Fundação CECIERJ

Consórcio cederj

Centro de Educação Superior a Distância do Estado do Rio de Janeiro

Álgebra I

Volume 4

Hernando Bedoya

Ricardo Camelier

GOVERNO DO Rio de Janeiro

SECRETARIA DE CIÊNCIA E TECNOLOGIA

UNIVERSIDADE ABERTA DO BRASIL

Ministério da Educação

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Apoio:

FAPERJ

Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro

Fundação Cecierj / Consórcio Cederj

Rua da Ajuda, 5 – Centro – Rio de Janeiro, RJ – CEP 20040-000
Tel.: (21) 2333-1112 Fax: (21) 2333-1116

Presidente
Carlos Eduardo Bielschowsky

Vice-presidente
Masako Oya Masuda

Coordenação do Curso de Matemática
UFF - Marcelo Correa
UNIRIO - Luiz Pedro San Gil Jutuca

Material Didático

ELABORAÇÃO DE CONTEÚDO
Hernando Bedoya
Ricardo Camelier

COORDENAÇÃO DE DESENVOLVIMENTO INSTRUCIONAL
Cristine Costa Barreto

COORDENAÇÃO DE AVALIAÇÃO DO MATERIAL DIDÁTICO
Débora Barreiros

AVALIAÇÃO DO MATERIAL DIDÁTICO
Letícia Calhau

Departamento de Produção

EDITOR
Tereza Queiroz

COORDENAÇÃO DE PRODUÇÃO
Jorge Moura

CAPA
Eduardo Bordoni

PRODUÇÃO GRÁFICA
Verônica Paranhos

B412a

Bedoya, Hernando.
Álgebra I. v. 4 / Hernando Bedoya; Ricardo Camelier. – Rio de Janeiro : Fundação CECIERJ, 2013.
56p.; 19 x 26,5 cm.

ISBN: 85-7648-313-0

1. Equações polinominais. 2. Teorias dos anéis.
I. Camelier, Ricardo. II. Título.

CDD: 512

Referências Bibliográficas e catalogação na fonte, de acordo com as normas da ABNT.

Governo do Estado do Rio de Janeiro

Governador
Sérgio Cabral Filho

Secretário de Estado de Ciência e Tecnologia
Gustavo Reis Ferreira

Universidades Consorciadas

CEFET/RJ - CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
Diretor-geral: Carlos Henrique Figueiredo Alves

UENF - UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE DARCY RIBEIRO
Reitor: Silvério de Paiva Freitas

UERJ - UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
Reitor: Ricardo Vieiralves de Castro

UFF - UNIVERSIDADE FEDERAL FLUMINENSE
Reitor: Roberto de Souza Salles

UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Reitor: Carlos Levi

UFRRJ - UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
Reitora: Ana Maria Dantas Soares

UNIRIO - UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
Reitor: Luiz Pedro San Gil Jutuca

SUMÁRIO

Aula 19 – Uma introdução histórica _____ **7**
Hernando Bedoya / Ricardo Camelier

Aula 20 – As primeiras equações polinomiais _____ **15**
Hernando Bedoya / Ricardo Camelier

Aula 21 – Teoria dos anéis – 1ª parte _____ **23**
Hernando Bedoya / Ricardo Camelier

Aula 22 – Teoria dos anéis – 2ª parte _____ **31**
Hernando Bedoya / Ricardo Camelier

Aula 23 – Subanéis e ideais _____ **43**
Hernando Bedoya / Ricardo Camelier

Referências _____ **55**

Uma introdução histórica

AULA 19

Meta da aula

Apresentar alguns problemas clássicos que motivaram as estruturas algébricas modernas.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as raízes históricas de problemas que propiciaram grande desenvolvimento no campo da Álgebra.
- Descrever problemas da Geometria que são traduzidos para problemas da Álgebra.

