Um Curso de Álgebra

Textuniversitários 43

Comissão editorial:
Thiago Augusto Silva Dourado
César Polcino Milies
Carlos Gustavo Moreira
Fábio Maia Bertato
Willian Diego Oliveira
Gerardo Barrera Vargas

César Polcino Milies

Um Curso de Álgebra

Editora Livraria da Física
São Paulo — 2026

Copyright © 2026 LF Editorial

1a. Edição

Editor: Victor Pereira Marinho / José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

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

Milies, César Polcino
Um curso de álgebra / César Polcino Milies. –– São Paulo : LF Editorial, 2026. –– (Textuniversitarios ; 43)

Bibliografia.
ISBN 978-65-5563-824-0

1. Álgebra – Estudo e ensino 2. Matemática I. Título. II. Série.

26-398541.0 CDD-512

Índices para catálogo sistemático:

1. Álgebra : Matemática 512

Eliane de Freitas Leite – Bibliotecária – CRB 8/8415

Todos os direitos reservados. Nenhuma parte desta obra poderá ser reproduzida sejam quais forem os meios empregados sem a permissão da Editora. Aos infratores aplicam-se as sanções previstas nos artigos 102, 104, 106 e 107 da Lei n. 9.610, de 19 de fevereiro de 1998.

Impresso no Brasil
Printed in Brazil

www.lfeditorial.com.br
Visite nossa livraria no Instituto de Física da USP
www.livrariadafisica.com.br
Telefones:
(11) 2648-6666 | Loja do Instituto de Física da USP
(11) 3936-3413 | Editora

A Alfredo Jones.
Professor, orientador, amigo.

Prefácio

Este livro foi concebido para servir como *texto para um curso* de álgebra e não apenas como uma exposição de conteúdos técnicos sobre a matéria. Na nossa opinião um curso, em qualquer área de matemática, deve oferecer ao aluno pelo menos três elementos essenciais para sua formação: *motivação, informação e aplicações*.

Cursos sobre cálculo ou geometria, por exemplo, podem oferecer motivações de modo relativamente simples e direto, apelando à intuição sobre o mundo real, ao nosso conhecimento informal do mundo físico. Da mesma forma, não é difícil encontrar aplicações relacionadas com a nossa experiência quotidiana, por exemplo, na física, na química, na economia etc.

Já no caso da álgebra isto resulta mais difícil, fundamentalmente porque esta disciplina surge como resposta a questões internas da própria matemática, como formular e resolver problemas. Por esse motivo, ela parece bem mais distante da realidade do aluno. Ainda, ao longo dos últimos dois séculos, esta disciplina tem-se tornado cada vez mais abstrata e seu formalismo produz em quem a encontra pela primeira vez uma sensação de estranhamento e, às vezes, até de desconforto.

Por causa disso, ao longo do livro, apelamos constantemente à história da disciplina, porque é justamente através dela que se percebe a necessidade de introduzir novos conceitos e se pode compreender que cada um deles foi formulado como resposta natural a um determinado problema. Precisamente por causa disso, nossas informações históricas não aparecem como notas de rodapé ou como apêndices de cada capítulo, mas como parte integrante do próprio texto.

Um ponto importante que molda a organização da exposição é nossa convicção de que as abstrações não fazem sentido por si mesmas, especialmente para o aluno que as encontra pela primeira vez. Elas só fazem sentido — e assim foi de fato ao longo da história desta disciplina — quando inspiradas numa vasta experiência concreta, quando é possível perceber que há elementos comuns em várias situações distintas. Por causa disso, ao introduzir os conceitos básicos incluímos uma longa lista de exemplos. Em particular, nos preocupamos em escolher aqueles que estão relacionados com tópicos que futuros matemáticos irão encontrar na sua prática profissional e que é importante que conheçam com certa profundidade.

Quanto às aplicações, além de incluirmos as mais usuais na aritmética e as que dizem respeito às construções geométricas, incluímos uma introdução a assuntos mais recentes, como a criptografia RSA e a teoria de Códigos Corretores de Erros.

Acreditamos que o material contido no texto é mais do que suficiente para pelo menos três semestres de álgebra na graduação e, eventualmente, para cursos de pós-graduação. O seu uso, para cada uma destas finalidades, dependerá da escolha dos capítulos a serem estudados.

