casos em que $\mathbb{K}$ é um corpo, um $\mathbb{K}$-módulo é chamado de um $\mathbb{K}$-espaço vetorial.

Exemplo 4.1.1. *Todo anel R é um R-módulo. Neste contexto o R-módulo R será denotado por ${}_R R$.*

Exemplo 4.1.2. *Seja R um anel com unidade e $R^n = \{(r_1, r_2, \cdots, r_n) | r_i \in R\}$ para todo $i \in \mathbb{N}$, com soma e produto definidos de forma usual. R^n é um módulo sobre R.*

Exemplo 4.1.3. *O conjunto $M_n[R]$ das matrizes quadradas de ordem n com soma com entradas no anel R com unidade é um R-módulo se consideradas as operações usuais.*

Exemplo 4.1.4. *Todo grupo abeliano G pode ser considerado como um módulo sobre o anel $\mathbb{Z}$ dos números inteiros definindo o produto de um inteiro n por um elemento $h \in G$ por:*

$$nh = h + \cdots + h \text{ (n vezes) se } n > 0$$

$$nh = (-h) + \cdots + (-h) \text{ (/n/ vezes) se } n < 0$$

$$0_{\mathbb{Z}}h = 0_G.$$

4.2 SUBMÓDULOS

Definição 4.2.1. *Seja M um R-módulo. Um subconjunto não vazio $N \subset M$ diz-se um R-submódulo de M se:*

i) N é um subgrupo aditivo de M.

ii) N é fechado em relação à multiplicação por escalares, isto é, para todo $a \in R$ e todo $n \in N$, tem-se que $an \in N$.

Proposição 4.2.1. *Seja R um anel. Os R-submódulos de ${}_RR$ serão seus ideias à esquerda.*

Demonstração. Segue do fato que dado S um submódulo de ${}_RR$, por definição de submódulo, $S \subset {}_RR$, e $s - s' \in S$ para quaisquer $s, s' \in S$. Por fim, para qualquer $a \in {}_RR$, $as \in S$. As condições para que S seja ideal de R estão satisfeitas.

□

4.3 MÓDULO QUOCIENTE

Seja M um R-módulo e N um submódulo de M. De maneira semelhante ao anel quociente, é possível construir o módulo quociente onde $m + N = \{m + n | n \in N\}$. Para que o conjunto seja *R-módulo* basta considerar: $(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$ e definir uma multiplicação por escalares de R: ao par $(a, m + N) \in R \times M/N$ associa-se o elemento $am + N \in M/N$. A demonstração que as definições acima independem dos representantes utiliza o mesmo raciocínio que foi feito para anéis. Assim, M/N apresenta estrutura de R-módulo.

Definição 4.3.1. *O R-módulo M/N chama-se de módulo quociente de M pelo submódulo N.*

A verificação das propriedades *i*) e *iv*) da **Definição 4.3.1** é imediata a partir do fato de que M é R-módulo.

4.4 HOMOMORFISMO DE R-MÓDULOS

Sejam M e N dois R-módulos. Uma função $f : M \to N$ diz-se um *homomorfismo de R-módulos* ou um *R-homomorfismo* se para todo $m_1, m_2 \in M$ e todo $a \in R$ se verifica:

i) $f(m_1 + m_2) = f(m_1) + f(m_2)$

ii) $f(am_1) = af(m_1)$.

Os conceitos de *epimorfismo* e *monomorfismo* são semelhantes para os homomorfismos de anéis. Da mesma maneira quando o R-homomorfismo é injetor e sobrejetor ele é chamado de *isomorfismo*.

Dado um R-homomorfismo $f : M \to N$, chama-se *imagem* de f e *núcleo* ou *kernel* de f respectivamente aos conjuntos:

$$Im(f) = \{f(m)|m \in M\}$$

$$Ker(f) = \{m \in M|\ f(m) = 0_N\}.$$

Proposição 4.4.1. *Seja $f : M \longrightarrow N$ um R-homomorfismo. O conjunto $Ker(f)$ é um submódulo de M.*

Demonstração. Sejam $m_1, m_2 \in Ker(f)$. De fato, $m_1 - m_2 \in Ker(f)$, pois $f(m_1 - m_2) = f(m_1) - f(m_2) = 0_N$ e dado $a \in R$, $f(am_1) = af(m_1) = 0_N$, já que $a0_M = 0_M$ para todo a.

□

Teorema 4.4.1. *(Teorema do homomorfismo para módulos) Sejam M e N R-módulos, $f : M \to N$ um R-homomorfismo, $j : M \to M/Ker(f)$ a projeção canônica ao quociente e $i : Im(f) \to N$ a inclusão. Existe uma única função*

$$f^* : M/Ker(f) \to Im(f)$$

tal que:

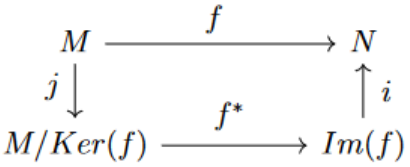
i) $f = i \circ f^* \circ j$.

ii) f^* é um isomorfismo.

A demonstração segue raciocínio utilizado no Teorema equivalente no próximo capítulo sobre álgebras.

O diagrama a seguir é uma representação das relações entre as funções.

Figura 2 – Diagrama para o Teorema do Homomorfismo de Módulos.



Fonte: Elaborada pelo autor.

5 ÁLGEBRAS

A primeira definição abstrata de álgebra – embora dependesse em parte, do conceito de coordenada – foi dada em 1903 por Leonard Eugene Dickson. Em 1923 uma definição puramente abstrata, livre de coordenadas, foi dada pelo próprio Dickson.(MILIES, 2004)

Ao longo do texto, R sempre será um anel comutativo com unidade.

5.1 ÁLGEBRAS

Definição 5.1.1. *Seja R um anel comutativo com unidade. Uma R-álgebra (ou álgebra sobre R) é um anel com unidade A que possui também estrutura de um R-módulo de modo que para todo $\alpha \in R$ e para todos $a,\ b \in A$ vale*

$$\alpha(ab) = (\alpha a)b = a(\alpha b).$$

No caso em que R é um corpo, a álgebra A é um R-espaço vetorial.

Definição 5.1.2. *Seja A uma R-álgebra. Diz-se que um subanel S de A é uma subálgebra de R se $\alpha a \in S$ para todos $\alpha \in R$ e $a \in S$.*

A definição acima também pode ser expressa da seguinte maneira: Seja A uma R-álgebra. A subálgebra S é um subanel de A que é também um R-submódulo.

5.2 ALGUNS EXEMPLOS DE ÁLGEBRAS

As álgebras são estruturas com bastante aplicações em diversas teorias algébricas. Neste texto serão apresentados exemplos de álgebra que comumente aparecem em artigos e livros de álgebra em nível de pós graduação.

Os primeiros exemplos são os numéricos. Qualquer corpo $\mathbb{K}$ pode ser visto como $\mathbb{K}$-álgebra, usando a multiplicação como operação interna e externa.

Da mesma forma, o R-módulo ${}_RR$ pode ser visto como uma R-álgebra, já que

$$\begin{aligned} \alpha(ab) &= (\alpha a)b \\ &= (a\alpha)b \\ &= a(\alpha b). \end{aligned}$$

5.2.1 Álgebras de Matrizes

Álgebras de matrizes são um dos principais exemplos de álgebras uma vez que muitas outras têm comportamento parecido (vide o teorema de Weddenburn-Artin em (MILIES, 1972)).

Neste texto, optou-se por definir o anel de matrizes sobre um corpo $\mathbb{K}$, mas é possível generalizá-lo usando um anel R como conjunto de escalares.

Seja $M_n[\mathbb{K}]$ o conjunto das matrizes quadradas de ordem n com coeficientes em $\mathbb{K}$, sendo $\mathbb{K}$ um corpo. Pode-se descrever uma matriz $A \in M_n[\mathbb{K}]$ por seus elementos fazendo $A = [a_{ij}]$.

