Estruturas Algébricas

Um Primeiro Curso

Textuniversitários 34

Vandenberg Lopes Vieira

Estruturas Algébricas
Um Primeiro Curso

LF Editorial
São Paulo — 2025

1a. Edição

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

Texto em conformidade com as novas regras ortográficas do Acordo da Língua Portuguesa.

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

Vieira, Vandenberg Lopes
Estruturas algébricas : um primeiro curso / Vandenberg Lopes Vieira. –– São Paulo : LF Editorial, 2025. –– (Textuniversitários ; 34)

Bibliografia.
ISBN 978-65-5563-654-3

1. Álgebra I. Título. II. Série.

25-304584.0 CDD–512

Índices para catálogo sistemático:

1. Álgebra : Matemática 512

Eliete Marques da Silva – Bibliotecária – CRB-8/9380

Impresso no Brasil
Printed in Brazil

LF
EDITORIAL

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

À minha esposa Kátia (in memoriam) e à minha filha Heloísa, a quem amo de verdade!

DEDICO

O que é já foi, e o que há de ser também já foi; Deus fará renovar-se o que se passou.

Eclesiastes 3:15

Prefácio

Seria no mínimo curioso que um autor ao escrever um livro-texto não tenha a intenção de que ele venha auxiliar o maior número possível de leitores. Acreditamos que todos os autores tenham um objetivo em comum: apresentar um texto claro, agradável, útil para o fim que lhe foi designado. Por esta razão, muitos cuidados foram minuciosamente trabalhados de modo a oferecer uma linha de análise que todo bom livro deve apresentar.

É notório que há excelentes livros de Álgebra Abstrata adotados nos cursos de graduação em Matemática. Sendo assim, faz-se necessário que uma justificativa seja dada à comunidade acadêmica, aos colegas professores e aos alunos sobre um novo livro que versa sobre tópicos em comum. Neste prefácio, tentaremos justificar nossa proposta.

Em primeiro lugar, a elaboração de um livro pode ser, além de outras coisas, uma demonstração de que algo poderia ser melhorado em alguns aspectos, tais como: a forma com que cada conteúdo é apresentado; a quantidade e o nível dos exemplos, incluindo o modo como eles são explorados após cada conceito definido; e as divisões dos conteúdos nas respectivas seções.

Em geral, os cursos em Álgebra Abstrata são vistos após os cursos de Introdução em Teoria dos Números e Álgebra Linear. É inegável que eles auxiliam o leitor a compreender certos resultados relacionados a grupos e anéis. No entanto, o livro não exige um conhecimento especializado de tópicos prévios, pois os conceitos básicos necessários ao seu desenvolvimento são apresentados em seus capítulos iniciais, de modo que, qualquer estudante de Matemática ou até mesmo de outras áreas, como Ciência da Computação e Engenharia Elétrica, que esteja interessado em estudar estruturas algébricas, não tenha dificuldades ao lê-lo.

Objetivos do livro

O objetivo principal deste livro é oferecer um curso inicial em Álgebra Abstrata para Licenciatura em Matemática. Particularmente, ele foi planejado para cursos básicos de grupos e anéis. Por ter esse foco, justifica-se nele a ausência de alguns resultados mais avançados, os quais são precisamente apresentados nos cursos de Bacharelado. No entanto, os Capítulos 8 e 9, este último opcional, tratam de tópicos específicos de Bacharelado, e tem como finalidade alcançar os estudantes que desejam aperfeiçoar mais seus estudos na Teoria dos Anéis. Em linhas gerais, acreditamos que o livro seja útil aos alunos que almejam obter conhecimentos básicos em Álgebra Abstrata, bem como para àqueles que desejam aprofundar-se em tópicos específicos.

Espera-se que a maneira com a qual os conteúdos teóricos aqui explorados seja diferente daquela apresentada no Bacharelado. Nessa perspectiva, faz-se necessário destacar ao menos dois critérios essenciais: o primeiro é que os exemplos sejam considerados com mais detalhes e com grau de dificuldade crescente; e o segundo é que expressões como "fácil ver" e "imediato", tão comuns em textos matemáticos, não sejam usadas com desprezo para com o estudante, mas que tenham a finalidade de sinalizá-lo de que alguns detalhes superficiais de um determinado resultado foram compactados.

