Trabalho de Conclusão de Curso 1 - Bacharelado em Matemática

Álgebras e Identidades com Involução

Lucas Vasconcellos de Souza

Universidade Federal do ABC

Lucas Vasconcellos de Souza

Álgebras e Identidades com Involução

Trabalho Conclusão do Curso de Graduação em Bacharelado em Matemática da Universidade Federal do ABC como requisito para a obtenção do título de Bacharel em Matemática.

Orientador: Prof Dr. Alexandr Kornev

Santo André
2020

Sumário

Resumo

Pretendemos considerar os aspectos básicos da teoria de identidades em álgebras. Tais como identidades, variedades de álgebras, álgebras livres, etc... Construir seus análogos para álgebras com involução e estudar o teorema de Birkhoff neste caso.

Palavras Chaves: Involução, Teorema de Birkhoff, Variedades de Algebra

Abstract

We intend to consider the basic aspects of algebra identity theory. Such as identities, algebraic variety, free algebras, etc. Build such analogs for involution algebras and study Birkhoff's theorem in this case.

Keywords: Involution, Birkhoff's Theorem, Algebraic variety

1 Introdução

Alfred N. Whitehead, em seu livro A Treatise on Universal Algebra, de 1898, define que a álgebra universal é o estudo das estruturas algébricas por elas mesmo. Diferente da Álgebra Abstrata e a Teoria dos Modelos que estudavam exemplos de álgebras ou de estruturas algébricas.

Com a percepção de que certas estruturas algébricas não possuíam a propriedade associativa nas classes de operações multiplicativas, por exemplo com a álgebra de Lie na penúltima década do século XIX, foi preciso criar uma teoria que não apenas expandisse as estruturas já existentes de álgebras, mas de comparar diferentes estruturas. Assim, surge a álgebra universal.

O trabalho de Whitehead examinava e descrevia diferentes tipos de álgebras, como a álgebra de Grassmann, a álgebra booleana, e a álgebra dos quarteniões hiperbólicos de Hamilton.

Entretanto, Whitehead não fez muitos avanços significativos na área. E a área permaneceu estagnada até a década de trinta. Que agora com os avanços de Birkhoff e Ore, quando as definições básicas da álgebra universal começaram a ser formuladas, assim como a caracterização de variedades de álgebras e a formulação e prova do teorema de Birkhoff, ou também chamado de teorema HSP, diminutivo de Homomorfismo, Subálgebra e Produto.

Tal teorema teve um impacto significativo na área por sua caracterização e identificação de variedades de álgebras. Uma das consequências, por exemplo foi de mostrar que os axiomas de um corpo não formavam uma variedade de álgebra. Tal fato decorre do produto de dois corpos não formam um corpo, logo, pelo teorema HSP, não forma uma variedade.

2 Conceitos Preliminares

Começaremos com os conceitos mais básicos em álgebra abstrata.

2.1 Grupos

2.1.1 Noção intuitiva de grupos

Podemos extrair a noção geral do que um grupo é através de, por exemplo, o conjunto dos números inteiros.

Exemplo 2.1 *Seja o conjunto $\mathbb{Z}$ e seja a operação de adição, podemos extrair algumas propriedades básicas com esta operação. A começar, podemos ver que, para quaisquer x, y, $z \in \mathbb{Z}$:*

$$\begin{aligned} &i.\ (x \in \mathbb{Z}) \wedge (y \in \mathbb{Z}) \rightarrow (x+y) \in \mathbb{Z} \\ &ii.\ x+(y+z) = (x+y)+z \\ &iii.\ \forall x \in \mathbb{Z}, x+0 = x \\ &iv.\ \forall x \in \mathbb{Z}, x+(-x) = 0 \end{aligned} \tag{2.1}$$

Tais propriedades formam o conjunto de axiomas que definem um grupo. Um grupo é composto por um conjunto e uma operação binária. Para definirmos mais precisamente o que é um grupo, iremos definir e fazer algumas considerações sobre operações binárias.

2.1.2 Operações binárias

Definição 2.2 (Par ordenado) *Sejam a, b dois objetos quaisquer, diremos que o **par ordenado** de a,b, denotado por (a,b) é uma lista de objetos que contém os dois elementos a, b em que a ordem que aparecem os objetos importa, com a seguinte propriedade: $(a,b) = (c,d)$ se, e somente se, $a = c, b = d$. Uma n-upla ordenada é uma lista de n elementos em que a posição de todos os n na lista importam.*

Definição 2.3 (Produto cartesiano) *Sejam A, B não vazios, definimos* ***produto cartesiano*** *como o conjunto de pares ordenados (a,b) de todas as combinações de elementos onde* $a \in A, b \in B$. *Denotamos o produto cartesiano de A,B por* $A \times B$.

Definição 2.4 (Relação binária) *Sejam* A, B *dois conjuntos quaisquer não vazios, e* $A \times B$ *o produto cartesiano entre eles. Uma* ***relação binária*** R *é um subconjunto de* $A \times B$. *Onde A é chamado de domínio, enquanto B é chamado de contradomínio. Quando* (a, b) *é um elemento de R, diremos que a é R-relacionado por b, e denotaremos como aRb.*

Definição 2.5 (Função) *Sejam* A, B *conjuntos não vazios quaisquer, e* f *uma relação binária.* f *será uma função se satisfazer essas duas condições:*

i. $\forall a \in A, \forall b, c \in B((a, b) \in f \land (a, c) \in f) \implies b = c$.
ii. $\forall a \in A, \exists b \in B, (a, b) \in f$.

Denotaremos esta função f no cartesiano $A \times B$ como $f : A \to B$.

Definição 2.6 (Operação binária) *Uma operação binária é uma função* $f : A \times A \to A$ *que mapeia um elemento* (a, b) *do produto cartesiano* $A \times A$ *para dentro do próprio conjunto A. Denotaremos uma operação binária* $f(a, b)$ *como* $a \star b$ *ou* $a * b$, *onde* $\star, *$ *denota o tipo de função definida na operação binária. Para termos uma operação binária em A, necessariamente* $a \star b = c, c \in A$

Operações binárias podem ser **comutativas**, isto é, $f(a, b) = f(b, a) = a \star b = b \star a$. Dentre os exemplos mais comuns estão as operações binárias de soma e multiplicação.

Um dos exemplos mais intuitivos de pensar em uma operação binária não comutativa é pegar uma família não vazia de funções $f_i : A \to A$ e munir da operação binária $\circ$ definida como $(f \circ g)(a) = f(g(a))$. Dada duas funções arbitrárias $f_1, f_2 \in \{f_i\}_{i \in I}$, temos que não é sempre verdade que $(f_1 \circ f_2)(a) = (f_2 \circ f_1)(a)$.

Por exemplo, as funções definidas nos reais para os reais $f_1(x) = x^2, f_2(x) = x + 1$, temos que $(f_1 \circ f_2)(x) = (x + 1)^2$ e $(f_2 \circ f_1)(x) = x^2 + 1$.

Quando uma operação binária $\star$ tem a seguinte propriedade $a \star b = -b \star a$(para conjuntos onde faça sentido falar de elementos negativos), diremos que a operação é **anticomutativa**.

Operações binárias podem ser **associativas**. Isto é, dada uma operação binária $\star$ num conjunto A, temos um problema que é o de determinar se a ordem com que realizamos as operações importa.

Isto é, sejam $a, b, c \in A$ munidos da operação $\star$, precisamos decidir se $a \star (b \star c) = (a \star b) \star c$. Precisamos decidir se primeiro operarmos o par $b \star c$ e depois pegarmos o resultado deste e operarmos com a terá o mesmo resultado de primeiro operarmos $a \star b$ e depois pegarmos este resultado e operar com c, quando temos que as duas formas dão o mesmo resultado, então a operação é associativa e podemos representar $a \star (b \star c) = (a \star b) \star c$ simplesmente como $a \star b \star c$.

Um dos exemplos mais básicos que podemos ver de uma operação não associativa, é a operação binária de exponenciação $a \star b = a^b$. Ela não associativa, pois $a \star (b \star c) = a^{b^c}$ enquanto $(a \star b) \star c = (a^b)^c = a^{bc}$.

Um exemplo extremamente importante de uma operação não associativa é a operação chamada de **comutador de lie**, veremos com maior atenção no capitulo referente a álgebras.

Por último, podemos definir uma operação binária exterior. Isto é, as operações binárias usuais são definidas como uma função do produto cartesiano $A \times A$ para A. Uma operação exterior é uma operação que, dado um conjunto não vazio B, de forma que o domínio da função será cartesiano $B \times A$ (ou $A \times B$) e a imagem será o próprio conjunto A.

Esta é apenas uma lista breve de algumas propriedades de operações binárias. Mais algumas propriedades serão apresentadas no Capitulo 4.

2.1.3 Definição axiomática de grupos

Definição 2.7 (definição de grupo) *Definimos um grupo G como um conjunto não-vazio qualquer $\mathbb{G}$ e um operação binária $\star$ onde os seguintes axiomas são respeitados:*

i. $\forall (x, y, z \in \mathbb{G}) \ : \ x \star (y \star z) = (x \star y) \star z$ ***(Associatividade)***
ii. $(\forall x \in \mathbb{G})(\exists e \in \mathbb{G}) \ : \ a \star e = a = e \star a$ ***(Existência de elemento neutro)***
iii. $(\forall x \in \mathbb{G})(\exists a' \in \mathbb{G}) \ : \ a \star a' = e = a' \star a$ ***(Existência de elemento inverso)***

Adicionalmente (apesar de não ser necessário), podemos adicionar uma propriedade chamada de comutativa(ou abeliana):
$(\forall x, y \in \mathbb{G}) : x \star y = y \star x$ ***(Comutatividade)***

2.1.4 Exemplos de grupos

Nesta seção iremos apresentar dois exemplos de grupos.

Exemplo 2.8 *Denotamos como $\mathbb{G}_1$ o conjunto formado por: $\mathbb{G}_1 = \{1, -1, i, -i\}$. Onde $i = \sqrt{-1}$. A operação do grupo é definida como a operação de multiplicação usual dos números complexos. Dado os quatro axiomas acima mencionados com a operação de multiplicação, teremos um grupo.*

O próximos exemplo irá envolver a operação de composição de funções.

Exemplo 2.9 *Seja o conjunto $\mathbb{M}$ de 5 elementos, um exemplo de permutação s é:*

$$s = \begin{pmatrix} a & b & c & d & f \\ b & c & d & f & a \end{pmatrix} \qquad \text{(permutação)}$$

O grupo de permutações, definimos então, como um conjunto de funções bijetoras de $\mathbb{M}$ para ele mesmo com a operação de grupos sendo a composição de funções .