Consideram-se as operações usuais de matrizes, ou seja, dados $A = [a_{ij}]$ e $B = [b_{ij}]$ tem-se que:

$$A + B = [a_{ij} + b_{ij}]$$

$$A \cdot B = [c_{ij}]$$

com

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}.$$

Proposição 5.2.1. *O conjunto das matrizes quadradas de ordem n com as operações definidas acima é um anel com unidade.*

Demonstração. Dados $A = [a_{ij}]$, $B = [b_{ij}]$ e $C = [c_{ij}]$ verificam-se

i) Associatividade para a adição:

$$\begin{aligned}(A + B) + C &= [a_{ij} + b_{ij}] + [c_{ij}] \\ &= [(a_{ij} + b_{ij}) + c_{ij}] \\ &= [a_{ij} + (b_{ij} + c_{ij})] \\ &= [a_{ij}] + [b_{ij} + c_{ij}] \\ &= A + (B + C).\end{aligned}$$

ii) Comutatividade para a adição:

$$\begin{aligned}A + B &= [a_{ij}] + [b_{ij}] \\ &= [a_{ij} + b_{ij}] \\ &= [b_{ij} + a_{ij}] \\ &= [b_{ij}] + [a_{ij}] \\ &= B + A.\end{aligned}$$

iii) Existência de neutro para a adição. Seja a matriz $E = [e_{ij}]$ tal que $e_{ij} = 0_{\mathbb{K}}$ para todos $i, j \in \mathbb{N}$:

$$\begin{aligned} A + E &= [a_{ij}] + [e_{ij}] \\ &= [a_{ij} + 0_{\mathbb{K}}] \\ &= [a_{ij}] \\ &= A. \end{aligned}$$

Ou seja, existe neutro para a adição que é E.

iv) A existência de oposto para a adição. Dada $A \in M_n[\mathbb{K}]$ existe $B \in M_n[\mathbb{K}]$ tal que $A + B = E$. De fato, para $A = [a_{ij}]$ toma-se $B = [-a_{ij}]$ e com isso:

$$\begin{aligned} A + B &= [a_{ij}] + [-a_{ij}] \\ &= [a_{ij} + (-a_{ij})] \\ &= [0_{\mathbb{K}}] \\ &= E. \end{aligned}$$

v) Associatividade para a multiplicação. Faz-se necessário considerar as seguintes relações:

$$[b_{ij}][c_{ij}] = [x_{ij}], \text{ com } x_{ij} = \sum_{t=1}^{n} b_{it}c_{tj}$$

$$[a_{ij}][x_{ij}] = [y_{ij}], \text{ com } y_{ij} = \sum_{k=1}^{n} a_{ik}x_{kj}$$

$$[a_{ij}][b_{ij}] = [z_{ij}], \text{ com } z_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

$$[z_{ij}][c_{ij}] = [w_{ij}], \text{ com } w_{ij} = \sum_{t=1}^{n} z_{it}c_{tj}$$

A partir das relações acima, deve-se ter $[y_{ij}] = [w_{ij}]$. De fato:

$$\begin{aligned} y_{ij} &= \sum_{k=1}^{n} a_{ik}x_{kj} \\ &= \sum_{k=1}^{n} a_{ik} \sum_{t=1}^{n} b_{kt}c_{tj} \\ &= \sum_{k=1}^{n} \sum_{t=1}^{n} a_{ik}(b_{kt}c_{tj}) \\ &= \sum_{t=1}^{n} \sum_{k=1}^{n} (a_{ik}b_{kt})c_{tj} \\ &= \sum_{t=1}^{n} z_{it}c_{tj} \\ &= w_{ij}. \end{aligned}$$

vi) A distributividade da multiplicação em relação a adição. Toma-se $[a_{ij}]([b_{ij}] + [c_{ij}]) = [x_{ij}]$, onde

$$\begin{aligned} x_{ij} &= \sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) \\ &= \sum_{k=1}^{n} (a_{ik}b_{kj} + a_{ik}c_{kj}) \\ &= \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1} a_{ik}c_{kj}. \end{aligned}$$

Por outro lado, $[a_{ij}][b_{ij}] + [a_{ij}][c_{ij}] = [y_{ij}] + [z_{ij}]$, em que $y_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$ e $z_{ij} = \sum_{k=1}^{n} a_{ik}c_{kj}$. Segue que $[y_{ij}] + [z_{ij}] = [x_{ij}]$ e portanto

$$[a_{ij}]([b_{ij}] + [c_{ij}]) = [a_{ij}][b_{ij}] + [a_{ij}][c_{ij}].$$

De maneira análoga, prova-se que $([a_{ij}] + [b_{ij}])[c_{ij}]$.

vii) O anel $M_n[\mathbb{K}]$ possui unidade: a matriz chamada *matriz identidade*

$$I = [\delta_{ij}] \text{ onde } \begin{cases} \mathrm{i}_{ij} = 1 \ se \ i = j \\ \mathrm{i}_{ij} = 0 \ se \ i \neq j \end{cases}$$

De fato, se $A = [a_{ij}]$ e $I = [\delta_{ij}]$ como definido anteriormente, então $AI = [c_{ij}]$ onde $c_{ij} = c_{ij} = \sum_{r=1}^{n} a_{ir}\delta_{rj}$.

Mas se $r \neq j$ então $\delta_{ij} = 0$ e, portanto, $c_{ij} = a_{ij}\delta_{jj} = a_{ij}1_{\mathbb{K}} = a_{ij}$. E assim, para todos $i, j \in \{1, \cdots, n\}$ $c_{ij} = a_{ij}$. Logo $AI = A$. De maneira análoga, prova-se que $IA = A$.

□

Perceba que a comutatividade não vale para o anel de matrizes quadradas de ordem n.

Veja o contraexemplo em $M_2[\mathbb{R}]$:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 4 & 10 \\ 10 & 24 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 14 & 20 \\ 10 & 14 \end{bmatrix}$$

Logo

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix} \neq \begin{bmatrix} 2 & 4 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$$

Para que $M_n[\mathbb{K}]$ seja um $\mathbb{K}$-espaço vetorial, define-se a multiplicação por escalar da forma:

$$\mathbb{K} \times M_n[\mathbb{K}] \longrightarrow M_n[\mathbb{K}]$$

$$(k, A) \mapsto kA = [ka_{ij}]$$

Com $k \in \mathbb{K}$ e $A \in M_n[\mathbb{K}]$.

Proposição 5.2.2. *O conjunto das matrizes quadradas de n é um $\mathbb{K}$-espaço vetorial com a multiplicação por escalar definida acima.*

Demonstração. Dados $k_1,\ k_2 \in \mathbb{K}$ e $A = [a_{ij}],\ B = [b_{ij}] \in M_n[\mathbb{K}]$. Verificam-se:

i) $1_{\mathbb{K}}A = A$.

$$\begin{aligned} 1_{\mathbb{K}}A &= 1_{\mathbb{K}}[a_{ij}] \\ &= [1_{\mathbb{K}}a_{ij}] \\ &= [a_{ij}] \\ &= A. \end{aligned}$$

ii) $(k_1k_2)A = k_1(k_2A)$.

$$\begin{aligned}(k_1k_2)A &= (k_1k_2)[a_{ij}] \\ &= k_1[k_2a_{ij}] \\ &= k_1(k_2A).\end{aligned}$$

iii) $(k_1 + k_2)A = k_1A + k_2A$.

$$\begin{aligned}(k_1 + k_2)A &= (k_1 + k_2)[a_{ij}] \\ &= ((k_1 + k_2)[a_{ij}]) \\ &= [k_1a_{ij}] + [k_2a_{ij}] \\ &= k_1[a_{ij}] + k_2[a_{ij}] \\ &= k_1A + k_2A.\end{aligned}$$

iv) $k(A + B) = kA + kB$.

$$\begin{aligned}k_1(A + B) &= k_1[a_{ij} + b_{ij}] \\ &= [k_1(a_{ij} + b_{ij})] \\ &= [k_1(a_{ij}) + k_1(b_{ij})] \\ &= k_1[a_{ij}] + k_1[b_{ij}] \\ &= k_1A + k_1B.\end{aligned}$$

□

Proposição 5.2.3. *$M_n[\mathbb{K}]$ tem estrutura de $\mathbb{K}$-álgebra.*

Demonstração. De fato verifica-se

$$\lambda(AB) = (\lambda A)B = A(\lambda B).$$

Dados $A,\ B \in M_n[\mathbb{K}]$ seja $AB = C$ ou $[a_{ij}][b_{ij}] = [c_{ij}]$ tal que $c_{ij} = \sum_{k=1}^{n}(a_{ik}b_{kj})$. Dado $\lambda \in \mathbb{K}$.

$$\lambda(AB) = \lambda C \ = \ \lambda[c_{ij}] = [\lambda c_{ij}].$$

De

$$\lambda C = [\lambda c_{ij}]$$

$$\begin{aligned}\left[\lambda\sum_{k=1}^{n}(a_{ik}b_{kj})\right] &= \left[\sum_{k=1}^{n}\lambda(a_{ik}b_{kj})\right] \\ &= \left[\sum_{k=1}^{n}(\lambda a_{ik})b_{kj}\right] \\ &= (\lambda A)B.\end{aligned}$$

Como

$$\sum_{k=1}^{n}\lambda(a_{ik}b_{kj}) = \sum_{k=1}^{n}a_{ik}(\lambda b_{kj}),$$

tem-se também $\lambda(AB) = A(\lambda B)$.
Logo, $M_n[\mathbb{K}]$ é uma $\mathbb{K}$-álgebra.