É muito comum o professor de um curso em Licenciatura em Matemática ouvir de seus alunos questionamentos sobre a real necessidade de demonstrações de teoremas em um curso que objetiva a formação de professor para o ensino básico. Estamos convencidos de que demonstrar um dado resultado em Álgebra pode trazer certo temor para alguns. Sabemos, também, que muitos podem encarar esse momento como menos agradável do curso. Para o estudante, muitas definições, teoremas escritos de modo extremamente formal e, após isso, demonstrações cuidadosas cercadas de símbolos lógicos podem ser um convite à desistência do curso. Ocorrem vezes que conseguimos nos distanciar um pouco disso, mas em outras, não. Pedimos a cada estudante que, ao se deparar com os teoremas, principalmente os mais complexos, não se sinta convidado a desistir de entendê-los!

Diferente do que ocorre com Cálculo, cuja essência consiste predominantemente não em demonstrações de resultados, mas em como aplicá-los em problemas que o envolvem, a Álgebra Abstrata tem a princípio um enfoque diferente. Nela, manipulação de teoremas, símbolos e expressões são coisas que ocorrem com muita frequência. Tudo isso pode ser bastante útil à formação do estudante, sendo, portanto, uma ferramenta que pode ajudá-lo em sua forma de raciocinar e assimilar novas ideias matemáticas.

Todo estudante que faz um curso em Cálculo Diferencial e Integral sabe de quão importante é a Matemática para as outras ciências. Suas aplicações são comuns em Física, Biologia, Química, Engenharia e Economia, por exemplo. Da mesma forma, em um curso de Álgebra Linear, o professor não tem dificuldade de apresentar aos seus alunos aplicações em um nível acessível. É comum depararmo-nos com um livro cujo título é *Álgebra Linear com Aplicações*! Por esse motivo, espera-se que todos que estudam Álgebra Abstrata tragam em si a expectativa de ver aplicações dos conceitos de grupo, anel e corpo. Todavia, isso não é tão comum em nível elementar. Em geral, suas aplicações não são acessíveis para um curso de introdução. Desse modo, preferimos não apresentar nenhuma seção a respeito.

O conteúdo do livro

O livro é constituído de nove capítulos e são divididos em três partes. A primeira (Preliminares) compreende os Capítulos 1 e 2; a segunda

(Grupos) vai do Capítulo 3 ao 5; e a terceira (Anéis) do Capítulo 6 ao 9. Embora o sumário transpareça as divisões desses capítulos, faremos comentários de cada um deles.

O Capítulo 1 traz uma revisão dos conceitos e resultados básicos de conjunto, relação e função. As seções relacionadas aos dois primeiros fazem exposições resumidas. Assim, elas não representam em nenhuma hipótese um estudo aprofundado sobre eles (e não haveria aqui motivos para tal). Caso o leitor tenha feito um curso de introdução em Cálculo, que apresenta uma abordagem desses conceitos, mesmo que sucintamente, pode prescindir de consultá-las. No entanto, elas podem servir de base para o estudante que, casualmente, sinta a necessidade de rever alguns resultados sobre conjunto das partes, imagens direta e inversa de um conjunto, função injetiva, etc.

Ainda no Capítulo 1, a seção que necessita ser lida com mais atenção é a que aborda o conceito e resultados sobre relação de equivalência e outros inerentes. Esse conceito é usado com muita frequência em Álgebra Abstrata e em outros ramos da Matemática. Tais resultados são imprescindíveis no estudo de estruturas algébricas quocientes e, por isso, o estudante com dificuldades em trabalhar com classes de equivalência e partição deverá ler essa seção com bastante atenção, analisando principalmente seus exemplos.

