UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
UNIDADE UNIVERSITÁRIA DE CASSILÂNDIA
LICENCIATURA EM MATEMÁTICA
(Graduação)

MILENA AMALIA GIOLI RULLI

Elementos de Álgebras de Lie

Cassilândia-MS
2018

MILENA AMALIA GIOLI RULLI

Elementos de Álgebras de Lie

Trabalho de Conclusão de Curso apresentado à Universidade Estadual de Mato Grosso do Sul, Unidade Universitária de Cassilândia, como requisito parcial para a obtenção do grau de Licenciada em Matemática.

Orientador: Prof. Dr. Ailton Ribeiro de Oliveira

Cassilândia-MS
2018

R888e Rulli, Milena Amalia Gioli
Elementos de álgebras de Lie / Milena Amalia Gioli Rulli. Cassilândia, MS: UEMS, 2018.
77p. ; 30cm.

Monografia (Graduação) – Matemática – Universidade Estadual de Mato Grosso do Sul, 2018.
Orientador: Prof. Dr. Ailton Ribeiro de Oliveira.

1.Grupos 2. Anéis 3. Álgebras de Lie I. Título.

CDD 23.ed. 512.55

Elementos de Álgebras de Lie

Milena Amalia Gioli Rulli

Trabalho de Graduação apresentado ao Curso de Licenciatura em Matemática, da Universidade Estado de Mato Grosso do Sul, como requisito parcial para a obtenção do grau de Licenciada em Matemática.

Aprovada por:

Prof. Dr. Ailton Ribeiro de Oliveira ....
(Orientador)

Prof. Dr. Adilson Lelis Nunes Júnior ....

Profa. Dra. Irene Coelho de Araujo ....

Cassilândia

Novembro - 2018

Aos meus pais, Leandro Rulli e Elizângela Gioli,

e à minha irmã Ana Luiza.

“Nada é tão nosso como os nossos sonhos.”

Friedrich Nietzsche.

Agradecimentos

Agradeço primeiramente a Deus por me capacitar durante todo o desenvolvimento deste trabalho, colocar as pessoas certas em meu caminho e por me dar forças para concluir algo de tamanha importância em minha vida.

Aos meus pais, Leandro e Elizângela, pela excelente educação que me deram e meus avós maternos Domingos e Maria, e paternos João e Dozolina, por todo o carinho que sempre tiveram comigo durante a minha criação. À toda minha família, em especial, às minhas tias Elaine e Eliane e meu tio Mario, que estiveram presentes em todos os momentos da minha vida, me apoiando, me dando muito amor e forças para continuar. E às duas pequenas, Ana Luiza e Amanda, que me motivam diariamente a vencer e um dia ser um exemplo para elas.

Às minhas amigas de infância, Letícia e Luana que desde o início estiveram ao meu lado, torcendo pelo meu êxito. E a todos os meus colegas de graduação, em especial, a Daniele e Suelen que se tornaram grandes amigas e os colegas, Bruno, Cristina, Daniel, Ederson, Elaine, Fernanda, Kauan, Letiele, Marcos e Viviane que fizeram parte da minha vida acadêmica durante esses anos, que foram difíceis, mas pela graça de Deus, vencidos.

Ao meu orientador, professor Ailton, por trabalhar comigo no desenvolvimento deste trabalho e da iniciação científica. Por toda a paciência, atenção, esclarecimentos e disponibilidade para me atender nesses últimos anos. Gostaria de agradecer também, a todos os professores e funcionários que tiveram parte na minha formação.

A família/instituição UEMS, por todo o apoio e oportunidades no decorrer desses quatro anos. E, também, a todas as pessoas que não mencionei, mas que de uma forma ou de outra contribuíram para a conclusão desse trabalho.

Resumo

Uma álgebra de Lie é uma estrutura algébrica, ou melhor, uma álgebra não-comutativa cujo principal uso está no estudo dos grupos de Lie e das variedades diferenciáveis. As álgebras de Lie formam o aparato básico do que é conhecido hoje como teoria de Lie. Nesse trabalho visamos um estudo introdutório sobre as álgebras de Lie, focando em exemplos geométricos e de grupos de matrizes.

Em geral, os cursos de licenciatura em Matemática fazem um estudo sobre as estruturas algébricas, mas se limitam nos conceitos de grupos, anéis, homomorfismos, por diversos fatores. Daí surgiu a ideia de fazer esse estudo, que se aprofunda nos conceitos de estruturas algébricas e fala um pouco das álgebras de Lie, as quais, na maioria das vezes, não são vistas na graduação.

Para iniciar um estudo sobre álgebra de Lie, não é necessário fazer esse "passeio"pelas estruturas algébricas, como fizemos. Mas é importante ter uma noção de Grupos e Álgebra Linear. No entanto, decidimos fazer um estudo base, que envolve conceitos iniciais de Estruturas Algébricas, com o intuito de facilitar a compreensão dos conceitos de Álgebra de Lie mais adiante no Trabalho.

Palavras chave: Álgebras de Lie, Grupos, Anéis, Geometria, Matemática.

Abstract

A Lie algebra is an algebraic structure, or rather a non-commutative algebra whose main use is in the study of Lie groups and differentiable varieties. Lie algebras form the basic apparatus of what is now known as Lie theory. In this paper, we present an introductory study on Lie algebras, focusing on geometric examples and matrix groups.

In general, undergraduate courses in Mathematics study algebraic structures, but are limited in the concepts of groups, rings, homomorphisms, by several factors. Hence came the idea of doing this study, which goes deeper into the concepts of algebraic structures and speaks a little of Lie algebras, which, most of the time, are not seen in the undergraduate.

To begin a study of Lie algebra, it is not necessary to do this "walk" by algebraic structures, as we did. But it is important to have a notion of Groups and Linear Algebra. However, we decided to make a base study, which involves initial concepts of Algebraic Structures, in order to facilitate the understanding of the concepts of Lie Algebra later in the Work.

Key words: Lie algebras, Groups, Rings, Geometry, Mathematics.

Sumário

Introdução

Uma álgebra de Lie é uma estrutura algébrica, ou melhor, uma álgebra não-comutativa cujo principal uso está no estudo dos grupos de Lie e das variedades diferenciáveis. As álgebras de Lie formam o aparato básico do que é conhecido hoje como teoria de Lie.

Originada por volta de 1870, uma ideia de abordar as equações diferenciais sob o mesmo ponto de vista que o adotado por Galois para equações algébricas. Sophus Lie e Felix Klein estudaram as equações diferenciais via seus grupos de simetrias. Evidenciaram os grupos contínuos de transformações, uma extensa teoria com ramificações nas mais diversas áreas da matemática e de suas aplicações.

Nos primeiros trabalhos de Lie, a idéia era construir uma teoria de grupos contínuos, para complementar a teoria dos grupos discretos que se desenvolveram na teoria das formas modulares, nas mãos de Felix Klein e Henri Poincaré. A aplicação inicial que Lie tinha em mente era a teoria das equações diferenciais. No modelo da teoria de Galois e das equações polinomiais, a concepção motriz era de uma teoria capaz de unificar, pelo estudo da simetria, toda a área das equações diferenciais ordinárias.

De acordo com o historiador Thomas W. Hawkins, foi Élie Cartan que fez da teoria de Lie, ou seja, enquanto Lie tinha muitas idéias férteis, Cartan era o principal responsável pelas extensões e aplicações de sua teoria que o tornaram um componente básico da matemática moderna. Foi ele quem, com alguma ajuda da Weyl, desenvolveu as idéias seminal, essencialmente algébricas de Matar na teoria da estrutura e representação de álgebras semisimples de Lie que desempenha um papel tão fundamental na atual teoria da Lie.

E, embora Lie considerasse as aplicações de sua teoria à geometria, foi Cartan quem realmente as criou, por exemplo através de suas teorias de espaços simétricos e generalizados, incluindo todos os aparelhos auxiliares. Sophus Lie, descobriu os grupos infinitesimais ou, como se diz hoje em dia, das álgebras de Lie. Resultados pioneiros da teoria são a relação entre os grupos de transformações, denominados atualmente de grupos de Lie, e as álgebras de Lie, através da aplicação exponencial. Relação álgebra-geometria, os grupos de Lie têm uma natureza geométrica enquanto que as álgebras de Lie são objetos algébricos por excelência.

Aa Álgebras de Lie podem ser aplicadas na Física experimental, engenharia, teoria de representação, geometria de variedades, dentre outras várias áreas. O primeiro grande avanço se deu com a descoberta das álgebras de Lie, posteriormente, a teoria de Lie foi aplicada a quase todos os ramos da matemática e da física como por exemplo no estudo das partículas elementares, a teoria de Lie também tem sido útil na física matemática, uma vez que descreve importantes grupos físicos como o grupo galileu, o grupo Lorentz e o grupo Poincaré.

O estudo das álgebras de Lie, os grupos de Lie englobam os aspectos geométricos, topológicos (estudo de propriedades da figura através de conceitos como limites, continuidade, interior, exterior etc.), analíticos e algébricos. Através do conceito de grupo, automaticamente se estabelece a ideia de simetria, possibilitando a obtenção de dados locais ou globais em seus conjuntos. Assim, estabelecem para si a estrutura algébrica de grupo em conjunto com uma estrutura de variedade diferenciável (cálculo diferencial e integral).

Como sabemos, em álgebra, uma álgebra de Lie é uma estrutura algébrica cujo principal uso está no estudo dos grupos de Lie e das variedades diferenciáveis. As álgebras de Lie foram introduzidas como ferramenta para o estudo das rotação infinitesimais. O termo "Álgebra de Lie"é uma referência a Sophus Lie, e foi cunhado pelo matemático Hermann Weyl na década de 1930.

A correspondência entre álgebras de Lie e grupos de Lie é utilizada de diversas maneiras, incluindo-se na elaboração da lista dos grupos de Lie simples e na teoria da representação dos grupos de Lie. Toda representação de uma álgebra de Lie é levantada de forma única para um representação do grupo de Lie conexo e simplesmente conexo correspondente. De forma recíproca, toda representação de um grupo de Lie induz uma representação da sua álgebra de Lie; suas representações estão biunivocamente correspondidas.

Em geral, a maioria dos cursos de graduação em matemática se limitam no ensino da álgebra, dando ênfase às álgebras Lineares e às estruturas algébricas. Esse trabalho visa apresentar uma base sobre estruturas algébricas e álgebras lineares a fim de introduzir a teoria básica de álgebras de Lie. Desta forma, o trabalho fornece uma forma clara e detalhada para dar um início aos estudos sobre álgebras de Lie. Assim, nesse trabalho visamos um estudo introdutório sobre as álgebras de Lie, focando em exemplos geométricos e de grupos de matrizes.

O desenvolvimento do trabalho se dá da seguinte maneira:

No primeiro capítulo, iniciamos com alguns conceitos base sobre a Teoria de Grupos. Onde apresentamos alguns resultados sobre a estrutura algébrica de grupos. Veremos também que semigrupos é uma estrutura mais simples do que grupos, subgrupo de um grupo, os quais são subconjuntos de um grupo que ainda possuem estrutura de grupo, homomorfismos de grupos, que por sua vez, são aplicações entre grupos que preservam as respectivas operações dos grupos e por fim, mas não menos importante, subgrupos normais.

Na sequencia, o segundo capítulo, iniciamos falando de alguns resultados sobre a estrutura algébrica de anel. Veremos ainda algumas classes importantes de anéis que são domínios de integridade, os anéis de divisão e os corpos, subanéis de um anel, que são subconjuntos do anel que também são anéis, homomorfismo de anéis, que são aplicações entre anéis que preservam estas estruturas algébricas.

Por fim, iremos introduzir a teoria das álgebras de Lie. Iniciaremos com alguns conhecimentos de conceitos básicos da álgebra linear, como espaço vetorial, base, dimensão e transformação linear. E seguiremos apresentando as definições básicas desta teoria e, na sequencia, um pouco da estrutura algébrica das álgebras de Lie.

Capítulo 1

Teoria de Grupos

Apresentaremos alguns resultados sobre a estrutura algébrica de grupos. Além disso, veremos semigrupos, que é uma estrutura mais simples do que grupos, subgrupos de um grupo, que são subconjuntos de um grupo que ainda possuem estrutura de grupo, homomorfismo de grupos, que são aplicações entre grupos que preservam as respectivas operações dos grupos e subgrupos normais. Esse capítulo foi baseado nas referências [1] e [5].

1.1 Grupos

Uma operação interna em um conjunto X é uma aplicação ρ do produto cartesiano $X \times X$ no conjunto X, que associa a cada par $(x, y) \in X \times X$ um elemento $\rho(x, y) \in X$:

$$\begin{array}{rcl} \rho : X \times X & \to & X \\ (x, y) & \mapsto & \rho(x, y). \end{array}$$

Denotamos por (x, ρ) o conjunto X munido da operação ρ.

Exemplo 1.1. *Seja $X = \mathbb{R}^+$ o conjunto dos números reais não negativos. Como o produto de dois números reais não negativos também é um número real não negativo, temos que, para $x, y \in \mathbb{R}^+$, podemos definir a operação interna $\rho(x, y) = x \cdot y$ no conjunto $\mathbb{R}^+$.*

$$\{x \cdot y : x, y \in \mathbb{R}^+\}$$

Exemplo 1.2. *Consideremos o produto cartesiano*

$$\begin{array}{rcl} X & = & \mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R} \ (n \text{ vezes}) \\ & = & \{(x_1, \cdots, x_n) : x_1, \cdots, x_n \in \mathbb{R}\}. \end{array}$$

Uma operação interna em $\mathbb{R}^n$ é dada por

$$\rho((x_1,\cdots,x_n),(y_1,\cdots,y_n)) = (x_1+y_1,\cdots,x_n+y_n).$$

Exemplo 1.3. *A multiplicação de números reais negativos não é uma operação interna neste conjunto uma vez que o produto de dois números reais negativos não é um número real negativo, ou seja,*

$$\text{se } a,b>0, \text{ então } (-a)\cdot(-b) = ab > 0.$$

Exemplo 1.4. *Seja $X = \mathbb{R}^2 = \mathbb{R}\times\mathbb{R} = \{(x,y) : x,y \in \mathbb{R}\}$. Podemos definir uma operação interna em $\mathbb{R}^2$ através da soma componente a componente no par ordenado (x,y), ou seja,*

$$\rho((x_1,x_2),(y_1,y_2)) = (x_1+y_1, x_2+y_2).$$

Exemplo 1.5. *Denotaremos por $X = M(2\times 2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbb{R} \right\}$ o conjunto das matrizes com duas linhas e duas colunas com entradas reais. Tomemos $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ e $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ e definamos*

$$\rho(A_1,A_2) = A_1 + A_2 = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix}. \in M(2\times 2,\mathbb{R})$$

Logo, temos que ρ é uma operação interna em X.

A soma de matrizes é uma operação interna no conjunto $M(m\times n,\mathbb{R})$. Uma matriz $A \in M(n\times n,\mathbb{R})$ é chamada de matriz quadrada ou matriz de ordem n. No caso do conjunto das matrizes quadradas $M(n\times n,\mathbb{R})$, o produto de matrizes define uma operação interna neste conjunto. Definamos agora, a matriz identidade $I = (I_{i,j})$ de ordem n como a matriz tal que $I_{i,j} = 0$ para $i \neq j$ e $I_{i,j} = 1$ se $i = j$. Uma matriz A de ordem n é dita invertível se existe uma matriz B de ordem n tal que $A\cdot B = B\cdot A = I$.

Seja S um conjunto munido de uma operação interna que denotaremos por $s*t$. Dizemos que $(S,*)$ é um semigrupo se a propriedade associativa é satisfeita para os elementos de S, ou seja,

$$\forall\ s,t,u \in S, \text{ temos que } (s*t)*u = s*(t*u).$$

Exemplo 1.6. *Seja* $S = \{(x,y) \in \mathbb{R}^2 : x \geq 0 \text{ e } y \geq 0\}$. *Uma descrição geométrica de* S *é dada pelo primeiro quadrante do plano euclidiano. Temos que* E *é um semigrupo com a operação*

$$(x_1, y_1) * (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

De fato, $*$ *define uma operação interna em* S*, uma vez que a soma de números reais não negativos também é um número real não negativo. A associatividade desta operação segue da associatividade da soma de números reais. Com efeito,*

$$\begin{aligned}
(x_1, y_1) * (x_2, y_2) * (x_3, y_3) &= (x_1 + x_2, y_1 + y_2) * (x_3, y_3) \\
&= ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3) \\
&= (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) \\
&= (x_1, y_1) * (x_2 + x_3, y_2 + y_3) \\
&= (x_1, y_1) * (x_2, y_2) * (x_3, y_3).
\end{aligned}$$

Exemplo 1.7. *O conjunto*

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \textit{ onde } a,b,c,d \textit{ são números reais não negativos} \right\}$$

é um semigrupo com o produto usual de matrizes. Com efeito, se as entradas das matrizes $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ *e* $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ *são números reais não negativos, definamos*

$$A_1 \cdot A_2 = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

Temos que $A_1 \cdot A_2$ *também tem entradas não negativas. Para a associatividade, de fato, se* $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$, $A_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ *e* $A_3 = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$, *temos que*

$(A_1 \cdot A_2) \cdot A_3$

$$= \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$$
$$= \begin{pmatrix} (a_1a_2 + b_1c_2)a_3 + (a_1b_2 + b_1d_2)c_3 & (a_1a_2 + b_1c_2)b_3 + (a_1b_2 + b_1d_2)d_3 \\ (c_1a_2 + d_1c_2)a_3 + (c_1b_2 + d_1d_2)c_3 & (c_1a_2 + d_1c_2)b_3 + (c_1b_2 + d_1d_2)d_3 \end{pmatrix}$$
$$= \begin{pmatrix} a_1(a_2a_3 + b_2c_3) + b_1(c_2a_3 + d_2c_3) & a_1(a_2b_3 + b_2d_3) + b_1(c_2b_3 + d_2d_3) \\ c_1(a_2a_3 + b_2c_3) + d_1(c_2a_3 + d_2c_3) & c_1(a_2b_3 + b_2d_3) + d_1(c_2b_3 + d_2d_3) \end{pmatrix}$$
$$= \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2a_3 + b_2c_3 & a_2b_3 + b_2d_3 \\ c_2a_3 + d_2c_3 & c_2b_3 + d_2d_3 \end{pmatrix}$$
$$= A_1 \cdot (A_2 \cdot A_3).$$

Um Grupo é um conjunto não vazio G munido de uma operação interna, que denotamos por $\rho(g, h) = g * h$, satisfazendo as propriedades:

1. Associativa: Para todos $g, h, k \in G$, tem-se $g * (h * k) = h * (g * k)$;

2. Existência do elemento neutro: Existe $e \in G$ tal que $g * e = e * g = g$, para todo $g \in G$;

3. Existência do elemento inverso: Para cada $g \in G$ existe $h \in G$ tal que $g * h = h * g = e$.

$(G, *)$ é a denotação do grupo G munido da operação $*$.