□

5.2.2 Álgebra de Polinômios Sobre um Anel

A partir das sequências de elementos de um anel comutativo com unidade R é possível construir o seguinte conjunto: se a_i indica a imagem do elemento genérico $n \in \mathbb{N}$ através da aplicação (sequência) f, tal sequência é indicada por

$$f = (a_0, a_1, a_2, \cdots, a_n, \cdots).$$

De forma simplificada, $f = (a_n)$, com $a_n \in R$ e $i \in \mathbb{N}$. Sejam $f = (a_n)$ e $g = (b_n)$, sequências de elementos de R. Veja que $f = g$ se, e somente se $a_n = b_n$ para todo $n \in \mathbb{N}$.

Definição 5.2.1. *Dado um anel A, uma sequência $(a_0, a_1, a_2, \cdots)$ sobre R é um polinômio caso exista um índice $r \in \mathbb{N}$ tal que $a_n = 0$ para todo $r \geq n$. $R[X]$ indicará o conjunto dos polinômios sobre R.*

O polinômio $X = (0_R, 1_R,)_R, \cdots)$ é chamado *indeterminada* de $R[X]$. Sua importância será apresentada posteriormente.

A soma de f com g será a sequência $h = (c_n)$ tal que $c_n = a_n + b_n$ para todo $n \in \mathbb{N}$. O produto de f com g será a sequência $h = (c_r)$ tal que

$$c_0 = a_0b_0$$

$$c_1 = a_0b_1 + a_1b_0$$

$$c_2 = a_0b_2 + a_1b_1 + a_2b_0$$

$$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$$

.....

$$c_r = a_0b_r + a_1b_{r-1} + a_2b_{r-2} + \cdots + a_rb_0$$

.....

Isso é, $c_r = \sum_{i=0}^{r} a_ib_{r-i}$ para cada $r \in \mathbb{N}$

Exemplo 5.2.1. *A sequência $f = (4, 3, 2, 1, 0, 0, \cdots, 0, \cdots)$, onde $a_n = 0$ para $n > 3$, é um polinômio sobre o anel $\mathbb{Z}$.*

Proposição 5.2.4. *A soma de dois polinômios é também um polinômio, ou seja, $R[X]$ é fechado para a adição.*

Demonstração. De fato, sejam $f = (a_i)$ e $g = (b_i)$ dois polinômios em R. Por definição, existe $r_0 \in \mathbb{N}$ tal que $a_i = 0$ para todo $i > r_0$ e existe também $r_1 \in \mathbb{N}$ tal que $b_i = 0$ para todo $i > r_1$. Toma-se $r = \text{máx}\{r_0, r_1\}$, então $a_i + b_i = 0$ para todo $i > r$. Assim, $f + g = (a_i + b_i)$ é um polinômio sobre R.

□

Proposição 5.2.5. *O produto de dois polinômios é também um polinômio, ou seja, $R[X]$ é fechado em relação a multiplicação.*

Demonstração. Sejam $f = (a_i)$ e $g = (b_j)$ dois polinômios sobre R. Por hipótese, existe $r_0 \in \mathbb{N}$ tal que $a_i = 0$ para todo $i \geq r_0$ e existe também $r_1 \in \mathbb{N}$ tal que $b_j = 0$ para todo $j \geq r_1$. Então o termo $c_{r_0+r_1+k}$ é tal que:

$$\begin{aligned} c_{r_0+r_1+k} &= \sum a_ib_{r_0+r_1+k-i} \\ &= a_0b_{r_0+r_1+k} + a_1b_{r_0+r_1+k-1} + \cdots \\ &\qquad + a_{r_0}b_{r_1+k-i} + a_{r_0+1}b_{r_1+k-1} + \cdots + a_{r_0+r_1+k}b_0 \end{aligned}$$

Como $b_{r_0+r_1+k} = b_{r_0+r_1+k-1} = \cdots = b_{r_1+k} = 0$ e $a_{r_0+r_1+k} = b_{r_0+r_1+k-1} = \cdots = b_{r_0+1} = 0$, decorre que $c_{r_0+r_1+k} = 0$.

□

Proposição 5.2.6. *$R[X]$ é um anel.*

Demonstração. Para todos $f, g, h \in R[X]$ e $i, m, k \in \mathbb{N}$ verificam-se:

i) Associatividade para a adição:

Sejam $f = (a_i)$, $g = (b_i)$, $h = (c_i)$, $(f+g)+h = (d_i)$ e $f+(g+h) = a_i+(e_i)$. Então

$$\begin{aligned}(d_i) &= (a_i + b_i) + (c_i)\\ &= ((a_i + b_i) + c_i)\\ &= (a_i + b_i + c_i)\\ &= ((a_i) + (b_i + c_i))\\ &= (a_i) + (b_i + c_i)\\ &= (e_i).\end{aligned}$$

ii) Comutatividade para a adição:

Sejam $f = (a_i)$ e $g = (b_i)$, $f + g = (c_i)$ e $g + f = (d_i)$. Então

$$\begin{aligned}(c_i) &= (a_i + b_i)\\ &= (b_i + a_i)\\ &= (d_i).\end{aligned}$$

iii) A existência de elemento neutro para adição. Sejam $e = (e_i)$ com $e_i = 0_R$ e $f = (a_i)$.

$$\begin{aligned}e + f &= (e_i) + (a_i)\\ &= (e_i + a_i)\\ &= (0_R + a_i)\\ &= (a_i)\\ &= f.\end{aligned}$$

Portanto e é o elemento neutro para adição de polinômios, chamado polinômio nulo.

iv) A existência de oposto para a adição. Sejam $f = (a_i)$ e $g = (-a_i)$.

$$\begin{aligned}f + g &= (a_i) + (-a_i)\\ &= (a_i + (-a_i))\\ &= (0_R)\\ &= e.\end{aligned}$$

v) A associatividade para a multiplicação:

Sejam $f = (a_i)$, $g = (b_j)$, $h = (c_k)$, $gh = (d_l)$, $f(gh) = (e_m)$, $(fg)h = (y_m)$ e $fg = (x_n)$.

Então

$$\begin{aligned}(e_m) &= \sum_{i+l=m}(a_i d_l)\\ &= \sum_{i+l=m}\left(a_i\left(\sum_{j+k=l} b_j c_k\right)\right)\\ &= \sum_{i+j+k=m}(a_i(b_j c_k))\end{aligned}$$

$$\begin{aligned}&= \sum_{i+j+k=m}(a_i b_j)(c_k)\\ &= \sum_{n+k=m}\left(\left(\sum_{ij=n} a_i b_j\right)c_k\right)\\ &= \sum_{n+k=m}(x_n c_k)\\ &= (y_m)\end{aligned}$$

vi) A distributividade da multiplicação em relação a adição:

Fazendo $f=(a_i)$, $g=(b_j)$, $h=(c_j)$, $f(g+h)=(d_k)$, $fg=(e_k)$ e $fh=(e'_k)$, tem-se

$$\begin{aligned}(d_k) &= \left(\sum_{j+i=k} a_i(b_j+c_j)\right)\\ &= \left(\sum_{j+i=k}(a_i b_j)+(a_i c_j)\right)\\ &= \left(\sum_{j+i=k} a_i b_j + \sum_{j+i=k} a_i c_j\right)\\ &= \left(\sum_{j+i=k} a_i b_j\right)+\left(\sum_{j+i=k} a_i c_j\right)\\ &= (e_k)+(e'_k).\end{aligned}$$

De forma análoga prova-se $(f+g)h = fh+fg$.