Pensando em facilitar a leitura, temos nos permitido, às vezes, algumas repetições que devem facilitar a tarefa do leitor. Nesse mesmo espírito, nos capítulos iniciais tentamos ser muito cuidadosos nas explicações e raras vezes empregamos expressões do tipo “é fácil ver que”. Quando o fizemos, tínhamos a convicção de que tal afirmação

era mesmo verdadeira e que o leitor conseguiria levar adiante a tarefa sem maiores dificuldades.

À medida que tratamos temas mais avançados, imaginamos que o leitor tem já mais experiência com os assuntos tratados no livro e consequentemente deixamos mais verificações a seu encargo, mas sempre com a certeza de que a tarefa está dentro de suas possibilidades. O texto pressupõe do leitor apenas conhecimentos muito básicos e uma certa familiaridade com os conceitos iniciais da álgebra linear.

Partes do texto foram utilizadas em muitos dos cursos que ministramos tanto na Universidade de São Paulo como na Universidade Federal do ABC e, naturalmente, devemos muito a nossos alunos e colegas pelas numerosas observações e comentários que recebemos ao longo dos anos. É impossível agradecer explicitamente a todos eles sem cometer injustas omissões, mas em particular somos gratos ao Prof. Thiago Augusto Silva Dourado por inúmeras correções à primeira versão do texto e por sua inestimável colaboração na formatação do livro.

Sumário

Prefácio **vii**

1 Relações e operações **1**
1.1 Relações 1
1.2 Diagramas de Hasse 5
1.3 Operações 6

2 Grupos **11**
2.1 Introdução 11
2.2 Propriedades elementares de um grupo 27
2.3 Subgrupos normais 32
2.4 Grupos quociente 37

3 Subgrupos **43**
3.1 Definição e primeiras propriedades 43
3.2 Teorema de Lagrange 54

4 Relações de equivalência e subgrupos **57**
4.1 A congruência módulo um subgrupo 57

4.2 A ordem de um elemento 66
4.3 Aplicações na aritmética 69
4.4 Uma aplicação: Criptografia RSA 75
4.5 Subgrupos normais 81
4.6 Grupos quociente 87

5 Homomorfismos **93**
5.1 Definição e exemplos 93
5.2 Propriedades dos homomorfismos 97
5.3 Isomorfismos 104
5.3.1 Como provar que dois grupos *não* são isomorfos? 108
5.3.2 O Teorema de Cayley. 109
5.4 Teorema do homomorfismo 113

6 Produtos diretos **119**
6.1 Produto direto externo 119
6.2 Produto direto interno 124

7 Grupos cíclicos **131**
7.1 Definição e primeiras propriedades 131
7.2 Subgrupos e quocientes de um grupo cíclico 133

8 Grupos abelianos **143**
8.1 Grupos abelianos finitos 143
8.2 Grupos abelianos finitamente gerados 155

9 Grupos de permutações **167**
9.1 O grupo S_n 167
9.2 A simplicidade de A_n 180

10 Teoremas de Sylow **189**
10.1 A ação de um grupo 189
10.2 Teoremas de Sylow 195

11 Anéis **203**
11.1 Definições e primeiros exemplos 203
11.2 Alguns exemplos interessantes 214
11.2.1 O Anel dos Inteiros de Gauss 214
11.2.2 O Anel dos Quatérnios Reais 217
11.2.3 Soma Direta de Anéis 222
11.3 A Característica de um anel 224

12 Ideais e homomorfismos **227**
12.1 Subanéis 227
12.2 Homomorfismos de anéis 233
12.3 Ideais 239
12.4 Anéis quociente 245
12.5 Teorema do homomorfismo para anéis 249
12.6 O corpo de frações de um anel de integridade 253

13 Anéis de polinômios **259**
13.1 Introdução 259
13.2 Funções polinomiais 269
13.3 Ideais e quocientes 273

14 Divisibilidade em anéis de integridade **277**
14.1 Introdução 277
14.2 Domínios fatoriais 285
14.3 Domínios euclidianos e domínios principais 293

