Tópicos de Álgebra Clássica

•

Um Prelúdio à
Álgebra Moderna

Textuniversitários 1

César Polcino Milies

Tópicos de Álgebra Clássica

•

Um Prelúdio à Álgebra Moderna

LF EDITORIAL

Editora Livraria da Física
São Paulo – 2020

1a. Edição

Editor: 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)

Milies, César Polcino
Tópicos de álgebra clássica : um prelúdio à álgebra moderna / César Polcino Milies. – São Paulo : Editora Livraria da Física, 2020. – (Série textuniversitários ; 1)

Bibliografia.
ISBN 978-85-7861-639-7

1. Álgebra 2. Álgebra - História 3. Matemática - Estudo e ensino 4. Professores - Formação I. Título. II. Série.

19-31521 CDD-512

Índices para catálogo sistemático:
1. Álgebra : Matemática 512

Maria Paula C. Riyuzo – Bibliotecária – CRB-8/7639

ISBN 978-85-7861-639-7

Impresso no Brasil
Printed in Brazil

LF EDITORIAL
Editora Livraria da Física
Tel./Fax: +55 11 3459-4327 / 3936-3413
www.livrariadafisica.com.br

Prefácio

[. . .] *devemos ser curiosos em conhecer a caminhada, muitas vezes indireta e penosa, dos inventores, os diferentes passos que foram dados para alcançar seu fim* [. . .] *Este conhecimento, alias, não é mera curiosidade:* [. . .] *sempre serve para lançar luz sobre os objetos com os quais estamos envolvidos.*

J.L. Lagrange[*]

A forma em que a álgebra é apresentada nos cursos de graduação passou por uma mudança radical. Não muito tempo atrás, ela ainda era vista na mesma forma em que C.F. Gauss a define no clássico *Disquisitiones Arithmeticae*, escrito quando o autor tinha apenas 21 anos e publicado em 1801[†]:

"A Álgebra é a arte de reduzir e resolver equações".

Um estudante de graduação contemporâneo certamente iria estranhar esta definição, pois está acostumado a que a álgebra lhe seja apresentada como o

[*] J.L. Lagrange, *Leçons élémentaires sur les mathématiques données à l'École Normale en 1795*, Œuvres complètes, tome 7, 183-288.

[†] C.F. Gauss, *Disquisitiones Arithmeticae* (English Edition), W.C. Waterhouse (Editor), Springer-Verlag, New York, 1986, 498 pp.

estudo de certas estruturas operatórias, definidas a partir de um conjunto de axiomas.

Esta forma moderna de apresentar a álgebra é o resultado de um longo processo de abstração e formalização que teve início no século XIX e passou gradativamente a permear toda a atividade matemática ao longo do século passado.

Quando este processo estava ainda em pleno desenvolvimento algumas vozes se alçaram advertindo contra os perigos de abstrações prematuras. De fato, Henri Lebesque (1875-1941), um dos grandes nomes da matemática contemporânea, escreveu[*]:

> *"Numa época em que as considerações abstratas desempenham um papel importante, mesmo na ciência experimental, deve-se lembrar que aqueles que se movem no abstrato mas fazem porém obra útil, têm um agudo senso de realidade.*
>
> *É este sentido que é necessário criar nos jovens e depois, só depois, a passagem à abstração pode resultar proveitoso. Sob a abstração é necessário ver o concreto, no geral, todas as coisas verdadeiramente úteis."*

Mais recentemente, ao tentar justificar o fato de que a primeira definição abstrata de *grupo*, dada por A. Cayley em 1854, passou desapercebida para os pesquisadores da época, M. Kline[†] observou que:

> *"Abstrações prematuras caem em ouvidos surdos, tanto quando estes pertencem a matemáticos como quando pertencem a estudantes."*

Este texto trata de alguns assuntos ao modo da álgebra clássica, com um duplo objetivo. Por um lado, esperamos transmitir ao leitor o "sentido de realidade" de que fala Lebesgue; pelo menos na medida em que isto é possível em álgebra.

Por outro lado esperamos contribuir para uma formação sólida, em especial dos estudantes de licenciatura e professores do ensino médio em

[*] H. Lebesgue, *Sur la mesure des grandeurs*, Gauthier-Villars, Paris, 1936, p.2.

[†] M. Kline, *Mathematical thought from ancient to modern times*, Oxford Univ. Press, New York, 1972.

temas que deverão tratar na sua prática docente, que está razoavelmente distante da álgebra abstrata.