Dessa forma $R[X]$ é grupo abeliano para adição e a operação de multiplicação é associativa e distributiva em relação a adição.

□

Proposição 5.2.7. *$R[X]$ é anel comutativo.*

Demonstração. Sejam $f = (a_i)$ e $g = (b_j)$, $fg = (c_k)$ e $gf = (d_k)$. Tem-se que $c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i = d_k$, para todo $k \in \mathbb{N}$, assim $fg = gf$, para todo $f, g \in R[X]$ e $R[X]$ é comutativo.

□

Proposição 5.2.8. *$R[X]$ tem unidade.*

Demonstração. Veja que se 1_R é a unidade de R, tomando $e_R = (1_R, 0, 0, \cdots, 0, \cdots)$ a multiplicação como está definida garante que $fe_R = e_R f = f$, portanto $R[X]$ possui unidade e é a sequência (e_R).

□

A segunda condição que $R[X]$ deve ter para que seja álgebra é ser também um R-módulo. A multiplicação por escalar pode ser definida para o conjunto $R[X]$ utilizando-se da ideia de imersão de R em $R[X]$.

5.2.2.1 Imersão de R em $R[X]$

Apesar de R e $R[X]$ serem conjuntos com elementos de naturezas distintas, é possível supor, através de um isomorfismo, que $R \subset R[X]$.

Proposição 5.2.9. *Se R é um anel, então $L = \{(a, 0, 0, \cdots, 0, \cdots) | a \in R\}$ é um subanel de $R[X]$.*

Demonstração. Como $(0, 0, 0, 0, \cdots, 0, \cdots) \in R[X]$ o conjunto não é vazio e se $f = (a, 0, 0, \cdots, 0, \cdots) \in L$ e $g = (b, 0, 0, \cdots, 0, \cdots) \in L$, então

$$f + g = (a + b, 0, 0, \cdots, 0, \cdots) \in L$$

e

$$f \cdot g = (ab, 0, 0, \cdots, 0, \cdots) \in L.$$

□

Proposição 5.2.10. *Sendo R um anel, R é isomorfo ao subanel $L = \{(a, 0, 0, \cdots, 0, \cdots) | a \in R\}$ de $R[X]$*

Demonstração. Para a demonstração, define-se a aplicação

$$F : R \longrightarrow L$$

$$x \mapsto F(a) = (a, 0, 0, \cdots, 0, \cdots).$$

F é isomorfismo de anéis, pois valem as seguintes propriedades para todos $a, b \in RR$:

i) F é um homomorfismo:

$$\begin{aligned} F(a+b) &= (a+b,0,0,\cdots,0,\cdots) \\ &= (a,0,0,\cdots,0,\cdots)+(b,0,0,\cdots,0,\cdots) \\ &= F(a)+F(b). \end{aligned}$$

$$\begin{aligned} F(ab) &= (ab,0,0,\cdots,0,\cdots) \\ &= (a,0,0,\cdots,0,\cdots)(b,0,0,\cdots,0,\cdots) \\ &= F(a)F(b). \end{aligned}$$

ii) F é injetora. Dados $a,b \in A$ tais que $F(a) = F(b)$ e vale $F(a) = F(b) \Rightarrow (a,0,0,\cdots,0,\cdots) = (b,0,0,\cdots,0,\cdots) \Rightarrow a = b$.

iii) F é sobrejetora. Dados $(a,0,0,\cdots,0,\cdots) \in L$, é imediato que $(a,0,0,\cdots,0,\cdots) = F(a)$, portanto F é sobrejetora.

Conclui-se que F é um *isomorfismo*.

□

A partir do isomorfismo de R em L, identifica-se cada $a \in R$ ao polinômio $(a,0,0,\cdots,0,\cdots) \in L$. Em particular, $0 = (0,0,0,\cdots,0,\cdots)$ e $1 = (1,0,0,\cdots,0,\cdots)$ e, ainda, $R \cong L$, e portanto, por abuso de linguagem, $R \subset R[X]$.

Sejam $a \in R$ e $g = (b_0,b_1,b_2,\cdots,b_n,0,0,\cdots) \in R[X]$, define-se a seguinte multiplicação por escalar:

$$a \cdot g = (a,0,0,\cdots,0,\cdots)(b_0,b_1,b_2,\cdots,b_n,0,0,\cdots) = (ab_0,ab_1,ab_2,\cdots,ab_n,0,0,\cdots).$$

Proposição 5.2.11. *O conjunto $R[X]$ é um R-módulo com a multiplicação por escalar definida acima.*

Demonstração. Dados $f,g \in R[X]$ e $a_1,a_2 \in R$ verificam-se:

i) $1_R f = f$. Sejam $1_R = (1_R,0,0,\cdots,0,\cdots)$ e $f = (b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)$.

$$\begin{aligned} 1_R f &= (1_R,0,0,\cdots,0,\cdots)(b_0,b_1,b_2,\cdots,b_i,0,0,\cdots) \\ &= (1_R b_0, 1_R b_1, 1_R b_2,\cdots,1_R b_i,0,0,\cdots) \\ &= (b_0,b_1,b_2,\cdots,b_i,0,0,\cdots) \\ &= f. \end{aligned}$$

ii) $(a_1a_2)f = a_1(a_2f)$.

$$\begin{aligned}
(a_1a_2)f &= ((a_1,0,0,\cdots)(a_2,0,0,\cdots))(b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)\\
&= (a_1a_2,0,0,\cdots)(b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)\\
&= ((a_1a_2)b_0,(a_1a_2)b_1,(a_1a_2)b_2,\cdots,(a_1a_2)b_i,0,0,\cdots)\\
&= (a_1(a_2b_0),a_1(a_2b_1),a_1(a_2b_2),\cdots,(a_1(a_2)b_i,0,0,\cdots)\\
&= (a_1,0,0,\cdots)(a_2b_0,a_2b_1,a_2b_2,\cdots,a_2b_i,0,0,\cdots)\\
&= a_1(a_2f).
\end{aligned}$$

iii) $(a_1+a_2)f = a_1f + a_2f$.

$$\begin{aligned}
(a_1+a_2)f &= ((a_1,0,0,\cdots)+(a_2,0,0,\cdots)(b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)\\
&= (a_1+a_2,0,0,\cdots)(b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)\\
&= ((a_1+a_2)b_0,(a_1+a_2)b_1,(a_1+a_2)b_2,\cdots,(a_1+a_2)b_i,0,0,\cdots)\\
&= (a_1b_0+a_2b_0,a_1b_1+a_2b_1,a_1b_2+a_2b_2,\cdots,a_1b_i+a_2b_i,0,0,\cdots)\\
&= (a_1b_0,a_1b_1,a_1b_2,\cdots,a_1b_i,0,0,\cdots)+\\
&\qquad (a_2b_0,a_2b_1,a_2b_2,\cdots,a_2b_i,0,0,\cdots)\\
&= a_1f+a_2f.
\end{aligned}$$

iv) $a_1(f+g) = a_1f + a_1g$.

$$\begin{aligned}
a_1(f+g) &= (a_1,0,0,\cdots)((b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)+\\
&\qquad (c_0,c_1,c_2,\cdots,c_i,0,0,\cdots))\\
&= (a_1,0,0,\cdots)(b_0+c_0,b_1+c_1,b_2+c_2,\cdots,b_i+c_i,0,0,\cdots)\\
&= (a_1(b_0+c_0),a_1(b_1+c_1),a_1(b_2+c_2),\cdots,a_1(b_i+c_i),0,0,\cdots)\\
&= (a_1b_0+a_1c_0,a_1b_1+a_1c_1,a_1b_2+a_1c_2,\cdots,a_1b_i+a_1c_i,0,0,\cdots)\\
&= (a_1b_0,a_1b_1,a_1b_2,\cdots,a_1b_i,0,0,\cdots)+\\
&\qquad (a_1c_0,a_1c_1,a_1c_2,\cdots,a_1c_i,0,0,\cdots)\\
&= a_1f+a_1g.
\end{aligned}$$

Logo $R[X]$ é um R-módulo.

□

Proposição 5.2.12. *$R[X]$ é uma R-álgebra.*

Demonstração. Para $R[X]$ ser álgebra basta que $a(fg) = (af)g = f(ag)$ com $f, g \in R[X]$ e $a \in R$.

