Álgebra

Felipe Vieira
Rafael Aleixo de Carvalho

Álgebra

2023

1ª Edição

Direção editorial: José Roberto Marinho

Capa: Fabrício Ribeiro

Edição revisada segundo o Novo Acordo Ortográfico da Língua Portuguesa

Dados Internacionais de Catalogação na publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Vieira, Felipe
Álgebra / Felipe Vieira, Rafael Aleixo de Carvalho. – 1. ed. – São Paulo: Livraria da Física, 2023.

Bibliografia.
ISBN 978-65-5563-378-8

1. Álgebra - Estudo e ensino 2. Matemática I. Carvalho, Rafael Aleixo de. II. Título.

23-173735 CDD-512.507

Índices para catálogo sistemático:
1. Álgebra linear: Matemática: Estudo e ensino 512.507

Aline Graziele Benitez - Bibliotecária - CRB-1/3129

LF EDITORIAL

Editora Livraria da Física
www.livrariadafisica.com.br
(11) 3815-8688 | Loja do Instituto de Física da USP
(11) 3936-3413 | Editora

Sumário

Sumário

Prefácio

Esse livro surgiu a partir das notas de aula dos autores, que ministraram seguidas vezes as disciplinas "Álgebra I" e "Álgebra II", que fazem parte do curso de Licenciatura em Matemática, do campus Blumenau da Universidade Federal de Santa Catarina.

Aqui em nosso campus, quando tais disciplinas foram criadas, tivemos de decidir como abordar tais assuntos, pois a forma como eles são apresentados pelo mundo não é unificada: há livros e cursos de graduação em que primeiro se apresentam os anéis, e há outros onde se começa com os grupos. E certamente ambos os caminhos possuem vantagens e desvantagens.

Pois bem, nós optamos por começar com a teoria de anéis pelo simples motivo pedagógico de que consideramos essa teoria menos abstrata e mais conectada com a Aritmética, quando comparada com a teoria de grupos. Tanto é que os axiomas que inspiram a definição de anel são todos inspirados nas propriedades do conjunto dos números inteiros.

Além disso, seus exemplos mais importantes são os também conjuntos numéricos dos racionais e dos reais, além dos conjuntos de matrizes, de funções, de polinômios e os conjuntos construídos através de análise dos restos de divisões euclidianas. Ou seja, toda a parte inicial de anéis é uma mera generalização daquilo que os jovens já conhecem e podem compreender com menos esforço.

Para isso, criamos uma seção própria para cada um desses exemplos não numéricos, para realizar uma análise calma, organizada, natural e bem intui-

tiva. Somente depois apresentamos aspectos mais profundos da teoria de anéis, como quocientes, elementos irredutíveis, além de alguns corpos bem específicos.

A segunda parte desse livro aborda a teoria de grupos, essa sim mais abstrata. Por conta disso, abordamos esse conteúdo em uma ordem diferente: começamos apresentando todos os principais conceitos da teoria para, somente depois, nos adentrarmos nos principais exemplos. Veremos que tais exemplos não são tão naturais, pois envolvem permutações, movimentos geometricamente rígidos de polígonos regulares, além dos produtos semidiretos, que são construções nada triviais feitas a partir do produto cartesiano.

Após ver todos esses exemplos clássicos, chegamos no objetivo principal da teoria de grupos, que é a sua classificação. A leitora, ou o leitor, perceberá que essa última seção contém muitos teoremas com demonstrações longas e encadeadas com outras proposições e teoremas prévios. Sua leitura certamente só deve ser realizada após um bom entendimento das seções anteriores.

Falando um pouco da parte burocrática apresentamos, ao longo do texto, biografias de matemáticas e matemáticos que contribuíram para a Álgebra. Essas informações foram retiradas do trabalho de J. J. O'Connor e E. F. Robertson, chamado *MacTutor History of Mathematics*, disponível em `www-history.mcs.st-and.ac.uk`. De seu banco de dados retiramos muitas imagens, e aquelas que não foram, possuem a fonte detalhada na legenda.

Parte dos exercícios foram criados, enquanto os demais foram retirados dos livros que constam na bibliografia. Em especial, em todas as seções temos exercícios com enunciado "Pesquise sobre", em que convidamos o leitor a se aprofundar por conta própria em temas que não couberam neste livro.

Para a leitura deste livro, é necessário um conhecimento prévio de Aritmética e de Lógica Matemática. Ademais, alguns poucos exemplos e exercícios requerem que o leitor saiba alguns conceitos de Cálculo e de Álgebra Linear. Por fim, para um pleno entendimento do Apêndice A, é necessária uma base de Análise, pois lidamos com convergência, *epsilons* e *deltas*.