BREVE HISTÓRICO

Sabemos que a maior contribuição dos matemáticos gregos da Antigüidade foi o desenvolvimento do método axiomático, segundo o qual toda teoria matemática é desenvolvida com base em objetos primitivos, definições, postulados, teoremas e dedução lógica. E é claro que o grande exemplo desenvolvido por eles de uma teoria matemática, segundo o método axiomático, foi a geometria euclidiana. O espaço, os pontos, as retas e os planos são exemplos de objetos primitivos, para os quais não temos uma definição, e, portanto, só contamos com nossa intuição para dar um sentido a eles. Os postulados, ou axiomas, são as propriedades fundamentais que os objetos primitivos devem satisfazer. Os postulados não são justificados, e, hoje, as principais restrições feitas sobre um sistema de postulados exigem que sejam independentes, isto é, nenhum deles deve ser deduzido a partir dos demais, e que sejam consistentes, ou seja, que eles não levem a uma contradição matemática. Por exemplo, na geometria euclidiana, o postulado mais conhecido é o Postulado de Euclides, que afirma que dados uma reta e um ponto fora dela, existe uma única reta que passa por este ponto e é paralela à reta dada. No desenvolvimento da teoria, cada novo conceito é estabelecido por meio de uma definição. Na geometria euclidiana, por exemplo, duas retas são definidas como perpendiculares quando elas se cortam formando um ângulo reto. Os teoremas são todas as propriedades que os objetos da teoria venham a satisfazer. Cada teorema deve ser acompanhado por uma demonstração, que é uma justificativa da validade desta propriedade, utilizando apenas os conhecimentos obtidos anteriormente e um método de dedução lógica. Na geometria euclidiana, o teorema mais conhecido é o Teorema de Pitágoras, que afirma que em todo triângulo retângulo, o quadrado da hipotenusa é igual à soma dos quadrados dos catetos. Tudo isto foi sistematizado nas obras *Os Elementos* de Euclides (cerca de 300 a.C.).

Um dos grandes interesses dos matemáticos gregos foi o problema da construção de figuras geométricas utilizando régua e compasso. Por régua, entendemos um instrumento capaz apenas de traçar uma reta por dois pontos dados. As réguas dos geômetras gregos não tinham um sistema de marcações que possibilitasse medir o comprimento de um segmento de reta. E, assim, eles foram capazes de realizar um grande número de construções geométricas, como a divisão de um segmento em duas partes iguais, a construção da bissetriz de um ângulo, a construção de uma reta perpendicular a uma reta dada e até a construção de um pentágono regular. No entanto, eles não foram capazes de resolver alguns problemas de construção aparentemente simples. Alguns destes problemas, por incrível que pareça, só foram resolvidos dois mil anos depois, no século XIX, e foram, em grande parte, responsáveis pelo surgimento das estruturas algébricas que são o objeto dos nossos estudos neste curso. Vamos apresentar três destes importantes problemas. O primeiro é o *problema da duplicação do cubo*, ou seja, construir um cubo cujo volume seja o dobro do volume de um cubo dado. O segundo é o *problema da trisecção de um ângulo*, que consiste em dividir um ângulo dado em três partes iguais. O terceiro é o *problema da quadratura do círculo*, que consiste em construir um quadrado cuja área seja igual à área de um círculo dado.

Somente no século XIX, a matemática se desenvolveu o suficiente para que os matemáticos pudessem, finalmente, concluir que estes três problemas clássicos são impossíveis, ou seja, estas três construções não podem, em geral, ser realizadas utilizando-se apenas instrumentos como a régua e o compasso. Para que isto pudesse acontecer, foi preciso desenvolver uma linguagem algébrica na qual estes problemas geométricos pudessem ser naturalmente traduzidos. Cada um deles foi transformado num problema equivalente na teoria de equações polinomiais, e foi a questão da resolução de equações polinomiais que levou os matemáticos a desenvolver as estruturas algébricas de grupos e anéis. É interessante notar que estes problemas geométricos foram resolvidos usando-se os novos métodos da álgebra, desenvolvidos em grande parte pelas idéias geniais de matemáticos como N. Abel (1802-1829) e E. Galois (1812-1832), e não por métodos geométricos. Isto vem ressaltar o papel central que a álgebra exerce dentro do conhecimento matemático.

O PROBLEMA DA DUPLICAÇÃO DO CUBO

Vamos traduzir os dois primeiros problemas para a linguagem algébrica das equações polinomiais. Um número *d* é *construtível* quando ele é o comprimento de um segmento de reta construtível por régua e compasso, a partir de um segmento de reta unitário. Para o problema da duplicação do cubo, dado um cubo de volume unitário, queremos construir a aresta x de um cubo de volume 2, isto é, queremos resolver a equação $x^3 = 2$. Em particular, queremos mostrar que a solução desta equação, $x = \sqrt[3]{2}$, é um número construtível.

O PROBLEMA DA TRISECÇÃO DO ÂNGULO

Para o problema da trisecção do ângulo, queremos construir o ângulo θ a partir de um ângulo dado 3θ. Agora, a construção do ângulo θ é equivalente à construção de $\cos\theta$, como sugere a **Figura 1.1**, considerando a reta perpendicular a um dos lados do ângulo θ no círculo unitário.