Sejam $a = (a, 0, 0, \cdots)$ $f = (b_0, b_1, b_2, \cdots, b_i, 0, 0, \cdots)$ e $g = (c_0, c_1, c_2, \cdots, c_j, 0, 0, \cdots)$.

$$\begin{aligned}
a(fg) &= (a,0,0,\cdots)((b_0,b_1,b_2,\cdots,b_i,0,0,\cdots)(c_0,c_1,c_2,\cdots,c_j,0,0,\cdots)) \\
&= (a,0,0,\cdots)(b_0c_0, b_0c_1+b_1c_0, b_0c_2+b_1c_1+b_2c_0, \\
&\qquad \cdots, b_0c_k+b_1c_{k-1}+b_2c_{k-2}+\cdots+b_kc_0, \cdots, 0) \\
&= (a(b_0c_0), a(b_0c_1+b_1c_0), a(b_0c_2+b_1c_1+b_2c_0), \cdots, \\
&\qquad a(b_0c_k+b_1c_{k-1}+b_2c_{k-2}+\cdots+b_kc_0), \cdots, 0) \\
&= ((ab_0)c_0, (ab_0)c_1+(ab_1)c_0, (ab_0)c_2+(ab_1)c_1+(ab_2)c_0, \cdots, \\
&\qquad (ab_0)c_k+(ab_1)c_{k-1}+(ab_2)c_{k-2}+\cdots+(ab_k)c_00, 0, \cdots) \\
&= (ab_0, ab_1, ab_2, \cdots, ab_i, 0, 0, \cdots)(c_0, c_1, c_2, \cdots, c_j, 0, 0, \cdots) \\
&= (af)g.
\end{aligned}$$

$$\begin{aligned}
a(fg) &= (a(b_0c_0), a(b_0c_1+b_1c_0), a(b_0c_2+b_1c_1+b_2c_0), \cdots, \\
&\qquad a(b_0c_k+b1c_{k-1}+b_2c_{k-2}+\cdots+b_kc_0), \cdots, 0) \\
&= (b_0(ac_0), b_0(ac_1)+b_1(ac_0), b_0(ac_2)+b_1(ac1)+b_2(ac_0), \cdots, \\
&\qquad b_0(ac_k)+b_1(ac_{k-1})+b_2(ac_{k-2})+\cdots+b_k(ac_0), \cdots, 0) \\
&= (b_0, b_1, b_2, \cdots, b_i, 0, 0, \cdots)(ac_0, ac_1, ac_2, \cdots, ac_j, 0, 0, \cdots) \\
&= (b_0, b_1, b_2, \cdots, b_i, 0, 0, \cdots)((a,0,0,\cdots)(c_0,c_1,c_2,\cdots,c_j,0,0,\cdots)) \\
&= f(ag).
\end{aligned}$$

Logo $R[X]$ é uma álgebra sobre R.

□

5.2.3 Notação usual dos polinômios

Por questões de praticidade, é possível representar os polinômios de uma outra maneira, de uma forma muito parecida com que se apresenta em Álgebra Elementar.

Na **Definição 5.2.1.**, foi apresentado que o polinômio

$$X = (0, 1, 0, 0, \cdots, 0, \cdots)$$

X que foi chamado de *indeterminada* sobre A. Pela definição do produto:

$$X^2 = X \cdot X = (0, 0, 1, 0, 0, \cdots, 0, \cdots)$$

$$X^3 = X^2 \cdot X = (0, 0, 0, 1, 0, \cdots, 0, \cdots).$$

De modo geral

$$X^n = (c_n) \text{ onde } c_n = \begin{cases} \mathrm{i}_{ij} = 1 \ se \ i = j \\ \mathrm{i}_{ij} = 0 \ se \ i \neq j \end{cases},$$

será um polinômio em que apenas $a_n \neq 0$ e $a_n = 1$.

Dado um polinômio $f = (a_0, a_1, a_2, \cdots, a_n, \cdots)$ em $R[X]$, é possível representar f da seguinte forma:

$$\begin{aligned} f &= (a_0, 0, 0, \cdots, 0, \cdots) + (0, a_1, 0, \cdots, 0, \cdots) + \\ &\qquad (0, 0, a_2, \cdots, 0, \cdots) + \cdots + (0, 0, 0, \cdots, a_n, \cdots) \\ &= a_0(1, 0, 0, \cdots, 0, \cdots) + a_1(0, 1, 0, \cdots, 0, \cdots) + \\ &\qquad a_2(0, 0, 1, \cdots, 0, \cdots) + \cdots + a_n(0, 0, 0, \cdots, 1, \cdots) \\ &= a_0 + a_1X + a_2X^2 + \cdots + a_nX^n. \end{aligned}$$

A notação $f = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ é dita *notação polinomial* justificando o uso da notação $R[X]$.

5.2.4 Álgebras de Grupo

Os anéis de grupo (e por consequência, as álgebras de grupo) são estruturas cujas construções aparecem frequentemente nos artigos e livros para servir de exemplo para casos mais gerais que os vistos até aqui.

A construção usa o conceito de somas formais, em que os elementos são "aglutinados", como faz-se na apresentação de polinômios. Apesar de ter-se construído o anel de polinômios de maneira formal no exemplos anterior, a apresentação mais comum não se importa em explicar o que significa $x+x^2$. Da mesma forma, dado um grupo $(G, \cdot)$, a construção de um espaço vetorial $\mathbb{K}G$ usando os elementos de G como base também não "explica"ou se importa com o significado de $g_1 + g_2$. Lembre que a operação que define G como grupo será denotada multiplicativamente.

É razoável imaginar que se G é finito com n elementos, como $\mathbb{K}$-espaço vetorial, $\mathbb{K}G$ é isomorfo a $\mathbb{K}^n$. E assim, mantendo uma maneira mais livre de denotar os elementos de $\mathbb{K}G$, será feita a construção da $\mathbb{K}$-álgebra sobre o grupo G como se segue:

Seja G um grupo e $\mathbb{K}$ um corpo.

Definição 5.2.2. *Denota-se por $\mathbb{K}G$ o conjunto de todas as combinações lineares da forma $\sum_i k_i g_i$ com $k_i \in \mathbb{K}$ e $g_i \in G$, onde os elementos k_i são todos nulos, a menos de um número finitos deles.*

$\mathbb{K}G$, com as operações:

$$\sum_i k_i g_i + \sum_i l_i g_i = \sum_i (k_i + l_i) g_i$$
$$\sum_i k_i . g_i \cdot \sum_j l_j \cdot g_j = \sum_{i,j} (k_i l_j)(g_i g_j)$$

Chamadas de adição e multiplicação respectivamente, é chamado anel do grupo G sobre $\mathbb{K}$.

Proposição 5.2.13. *$\mathbb{K}G$ tem estrutura de anel.*

Demonstração. Dados $k_i, l_i, r_i \in \mathbb{K}$ e $g_i \in G$, com $i, j, k \in \mathbb{N}$ verificam-se:

i) Associatividade para a adição:

$$\begin{aligned}
\left(\sum_i k_i g_i + \sum_i l_i g_i\right) + \sum_i r_i g_i &= \sum_i (k_i + l_i) g_i + \sum_i r_i g_i \\
&= \sum_i (k_i + l_i) + r_i g_i \\
&= \sum_i (k_i + l_i + r_i) g_i \\
&= \sum_i (k_i + (l_i + r_i)) g_i \\
&= \sum_i k_i g_i + \sum_i (l_i + r_i) g_i \\
&= \sum_i k_i g_i + \left(\sum_i l_i g_i + \sum_i r_i g_i\right).
\end{aligned}$$

ii) Comutatividade para a adição:

$$\begin{aligned}
\sum_i k_i g_i + \sum_i l_i g_i &= \sum_i (k_i + l_i) g_i \\
&= \sum_i (l_i + k_i) g_i \\
&= \sum_i l_i g_i + \sum_i k_i g_i.
\end{aligned}$$

iii) Existência de neutro para a adição. Deve existir $\sum_i l_i g_i$ tal que $\sum_i k_i g_i + \sum_i l_i g_i = \sum_i k_i g_i = \sum_i l_i g_i + \sum_i k_i g_i$. Tomando $\sum_i 0_{\mathbb{K}} g_i$ logo

$$\begin{aligned}
\sum_i k_i g_i + \sum_i 0_{\mathbb{K}} g_i &= \sum_i (k_i + 0_{\mathbb{K}}) g_i \\
&= \sum_i k_i g_i.
\end{aligned}$$

iv) Existência de oposto para a adição. Deve existir $\sum_i l_i g_i$ tal que $\sum_i k_i g_i + \sum_i l_i g_i = \sum_i 0_{\mathbb{K}} g_i$. Basta tomar $\sum_i -k_i g_i$,

$$\begin{aligned}\sum_i k_i g_i + \sum_i -k_i g_i &= \sum_i (k_i - k_i) g_i \\ &= \sum_i 0_{\mathbb{K}} g_i.\end{aligned}$$