Assim, podemos satisfazer os quatro axiomas do grupo, dado o conjunto $\mathbb{M} = a, b, c, d, f$:

$$\begin{aligned} s &= \begin{pmatrix} a & b & c & d & f \\ b & c & d & f & a \end{pmatrix} \\ t &= \begin{pmatrix} a & b & c & d & f \\ b & d & a & c & f \end{pmatrix} \\ t(s(m)) = ts &= \begin{pmatrix} a & b & c & d & f \\ d & a & c & f & b \end{pmatrix} \end{aligned} \tag{2.2}$$

$$s(tu) = (st)u \tag{2.3}$$

$$I = \begin{pmatrix} a & b & c & d & f \\ a & b & c & d & f \end{pmatrix} \tag{2.4}$$

$$s^{-1}s = I \tag{2.5}$$

Por exemplo, a permutação u é o inverso de s:

$$\begin{aligned} s &= \begin{pmatrix} a & b & c & d & f \\ b & c & d & f & a \end{pmatrix} \\ u &= \begin{pmatrix} a & b & c & d & f \\ f & a & b & a & d \end{pmatrix} \qquad \text{(elemento inverso de s)} \\ su = I &= \begin{pmatrix} a & b & c & d & f \\ a & b & c & d & f \end{pmatrix} \end{aligned}$$

2.2 Anéis

2.2.1 Noção intuitiva de anéis

Consideremos um polinômio qualquer, com coeficientes a_i reais, $a = a_0 + a_1x + a_2x^2 + ... + a_nx^n$. Poderíamos pegar outros dois polinômios, $b = b_0 + b_1x + b_2x^2 + ... + b_nx^n$, $c = c_0 + c_1x + c_2x^2 + ... + c_nx^n$ e estabelecer algumas regras.

Temos um grupo em respeito a operação de adição. Isto é, temos que dada a operação de adição bem definida, então:
i. $a + (b + c) = (a + b) + c$
ii. $a + 0 = a$
iii. $a - a = 0$

Temos uma operação bem definida, chamada de multiplicação, que tem as seguintes propriedades:
i. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
ii. $a * 1 = a$

Temos certas identidades em relação a interação entre a adição e multiplicação:
i. $a \cdot (b + c) = a \cdot b + a \cdot c$
ii. $(a + b) \cdot c = a \cdot c + b \cdot c$

Teríamos também a comutatividade em relação a adição, e em relação a multiplicação. Em relação ao primeiro, nós dizemos que o grupo em relação a adição é comutativo.

Apesar de um anel em geral não ser comutativo em relação a multiplicação, uma operação envolvendo polinômios nos dá um ótima ideia do que seria um anel. Por exemplo, não temos, necessariamente, um inverso multiplicativo para todos os elementos do anel.

2.2.2 Definição de um anel e exemplos

Definição 2.10 (Definição de um anel) *Seja um ϕ conjunto não vazio munido com duas operações binárias $+, .$, então $(\phi, +, .)$ será um anel se:*
i. ϕ *é um grupo abeliano sobre a adição.*
ii. $\forall a,\ b,\ c \in \phi, (a . b) . c = a . (b . c)$
iii. $\forall a \in \phi, \exists 1$ *tal que* $a . 1 = 1 . a = a$
iv.$\forall a, b, c \in \phi, a . (b + c) = a . b + a . c.$
v. $\forall a, b, c \in \phi, (b + c) . a = b . a + c . a$

Dentre os exemplos mais conhecidos e interessantes está o anel das pelas classes de congruência módulo n. Iremos construir da seguinte forma:

Considere o conjunto dos números inteiros $\mathbb{Z}$. Seja n um inteiro maior que 1.Dois inteiros x,y serão ditos **congruentes módulo n** , se $x - y = kn$ para algum inteiro k. Denotaremos a congruência de dois elementos x, y módulo n por $x \equiv y(mod n)$

A congruência módulo n é uma relação de equivalência. Isto é, é simétrica, reflexiva e transitiva.

Com as operações usuais de soma e multiplicação nos inteiros, a relação de congruência módulo n é compatível com as operações. Isto é:

$$a \equiv b(mod n) \implies a + x \equiv b + x(mod n), \forall x \in \mathbb{Z}$$

$$a \equiv b(mod n) \implies ax \equiv bx(mod n), \forall x \in \mathbb{Z}$$

De forma mais sucinta, definiremos uma relação de congruência de forma:

Definição 2.11 (Congruência) *Seja A um conjunto com operações binárias definidas neste conjunto. Um subconjunto $A/\backsim$ do produto direto $A \times A$ será uma relação de*

congruência de A se:
i. $\backsim$ *é uma relação de equivalência de A.*
ii. As operações do conjunto A estão bem definidas no subconjunto A/ $\backsim$ *e satisfazem todas as propriedades que o conjunto A satisfaz.*

Exemplo 2.12 *Seja* $\mathbb{Z}$ *o anel dos inteiros com as operações de soma e multiplicação usuais. Considere n=4 e para todos os elementos deste conjunto, vamos aplicar a congruência módulo 4. Assim, pela congruência módulo 4 ser uma relação de equivalência, temos que teremos classes de equivalência módulo 4. Tais classes de equivalência serão os elementos inteiros advindos do resto da divisão por 4 e serão o conjunto* $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. *Temos que as operações são compatíveis com este conjunto.*

Assim, um exemplo de anel finito é o anel $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ com as operações de soma e multiplicação definidas no anel dos inteiros.

De forma mais geral, podemos extender este conceito para qualquer inteiro n e obter um anel finito formado pelas classes de congruência módulo n. Tal anel será denotado por $\mathbb{Z}/n\mathbb{N}$.

Notemos que o $\mathbb{Z}/4\mathbb{Z}$ não tem um inverso multiplicativo para todos os elementos, neste caso, o elemento $2 \in \mathbb{Z}/4\mathbb{Z}$. Caso peguemos o 2 e o multiplicarmos por ele mesmo, obteremos o representante de classe 4, que neste anel o elemento pertence a classe de congruência de 0. Temos assim um divisor por zero.

Definição 2.13 *Divisor de zero. Seja* ϕ *um anel bem definido. O elemento a será chamado de divisor de zero à direita de um anel se* $ax = 0, x \in \phi, x \neq 0$. *Um elemento b será chamado de divisor de zero à esquerda, se* $xb = 0, x \in \phi, x \neq 0$. *Se ele é tanto divisor de zero à direita quanto à esquerda, então chamamos de divisor de zero.*

Outra propriedade que o anel $\mathbb{Z}/4\mathbb{Z}$ têm é a existência de um elemento nilpotente.

Definição 2.14 (Elemento nilpotente) *Seja* ϕ *um anel. Um elemento* $a \in \phi$ *será chamado de nilpotente se ele for diferente de 0 e para algum inteiro n, temos que* $a^n = 0$

Considere agora o anel $\mathbb{Z}/6\mathbb{Z}$, formado pelas classes de congruência $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Vamos pegar um elemento $n \in \mathbb{Z}/6\mathbb{Z}$ e encontrar n^2. Temos que: $0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 9 = \bar{3},\ 4^2 = 16 = \bar{4}, 5^2 = 25 = \bar{1}$.

Observamos que, no anel $\mathbb{Z}/6\mathbb{Z}$, temos 4 elementos que multiplicados por ele mesmo, nos dá o próprio elemento. Assim.

Definição 2.15 (Elemento idempotente) *Seja ϕ um anel, e $a \in \phi$. O elemento a será chamado de idempotente se $a^2 = a$*

2.3 Corpos

2.3.1 Noção intuitiva de corpos

Assim como os grupos, podemos extrair a noção geral de corpos, olhando para um conjunto. Desta vez, o conjunto dos $\mathbb{R}$. Através deste conjunto, e usando as operações + e ×, podemos extrair as seguintes propriedades, para quaisquer x, y, z $\in \mathbb{R}$

$i.\ (x \in \mathbb{R}) \wedge (y \in \mathbb{R}) \rightarrow (x + y) \in \mathbb{R}$
$ii.\ x + (y + z) = (x + y) + z$
$iii.\ \forall x \in \mathbb{R}, a + e = a$
$iv.\ \forall x \in \mathbb{R}, a + (-a) = e$
$v.\ \forall x, y \in \mathbb{R}, x + y = y + x$
$vi.\ (x \in \mathbb{R}) \wedge (y \in \mathbb{R}) \rightarrow (x \times y) \in \mathbb{R}$ (propriedades dos números reais)
$vii.\ x \times (y \times z) = (x \times y) \times z$
$viii.\ \forall x \in \mathbb{R}, a \times 1 = a$
$ix.\ \forall x \in \mathbb{R} \setminus \{0\}, a \times (1/a) = 1$
$x.\ \forall x, y \in \mathbb{R}, x \times y = y \times x$
$xi.\ \forall x, y, z \in \mathbb{R}, x \times (y + z) = x \times y + x \times z$

Tais propriedades denotam a definição de um corpo, no caso especifico temos o corpo dos reais. Na próxima seção, veremos uma definição mais abstrata e exemplos usando outros conjuntos e conjuntos finitos.

2.3.2 Definição axiomática de um corpo

Definição 2.16 (Definição axiomática de corpo) *Dado um conjunto K com as operações binárias +,-, K será corpo se:*

$$i.\forall x,y \in K : (x \in K) \wedge (y \in G) \rightarrow (x+y) \in K \wedge (x \times y) \in K$$
(Fechamento da operação binária em um conjunto)

$$ii.\forall x,y,z \in K : (x+(y+z) = (x+y)+z) \wedge (x \times (y \times z) = (x \times y) \times z)$$ (Lei da Associatividade)

$$iii.\exists 0 \in K, \forall x \in K \in \mathbb{K} : a+0 = a = 0+a$$ (Existência de um elemento neutro aditivo)

$$iv.\forall x \in K, \exists -a \in K : a + -a = 0$$ (Existência de um elemento inverso)

$$v\forall x,y \in K : (x+y = y+x) \wedge (x \times y = y \times x)$$ (Comutatividade)

$$vi.\forall x \in K, \exists 1 \in \mathbb{K} : a \times 1 = a$$ (existência de um elemento neutro multiplicativo)

$$vii.\exists a' \in K, \forall x \in K : a \times a' = 1 = a' \times a$$ (Existência de um elemento simétrico)

$$viii.\forall x,y,z \in R, x \times (y+z) = x \times y + x \times z$$ (Distributividade)

Como vimos na subseção anterior, temos que os reais formam um corpo com as operações usuais de soma e multiplicação. Podemos também citar os números complexos, e os racionais. Os números inteiros não formam um corpo por faltar a existência de um elemento simétrico.

De forma semelhante à construção de um anel finito através de classes de congruência gerada por módulo n, podemos fazer a mesma construção e gerar um corpo finito. Entretanto, pelos axiomas acima que definem um corpo, temos que um corpo

não tem divisor por zero, elementos nilpotentes e os únicos elementos idempotentes de um corpo são 0 e 1. Assim, as únicas construções possíveis de um corpo finito gerado por classes de congruência módulo n são aqueles em que n é um número primo. Uma explicação para tal fato está em

2.4 Espaço vetorial

2.4.1 Noção intuitiva de espaço vetorial

Peguemos um corpo qualquer. Por exemplo o corpo $\mathbb{R}$. Iremos construir um produto cartesiano $\mathbb{R} \times \mathbb{R}$ de forma que podemos somar elementos e multiplicar entre eles. Isto é, sejam dois elementos do produto cartesiano $\mathbb{R} \times \mathbb{R}$ denotados por (a,b) e (c,d), podemos somar eles de forma que (a,b) + (c,d) se torne um terceiro elemento elemento dentro do produto cartesiano que tem a forma de (a+c, b+d).