Um grupo $(G, *)$ é dito *abeliano* se satisfaz a propriedade comutativa, ou seja, para todos $g, h \in G$ temos que $g * h = h * g$.

Exemplo 1.8. *Verifiquemos, a seguir, que o conjunto $\mathbb{R}^2$ com a operação interna $(x_1, y_1) * (x_2, y_2) = (x_1 + y_1, x_2 + y_2)$ é um grupo abeliano. Mostremos a propriedade comutativa:*

$$\begin{aligned} (x_1, x_2) * (y_1, y_2) &= (x_1 + y_1, x_2 + y_2) \\ &= (y_1 + x_1, y_2 + x_2) \\ &= (y_1, y_2) * (x_1 + x_2). \end{aligned}$$

Temos também a propriedade associativa:

$$\begin{aligned} ((x_1, x_2) * (y_1, y_2)) * (z_1, z_2) &= (x_1 + y_1, x_2 + y_2) * (z_1, z_2) \\ &= ((x_1 + y_1) + z_1, (x_2 + y_2) + z_2) \\ &= (x_1 + (y_1 + z_1), x_2 + (y_2 + z_2)) \\ &= (x_1, x_2) * (y_1 + z_1, y_2 + z_2) \\ &= (x_1, x_2) * ((y_1, y_2) * (z_1, z_2)) \end{aligned}$$

uma vez que a propriedade associativa também é satisfeita para a soma de números reais.

O elemento neutro de $\mathbb{R}^2$ *é* $(0,0)$ *pois*

$$(x_1, x_2) * (0,0) = (x_1 + 0, x_2 + 0) = (x_1, x_2) \text{ e } (0,0) * (x_1, x_2) = (x_1, x_2).$$

O inverso de um elemento $(x_1, x_2) \in \mathbb{R}^2$ *é o elemento* $(-x_1, -x_2)$*, uma vez que*

$$(x_1, x_2) * (-x_1, -x_2) = (x_1 + (-x_1), x_2 + (-x_2)) = (0,0) = (x_1, x_2) * (-x_1, -x_2).$$

Proposição 1.9. *Seja (G,$*$) um grupo. Então valem:*

(1) Existe um único $e \in G$ *que satisfaz* $g * e = e * g = g$ *para todo* $g \in G$.

(2) Para cada $g \in G$ *existe um único* $h \in G$ *tal que* $g * h = h * g = e$.

(3) Para todo $g \in G$ *temos* $(g^{-1})^{-1} = g$.

(4) Para todos $g, h \in G$ *temos que* $(g * h)^{-1} = h^{-1} * g$.

Demonstração:

(1) De fato, se e *e* f *são elementos neutros para* G *temos, pela definição de elemento neutro, que* $e = e * f = f$.

(2) Se h *e* k *são elementos inversos de* g *temos* $h = h*e = h*(g*k) = (h*g)*k = e*k = k$.

(3) Como $g * g^{-1} = g^{-1} * g = e$ *concluímos que o inverso de* g^{-1} *é* g*, ou seja,* $(g^{-1})^{-1} = g$.

(3) Temos que, $(g * h) * (h^{-1} * g^{-1}) = g * e * g^{-1} = e$*. Analogamente, tem-se que* $(h^{-1} * g^{-1}) * (g * h) = e$*, portanto,* $(g * h)^{-1} = h^{-1} * g^{-1}$.

Proposição 1.10 (Lei do cancelamento)**.** *Seja* $(G, *)$ *um grupo e sejam* g *e* h *elementos quaisquer de* G*. Para qualquer* $k \in G$ *tem-se que*

(1) Se $k * g = k * h$, então $g = h$.

(2) Se $g * k = h * k$, então $g = h$.

Demonstração. (1) Se admitirmos que $k * g = k * h$ temos que $k^{-1} * (k * g) = k^{-1} * (k * h)$. Daí concluímos que $e * g = e * h$ e, portanto, $g = h$.

(2) Temos que, $g * k = h * k$, assim, $(g * k) * k^{-1} = (h * k) * k^{-1}$, desta forma, temos que, $g * e = h * e$ e, portanto, $g = h$.

□

Exemplo 1.11. *Assumimos o conjunto das matrizes reais* 3×3 *definidas por*

$$H = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}.$$

Consideremos em H *o produto usual de matrizes*

$$\begin{pmatrix} 1 & a_1 & c_1 \\ 0 & 1 & b_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & c_2 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & a_1 b_2 + c_1 + c_2 \\ 0 & 1 & b_1 + b_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Como o produto de matrizes é associativo temos também que este produto realizado com elementos de H *também é associativo.*

A matriz identidade de ordem 3 *é um elemento de* H *e, portanto, será o elemento neutro de* H*.*

Tem-se também que a inversa da matriz

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

é a matriz

$$\begin{pmatrix} 1 & -a & ab - c \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

que é elemento de H*. Assim,* H *é um grupo. Este grupo é chamado de Grupo de Heisenberg.*

Exemplo 1.12 (Grupos de Permutações)**.** *Seja X um conjunto não vazio qualquer e $B(X)$ o conjunto das aplicações bijetivas definidas em X e a valores neste mesmo conjunto, mais especificamente, $B(X) = \{f : X \to X : f$ é bijetiva$\}$.*

Como a composta de duas aplicações bijetivas ainda é uma aplicação bijetiva, podemos definir a operação interna em $B(X)$ dada pela composição $fog(x) = f(g(x))$ para $x \in X$.

Afirmação: $B(X)$ é um grupo com a operação de composição de aplicações definida acima. Com efeito, a aplicação $Id : X \to X$ definida por $Id(x) = x$ é o elemento neutro de $B(X)$. Dada $f \in B(X)$ seu inverso será a aplicação inversa f^{-1}. O grupo $B(X)$ é chamado de Grupo de permutação de elementos de X e $f \in B(X)$ é chamada uma permutação. É interessante observar que se X for um conjunto com um número finito de elementos, então $B(X)$ será um grupo com um número finito de elementos. Neste caso, $B(X)$ é chamado grupo de permutação de n elementos.

Exemplo 1.13. *Definimos*

$$\begin{aligned} Sl(2,\mathbb{R}) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2\times 2,\mathbb{R}) : ad - bc = 1 \right\}. \\ &= \{A \in M(2\times 2,\mathbb{R}) : \det(A) = 1\}. \end{aligned}$$

Considere a operação interna em $Sl(2,\mathbb{R})$ dada pelo produto usual de matrizes. Esta operação está bem definida, pois

$$\det(AB) = \det(A)\det(B) = 1,$$

para $A, B \in Sl(2,\mathbb{R})$.

A propriedade associativa em $Sl(2,\mathbb{R})$ segue da propriedade associativa para o produto de matrizes em geral.

O elemento neutro é a matriz identidade de ordem 2

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in Sl(2,\mathbb{R}),$$

pois $\det(I_2) = 1$.

Seja $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2,\mathbb{R})$. *Assim, a inversa de* A *é dada por* $A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, *pois*

$$\begin{aligned}
\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} &= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Logo, $(Sl(2,\mathbb{R},\cdot)$, *onde* $\cdot$ *é a multiplicação usual de matrizes, é um grupo,* ***denominado grupo linear especial.***

Este grupo não é abeliano, pois

$$\begin{pmatrix} 1/2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ -1/3 & 0 \end{pmatrix} \in Sl(2,\mathbb{R})$$

e

$$\begin{pmatrix} 1/2 & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ -1/3 & 0 \end{pmatrix} = \begin{pmatrix} 2/3 & 3/2 \\ -2/3 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 \\ -1/3 & 0 \end{pmatrix}\begin{pmatrix} 1/2 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 8 \\ -1/6 & -1/3 \end{pmatrix}.$$

Exemplo 1.14. *Definimos*

$$SO(2,\mathbb{R}) = \left\{ \begin{pmatrix} cos\theta & -sen\theta \\ sen\theta & cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}.$$

Observe que $SO(2,\mathbb{R})$ *é um subconjunto de* $Sl(2,\mathbb{R})$ *porque*

$$\det \begin{pmatrix} cos\theta & -sen\theta \\ sen\theta & cos\theta \end{pmatrix} = sen^2\theta + cos^2\theta = 1.$$

Consideremos a operação interna em $SO(2,\mathbb{R})$ *como sendo o produto usual de matrizes.*

Essa operação está bem definida, pois

$$\begin{pmatrix} cos\theta_1 & -sen\theta_1 \\ sen\theta_1 & cos\theta_1 \end{pmatrix} \begin{pmatrix} cos\theta_2 & -sen\theta_2 \\ sen\theta_2 & cos\theta_2 \end{pmatrix}$$
$$= \begin{pmatrix} cos\theta_1 cos\theta_2 - sen\theta_1 sen\theta_2 & -cos\theta_1 sen\theta_2 - sen\theta_1 cos\theta_2 \\ sen\theta_1 cos\theta_2 + cos\theta_1 sen\theta_2 & cos\theta_1 cos\theta_2 - sen\theta_1 sen\theta_2 \end{pmatrix}$$
$$= \begin{pmatrix} cos(\theta_1+\theta_2) & -sen(\theta_1+\theta_2) \\ sen(\theta_1+\theta_2) & cos(\theta_1+\theta_2) \end{pmatrix} \in SO(2,\mathbb{R}).$$

Novamente, a propriedade associativa segue da associativa do produto usual de matrizes.

Temos que

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} cos0 & -sen0 \\ sen0 & cos0 \end{pmatrix} \in SO(2,\mathbb{R})$$

é o elemento neutro.

Se $A = \begin{pmatrix} cos\theta & -sen\theta \\ sen\theta & cos\theta \end{pmatrix} \in SO(2,\mathbb{R}),$ *então*

$A^{-1} = \begin{pmatrix} cos(-\theta) & -sen(-\theta) \\ sen(-\theta) & cos(-\theta) \end{pmatrix} \in SO(2,\mathbb{R}),$ *ou seja, todo elemento de* $SO(2,\mathbb{R})$ *possui inverso.*

Portanto, $SO(2,\mathbb{R})$ *é um grupo, denominado grupo ortogonal especial ou grupo de rotação.*

1.2 Subgrupos

Sejam $(G, *)$ um grupo e H um subconjunto não vazio de G. Se H com a mesma operação $*$ de G for um grupo, dizemos que H é um subgrupo de G. Se $(H, *)$ for um grupo abeliano, dizemos que H é um subgrupo abeliano de G.

O resultado a seguir nos permite determinar se um subconjunto de um grupo é um subgrupo de uma maneira mais simples.

Proposição 1.15. *Um subconjunto* $H \neq 0$ *de um grupo* $(G, *)$ *é um subgrupo se, e somente se, satisfaz às seguintes condições:*

i) Se $g, h \in H$, *então* $g * h \in H$.

ii) Se $g \in H$, então $g^{-1} \in H$.

Demonstração. ($\Rightarrow$)Se H é um subgrupo de G, então segue imediatamente da definição de subgrupo que as condições i) e ii) são satisfeitas. Assumamos, agora, que as condições i) e ii) são verdadeiras. Da condição i), segue que a operação $*$ está bem definida em H. Como $H \neq \emptyset$, existe $k \in H$ e da condição ii) conclui-se que $k^{-1} \in H$. Utilizando a condição i) novamente, obtemos que $k * k^{-1} = e \in H$, onde é o elemento neutro de G.

($\Leftarrow$)Agora, se h é um elemento qualquer de H, e como $H \subset G$, temos que $h * e = h = e * h$ e, portanto, e é o elemento neutro de H. A condição ii) garante a existência de inverso em H. Como todo elemento de H também é elemento de G e a propriedade associativa é satisfeita para elementos em G, temos que ela também é satisfeita para elementos em H, mostrando assim que $(H, *)$ é um grupo. □

Definição 1.16. *Seja A um subconjunto não vazio de um grupo $(G, *)$. Então o centralizador de A em G é definido por*

$$C(A) = \{g \in G : g * a = a * g, \textit{ para todo } a \in A\}.$$

Proposição 1.17. *Tem-se que $C(A)$ é um subgrupo de G.*

Demonstração. Inicialmente, temos que $e \in C(A)$ pois $a * e = e * a$, para todo $a \in A$.

Tomemos $g_1, g_2 \in C(A)$.

Pela definição de $C(A)$ segue que $a * g_1 = g_1 * a$ e $a * g_2 = g_2 * a$, para todo $a \in A$.

Portanto, se $a \in A$ temos $a * g_1 * g_2 = g_1 * a * g_2 = g1_1 * g_2 * a$ mostrando que $g_1 * g_2 \in C(A)$.

Suponhamos agora que $g \in C(A)$ e tomemos $a \in A$.

Tem-se que $g * a = a * g$ e daí $g * a * g^{-1}$.

Segue daí que $g * a * g^{-1} = a$ e, portanto, $a * g^{-1} = g^{-1} * a$ mostrando que $g^{-1} \in C(A)$. □

Definição 1.18. *O centro de um grupo $(G, *)$ é definido como $C = \{h \in G : g * h = h * g$, para todo $g \in G\}$.*

Como o centralizador de G é o centro de G temos, pela observação anterior, que o centro de um grupo é um subgrupo de G. Além disso, decorre da definição de C que ele é um subgrupo abeliano de G.

Definição 1.19. *Para um subconjunto não vazio A de um grupo $(G,*)$ definimos normalizador de A em G como o conjunto $N(A) = \{g \in G : g * A * g^{-1} = A\}$.*

Exemplo 1.20. *Seja A um subconjunto não vazio de um grupo $(G,*)$. Então o normalizador de A em G é um subgrupo de G.*

De fato, se $g, h \in N(A)$, então $g * A * g^{-1} = A$ e $h * A * h^{-1} = A$. Portanto,

$$(g * h) * A * (g * h)^{-1} = g * (h * A * h^{-1}) * g^{-1} = g * A * g^{-1} = A$$

o que implica em $g * h \in N(A)$.

Por outro lado, $g \in N(A)$, então $g * A * g^{-1} = A$ e daí

$$g^{-1} * (g * A * g^{-1}) * g^{-1} = g^{-1} * A * g$$

ou ainda,

$$A = g^{-1} * A * g.$$

Logo $g^{-1} \in N(A)$.

Se G é um grupo, então G também é um subgrupo dele mesmo. Também, se e é o elemento neutro de G, então $\{e\}$ é um subgrupo de G. Eles são os chamados subgrupos triviais de G.

1.3 Classes Laterais

Definição 1.21. *Sejam G um grupo e H um subgrupo deste grupo. Definimos a relação $\equiv_H$ em G por:*

$$g \equiv_H h \text{ se, e somente se, } g * h^{-1} \in H.$$

Proposição 1.22. *A relação $\equiv_H$ é uma relação de equivalência em G.*

Demonstração. A propriedade reflexiva $g \equiv_H g$ é verdadeira, pois $g * g^{-1} = e \in H$, e H é subgrupo de G. Para mostrar a propriedade simétrica, assuma que $g \equiv_H h$. Pela definição da relação $\equiv_H$, temos que $g * h^{-1} \in H$. Como H é subgrupo de G segue que

$(g * h^{-1})^{-1} = h * g^{-1} \in H$, mostrando que $h \equiv_H g$. Para mostrar a transitividade, suponha que $g \equiv_H h$ e que $h \equiv_H k$. Pela definição da relação $\equiv_H$ temos que $g * h^{-1} \in H$ e $h * k^{-1} \in H$ e, portanto, $g * k^{-1} = (g * h^{-1}) * (h * k^{-1}) \in H$, ou seja, $g \equiv_H k$. $\square$

Definição 1.23. *Seja H um subgrupo de um grupo $(G, *)$. Dado $a \in G$ indicamos por $a * H$ (respectivamente por $H * a$) e chamaremos de classe lateral à esquerda (respectivamente à direita), módulo H, definida por a, o seguinte subconjunto de G*

$$a * H = \{a * h : \ h \in H\} \ (\textit{respectivamente } H * a = \{h * a : \ h \in H\}).$$

Se G é um grupo comutativo, tem-se $a * H = H * a$, para todo $a \in G$.

Proposição 1.24. *(1) A união de todas as classes laterais módulo H é igual a G.*

(2) Para todos $a, b \in G$, tem-se $aH = bH$ se, e somente se, $a^{-1}b \in H$.

(3) Sejam aH e bH duas classes laterais módulo H genéricas. Então $aH \cap bH = \emptyset$ ou $aH = bH$.

(4) Toda classe lateral aH é equipotente a H.

A demonstração pode ser encontrada em Hoffman, K. e Kunze, R., Álgebra linear. Editora Polígono, São Paulo, 1971.

Um grupo finito é um grupo $(G, *)$ no qual o conjunto G é finito. Nesse caso, o número de elementos de G é chamado de ordem de G, ou seja, $\circ(G)$.

Dado um subgrupo H de um grupo G, definimos o índice de H em G como sendo o número de classes laterais módulo H em G, ou seja, $i_G(H)$.

Veremos no resultado a seguir que a ordem de um subgrupo divide a ordem do grupo.