Dados $k_i, l_j, r_k \in \mathbb{K}$ e $g_i, g_j, g_k \in G$, com $i, j, k \in \mathbb{N}$, verificam-se:

i) Associatividade para a multiplicação:

$$\begin{aligned}\left(\sum_i k_i g_i \sum_j l_j g_j\right) \sum_k r_k g_k &= \sum_{i,j} (k_i l_j)(g_i g_j) \sum_k r_k g_k \\ &= \sum_{i,j,k} ((k_i l_i) r_i)((g_i g_j) g_k) \\ &= \sum_{i,j,k} (k_i l_i r_i)(g_i g_j g_k) \\ &= \sum_{i,j,k} k_i (l_i r_i)(g_i (g_j g_k)) \\ &= \sum_i k_i g_i \sum_{j,k} (l_j r_k)(g_j g_k) \\ &= \sum_i k_i g_i \left(\sum_j l_j g_j \sum_k r_k g_k\right)\end{aligned}$$

ii) A distributividade da multiplicação em relação a adição, isso é

$$\left(\sum_i k_i g_i + \sum_j l_j g_j\right) \sum_k r_k g_k = \sum_i k_i g_i \sum_k r_k g_k + \sum_j l_j g_j \sum_k r_k g_k$$

e

$$\sum_i k_i g_i \left(\sum_j l_j g_j + \sum_k r_k g_k\right) = \sum_i k_i g_i \sum_j l_j g_j + \sum_i k_i g_i \sum_k r_k g_k.$$

Para a primeira condição:

$$\begin{aligned}(\sum_i k_i g_i + \sum_j l_j g_j)\sum_k r_k g_k &= \sum_{i,j}(k_i + l_j)(g_i g_j)\sum_k r_k g_k \\ &= \sum_{i,j,k}((k_i + l_j)r_k)(g_i g_j g_k) \\ &= \sum_{i,j,k}(k_i r_k) + (l_j r_k)(g_i g_j g_k) \\ &= \sum_{i,k}(k_i r_k)(g_i g_k) + \sum_{j,k}(l_j r_k)(g_j g_k) = \\ &= \sum_i k_i g_i \sum_k r_k g_k + \sum_j l_j g_j \sum_k r_k g_k.\end{aligned}$$

De maneira análoga prova-se a segunda condição.

□

Proposição 5.2.14. $\mathbb{K}G$ *é anel com unidade.*

Demonstração. Considere $1_{\mathbb{K}G} = \sum_i 1_{\mathbb{K}} g_i$.

$$1_{\mathbb{K}G}\sum_i k_i g_i = \sum_i 1_{\mathbb{K}} g_i \sum_i k_i g_i = \sum_i 1_{\mathbb{K}} k_i g_i = \sum_i k_i g_i.$$

□

Agora, $\mathbb{K}G$ será munido de uma operação que fará $\mathbb{K}G$ um $\mathbb{K}$-espaço vetorial.
Define-se a multiplicação por escalar da seguinte forma; dados $\alpha \in \mathbb{K}$ e $\sum_i k_i g_i \in \mathbb{K}G$:

$$\alpha\left(\sum_i k_i g_i\right) = \sum_i (\alpha k_i) g_i.$$

Proposição 5.2.15. $\mathbb{K}G$ *tem estrutura de* $\mathbb{K}$*-espaço vetorial com a multiplicação definida acima.*

Demonstração. Verificam-se:
Dados $k = \sum_i k_i g_i$ e $k = \sum_i l_i g_i \in \mathbb{K}G$ e $\alpha, \beta \in \mathbb{K}$.

i) $1_{\mathbb{K}} k = k$.

$$\begin{aligned}1_{\mathbb{K}}\left(\sum_i k_i g_i\right) &= \sum_i (1_{\mathbb{K}} k_i) g_i \\ &= \sum_i k_i g_i.\end{aligned}$$

ii) $\alpha(\beta k) = (\alpha\beta)k$. De fato,

$$\begin{aligned}
\alpha(\beta \sum_i k_i g_i) &= \alpha \sum_i (\beta k_i) g_i \\
&= \sum_i \alpha(\beta k_i) g_i \\
&= \sum_i (\alpha\beta k_i) g_i \\
&= \sum_i (\alpha\beta) k_i g_i \\
&= (\alpha\beta) \sum_i k_i g_i.
\end{aligned}$$

iii) Distributividade de um escalar em relação à soma de elementos em $\mathbb{K}G$. Isso é, $\alpha(k + l) = (\alpha k) + (\alpha l)$. Percebe-se que

$$\begin{aligned}
\alpha \left(\sum_i k_i g_i + \sum_i l_i g_i \right) &= \alpha \left(\sum_i k_i + l_i g_i \right) \\
&= \left(\sum_i (\alpha k_i + \alpha l_i) g_i \right) \\
&= \left(\sum_i (\alpha k_i) g_i \right) + \left(\sum_i (\alpha l_i) g_i \right) \\
&= \alpha \sum_i k_i g_i + \left(\alpha \sum_i l_i g_i \right).
\end{aligned}$$

iv) Distributividade da soma de escalares em relação a um vetor. Isso é, $(\alpha + \beta)k = (\alpha k) + (\beta k) = \alpha k + \beta k$

De modo que $\mathbb{K}G$ é um $\mathbb{K}$-espaço vetorial.

□

Proposição 5.2.16. *$\mathbb{K}G$ tem estrutura de $\mathbb{K}$-álgebra.*

Demonstração. De fato, com as notações da proposição acima.

$$\alpha \left(\sum_i k_i g_i \sum_i l_i g_i \right) = \left(\alpha . \sum_i k_i g_i \right) \sum_i l_i g_i = \sum_i k_i g_i \left(\alpha \sum_i l_i g_i \right).$$

Como $\alpha, k_i, l_j \in \mathbb{K}$ e $\mathbb{K}$ é corpo,

$$\alpha \left(\sum_i k_i g_i \sum_j l_j g_j \right) = \sum_{ij} \alpha(k_i l_j)(g_i g_j) = \sum_{ij} ((\alpha k_i) l_j)(g_i g_j) = \left(\sum_i \alpha k_i g_i \right) \sum_j l_j g_j.$$

Perceba que

$$\begin{aligned}\sum_{ij}\alpha(k_il_j)(g_ig_j) &= \sum_{ij}(k_i(\alpha l_j))(g_ig_j)\\ &= \sum_i k_ig_i\left(\sum_j \alpha l_jg_j\right)\\ &= \sum_i k_ig_i\left(\alpha\sum_j l_jg_j\right),\end{aligned}$$

de modo que o conjunto $\mathbb{K}G$ é uma $\mathbb{K}$-álgebra.

□

5.2.5 Álgebra End(M)

Seja R um anel com unidade e M um R-módulo. O conjunto de todos os endomorfismos de M, ou seja, $End_R(M) = \{f : M \to M \mid f \text{ é homomorfismo}\}$ definem-se as seguintes operações:

$$\begin{aligned} f+g : M &\to M\\ x &\mapsto (f+g)(x) = f(x)+g(x)\\ f\cdot g : M &\to M\\ x &\mapsto (f\cdot g)(x) = f(g(x))\end{aligned}$$

chamadas adição e multiplicação, respectivamente.