O Capítulo 2 apresenta os resultados principais sobre os números inteiros, $\mathbb{Z}$, e os números complexos, $\mathbb{C}$. A seção dedicada ao conjunto $\mathbb{Z}$ não traz sua construção por meio de relação de equivalência, o que em geral é feito em um curso de introdução em Teoria dos Conjuntos. No entanto, descreve resultados relevantes que, frequentemente, são usados em outros capítulos. Destacam-se, especialmente, o Princípio de Indução Finita, o conceito de divisibilidade (incluindo o máximo divisor comum) e, como não poderia deixar de ser, o Algoritmo da Divisão e resultados básicos sobre números primos. O leitor que porventura venha a estudar outros capítulos se convencerá da importância de tais conceitos. Por exemplo, no Capítulo 8, a definição de divisibilidade sobre os inteiros e muitos de seus resultados são estendidos para um domínio arbitrário.

A seção dedicada ao estudo do conjunto $\mathbb{C}$ tem finalidade similar à da seção sobre $\mathbb{Z}$. Nela, são apresentados resultados elementares sobre os complexos que, em geral, são vistos em um curso básico.

No Capítulo 3, inicia-se o estudo sobre estruturas algébricas, considerando inicialmente o conceito de grupo. Antes deste, há uma seção abordando o que de fato é necessário ao desenvolvimento do capítulo. O conceito de operação binária é apresentado juntamente com algumas notações frequentemente usadas para representá-las. Há também uma quantidade razoável de exemplos, incluindo também os contraexemplos; aliás, isso é muito comum em todo livro. Destacamos as principais propriedades relacionadas às operações, tais como associatividade, distributividade, existência de elemento neutro e elementos invertíveis. Após isso, o conceito de grupo segue naturalmente.

Queremos aqui fazer um comentário adicional sobre a seção que versa sobre operações binárias. Alguns professores preferem não dedicar mais do que três aulas para apresentar os resultados principais sobre elas. Particularmente, não vemos muitas vantagens em alongá-las, mesmo porque tais resultados são facilmente absorvidos a partir da própria definição de grupo. No entanto, alguns colegas são testemunhas de que dificilmente se leciona para turmas homogêneas. O que frequentemente ocorre é que, em uma mesma turma, estudantes formam grupos de diferentes níveis de conhecimento; às vezes, isso pode impossibilitar que o professor seja sucinto no que concerne aos tópicos básicos. Algo semelhante ocorre com frequência em um curso de Cálculo Diferencial. Muitas vezes, devido à dificuldade da turma, o professor é "forçado" a fazer uma revisão considerável sobre funções e números reais. Foi pensando nisso que preferimos abordar operações binárias separadamente.

Há dez seções que abordam tópicos estudados em um curso básico sobre grupos, entre os quais estão os conceitos de subgrupo, classe lateral e grupo quociente. Eles foram apresentados detalhadamente em seções separadas, de modo a possibilitar um bom entendimento por parte do estudante.

No Capítulo 4, estudamos homomorfismos de grupos, que são as principais funções entre grupos, cuja seção principal é a que destaca o Teorema Fundamental dos Homomorfismos, seguido de algumas de suas aplicações. Essa seção foi desenvolvida pensando na dificuldade que os alunos apresentam em trabalhar com esse teorema. As demonstrações dos corolários que lhe sucedem (em alguns livros são deixadas como exercícios) foram feitas de modo que o leitor obtenha familiaridade com o processo de construção do epimorfismo inicial. É claro que isso não é suficiente, e o estudante há de se conscientizar de que familiarizar-se com o uso deste teorema é uma questão de prática.

O Capítulo 5 apresenta os grupos alternados (ou grupo das permutações pares). É um capítulo sucinto, mas apresenta resultados básicos e importantes sobre esses grupos. Eles são imprescindíveis no estudo sobre solubilidade de equações algébricas por radicais (a essência da Teoria de Galois). No entanto, isso não significa dizer que ele só deva ser consultado para esse fim. Ele pode ser útil a todo leitor interessado em se aprofundar mais sobre grupos de permutações.