Teorema 1.25 (Teorema de Lagrange)**.** *Seja H um subgrupo de um grupo finito G. Então*

$$o(H)|o(G) \ \textit{e} \ o(G) = o(H)(G : H).$$

Demonstração. Suponhamos que $(G : H) = r$ e seja $\{a_1H, \cdots, a_rH\}$ o conjunto de todas as classes laterais de à esquerda módulo H. Então, $a_1H \cup \ldots \cup a_rH = G$. Como cada elemento de G figura numa única dessas classes e como o número de elementos de cada classe é $o(H)$, então $r \cdot o(H) = o(G)$, ou seja, $(G : H) \cdot o(H) = o(G)$. $\square$

Definição 1.26. *Seja G um grupo multiplicativo qualquer. Se existe um $a \in G$ tal que $G = \{a^x : x \in \mathbb{Z}\}$ dizemos que G é um grupo cíclico. O elemento a é chamado de gerador de G. notação: $G =< a >$ ou $G = [a]$.*

Corolário 1.27. *Sejam $a \in G$ e $H = [a]$. Então o período de a divide a ordem de G e o quociente nessa divisão é $(G : H)$.*

Demonstração. Como H é um subgrupo de G, temos pelo teorema de Lagrange que $o(H)(G : H) = o(G)$. Como o(H)=o(a), o resultado segue. □

Corolário 1.28. *Se a é um elemento de G, então $a^{o(G)} = a$.*

Demonstração. Seja $H = [a]$. Então $o(G) = o(H)(G : H) = o(a)(G : H)$. Mas $a^{o(a)} = e$. Assim,

$$a^{o(G)} = (a^{o(a)})^{(G:H)} = e^{(G:H)} = e.$$

□

Corolário 1.29. *Todo grupo de ordem prima é cíclico.*

Demonstração. Seja G um grupo e $|G| = p$, onde p é um número primo. Se $x \in G$, com $x \neq e$, então $H = [x]$ é um subgrupo de G contendo o conjunto $\{e, x\}$. Assim, pelo teorema de Lagrange, $|H|$ é um divisor da $|G| = p$ e $|H| > 1$. Portanto, $|H| = p$ e, assim, $G = H = [x]$, isto é, G é cíclico. □

1.4 Homomorfismo de Grupos

Sejam $(G, *_1)$ e $(H, *_2)$ dois grupos. Uma aplicação $\phi : G \to H$ é um homomorfismo se satisfaz a seguinte propriedade:

$$\phi(g *_1 h) = \phi(g) *_2 (h).$$

Proposição 1.30. *Seja $\phi : G \to H$ um homomorfismo entre dois grupos cujos elementos neutros são $e \in G$ e $f \in H$. Então $\phi(e) = f$ e $\phi(g^{-1}) = (\phi(g))^{-1}$.*

Demonstração. Note que, $\phi(e) = \phi(e * e) = \phi(e) * \phi(e)$. Assim $f * \phi(e) = \phi(e) * \phi(e)$. Aplicando a lei do cancelamento obtemos que $f = \phi(e)$.

Temos que $\phi(g) * \phi(g^{-1}) = \phi(g * g^{-1}) = \phi(e) = f$.

Da mesma forma, temos $\phi(g^{-1}) * \phi(g) = \phi(g^{-1} * g) = \phi(e) = f$.

Logo $(\phi(g))^{-1} = \phi(g^{-1})$. □

A seguir, vamos definir o conceito de grupos isomorfos, que ocorre quando dois grupos possuem entre eles uma aplicação bijetiva que mantém as operações, ou seja, são isomorfos se eles são "iguais"do ponto de vista das estruturas algébricas de grupos.

Definição 1.31. *Dois Grupos G e H são isomorfos se existe um homomorfismo bijetivo $\phi : G \to H$. Neste caso, ϕ é dito um isomorfismo. Um isomorfismo $\phi : G \to G$ é dito um automorfismo de G.*

Exemplo 1.32. *Seja $(G, *)$ um grupo. A aplicação identidade $Id : G \to G$ definida por $Id(g) = g$ para $g \in G$ é um automorfismo de G.*

1.5 Grupos quocientes

Observe que se H é um subgrupo de G então $H * H = H$. De fato, por definição de subgrupo, temos que $H * H \subset H$. Por outro lado, como $e \in H$ temos que $H = H * e \subset H * H$. Lembramos também que

$$g * H = \{g * h : H \in H\} = g * H \text{ e } H * g = \{h * g : h \in\} = H * g.$$

Proposição 1.33. *Seja N um subgrupo de um grupo G. Então são equivalentes:*

a) $Ng = gN$, para todo $g \in G$;

b) $g^{-1} * N * g = N$, para todo $g \in G$;

c) N é invariante pela conjugação, ou seja, $C_g(N) \subset N$, para todo $g \in G$.

d) $g^{-1} * N * g \subset N$, para todo $g \in G$.

e) Toda classe lateral à direita também é uma classe lateral à esquerda.

Definição 1.34. *Um subgrupo N de um grupo G é dito subgrupo normal de G se ele satisfaz qualquer uma das condições equivalentes da proposição anterior.*

Definição 1.35. *Sejam G e H gupos e f o elemento neutro de H. O núcleo de um homomorfismo $\phi : G \longrightarrow H$ é o conjunto*

$$Nuc(\phi) = \{g \in G : \phi(g) = f\}.$$

A imagem do homomorfismo ϕ é definida por

$$Im(\phi) = \{\phi(g) : g \in G\}.$$

Corolário 1.36. *Seja $\phi : G \longrightarrow H$ um homomorfismo de grupos. Então $Nuc(\phi)$ é um subgrupo de G e $Im(\phi)$ é um subgrupo de H.*

Demonstração. Seja e o elemento neutro de H. Aplicando $N = \{e\}$ e K = G uma vez que $\phi^{-1}(\{e\}) = Nuc(\phi)$ e $\phi(G) = Im(\phi)$.

□

Definição 1.37. *Se N é um subgrupo normal de um grupo G então o grupo G/N é chamado de grupo quociente de G por N.*

Teorema 1.38. *Suponha que $\phi : G \to H$ é um homomorfismo de grupos. Então $G/Nuc(\phi)$ é um grupo isomorfo a $Im(\phi)$. Em particular, se ϕ é sobrejetora então que $G/Nuc(\phi)$ é isomorfo a H.*

Demonstração. Basta aplicar $N = \{e\}$. □

Em particular, se G é um grupo finito, temos que

$$\circ(G/Nuc(\phi)) = \circ(G)/\circ(Nuc(\phi)) = \circ(Im(\phi))$$

E, portanto, $\circ(G) = \circ(Nuc(\phi))\circ(Im(\phi))$.

Capítulo 2

Teoria de Anéis

Apresentaremos agora alguns resultados sobre a estrutura algébrica de anel. Além disso, veremos algumas classes importantes de anéis que são os domínios de integridade, os anéis de divisão e os corpos, os subanéis de um anel, que são subconjuntos do anel que também são anéis, e os homomorfismo de anéis, que são aplicações entre anéis que preservam estas estruturas algébricas. Esse capítulo foi baseado na referência [1] e [5].

2.1 Conceito de Anel

Um anel é um conjunto não vazio A munido de duas operações internas, uma chamada por soma, e denotada por $+$, e outra chamada de multiplicação, e denotada por $\cdot$, satisfazendo as seguintes propriedades:

1. O conjunto A é um grupo abeliano em relação a soma, isto é:
   a) Para quaisquer $a, b \in A$ tem-se $a + b = b + a$.
   b) Para quaisquer $a, b, c \in A$ tem-se $a + (b + c) = (a + b) + c$.
   c) Existe $0 \in A$ tal que $a + 0 = a$ para qualquer $a \in A$.
   d) Para qualquer $a \in A$ existe $-a \in A$ tal que $a + (-a) = 0$.

2. O conjunto A é associativo e distributivo em relação a multiplicação, isto é:
   a) Para quaisquer $a, b, c \in A$ tem-se $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
   b) Para quaisquer $a, b, c \in A$ tem-se $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(b + c) \cdot a = b \cdot a + c \cdot a$.

Definição 2.1. *Nas condições apresentadas acima dizemos que o conjunto A é um anel em relação à adição e à multiplicação consideradas. Ou ainda, que a terna ordenada formada* *pelo conjunto A, a adição e a multiplicação $(A, +, \cdot)$ é um anel. Às vezes diremos apenas "A é um anel"ou falaremos do "anel A", por simplificação de linguagem, mas isso pressupõe um par de leis de composições internas em A.*

Definição 2.2. *Um anel $(A, +, \cdot)$ é dito anel com unidade se existe $1 \in A$ satisfazendo $1 \cdot a = a \cdot 1 = a$.*

Definição 2.3. *Um anel $(A, +, \cdot)$ é dito anel comutativo se satisfaz $a \cdot b = b \cdot a$ para todos $a, b \in A$.*

Exemplo 2.4. *Consideremos em $\mathbb{Z}$ as operações usuais de soma e multiplicação de números inteiros. Observe que $(\mathbb{Z}, +, \cdot)$ é um anel comutativo com unidade.*

Exemplo 2.5. *Cada conjunto $\overline{\mathbb{Z}}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$, $\forall m \in \mathbb{Z}, m > 1$, é um anel em relação às operações já definidas.*

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

$$e$$

$$\begin{array}{rcl} \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m \\ (\overline{a}, \overline{b}) & \mapsto & \overline{a}\overline{b} = \overline{ab} \end{array}$$

$$\overline{a}\overline{b} = \overline{ab}, \forall \overline{a}, \overline{b}, \in \overline{\mathbb{Z}}_m$$

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a}(\overline{b+c}) = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = \overline{a}\overline{b} + \overline{ac}$$

Portanto, $\mathbb{Z}_m$ é distributiva.
Logo $\overline{\mathbb{Z}}_m$ é um anel $(\overline{\mathbb{Z}}, +, \cdot)$

Exemplo 2.6. *Consideremos os conjuntos $M_n(\mathbb{Z})$ com $\forall n \geqslant 1$. Sabemos que as propriedades sobre matrizes quadradas é o suficiente para podermos dizer agora que cada $M_n(\mathbb{Z})$ é um anel em relação a adição e a multiplicação de matrizes $n \times n$.*

Sejam as matrizes $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, , $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, e $C = \begin{bmatrix} i & j \\ k & l \end{bmatrix}$, temos que $(M_n(\mathbb{Z}), +, \cdot)$ é um anel, pois $(M_n(\mathbb{Z}), +)$ é um grupo abeliano e $A(BC) = (AB)C$ é associativo, e também, $A(B+C) = (AB) + (AC)$ é distributivo.

Consideremos um anel $(A, +, \cdot)$

(a) Quanto à adição, A é um grupo abeliano. Então são verdadeiras as seguintes propriedades:

O zero do anel A é único; Para cada $a \in A$ existe um único simétrico aditivo;

Dados $a_1, ..., a_n \in A (n \geq 2)$, $-(a_1 + ... + a_n) = (-a_1) + ... + (-a_n)$

$$\forall a \in A \quad -(-a) = a$$
$$\forall a, x, y \in A \;\; a + x = a + y \Longrightarrow x = y)$$

O conjunto-solução de uma equação $a + x = b$, onde a e b são elementos dados de A e x é variável em A é $\{(-a) + b\}$.

(b) $(\forall a \in A \Longrightarrow a0 = 0a = 0)$ Com efeito,

$$0 + a0 = a0 = a(0 + 0) = a0 + a0$$

Assim, $0 = a0$. Por outro lado, temos que,

$$0 + 0a = 0a = (0 + 0)a = 0a + 0a.$$

Segue que, $0 = 0a$.

(c) $(\forall a, b \in A \Longrightarrow a(-b) = (-a)b = -(ab))$ De fato,

$$ab + [-(ab)] = 0 = a0 = a[b + (-b)] = ab + a(-b)$$
$$\text{então, } -(ab) = a(-b)$$

por outro lado, temos

$$ab + [-(ab)] = 0 = 0b = [a + (-a)]b = ab + (-a)b$$
$$\text{assim, } -(ab) = (-a)b.$$

(d) $(\forall a, b \in A \Longrightarrow ab = (-a)(-b))$, pois,

$$(-a)(-b) = -[(-a)b] = -[-(ab)] = ab.$$

Definição 2.7. *Dados dois elementos a e b de um anel A, a diferença entre a e b, que indicaremos por $a - b$, é o elemento $a + (-b)$. Assim, $a - b = a + (-b)$.*

(e) $\forall a, b, c \in A \Longrightarrow a(b - c) = ab - ac$, pois,

$a(b - c) = a[b + (-c)] = ab + a(-c) = ab + [-(ac)] = ab - ac.$

Definição 2.8. *Dados $a \in A$ e $n \in \mathbb{N}^*$, defini-se a^n por recorrência do seguinte modo:*

$$a^1 = a \text{ e } a^n = a^{n-1}a \ (\forall n > 1).$$

(f) $\forall a \in A$ e $\forall m, n \in \mathbb{N}^*$ tem-se $a^m a^n = a^{m+n}$

provaremos essa propriedade por indução sobre n, Suponhamos $n = 1$. Então, $a^m a^1 = a^m a = a^{m+1}$, pela própria definição. Suponhamos $a^m a^r = a^{m+r}$ e mostraremos que a afirmação vale para $n = r + 1$. Então,

$$a^m a^{r+1} = a^m(a^r a^1) = (a^m a^r)a^1 = a^{m+r}a = a^{(m+r)+1} = a^{m+(r+1)}.$$

(g) $\forall a \in A$ e $\forall m, n \in \mathbb{N}^*$ tem-se $(a^m)^n = a^{mn}$.

A demonstração será feita por indução sobre n.

Para $n = 1$, temos que $(a^m)^1 = a^m$, por definição. Suponhamos $(a^m)^r = a^{mr}$, com $r \geq 1$. Então,

$$(a^m)^{r+1} = (a^m)^r a^m = a^{mr}a^m = a^{mr+m} = a^{m(r+1)},$$

Isto é, a afirmação vale para $n = r + 1$ e, consequentemente, está provada.

2.2 Subanéis

Definição 2.9. *Seja $(A, +, \cdot)$ um anel. Dizemos que um subconjunto $L \subset A, L \neq \phi$, é um subanel de A se, e somente se,* *i) L é fechado para ambas as operações de A, isto é,*

$$\forall a, b \in A \Longrightarrow a + b \in L \text{ e } a \cdot b \in L.$$

ii) $(L, +, \cdot)$ também é um anel.

Exemplo 2.10. *O conjunto dos números pares, $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. De fato, a soma e o produto de dois números pares são números pares. Além disso, tanto a adição como a multiplicação de números pares são associativas, a adição é comutativa, o número zero é par e o oposto de um número par é também um número par. Finalmente a multiplicação de números pares é distributiva em relação à adição.*

Exemplo 2.11. *$M_n(\mathbb{Z})$ é um subanel de $M_n(\mathbb{R})$.*

Proposição 2.12. *Sejam A um anel e L um subconjunto de A. Então L é um subanel de A se, e somente se,*

$$\forall a, b \in L \Longrightarrow a - b \in L \text{ e } ab \in L,$$

ou seja, L é fechado para a subtração e para a multiplicação de A.

Demonstração. $(\Longrightarrow)$ Por hipótese $(L, +)$ é um subgrupo do grupo $(A, +)$. Logo,

$$\forall a, b \in L \Longrightarrow a - b \in L.$$

Por hipótese, L é fechado para a multiplicação de A. Isto conclui a demonstração desta parte.
$(\Longleftarrow)$ Da hipótese

$$a, b \in L \Longrightarrow a - b \in L$$

decorre que L é um subgrupo de $(A, +)$. Logo $(L, +)$ é um grupo abeliano.
Por outro lado, como $L \subset A$ e L é fechado para a multiplicação de A, então

$$\forall a, b, c \in L \Longrightarrow a, b, c \in A \Longrightarrow a(bc) = (ab)c$$

é a propriedade associativa da multiplicação em L e

$$\forall a, b, c \in L \Longrightarrow a, b, c \in A \Longrightarrow a(b + c) = ab + ac \text{ e } (a + b)c = ac + bc$$

é a propriedade distributiva da multiplicação em relação à adição em L. $\square$

Exemplo 2.13. *Seja A um anel das funções definidas em um intervalo fechado [a,b] e a valores vonjunto dos números reais $\mathbb{R}$. Para $c \in [a, b]$ definamos $B = \{f \in A : f(c) = 0\}$. B é um subanel A. Com efeito, se $f_1 e f_2 \in B$, então*

$$(f_1 + f_2)(c) = f_1(c) + f_2(c) = 0 + 0 = 0$$
$$(-f_1)(c) = -(f_1(c)) = -0 = 0$$
$$(f_1 \cdot f_2)(c) = f_1(c) \cdot f_2(c) = 0 \cdot 0 = 0$$

e, portanto, $f_1 + f_2$, $-f_1$ $f_1 \cdot f_2 \in B$.

Sejam A um anel e L um subanel de A. Suponhamos que A é um anel com unidade. Quanto a L poderá então acontecer o seguinte: ou não tem unidade, ou tem unidade igual a de A ou L tem unidade e esta é diferente da de A. Vejamos no exemplo abaixo.

Exemplo 2.14. *a) $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Existe a unidade de $\mathbb{Z}$ mas não a de $2\mathbb{Z}$.*

b) $\mathbb{Z}$ é subanel de $\mathbb{Q}$ e ambos admitem a mesma unidade.

c) Considerando o produto direto $\mathbb{Z} \times \mathbb{Z}$ verifica-se que $\{0\} \times \mathbb{Z}$ é um subanel de $\mathbb{Z} \times \mathbb{Z}$. Contudo, enquanto que $(1, 1)$ é a unidade de $\mathbb{Z} \times \mathbb{Z}$, a de $\{0\} \times \mathbb{Z}$ é $(0, 1)$ pois $(0, 1)(0, b) = (0, b)$, $\forall (0, b) \in \{0\} \times \mathbb{Z}$.

Seja A um anel de integridade e B um subanel de A com unidade. Como $1_A \cdot 1_B = 1_B = 1_B \cdot 1_B$, então $1_A = 1_B$.

Se A é um anel com unidade e se B é um subanel de A tal que existe unidade de B e $1_A = 1_B$, então diremos que B é um subanel unitário de A.