Proposição 5.2.17. *$End_R(M)$ tem estrutura de anel.*

Demonstração. Dados $f, g, h : M \longrightarrow M$ e $x \in M$ verificam-se:

i) Associatividade para a adição:

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

Para todo $x \in M$. Logo $(f+g)+h = f+(g+h)$.

ii) Comutatividade para a adição:

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

iii) Existência de elemento neutro para a adição. Tome $g : M \longrightarrow M$ tal que $x \mapsto O_M$:

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ &= f(x)+0_M\\ &= f(x).\end{aligned}$$

Denomina-se $g(x)$ de elemento neutro de $End_R(M)$.

iv) Existência de oposto. Dada $f \in End_R(M)(M)$ toma-se $g \in End_R(M)(M)$ tal que $g(x) = -f(x)$:

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ &= f(x)+(-f(x))\\ &= f(x+(-x))\\ &= f(0_M)\\ &= 0_M.\end{aligned}$$

v) Associatividade para a multiplicação:

$$\begin{aligned}((fg)h)(x) &= (fg(h(x))\\ &= (f(g(h(x)))\\ &= (f(gh(x)))\\ &= (f(gh)(x))\\ &= f(gh)(x).\end{aligned}$$

vi) Distributividade da multiplicação em relação a adição:

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

O mesmo vale para $(f(g+h))(x) = (fg)(x) + (fh)(x)$.

De modo que $End_R(M)$ é anel.

□

Proposição 5.2.18. *$End(M)$ é anel com unidade.*

Demonstração. Seja $I(x) = x$, $(fI)(x) = f(I(x)) = f(x)$, então $(fI)(x) = f(x)$. I é a unidade do anel $End_R(M)$.

□

Define-se a seguinte multiplicação por escalar:

$$\alpha f : R \times End_R(M) \to End_R(M)$$

$$(k, f) \mapsto (kf)(x) = f(kx).$$

Proposição 5.2.19. *$End_R(M)$ tem estrutura de R-módulo com a multiplicação por escalar definida acima.*

Demonstração. Para quaisquer $k \in R$ e $f \in End_R(M)$.

i)

$$\begin{aligned}(1_R f)(x) &= (f(1_R x)) \\ &= f(x).\end{aligned}$$

ii) Para cada $x \in M$, para todos $\gamma, \lambda \in A$ e $f, g \in End_R(M)(M)$.

$$\begin{aligned}((\lambda\gamma)f)(x) &= f((\lambda\gamma)x) \\ &= f(\lambda(\gamma x)) \\ &= \lambda f(\gamma x) \\ &= \lambda(\gamma(f(x))) \\ &= \lambda((\gamma f)(x))\end{aligned}$$

iii)

$$\begin{aligned}((\lambda+\gamma)f)(x) &= f((\lambda+\gamma)x) \\ &= f(\lambda x + \gamma x) \\ &= f(\lambda x) + f(\gamma x) \\ &= (\lambda f)(x) + (\gamma f)(x).\end{aligned}$$

iv)

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

□

Proposição 5.2.20. *$End_R(M)$ tem estrutura de R-álgebra.*

Demonstraçao. De fato, as funções $(\alpha f)g$, $\alpha(fg)$ e $f(\alpha g)$ são iguais.
Ora, sejam $\alpha \in A$, $f, g \in End_R(M)$ e $x \in M$. Então

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

e

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

De modo que $End_R(M)$ é uma R-álgebra a partir das operações definidas.

□

5.2.6 Álgebras de Caminhos

A próxima construção aparece como exemplos iniciais na *teoria de representação* através dos métodos diagramáticos. Esta técnica permite, por meio do *teorema de Gabriel*, identificar álgebras básicas com quocientes de álgebras de caminho. Não se busca neste texto a demonstração de tal teorema, mas apresentar ao leitor iniciante como construir uma álgebra usando grafos.

Para mais detalhes, o leitor interessado pode procurar informações em (CIBILIS; LARRIÓN; SALMERÓN, 1982) e (COELHO, 2000).

Definição 5.2.3. *Uma aljava Q é dada por dois conjuntos Q_0 e Q_1 e um par de funções $s, e : Q_1 \to Q_0$. Os elementos de Q_0 são chamados de vértices de Q enquanto os de Q_1 são as flechas de Q. Dada uma flecha $\alpha \in Q_1$, $s(\alpha)$ é o vértice inicial de α enquanto que $e(\alpha)$ é o vértice final de α.*

A partir dessa definição, é possível representar uma aljava de maneira pictórica.

Exemplo 5.2.2. *Se $Q_0 = \{3, 4\}$, $Q_1 = \{\lambda\}$, $s(\lambda) = 3$ e $e(\lambda) = 4$, representa-se da seguinte maneira:*

Figura 3 – Álgebra de Caminho.

$$3 \xrightarrow{\lambda} 4$$

Fonte: Elaborada pelo autor.

Definição 5.2.4. *Um caminho γ em $Q = (Q_0, Q_1, s, e)$, é descrito da seguinte forma: $\gamma = \alpha_n \cdots \alpha_1$ tal que para $1 \leq i \leq n-1$, $e(\alpha_i) = s(\alpha_{i+1})$.*

Definição 5.2.5. *O comprimento de γ será o seu número n de flechas e é denotado por $l(\gamma)$.*

Definição 5.2.6. *Um caminho trivial é um caminho sem flechas associado a um vértice $a \in Q_0$ e denotado por e_a. Ele representa a ideia de manter-se no lugar.*

Dado um caminho $\gamma = \alpha_n \cdots \alpha_1$, denota-se $s(\gamma) = s(\alpha_1)$ o *vértice inicial de* γ e por $e(\gamma) = e(\alpha_n)$ o *vértice final de* γ.

Definição 5.2.7. *Se $s(\gamma) = e(\gamma)$ e este não é um caminho trivial, então diz-se que γ é um caminho orientado.*

A notação é assim: $\gamma = (b|\alpha_n \cdots \alpha_1|a)$ para $\gamma = \alpha_n \cdots \alpha_1$ com $s(\gamma) = a$ e $e(\gamma) = b$. Um caminho trivial pode ser denotado por $(a||a)$.

Assumindo $\mathbb{K}$ um corpo e $Q = (Q_0, Q_1, s, e)$ uma aljava finita, isto é onde o conjuntos Q_0 e Q_1 são finitos, é possível a partir de $\mathbb{K}$ e Q definir uma álgebra $\mathbb{K}Q$. Seja B o conjunto formado por todos *os caminhos* de Q, incluindo os triviais. Considere agora $\mathbb{K}Q$ o $\mathbb{K}$-espaço vetorial com base B. B é chamada de base usual de $\mathbb{K}Q$.

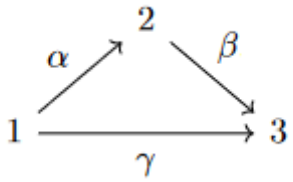
Para $\mathbb{K}Q$ ser uma álgebra, falta ainda definir uma multiplicação nos elementos da base. Dados dois caminhos de Q, $\gamma_1 = (b|\alpha_n \cdots \alpha_1|a)$ e $\gamma_2 = (d|\beta_m \cdots \beta_1|c)$ define-se:

$$\gamma_1 . \gamma_2 = \begin{cases} (\text{b}|\ \alpha_n \cdots \alpha_1 \beta_m \cdots \beta_1|c) & \text{se } a = d \\ 0_{\mathbb{K}Q} & \text{caso contrário.} \end{cases}$$

Estendendo por linearidade tal multiplicação a todos os seus elementos, define-se em $\mathbb{K}Q$ uma estrutura de $\mathbb{K}$-álgebra.

Exemplo 5.2.3. *Seja Q:*

Figura 4 – Álgebra de Caminho.



Fonte: Elaborada pelo autor.

Como espaço vetorial $\mathbb{K}Q$ tem como base $B = \{\epsilon_1, \epsilon_2, \epsilon_3, \alpha, \beta, \gamma, \beta\alpha\}$. A tabela de multiplicação dos elementos na base B é:

Quadro 1 – Quadro de multiplicação para a Álgebra de Caminhos.

	ϵ_1	ϵ_2	ϵ_3	α	β	γ	$\beta\alpha$
ϵ_1	ϵ_1	0	0	0	0	0	0
ϵ_2	0	ϵ_2	0	α	0	0	0
ϵ_3	0	0	ϵ_3	0	β	γ	$\beta\alpha$
α	α	0	0	0	0	0	0
β	0	β	0	$\beta\alpha$	0	0	0
γ	γ	0	0	0	0	0	0
$\beta\alpha$	$\beta\alpha$	0	0	0	0	0	0

Fonte: Elaborado pelo autor.

5.3 ÁLGEBRA QUOCIENTE

Os conceitos de *anel quociente* e *módulo quociente* podem ser estendidos a um conjunto quociente sobre uma álgebra. Perceba que já foi verificado que para um anel A, considerando sua estrutura de A-módulo, os ideais de A e os submódulos coincidem (**Exemplo 3.2.1**). Isto é um caso particular da seguinte proposição.