Os autores agradecem aos estudantes, pela paciência no desenvolvimento desse material em suas disciplinas, e a todo o apoio do Departamento de Matemática da UFSC - Blumenau na escrita deste livro.

Blumenau, outubro de 2023

Felipe Vieira
Rafael Aleixo de Carvalho

CAPÍTULO 1

Introdução

A palavra Álgebra tem suas origens no nome al-Khwarizmi, um persa que popularizou símbolos muito parecidos aos que utilizamos hoje para representar números (embora ele os tenha atribuído aos indianos). E por muito tempo, a álgebra esteve relacionada e apenas preocupada em estudar os números, sejam os naturais, inteiros, racionais ou reais.

Foi em meados do século XVIII que a álgebra se tornou abstrata, através da generalização de conceitos já bem conhecidos da aritmética. Essa generalização, embora pouco axiomática, foi amadurecendo através de publicações de vários matemáticos que estudavam, principalmente, equações algébricas. Eles perceberam que os conjuntos numéricos tradicionais não eram mais suficientes para se descrever a natureza e todos seus eventos.

Na verdade, lidamos com esse problema quando tentamos resolver uma equação do tipo

$$x^2 + 1 = 0$$

contando apenas com números reais. Parece haver espaço para a criação de algo a mais, algo em princípio contra-intuitivo, que são as raízes quadradas de números negativos.

Assim, em vez de estudar apenas conjuntos numéricos tradicionais, a comunidade matemática começou a generalizar muitos dos conceitos conhecidos para conjuntos abstratos quaisquer, através de notações não numéricas. Esses conjuntos não necessariamente possuíam uma aplicação prática e eram definidos por meio de letras – seus geradores – e propriedades desejadas.

Por conta disso, inicialmente já não era mais necessário se preocupar com a origem numérica ou a aplicação do conjunto no qual se trabalhava, mas sim com a sua definição. Ou seja, com a forma como ele era representado e com as propriedades que seus elementos satisfaziam através das operações envolvidas.

A partir dessa mudança de interpretação, foram criados e estudados muitos conjuntos que, inicialmente, eram completamente abstratos. Somente depois de algum tempo é que se encontrou aplicações práticas para tais conjuntos, especialmente através de aplicações na física – em particular os números complexos e os quatérnios, que veremos mais adiante.

Porém, apesar de tais aplicações terem sido encontradas, ainda faltava uma definição unificada para muitas dessas estruturas, o que se tornou realidade no final do século XIX.

Neste livro, apresentamos a teoria de anéis e a teoria de grupos, assuntos que são comuns a todo curso de Licenciatura ou Bacharelado em Matemática – metade do livro para cada um. O objetivo que traçamos na apresentação da teoria de anéis é o de sempre estarmos conectados com conceitos numéricos para generalizá-los, como a divisibilidade, os números primos e as frações.

Tais assuntos já são conhecidos pelos jovens ingressantes na universidade, o que nos permite introduzir o pensamento algébrico de forma fluida e intuitiva.

Na sequência apresentamos a teoria de grupos, e a apresentamos de uma forma diferente, uma forma mais direta e abstrata. Fornecemos toda a base necessária para estudar seus exemplos principais, exemplos estes que não são tão triviais quanto aqueles de anéis.

Ademais, o nosso objetivo principal ao apresentar a teoria de grupos é apresentar uma pincelada de sua classificação – isto é, uma lista de todos os grupos possíveis – e, para isso, precisamos nos aventurar dentro da teoria das ações, das classes de conjugação e das ordens.

Esses conteúdos são realmente abstratos, profundos, e desafiam a nossa intuição. Portanto, colocando-os após toda a teoria de anéis e toda uma introdução à teoria dos grupos, acreditamos que o leitor terá a abstração necessária para entendê-los da melhor forma possível.

Agora, poderíamos nos perguntar *pra quê serve a Álgebra?*

Bem, como sua própria origem têm motivações em aplicações, podemos citar muitas delas. Os anéis são parte importante no estudo da Teoria de códigos, dentro da programação, além de serem cruciais para o estabelecimento da criptografia RSA, base da segurança da internet.

A teoria de grupos auxilia no pleno entendimento das simetrias, sendo parte fundamental no desenvolvimento da Visão computacional na Robótica, na Cristalografia e no estudo da Teoria dos orbitais moleculares, na Química, e mesmo na Espectroscopia molecular, que reside entre a última e a Física. Mesmo na arte e nos padrões têxteis, surgem os grupos *wallpaper* ou, simplesmente, grupos papel de parede.