Consideremos o anel $\mathbb{Z}$ dos inteiros e o anel $\mathbb{Z}_{\mathbb{Z}}$ das funções de $\mathbb{Z}$ em $\mathbb{Z}$. Ambos são anéis comutativos com unidade. Contudo há uma diferença fundamental entre os dois. Enquanto que no anel $\mathbb{Z}$ é verdadeira a frase

$$\forall a, b \in \mathbb{Z} \; ab = 0 \Longrightarrow a = 0 \text{ ou } b = 0,$$

no anel $\mathbb{Z}_{\mathbb{Z}}$ não acontece o mesmo. De fato, consideremos as funções f e g de $\mathbb{Z}$ em $\mathbb{Z}$ dadas por

$$f(0) = 1 \text{ e } f(x) = 0, \forall x \neq 0, \tag{2.1}$$

$$g(0) = 0 \text{ e } g(x) = 1, \forall x \neq 0. \tag{2.2}$$

Trata-se obviamente de duas funções não nulas. Apesar disso o produto fg é nulo pois

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

e, para todo $x \neq 0$,

$$(fg)(x) = f(x)g(x) = 0 \cdot 1 = 0.$$

Esse tipo de observação motiva a definição a seguir.

Definição 2.15. *Um anel A, comutativo com unidade, è um anel de integridade*

$$\textit{Se } ab = 0_A \Longrightarrow a = 0_A \textit{ ou } b = 0_A, \textit{ para todos } a, b \in A$$

A expressão acima é chamada lei do anulamento do produto. Logo, um anel de integridade é um anel comutativo com unidade em que vale a lei do anulamento do produto. Se a e b são elementos não nulos de um anel A tais que $ab = 0_A$ ou $ba = 0_A$, dizemos que a e b são divisores próprios do zero em A.

Uma outra maneira de afirmar que um anel é de integridade é dada pela proposição abaixo.

Proposição 2.16. *Um anel A, comutativo com unidade, é um anel de integridade se, e somente se, todo elemento não nulo de A é regular quanto a multiplicação, isto é,*

$$\forall a, b, c \in A, \textit{ com } a \neq 0,\ ab = ac \Longrightarrow b = c.$$

Demonstração. ($\Longrightarrow$) Tomando $a \neq 0$ e supondo $ab = ac$, com $a, b, c \in A$, então $a(b - c) = 0$. Devido à hipótese podemos concluir então que $b - c = 0$, ou seja, $b = c$.
($\Longleftarrow$) Se existissem $a, b \in A$, ambos não nulos, de maneiras que $ab = 0$, teríamos $ab = a0$. Daí (pela hipótese): $b = 0$. O que é um absurdo. $\square$

Exemplo 2.17. *Já sabemos que todo anel $\mathbb{Z}_m$ de classes de restos é um anel comutativo com unidade. Mostraremos a seguir que $\mathbb{Z}_m$ é anel de integridade se, e somente se, m é primo.*
($\Longrightarrow$) *Se m não fosse primo, existiriam $r, s \in \mathbb{Z}$, de tal forma que $1 < r,\ s < m$ e $rs = m$. Daí $0 = m = rs$. Quer dizer, existiriam divisores próprios do zero em $\mathbb{Z}_m$ o que seria contrário à hipótese.*

($\Longleftarrow$) *Suponhamos que existissem* $a, b \in \mathbb{Z}_m$ *tais que* $ab = 0$. *Então* $m|ab$. *Como* m *é primo, conclui-se que* $m|a$ *ou* $m|b$. *Isto significa que* $a = 0$ *ou* $b = 0$.

Os anéis $\mathbb{Z}$ e $\mathbb{Q}$ são ambos comutativos com unidade. Para ambos vale a lei do anulamento do produto. Mas, enquanto que no anel $\mathbb{Z}$ somente os elementos 1 e -1 admitem simétrico multiplicativo, no anel $\mathbb{Q}$ todo elemento não nulo admite simétrico multiplicativo. Fatos como esse sugerem a definição a seguir.

Definição 2.18. *Um anel* K*, comutativo com unidade, recebe o nome de corpo se todo elemento não nulo de* K *admite simétrico multiplicativo, ou seja*

$$\forall a \in K, a \neq 0, \text{ existe } b \in K \text{ tal que } ab = 1.$$

O elemento b *descrito acima é chamado inverso de* a *e será indicado, daqui para a frente, por* a^{-1}.

Num anel A com unidade indicaremos por $U(A)$ o subconjunto de A formado pelos elementos para os quais existe simétrico multiplicativo (inverso). Esses elementos são chamados de inversíveis. Assim, um corpo K é um anel comutativo com unidade tal que $U(K) = K^* = K - 0$.

Proposição 2.19. *Todo corpo* K *é um anel de integridade.*

Demonstração. Sejam a e b elementos de K tais que $ab = 0$. Suponhamos que um deles, por exemplo a, é não nulo. Então existe $a^{-1} \in K$. E $a^{-1}(ab) = a^{-1}0$ segue que $(a^{-1}a)b = 0$ e, assim, $b = 0$.
Assim provamos que vale a lei do anulamento do produto em K. □

Proposição 2.20. *Todo anel de integridade finito é um corpo.*

Demonstração. Seja $K = \{a_1, a_2, ..., a_n\}$ um anel de integridade formado de n elementos. Para todo $a \in K$, com $a \neq 0$, a aplicação

$$a_i \longrightarrow aa_i$$

é injetora, de K nele próprio, uma vez que

$$aa_i = aa_j \Longrightarrow a_i = a_j.$$

Como K é finito essa aplicação é também sobrejetora, do que resulta

$$aK = \{aa_1, aa_2, ..., aa_n\} = K.$$

Então a unidade de K poderá ser expressa do seguinte modo:

$$1 = aa_r,$$

onde a_r é um elemento conveniente de K. Dessa forma mostramos que todo elemento não nulo $a \in K$ possui inverso. □

2.3 Homomorfismos de Anéis

Sejam A e B anéis arbitrários. Dentre as aplicações existentes de A em B, têm importância destacada aquelas que "preservam"as leis de composição internas que fazem de A e B anéis, conforme estamos considerando.

Definição 2.21. *Sejam A e B dois anéis. Uma aplicação $f : A \longrightarrow B$ é chamada homomorfismo de A em B se as seguintes condições de verificam:*

(i) $(\forall x, y)(x, y \in A \Longrightarrow f(x + y) = f(x) + f(y))$

(ii) $(\forall x, y)(x, y \in A \Longrightarrow f(xy) = f(x)f(y))$.

Exemplo 2.22. *Sejam $A = \mathbb{Z}$ e $B = \mathbb{Z} \times \mathbb{Z}$ (produto direto). A aplicação $f : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, dada por $f(x) = (x, 0)$, $\forall x \in \mathbb{Z}$, é um homomorfismo de anéis porque*

$$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y) \text{ e}$$
$$f(xy) = (xy, 0) = (x, 0)(y, 0) = f(x)f(y)$$

Definição 2.23. *Dado um homomorfismo de anéis $f : A \longrightarrow B$, o núcleo de f é o subconjunto $N(f) \subset A$, definido da seguinte maneira:*

$$N(f) = \{x \in A : f(x) = 0_B\}.$$

Assim como vimos em grupos, podemos também definir isomorfismo de anéis. A seguir temos a definição sobre isomorfismo de anéis.

Definição 2.24. *Sejam A e B anéis quaisquer. Uma aplicação $f : A \longrightarrow B$ é chamada isomorfismo de A em B se*

(i) f é bijetora;

(ii) f é um homomorfismo de anéis.

Exemplo 2.25. *Sejam A e B anéis arbitrários. Indiquemos o zero do anel B simplesmente por 0. Sendo assim, se construirmos o produto direto $A \times B$, o subconjunto $A \times \{0\}$ é um subanel de $A \times B$. De fato além de $A \times \{0\}$ ser um subconjunto não vazio, temos, para $(a, 0), (b, 0) \in A \times \{0\}$ que*

$$(a, 0) - (b, 0) = (a - b, 0) \in A \times \{0\} \text{ e } (a, 0)(b, 0) = (ab, 0) \in A \times \{0\}.$$

Tal subanel é isomorfo ao anel A mediante a aplicação $f : A \longrightarrow A \times \{0\}$ dada por $f(x) = (x, 0), \forall x \in A$. Com efeito,

(a) $f(x) = f(y) \Longrightarrow (x, 0) = (y, 0) \Longrightarrow x = y$. Logo f é injetora.

(b) Dado $(b, 0) \in A \times \{0\}$, é claro que tomando $b \in A$ teremos $f(b) = (b, 0)$. Isso mostra que f é sobrejetora.

(c) $\forall x, y \in A, f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y)$

(d) $\forall x, y \in A, f(xy) = (xy, 0) = (x, 0) \cdot (y, 0) = f(x) \cdot f(y)$.

2.4 Ideais

Definição 2.26. *Seja A um anel comutativo. Dizemos que um subconjunto $I \subset A$, $I \neq \phi$, é um ideal em A se, e somente se,*

(i) $(\forall x, y)(x, y \in I \Longrightarrow x - y \in I)$;

(ii) $(\forall a, x)(a \in A \text{ e } x \in I \Longrightarrow ax \in I)$.

Exemplo 2.27. *No anel* $\mathbb{Z}$ *dos inteiros todos os subconjuntos* $n\mathbb{Z} = \{nq | q \in \mathbb{Z}\}$, *onde* n *é o número inteiro dado, são ideais. De fato:*

i $0 \in n\mathbb{Z}$ *uma vez que* $0 = n0$.

ii $nq_1 - nq_2 = n(q_1 - q_2) \in n\mathbb{Z}$.

iii $a(nq) = n(aq) \in n\mathbb{Z}, \forall a \in \mathbb{Z}$.

Exemplo 2.28. *Para todo anel* A *são ideais em* A, *os subconjuntos* $\{0\}$ *e* A *eles são chamados ideais triviais de* A.

Exemplo 2.29. *Seja* A *o anel das funções de* $\mathbb{R}$ *em* $\mathbb{R}$. *Mostraremos que é ideal em* A *o seguinte subconjunto de* $A : I = \{f : \mathbb{R} \longrightarrow \mathbb{R} | f(1) = 0\}$.

i A função nula pertence a I *pois evidentemente se anula no ponto* 1.

ii Sejam f *e* g *funções de* I. *Então* $f(1) = g(1) = 0$. *Donde* $(f - g)(1) = f(1) - g(1) = 0 - 0 = 0$. *Ou seja,* $f - g \in I$.

iii Seja f *uma função de* I *e* h *uma função de* A. *Então* $(hf)(1) = h(1)f(1) = h(1) \cdot 0 = 0$. *Logo* $hf \in I$.

Exemplo 2.30. *Seja* $f : A \longrightarrow B$ *um homomorfismo de anéis. Mostremos que o núcleo* $N(f)$ *é um ideal em* A. *Lembremos que* $N(f) = \{x \in A \mid f(x) = 0_B \text{ (zero de } B)\}$.

? *Como* $f(0_A) = 0_B$, *então* $0_A \in N(f)$

? *Suponhamos* $x, y \in N(f)$. *Então* $f(x) = f(y) = 0$. *Daí* $f(x - y) = f(x) - f(y) = 0 - 0 = 0$. *Donde* $x - y \in N(f)$.

? *Suponhamos* $x \in N(f)$ *e* $a \in A$. *Então* $f(ax) = f(a)f(x) = f(a)0 = 0$ *o que quer dizer que* $ax \in N(f)$.

Nota: É claro que todo ideal num anel A é um sub anel de A. Contudo a recíproca não vale. Por exemplo, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$ mas não é um ideal em $\mathbb{Q}$. Basta notar que $1 \in \mathbb{Z}, \frac{1}{2} \in \mathbb{Q}$, mas $\frac{1}{2} \cdot 1 = \frac{1}{2}$ não pertence ao conjunto dos inteiros $\mathbb{Z}$.

Proposição 2.31. *Seja I um ideal num anel comutativo A. Então:*

(a) $0 \in I$ *(Isto é, o zero de A pertence a I);*

(b) $(\forall a)\ (a \in I \Longrightarrow -a \in I)$*;*

(c) $(\forall a, b)\ (a, b \in I \Longrightarrow a + b \in I)$*;*

(d) Se o anel A possui unidade e se existe um elemento inversível $u \in A$ tal que $u \in I$, então $I = A$.

Demonstração. (a) $I \neq \phi \Longrightarrow \exists a \in I \Longrightarrow a - a \in I \Longrightarrow 0 \in I$.

(b) $a \in I$, por hipótese, e $0 \in I$, devido à parte (a). Logo, $0 - a \in I$, isto é, $a \in I$.

(c) Como a e b pertencem a I, por hipótese, então a e $-b$ pertencem a I; logo, $a-(-b) \in I$. Donde $a + b \in I$.

(d) Seja $a \in I$. Podemos escrever $a = a \cdot 1$. Como u é inversível, existe um elemento $v \in A$ de maneira que uv=1. De onde $a = (au)v$ e usando a condição (ii) da definição, temos:

$$a \in A \text{ e } u \in I \Longrightarrow au \in I$$
$$au \in I \text{ e } v \in A \Longrightarrow (au)v \in I$$

e podemos concluir que $a \in I$. Provamos assim que $A \subset I$. Como obviamente $I \subset A$, então temos a igualdade proposta.

$\square$

CAPÍTULO 3

Álgebras de Lie

Apresentaremos agora uma introdução à teoria das álgebras de Lie, as quais nos baseamos na referência [1]. Iniciaremos apresentando as definições básicas de álgebra linear e, na sequência, um pouco da estrutura algébrica das álgebras de Lie. Para um estudo mais completo sobre as álgebras de Lie, sugere-se ler as referências [10] e [**?**]

3.1 Conceitos básicos de Álgebra Linear

Vamos apresentar alguns conceitos de álgebra linear que necessitamos para explorar a noção de álgebra de Lie. Esta seção foi baseada nas referências [2], [7] e [**?**].

Definição 3.1. *Um espaço vetorial sobre um corpo de escalares $\mathbb{F}$ é um conjunto não vazio, com duas operações: soma, $V \times V \xrightarrow{+} V$, e multiplicação por escalar, $\mathbb{F} \times V \xrightarrow{\cdot} V$, tais que para quaisquer u, v e $w \in \mathbb{R}$, as propriedades abaixo estão satisfeitas.*

Para a operação de soma:

i) Associatividade: $u + (v + w) = (u + v) + w$; para todo u, v e $w \in V$.

ii) Comutatividade: $u + v = v + u$; para todo $u, v \in V$.

iii) Elemento Neutro: Existe um elemento $0 \in V$ tal que $u + 0 = u$, para todo $u \in V$.

iv) Elemento Simétrico: Para todo elemento $u \in V$ existe o elemento $-u \in V$ tal que $u + (-u) = 0$; para todo $u \in V$.

Para a operação de multiplicação:

v) Distributividade para a Adição de Elementos: $a(u+v) = au + av$; para todo $u, v \in V$ e $\forall\ a \in \mathbb{F}$.

vi) Distributividade para a Multiplicação por Escalar: $(a+b)v = av + bv$*; para todo* $v \in V$ *e para todo* $a, b \in \mathbb{F}$*.*

vii) Associatividade: $(ab)v = a(bv)$*; para todo* $v \in V$ *e para todo* $a, b \in \mathbb{F}$*.*

viii) Elemento Identidade: $1u = u$ *; para todo* $u \in V$*.*

Os elementos de um espaço vetorial usualmente são chamados de vetores.

Note que um espaço vetorial é considerado um grupo abeliano com a operação de soma.

Muitos dos resultados descritos nesse trabalho valem para qualquer corpo de escalares, contudo, daqui para frente, vamos trabalhar somente com espaços vetoriais em que $\mathbb{F} = \mathbb{R}$, ou seja, os espaços vetoriais sobre $\mathbb{R}$. A teoria de espaços vetoriais sobre $\mathbb{C}$ ou sobre um corpo qualquer pode ser vista em [7]. Para mais informações sobre corpo e suas propriedades, ver

Exemplo 3.2. *O conjunto dos números reais, com as operações de soma e multiplicação usuais de números reais, é um espaço vetorial real.*

Exemplo 3.3. *O conjunto* $M(m \times n, \mathbb{R})$*, das matrizes* m *por* n *com entradas reais.*

i) Soma. *Dadas* $A = (a_{ij}), B = (bij) \in M_{n\times m}(\mathbb{R})$*, a soma de* A *com* B*,* $A+B$*, é definida por*

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \cdots & a_{1n} + b_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \cdots & a_{mn} + b_{mn} \end{pmatrix}.$$

ii) Multiplicação por escalar. *Sejam* $A = (a_{ij}) \in M_{n\times m}(\mathbb{R})$ *e* $\alpha \in \mathbb{R}$*. O produto de* α *por* A*,* αA*, é definida por*

$$\alpha A = \begin{pmatrix} \alpha a_{11} & \alpha a_{12} & \cdots & \alpha a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha a_{m1} & \alpha a_{m2} & \cdots & \alpha a_{mn} \end{pmatrix}.$$

O conjunto $M(m \times n, \mathbb{R})$*, com as operações de soma e multiplicação por escalar dadas acima, é um espaço vetorial real.*

Definição 3.4. *Dado um espaço vetorial* V*, um subconjunto* W*, não vazio, é um subespaço vetorial de* V *se* W *é um espaço vetorial com as operações de adição e multiplicação por escalar em* V*.*

Para verificar que um conjunto é um subespaço vetorial não precisamos analisar todas as propriedades de espaço vetorial, mas apenas duas propriedades.

Teorema 3.5. *Um subconjunto não vazio U de um espaço vetorial V é um subespaço vetorial de V se, e somente se, para quaisquer elementos u, $v \in U$ e para qualquer escalar $\alpha \in \mathbb{R}$, tem-se que $u + v \in U$ e $\alpha u \in U$, isto é, U é fechado com relação as operações de soma e multiplicação por escalar.*

Demonstração. ($\Longrightarrow$) Se U é um subespaço vetorial V, então satisfaz as propriedades de espaço vetorial, em particular as propriedades de fechamento.

($\Longleftarrow$) Agora, serão mostradas que se U satisfaz as propriedades de fechamento, então satisfaz as propriedades da adição de elementos e da multiplicação por escalar. Como $U \subset V$, as propriedades comutativa e associativa da adição são automaticamente satisfeitas, pois são válidas para todos os elementos de V. De modo análogo, as propriedades: associatividade, distributividade para adição de elementos, distributividade para a multiplicação por escalar e a do elemento identidade da operação de multiplicação por escalar, são automaticamente satisfeitas. Agora será provada as propriedades do elemento neutro e do elemento simétrico da operação de adição.

Para quaisquer $u \in U$ e $\lambda \in \mathbb{R}$, temos que $\lambda u \in U$. Fazendo $\lambda = 0$, obtemos $0u = 0 \in U$. Logo, U possui elemento neutro.