Também podemos ver que tal construção também tem uma noção de "tamanho", por exemplo, se somarmos dois pares ordenados iguais (a,b)+(a,b), é o mesmo que dizer que (a,b)+(a,b)=(a+a, b+b)=2*(a,b)=(2a,2b). Generalizando isso, podemos estender isso para qualquer número de forma que $\lambda(a,b) = (\lambda a, \lambda b)$. Veja que essa construção não consegue definir algumas expressões como (a,b) + c, onde $(a,b) \in \mathbb{R}X\mathbb{R}$ e $c \in \mathbb{R}$. Assim como a multiplicação de vetores por vetores.

Tal construção acima é um dos exemplos mais intuitivos e naturais de pensar em um espaço vetorial.

2.4.2 Definição axiomática de espaço vetorial e exemplos

Definição 2.17 *Seja K um corpo, e V um conjunto não vazio. Diremos que V é um K-espaço vetorial (ou espaço vetorial sobre K) se dada duas operações binárias $+, .$ em V e uma operação binária externa $*$ de $K \times V$ em V, temos que para todos elementos u, v em V, os seguintes axiomas se satisfazem:*

i. Associatividade da adição em V.
ii. Comutatividade da adição em V.
iii.Existência de elemento inverso aditivo e neutro aditivo em V.
iv. Operação exterior do corpo K no conjunto V bem definida: $(\forall \alpha, \beta \in K)(\forall u \in V)$: $\alpha * (\beta * u) = (\alpha * \beta) * u$

v. Elemento neutro multiplicativo do corpo de escalares também é neutro em multiplicação de vetores: $(\forall u \in V) : 1 \cdot v = v$
vi. Distributividade da multiplicação por escalar em relação à adição de vetores: $(\forall \alpha \in K)(\forall u, v \in V) : \alpha * (u + v) = \alpha * u + \alpha * v$
vii. Distributividade da multiplicação por escalar em relação a adição do corpo : $(\forall \alpha, \beta \in K)(\forall u \in V) : (\alpha + \beta) * u = \alpha * u + \beta * u$

Todo elemento $\alpha \in K$ sera chamado de escalar, enquanto que todo elemento $u \in V$ será chamado de vetor. Exceto quando não houver confusão, denotaremos um vetor com uma flecha em cima, por exemplo $\vec{u} \in V$

Definição 2.18 (Combinação linear) *Seja $x \in V$ um vetor qualquer. Dizemos que x será uma combinação linear dos vetores x_i se existir constantes $\alpha_i \in K$ tal que $x = \sum_{i=1}^{k} \alpha_i x_i$ onde k é um número natural finito.*

Exemplo 2.19 *Seja um vetor v em $R^2, v = (2,1)$, temos que $v_1 = (2,0)$ e $v_2(0,1)$ tem como combinação linear $v_1 + v_2 = (2,1) = v$.*

Definição 2.20 (linearmente dependente e independente) *Seja $x = (x_1, x_2, ..., x_n)$ uma sequência de vetores de V. Diremos que x são **linearmente dependentes** se existem $\alpha_1, \alpha_2, ..., \alpha_n$ não nulos tal que $\alpha_1 x_1 + \alpha_2 x_2 + ... + \alpha_n x_n = \vec{0}$. Caso a única constante α_i que faça a igualdade acima valer é a constante 0, então diremos que a sequência de vetores é **linearmente independente**.*

Definição 2.21 (Espaço gerado e conjunto gerador) *Seja um espaço vetorial V sobre um corpo K, o **conjunto gerador** S é um subconjunto de V tal que tomando todas as possíveis combinações lineares finitas, gere um subespaço vetorial, chamado de **espaço gerado** por S.*

Ou seja, dado $S \subset V$, o espaço gerado, denotado por $span(S)$ será:

$$span(S) = \{\sum_{i=1}^{k} \alpha_i v_i | k \in \mathbb{N}, v_i \in S, \alpha_i \in K\}$$

Definição 2.22 (Base de um espaço vetorial) *Diremos que um conjunto de vetores $B = \{e_1, e_2, ..., e_n\}$ é uma base de um espaço vetorial se B é um conjunto linearmente independente e se $span(B) = V$*

Exemplo 2.23 *Seja $\mathbb{R}$ o corpo dos reais, definiremos o espaço vetorial $\mathbb{R}^n$ como sendo o produto cartesiano de $\mathbb{R}$ n vezes mais as operações que definem um espaço vetorial.*

Exemplo 2.24 (base canônica no $\mathbb{R}^3$) *Seja $\mathbb{R}^3$ um espaço vetorial. Sejam $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1)$. Temos que o conjunto de vetores $B = \{e_1, e_2, e_3\}$ é uma base. Essa base é chamada de base canônica no $\mathbb{R}^3$.*

Exemplo 2.25 (Base canônica em $\mathbb{R}^n$) *Dado o espaço vetorial $\mathbb{R}^n$ e o conjunto de vetores $B = \{e_1, e_2, ..., e_n\}$. Onde $e_1 = (1_1, 0_2, ...0_i, ..., 0_n), e_2 = (0_1, 1_2, ..., 0_i, ...0_n), e_i = (0_1, 0_2, ..., 1_i, 0_n), e_n = (0_1, 0_2, ..., 0_i, ..., 1_n)$. Temos que B é uma base de $\mathbb{R}^n$ e é chamada de base canônica*

Podemos representar um vetor $x = (x_1, x_2, ..., x_n)$ através de matriz colunas. Isto é, $x = (x_1, x_2, ..., x_n) = [x_1 x_2 ... x_n]$

3 Homomorfismos

Neste capitulo estudaremos um dos aspectos mais importantes no estudo da Álgebra, o estudo de funções que preservam a estrutura algébrica de um objeto.

Na seção anterior, definimos o que era anel finito de classes de congruência módulo n geradas através do conjunto $\mathbb{Z}$, e denotamos tal anel como sendo $\mathbb{Z}/n\mathbb{Z}$. Nesta seção, usaremos a mesma construção, entretanto, para casos de grupos, teremos um grupo com a operação de adição, e denotaremos o grupo gerado pelas classes de congruência módulo n por $\mathbb{Z}_n$. Observemos que $\mathbb{Z}$ com a operação de adição, é um grupo também.

3.1 Normalidade e grupos quocientes

Antes de estudarmos homomorfismos de grupos, primeiro iremos introduzir dois objetos muito importantes para o estudo de homomorfismos.

Definição 3.1 *Seja G um grupo, H um subgrupo de G e $a, b \in G$, diremos que a é **congruente à direita** para b **modulo** H, denotado por $a \equiv_r b \mod H$ se $a * b^{-1} \in H$. De maneira equivalente, diremos que a é **congruente à esquerda** para b **modulo** H, denotado por $a \equiv_l b \mod H$ se $a * b^{-1} \in H$ se $a^{-1} * b \in H$*

Exemplo 3.2 *Seja G o grupo $\mathbb{Z}_6$ aditivo e H o subgrupo $\mathbb{Z}_3$ de $\mathbb{Z}_6$ dado pelos elementos $\mathbb{Z}_3 < \mathbb{Z}_6 | \mathbb{Z}_3 = \{0, 2, 4\}$. Dado os elementos 2 e 4, temos que $2 \equiv_{r/l} 4 \mod \mathbb{Z}_3$ pois $2 * 4^{-1} = 2 * 2 = 4$, e $4 \in \mathbb{Z}_3$.*

Exemplo 3.3 *Sejam os mesmos grupos e subgrupos acima, temos que os elementos 2,3 não são congruentes, pois $2 + 3^{-1} = 2 + 3 = 5$, e $5 \notin \mathbb{Z}_3$.*

Os dois exemplos acima não diferem entre congruência à esquerda ou à direita, isso se deve a todos os subgrupos de $\mathbb{Z}_6$ serem normais, explicaremos o conceito de

normalidade mais adiante.

Teorema 3.4 *Seja H um grupo de G.*

i. Congruência à direita (ou à esquerda) módulo H é uma relação de equivalência.
ii. A classe de equivalência $a \in G$ em relação a congruência à direita é o conjunto Ha, onde $Ha = \{ha, \forall h \in H\}$. Para a congruência a esquerda é o conjunto aH, onde $aH = \{ah, \forall h \in H\}$
iii. A ordem de $|H|$ é igual a ordem de $|Ha|$ e $|aH|$.

Chamaremos o conjunto aH de coset à direita e Ha de coset à esquerda. Tal definição e teorema acima tem um corolário muito importante:

Corolário 3.5 *Seja H um subgrupo de G.*

i. G é a união dos cosets à esquerda (ou direita) de $H < G$.
ii. Dois cosets à esquerda (ou à direita) ou são iguais ou são disjuntos.
iii. $\forall a, b \in G : Ha = Hb \iff ab^{-1} \in H$ e $aH = bH \iff a^{-1}b \in H$
iv. Se R é o conjunto formado por todos os cosets à direita, e L o conjunto formado por todos os cosets à esquerda, então $|L| = |R|$

Uma consequência bem importante do teorema acima é que dado um subgrupo qualquer N, apesar da quantidade de cosets a esquerda e à direita serem iguais, isso não equivale a dizer que o coset à esquerda aH é o mesmo coset à direita Ha. O teorema abaixo nos dá um condição necessária e suficiente para dizer quando os dois cosets serão iguais.

Teorema 3.6 *Seja G um grupo, e N um subgrupo de G, então as seguintes condições são equivalentes.*

i. Todo coset à esquerda é um coset à direita, e vise-versa
ii. As congruências à esquerda e à direita módulo N coincidem.
iii. aN=Na para todo a em G
iv. $\forall a \in G, aNa^{-1} \subset N$, onde $aNa^{-1} = \{ana^{-1}, \forall n \in N\}$
v. $\forall a \in G, aNa^{-1} = N$

Por conta da importância deste teorema, iremos colocar a prova dele.

Demonstração: $i. \implies iii.$: Se $aN = Nb$ para algum $b \in G$, então $a \in Nb \cap Na$. Como dois cosets ou são iguais ou são disjuntos, segue-se que $Nb = Na$.
$ii. \iff iii.$ Duas classes de equivalência A,B são idênticas se e somente se a classe de equivalência de cada elemento de A coincide com a classe de equivalência de cada elemento de B. Ou seja, as classes de equivalências são os cosets à direita e os cosets à esquerda.
$iii. \implies iv.$: Segue-se das definições.
$iv. \implies v.$: Temos que $aNa^{-1} \subset N$, basta provar a outra inclusão. Para isso, temos que $\forall n \in N, n = a^{-1}(ana^{-1})a \in aNa^{-1}$. Logo, $N \in aNa^{-1}$.
$v. \implies i.$: Segue-se da definição.

Chamaremos o subgrupo $N < G$ que satisfaz o teorema acima de Subgrupo Normal, denotado por $N \triangleleft G$.

Exemplo 3.7 *Todo subgrupo de um grupo abeliano é um subgrupo normal.*

Exemplo 3.8 *Todo grupo tem ao menos dois subgrupos normais. Ele mesmo e o grupo trivial* $\{e\}$.