Ao longo do texto, apelamos frequentemente à história da disciplina, porque é justamente aí onde fica evidente a necessidade de introduzir novos conceitos e onde pode-se perceber 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.

O livro teve origem em notas que preparamos para a disciplina de álgebra ministrada no mestrado profissionalizante oferecido pelo Instituo de Matemática e Estatística da Universidade de São Paulo. Ao ministrar a disciplina tínhamos em mente justamente a ideia de antecipar, no contexto que é mais familiar ao leitor, ideias que depois seriam apresentadas do ponto de vista abstrato.

No primeiro capítulo apresentamos os números inteiros de forma axiomática – embora não excessivamente formalizada – e damos especial atenção ao princípio de indução. Aproveitamos para tratar de aplicações importantes, como o Teorema do Binômio e a sequência de Fibonacci.

No capítulo seguinte tratamos da aritmética modular, assunto de capital importância não somente pela sua aplicação à teoria elementar de números, como também pelo fato de que pode ser utilizada como exemplo paradigmático a fim introduzir, em cursos mais avançados a ideia de estrutura quociente.

No terceiro capítulo tratamos da história e métodos de resolução de equações de terceiro e quarto graus. Esses assuntos não são tão relevantes do ponto de vista da prática do professor de ensino médio e podem ser omitidos numa primeira leitura. Porém, eles são de fundamental importância do ponto de vista histórico pois trazem em si a motivação para a introdução dos números complexos.

O capítulo quarto é dos mais importantes. Nele introduzimos a noção de número complexo que é fundamental nas mais variadas áreas da matemática. Nele tentamos não somente fazer uma exposição que contribua para dar uma formação sólida ao leitor como também dar uma perspectiva histórica e uma noção das várias formas de fundamentar esta teoria.

No capítulo seguinte tratamos de polinômios e equações algébricas. Talvez seria mais natural, do ponto de vista formal, tratar primeiro deste assunto antes de equações particulares ou dos números complexos. Nós optamos por uma ordem mais próxima da origem histórica. A publicação do método de resolução das equações de terceiro e quarto graus é de 1545, a primeira exposição dos polinômios como conjunto de entes matemáticos entre os quais estão definidas operações – semelhante ao conjunto dos números inteiros, nas palavras do seu autor – é devida a Simon Stevi, em 1585, e finalmente, a notação atual é essencialmente devida a Descartes, em 1637.

Vale a pena observar que discutimos apenas conceitos próximos à prática do professor do ensino médio. Conceitos importantíssimoos, tais como irredutibilidade de polinômios e suas consequências são aqui apenas mencionados, pois seu estudo aprofundado é mais natural no contexto abstrato.

No capítulo sexto tratamos de alguns aspectos importantes da teoria do ponto de vista da resolução de equações e o capítulo culmina com uma demonstração razoavelmente elementar do Teorema Fundamental da Álgebra.

No capítulo seguinte nos aproximamos já da álgebra abstrata. Tratamos da teoria de permutações que, embora tivesse sua origem na teoria de equações e seja aqui explorada no contexto o mais concreto possível, contém em si a motivação para teoria de grupos bem como suas ideias mais fundamentais.

O capítulo final contém uma exposição muito breve das estruturas fundamentais da álgebra abstrata onde ilustramos os conceitos básicos com exemplos da álgebra clássica incluídos anteriormente no texto.

Na disciplina do mestrado profissionalizante em que nasceram estas notas concluímos o curso tratando dos conceitos fundamentais da teoria de corpos e aplicamos estas noções para discutir a não resolubilidade dos problemas clássicos da geometria elementar por meio da régua e do compasso. Não incluímos aqui esta exposição porque ela resulta mais natural num curso de álgebra abstrata e esperamos nos ocupar dela oportunamente*.

Agradecemos ao nosso aluno e amigo Thiago Augusto Silva Dourado pela inestimável colaboração na produção da versão final do texto. Embora ele tenha corrigido inúmeros erros de digitação e revisado cuidadosamente todos os exercícios, os erros que subsistirem são da nossa inteira responsabilidade.

* C. Polcino Milies, *Um curso de álgebra (com perspectiva história e aplicações)*, a ser publicado.

Sumário

1

Números Inteiros

1.1 Introdução

A geometria foi considerada uma ciência lógico-dedutiva, estabelecida sobre bases sólidas, desde o século IV a.C., quando foram publicados os *Elementos* de Euclides de Alexandria (c.325–265 a.C.). Esta obra foi tida como um modelo de rigor e elegância na exposição durante mais de dois mil anos, pois desenvolve o assunto enunciando uma série de postulados e, a partir destes, demonstra logicamente todas as afirmações feitas. É a obra mais publicada na história da humanidade, depois da Bíblia; dela foram feitas mais de mil edições.