Para quaisquer $u \in U$ e $\lambda \in \mathbb{R}$, temos que $\lambda u \in U$. Fazendo $\lambda = -1$, obtemos $-1u = 1(-u) = -u \in U$. Logo, todo elemento de U possui o elemento simétrico. O que completa a demonstração. □

Exemplo 3.6. *Se V é um espaço vetorial, então V é um subespaço vetorial dele próprio. O subespaço $W = \{0\}$ é um subespaço vetorial de V, dito subespaço nulo.*

Exemplo 3.7. *Seja $V = \mathbb{R}^5$ um espaço vetorial e $W = \{(0, x_2, x_3, x_4, x_5);\ x_i \in \mathbb{R}\}$. Isto é, W é o conjunto dos vetores de $\mathbb{R}^5$, cuja primeira coordenada é nula.*

Verifiquemos as condições (i) e (ii) do teorema interior:

i) Sejam $u = (0, x_2, x_3, x_4, x_5)$ e $v = (0, y_2, y_3, y_4, y_5) \in W$.

Então $u + v = (0, x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5)$ *que ainda pertence a* W*, pois tem a primeira coordenada nula.*

ii) $ku = (0, kx_2, kx_3, kx_4, kx_5) \in W$*, pois a primeira coordenada é nula.*

Portanto, W *é um subespaço vetorial de* $\mathbb{R}^5$*.*

Definição 3.8. *Sejam* V *um espaço vetorial real,* $v_1, v_2, \cdots, v_n \in V$ *e* $a_1, a_2, \cdots, a_n$ *números reais. Então, o vetor*

$$v = a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

é um elemento de V *ao que chamamos Combinação Linear de* $v_1, v_2, \cdots, v_n$*.*

Definição 3.9. *Sejam* V *um espaço vetorial e* $v_1, \cdots, v_n \in V$*. Dizemos que o conjunto* $\{v_1, \cdots, v_n\}$ *é Linearmente Independente (LI), ou que os vetores* $v_1, \cdots, v_n$ *são LI, se a equação*

$$a_1v_1 + \cdots + a_nv_n = 0, \tag{3.1}$$

implica que $a_1 = a_2 = \cdots = a_n = 0$*. No caso em que exista algum* $a_i \neq 0$ *que satisfaz a Equação (3.1), dizemos que* $\{v_1, \cdots, v_n\}$ *é linearmente dependente (LD), ou que os vetores* $v_1, \cdots, v_n$ *são LD.*

Podemos ainda caracterizar os vetores linearmente dependentes de outra maneira.

Teorema 3.10. *O conjunto* $\{v_1, \cdots, v_n\}$ *é LD se, e somente se, um destes vetores for uma combinação linear dos outros.*

Demonstração. Sejam $v_1, \cdots, v_n$ vetores LD e

$$a_1v_1 + \cdots + a_jv_j + \cdots + a_nv_n = 0.$$

Por definição, um dos coeficientes deve ser diferente de zero. Suponhamos que $a_j \neq 0$. Então

$$v_j = -\frac{1}{a_j}(a_1v_1 + \cdots + a_{j-1}v_{j-1} + a_{j+1}v_{j+1} + \cdots + a_nv_n),$$

e portanto,

$$v_j = -\frac{a_1}{a_j}v_1 + \cdots - \frac{a_n}{a_j}v_n.$$

Logo, v_j é uma combinação linear dos outros vetores. Por outro lado, se tivermos $\{v_1, \cdots, v_j, \cdots, v_n\}$ tal que para algum j,

$$v_j = b_1 v_1 + \cdots + b_{j-1} v_{j-1} + b_{j+1} v_{j+1} + \cdots + b_n v_n,$$

temos,

$$b_1 v_1 + \cdots - 1 v_j + \cdots + b_n v_n = -1 \quad \text{e},$$

portanto, $\{v_1, \cdots, v_n\}$ é LD. $\square$

Exemplo 3.11. *Seja o espaço vetorial* $V = \mathbb{R}^2$ *e* $e_1 = (1, 0)$ *e* $e_1 = (0, 1)$*, vetores de* V*.*

Os vetores e_1 *e* e_2 *são LI, pois*

$$\begin{aligned} a_1 e_1 + a_2 e_2 &= 0 \\ a_1(1, 0) + a_2(0, 1) &= (0, 0) \\ (a_1, a_2) &= (0, 0). \end{aligned}$$

Logo, $a_1 = 0$ *e* $a_2 = 0$*.*

Definição 3.12. *Um conjunto* $\{v_1, \cdots, v_n\}$ *de vetores de* V *será uma base de* V *se:*

i) $\{v_1, \cdots, v_n\}$ *é LI,*

ii) $[v_1, \cdots, v_n] = V$*.*

De acordo com o resultado a seguir, uma base caracteriza os vetores de um espaço vetorial, pois vetores diferentes são escritos de maneira distinta como combinação linear dos elementos da base.

Teorema 3.13. *Dada uma base* $\beta = \{v_1, v_2, \cdots, v_n\}$ *de* V*, cada vetor de* V *é escrito de maneira única como combinação linear de* $v_1, v_2, \cdots, v_n$*.*

Exemplo 3.14. *Considere o espaço vetorial real* $\mathbb{R}^3$*. O conjunto*

$$\beta = [(1, 0, 0), (0, 1, 0), (0, 0, 1)] \text{ é uma base de } \mathbb{R}^3.$$

Dado $(x, y, z) \in \mathbb{R}^3$*, então podemos escrevê-los como combinação linear dos vetores em* β*,*

$$(x, y, z) = x(1, 0, 0) + y(0, 1, 0) + z(0, 0, 1).$$

Logo β gera $\mathbb{R}^3$. E ainda é LI, pois:

$$\begin{aligned}(x,y,z) &= x(1+0+0)+y(0+1+0)+z(0+0+1)=(0,0,0)\\ &= (x,y,z)=(0,0,0).\end{aligned}$$

Ou seja, $x=y=z=0$. Então temos que β é linearmente independente em $\mathbb{R}^3$ e gera o espaço $\mathbb{R}^3$.

Logo, β é uma base para $\mathbb{R}^3$, denominada base canônica.

Definição 3.15. *Seja V um espaço vetorial real. Dizemos que V é um espaço vetorial de dimensão finita se V possui uma base finita.*

Definição 3.16. *Sejam V um espaço vetorial e α uma base qualquer de V. O número de elementos de α é chamado de Dimensão de V, e denotado $dimV$.*

Exemplo 3.17. *Seja o espaço vetorial $V=\mathbb{R}^2$.*

Como $\{(1,0),(0,1)\}$ e $\{(1,1),(0,1)\}$ são bases de V. Então dim $V=2$.

Vamos definir conjuntos que são translações de subespaços vetoriais.

Sejam V um espaço vetorial sobre $\mathbb{R}$ e W um subespaço de V. A relação

$$\{(u,v)\in V\times V : u-v\in W\}$$

é uma relação de equivalência sobre V. As classes de equivalência desta relação são da forma

$$v+W := \{u\in V : u-v\in W\}=\{v+w : w\in W\},$$

e são chamadas de subespaços afins de V, gerados por W. Subespaos vetoriais são subespaços afins, mas a recíproca nem sempre vale. Como subespaços afins são classes de equivalência, a intersecção de dois subespaços de dois subespaços afins é o conjunto vazio ou um subespaço afim. Denotaremos por V/W o conjunto de todos os subespaços afins de V. Definimos as seguintes operações sobre V/W:

1. Soma: $(u+w)+(v+w)=(u+v)+W$
2. Multiplicação por escalar: $\alpha(u+W)=(\alpha u)+W$,

para $u,v\in V$ e $\alpha\in\mathbb{R}$.

O espaço V/W com as operações de soma e multiplicação por escalar definidas acima é um espaço vetorial, chamado de espaço quociente de V por W.

Sejam V um espaço vetorial sobre $\mathbb{R}$ e W um subespaço de V. A codimensão de W em V é a dimensão de V/W sobre $\mathbb{R}$.

Exemplo 3.18. *No espaço $\mathbb{R}^3$, considere o subespaço $W = \{(\alpha, 0, 0) : \alpha \in \mathbb{R}\}$. Os elementos de $\mathbb{R}^3/W$ são da forma*

$$(\alpha, \beta, \gamma) + W = \{(\alpha, \beta, \gamma) + \lambda(1, 0, 0) : \lambda \in \mathbb{R}\}.$$

Geometricamente, os subespaços afins de $\mathbb{R}^3$ são retas com direção $(1, 0, 0)$.

Vamos iniciar este estudo introduzindo o conceito de colchete de Lie para matrizes quadradas. Sabendo que o produto de matrizes quadradas não é comutativo, definimos o colchete de duas matrizes quadradas A e B como o produto

$$AB - BA.$$

Usamos a notação $[A, B] = AB - BA$. Observe que se A e B comutam, então $[A, B] = 0$. Assim, o colchete pode ser interpretado como uma maneira de se medir a comutatividade do produto de matrizes.

A seguir, temos uma proposição mostrando algumas propriedades que são satisfeitas pelo colchete de matrizes quadradas.

Proposição 3.19. *Para quaisquer matrizes quadradas A, B e C e números reais a e b temos que:*

(1) O colchete é bilinear, ou seja, $[aA + bB, C] = a[A, C] + b[B, C]$ e $[C, aA + bB] = a[C, A] + b[C, B]$.

(2) Para toda matriz A vale a igualdade $[A, A] = 0$.

(3) A identidade de Jacobi

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

é satisfeita.

Demonstração. (1): Por definição de colchete de matrizes temos:

$$\begin{aligned} [aA+bB,C] &= (aA+bB)C - C(aA+bB) \\ &= aAC + bBC - aCA - bCB \\ &= a(AC-CA) + b(BC-CB) \\ &= a[A,C] + b[B,C]. \end{aligned}$$

e, por outro lado, temos

$$\begin{aligned} [C,aA+bB] &= C(aA+bB) - (aA+bB)C \\ &= aCA + bCB - aAC - bBC \\ &= a(CA-AC) + b(CB-BC) \\ &= a[C,A] + b[C,B] \end{aligned}.$$

(2): Note que:

$$\begin{aligned} [A,A] &= AA - AA \\ &= A^2 - A^2 \\ &= 0. \end{aligned}$$

Para qualquer matriz quadrada A.

(3): A identidade de Jacobi também é satisfeita, pois

$$\begin{aligned} & [A,[B,C]] + [B,[C,A]] + [C,[A,B]] \\ = \ & A[B,C] - [B,C]A + B[C,A] - [C,A]B + C[A,B] - [A,B]C \\ = \ & A(BC-CB) - (BC-CB)A + B(CA-AC) - (CA-AC)B \\ + \ & C(AB-BA) - (AB-BA)C \\ = \ & ABC - ACB - BCA + CBA + BCA - BAC - CAB \\ + \ & ACB + CAB - CBA - ABC + BAC \\ = \ & 0 \end{aligned}$$

□

Sabemos que o conjunto das matrizes quadradas reais $M(n \times n, \mathbb{R})$ com as operações usuais de soma e produto por um número real é um espaço vetorial, dessa forma, podemos generalizar esse conceito e definir álgebra de Lie, que também será um espaço vetorial acrescido de uma operação chamada colchete. Na sequência apresentaremos uma definição de álgebra de Lie, considerando sempre espaços vetoriais sobre o corpo de números reais.

Definição 3.20. *Uma **Álgebra de Lie** é um espaço vetorial $\mathfrak{a}$ munido de uma operação*

$$\begin{aligned} [\cdot,\cdot] : \mathfrak{a} \times \mathfrak{a} &\longrightarrow \mathfrak{a} \\ (X,Y) &\longmapsto [X,Y] \end{aligned}$$

*chamada de **colchete de Lie**, que satisfaz as seguintes propriedades:*

(1) O colchete de Lie é bilinear, ou seja,

$$[aX + bY, Z] = a[X,Z] + b[Y,Z]$$
$$e$$
$$[Z, aX + bY] = a[Z,X] + b[Z,Y]$$

para quaisquer números reais a, b e quaisquer $X, Y, Z \in \mathfrak{a}$.

(2) O colchete de Lie é anti-simétrico, ou seja,

$$[X,X] = 0$$

para qualquer $X \in \mathfrak{a}$.

(3) A identidade de Jacobi

$$[A,[B,C]] + [B,[C,A]] + [C,[A,B]] = 0$$

é satisfeita para quaisquer X, Y e $Z \in \mathfrak{a}$.

Agora, apresentaremos uma proposição da álgebra de Lie, em que o colchete é nulo se, e somente se, $[X,Y] = -[Y,X]$.

Proposição 3.21. *Numa álgebra de Lie, tem-se que $[X,X] = 0$ para qualquer $X \in \mathfrak{a}$ se, e somente se, $[X,Y] = -[Y,X]$.*

Demonstração. Notemos que

$$\begin{aligned} 0 &= [X+Y, X+Y] \\ &= [X, X+Y] + [Y, X+Y] \\ &= [X,X] + [X,Y] + [Y,X] + [Y,Y]. \end{aligned}$$

Pela hipótese, temos que $[X,X] = 0$ para qualquer $X \in \mathfrak{a}$. Assim, pela igualdade acima, temos que $[X,Y] = -[Y,X]$.

Reciprocamente, suponhamos que $[X,Y] = -[Y,X]$. Daí,

$$[X,Y] + [Y,X] = 0 \text{ para qualquer } X, Y \in \mathfrak{a}.$$

Assim, se Y = X, temos que $[X,X] + [X,X] = 0$ e concluímos que $[X,X] = 0$. □

Ao se estudar as álgebras de Lie, vamos assumir as propriedades de espaços vetoriais e, assim, analisaremos apenas as propriedades que seguem da operação produto dada pelo colchete.

A seguir, temos um exemplo de álgebra de Lie com o espaço vetorial das matrizes quadradas reais $M(n \times n, \mathbb{R})$.

Exemplo 3.22. *O espaço vetorial das matrizes quadradas reais $M(n \times n, \mathbb{R})$ é uma álgebra de Lie com o colchete definido por*

$$[A,B] = AB - BA.$$

Este colchete satisfaz a bilinearidade, ou seja, $[aA+bB, C] = a[A,C]+b[B,C]$ e $[C, aA+bB] = a[C,A] + b[C,B]$.
Por definição de colchete de matrizes quadradas reais $M(n \times n, \mathbb{R})$, temos:

$$\begin{aligned} [aA+bB, C] &= (aA+bB)C - C(aA+bB) \\ &= aAC + bBC - aCA - bCB \\ &= a(AC - CA) + b(BC - CB) \\ &= a[A,C] + b[B,C]. \end{aligned}$$

e por outro lado, temos

$$\begin{aligned}[C, aA + bB] &= C(aA + bB) - (aA + bB)C \\ &= aCA + bCB - aAC - bBC \\ &= a(CA - AC) + b(CB - BC) \\ &= a[C, A] + b[C, B].\end{aligned}$$

Para toda matriz quadrada real A pertencente a $M(n \times n, \mathbb{R})$, vale a igualdade $[A, A] = 0$. Temos que

$$\begin{aligned}[A, A] &= AA - AA \\ &= A^2 - A^2 \\ &= 0.\end{aligned}$$

E a identidade de Jacobi

$$[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = 0$$

é satisfeita, uma vez que

$$\begin{aligned}&[A, [B, C]] + [B, [C, A]] + [C, [A, B]] = \\ &= A(BC - CB) - (BC - CB)A + B(CA - AC) - (CA - AC)B + C(AB - BA) - (AB - BA)C \\ &= ABC - ACB - BCA + CBA + BCA - BAC - CAB + ACB + CAB - CBA - ABC + BAC \\ &= 0.\end{aligned}$$

No exemplo abaixo, temos uma álgebra de Lie abeliana, por conta de seu colchete comutativo.

Exemplo 3.23. *Seja $\mathfrak{b}$ um espaço vetorial qualquer e definamos*

$$[X, Y] = 0, \text{ para quaisquer } X, Y \in \mathfrak{b}.$$

Então $\mathfrak{b}$ é uma álgebra de Lie.

Prova:

(i) $\forall a, b \in \mathbb{R}$ *e* $X, Y, Z \in \mathfrak{b}$

$$\begin{aligned}[aX + bY, Z] &= (aX + bY)Z - Z(aX + bY) \\ &= aXZ + bYZ - aZX - bZY \\ &= a(XZ - ZX) + b(YZ - ZY) \\ &= a[X, Z] + b[Y, Z] \\ &= a0 + b0 \\ &= 0 + 0 \\ &= 0.\end{aligned}$$

e, por outro lado

$$\begin{aligned}[Z, aX + bY] =&Z(aX + bY) - (aX + bY)Z \\ =&aZX - bZY - aXZ + bYZ \\ =&a(ZX - XZ) + b(ZY - YZ) \\ =&a[Z, X] + b[Z, Y] \\ =&a0 + b0 \\ =&0 + 0 \\ =&0.\end{aligned}$$

(ii) *O colchete é anti-simétrico, pois, por definição*

$$[A, A] = 0.$$

(iii) *Identidade de Jacobi*

$$\begin{aligned}[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] &= [X, 0] + [Y, 0] + [Z, 0] \\ &= 0 + 0 + 0 \\ &= 0.\end{aligned}$$

As álgebras de Lie com o colchete definido desta forma recebem o nome de álgebras de Lie abelianas.

A seguir, temos dois exemplos onde os colchetes definidos não são uma álgebra de Lie, por não satisfazerem as propriedades vistas inicialmente.

Exemplo 3.24. *Consideremos o espaço vetorial* $\mathbb{R}$*, com o colchete definido por* $[x, y] = x + y$*. Com este colchete* $\mathbb{R}$ *não é uma álgebra de Lie. De fato, não vale, por exemplo, a bilinearidade, pois*

$$[2x, y] = 2x + y \neq 2[x, y] = 2x + 2y.$$

Exemplo 3.25. *Consideremos o espaço vetorial* $\mathbb{R}$*, com o colchete definido pela multiplicação* $[x, y] = xy$*. Neste caso, o espaço* $\mathbb{R}$ *não é álgebra de Lie, pois* $[x, x] = x^2 \neq 0$ *se* $x \neq 0$*.*

3.2 Subálgebras e Ideais

Apresentemos agora, a definição de subálgebra de Lie.