Exemplo 3.9 *Todo subgrupo cíclico de* $\mathbb{Z}$ *é um subgrupo normal.*

Exemplo 3.10 *A união de dois subgrupos normais não necessariamente é normal. Um exemplo que especifica bem tal fato é o grupo abeliano* $\mathbb{Z}_6$ *aditivo e os subgrupos normais* $\mathbb{Z}_2, \mathbb{Z}_3$. *Temos que dado* $2, 3 \in \mathbb{Z}_2 \cup \mathbb{Z}_3$, *mas* $2 + 3 = 5 \notin \mathbb{Z}_2 \cup \mathbb{Z}_3$. *Ou seja, a união desses dois subgrupos não é um subgrupo, e logo não é um subgrupo normal.*

Exemplo 3.11 *A intersecção de dois subgrupos normais é normal. Isso decorre do fato de que dados dois subgrupos normais* $H_1, H_2 \triangleleft G$ *tal que* $x \in H_1 \cap H_2 \iff (x \in H_1) \wedge (x \in H_2)$. *Como* H_1 *é normal, então* $xh_1x^{-1} \in H_1, \forall h_1 \in H_1$ *e de maneira semelhante para* H_2, $xh_2x^{-1} \in H_2, \forall h_2 \in H_1$. *Dado um* $h \in H_1 \cap H_2$, *então* $xhx^{-1} \in H_1 \cap H_2$, *logo* $x(H_1 \cap H_2)x^{-1} \subset H_1 \cap H_2$ *para todo* $x \in G$. *Portanto a intersecção é normal.*

Teorema 3.12 *Seja N um subgrupo normal de um grupo G, se G/N é o conjunto de todos os cosets (à esquerda) de N em G. Então G/N é um grupo de ordem [G:N] com uma operação binária definida por* $(a \star N) \star (b \star N) = (a \star b) \star N$.

Chamaremos G/N de grupo quociente.

Exemplo 3.13 *Seja $\mathbb{Z}_6$ o grupo aditivo módulo 6 e $\mathbb{Z}_2$ o subgrupo normal de $\mathbb{Z}_6$ dado pelos elementos $\mathbb{Z}_3 = \{0, 3\}$. O grupo quociente $\mathbb{Z}_6/\mathbb{Z}_3$ será o grupo $\mathbb{Z}_6/\mathbb{Z}_3 = \{a + N, \forall a \in G\} = \{\{0, 3\}, \{1, 4\}, \{2, 5\}\} = \{0 + N, 1 + N, 2 + N\}$. Esta conjunto de todos os cosets (à esquerda) foram um grupo quociente pela relação binária definida acima. Este grupo é isomorfo ao $\mathbb{Z}_3$.*

Definição 3.14 *Sejam H,G dois grupos. Um homomorfismo de grupo é definido por uma função $f : G \to H$ com a seguinte característica:*

$$f(a \star b) = f(a) \star f(b) \tag{3.1}$$

Quando um homomorfismo é injetor, chamaremos de monomorfismo. Quando um homomorfismo é sobrejetor, chamaremos de epimorfismo. Quando um homomorfismo é bijetivo, será um isomorfismo.

Exemplo 3.15 *A função identidade é um isomorfismo de G em G (um isomorfismo G em G também é de automorfismo).*

Definição 3.16 (Núcleo e imagem) *Seja $f : G \to H$ um homomorfismo de grupos. O núcleo (ou kernel) de um homomorfismo é o conjunto $ker f := \{f(a_G) = e_H\}$. A imagem de um homomorfismo é um conjunto, denotado por $f(G)$ onde $f(G) = \{h \in H | h = f(a)$ para algum $a \in G\}$. Chamaremos a imagem inversa de f o conjunto $f^{-1}(H) := \{a \in G | f(a) \in H\}$.*

Um dos teoremas mais imediatos e mais importantes em caracterizações de homomorfismos é o seguinte teorema:

Teorema 3.17 *Seja $f : G \to H$ um homomorfismo. Então:*
i. f é um monomorfismo (é injetor) se e somente se $Ker f = \{e_G\}$
ii. f é um isomorfismo (é bijetor) se e somente $f f^{-1} = e_H$ e $f^{-1} f = e_G$

Teorema 3.18 *Se $f : G \to H$ é um homomorfismo, então o núcleo de f é um subgrupo normal de G. Se N é um subgrupo normal de G, então o mapa $\pi : G \to G/N$ dado por $\pi(a) = aN$ é um homomorfismo sobrejetor onde o núcleo é N. O mapa $\pi : G \to G/N$ é chamado de projeção canônica.*

A prova neste teorema se dá da seguinte forma: Se $x \in ker f$ e $a \in G$, então temos que $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)ef(a^{-1}) = e$ e assim $axa^{-1} \in ker f$. Assim,

$a(kerf)a^{-1} \subset kerf$ e $kerf \triangleleft G$.

O mapa $\pi : G \to G/N$, por definição, é sobrejetivo, e como $\pi(ab) = abN = aNbN = \pi(a)\pi(b)$ é um epimorfismo. Assim $ker\pi = \{a \in G | \pi(a) = eN = N\} = \{a \in G | aN = N\} = \{a \in G | a \in N\} = N$.

Definição 3.19 (Produto de grupos) *Sejam dois grupos G,H, com G com uma operação $*$ e H com operação $\triangle$. Seja $G \times H$ o produto cartesiano. Existe um grupo, formado pelo cartesiano $G \times H$ e com uma operação $\cdot$ definido como:*

i. O conjunto deste grupo é o produto cartesiano. De forma que $(g,h) \in G \times H$ se $g \in G, h \in H$.
ii. A operação de grupo $\cdot$ é definida como: $(g_1,h_1) \cdot (g_2,h_2) = (g_1 * g_2, h_1 \triangle h_2)$

Caso não houver confusão, denotaremos $G \times H$ como GH. A definição de produto de grupos pode ser extendida para subgrupos H,K de G, e seu produto, HK.

3.1.1 Teoremas de isomorfismos para grupos

Teorema 3.20 (Primeiro teorema do isomorfismo) *Seja $f : G \to H$ um homomorfismo de grupo.*

i. O núcleo de f é um grupo normal de G.
ii. A imagem de f é um subgrupo de H.
iii. A imagem de f é isomorfa ao grupo G/ ker f.

Se f é um epimorfismo, então G/ker f e H são isomorfos.

Demonstração: Este teorema é um caso especial do seguinte lema.

Lema 3.21 *Se $f : G \to H$ é um homomorfismo de grupos e N um subgrupo normal de G que contém o núcleo de f. Então existe um único homomorfismo $\overline{f} : G/N \to H$ tal que $\overline{f}(aN) = f(a), \forall a \in G$. Temos que $Imf = Im\overline{f}$ e $ker\overline{f} = (kerf)/N$. $\overline{f}$ será um isomorfismo se e somente se f é um epimorfismo e $K = kerf$*

A prova deste lema começa com o seguinte fato. Se $b \in aN$ então $b = an, n \in N$ e $f(b) = f(an) = f(a)f(kerf) = f(a)e = f(a)$. Assim, $\overline{f} : G/N \to H$ dado por $\overline{f}(a) =$

$f(aN)$ é uma função bem definida. Usando a normalidade, temos que $\overline{f}(aNbN) = \overline{f}(abN) = f(ab) = f(a)f(b) = \overline{f}(aN)\overline{f}(bN)$ e logo $\overline{f}$ é um homomorfismo. Assim $im\overline{f} = imf$ e $aN \in ker\overline{f}$ se e somente se $f(a) = e$ se e somente se $a \in kerf$

Assim temos que $ker\overline{f} = \{aN | a \in kerf\} = (kerf)/N$ nos dá que $\overline{f}$ é única, pois é determinada por f. Por último, $\overline{f}$ é um isomorfismo se e somente se f também for.

Temos que f é injetor se e somente se $kerf = N$. Isso prova o lema.

Se f for sobrejetor, então temos o primeiro teorema do isomorfismo provado, com $kerf = N$

Definição 3.22 *Seja G um grupo e H e K dois subgrupos de G. $H \vee K$ será denotado como subgrupo gerado pela união de H e K*

Teorema 3.23 (Segundo teorema do isomorfismo.) *Seja G um grupo, S um subgrupo de G e N um subgrupo normal de G.*

i. O produto S$\vee N$ é um subgrupo de G.
ii. A intersecção $S \cap N$ é um subgrupo normal de S
iii. Os grupos quocientes SN/N e $N/(N \cap S)$ são isomorfos

Demonstração: Para provar o segundo teorema, vamos provar o seguinte lema.

Lema 3.24 *Se S e N são subgrupos de um grupo G com N sendo normal em G. Então:*

i. $N \cap S$ é um subgrupo normal de S.
ii. N é um subgrupo normal de $N \vee S$
iii.NS=$N \vee S$= SN
iv. Se S é normal em G e $S \cap N = \{e\}$, então ns=sn $\forall s \in S, \forall n \in N$

Para provar (i), se $n \in N \cap S$ e $a \in S$, então $ana^{-1} \in N$, pois $N \triangleleft S$ e $ana^{-1} \in S$ pois $S < G$. Assim, $a(N \cap S)a^{-1} \subset N \cap S$ e $N \cap S$ e $N \cap S \triangleleft S$.

Para provar (ii), basta notar que $NS < N \vee S$.

Para provar (iii), temos que $NS \subset N \cup S$. Para mostrar a outra inclusão, seja $x \in N \vee S$, ele será um elemento de forma $n_1 s_1 n_2 s_2 ... n_m s_m$ para $n_i \in N, s_i \in$. Usando o fato de $N \triangleleft G$ então $n_i s_j = s_j n_i'$, onde $n_i' \in N$. Logo, x pode ser escrito de forma $n(s_1 ... s_m)$. Assim, temos que $N \cup S \subset NS$ De forma semelhante, o mesmo argumento serve para $SN = N \vee S$.

Por último, para provar (iv) considere $s \in S$ e $n \in N$. Então $nsn^{-1} \in S$ pois $S \triangleleft G$ e $kn^{-1}k^{-1} \in N$ pois $N \triangleleft G$. Assim, $(nkn^{-1})k^{-1} = n(kn^{-1}k^{-1} \in N \cap K = \{e\}$. Logo, $kn = sn$.

Isso completa o lema.

Para provar o teorema, considere que $N \triangleleft NS = N \vee S$. Pela composição $f : (S \to NS \to NS/N)$ é um homomorfismo, pelo teorema 3.33, onde $kerf = S \cap N$. Assim, $\overline{f} : N/N \cap N \cong Imf$ pelo primeiro teorema do isomorfismo.

Todo elemento em NS/N é da forma de nsN. A normalidade de N implica que $ns = sn_1$. Assim, $nsN = sn_1N = sN = f(s)$. Assim, temos um epimorfismo em f, e $Imf \cong NS/N$.