CAPÍTULO 2

Anéis, domínios de integridade e corpos

O desenvolvimento da teoria dos anéis foi motivado, dentre vários motivos, pelas tentativas de resolução do último Teorema de Fermat [35]. Uma dessas tentativas foi dada pela matemática Sophie Germain.

Sophie Germain

Marie-Sophie Germain (Paris, 01 de abril de 1776 - Paris, 27 de junho de 1831) foi uma matemática francesa. Mesmo tendo que lidar com a discriminação – chegou a utilizar um nome masculino em cartas, *M. LeBlanc*, contribuiu para o desenvolvimento da teoria dos números, em especial sobre números primos. Há um teorema com seu nome, um resultado que aborda o últmo Teorema de Fermat.

Além de Sophie, em suas tentativas de demonstrar tal teorema, Euler, Gauss, Lamé e muitos outros perceberam que a aritmética sobre conjuntos numéricos tradicionais não seria ferramenta suficiente para essa tarefa.

Gabriel Lamé

Gabriel Lamé (Tours, 22 de julho de 1795 - Paris, 01 de maio de 1870) foi um matemático francês. Estudou geometria diferencial, a teoria da elasticidade e, dentre algumas contribuições na teoria dos números, demonstrou o Último Teorema de Fermat para $n = 7$.

Por isso, em meados do século XVIII começou-se a generalizar muitos dos conceitos que lidamos naturalmente nos conjuntos numéricos tradicionais $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$. Mesmo assim, essa generalização demorou a ser organizada e axiomatizada em regras que se aplicariam a vários conjuntos.

Um importante passo foi dado por Hamilton em 1843, quando ele criou o conjunto dos quatérnios, que veremos no Exemplo 2.14. Depois, foi Cayley quem ajudou nessa ampliação dos conceitos ao estudar as matrizes, em 1850. Em 1897, David Hilbert cunhou o termo **anel**, enquanto Joseph Wedderburn continuou esse estudo em 1905.

Posteriormente, Adolf Abraham Halevi Fraenkel apresentou uma definição abstrata de anel em sua tese de doutorado [15] em 1914 até que, na década de 1920, Emmy Noether apresentou muitos importantes resultados que, devido à discriminação contra as mulheres, ficaram conhecidos apenas em 1930 quando Van der Waerden publicou [36].

Na primeira seção deste capítulo, estudamos os princípios da definição de anéis, domínios de integridade e corpos. Além disso, veremos importantes propriedades e analisamos exemplos simples e numéricos, que serão utilizados no decorrer deste livro.

Nas demais seções, estudamos individualmente os exemplos clássicos mais importantes dentro da teoria de anéis, a saber, matrizes, funções, produtos diretos, anéis de inteiros módulo n e polinômios. Cada seção estará concentrada em analisar muitas das propriedades que cada um desses conjuntos satisfaz.

2.1 Definições, exemplos e propriedades

Um anel é, simplesmente, um conjunto com duas operações fechadas que satisfazem algumas propriedades. Por operação fechada, queremos dizer que, dados quaisquer dois elementos desse conjunto, quando os operamos por quaisquer uma das duas operações, o resultado também estará nesse conjunto. Por exemplo, a operação de subtração não é fechada no conjunto dos números naturais, pois $2-5$ não pertence a $\mathbb{N}$, enquanto a mesma subtração é fechada em $\mathbb{Z}$, além da adição e da multiplicação.

E é o conjunto dos números inteiros com suas operações de adição e multiplicação, que motivam a definição de anel. Ainda em idade escolar, aprendemos que tal conjunto satisfaz várias propriedades. Por exemplo, sabemos que a ordem na qual somamos dois números inteiros não interfere no resultado $(3+6=6+3)$. Matematicamente falando, isso significa que a adição é **comutativa** em $\mathbb{Z}$. Também sabemos que ao somarmos qualquer número com o 0, a resposta é o próprio número inicial $(2+0=0+2=2)$. Dizemos então que 0 é seu **elemento neutro da adição**.

Assim, analisando as propriedades mais básicas a respeito de $\mathbb{Z}$ com as operações $+$ e $\cdot$, conseguimos definir, de modo geral, o conceito de anel. Aliás, visto que boa parte dos exemplos de anel têm suas duas operações similares à adição e à multiplicação como conhecemos, normalmente utiliza-se os símbolos $+$ e $\cdot$ para representá-las, embora nós veremos alguns exemplos em que as operações tenham naturezas distintas.