Definição 3.26. *Sejam* $\mathfrak{a}$ *uma álgebra de Lie e* $\mathfrak{b}$ *um subespaço vetorial de* $\mathfrak{a}$*. Dizemos que* $\mathfrak{b}$ *é uma subálgebra de Lie de* $\mathfrak{a}$ *se, e somente se,* $X, Y \in \mathfrak{b}$ *implicar em* $[X, Y] \in \mathfrak{b}$*.*

Assim, toda subálgebra de Lie de uma álgebra de Lie também é uma álgebra de Lie.

Uma subálgebra de uma álgebra de Lie que é uma álgebra abeliana é chamada subálgebra abeliana.

Apresentemos agora um teorema sobre subálgebra abeliana.

Teorema 3.27. *Seja* $\mathfrak{a}$ *uma álgebra de Lie e* $\mathfrak{b}$ *um subespaço unidimensional de* $\mathfrak{a}$*. Então,* $\mathfrak{b}$ *é uma subálgebra abeliana de* $\mathfrak{a}$*.*

Demonstração: *Seja* Z *uma base de* $\mathfrak{b}$*. Se* $X, Y \in \mathfrak{b}$*, então existem* $\alpha, \beta \in \mathbb{R}$ *tais que* $X = \alpha Z$ *e* $Y = \beta Z$*. Portanto,*

$$[X, Y] = [\alpha Z, \beta Z] = \alpha\beta[Z, Z] = 0 \in \mathfrak{b}.$$

Assim, dada uma álgebra de Lie, só existem subálgebras não abelianas de dimensão maior que um.

Uma outra consequência do teorema anterior é a seguinte corolário, o qual caracteriza as álgebras unidimensionais.

Corolário 3.28. *Toda álgebra de Lie unidimensional é abeliana.*

Demonstração. Seja $\mathfrak{a}$ uma álgebra de Lie unidimensional. Como $\mathfrak{a}$ é um subespaço unidimensional dela mesma, segue da proposição anterior que $\mathfrak{a}$ é abeliana. □

Segue adiante, mais um teorema sobre subálgebra de uma álgebra de Lie.

Teorema 3.29. *Seja $\mathfrak{a}$ uma álgebra de Lie e $\mathfrak{b}$ uma subálgebra de dimensão 2 de $\mathfrak{a}$. Então, ou $\mathfrak{b}$ é abeliana ou existe uma base $\{A, B\}$ de $\mathfrak{b}$ tal que $[A, B] = B$.*

Demonstração. Suponhamos que $\mathfrak{b}$ seja uma subálgebra não abeliana de dimensão 2 e tomemos uma base $\{X, Y\}$ de $\mathfrak{b}$. Como $\mathfrak{b}$ é uma subálgebra não abeliana e $X, Y \in \mathfrak{b}$, temos que $[X, Y] \neq 0$. Definamos $Y' = [X, Y]$ e escolhamos $X' \in \mathfrak{b}$ de modo que $\{X', Y'\}$ seja uma base de $\mathfrak{b}$. Como X' e Y' são elementos de $\mathfrak{b}$, temos que $X' = aX + bY$, $Y' = cX + dY$ e

$$[X', Y'] = [aX + bY, cX + dY] = (ad - bc)[X, Y] = (ad - bc)Y'.$$

Como $\mathfrak{b}$ não é abeliana, temos que $(ad - bc) \neq 0$. Definamos $A = (ad - bc)^{-1}X''$ e $B = Y'$. Logo, a base que estamos procurando é $\{A, B\}$. □

Decorre do teorema o próximo corolário apresentado, que por sua vez caracteriza as álgebras de dimensão dois.

Corolário 3.30. *Seja $\mathfrak{a}$ uma álgebra de Lie de dimensão 2. Então, ou $\mathfrak{a}$ é abeliana ou existe uma base $\{A, B\}$ de $\mathfrak{a}$ tal que $[A, B] = B$.*

Apresentemos agora uma proposição sobre interseção de subálgebras de uma álgebra de Lie. Essa proposição é de grande utilidade nos estudos das álgebras de Lie, pelo fato de auxiliar a encontrar novas álgebras por meio da interseção. Dessa forma, é possível encontrar mais exemplos de álgebras, com a interseção de duas subálgebras. Veja a seguir.

Proposição 3.31. *A interseção de duas subálgebras de uma álgebra de Lie $\mathfrak{a}$ também é uma subálgebra de Lie de $\mathfrak{a}$.*

Demonstração. Sejam $\mathfrak{b}_1$ e $\mathfrak{b}_2$ duas subálgebras de uma álgebra de Lie $\mathfrak{a}$. Pela teoria de espaços vetoriais, temos que a interseção $\mathfrak{b}_1 \cap \mathfrak{b}_2$ é um subespaço vetorial. É imediato que se $X, Y \in \mathfrak{b}_1 \cap \mathfrak{b}_2$, então $[X, Y] \in \mathfrak{b}_1 \cap \mathfrak{b}_2$. □

Agora iremos ver alguns exemplos de subálgebras da álgebra de Lie de todas as matrizes.

Exemplo 3.32. *Seja $\mathfrak{a}$ o conjunto de todas as matrizes reais quadradas de ordem* n *que possuem elementos não nulos somente na diagonal. Um elemento típico de $\mathfrak{a}$ pode ser escrito como*

$$\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix}.$$

Sabemos que $\mathfrak{a}$ é um subespaço do espaço de todas as matrizes quadradas $M(n \times n, \mathbb{R})$. Considerando o colchete de Lie $[A, B] = AB - BA$ e tomando

$$A = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix} \text{ e } B = \begin{pmatrix} b_1 & 0 & \cdots & 0 \\ 0 & b_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & b_n \end{pmatrix}$$

elementos genéricos de $\mathfrak{a}$, temos que

$$[A, B] = \begin{pmatrix} a_1b_1 - b_1a_1 & 0 & \cdots & 0 \\ 0 & a_2b_2 - b_2a_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_nb_n - b_na_n \end{pmatrix}, \text{ ou seja,}$$

$$[A, B] = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 \end{pmatrix} \in \mathfrak{a}$$

e, portanto, $\mathfrak{a}$ é uma subálgebra abeliana da álgebra de Lie $M(n \times n, \mathbb{R})$.

Exemplo 3.33. *O conjunto das matrizes quadradas de traço zero, que será denotada por*

$$\mathfrak{sl}(n, \mathbb{R}) = \{A \in M(n \times n, \mathbb{R}) : tr(A) = 0\},$$

é subálgebra de $M(n \times n, \mathbb{R})$.

De fato,

$$tr([A,B]) = tr(AB - BA) = tr(AB) - tr(BA) = 0$$

e, portanto, $[A,B] \in \mathfrak{sl}(n,\mathbb{R})$.

Exemplo 3.34. *O conjunto das matrizes quadradas triangulares superiores*

$$G(n,\mathbb{R}) = \left\{ A \in M(n \times n, \mathbb{R}) : A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix} \right\}$$

é subálgebra de $M(n \times n, \mathbb{R})$.

Exemplo 3.35. *O espaço das matrizes triangulares superiores com zeros na diagonal*

$$N(n,\mathbb{R}) = \left\{ A \in M(n \times n, \mathbb{R}) : A = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1n} \\ 0 & \cdots & 0 & 0 \end{pmatrix} \right\}$$

é uma subálgebra de Lie de $M(n \times n, \mathbb{R})$.

Exemplo 3.36. *Consideremos os subespaços de* $M(n \times n, \mathbb{R})$ *definidos por*

$$\mathfrak{so}(n,\mathbb{R}) = \{A \in M(n \times n, \mathbb{R}) : A^t = -A\},$$

e, chamando de subespaço das matrizes anti-simétricas, e

$$\mathfrak{s}(n,\mathbb{R}) = \{A \in M(n \times n, \mathbb{R}) : A^t = A\},$$

chamado subespaço das matrizes simétricas. Sabemos que

$$M(n \times n, \mathbb{R}) = \mathfrak{so}(n,\mathbb{R}) \oplus \mathfrak{s}(n,\mathbb{R})$$

uma vez que uma matriz $A \in M(n \times n, \mathbb{R})$ *pode ser escrita como*

$$A = \frac{A - A^t}{2} + \frac{A + A^t}{2},$$

com $\dfrac{A - A^t}{2} \in \mathfrak{so}(n, \mathbb{R})$ *e* $\dfrac{A + A^t}{2} \in \mathfrak{s}(n, \mathbb{R})$.

Temos que $\mathfrak{so}(n, \mathbb{R})$ *é uma subálgebra de Lie de* $M(n \times n, \mathbb{R})$, *pois se* $A, B \in \mathfrak{so}(n, \mathbb{R})$, *então*

$$\begin{aligned} [A, B]^t &= (AB - BA)^t \\ &= B^t A^t - A^t B^t \\ &= (-B)(-A) - (-A)(-B) \\ &= -[A, B]. \end{aligned}$$

e, portanto, $[A, B] \in \mathfrak{so}(n, \mathbb{R})$. *No entanto,* $\mathfrak{s}(n, \mathbb{R})$ *não é subálgebra de Lie de* $M(n \times n, \mathbb{R})$. *Isto ocorre porque o colchete de duas matrizes simétricas é anti-simétrica (e, portanto, não é simétrica se não for nula). Dessa forma, segue que*

$$\begin{aligned} [A, B]^t &= B^t A^t - A^t B^t \\ &= BA - AB \\ &= -[A, B]. \end{aligned}$$

Uma classe importante de subálgebras são os ideais.

Iremos definir agora Ideal de álgebra de Lie.

Definição 3.37. *Seja* $\mathfrak{a}$ *uma álgebra de Lie e* $\mathfrak{b}$ *um subespaço de* $\mathfrak{a}$. *Dizemos que* $\mathfrak{b}$ *é um ideal de* $\mathfrak{a}$ *se, dados quaisquer* $X \in \mathfrak{a}$ *e* $Y \in \mathfrak{b}$, $[X, Y] \in \mathfrak{b}$.

Em particular, todo ideal é uma subálgebra, mas a recíproca é falsa, ou seja, nem toda subálgebra é ideal. É isso que veremos no exemplo a seguir.

Exemplo 3.38. *Seja* $\mathfrak{so}(2, \mathbb{R})$ *a subálgebra das matrizes quadradas antissimétricas de ordem 2 do exemplo anterior. Temos que* $\mathfrak{so}(2, \mathbb{R})$ *não é um ideal de* $M(2 \times 2, \mathbb{R})$. *Com efeito,*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathfrak{so}(2, \mathbb{R})$$

mas

$$
\begin{aligned}
&\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\right] = \\
&= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} - \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 4 & -2 \\ -2 & -4 \end{pmatrix} \notin \mathfrak{so}(2,\mathbb{R}).
\end{aligned}
$$

Exemplo 3.39. *Seja $\mathfrak{a}$ uma álgebra abeliana. Então, todo subespaço $\mathfrak{b}$ de $\mathfrak{a}$ é um ideal. De fato, se $X \in \mathfrak{b}$ e $Y \in \mathfrak{a}$ temos que $[X,Y] = 0 \in \mathfrak{b}$.*

A proposição a seguir nos mostra que a interseção de dois ideais de uma álgebra também é um ideal desta álgebra.

Proposição 3.40. *A soma e a interseção de dois ideais de uma álgebra de Lie também é um ideal desta álgebra de Lie.*

Demonstração. Sejam $\mathfrak{b}_1$ e $\mathfrak{b}_2$ dois ideais de uma álgebra de Lie $\mathfrak{a}$. Decorre da teoria de espaços vetoriais que a interseção e a soma de dois subespaços também é um subespaço. Se tomarmos $X \in \mathfrak{b}_1 \cap \mathfrak{b}_2$ e $Y \in \mathfrak{a}$, é imediato da definição de ideal que $[X,Y] \in \mathfrak{b}_1 \cap \mathfrak{b}_2$. Suponhamos agora que $X \in \mathfrak{b}_1 + \mathfrak{b}_2$ e $Y \in \mathfrak{a}$. Assim, $X = X_1 + X_2$ com $X_1 \in \mathfrak{b}_1$ e $X_2 \in \mathfrak{b}_2$. Daí, temos que

$$[X,Y] = [X_1,Y] + [X_2,Y] \in \mathfrak{b}_1 + \mathfrak{b}_2.$$

□

A seguir, definimos o centralizador de um subconjunto de uma álgebra de Lie. Este, por sua vez, será o conjunto ds elementos da álgebra que possuem colchete nulo com todos os elementos do conjunto.

Definição 3.41. *Seja B um subconjunto de $\mathfrak{a}$, chamamos de **centralizador** de B em $\mathfrak{a}$, ou simplesmente centralizador de B, ao conjunto*

$$z(B) = \{X \in \mathfrak{a} \text{ tal que } [X,Y] = 0 \text{ para qualquer } Y \in B\}.$$

O centralizador de $\mathfrak{a}$ em $\mathfrak{a}$ é chamado de ***centro*** *de $\mathfrak{a}$.*

Proposição 3.42. *Seja $\mathfrak{b}$ um ideal de uma álgebra de Lie $\mathfrak{a}$. Então, $z(\mathfrak{b})$ também é um ideal de $\mathfrak{a}$.*

Demonstração. $z(\mathfrak{b})$ é subespaço vetorial de $\mathfrak{a}$. Agora, sejam $X \in z(\mathfrak{b})$, $Y \in \mathfrak{a}$ e $Z \in \mathfrak{b}$. A identidade de Jacobi nos diz que

$$[[X, Y], Z] + [[Z, X], Y] + [[Y, Z], X] = 0.$$

Como $\mathfrak{b}$ é ideal, temos que $[Y, Z] \in \mathfrak{b}$, e, portanto, da definição de $z(\mathfrak{b})$, concluímos que $[X, [Y, Z]] = 0$. Além disso, como $[Z, X] = 0$, tem-se que $[Y, [Z, X]] = 0$. Logo,

$$[[X, Y], Z] = 0 \ \text{ e } \ [X, Y] \in z(\mathfrak{b}).$$

Isto mostra que $z(\mathfrak{b})$ é um ideal de $\mathfrak{a}$. $\square$

Decorre da última proposição que o centro de uma álgebra de Lie é um ideal desta álgebra. Para as álgebras de Lie bidimensionais, temos o seguinte resultado.

Proposição 3.43. *Seja $\mathfrak{a}$ uma álgebra de Lie bidimensional e não abeliana. Então, o centro de $\mathfrak{a}$ é nulo.*

Demonstração. Seja $\{X, Y\}$ uma base de $\mathfrak{a}$ com $[X, Y] = Y$. Tomemos um elemento A no centro de $\mathfrak{a}$. Como $A \in \mathfrak{a}$, temos que $A = aX + bY$ e, assim,

$$\begin{aligned} [A, X] &= [aX + bY, X] \\ &= [aX, X] + [bY, X] \\ &= a[X, X] + b[Y, X] \\ &= b[Y, X] \\ &= -b[X, Y] \\ &= -bY. \end{aligned}$$

Pela definição de centro, temos que $b = 0$.

Por outro lado, temos que

$$\begin{aligned}[A,Y] &= [aX+bY,Y]\\ &= [aX,Y]+[bY,Y]\\ &= a[X,Y]+b[Y,Y]\\ &= a[X,Y]\\ &= aY.\end{aligned}$$

Assim, concluímos que $a=0$. Portanto, $A=0$. $\square$

Um outro conceito importante é o de quociente de álgebras de Lie. Sejam $\mathfrak{a}$ uma álgebra de Lie e $\mathfrak{b}$ um ideal de $\mathfrak{a}$. Como $\mathfrak{b}$ é um subespaço vetorial de $\mathfrak{a}$, podemos determinar o espaço quociente

$$\mathfrak{a}/\mathfrak{b} = \{X+\mathfrak{b} : X\in\mathfrak{a}\}.$$

A relação de equivalência é dada por

$$(X+\mathfrak{b}) = (Y+\mathfrak{b}) \text{ se, e somente se, } X-Y\in\mathfrak{b}.$$

Sabemos que $\mathfrak{a}/\mathfrak{b}$ é um espaço vetorial com as operações definidas por

$$\begin{gathered}(X+\mathfrak{b})+(Y+\mathfrak{b}) = (X+Y)+\mathfrak{b} \quad \text{e}\\ \alpha(X+\mathfrak{b}) = (\alpha X)+\mathfrak{b}, \text{ para } \alpha\in\mathbb{R}.\end{gathered}$$

Veremos agora, que $\mathfrak{a}/\mathfrak{b}$ é uma álgebra de Lie com o colchete

$$[(X+\mathfrak{b}),(Y+\mathfrak{b})] = [X,Y]+\mathfrak{b}.$$

1. Este colchete está bem definido.

Com efeito, se $(X+\mathfrak{b}) = (X_1+\mathfrak{b})$ e $(Y+\mathfrak{b}) = (Y_1+\mathfrak{b})$, então $X-X_1, Y-Y_1\in\mathfrak{b}$ e, assim, $X = X_1+Z_1$ e $Y = Y_1+Z_2$, com $Z_1, Z_2\in\mathfrak{b}$. Logo,

$$\begin{aligned}[X,Y] &= [X_1+Z_1, Y_1+Z_2]\\ &= [X_1,Y_1]+[X_1,Z_2]+[Z_1,Y_1]+[Z_1,Z_2].\end{aligned}$$

Como $\mathfrak{b}$ é um ideal de $\mathfrak{a}$, temos que $[X_1,Z_2],[Z_1,Y_1],[Z_1,Z_2]\in\mathfrak{b}$. Portanto,

$$[X,Y]+\mathfrak{b} = [X_1,Y_1]+\mathfrak{b},$$

mostrando que este colchete está bem definido. Na demonstração acima pode-se observar que é necessário $\mathfrak{b}$ ser um ideal. Se $\mathfrak{b}$ for apenas uma subálgebra o colchete não fica necessariamente bem definido.