Teorema 3.25 (Terceiro teorema do isomorfismo) *Seja G um grupo e H,K subgrupos normais de G. Tal que $K < H$, então H/K é um subgrupo normal de G/K e $(G/K)/(H/K) \cong G/H$*

Demonstração: Temos que $1_G : G \to G$ implica que $1_G(K) < H$. Assim, temos um epimorfismo $i : G/K \to G/H$, com $i(ak) = aH$. Assim, $H = i(aK)$ se e somente se $a \in H$, $keri = \{aK | a \in H\} = H/K$. Assim, $H/K \triangleleft G/K$, e o teorema 3.33 temos que $G/H = Imf \cong (G/K)/Keri = (G/K)/(H/K)$

3.2 Ideais e os teoremas do isomorfismo para anéis

Definição 3.26 (Homomorfismo de anéis) *Seja ϕ, π anéis. Uma função $f : \phi \to \pi$ será um homomorfismo de anéis se:*

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(ab) &= f(a)f(b) \end{aligned} \tag{3.2}$$

De maneira similar a grupos, quando um homomorfismo é injetor, chamaremos de monomorfismo. Quando um homomorfismo é sobrejetor, chamaremos de epimor-

fismo. Quando um homomorfismo é bijetivo, será um isomorfismo.

Exemplo 3.27 *Sejam G,H grupos multiplicativos, e $f : G \to H$ um homomorfismo de grupos. Seja ϕ um anel, definiremos uma função $f' : \phi(G) \to \phi(H)$ dada por:*

$$f'(\sum_{i=1}^{n} r_i g_i) = \sum_{i=1}^{n} r_i f(g_i) \tag{3.3}$$

Então f' é um homomorfismo de anéis.

Definição 3.28 (Ideais) *Seja ϕ um anel e S um conjunto não vazio de ϕ que é fechado sob as operações de adição e multiplicação definidas em ϕ. Se S é um anel por si próprio, então S é um subanel de ϕ. Um subanel I de ϕ é chamado de um ideal à esquerda se:*

$$(r \in \phi) \wedge (x \in I) \Longrightarrow rx \in I \tag{3.4}$$

Um subanel I de ϕ é chamado de ideal à direita se:

$$(r \in \phi) \wedge (x \in I) \Longrightarrow xr \in I \tag{3.5}$$

I será chamado de ideal se é tanto ideal à esquerda quanto à direita.

Ideal para anéis é, de certa forma, o termo equivalente de normalidade para grupos. Assim, podemos estender facilmente o conceito de grupos quocientes para anéis quocientes.

Definição 3.29 (Anel quociente) *Seja ϕ um anel e I um ideal de ambos os lados de ϕ. Podemos definir uma relação de equivalência em ϕ tal que:*

$$a\ b \Longleftrightarrow a - b \in I \tag{3.6}$$

A classe de equivalência de um elemento $a \in \phi$, denotada por $[a]$ será $[a] = a + I = \{a + r, \forall r \in I\}$.

O conjunto de todas as classes de equivalência será denotado por ϕ/I, ϕ/I será um

anel se definirmos as seguintes operações neste conjunto:

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+I \\ (a+I)(b+I) &= (ab)+I\end{aligned} \tag{3.7}$$

O anel ϕ/I definido pelas operações acima será chamado de anel quociente.

Assim, podemos estender também os teoremas de isomorfismos de grupos para isomorfismos para anéis, fazendo as devidas alterações.

Teorema 3.30 (Primeiro teorema do isomorfismo para anéis) *Seja $f : \phi \to \pi$ um homomorfismo de anéis.*

i. O núcleo de f é um ideal de ϕ.
ii. A imagem de f é um subanel de π.
iii. A imagem de f é isomorfa ao anel $\phi/kerf$.

Se f é um epimorfismo, então $\phi/kerf$ e π são isomorfos.

Teorema 3.31 (Segundo teorema do isomorfismo para anéis) *Seja ϕ um anel, S um subanel de ϕ e I um ideal de ϕ.*
i. A soma $S+I$ é um subanel de ϕ.

ii. A intersecção $S \cap I$ é um ideal de I
iii. Os anéis quocientes $(S+I)/I$ e $I/(I \cap S)$ são isomorfos

Teorema 3.32 (Terceiro teorema do isomorfismo para anéis) *Seja ϕ um grupo e I,J ideais de ϕ. Tal que $J < I$, então I/J é um ideal de ϕ/J e $(\phi/I)/(I/J) \cong \phi/J$*

Podemos estender os teoremas do isomorfismo para álgebras em geral, iremos fazer nos próximo capitulo.

4.1 Conceitos básicos

4.1.1 Noção intuitiva de álgebra

Consideremos um exemplo clássico da álgebra linear. Seja o espaço vetorial $\mathbb{R}^3$. Dado dois vetores linearmente independentes a, b de forma $a = (a_1, a_2, a_3) = (a_1 i + a_2 j + a_3 k,\ b = (b_1, b_2, b_3) = (b_1 i + b_2 j + b_3 k)$. Além da operações binárias do espaço vetorial comum que temos dentro do conjunto de vetores, como a adição de vetores e multiplicação de vetores, vamos definir uma outra operação binária, chamada de **produto vetorial** em a, b, simbolizada por $a \times b$. Ela terá a seguinte propriedade:

$$\begin{aligned} i * i = j * j = k * k = 0 \\ i * j = k \\ j * k = i \\ k * i = j \\ j * i = -k \\ k * j = -i \\ i * k = -j \end{aligned} \tag{4.1}$$

Assim, definiremos o produto vetorial $a \times b$ por:

$$\begin{aligned} a \times b =& (a_1 i + a_2 j + a_3 k) \times (b_1 i + b_2 j + b_3 k) \\ =& a_1 b_1 (i * i) + a_1 b_2 (i * j) + a_1 b_3 (i * k) \\ & a_2 b_1 (j * i) + a_2 b_2 (j * j) + a_2 b_3 (j * k) \\ & a_3 b_1 (k * i) + a_3 b_2 (k * j) + a_3 b_3 (k * k) \\ =& (a_2 b_3 - a_3 b_2) i + (a_3 b_1 - a_1 b_3) j + (a_1 b_2 - a_2 b_1) \end{aligned} \tag{4.2}$$

Tal operação é binária e gera um terceiro elemento dentro do espaço vetorial $\mathbb{R}^3$.

Podemos extrair três propriedades desta operação operação, que são:

$$\begin{aligned}
&(a+b)\times c = a\times c + b\times c, \forall a,b,c \in \mathbb{R}^3 \\
&c\times(a+b) = c\times a + c\times b, \forall a,b,c \in \mathbb{R}^3 \\
&(\alpha a)\times(\beta b) = (\alpha\beta)a\times b, \forall a,b \in R^3, \forall \alpha,\beta \in \mathbb{R}^3
\end{aligned} \tag{4.3}$$

Este exemplo é interessante pois além das 3 propriedades vistas acima, mais nada podemos garantir sobre esta operação binária, do ponto de vista axiomático. Isto é, não temos comutatividade e, mais importante, associatividade. Tal exemplo ilustra bem o conceito de álgebra, neste caso, de uma álgebra sobre um corpo.

4.1.2 Definição axiomática de álgebra

Definição 4.1 (Definição axiomática de álgebra) *Seja ϕ um anel comutativo, associativo e com unidade multiplicativa. Um conjunto não vazio A é chamado de álgebra sobre o anel ϕ se:*
i. A tem uma estrutura bem definida de espaço vetorial sobre o anel ϕ
ii. A tem uma operação binária $\star$ dada pelas seguintes propriedades:

$$\begin{aligned}
&(a+b)\star c = a\star c + b\star c, \forall a,b,c \in A \\
&c\star(a+b) = c\star a + c\star b, \forall a,b,c \in A \\
&(\alpha a)\star(\beta b) = (\alpha\beta)a\star b, \forall a,b \in A, \forall \alpha,\beta \in \phi
\end{aligned} \tag{4.4}$$

Chamaremos A de álgebra sobre o anel ϕ.

Vemos que, como visto na seção onde tratamos de operações binárias, não temos nenhum requisito da operação definida ser associativa, comutativa, ou em alguns casos, se um produto interno de elemento.

Definição 4.2 (Subálgebra) *Seja A um álgebra sobre um anel ϕ e com uma operação binária $\star$. Um subconjunto $B \subset A$ será uma subálgebra se:*
i. B tem uma estrutura bem definida de espaço vetorial sobre o anel ϕ
ii. B é fechada sobre a operação $\star$.

4.2 Exemplos de álgebra

4.2.1 Álgebra de Lie

O exemplo que motivou nossa definição de álgebra, um espaço vetorial dotado de produto vetorial é um tipo de álgebra. Esta álgebra está definida no espaço $\mathbb{R}^3$.

Definição 4.3 (Anticomutatividade) *Enquanto a comutatividade garante que $a \star b = b \star a$. A anticomutatividade é a propriedade oriunda de estruturas algébricas que além de contar com uma operação binária $\star$, também tem a soma definida nesta estrutura. Assim, a anticomutatividade é definida como $a \star b = -b \star a$.*

No caso do espaço vetorial dotado de um produto vetorial, temos que: $a \times b = -b \times a$.
No caso da produto vetorial, temos: $a \times a = 0$.

Definição 4.4 (Operação linear) *A linearidade é um tipo especial de homomorfismo em espaços vetoriais. É uma função $f(x)$ com as seguintes propriedades.*

i. $f(x+y) = f(x) + f(y)$
ii. $f(\alpha x) = \alpha f(x), \alpha \in K$

Podemos resumir essas duas propriedades simplesmente como $f(\alpha x + y) = \alpha f(x) + f(y)$.

Como o produto vetorial é uma função de dois elementos, vemos que ela não apenas satisfaz a linearidade (caso fixemos um elemento), mas um tipo mais forte que é a ***bilinearidade***.

Definição 4.5 (Operação bilinear) *Uma operação binária é bilinear se é linear em ambos os argumentos da função. Isto é, $f(x,y) = x \star y$ é bilinear se:*

i. $f(\alpha x + x', y) = f(\alpha x, y) + f(x', y) = (\alpha x + x') \star y = \alpha x \star y + x' \star y$.
ii. $f(x, \alpha y + y') = f(x, \alpha y) + f(x, y') = x \star (\alpha y + y') = x \star \alpha y + x \star y'$.

Assim o produto vetorial $\times$ é uma operação bilinear.

Temos que o produto vetorial não é uma operação associativa. Entretanto, podemos extrair uma propriedade interessante desta álgebra que é a "identidade de Jacobi".

Definição 4.6 (Identidade de Jacobi) . *Dada uma operação binária $f(x,y) = x \star y$, a operação satisfaz a identidade de Jacobi se:*

$$\begin{aligned} &f(x,f(y,z)) + f(y,f(z,x)) + f(z,f(x,y)) = 0 \\ &x\star(y\star z) + y\star(z\star x) + z\star(x\star y) = 0 \end{aligned} \tag{4.5}$$

Podemos generalizar o produto vetorial contido em $\mathbb{R}^3$ para uma classe inteira de álgebras, chamada de álgebra de Lie.

Definição 4.7 (Álgebra de Lie) *Dada uma operação binária $f(x,y)$ em um espaço vetorial X que denotaremos como $[x,y]$, onde $[.,.]$ é chamada de colchete de Lie, a álgebra sobre este espaço vetorial será chamada de álgebra de Lie, denotada por* **g** *se satisfaz:*

i. Anticomutatividade. $[x,y] = -[y,x]$
ii. Identidade de Jacobi. $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$.
iii. Bilinearidade.
$[\alpha x + x', y] = \alpha[x,y] + [x',y]$
$[x, \alpha y + y'] = \alpha[x,y] + [x,y']$.