15 Corpos **305**
15.1 Introdução 305
15.2 Corpos primos 309
15.3 Elementos algébricos e transcendentes 313
15.4 Um pouco de álgebra linear 321

16 Problemas clássicos **329**
16.1 Números construtíveis 329
16.2 Os problemas clássicos 341

16.2.1 A trissecção do ângulo. 342
16.2.2 A quadratura do círculo. 343
16.2.3 A duplicação do cubo. 344

17 Mais sobre extensões e raízes **345**
17.1 Corpo de raízes de um polinômio 345
17.2 Extensões normais 357
17.3 Extensões separáveis 361

18 Breve incursão na teoria de Galois **369**
18.1 Introdução 369
18.2 Grupos de automorfismos 370
18.3 Teorema fundamental 380
18.4 Uma demonstração do teorema fundamental da álgebra 388

19 Resolução de equações algébricas por radicais **393**
19.1 Funções racionais simétricas 393
19.2 Extensões Radicais 396
19.3 Teorema de Ruffini-Abel 403

20 Corpos finitos **409**
20.1 A classificação dos corpos finitos 409
20.2 Automorfismos de corpos finitos 415

21 Códigos corretores de erros **421**
21.1 Introdução 421
21.2 Conceitos básicos 423
21.3 Códigos lineares 428
21.4 Decodificação 436

Referências Bibliográficas **441**

Notações **447**

Índice Remissivo **451**

1 Relações e operações

As noções de relação *e* operação *desempenham um papel central na Álgebra Abstrata. Elas podem ser usadas num sentido intuitivo por se tratar de conceitos que devem ser muito familiares ao leitor. Neste capítulo vamos descrever muito brevemente estes conceitos com um certo rigor mas sem incorrer em excessivas formalizações. Nossa intenção é apenas estabelecer uma linguagem em comum com o leitor que será utilizada nos capítulos subsequentes. Para tanto, vamos assumir que o leitor está familiarizado com os conceitos mais básicos da teoria intuitiva de conjuntos e com as notações correspondentes.*

1.1 Relações

Sejam A e B conjuntos. Chama-se *produto cartesiano* de A e B ao conjunto

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

Estabelecer uma relação binária num conjunto A é, intuitivamente, dar um critério que nos permita dizer se dois elementos quaisquer a e b de A estão, ou não, relacionados.

Formalmente, dar uma relação binária, que representaremos pelo símbolo R, num conjunto A é dar um subconjunto V_R do produto cartesiano $A \times A$. Dados dois elementos a e b de A, diremos que a está na relação R com b se o par (a, b) pertence a V_R. Para indicar este fato escreveremos aRb.

Definição 1.1.1 Uma relação binária R num conjunto A diz-se uma *relação de equivalência* se ela satisfaz as seguintes propriedades:

(i) Para todo $a \in A$ tem-se que aRa (propriedade reflexiva).

(ii) Se aRb então bRa (propriedade simétrica).

(iii) Para todos a, b e c em A, se aRb e bRc então aRc (propriedade transitiva).

Se R é uma relação de equivalência e aRb, diz-se que *a é equivalente* a b.

Exemplo 1.1.2 No espaço $\mathbb{R}^2$ definimos a distância do ponto $P = (a, b)$ à origem $O = (0, 0)$ pela fórmula

$$d(P, O) = \sqrt{a^2 + b^2}.$$

Podemos definir uma relação em $\mathbb{R}^2$ como segue. Dados $P_1 = (a_1, b_1)$ e $P_2 = (a_2, b_2)$ diremos que $P_1 \sim P_2$ (P_1 é equivalente a P_2) se

$$d(P_1, O) = d(P_2, O).$$

A verificação de que as três propriedades da definição 1.1.1 valem neste caso é imediata.

Definição 1.1.3 Dada uma relação de equivalência R num conjunto A, para cada elemento $a \in A$ chama-se *classe de equivalência* de a ao conjunto:

$$\overline{a} = \{x \in A \mid aRx\}.$$

Cada elemento de uma classe de equivalência diz-se um *representante*. Um conjunto de elementos de A que consta de um único

elemento de cada classe de equivalência diz-se um *conjunto completo de representantes* dessas classes.