As demais propriedades do colchete decorrem das propriedades do colchete para a álgebra de Lie $\mathfrak{a}$. Como exemplo, a identidade de Jacobi pode ser demonstrada da seguinte maneira:

$$\begin{aligned} & [X+\mathfrak{b},[Y+\mathfrak{b},Z+\mathfrak{b}]]+[Y+\mathfrak{b},[Z+\mathfrak{b},X+\mathfrak{b}]]+[Z+\mathfrak{b},[X+\mathfrak{b},Y+\mathfrak{b}]] \\ = \ & [X+\mathfrak{b},[Y,Z]+\mathfrak{b}]+[Y+\mathfrak{b},[Z,X]+\mathfrak{b}]+[Z+\mathfrak{b},[X,Y]+\mathfrak{b}] \\ = \ & [X,[Y,Z]]+\mathfrak{b}+[Y,[Z,X]+\mathfrak{b}+[Z,[X,Y]]+\mathfrak{b} \\ = \ & [X,[Y,Z]]+[Y,[Z,X]+[Z,[X,Y]]+\mathfrak{b} \\ = \ & 0+\mathfrak{b}=\mathfrak{b}, \ \text{(que é o elemento neutro de } \mathfrak{a}/\mathfrak{b}). \end{aligned}$$

Portanto, $\mathfrak{a}/\mathfrak{b}$ é uma álgebra de Lie.

Exemplo de álgebra de Lie quociente.

Sejam a álgebra de Heisenberg,

$$\mathfrak{g}=\left\{X\in\mathfrak{gl}(3,\mathbb{K}):\begin{pmatrix}0&*&*\\0&0&*\\0&0&0\end{pmatrix}\right\},$$

e a álgebra

$$\mathfrak{h}=\left\{X\in\mathfrak{gl}(3,\mathbb{K}):\begin{pmatrix}0&0&*\\0&0&0\\0&0&0\end{pmatrix}\right\}.$$

Note que $\mathfrak{h}$ é ideal de $\mathfrak{g}$, pois, para todo $X\in\mathfrak{h}$ e todo $Y\in\mathfrak{g}$, temos que $[X,Y]=0$. O quociente $\mathfrak{g}/\mathfrak{h}$ é uma álgebra abeliana bidimensional, uma vez que

$$[X,Y]\in\mathfrak{h}, \ \text{para todos } X,Y\in\mathfrak{g}.$$

Mostraremos, a seguir, que a soma direta de álgebras de Lie também é uma álgebra de Lie. E, mais, que o colchete dessa álgebra é a soma dos colchetes restritos a cada subálgebra de Lie.

Sejam $\mathfrak{a}_1,\mathfrak{a}_2,\ldots,\mathfrak{a}_n$ álgebras de Lie. Como $\mathfrak{a}_1,\mathfrak{a}_2,\ldots,\mathfrak{a}_n$ são espaços vetoriais, podemos considerar a soma direta de espaços vetoriais

$$\mathfrak{a} = \mathfrak{a}_1 \oplus \mathfrak{a}_2 \oplus \ldots \oplus \mathfrak{a}_n.$$

Seja $[.,.]_i$ o colchete em $\mathfrak{a}_i$. Sejam $X = X_1 + \ldots + X_n$ e $Y = Y_1 + \ldots + Y_n \in \mathfrak{a}$. Temos que $X+Y = (X_1+Y_1)+\ldots+(X_n+Y_n)$ e $\alpha X = \alpha X_1 + \ldots + \alpha X_n$. Assim, temos que $\mathfrak{a}$ se torna uma álgebra de Lie com o colchete definido por

$$[X,Y] = [X_1,Y_1]_1 + \ldots + [X_n,Y_n]_n.$$

3.3 Transformações Lineares

Nesta seção, veremos que a aplicação que preserva as operações do espaço vetorial de um espaço vetorial em outro espaço vetorial, é denominado de transformação linear.

Definição 3.44. *Sejam V e W dois espaços vetoriais. Uma Transformação Linear (ou aplicação linear) é uma função de V em W, $T : V \longrightarrow W$, que satisfaz as seguintes condições:*

1. *Quaisquer que sejam u e v em V.*

$$T(u+v) = T(u) + T(v).$$

2. *Quaisquer que sejam $k \in \mathbb{R}$ e $v \in V$,*

$$T(kv) = kT(v).$$

Exemplo 3.45. *Sejam os espaços vetoriais $V = \mathbb{R}$ e $W = \mathbb{R}$.*

$$\begin{array}{rccl} \textit{Considere } T: & \mathbb{R} & \longrightarrow & \mathbb{R} \\ & u & \longrightarrow & \alpha u \qquad \textit{ou} \;\; T(u) = \alpha u. \end{array}$$

Temos que

$$T(u+v) = \alpha(u+v) = \alpha u + \alpha v = T(u) + T(v)$$

, isto é, T satisfaz a propriedade 1 da definição 3.44, e como

$$T(ku) = \alpha(ku) = k(\alpha u) = kT(u),$$

ou seja, T satisfaz a propriedade 2 da definição 3.44. Logo T é uma transformação linear.

Mas ainda, toda transformação linear de $\mathbb{R}$ em $\mathbb{R}$ só pode ser deste tipo. De fato, $T(x) = T(x \cdot 1)$ e como T é uma transformação linear e x um escalar, $T(x \cdot 1) = x \cdot T(1)$. Chamando $T(1) = \alpha$, temos $T(x) = \alpha x$.

Exemplo 3.46. *Seja $T : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $T(u) = u^2$.*

Pode-se concluir que T não é linear, pois,

$T(u + v) = (u + v)^2 = u^2 + 2uv + v^2$

$T(u) + T(v) = u^2 + v^2$.

Portanto, $T(u + v) \neq T(u) + T(v)$.

Exemplo 3.47. *Considere os espaços vetoriais $V = \mathbb{R}^2$ e $W = \mathbb{R}^3$, e*

$$\begin{array}{rcl} T : \mathbb{R}^2 & \longrightarrow & \mathbb{R}^3 \\ (x, y) & \longrightarrow & (2x, 0, x + y) \quad ou \quad T(x, y) = (2x, 0, x + y). \end{array}$$

Tem-se que:

$$\begin{array}{rcl} T(u + v) & = & T((x_1, y_1) + (x_2, y_2)) = T(x_1 + x_2, y_1 + y_2) \\ & = & (2(x_1 + x_2), 0, (x_1 + x_2) + (y_1 + y_2)) \\ & = & (2x_1, 0, x_1 + y_1) + (2x_2, 0, x_2 + y_2) \\ & = & T(u) \ + \ T(v) \quad \text{isto é,} \\ T(u + v) & = & T(u) + T(v). \end{array}$$

Logo, a propriedade 1 da definição 3.44 é satisfeita. Mais ainda,

$$\begin{array}{rcl} T(ku) & = & T(k(x, y)) \\ & = & T(kx, ky) \\ & = & (2kx, 0, kx + ky) \\ & = & k(2x, 0, x + y) \\ & = & kT(u), \end{array}$$

e a propriedade 2 da definição 3.44 é satisfeita. Então T é uma transformação linear.

Uma transformação linear é completamente determinada conhecendo seu valor nos elementos de uma base.

Teorema 3.48. *Dados dois espaços vetoriais V e W e uma base de V, $\{v_1, \cdots, v_n\}$, sejam $w_1, \cdots, w_n$ elementos arbitrários de W. Então existe uma única aplicação linear $T : V \longrightarrow$*

W tal que $T(v_1) = w_1, \cdots, T(v_n) = w_n$. Esta aplicação é dada por: se $v = a_1v_1 + \cdots + a_nv_n$, então

$$\begin{aligned} T(v) &= a_1T(v_1) + \cdots + a_nT(v_n) \\ &= a_1w_1 + \cdots + a_nw_n. \end{aligned}$$

Definição 3.49. *Seja $T : V \longrightarrow W$ uma aplicação linear.*

1. *A imagem de T é o conjunto dos vetores $w \in W$ tais que existe um vetor $v \in V$, que satisfaz $T(v) = w$. Ou seja,*

$$Im(T) = \{w \in W;\ T(v) = w,\ v \in V\}$$

2. *O conjunto de todos os vetores $v \in V$ tais que $T(v) = 0$ é chamado de núcleo de T, sendo denotado por ker(T). Isto é*

$$ker(T) = \{v \in V;\ T(v) = 0\}.$$

Exemplo 3.50. *Determinar o núcleo da transformação linear*

$$\begin{array}{rccl} T: & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & (x, y) & \longrightarrow & T(x, y) = 3x + 2y \ . \end{array}$$

Observe que,

$$T(x, y) = 3x + 2y = 0$$

Logo, o núcleo é formado pelos pontos $y = (x, -\frac{3}{2}x),\ \forall\ x \in \mathbb{R}$.

Exemplo 3.51. *Seja a transformação linear*

$$\begin{array}{rccl} T: & \mathbb{R}^2 & \longrightarrow & \mathbb{R} \\ & (x, y) & \longrightarrow & x\ +\ y. \end{array}$$

Neste caso temos ker $T = \{(x, y) \in \mathbb{R}^2;\ x + y = 0\}$, isto é, ker T é a reta $y = -x$. Podemos dizer ainda que ker $T = \{(x, -x);\ x \in \mathbb{R}\} = \{x(1, -1);\ x \in \mathbb{R}\} = [(1, -1)]$.

Além disso, $Im\ T = \mathbb{R}$, pois dado $w \in \mathbb{R},\ w = T(w, 0)$.

Proposição 3.52. *Seja $T : U \longrightarrow V$ uma transformação linear. Então:*

i) $Ker(T)$ é um subespaço vetorial de U;

ii) A transformação linear T é injetora se, e somente se, $Ker(T) = \{0\}$.

iii) $Im(T)$ é um subespaço vetorial de V.

Exemplo 3.53. *Seja a transformação linear $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ dada por $T(x, y, z) = (x, 2y, 0)$. Então a imagem de T*

$$\begin{aligned} Im(T) &= \{(x, 2y, 0) : \ x, \ y \in \mathbb{R}\} \\ &= \{x(1, 0, 0) + y(0, 2, 0) : \ x, \ y \in \mathbb{R}\} \\ &= [(1, 0, 0), (0, 2, 0)]. \end{aligned}$$

Observe que $dim\ Im(T) = 2$.

O núcleo de T é dado por:

$$\begin{aligned} ker(T) &= \{(x, y, z) : \ T(x, y, z) \ = \ (0, 0, 0)\} \\ &= \{(x, y, z) : \ (x, 2y, 0) \ = \ (0, 0, 0)\} \\ &= \{(0, 0, z) : \ z \in \mathbb{R}\} \\ &= \{z(0, 0, 1) : \ z \in \mathbb{R}\} \\ &= [(0, 0, 1)]. \end{aligned}$$

Observe que $dim\ ker(T) = 1$.

O resultado a seguir diz que, o núcleo e a imagem de uma transformação linear tem uma estrutura de espaço vetorial. Além disso, apresentamos uma outra caracterização de transformações lineares injetoras.

O teorema abaixo é um dos resultados mais importantes de álgebra linear. Ele relaciona as dimensões do núcleo e da imagem de uma transformação linear com a dimensão do espaço vetorial.

Teorema 3.54 (Teorema do Núcleo e da Imagem)**.** *Sejam U e V espaços vetoriais de dimensão finita sobre $\mathbb{R}$. Dada uma transformação linear $T : U \longrightarrow V$, então*

$$dim\ U = dim\ Ker(T) + dim\ Im(T).$$

Demonstração. Seja $\beta_1 = \{u_1, \cdots, u_r\}$ uma base de $Ker(T)$. Essa base pode ser estendida a uma base $\beta_2 = \{u_1, \cdots, u_r, v_1, \cdots, v_s\}$ de U conforme o teorema do completamento.

Mostremos que $\beta = \{T(v_1), \cdots, T(v_s)\}$ é uma base de $Im(T)$.

a) Dado $v \in Im(T)$, existe $u \in U$ tal que $T(u) = v$. Mas u é combinação linear de $\beta_2 : u = \alpha_1 u_1 + \cdots + \alpha_r u_r + \beta_1 v_1 + \cdots + \beta_s v_s$, com os α_i e os β_j em $\mathbb{R}$, já que β_2 é base de

U. Logo:

$$\begin{aligned} v &= T(\alpha_1 u_1 + \cdots + \alpha_r u_r + \beta_1 v_1 + \cdots + \beta_s v_s) \\ &= \alpha_1 T(u_1) + \cdots + \alpha_r T(u_r) + \beta_1 T(v_1) + \cdots + \beta_s T(v_s) \\ &= \beta_1 T(v_1) + \cdots + \beta_s T(v_s), \end{aligned}$$

pois como $u_1, \cdots, u_r \in Ker(T)$, então suas imagens, por T, são nulas. Então $[B] = Im(T)$.

b) Suponhamos $\beta_1 T(v_1) + \cdots + \beta_s T(v_s) = 0$ com $\beta_1, \cdots, \beta_s \in \mathbb{R}$. Então $\beta_1 v_1 + \cdots + \beta_s v_s \in Ker(T)$. Logo existem $\alpha_1, \cdots, \alpha_r \in \mathbb{R}$ de maneira que:

$$\beta_1 v_1 + \cdots + \beta_s v_s = \alpha_1 u_1 + \cdots + \alpha_r u_r.$$

Daí, temos que

$$\alpha_1 u_1 + \cdots + \alpha_r u_r + (-\beta_1) v_1 + \cdots + (-\beta_s) v_s = 0.$$

Como o conjunto B_2 é LI, podemos concluir que todos os escalares da última igualdade são nulos. Em particular $\beta_1 = \beta_2 = \cdots = \beta_s = 0$. Portanto, B é LI.

Para terminar a demonstração, basta observar que, como $dim\ Ker(T) = r$, $dim\ U = r+s$ e $dim\ Im(T) = s$, então $dim\ U = dim\ Ker(T) + dim\ Im(T)$. $\square$

Sejam U e V espaços vetoriais de dimensão n e m, respectivamente, sobre $\mathbb{R}$. Consideramos uma transformação linear $T : U \longrightarrow V$. Dadas as bases $\beta = \{u_1, \cdots, u_n\}$ de U e $\gamma = \{v_1, \cdots, v_m\}$ de V, então cada um dos vetores $T(u_1), \cdots, T(u_n)$ está em V e consequentemente é combinação linear da base γ:

$$\begin{array}{ccccccccc} T(u_1) & = & \alpha_{11} v_1 & + & \alpha_{21} v_2 & + & \cdots & + & \alpha_{m1} v_m \\ T(u_2) & = & \alpha_{12} v_1 & + & \alpha_{22} v_2 & + & \cdots & + & \alpha_{m2} v_m \\ \vdots & = & \vdots & + & \vdots & + & \vdots & + & \vdots \\ T(u_n) & = & \alpha_{1n} v_1 & + & \alpha_{2n} v_2 & + & \cdots & + & \alpha_{mn} v_m, \end{array}$$

ou simplesmente,

$$T(u_j) \ = \ \sum_{i=1}^{m} \alpha_{ij} v_i \ (j = 1, 2, \cdots, n),$$

onde os α_{ij} estão univocamente determinados.

Definição 3.55. *A matriz $m \times n$ sobre $\mathbb{R}$,*

$$(\alpha_{ij})_{m\times n} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix},$$

que se obtém das considerações anteriores é chamada matriz de T em relação as bases β e γ. Usaremos para indicar essa matriz a notação:

$$[T]_\gamma^\beta.$$

Notas:

1. Se T é um operador linear e considerarmos $\beta = \gamma$, então diremos apenas matriz de T em relação à base β para indicar a matriz acima definida e usaremos a notação $[T]_\beta^\beta$ para representá-la.

2. Sempre que não haja dúvidas quanto ao par de bases que estamos considerando escreveremos apenas $[T]$ para indicar a matriz de T em relação a esse par de bases.

Exemplo 3.56. *A matriz de $T : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ dada por $T(x, y, z) = (x + y, y + z)$, em relação às bases*

$$\begin{aligned} \beta &= \{u_1 = (1,0,0);\ u_2 = (0,1,0);\ u_3 = (0,0,1)\};\ e \\ \gamma &= \{v_1 = (1,0);\ v_2 = (0,1)\}, \end{aligned}$$

$$\begin{aligned} T(u_1) &= (1,0) = 1v_1\ +\ 0v_2 \\ T(u_2) &= (1,1) = 0v_1\ +\ 1v_2 \\ T(u_3) &= (0,1) = -v_1\ +\ v_2. \end{aligned}$$

Logo,

$$[T]_\gamma^\beta = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Exemplo 3.57. *Seja U um espaço vetorial sobre $\mathbb{R}$ e seja I o operador idêntico de U. Dadas as bases β e γ de U, determinaremos então $[I]_\gamma^\beta$.*

Suponhamos $\beta = \{u_1, \cdots, u_n\}$ *e* $\gamma = \{v_1, \cdots, v_n\}$. *Então, se* $[I]_\gamma^\beta = (\alpha_{ij})$,

$$\begin{array}{ccccccc} I(u_1) & = u_1 & = & \alpha_{11}v_1 & + \cdots + & \alpha_{n1}v_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ I(u_n) & = u_n & = & \alpha_{1n}v_1 & + \cdots + & \alpha_{nn}v_n, \end{array}$$

o que mostra que $[I]_\gamma^\beta$ *é a matriz de mudança da base* β *para a base* γ.

Agora, vamos analisar quando dois espaços vetoriais são indistinguíveis do ponto de vista da álgebra linear.

Definição 3.58. *Entende-se por isomorfismo do espaço vetorial* U *no espaço vetorial* V *uma transformação linear* $T : U \longrightarrow V$ *que seja bijetora. Um isomorfismo* $T : U \longrightarrow U$ *é um automorfismo de* U.

Exemplo 3.59. *O operador idêntico* $I : U \longrightarrow U$ *dado por* $I(u) = u$ *para todo vetor* u *do espaço vetorial é trivialmente um automorfismo de* U.

O resultado abaixo mostra que em dimensão finita todos os espaços vetoriais de mesma dimensão têm as mesmas propriedades de álgebra linear.

Teorema 3.60. *Dois espaços vetoriais* U *e* V *de dimensão finita são isomorfos se, e somente se,* $\dim U = \dim V$.