Proposição 5.3.1. *Se A é uma R-álgebra e se $I \subset A$ é um ideal bilateral de A, então I é também um R-sub módulo de A.*

Demonstração. De fato, se $\alpha \in R$ e $i \in I$, então $\alpha i = \alpha \cdot (1_A i) = (\alpha 1_A)i \in I$.

□

Assim, perceba que é possível, dado um ideal $I \subset A$, construir também um conceito de "álgebra quociente", já que o conjunto A/I conforme definido nos capítulos anteriores tem tanto estrutura de anel como de R-módulo, fazendo:

$$A/I \times A/I \longrightarrow A/I$$

$$(a+I, b+I) \mapsto (a+b)+I$$

$$A/I \times A/I \longrightarrow A/I$$

$$(a+I, b+I) \mapsto (a \cdot b)+I$$

$$R \times A/I \longrightarrow A/I$$

$$(\alpha, a+I) \mapsto (\alpha a)+I$$

Nas seções anteriores mostrou-se que essas operações estão bem definidas. Mas para que A/I seja uma R-álgebra, é preciso verificar que

$$\alpha[(a+I)(b+I)] = [\alpha(a+I)](b+I) = (a+I)[\alpha(b+I)].$$

Com efeito,

$$\begin{aligned} \alpha[(a+I)(b+I)] &= \alpha(ab+I) \\ &= \alpha(ab)+I \\ &= (\alpha a)b+I \\ &= (\alpha a+I)(b+I) \\ &= [\alpha(a+I)](b+I). \end{aligned}$$

Por outro lado, como A é uma R-álgebra, $\alpha(ab) = a(\alpha)b$ e portanto

$$\begin{aligned} \alpha[(a+I)(b+I)] &= \alpha[(ab+I)] \\ &= \alpha(ab)+I \\ &= (a+I)[\alpha(b+I)]. \end{aligned}$$

5.4 HOMOMORFISMOS DE ÁLGEBRAS

Definição 5.4.1. *Seja R um anel comutativo com unidade e sejam A e A' duas R-álgebras. Um homomorfismo de R-álgebra será um homomorfismo de anéis que também é um homomorfismo de módulos. Ou seja, para que $\varphi : A \longrightarrow A'$ seja um homomorfismo de álgebras deve-se verificar:*

i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

ii) $\varphi(ab) = \varphi(a)\varphi(b)$

iii) $\varphi(ka) = k\varphi(a)$

As definições para $Im(\varphi)$ e $Ker(\varphi)$ são as mesmas dadas em homomorfismos de anéis e módulos. O mesmo vale para as definições de *epimorfismo*, *monomorfismo* e *isomorfismo*.

Teorema 5.4.1. *(Teorema do homomorfismo para Álgebras) Sejam A e A' duas R-álgebras, $\varphi : A \to A'$ um homomorfismo, j a projeção canônica de A no quociente $A/Ker(\varphi)$ e i a inclusão de $Im(\varphi)$ em A'. Existe uma única função*

$$\varphi^* : A/Ker(\varphi) \to Im(\varphi)$$

tal que:

i) $\varphi = i \circ \varphi^* \circ j$.

ii) φ^* é um isomorfismo.

O diagrama a seguir é uma representação das relações entre as funções.

Figura 5 – Diagrama para o Teorema do Homomorfismo de Álgebras.

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ {\scriptstyle j}\downarrow & & \uparrow{\scriptstyle i} \\ A/Ker(\varphi) & \xrightarrow{\varphi^*} & Im(\varphi) \end{array}$$

Fonte: Elaborada pelo autor.

Demonstração. Para a demonstração define-se a seguinte função:

$$\varphi^* : A/Ker(\varphi) \to Im(\varphi)$$

$$a + Ker(\varphi) \mapsto \varphi(a).$$

A função φ^* deve estar bem definida, isso é, que independe do representante. Assim, dado um outro representante $a' \in a + Ker(\varphi)$ tem-se que $a' - a \in Ker(\varphi)$. Logo $\varphi(a - a') = \varphi(a) - \varphi(a') = 0$ de onde $\varphi(a) = \varphi(a')$ e φ^* está bem definida. A condição $i)$ vem direto de $i \circ \varphi^* \circ j(a) = i \circ \varphi^*(a + Ker(\varphi)) = i(\varphi(a)) = \varphi(a)$, para todo $a \in A$. De modo que $\varphi = i \circ \varphi^* \circ j$. Para provar que φ^* é isomorfismo, veja que:

i) φ^* é homomorfismo de álgebras. De fato,

$$\begin{aligned} \varphi^*((a + Ker(\varphi) + b + Ker(\varphi)) &= \varphi^*(a + b + Ker(\varphi)) \\ &= \varphi(a + b) \\ &= \varphi(a) + \varphi(b) \\ &= \varphi^*(a + Ker(\varphi)) + \varphi^*(b + Ker(\varphi)) \end{aligned}$$

e

$$\begin{aligned}\varphi^*((a+Ker(\varphi)(b+Ker(\varphi)) &= \varphi^*(ab+Ker(\varphi)) \\ &= \varphi(ab) \\ &= \varphi(a)\varphi(b) \\ &= \varphi^*(a+Ker(\varphi))\varphi^*(b+Ker(\varphi))\end{aligned}$$

e se $\alpha \in R$,

$$\begin{aligned}\alpha\varphi^*(a+Ker(\varphi)) &= \alpha\varphi(a) \\ &= \varphi(\alpha a) \\ &= \varphi^*(\alpha a+Ker(\varphi).\end{aligned}$$

ii) φ^* é sobrejetora. De fato, se $y \in Im(\varphi)$ então existe $a \in A$ tal que $\varphi(a) = y$. Como $\varphi(a) = \varphi^*(a + Ker(\varphi))$ então existe um elemento $a + Ker(\varphi) \in A/Ker(\varphi)$ tal que $\varphi^*(a + Ker(\varphi)) = y$.

iii) φ^* é injetora. De fato, dados $a+Ker(\varphi)$, $a'+Ker(\varphi)$ duas classes de $A/Ker(\varphi)$ tais que $\varphi^*(a + Ker(\varphi)) = \varphi^*(a' + Ker(\varphi))$. Da definição de φ^* vem que $\varphi(a) = \varphi(a')$, logo $\varphi(a - a') = 0$ e $a - a' \in Ker(\varphi)$, logo, $a + Ker(\varphi) = a' + Ker(\varphi)$.

□

Então como corolário fica demonstrado que se $\varphi : A \longrightarrow A'$ é um epimorfismo então $A/Ker(\varphi)$ é uma R-álgebra isomorfa à álgebra A'.

Esse resultado é fundamental na construção de muitos teoremas na teoria de anéis e álgebras. Com ele, por exemplo, se demonstra o de Gabriel, o de Wedderburn-Artin, entre outros.

6 CONCLUSÃO

O objetivo do trabalho foi alcançado, visto que foi possível definir a estrutura de Álgebra, apresentar exemplos interessantes e importantes para o assunto assim como estender alguns conceitos presentes em anéis e módulos. Vale ressaltar que o desenvolvimento do trabalho também permitiu o contato com estruturas algébricas que geralmente não são vistas em uma graduação em Licenciatura de Matemática.

Cada tipo de álgebra tem sua importância dependendo da área que está sendo trabalhada. A partir deste trabalho foi possível construir as partes fundamentais para um bom entendimento das suas definições e proposições. E desta forma, proporciona um bom guia para o estudos das estruturas de anel, módulo e álgebras.

REFERÊNCIAS

CIBILIS, C.; LARRIÓN, F.; SALMERÓN, L. **Métodos diagramáticos en teoría de representaciones**. México: Monografías del Instituto de Matemáticas, 1982.

COELHO, F. U. **Uma Introdução à Teoria de Representações de Álgebras**. Apostila (mini-curso escola de Álgebra). São Paulo: Instituto de Matemática e Estatística, Universidade de São Paulo, 2000.

DOMINGUES H. H.; IEZZI, G. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003.

MILIES, F. C. P. **ANÉIS E MÓDULOS**. São Paulo: Instituto de Matemática e Estatística, 1972.

MILIES, F. C. P. **Breve História da Álgebra Abstrata**. Apostila (mini-curso). Bahia: II Bienal da Sociedade Brasileira de Matemática, 2004.