No Capítulo 6, inicia-se o estudo básico sobre anéis. Seu desenvolvimento é bastante similar ao do Capítulo 3. A partir do conceito de anel, há uma sequência natural de outros relacionados, tais como subanel, domínio, corpo, homomorfismo de anéis, ideal e anel quociente.

O Capítulo 7 trata sobre anéis de polinômios e é uma continuação do Capítulo 6. A importância desse tema e os detalhes apresentados justificam o fato de ele ter sido destacado em capítulo à parte. Apresentamos resultados clássicos sobre raízes e fatores de polinômios e polinômios irredutíveis sobre corpos. Ao estudá-lo, o leitor perceberá que alguns resultados relacionados aos polinômios irredutíveis são similares aos obtidos sobre números primos. Existência de máximo divisor comum entre dois polinômios (incluindo alguns inerentes), Identidade de Bachet-Bézout (para polinômios) e fatoração de um dado polinômio como produto de polinômios irredutíveis levarão o leitor a recordar o Capítulo 2.

O Capítulo 8 também é uma continuação do estudo sobre anéis. Nele se estuda domínios de forma mais aprofundada. Particularmente, aborda três importantes tipos de domínios: domínio de ideais principais, domínio de fatoração única e domínio euclidiano. Inicia-se destacando domínios de ideais principais com resultados similares a alguns obtidos sobre o domínio dos números inteiros (um exemplo importante deles). Nessa parte, destaca-se, especialmente, o tratamento dado aos domínios quadráticos dotados da função norma. Em seguida, são considerados domínios de fatoração única, começando com um breve histórico destacando a importância desses domínios, não apenas para a Álgebra em si, mas também para a Teoria dos Números Algébricos, por exemplo. Seu desenvolvimento se dá objetivando mostrar que todo domínio de ideais principais é um domínio de fatoração única e que a propriedade de fatoração única em um domínio pode ser estendida para anéis de polinômios. O estudo dele se completa com domínios euclidianos.

O Capítulo 9 (opcional) se apresenta resumidamente, pois não se tem a intenção de explorar com detalhes os tópicos nele estudados. Ele traz resultados básicos sobre extensões de corpos, objetivando considerar o conceito de corpo de raízes de um polinômio. Abordamos, especialmente, as extensões finitas dos racionais, as quais são construídas pelo processo clássico de adjunção de raízes, o que é preponderante para alcançar o seu objetivo. Aproveitamos, também, a inclusão desse capítulo para demonstrar alguns resultados que foram apenas apresentados e usados em capítulos anteriores.

Referência Cruzada

Cabe uma palavra adicional sobre a citação de cada resultado ao longo do livro. A fim de que o leitor possa localizar com mais agilidade os resultados citados por referência cruzada, decidimos incluir também a página na qual o resultado está localizado, a menos que ele se encontre no mesmo capítulo referenciado. Por exemplo, ao mencionar, no Capítulo 4, o Exemplo 3.8.12, escrevemos: pelo Exemplo 3.8.12 (pág. 186). Por outro lado, ao citar este mesmo exemplo no Capítulo 3, escrevemos simplesmente: pelo Exemplo 3.8.12.

Os exercícios propostos e soluções

Uma parte relevante e que desperta maior interesse no estudante é a que contém os exercícios propostos. Há mais de 680 deles ao longo do livro, e sua maioria tem a finalidade de fixar a aprendizagem, enquanto uma pequena parte surge como uma forma de acrescentar algo à teoria apresentada no texto.

Quando se estuda por um determinado livro — e este não é exceção —, o estudante é praticamente levado a seguir o caminho estabelecido pelo autor. As divisões dos capítulos, as ordens com que as seções foram dispostas, a prova ou não de um dado teorema são a forma de guiá-lo ao longo do livro. No entanto, isso não ocorre com as seções dos exercícios propostos. Uma de suas características é conduzi-lo com relativa independência.