4.2.2 Álgebra quociente

Já construímos espaços quocientes sobre certas estruturas algébricas. Em especial, podemos extender a noção de um anel quociente para uma álgebra dotada de uma operação binária, desde que a relação de equivalência que construiremos seja compatível com nossa operação binária.

Primeiro, vamos retomar o conceito de ideal de um anel

Seja ϕ um anel e S um conjunto não vazio de ϕ que é fechado sob as operações de adição e multiplicação definidas em ϕ. Se S é um anel por si próprio, então S é um

subanel de ϕ. Um subanel I de ϕ é chamado de um ideal se:

$$\begin{aligned}(r \in \phi) \wedge (x \in I) &\Longrightarrow rx \in I \\ (r \in \phi) \wedge (x \in I) &\Longrightarrow xr \in I\end{aligned} \tag{4.6}$$

Definição 4.8 (Ideal de uma álgebra) *Quando A é uma álgebra associativa, I será um ideal de álgebra de A se além de ser um ideal de A, também satisfazer a seguintes propriedades:*
i. $(r \in \phi) \wedge (x \in I) \Longrightarrow r \star x \in I$
$ii.(r \in \phi) \wedge (x \in I) \Longrightarrow x \star r \in I$
Onde $\star$ *denota a operação binária desta álgebra.*

Assim, podemos definir uma álgebra quociente A/I por uma relação de congruência . A relação de congruência pode ser construída a partir de um homomorfismo $\pi : A \to A'$ nesta álgebra $\pi(a \star b) = \pi(a) \star \pi(b)$
de forma que o núcleo do homomorfismo $ker(\pi)$sejam os elementos do ideal.

Assim, temos uma álgebra associativa quociente.

Podemos fazer a mesma construção para uma álgebra de Lie **g**. De modo similar a construção acima, seja $\mathbf{h} \subset \mathbf{g}$ um subespaço de álgebra de Lie, e $\mathbf{g}'$ uma outra álgebra de Lie. Se $[\mathbf{g}, \mathbf{h}] \subset \mathbf{h}$, então **h** é um ideal de **g** e por uma relação de congruência dada por um homomorfismo $\pi : \mathbf{g} \to \mathbf{g}'$ nesta álgebra $\pi([a, b]) = [\pi(a), \pi(b)])$ podemos construir uma álgebra de Lie quociente **g/h** se **h** for o kernel deste homomorfismo.

As duas construções acima são verdadeiras por conta primeiro teorema do homomorfismo para álgebras

Teorema 4.9 (Primeiro teorema do isomorfismo) *Seja* $\pi : A \to B$ *um homomorfismo de álgebra. A imagem de* π *é uma subálgebra de B, a relação dada por* $\phi : \pi(a) = \pi(b)$*(o núcleo de* π *é uma relação de congruência em A, e as álgebras* A/ϕ *e* $im\pi$ *são isomórficas.*

4.2.3 Álgebra tensorial

Vamos considerar agora um exemplo muito especifico de uma álgebra quociente. Ela se origina primeiro como um produto de dois espaços vetoriais E,F.

Primeiramente, vamos pegar dois espaços vetoriais X,Y de dimensão finita quaisquer e fazer seu produto cartesiano $X \times Y$. Tal conjunto será dotado de uma operação binária $x \otimes y, x \in X, y \in Y$ que iremos nomear de produto diatico (ou outer product).

$$x \otimes y = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j (e_i \otimes f_j) \tag{4.7}$$

De forma que n, m se referem a dimensão de X,Y respectivamente. E e_i é a base de X e f_i a base de Y

Vemos que o outer product é uma operação binária que pega um elemento do espaço vetorial X e pega outro elemento do espaço vetorial Y e agora esse elemento não pertence nem a X nem a Y. Mas sim ao produto $F(X \times Y)$. Tal produto é denominado como espaço vetorial livre.

Se munirmos esse conjunto das mesmas operações de multiplicação por escalares e adição vetores, e pegarmos os geradores do espaço X e os geradores do espaço Y teremos o espaço vetorial livre $X \times Y$.

Definição 4.10 (Espaço Vetorial Livre) *Para um espaço vetorial V definido em um corpo F, um conjunto $B \subset V$ será uma base de V se:*
i. B é um conjunto gerador de M.
ii. B é um conjunto linearmente independente.
V será um espaço vetorial livre se ele tiver uma base B.

Assim, definiremos o espaço vetorial livre de $X \times Y$, denotado por $F(X \times Y)$ como sendo o espaço vetorial gerado por $X \times Y$. Em outras palavras, $F(X \times Y)$ é o espaço vetorial que tem $X \times Y$ como base.

Entretanto, este espaço vetorial é muito grande, tem muitos elementos que não precisamos. No sentido de que existem vários elementos que são muitos parecidos

entre si.

Por exemplo, peguemos dois vetores $x \in \mathbb{R}^2, y \in \mathbb{R}^2$. Sabemos que um vetor $x \in X$ tem duas representações do mesmo elemento. Isto é, $x = [x_1\ x_2]$ e $x = x_1e_1 + x_2e_2$. Eles representam o mesmo elemento e o mesmo podemos dizer para $y \in \mathbb{R}^2$.

Naturalmente, gostaríamos que essas duas representações também valessem no caso de $F(X \times Y) = F(\mathbb{R}^2 \times \mathbb{R}^2)$. Isto é, se pegarmos dois vetores e usarmos o outer product $T = x \times y$, teremos:

$$[x_1\ x_2] \otimes [y_1\ x_2]^T = \begin{pmatrix} x_1y_1 & x_2y_1 \\ x_1y_2 & x_2y_2 \end{pmatrix} \tag{4.8}$$

Entretanto, esse produto é diferente deste aqui, no espaço vetorial livre:

$$(x_1e_1+x_2e_2)\otimes(y_1e_1+y_2e_2) = x_1y_1(e_1\otimes e_1)+x_1y_2(e_1\otimes e_2)+x_2y_1(e_2\otimes e_1)+x_2y_2(e_2\otimes e_2) \tag{4.9}$$

Tal fator decorre de que o outerproduct pode ser visto como uma aplicação bilinear, isto é, podemos ver o outer product como $x \otimes y = x^t T y = T(x, y)$.

E usando a definição do outer product $x \otimes y = T(x, y)$, vemos que,

$$\begin{aligned} [x_1\ x_2] \otimes [y_1\ x_2]^T &= T(x, y) \\ (x_1e_1 + x_2e_2) \otimes (y_1e_1 + y_2e_2) &= x_1y_1T(e_1, e_1) + x_1y_2T(e_1, e_2) + x_2y_1T(e_2, e_1) + x_2y_2T(e_2, e_2) \end{aligned} \tag{4.10}$$

Assim, gostaríamos de diminuir esse espaço vetorial. A maneira mais natural de fazermos isso é quocientar por uma relação de equivalência $\sim$, chamada de igualdade

formal, de forma que, para $x, x' \in X, y, y' \in Y$, temos:

$$\begin{aligned} &T(x,y) \sim T(y,x) \\ &T(x+x',y) \sim T(x,y) + T(x',y) \\ &T(x,y+y') \sim T(x,y) + T(x,y') \\ &T(\alpha x, y) \sim \alpha T(x,y) \sim T(x, \alpha y) \end{aligned} \tag{4.11}$$

Dadas essas relações, podemos quocientar o espaço vetorial livre $F(X \times Y)$ para obtermos o produto tensorial de X e Y, denotado por $X \otimes Y$ ou $F(X \times Y)/\sim$. Um elemento de $X \otimes Y$ será chamado de tensor e ele terá dimensão mn onde m é a dimensão de X e n é a dimensão de Y. Um tensor com dimensão mn é chamado tensor de ordem mn.

Definição 4.11 (k-ésima potencia tensorial de V) *Dado um inteiro não negativo k, podemos definir o k-ésimo produto tensorial de V com ele mesmo, de forma* $T^K V = V^{\otimes k} = V \otimes V \otimes ... \otimes V$.

Por convenção, temos que $T^0 V = \mathbb{K}$, onde $\mathbb{K}$ é o corpo do espaço de V. $T^k V$ consiste de todos os tensores de ordem K.

Definição 4.12 (Soma direta) *Seja W, V dois subespaços vetoriais quaisquer com o vetor nulo. A soma direta $W \oplus V$ será um novo espaço vetorial formado a partir destes dois seguindo as seguintes regras.*

i.Seja $w_1, w_2 \in W$, $v_1, v_2 \in V$. Então $(w_1, v_1) + (w_2, v_2) = (w_1 + w_2, v_1 + v_2$
ii. Seja $w \in W, v \in V, \alpha \in K$. Então $\alpha(w, v) = (\alpha w, \alpha v)$

Dada essas regras, podemos generalizar para qualquer n uma soma direta de n subespaços W_k. Denotaremos a soma direta de n subespaços W_k como $\bigoplus_{k=1}^{n} W_k$

Assim, podemos construir a álgebra tensorial, denotada por T(V) como a soma direta de todas as potenciais tensoriais de V. Ou seja:

$$T(V) = \bigoplus_{k=0}^{\infty} T^k V = \mathbb{K} \oplus V \oplus (V \otimes V) \oplus .... \tag{4.12}$$

A operação desta álgebra será o outer product, que além do que definimos acima, tem uma condição a mais:

$$T^k V \otimes T^l V = T^{k+l} V \tag{4.13}$$

Assim, temos uma álgebra, a álgebra tensorial.

5 Involuções

Um dos melhores exemplos para introduzir o conceito de involução é se pegarmos a função $f(x) = -x$. A inversa dessa função é justamente ela mesmo. Isto é, $f \circ f(x) = x$. Tal função, por ela mesmo ser sua inversa, tem propriedades e características interessantes. Chamamos esta função que é sua própria inversa, de involução.

Definição 5.1 *Seja A uma álgebra. Seja $* : A \to A$ uma transformação linear. $*$ será chamada de involução se satisfaz as seguintes propriedades:*

i) $a^{**} = a, \forall a \in A$
ii) $(ab)^* = b^*a^*, \forall a, b \in A$

Alguns exemplos desta definição são:

Definição 5.2 (Complexo conjugado) *Seja $\mathbb{C}$ o conjunto dos complexos visto como uma $\mathbb{R}$-álgebra. A seguinte função, chamada de complexo conjugado, será uma involução:* $\forall a, bi \in \mathbb{C}, \overline{a + bi} = a - bi$

Exemplo 5.3 *Seja $M_n[F]$ o conjunto de todas as matrizes $n \times n$ no corpo F. A matriz transposta de $A \in M_n[F]$, denotada por A^t é uma involução. Onde $(A^t)^t = A$ e $(AB)^t = B^tA^t, \forall A, B \in M_n[F]$.*

Exemplo 5.4 *Seja $M_2[F]$ o conjunto de todas as matrizes quadradas 2×2 sobre o corpo F.*

Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \forall a, b, c, d \in F$. Definiremos uma transformação linear, chamada de transformação simplética como: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Esta transformação é uma involução.