Antes da definição de um anel, lembre que dado um conjunto A, definimos o produto cartesiano

$$A \times A = \{(a,b) \,:\, a \in A, b \in A\}.$$

Definição 2.1. *Seja A um conjunto com duas operações*

$$\begin{aligned} + : A \times A &\to A \\ (a,b) &\mapsto a+b \end{aligned}$$

e

$$\begin{aligned} \cdot : A \times A &\to A \\ (a,b) &\mapsto ab. \end{aligned}$$

Assim, $(A, +, \cdot)$ *é um anel se valem,* $\forall\, a, b, c \in A$*, as seguintes seis propriedades:*

(A1) Associatividade da adição:

$$(a + b) + c = a + (b + c).$$

(A2) Comutatividade da adição:

$$a + b = b + a.$$

(A3) Elemento neutro da adição:

$$\exists\, 0 \in A \,:\, \forall\, d \in A,\, d + 0 = d.$$

(A4) Elemento oposto da adição:

$$\forall\, d \in A,\, \exists\, e \in A \,:\, d + e = 0.$$

(A5) Associatividade da multiplicação:

$$(ab)c = a(bc).$$

(A6) Distributividade:

$$\begin{cases} a(b + c) = ab + ac \\ (a + b)c = ac + bc. \end{cases}$$

Para que tenhamos a notação mais agradável possível, sempre que as operações forem naturais ou óbvias, nos referiremos apenas ao conjunto, sem repetir os símbolos das operações. Também, sempre que possível denotaremos anéis genéricos por A, e seu elemento neutro da adição por 0. Se estivermos nos referindo a mais de um anel em uma mesma sentença, utilizaremos letras maiúsculas A, B, C, ... com elementos neutros 0_A, 0_B, 0_C, ... respectivamente.

Analisando essa definição, perceba que o item $(A3)$ nos indica que o conjunto vazio não pode ser um anel.

Já sabemos (ou assumimos) que $\mathbb{Z}$ é um anel com suas adição e multiplicação usuais. Com isso, vamos definir outro anel muito importante a seguir.

Exemplo 2.1. *O conjunto dos números racionais*

$$\mathbb{Q} = \left\{ \frac{a}{b} \,:\, a \in \mathbb{Z},\, b \in \mathbb{Z}_+^* \right\}$$

com as operações usuais

$$\begin{aligned} + : \mathbb{Q} \times \mathbb{Q} &\to \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{ad+bc}{bd} \end{aligned}$$

e

$$\begin{aligned} \cdot : \mathbb{Q} \times \mathbb{Q} &\to \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) &\mapsto \frac{ac}{bd} \end{aligned}$$

é um anel.
Antes de provarmos que $\mathbb{Q}$ é um anel com essas operações, vamos lembrar algumas propriedades importantes. Primeiro, para uma notação mais limpa, as frações com o número 1 embaixo são denotadas apenas como o número de cima, por exemplo,

$$\frac{3}{1} = 3.$$

Ademais, lembre que em $\mathbb{Q}$,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc.$$

Isso nos permite concluir que

$$\frac{a}{a} = 1,$$

$\forall\, a \in \mathbb{Z}$ *e*

$$\frac{0}{b} = \frac{0}{c} = \frac{0}{1} = 0,$$

$\forall\, b, c \neq 0 \in \mathbb{Z}$.
Para que, de fato, $\mathbb{Q}$ seja um anel devemos provar a validade das seis propriedades da Definição 2.1.

($A1$)

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} &= \frac{ad+bc}{bd}+\frac{e}{f}\\ &= \frac{(ad+bc)f+(bd)e}{(bd)f}\\ &= \frac{adf+bcf+bde}{bdf}\\ &= \frac{a(df)+b(cf+de)}{b(df)}\\ &= \frac{a}{b}+\left(\frac{cf+de}{df}\right)\\ &= \frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right).\end{aligned}$$

($A2$)

$$\begin{aligned}\frac{a}{b}+\frac{c}{d} &= \frac{ad+bc}{bd}\\ &= \frac{bc+ad}{bd}\\ &= \frac{cb+da}{db}\\ &= \frac{c}{d}+\frac{a}{b}.\end{aligned}$$

($A3$) *Vamos provar que* 0 *é o elemento neutro de* $\mathbb{Q}$*:*

$$\begin{aligned}\frac{a}{b}+0 &= \frac{a}{b}+\frac{0}{1}\\ &= \frac{a\cdot 1+b\cdot 0}{b\cdot 1}\\ &= \frac{a}{b}.\end{aligned}$$