Já a aritmética foi estudada inicialmente desde um ponto de vista mais ingênuo. Os inteiros positivos $1, 2, 3, \ldots$ são tão comuns à nossa experiência, que foram chamados de *números naturais*. Os matemáticos trabalharam com eles sem sentir a necessidade de uma formalização rigorosa das idéias.

O mesmo não aconteceu com os inteiros negativos. Eles foram relativamente bem aceitos na coletividade matemática graças às suas diversas interpretações e usus práticos, como representando dívidas, ou como medidas de temperaturas "abaixo de zero", etc. Porém, as dúvidas quanto a sua legitimidade apareceram em diversas ocasiões. Em 1543, Michael Stifel (1548–1567) ainda os chamava de *números absurdos* e Girolamo Cardano (1501–1576), um contemporâneo de Stifel, os considerava *soluções falsas de uma equação*.

A situação se agravou com a introdução dos números complexos no século XVI, quando estes tornaram-se necessários para compreender certos casos que aparecem na resolução de equações de terceiro grau. Eles foram sendo aceitos aos poucos por causa de sua grande utilidade, tanto na matemática com em algumas de suas aplicações.

Porém, as dúvidas quanto à sua legitimidade permaneceram e o próprio Leonhard Euler (1707–1783), que os utilizara magistralmente em muitos de seus trabalhos (vide pág. 103).

Nas primeiras décadas do século XIX, um grupo de matemáticos ingleses tentou colocar a álgebra em bases tão sólidas quanto se considerava fossem as da geometria. Para isso, eles tentaram compreender e explicitar "os axiomas da álgebra". George Peacock (1791–1858), no seu *Tratise on Algebra*, publicado em 1830 e ampliado a dois volumes em 1845, destaca pela primeira vez a importância das chamadas "leis formais", que passam a desempenhar o papel dos axiomas na álgebra. O seu contemporâneo e amigo, Augusto de Morgan (1806–1871) assumiu uma atitude parecida na sua *Trigonometry and double algebra*, publicada também em 1830. Com esta primeira tentativa de axiomatização começa um longo processo em direção a álgebra abstrata.

1.2 Números Inteiros: Primeiras Propriedades

Acreditamos que o leitor já deve estar familiarizado com os números inteiros e suas principais propriedades. Mesmo assim, vamos resumir rapidamente algumas delas, que serão necessárias ao longo do texto. Os conceitos de relação e operação podem ser definidos formalmente, mas no momento os empregaremos apenas num sentido intuitivo que seguramente é familiar ao leitor.

Os números inteiros foram um conjunto que denotaremos por $\mathbb{Z}$, no qual estão definidas duas operações, que chamaremos de *adição* e *multiplicação* e representaremos por $+$ e $\cdot$ respectivamente. Dados dois inteiros $a, b \in \mathbb{Z}$, o resultado da adição de a e b será denotado por $a+b$ e será chamado chamado a *soma* destes números. Da mesma forma, o resultado da multiplicação será denotado por $a \cdot b$ ou, quando conveniente, simplesmente por ab e será chamado de *produto* de a e b.

Aceitaremos que valem as propriedades seguintes, que serão os *axiomas* do conjunto dos números inteiros.

Para a soma:

(A.1) (Propriedade Associativa) *Para toda terna de inteiros* a, b *e* c *tem-se que:*

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

(A.2) (Existência de neutro) *Existe um elemento, que denotaremos por* 0, *denominado* neutro aditivo, *tal que:*

$$a+0 = 0+a = a, \text{ para todo } a \in \mathbb{Z}.$$

(A.3) (Existência de oposto) *Para cada inteiro* a *existe um outro inteiro, que denotaremos por* $-a$ *e chamaremos de seu* oposto *tal que:*

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

(A.4) (Propriedade comutativa) *Para cada par de inteiros* a *e* b *tem-se que:*

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

Para o produto:

(A.5) (Propriedade Associativa) *Para toda terna de inteiros* a, b *e* c *tem-se que:*