Demonstração: A demonstração da involução de uma matriz quadrada qualquer é trivial. Vejamos $(AB)^*$. Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $B = \begin{pmatrix} f & g \\ h & l \end{pmatrix}$. Temos que $AB = \begin{pmatrix} af+bh & ag+bl \\ cf+dh & cg+dl \end{pmatrix}$ e sua involução será $(AB)^* = \begin{pmatrix} cg+dl & -(ag+bl) \\ -(cf+dh) & af+bh \end{pmatrix}$.

Vejamos agora $(B^*A^*) = \begin{pmatrix} l & -g \\ -h & f \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} cg+dl & -(ag+bl) \\ -(cf+dh)(ag+bl) & af+bh \end{pmatrix}$

Dada tal definição e exemplos, podemos definir agora um novo tipo de álgebra, chamada de álgebra com involução.

Definição 5.5 *Seja A uma álgebra, $*$ uma involução definida em A, definiremos a álgebra com involução como sendo a álgebra A com uma operação a mais, que é a operação unária $*$ atuando como um operador linear em A. Assim, teremos duas operações binárias, $+, \times$ e uma operação unária $*$.*

Podemos falar agora de isomorfismo de álgebras com involução.

Definição 5.6 *Sejam A,B duas álgebras sobre o mesmo corpo com involução. Seja $f : A \to B$ uma transformação linear entre essas duas álgebras. f será um homomorfismo se:*

i) $f(ab) = f(a)f(b), \forall a, b \in A$
ii) $f(a^*) = f(a)^*, \forall a \in A$

Dado tal homomorfismo, podemos falar sobre os teoremas do isomorfismo e sobre os ideais destas álgebras.

Definição 5.7 *Ideal de uma álgebra com involução. Seja A uma álgebra com Involução (ACI), seja $I \subset A$ um subespaço de A. I será um ideal de uma ACI se:*
i)$\forall r \in I, \forall a \in A : ar \in I, ra \in I$
ii)$\forall r \in I : r^* \in I$

Assim, podemos enunciar os teoremas dos isomorfismos para ACI.

Teorema 5.8 (Primeiro teorema do isomorfismo para ACI) *Seja $\pi : A \to B$ um homomorfismo de ACIs, seja I um ideal de A:*

i) $Im(\pi) \cong A/ker(\pi)$
ii) $(r+I)^* = r^* + I$

Para falarmos dos outros teoremas de isomorfismo, precisamos de um novo conceito, que já foi mencionado anteriormente de maneira mais intuitiva:

Definição 5.9 (Congruência) *Seja uma álgebra A. Um subconjunto do produto direto $A \times A$ será uma relação de congruência de A se:*
i. É uma relação de equivalência de A.
ii. É uma subálgebra de A.

Exemplo 5.10 *Seja $f : A \to B$ um homomorfismo entre duas álgebras , seja $ker f$ o núcleo de f. Então a álgebra quociente $A/ker f$ é uma relação de congruência, de forma que todo elemento de A é mapeado para sua classe de equivalência em $A/ker f$*

Teorema 5.11 (Segundo teorema do isomorfismo para ACI) *Seja A uma álgebra, B uma subálgebra de A e $\backsim$ uma relação de congruência em A. Definiremos $\backsim_B$ como sendo $\backsim$ restrito a B, isto é, $\backsim_B = \backsim \cap (B \times B)$. Definiremos $[B]^{\backsim}$ como a coleção de classes de equivalência de A que intersectam B. Isto é $[B]^{\backsim} = \{K \in A/\backsim \text{ tal que } K \cap B \neq \emptyset\}$ então:*
i.$\backsim_B$ é uma relação de congruência em B.
ii.$[B]^{\backsim}$ é uma subálgebra de $A/\backsim$.
iii. a álgebra $[B]^{\backsim}$ é isomórfica a álgebra $B/\backsim_B$

5.1 Subespaços de elementos simétricos e anti simétricos

Seja A um ACI, definiremos dois tipos de elementos importantes no estudo de involuções.

Definição 5.12 (Elemento simétrico e anti simétrico) *Seja $a \in A$, a será chamado de elemento simétrico se $a^* = a$.*
Se $a^* = -a$, então a será chamado de elemento antissimétrico.

Elementos simétricos e antissimétricos aparecem na álgebra linear quando pensamos em autovalores e autovetores de uma transformação linear no espaço de funções lineares.. Um elemento *a* será simétrico se ele é autovetor de autovalor 1. E um elemento será antissimétrico se ele é autovetor de autovalor -1.

Podemos agora pegar o conjunto de todos os elementos simétricos e o conjunto de todos os antissimétricos formar um subespaço de uma ACI.

Teorema 5.13 *i)Seja A uma ACI, o conjunto de todos os elementos simétricos, denotado por A^+, será uma subálgebra de A em relação operação binária $a \circ b = ab + ba$(produto simétrico).*
ii) Seja A uma ACI, o conjunto de todos os elementos anti-simétricos, denotado por A^-, será uma subálgebra de A em relação a a operação binária $[a, b] = ab - ba$(comutador)

Demonstração:
Temos que todas as propriedades de operações binárias que A carrega, qualquer subconjunto dessa álgebra irá carregar. Basta apenas mostrar que as operações induzidas acima são fechadas neste conjunto.

Vamos provar (i). Primeiro, vejamos como a operação $\circ$ se comporta em A^+ : $a^* \circ b = ab + ba = a \circ b$. Vejamos o produto simétrico de dois elementos simétricos é um elemento simétrico: $a^* \circ b^* = ab + ba = (ab + ba)^* = (a \circ b)^*$

Assim, A^+ será uma subálgebra com a operação binária $a \circ b$

Vamos provar (ii), primeiro, vejamos como o comutador se comporta em A^- : $[a^*, b] = [-a, b] = -ab + ba = ba - ab = [a, b^*] = [b, a] = [a, b]^* = -[a, b]$. Vejamos se o comutador de dois antissimétricos é um elemento antissimétrico: $[a^*, b^*] = [-a, -b] = (-a)(-b) - (-b)(-a) = ab - ba = (ba - ab)^* = [b, a]^*$

Assim, A^- será uma subálgebra com a operação binária $[a, b]$

5.2 Álgebra livre

Seja $X = \{x_1, x_2, ...\}$ um conjunto de símbolos, podendo o conjunto ser infinito ou não. Cada elemento $x_n \in X$ será único e chamado de gerador livre.

Definição 5.14 (Monômio) *Seja X um conjunto de geradores livres, um monômio será uma sequência ordenada de geradores livres x_i e "(", ")"que satisfaz:*

i) $\forall x_i \in X, x_i$ é monômio
ii) Se u, v são monômios, então (uv) é monômio.

Tais condições são necessárias para definir um monômio de forma única e sem ambiguidades. Por exemplo, caso as condições acima não valessem, então a seguinte combinações de símbolos seria um monômio: $x_1)x_2,))$

Assim, apenas as sequências de símbolos construídos seguindo as duas condições acima são monômios.

Exemplo 5.15 *As seguintes sequências de símbolos são monômios:* $x_1y_2, (y_1y_2)((x_1x_2)x_3)$

Definição 5.16 (Produto de monômios) . *Sejam u, v dois monômios bem definidos. Então o produto $u \cdot v$ será apenas um dos três monômios abaixo:*

i) $u \cdot v = x_i v$, se $u = x_i$
ii) $u \cdot v = ux_j$, se $v = x_j$
iii) $u \cdot v = (u)(v)$

Exemplo 5.17 (produto de monômios não é comutativo) *Seja x_1y_2 um monômio bem definido, então $x_1y_2 \neq y_2x_1$*

Parênteses em um monômio representam um monômio de forma única. Seja o monômio $(x_1x_2)((x_3x_1)x_2)$ um monômio bem definido, então $(x_1x_2)((x_3x_1)x_2) \neq (x_1x_2)(x_3x_1)x_2$. Ou seja, produto de monômios não são associativos.

Podemos agora definir algumas operações sobre monômios sobre um certo conjunto de geradores livres X.

Exemplo 5.18 *Seja $u = (x_1x_2)x_3, v = x_3(x_3x_4)$, então $u \cdot v = ((x_1x_2)x_3)((x_1x_2)x_3)$*

Definição 5.19 (Grau de um monômio) *Seja X um conjunto de geradores livres, x_i monômio. Um expoente é o produto de potencias com repetição. Definiremos o grau de um monômio como a soma dos expoente de um monômio. Caso dois ou mais monômios estejam multiplicados entre si, o grau do monômio será a soma dos expoentes de cada gerador livre*

Exemplo 5.20 *Seja u um monômio qualquer. Temos que* $u \cdot u = u^2$. *Isto nos dá que o expoente de u é 2 e o grau deste monômio é 2.*

Exemplo 5.21 *Sejam* u, v *dois monômios quaisquer. Temos que* $u \cdot u \cdot v = u^2 v$. *Onde o expoente de u é 2, o expoente de v é 1, e o grau do monômio é 3.*

Definição 5.22 *Dado a definição e o produto de monômios, podemos falar agora sobre a Álgebra Livre.*
[Álgebra livre de polinômios] Seja M um conjunto de geradores livre m_i.
Seja F um corpo. Definiremos como álgebra livre de polinômios $F\{M\}$ *o espaço vetorial gerado* $span(m_i)$ *de forma que os monômios* m_i *formam uma base deste espaço e um elemento qualquer do espaço* $F\{M\}$ *pode ser escrito como* $\sum_{i=1}^{m} \alpha_i m_i$, *onde* m_i *denota algum gerador livre no espaço M,* α_i *é um elemento do corpo F*

A álgebra livre será uma álgebra de polinômios, semelhante ao anel de polinômios em um corpo K. Entretanto, a álgebra livre não terá unidade multiplicativa, não é associativa e nem comutativa.

Exemplo 5.23 *O seguinte polinômio é um exemplo de polinômio livre já reduzido em sua forma canônica, isto é, não tem como reduzir ou simplificar ele:* $2x_1 - 3x_2 + (x_1 x_3)x_4 - 3((x_2 x_4)(x_2 x_4))x_5$

Um dos teoremas mais importantes quando observamos álgebras livres é o seguinte:

Teorema 5.24 *Seja A uma álgebra qualquer, X um conjunto de geradores livres, F um corpo, e* $f : X \to A$ *uma transformação qualquer. Então existe um homomorfismo* $\overline{f} : F\{X\} \to A$ *tal que:*$\overline{f}(x_i) = f(x_i)$, $\forall x_i \in X$

5.3 Álgebra livre com involução

Dadas as ferramentas acima, podemos falar da relação entre álgebra livre e involução.

Definição 5.25 (Álgebra livre com involução) *Seja X um conjunto de geradores de livres, Y um outro conjunto distinto de geradores livres, e* $F\{X \cup Y\}$ *a álgebra livre de* $X \cup Y$. *Seja* $* : F\{X \cup Y\} \to F\{X \cup Y\}$ *uma transformação linear tal que:*

i. $(x_i^* = y_i), (y_i^* = x_i)$
ii. $(uv)^* = v^*u^*, \forall u, v \in F\{X \cup Y\}$ *Tal operação neste espaço define uma álgebra livre com involução.*

Exemplo 5.26 *Seja* $x_1, x_2, x_3, y_1, y_2, y_3$ *elementos de uma álgebra livre com* $F\{X \cup Y\}$*, e uma involução* $* : F\{X \cup Y\} \to F\{X \cup Y\}$*, então:*
$((x_1x_2)x_3)^* = y_3(y_2y_1)$
$x_1((x_1y_2)(y *_3 y_4))^* = ((x_4x_3)(x_2y_1))y_1$.