Os exercícios são sempre apresentados em três níveis: fácil, médio e difícil. A variedade deles (excetuando a Seção 3.10) objetiva fazer o estudante assimilar gradativamente os resultados abordados, e ao iniciar a resolução dos exercícios, ele terá condições de saber até que ponto está sabendo usar os conceitos e teoremas. Há uma diferença considerável em absorver o resultado de um teorema e saber aplicá-lo depois!

A distribuição dos exercícios relacionados a cada tópico foi feita buscando dispô-los em ordem crescente com respeito ao nível de dificuldade. De certa forma, há uma coerência entre eles e os exemplos que foram trabalhados ao longo do texto, no sentido de que, no texto, o nível aumenta gradativamente, exigindo do estudante um pouco mais de atenção à medida que ele avança na leitura. Pela boa didática, é natural que se inicie uma sequência de exemplos com os mais simples, de modo a motivar propostas mais complexas. Entendemos que um de fácil solução seja uma boa forma de estimular o leitor a prosseguir.

Foi nessa linha de raciocínio que elaboramos e dispusemos os exercícios. Alguns contêm mais de seis itens, e isto pode tornar algo repetitivo e enfadonho. Mas, resolver todos ou não é uma decisão que só cabe ao estudante. Se ele já se sente seguro sobre os conceitos exigidos em um dado exercício, então, não vemos motivo para que resolva do item (a) ao item (f). Já ciente disto, ele será automaticamente convidado a encarar seu próximo desafio, um problema de outro nível ou que envolva outros conceitos.

Os exercícios marcados com asterisco $(*)$ são os que exigirão um pouco mais de empenho do aluno, forçando-o a obter mais familiaridade no trato dos conceitos relacionados. O fato é que alguns poderiam até ser destacados com dois asteriscos, $(**)$, dando uma conotação de mais difíceis. Contudo, acreditamos que muitos acharão que determinados problemas sem a estrelinha deveriam ser destacados com ela e vice-versa. Sabemos o quanto esses são desafiadores para os estudantes e que os levam a certo pânico. Mas na realidade, não foram colocados para este fim. Foram selecionados para quem deseja gastar um pouco mais de energia.

Muitas vezes nos dedicamos exaustivamente na solução de um problema considerado difícil, porém podemos não resolvê-lo. É claro que isso pode trazer desânimo, mas quando se dedica um tempo extra na solução de um exercício dessa natureza, mesmo que não se tenha "sucesso", é inegável que algo da teoria envolvida é assimilada, e isso será útil em ocasião oportuna. Desse modo, o estudante não deve se desencorajar, mas encarar os exercícios marcados com as famosas estrelinhas. O fato é que alguns deles são muito difíceis. Todavia, após analisarmos o grau de dificuldade de todos, estamos convictos de que a maioria deles pode ser resolvida por aquele que é habituado a estudar algo a mais, que não se acostumou a estudar apenas para fazer provas e garantir aprovação.

No final do livro estão as soluções e/ou respostas dos exercícios ímpares. Entretanto, cabe-nos chamar a atenção daquele que muito se apressa em conferir respostas. É aconselhável que uma consulta a essa parte seja considerada como último recurso e que seja feita após algumas tentativas de solução. Não é conveniente que o estudante, ao menor sinal de dificuldade, recorra automaticamente às soluções dadas. Isso pode trazer prejuízo ao seu aprendizado, podendo levá-lo a ser um simples espectador.

Uma palavra aos estudantes

Queremos chamar a atenção de todo aquele que porventura venha a estudar por este livro. Como já mencionamos, as seções dos exercícios propostos de um livro-texto são a parte que desperta maior interesse, sendo um atrativo à parte; elas são um ambiente adequado de autoavaliação e, por isso, é perfeitamente compreensível que os mais afoitos busquem o mais rápido possível solucionar os exercícios.