Pode-se provar muito facilmente, usando as propriedades da definição, que o conjunto das classes de equivalência em A é uma *partição* de A; isto é, verifica:

(i) Todo elemento de A pertence a alguma classe de equivalência.

(ii) Se $\overline{a} \neq \overline{b}$ então $\overline{a} \cap \overline{b} = \emptyset$.

Pode-se verificar diretamente que as classes de equivalência da relação definida no Exemplo 1.1.2 são as circunferências com centro na origem.

Definição 1.1.4 O conjunto de todas as classes de equivalência de um conjunto A definidas por uma relação de equivalência R chama-se o *conjunto quociente* de A pela relação R e se denota pelo símbolo A/R.

Exemplo 1.1.5 Seja $f : A \to B$ uma função de um conjunto A num conjunto B. Definimos uma relação R em A da seguinte forma. Dados x e y em A, diremos que xRy se e somente se $f(x) = f(y)$.

O leitor pode verificar facilmente que esta é, de fato, uma relação de equivalência e que a classe $\overline{a}$ de um elemento $a \in A$ nada mais é do que a pré-imagem do elemento $f(a)$.

Vamos discutir agora um outro tipo de relação que será muito importante nas nossas discussões futuras.

Definição 1.1.6 Uma relação binária R num conjunto A diz-se uma *relação de ordem* se ela satisfaz as seguintes propriedades:

(i) Para todo $a \in A$ tem-se que aRa (propriedade reflexiva).

(ii) Se aRb e bRa então $a = b$ (propriedade antissimétrica).

(iii) Para todos a, b e c em A, se aRb e bRc então aRc (propriedade transitiva).

Se uma relação de ordem R num conjunto A verifica também a propriedade:

(iv) Quaisquer que sejam a e b em A tem-se que aRb ou bRa.

Então diz-se que R é uma relação de ordem *total*.

Frequentemente utilizaremos o símbolo $\prec$ para representar relações de ordem.

Há uma série de noções relativas às relações de ordem que o leitor provavelmente conhece mas que, para fixarmos a linguagem, explicitamos a seguir.

Definição 1.1.7 Seja N um subconjunto de um conjunto M, ordenado por uma relação $\prec$.

(i) Um elemento $y \in M$ diz-se um *majorante* de N se $x \prec y$ para todo $x \in N$.

(ii) O conjunto N diz-se *limitado superiormente* se tem um majorante.

(iii) Um elemento $x_0 \in N$ diz-se um *elemento maximal* se para todo $x \in N$ tem-se que $x_0 \prec x$ implica $x = x_0$ (isto é, se x_0 não é "menor" que qualquer outro elemento de N).

(iv) Um elemento $x_0 \in N$ diz-se um *máximo* se para todo $x \in N$ tem-se que $x \prec x_0$ (isto é, se x_0 é "maior" que qualquer outro elemento de N).

De forma análoga, invertendo as relações de ordem envolvidas, definem-se os conceitos de *minorante, elemento minimal e elemento mínimo* de N.

Exemplo 1.1.8 Pode-se verificar muito facilmente que a relação "divide" no conjunto dos números inteiros positivos é uma relação de ordem, mas não é uma ordem total. A relação "menor ou igual" neste mesmo conjunto é uma relação de ordem total.

Exemplo 1.1.9 Dado um conjunto X vamos indicar por $\mathscr{P}(X)$ o conjunto de todos os subconjuntos de X. A relação de inclusão $\subset$ é uma relação de ordem parcial em $\mathscr{P}(X)$, mas não é uma ordem total. Se V indica um espaço vetorial sobre um corpo $\mathbb{F}$, então $\subset$ é uma relação de ordem parcial no conjunto $\mathcal{S}$ de todos os subespaços de V.

Definição 1.1.10 Um conjunto parcialmente ordenado M diz-se um *reticulado* se todo par de elementos de M tem um *supremo*, isto é, um elemento que é o mínimo dos majorantes, e um *ínfimo*, isto é, um elemento que é o máximo dos minorantes.

Um conjunto ordenado em que todo par de elementos tem um supremo e um ínfimo chama-se um *reticulado*.