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

(A.6) (Existência de neutro) *Existe um elemento, que denotaremos por* 1, *denominado* neutro multiplicativo, *tal que:*

$$a1 = 1a = a, \text{ para todo } a \in \mathbb{Z}.$$

(A.7) (Propriedade cancelativa) *Dados inteiros* a, b *e* c *com* $a \neq 0$, *tem-se que:*

$$\text{se } ab = ac \text{ então } b = c.$$

(A.8) (Propriedade comutativa) *Para cada par de inteiros* a *e* b *tem-se que:*

$$ab = ba.$$

Relacionando ambas operações:

(A.9) (Propriedade Distributiva) *Para toda terna de inteiros a, b e c tem-se que:*

$$a\,(b+c) = ab + ac,$$
$$(a+b)\,c = ac + bc.$$

A partir destas propriedades, pode-se demonstrar todas as outras propriedades das operações que nos são familiares. Damos alguns exemplos nas listas de exercícios. O leitor interessado pode consultar diversos textos, como o de G. Birkhoff e S. MacLane [1], S.C. Coutinho [6], A. Hefez [12], L.H. Jacy Monteiro [14] e ainda nosso texto [5].

Em $\mathbb{Z}$ também está definida uma relação que permite comparar seus elementos, a relação "menor o igual", que denotaremos por $\leq$ e que tem as seguintes propriedades.

(A.10) (Propriedade Reflexiva) *Para todo inteiro a tem-se que: $a \leq a$.*

(A.11) (Propriedade Antissimétrica) *Dados dois inteiros a e b, tem-se que:*

$$\textit{se } a \leq b \textit{ e } b \leq a, \textit{ então } a = b.$$

(A.12) (Propriedade Transitiva) *Dados três inteiros a, b e c, tem-se que:*

$$\textit{se } a \leq b \textit{ e } b \leq c \textit{ então } a \leq c.$$

Devido a estas propriedades, costuma-se dizer que a relação $\leq$ é uma *relação de ordem.*

É comum utilizar o símbolo $a < b$ para indicar que $a \leq b$ mas $a \neq b$. Neste caso diz-se que *a é menor que b.* Em particular, se $a < 0$, diz-se que a é um inteiro *negativo* e se $0 < a$, diz-se um inteiro *positivo.*

(A.13) (Tricotomia) *Dados dois inteiros a e b, tem se que:*

$$a < b \quad \textit{ou} \quad a = b \quad \textit{ou} \quad b < a.$$

A relação "menor o igual" está intimamente vinculada as operações em $\mathbb{Z}$. Isto é explicitado nos próximos axiomas que expressam a *compatibilidade* da relação com as operações.

(A.14) *Para toda terna a, b e c de inteiros tem-se que:*

$$se\ a \leq b\ então\ a + c \leq b + c.$$

(A.15) *Para toda terna a, b e c de inteiros tem-se que:*

$$se\ a \leq b\ e\ 0 \leq c\ então\ ac \leq bc.$$

Também usamos $a \geq b$, respectivamente $a > b$, para indicar que $b \leq a$, respectivamente $b < a$, e dizemos que *a é maior ou igual a b*, respectivamente *a é maior que b*.

Para apresentar o último axioma, precisamos introduzir primeiro mais alguns conceitos.

Definição 1.2.1 Diz-se que um conjunto A de inteiros é *limitado inferiormente* se existe um inteiro k tal que $k \leq a$, para todo elemento $a \in A$.

Diz-se que um conjunto A de inteiros *tem elemento mínimo* se existe um elemento $a_0 \in A$ tal que $a_0 \leq a$, para todo elemento $a \in A$ (a tricotomia permite mostrar facilmente que, se A tem mínimo, este elemento é único). Neste caso, denotamos

$$a_0 = \min(A).$$

De forma análoga definem-se conjuntos *limitados superiormente* e o *elemento máximo* de um conjunto de inteiros.

Agora estamos em condições de enunciar nosso último axioma. Como o leitor verificará no decorrer do texto, ele é extremamente útil para a construção da teoria e para muitos demonstrações, nos mais diversos contextos.

(A.16) (Princípio da Boa Ordem) *Todo conjunto de inteiros limitado inferiormente tem mínimo.*

A partir destes axiomas, podem-se demonstrar todas as propriedades conhecidas dos números inteiros e suas operações. A título de ilustração provaremos algumas delas, seguramente bem conhecidas do leitor. Começaremos mostrando que, para a soma, também vale a propriedade cancelativa.