Podemos agora falar de um teorema importante que relaciona uma álgebra com involução, com uma álgebra livre com involução.

Teorema 5.27 *Seja A uma álgebra com involução, e* $f : X \to A$ *uma transformação qualquer. Então existe um homomorfismo de álgebras com involução* $\overline{f} : F\{X \cup Y\} \to A$ *tal que* $\overline{f}(x_i) = f(x_i)$.

Para demonstrar o teorema acima, basta mostrar que se $f(x_i) = a_i$, então $\overline{f}(y_i) = a_i^*$. E também $\overline{f}(x_i) = f(x_i) = a_i$.

Assim, temos que $\overline{f}(m(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m)) = m(a_1, a_2, ..., a_n, a_1^*, a_2^*, ..., a_m^*)$ é um homomorfismo. Onde $m(a, b, ..., c)$ denota um polinômio com geradores livres $(a, b, ..., c)$

Se $F\{X \cup Y\}$ é uma ACI, então poderemos denotar Y como sendo o espaço X^* e assim, a álgebra livre com involução será denotada por $F\{X \cup X^*\}$

6 Teorema de Birkhoff

Vamos mostrar o teorema de Birkhoff, com uma ênfase em especial para ACI.

Definição 6.1 (Produto de álgebras) *Seja I um conjunto e $A_{i\,i\in T}$ uma classe de álgebras com involuções. O conjunto de todas as transformações $f : I \to \bigcup_{i\in I} A_i$, tais que $f(i) \in A_i$ é uma álgebra com involução em relação a operações:* $(f+g)(i) = f(i) + g(i)$,
$fg(i) = f(i)g(i)$
$f^*(i) = (f(i))^*$

Podemos representar a álgebra acima para conjuntos com cardinalidade infinita enumerável. Por exemplo: $f = (a_1, a_2, ..., a_n, ...), a_i \in A_i, g = (b_1, b_2, ..., b_n, ...), f + g = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n, ...), fg = (a_1b_1, a_2b_2, ..., a_nb_n, ...), f^* = (a_1^*, a_2^*, ..., a_n^*, ...)$
A álgebra definida acima é chamada de produto direto das álgebras A_i, denotada por $\prod A_i$.

Definição 6.2 (Identidade de álgebra) *Seja A uma álgebra com involução e $L = F\{X \cup X^*\}$, onde X^* são elementos de involução de X. Dado um elemento $g(x_1, ..., x_n) \in L$ é uma identidade da álgebra A, se para qualquer homomorfismo $f : L \to A$, $f(g) = 0$.*

Temos que, como definido anteriormente, g é um polinômio definido nas variáveis $\{x_1, ..., x_n\}$, então podemos substituir as variáveis por elementos a_i pertencentes a álgebra A.
Para qualquer $a_1, a_2, ..., a_n \in A, g(a_1, a_1, ..., a_n) = 0$.

Exemplo 6.3 *Seja $\mathbb{C}$ o corpo dos complexos com as operações usuais de corpo e com a operação de álgebra definida com o complexo conjugado. A seguinte equação é uma identidade da álgebra dos complexos $xy - yx = 0$*

Exemplo 6.4 *Seja $M_2[F]$ a álgebra das matrizes de tamanho 2 com coeficientes no corpo F com a operação de involução simplética. Seja o comutador definido anteriormente, teremos a seguinte identidade $[X + X^*, Y] = 0$*

Demonstração: $X + X^* = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix}$

$$\text{Assim, } [X + X^*, Y] = \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} \cdot \begin{pmatrix} w & x \\ y & z \end{pmatrix} - \begin{pmatrix} w & x \\ y & z \end{pmatrix} \cdot \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} = 0$$

Definição 6.5 (Classe de álgebras) *Seja V uma coleção de álgebras. Dada uma álgebra $A \in V$. V será uma classe de álgebras se, dada uma álgebra $A' \cong A$, tem-se $A' \in V$*

Definição 6.6 (Variedade de álgebra) *Seja V um classe de álgebra. V será chamado de variedade de álgebras se: (i) existe um conjunto de polinômios da álgebra livre $G \subset L = F\{X \cup X^*\}$ tal que, dado $g \in G$, e $A \in V$, A álgebra, então g satisfaz A.*
(ii)Se alguma álgebra B satisfaz todas as identidades de G, então $B \in V$

Podemos agora enunciar e demonstrar o teorema de Birkhoff. Também chamado de Teorema HSP, as iniciais de Homomorfismo, Subálgebra e Produto.

Teorema 6.7 (Teorema HSP para ACI) *Uma classe de álgebras V com involução é uma variedade de álgebras se e somente se ela satisfaz:*

(i) Para qualquer álgebra A de V, se B é uma subálgebra de A, então $B \in V$.
(ii) Para todas $A \in V$, se I é um ideal de A, então $A/I \in V$.
(iii) Para todas $A_i \in V$, $\prod A_i \in V$

Demonstração:
Suponha que V seja uma variedade.

Se A satisfaz uma ou mais identidades, então todas as subálgebras de A satisfazem as identidades de A.

Como uma álgebra quociente A/I é uma imagem homomórfica de uma álgebra, então se a pré-imagem de A/I satisfaz a identidade, então por isomorfismo, a A/I também satisfaz.

Seja A_i uma componente de $\prod A_i \in V$ uma componente que satisfaz as identidades de V, então $\prod A_i$ também irá satisfazer por isomorfismo.

Basta agora provar a volta.

Suponha V uma classe de álgebra que satisfaz (i), (ii), (iii). Seja X um conjunto infinito e $L = F[X \cup X^*]$. Considere agora o conjunto J formado pelos ideais de L, tal que L/I está em V, isto é:$J = \{I\ ideal\ \in L$ t.q. $L/I \in V\}$.

(*)Se $I \in J$ e $I \subset I_1$, então $I_1 \subset J$.

Pelo segundo teorema do isomorfismo, temos: $L/I_1 \cong (L/I)/(I_1/I)$. Pela condição (ii) temos que $(L/I)/(I_1/I) \in V$, logo $L/I_1 \in V$ e logo $I_1 \in J$.

(**) Seja T uma família de índices tal que:
(***). se $\forall t \in T, S_t \in J$, então $\cap_{t\in T} S_t \in J$.

Para demonstrar (***), assuma que se $S_t \in J$, então $L/S_t \in V$. Pela condição (iii), temos que $\prod L/S_t \in V, t \in T$. Considere agora o seguinte homomorfismo: $f : L \to \prod L/S_t, t \in T$ tal que $f(g)(t) = g + S_t$. Temos que $f(g)(t)$ é uma classe de equivalência de S_t. Onde f é um homomorfismo.

Para mostrar isso, vemos que $f(g_1)(t)+f(g_2)(t) = g_1+g_2+S_t = f(g_1+g_2))(t)$, e também vemos $f(g_1)(t) \cdot f(g_2)(t) = g_1 \cdot g_2 + S_t g_2 + S_t g_1 + S_t = g_1 \cdot g_2 + S_t = f(g_1 \cdot g_2)$

Temos que a imagem inversa de f, $imf^{-1} \in V$. O primeiro teorema do isomorfismo nos diz que: $L/ker(f) \cong Imf \in V$. Por tanto, temos que $kerf \in J$.

Porém, $kerf$ é justamente todos os elementos de L de forma que $f(g)(t) = e + S_t$, onde e é elemento neutro. Ou seja, dado dois ideais S_{t_1}, S_{t_2}, os únicos elementos onde $f(g)(t_1) = e + S_{t_1} = e + S_{t2} = f(g)(t_2)$ são justamente os $S_{t_1} \cap S_{t_2}$. Para vermos se isto vale, vamos mostrar que $\cap S_t \in kerf$: seja $x \in \cap S_t$, então $\forall t \in T, x \in S_t$ e $f(x)(t) = x + S_t = S_t = \bar{0}$. Ou seja, $x \in kerf$.

Vamos mostrar que $kerf \subset \cap S_t$. Se $x \in kerf$, então $f(x) = 0$. Se $f(x) = 0$, então $\forall t \in T, f(x)(t) = 0$. Se $f(x)(t) = 0$, então $f(x)(t) = x + S_t = \bar{x} = \bar{0}$. E por fim, temos que $x \in S_t, \forall t \in T$. Logo, $x \in \cap S_t, t \in I$.

Considere $G = \cap_{I\in J} I$. Por (**), $G \in J$. Por definição de J, G é ideal de L. Nosso objetivo agora é mostrar que V é uma variedade gerada por G. Ou seja, precisamos mostrar que (1) qualquer polinômio de G é uma identidade de qualquer álgebra de

V. (2) Se alguma álgebra satisfaz todas as propriedades de G, então ela pertence a V.

Vamos mostrar (1).

Seja $g \in G, A \in V$. Então existe um homomorfismo $f : L \to A$ tal que f é sobrejetor. Isto é, qualquer álgebra é uma álgebra homomórfica de alguma álgebra livre. Como $L/kerf \cong A$, então $kerf \in J$.

Se $kerf \in J$, então $G \subset kerf$. Mas $G \subset kerf$ nos mostra que dado um elemento g, então existe uma expressão na álgebra livre L de forma que $g(x_1, x_2, ..., x_n) = 0$. Isto é, $g \in G$ é uma identidade, e logo, temos que qualquer polinômio $g \in G$ é uma identidade de toda álgebra $A \in V$.

Vamos mostrar (2).

Considere um homomorfismo $h : L \to B$ para alguma álgebra B, onde h é sobrejetor. Temos que $h(g) = 0, \forall g \in G$. Ou seja, $G \subset kerf$. Assim, o primeiro teorema do isomorfismo nos diz que $B \cong L/kerf = (L/G)/(kerh/G)$. E como $L/G \in V$, então $B \in V$. Assim, mostramos (**)

Referências Bibliográficas

[Smith, 1998] Smith, J.D.H.; Romanowska, A.B.; JI, L.; *Post-Modern Algebra*, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts; https://books.google.com.br/books?id=8tJ4G2lq3AYC, Wiley, 1998.

[Giambruno et al, 2003] Giambruno, A.; Regev, A.; Zaicev, M., *Polynomial Identities And Combinatorial Methods*, Lecture notes in pure and applied mathematics; https://books.google.com.br/books?id=DinG40kb0WMC, CRC Press, 2003.

[Bergman, 1995] Bergman, G.M.; *An invitation to general algebra and universal constructions*, Berkeley mathematics lecture notes; https://books.google.com.br/books?id=CvfuAAAAMAAJ, Center for Pure and Applied Mathematics, Dept. of Mathematics, University of California, 1995.

[Zhevlakov et al, 1982] Zhevlakov, K.A.; Ivan Shestakov; Arkadii M. Slinko; A.I.Shirshov; *Rings That are Nearly Associative*, ; https://books.google.com.br/books?id=7S-xISi8obEC, Elsevier Science, 1982.

[Hungerford, 1974] Hungerford, Thomas W.; *Algebra*, Graduate Texts in Mathematics; https://www.springer.com/gp/book/9780387905181, 1974.