Por mais delineados que sejam ministrados os conteúdos, é quase que impossível para o professor apresentar todos os detalhes de um dado tópico em sala de aula. Não que isso seja negativo, pelo contrário, é uma excelente forma de o professor conduzir o aluno à leitura dos livros-texto. Sendo assim, após cada aula, é razoável que o estudante estabeleça o hábito de se fazer um estudo do que foi visto, analisando com bastante atenção os exemplos trabalhados, uma vez que, em geral, eles são uma fonte de informações que pode auxiliar nas resoluções dos problemas e ajudar a fixar, se não todas, mas as principais ideias. Em seguida, ele deve procurar resolver os exercícios propostos, começando com os mais fáceis e, quem sabe, indo até aos mais difíceis. Na medida do possível, é apropriado estabelecer um procedimento de estudo, tornando-o mais agradável e interessante. Isso pode ser útil e decisivo em seu aprendizado.

Leia cada seção do texto pausadamente, reescrevendo cada definição e resultado sempre que houver necessidade. Às vezes, você terá que ler uma parte do texto mais de uma vez, revendo os exemplos, teoremas, demonstrações, etc. Se isto for necessário, faça-o com dedicação.

Agradecimentos

Expressamos nossos sinceros agradecimentos aos colegas professores Antônio Brandão e Thiago Dourado por suas valiosas sugestões, bem como à LF Editorial pela confiança. Nossa gratidão também a todos os autores dos livros que foram base para a elaboração deste texto.

Críticas e sugestões

Desde já agradecemos ao leitor que se dispuser em nos comunicar sobre os erros contidos no texto que porventura venham a ser detectados, enviando-nos por meio do e-mail: vandenberglv@yahoo.com.br. O leitor poderá também enviar suas críticas e sugestões. Todas serão bem-vindas e analisadas com bastante atenção.

VANDENBERG LOPES VIEIRA

Campina Grande, agosto de 2025

Sumário

Prefácio VII

Lista de Símbolos XXVII

I Preliminares 1

1 Conjuntos, Relações e Funções 3
1.1 Conjuntos . . . 3
1.1.1 Relação de Inclusão . . . 6
1.1.2 Conjuntos Finitos e Infinitos . . . 7
1.2 Operações entre Conjuntos . . . 8
1.2.1 Produto Cartesiano . . . 9
1.2.2 União, Interseção e Diferença entre Conjuntos . . . 11
1.2.3 Algumas Propriedades . . . 14
1.2.4 Conjunto das Partes . . . 17
1.2.5 Partição de um Conjunto . . . 18
1.2.6 Exemplos . . . 19
1.3 Exercícios . . . 20
1.4 Relações de Equivalência . . . 24
1.4.1 Exemplos . . . 24
1.4.2 Classe de Equivalência e Conjunto Quociente . . . 28
1.4.3 Exemplos . . . 29

1.4.4 Resultados Básicos 32
1.5 Exercícios 35
1.6 Funções 37
1.6.1 Uma Observação Importante 38
1.6.2 Exemplos 39
1.6.3 Funções Bijetivas 42
1.6.4 Composição de Funções 47
1.6.5 Funções Invertíveis 52
1.7 Exercícios 56

2 Conjuntos dos Números Inteiros e Complexos 61
2.1 Os Números Inteiros 62
2.1.1 Propriedades Básicas 64
2.1.2 Valor Absoluto 68
2.1.3 Princípio da Boa Ordenação 69
2.1.4 Indução Matemática 71
2.1.5 Potência em $\mathbb{Z}$ 75
2.1.6 Divisibilidade em $\mathbb{Z}$ 77
2.1.7 O Algoritmo da Divisão 79
2.1.8 Máximo Divisor Comum 83
2.1.9 Algoritmo de Euclides sobre $\mathbb{Z}$ 87
2.1.10 Algumas Consequências 90
2.1.11 Máximo Divisor Comum de Mais de Dois Inteiros 91
2.1.12 Mínimo Múltiplo Comum 93
2.1.13 Mínimo Múltiplo Comum de Mais de Dois Inteiros 95
2.2 O Teorema Fundamental da Aritmética 95
2.2.1 O Crivo de Eratóstenes 100
2.2.2 Fatoração de Fermat 101
2.3 Exercícios 104
2.4 Os Números Complexos 109
2.4.1 Algumas Propriedades 112
2.4.2 Raízes da Unidade 121
2.5 Exercícios 124