Proposição 1.2.2 *Sejam a, b e c inteiros.*

$$\textit{Se } a + c = b + c \textit{ então } a = b.$$

Demonstração: Somando o oposto de c a ambos membros da igualdade do enunciado, temos

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

e, aplicando a propriedade associativa da soma,

$$a + [c + (-c)] = b + [c + (-c)],$$

donde,

$$a + 0 = b + 0, \text{ o que implica } a = b.$$

□

Proposição 1.2.3 *(i) Para todo inteiro a tem-se que $a0 = 0$.*

(ii) Se a e b são inteiros tais que $ab = 0$ então $a = 0$ ou $b = 0$.

Demonstração: Para demonstrar *(i)* note que

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

Comparando o primeiro e último termo desta cadeia de igualdades e aplicando a propriedade cancelativa da soma, temos:

$$a0 = 0.$$

Para demonstrar *(ii)*, usando a parte anterior, podemos escrever a igualdade $ab = 0$ na forma

$$ab = a0.$$

Se $a = 0$, a nossa afirmação está demonstrada. Se $a \neq 0$, aplicando a propriedade cancelativa do produto, resulta $b = 0$. □

Muitas outras propriedades podem ser demonstradas de modo análogo. O leitor encontrará algumas delas propostas como exercícios.

Exercícios

1. Demonstre a *Regra dos Sinais*; isto é, prove que, se a e b são inteiros, então valem as seguintes igualdades:

   (a) $-(-a) = a$.

   (b) $(-a)\,b = -(ab) = a\,(-b)$.

   (c) $(-a)\,(-b) = ab$.

2. Sejam a e b inteiros. Provar que:

   (a) Se $a^2 = 0$ então $a = 0$.

   (b) Se $a^2 = a$ então $a = 0$ ou $a = 1$.

   (c) A equação $a + X = b$ tem uma única solução em $\mathbb{Z}$.

3. Demonstrar que, para todo par de inteiros a e b tais que $a < b$ tem-se que $-b < -a$.

4. Dado um inteiro a, chama-se *valor absoluto* de a, ao inteiro $|a|$ definido da seguinte forma:
$$|a| = \begin{cases} a & \text{se} \quad a \geq 0, \\ -a & \text{se} \quad a < 0. \end{cases}$$
   Provar que:

   (a) $|a| \leq 0$ se e somente se $a = 0$.

   (b) $-|a| \leq a \leq |a|$.

   (c) $|-a| = |a|$.

   (d) $|ab| = |a|\,|b|$.

   (e) $|a + b| \leq |a| + |b|$ (*Desigualdade Triangular*).

   (f) $||a| - |b|| \leq |a - b|$.

5. Lembramos que um inteiro a diz-se *positivo* se $a > 0$ e *negativo* se $a < 0$.

   (a) Provar que todo conjunto de inteiros positivos tem mínimo.

(b) Provar que a afirmação acima é equivalente ao Princípio da Boa Ordem; isto é, admitindo que todo conjunto de inteiros positivos tem mínimo, prove que o Princípio da Boa Ordem é verdadeiro.

6. Sejam a e b inteiros positivos. Provar que sempre existe um inteiro positivo n tal que $na > b$. (Esta afirmação é conhecida como *Propriedade Arquimediana*).

7. Provar que a equação $X^2 + 1 = 0$ não tem solução em $\mathbb{Z}$.

8. Para cada inteiro a, provar que o número $a - 1$ é o maior inteiro que é menor que a.

9. Provar que não existe nenhum inteiro x tal que $0 < x < 1$.

10. Sejam a, b e c inteiros. Provar que:

    (a) Se $c > 0$ e $ac < bc$, então $a < b$.

    (b) Se $c < 0$ e $ac < bc$ então $a > b$. (*Sugestão:* dividir em casos; por exemplo, supondo $a, b \geq 0$, etc.)

11. Provar que, se $a^7 = b^7$ então $a = b$. (*Sugestão:* dividir em casos; como no exercício anterior.)

12. Mostrar que para todo par de inteiros a e b tem-se que $a^2 - ab + b^2 \geq 0$.

13. Prove que não existe um número inteiro que seja *o maior de todos*; isto é, prove que o conjunto dos números inteiros não tem máximo.

1.3 O Princípio de Indução

As ciências naturais utilizam a chamada *indução empírica* para deduzir as leis que regem certos fenômenos. Assumindo que a natureza se comporta de forma regular, a partir de um grande número de observações é às vezes possível enunciar uma *lei* e esperar que ela seja verdadeira. Por exemplo, ninguém duvidaria de que, quando um corpo é liberado à ação do seu próprio peso, no vácuo, na superfície da terra, ele cai segundo a vertical local.