Exemplo 1.1.11 No conjunto dos números inteiros positivos, ordenado pela relação "divide", dados dois inteiros positivos a e b, temos que o $\text{mmc}(a, b)$ é o supremo destes elementos e o $\text{mdc}(a, b)$, o seu ínfimo.

Dados dois elementos A e B no conjunto $\mathscr{P}(X)$ de todos os subconjuntos de um conjunto fixado X, tem-se que $A \cup B$ é o supremo deste par e $A \cap B$ o seu ínfimo.

1.2 Diagramas de Hasse

Estes diagramas são *grafos* utilizados para representar conjuntos parcialmente ordenados e são chamados assim em homenagem a Helmut Hasse, que os usou sistematicamente, embora não tenha sido o primeiro a utilizá-los.

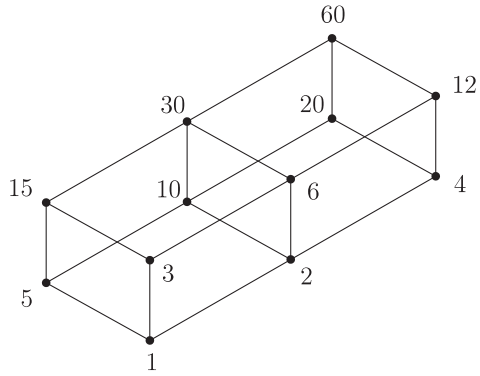
Um *grafo* é, simplesmente, um par de conjuntos (V, E), onde V é um conjunto não vazio de "pontos" chamados *vértices* e E é um conjunto de linhas, chamadas *arestas*, que ligam alguns dos vértices de V. (Quem desejar ser mais formal pode pensar nas arestas como pares não ordenados de vértices).

Dado um conjunto ordenado $(M, \prec)$ representa-se cada elemento de M por um vértice e se desenha uma aresta *ascendente* desde o ponto que representa um elemento x ao ponto que representa o elemento y toda vez que $x \prec y$.

Para simplificar o desenho, elimina-se a informação redundante da seguinte forma:

- Não se desenham arcos de um ponto em si mesmo, porque a *propriedade reflexiva* se considera subentendida.
- Não se desenham arestas que podem ser deduzidas da transitividade.

Como exemplo, damos a seguir o diagrama dos divisores de 60 ordenados pela relação "divide".



1.3 Operações

Também pode-se formalizar a noção de *operação* de forma análoga. Intuitivamente, uma operação num conjunto A é um critério que nos permite associar a cada par de elementos a e b de A um terceiro elemento c em A que chamamos o resultado da operação de a com b. Podemos precisar esta noção da seguinte forma.

Definição 1.3.1 Seja A um conjunto. Uma *operação binária* em A é uma função $f : A \times A \to A$.

Dados dois elementos a e b em A, o elemento $c = f(a, b)$ chama-se o *resultado* da operação de a com b.

Naturalmente, as operações de soma e produto que estudamos até agora, por exemplo entre inteiros ou entre inteiros módulo m ou ainda entre números complexos, são casos particulares de operações no sentido definido acima.

No que segue usaremos o signo $*$ para representar uma operação num conjunto A. Neste contexto mais geral, usa-se também a terminologia familiar ao leitor para designar propriedades particulares das operações:

(i) Uma operação diz-se *associativa* se dados três elementos quaisquer $a, b, c \in A$ tem-se que

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

(ii) A operação diz-se *comutativa* se para todo par de elementos $a, b \in A$ tem-se que

$$a * b = b * a.$$

(iii) Um elemento $e \in A$ diz-se um *neutro à esquerda* se, para todo $a \in A$ tem-se que

$$e * a = a,$$

e um *neutro à direita* se para todo $a \in A$ tem-se que

$$a * e = a.$$

O elemento e diz-se um *neutro* se ele é simultaneamente um neutro à esquerda e à direita.

(iv) Se e é um elemento neutro para uma operação $*$ num conjunto A, um elemento a' diz-se um *inverso à esquerda* de um elemento $a \in A$ se

$$a' * a = e$$

e um *inverso à direita* se

$$a * a' = e.$$

a' é um *inverso* de a se ele é simultaneamente inverso à esquerda e à direita.