3.4 Homomorfismo de álgebras de Lie

Nesse momento, iremos estudar algumas aplicações por meio de transformações lineares entre álgebras de Lie. Essas aplicações, por sua vez, preservam o colchete, e assim recebem o nome de homomorfismo de álgebras de Lie. Em específico, temos:

Definição 3.61. *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *álgebras de Lie. Uma transformação linear* $\phi : \mathfrak{a} \longrightarrow \mathfrak{b}$ *é um homomorfismo de álgebras de Lie se satisfaz a propriedade*

$$\phi([X, Y]) = [\phi(X), \phi(Y)].$$

Se ϕ é um isomorfismo entre espaços vetoriais e um homomorfismo de álgebras de Lie, dizemos que ϕ é um isomorfismo de álgebras de Lie. Um isomorfismo $\phi : \mathfrak{a} \longrightarrow \mathfrak{a}$ é dito automorfismo de álgebras de Lie.

A seguir veremos alguns exemplos relacionados a homomorfismos de álgebras de Lie.

Exemplo 3.62. *Sejam $\mathfrak{a}$ e $\mathfrak{b}$ álgebras abelianas e $\phi : \mathfrak{a} \longrightarrow \mathfrak{b}$ uma transformação linear. Como*

$$\phi([X,Y]) = \phi(0) = 0 = [\phi(X), \phi(Y)],$$

temos que ϕ é um homomorfismo de álgebras de Lie. Portanto, toda transformação linear entre álgebras abelianas é um homomorfismo de álgebras de Lie.

No exemplo a seguir, temos que a aplicação traço é um homomorfismo.

Exemplo 3.63. *A aplicação traço $tr : M(n\times n, \mathbb{R}) \longrightarrow \mathbb{R}$ é um homomorfismo, pois $tr(XY - YX) = 0$ para quaisquer matrizes X, Y e, portanto,*

$$tr[X,Y] = 0 = [trX, trY],$$

já que $\mathbb{R}$ tem dimensão 1 e, portanto, é uma álgebra abeliana.

No próximo exemplo, vamos mostrar a conjugação.

Exemplo 3.64. *Consideremos a álgebra de Lie das matrizes quadradas $M(n \times n, \mathbb{R})$ com colchete definido por*

$$[A,B] = AB - BA.$$

Seja J uma matriz invertível em $M(n \times n, \mathbb{R})$. Definamos a aplicação

$$\begin{array}{rcl} \phi : M(n \times n, \mathbb{R}) & \longrightarrow & M(n \times n, \mathbb{R}) \\ A & \longmapsto & JAJ^{-1}. \end{array}$$

Temos que ϕ é um automorfismo de álgebras de Lie. Com efeito, já sabemos que ϕ é um automorfismo de espaços vetoriais. Por outro lado,

$$\begin{array}{rcl} \phi([A,B]) & = & \phi(AB - BA) \\ & = & J(AB - BA)J^{-1} \\ & = & JAJ^{-1}JBJ^{-1} - JBJ^{-1}JAJ^{-1} \\ & = & [\phi A, \phi B]. \end{array}$$

Desta forma, ϕ é um automorfismo de álgebras de Lie. Esta aplicação ϕ é chamada de conjugação por J.

Na sequência, temos o homomorfismo canônico.

Exemplo 3.65. *Sejam $\mathfrak{a}$ uma álgebra de Lie e $\mathfrak{b}$ um ideal de $\mathfrak{a}$. Consideremos a álgebra de Lie quociente $\mathfrak{a}/\mathfrak{b} = \{X + \mathfrak{b} : X \in \mathfrak{a}\}$. Definamos a aplicação*

$$\begin{array}{rcl} \pi : \mathfrak{a} & \longrightarrow & \mathfrak{a}/\mathfrak{b} \\ X & \longmapsto & X + \mathfrak{b}. \end{array}$$

Temos que π é um homomorfismo de álgebras de Lie. Com efeito, pela definição das operações no espaço quociente $\mathfrak{a}/\mathfrak{b}$, conclui-se que π é linear. Para concluir a demonstração que π é um homomorfismo, observemos que

$$\begin{array}{rcl} \pi([X,Y]) & = & [X,Y] + \mathfrak{b} \\ & = & [X + \mathfrak{b}, Y + \mathfrak{b}] \\ & = & [\pi(X), \pi(Y)]. \end{array}$$

Este homomorfismo é chamado de homomorfismo canônico de $\mathfrak{a}$ em $\mathfrak{a}/\mathfrak{b}$.

No exemplo a seguir temos uma aplicação chamada de representação adjunta.

Exemplo 3.66. *Sejam $\mathfrak{a}$ uma álgebra de Lie e $gl(\mathfrak{a})$ a álgebra de Lie das transformações de $\mathfrak{a}$ em $\mathfrak{a}$. Para cada $X \in \mathfrak{a}$, definamos a transformação linear*

$$\begin{array}{rcl} ad(X) : \mathfrak{a} & \longrightarrow & \mathfrak{a}. \\ Y & \longmapsto & ad(X)(Y) = [X,Y]. \end{array}$$

Desse modo, a aplicação

$$\begin{array}{rcl} ad : \mathfrak{a} & \longrightarrow & gl(\mathfrak{a}) \\ Y & \longmapsto & ad(X) \end{array}$$

é um homomorfismo de álgebras de Lie. Com efeito, primeiro notemos que ad é transformação linear, pois

$$ad(X+Y)(Z) = [X+Y, Z] = [X,Z] + [Y,Z] = ad(X)(Z) + ad(Y)(Z),$$

ou seja,

$$ad(X) + ad(Y) = ad(X + Y).$$

Além disso, para $\alpha \in \mathbb{R}$*,*

$$ad(\alpha X)(Z) = [\alpha X, Z] = \alpha[X, Z] = \alpha ad(X)(Z).$$

assim,

$$ad(\alpha X) = \alpha ad(X).$$

Da identidade de Jacobi, segue que

$$\begin{aligned} ad([X,Y])(Z) &= [[X,Y],Z] \\ &= [X,[Y,Z]] - [Y,[X,Z]] \\ &= ad(X)(ad(Y)(Z)) - ad(Y)(ad(X)(Z)) \\ &= (ad(X) \circ ad(Y) - ad(Y) \circ ad(X))(Z) \\ &= [ad(X), ad(Y)](Z). \end{aligned}$$

Observemos que no caso particular em que $\mathfrak{a}$ *é uma álgebra abeliana temos que* $ad(X)$ *é a aplicação nula. A aplicação ad definida acima é chamada de representação adjunta da álgebra de Lie* $\mathfrak{a}$*.*

A seguir, mostraremos que o núcleo e a imagem de um homomorfismo são subálgebras de Lie. Em específico, mostraremos que o núcleo de um homomorfismo é um ideal.

Teorema 3.67. *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *álgebras de Lie e* $\phi : \mathfrak{a} \longrightarrow \mathfrak{b}$ *um homomorfismo de álgebras de Lie. Então, o núcleo de* ϕ*,* $Nuc(\phi)$*, é um ideal de* $\mathfrak{a}$ *e a imagem de* ϕ*,* $Im(\phi)$*, é uma subálgebra de* $\mathfrak{b}$*.*

Demonstração. Sejam $X \in \mathfrak{a}$ e $Y \in Nuc(\phi)$. Temos que

$$\phi([X,Y]) = [\phi(X), \phi(Y)] = [\phi(X), 0] = 0$$

e, portanto, $[X,Y] \in Nuc(\phi)$, isto é, $Nuc(\phi)$ é um ideal de $\mathfrak{a}$.

Por outro lado, tomando $X \in Im(\phi)$ e $Y \in Im(\phi)$, temos que $X = \phi(X_1)$ e $Y = \phi(Y_1)$ para algum $X_1 \in \mathfrak{b}$ e algum $Y_1 \in \mathfrak{b}$. Segue que

$$[X,Y] = [\phi(X_1), \phi(Y_1)] = \phi([X_1, Y_1]) \in Im(\phi),$$

mostrando que $Im(\phi)$ é uma subálgebra. $\square$

Na sequência, temos um teorema de isomorfismo para álgebras de Lie.

Teorema 3.68 (Teorema de isomorfismo de álgebras de Lie)**.** *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *álgebras de Lie e* $\phi : \mathfrak{a} \longrightarrow \mathfrak{b}$ *um homomorfismo de álgebras de Lie. Então,*

$$\mathfrak{a}/Nuc(\phi) \text{ é isomorfo a } Im(\phi).$$

A proposição abaixo nos garante que duas álgebras são isomorfas se possuem mesmas constantes de estrutura.

Demonstração. Sabemos da teoria de espaços vetoriais que a aplicação Ψ tal que $\Psi(X + Nuc(\phi)) = \phi(X)$ é um isomorfismo entre os espaços vetoriais $\mathfrak{a}/Nuc(\phi)$ e $Im(\phi)$. Verifiquemos que esta aplicação é um homomorfismo de álgebras de Lie. De fato,

$$\begin{aligned} \Psi([X + Nuc(\phi), Y + Nuc(\phi)]) &= \Psi([X, Y] + Nuc(\phi)) \\ &= \Psi([X, Y]) \\ &= \Psi[\phi(X), \phi(Y)] \\ &= [\Psi(X + Nuc(\phi)), \Psi(Y + Nuc(\phi))]. \end{aligned}$$

$\square$

Definição 3.69. *Sejam* $\mathfrak{a}$ *uma álgebra de Lie e* $\alpha = \{X_1, \cdots, X_n\}$ *uma base de* $\mathfrak{a}$*. Como* $[X_i, X_j]$ *é elemento de* $\mathfrak{a}$*, podemos escrevê-lo como combinação linear dos elementos desta base, ou seja,*

$$[X_i, X_j] = \sum_{k=1}^{n} c_{ij}^k X_k = c_{ij}^1 X_1 + \cdots + c_{ij}^n X_n.$$

Os coeficientes c_{ij}^k *são denominados constantes de estrutura da álgebra de Lie em relação à base* α*.*

A seguir iremos mostrar as constantes de estruturas, as quais determinam, a menos de um isomorfismo, a álgebra de Lie.

Proposição 3.70. *Duas álgebras de Lie são isomorfas se, e somente se, possuem as mesmas constantes de estrutura.*

Demonstração. Sejam $\mathfrak{a}$ e $\mathfrak{b}$ duas álgebras de Lie com bases $\{X_1, \cdots, X_m\}$ e $\{Y_1, \cdots, Y_n\}$, respectivamente, e com as mesmas constantes de estruturas c_{ij}^k. Notemos que se estas constantes são as mesmas, então, as álgebras de Lie têm a mesma dimensão, ou seja, $m = n$. Consideremos a transformação linear bijetiva $\psi : \mathfrak{a} \longrightarrow \mathfrak{b}$ que satisfaz $\psi(X_i) = Y_i$. Então se $X = \sum a^i X_i$ e $Y = \sum b^j X_j$, temos que

$$\begin{aligned} \psi([X,Y]) &= \psi([\textstyle\sum_i a^i X_i, \sum_j b^j X_j]) \\ &= \psi(\textstyle\sum_{ij} a^i b^j [X_i, X_j]) \\ &= \psi(\textstyle\sum_{ij} a^i b^j \sum_k c_{ij}^k X_k) \\ &= \textstyle\sum_{ijk} a^i b^j c_{ij}^k \psi(X_k) \\ &= \textstyle\sum_{ijk} a^i b^j c_{ij}^k Y_k \\ &= \textstyle\sum_{ijk} a^i b^j [Y_i, Y_j] \\ &= [\psi(X), \psi(Y)]. \end{aligned}$$

Assim, ψ é um isomorfismo.

Por outro lado, seja ψ um isomorfismo de $\mathfrak{a}$ e $\mathfrak{b}$. Temos, então, que a base de $\mathfrak{a}$, $\{X_1, \cdots, X_m\}$, tem o mesmo número de elementos que a base de $\mathfrak{b}$, $\{Y_1, \cdots, Y_n\}$. Ordenando novamente a base de $\mathfrak{b}$, podemos considerar $\psi(X_i) = Y_i$. Assim,

$$\psi([X_i, X_j]) = [\psi(X_i), \psi(X_j)] = [Y_i, Y_j].$$

Para $X_i, X_j \in \mathfrak{a}$, temos que

$$[X_i, X_j] = c_{ij}^1 X_1 + c_{ij}^2 X_2 + \ldots + c_{ij}^n X_n = \sum_k c_{ij}^k X_k.$$

Para $Y_i, Y_j \in \mathfrak{b}$, também tem-se que

$$[Y_i, Y_j] = b_{ij}^1 X_1 + b_{ij}^2 X_2 + \ldots + b_{ij}^n X_n = \sum_k b_{ij}^k X_k.$$

Como ψ é um isomorfismo, concluímos que

$$\begin{aligned} [Y_i, Y_j] &= \psi([X_i, X_j]) \\ &= \psi(c_{ij}^1 X_1 + c_{ij}^2 X_2 + \ldots + c_{ij}^n X_n) \\ &= c_{ij}^1 \psi(X_1) + c_{ij}^2 \psi(X_2) + \ldots + c_{ij}^n \psi(X_n) \\ &= c_{ij}^1 Y_1 + c_{ij}^2 Y_2 + \ldots + c_{ij}^n Y_n. \end{aligned}$$

Logo,

$$\sum_k c_{ij}^k X_k = \sum_k b_{ij}^k X_k,$$

o que implica em $\sum_k (c_{ij}^k - b_{ij}^k) X_k = 0$. Como $\{X_1, \cdots, X_m\}$ é uma base, temos que $(c_{ij}^k - b_{ij}^k) = 0$, para cada k e, portanto, $c_{ij}^k = b_{ij}^k$. □

Exemplos de isomorfismos de álgebras de Lie

Exemplo 3.71. *A menos de isomorfismo, existem apenas duas álgebras de Lie de dimensão dois. Uma delas é a abeliana e a outra é a que admite uma base $\{X, Y\}$ tal que $[X, Y] = Y$.*

Exemplo 3.72. *Considere as álgebras de Lie:*

$$\begin{aligned} \mathfrak{a}: &\quad \textit{base } \{a, b, c\} \textit{ tal que } [a, b] = b, \ [a, c] = [b, c] = 0 \\ \mathfrak{b}: &\quad \textit{base } \{a, b, c\} \textit{ tal que } [a, b] = c, \ [a, c] = [b, c] = 0. \end{aligned}$$

Como as constantes de estruturas são diferentes, concluímos que $\mathfrak{a}$ e $\mathfrak{b}$ não são isomorfas.

Exemplo 3.73. *Duas álgebras abelianas são isomorfas se, e somente se, têm a mesma dimensão.*

A seguir temos um exemplo de álgebra de Lie $\mathfrak{sl}(2, \mathbb{R})$, que se trata das matrizes quadradas de ordem dois com traço zero.

Exemplo 3.74. *As álgebras de Lie $\mathfrak{sl}(2, \mathbb{R})$ (com o colchete dado pelo comutador de matrizes) e $\mathbb{R}^3$ (com o colchete dado pelo produto vetorial) não são isomorfas.*

De fato, considere a base de $\mathfrak{sl}(2, \mathbb{R})$, $\{X, Y, Z\}$. dada por:

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} \ e \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Logo,

$$[X, Y] = Z, [X, Z] = -2X \ e \ [Y, Z] = 2Y.$$

Considere a base canônica de $\mathbb{R}^3$:

$$\{X = (1, 0, 0), Y = (0, 1, 0), Z = (0, 0, 1)\}.$$

Segue que

$$[X, Y] = Z, [X, Z] = -Y \ e \ [Y, Z] = X.$$

Como as constantes de estruturas das duas álgebras de Lie são diferentes, concluímos pelo teorema anterior que as álgebras de Lie $\mathfrak{sl}(2, \mathbb{R})$ *e* $\mathbb{R}^3$ *não são isomorfas.*

Considerações Finais

Acreditamos que é de suma importância aprofundar os estudos, principalmente quando se tem dificuldades. Dessa forma, buscando novos conhecimentos, podemos sanar as dificuldades anteriores. A busca pela aquisição do saber nos motiva a conhecer mais e continuar com os constantes aprendizados. A motivação para o desenvolvimento desse trabalho foi a curiosidade, saber "o que vem depois", assim como a Matemática, que não é uma ciência pronta e acabada.

Em geral, a maioria dos cursos se limitam no ensino da álgebra, no decorrer do curso de Licenciatura são abordados vários conteúdos nas disciplinas de Álgebra Linear e Estruturas Algébricas. Neste trabalho, estudamos esses conceitos de álgebra visto no curso e fomos além, seguindo para um estudo introdutório sobre as Álgebras de Lie.

Fizemos uma base de o que é necessário para iniciar o estudo das álgebras de Lie e apresentamos alguns conceitos introdutórios, fornecendo uma forma clara e detalhada sobre as álgebras de Lie, focando em exemplos geométricos e de grupos de matrizes. Para um estudo mais aprofundado sobre as Álgebras de Lie, a sugestão são os livros [9] e [10] e a referência [11].

Bibliografia

[1] BARROS, C. J. B.; SANTANA, A. J., **Estruturas Algébricas com ênfase em elementos da Teoria de Lie**. ed. (Maringá-PR): Eduem: Editora da Universidade Estadual de Maringá, 2011.

[2] BOLDRINI, J. L., COSTA, S. I. R., FIGUEIREDP, V. L. e WETZLER, H. G., **Álgebra Linear**. Ed. Harbra Ltda., São Paulo, 3a. Edição 1986.

[3] CALLIOLI, C. A.; DOMINGUES, H. H.; COSTA, R. C. F. **Álgebra linear e aplicações**. Atual, 2007.

[4] CURTIS, M. L., **Matrix Groups**. Second Edition, Springer-Verlag New York Inc,1984.

[5] DOMINGUES, H. e IEZZI, G., **Álgebra moderna**. 2ª. ed. Atual Editora. 1982.

[6] GONÇALVES, A., **Introdução a Álgebra**. IMPA, Rio de Janeiro, 1979.

[7] HOFFMAN, K. e KUNZE, R., **Álgebra linear**. Editora Polígono, São Paulo, 1971.

[8] JACOBSON, N., **Basic Algebra I**. 2. ed. [S.l.]: Dover Publications, Inc., 2009.

[9] HUMPHREYS, J. E., **Introduction to Lie algebras and representation theory**. Springer Science e Business Media, 2012.

[10] SAN MARTIN, L. A. B., **Álgebras de Lie**. Campinas-SP: Editora da Unicamp, 1999.

[11] SAN MARTIN, L. A. B., **Grupos de Lie**, Campinas-SP: Editora da Unicamp, 2016.

Índice