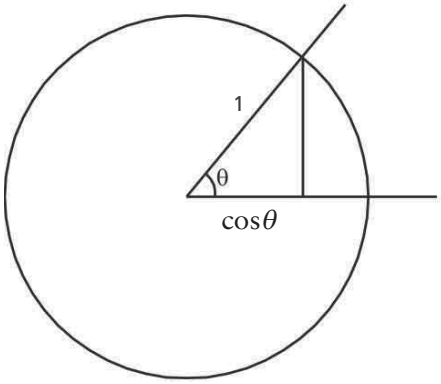

Figura 1.1: A construção de $\cos\theta$ a partir do ângulo θ.

Assim, a trisecção do ângulo é equivalente à construção de $\cos\theta$ a partir de $\cos 3\theta$.

ATIVIDADES

1. Exercite sua trigonometria demonstrando a identidade: $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.

Portanto, considerando $x = \cos\theta$ e $c = \cos 3\theta$, a identidade anterior é equivalente à equação polinomial:

$$4x^3 - 3x = c.$$

Para o caso particular da trisecção do ângulo de 60°, temos $c = \cos 60^o = 1/2$, o que nos dá $4x^3 - 3x = \frac{1}{2}$,

ou, multiplicando a equação por 2, obtemos: $8x^3 - 6x = 1$.

O problema da trisecção do ângulo de 60° é, então, equivalente a mostrar que a equação polinomial $8x^3 - 6x = 1$ tem raiz positiva construtível. Que isto não pode acontecer, assim como o número $\sqrt[3]{2}$ não é construtível, é um dos fatos que foram provados somente em 1837, pelo matemático P. L. Wantzel.

Uma generalização muito elegante do problema da trisecção do ângulo é a divisão em n partes iguais do círculo unitário ou, de forma equivalente, a construção do polígono regular de n lados. Esse problema também pode ser traduzido para a linguagem algébrica. Ele é equivalente a provar que o ponto de coordenadas $\left(\cos\frac{2\pi}{n}, \operatorname{sen}\frac{2\pi}{n}\right)$ é construtível. Denotando por

$Z = \cos\frac{2\pi}{n} + i\operatorname{sen}\frac{2\pi}{n}$, esse número é solução da equação $z^n = 1$.

2. Prove a identidade:

$$z^n - 1 = (z-1)\left(z^{n-1} + z^{n-2} + \ldots + z + 1\right).$$

Portanto, de $z^n = 1$, obtemos a equação

$$z^n - 1 = 0,$$

e, pela identidade da Atividade 1, queremos resolver a equação

$$(z-1)\left(z^{n-1} + z^{n-2} + \ldots + z + 1\right) = 0.$$

Como z tem de ser diferente de 1, o problema da construção do polígono regular de n lados é equivalente a encontrar soluções construtíveis da equação:

$$z^{n-1} + z^{n-2} + \ldots + z + 1 = 0.$$

CONCLUSÃO

Como você pode ver, muitos problemas geométricos são traduzidos naturalmente para problemas envolvendo soluções de equações polinomiais, o que já justifica plenamente a importância de uma teoria de equações polinomiais. E é uma compreensão profunda dessa teoria que dá origem às idéias fundamentais da álgebra moderna, como veremos na próxima aula.

Faremos uma pequena observação sobre o problema da quadratura do círculo. Esse problema é equivalente a mostrar que o número π é construtível. Mas este não é um problema da Álgebra, e sim da Análise. Foi o matemático F. Lindemann, no século XIX, que provou que o número π não é solução de nenhuma equação polinomial de coeficientes inteiros e que, conseqüentemente, não é construtível.

RESUMO

Alguns problemas geométricos surgidos na Antigüidade se transformam naturalmente em problemas sobre equações polinomiais. Na próxima aula, continuaremos a estudar problemas clássicos envolvendo equações polinomiais.

ATIVIDADES FINAIS

1. Mostre que a equação $z^4+z^3+z^2+z+1=0$ é equivalente a $z^2+z+1+\frac{1}{z}+\frac{1}{z^2}=0$.

2. Mostre que a equação $z^2+z+1+\frac{1}{z}+\frac{1}{z^2}=0$ é equivalente à equação quadrática $t^2+t-1=0$ na variável $t=z+\frac{1}{z}$.

RESPOSTAS

Atividade 1

Utilizando as fórmulas bem conhecidas:

$$\cos(a+b) = \cos a \cos b - \operatorname{sen} a \operatorname{sen} b,$$
$$\cos 2\theta = \cos^2\theta - \operatorname{sen}^2\theta \text{ e}$$
$$\operatorname{sen} 2\theta = 2\operatorname{sen}\theta\cos\theta,$$

obtemos

$$\begin{aligned}\cos(3\theta) &= \cos(2\theta+\theta)\\ &= \cos 2\theta\cos\theta - \operatorname{sen}2\theta\operatorname{sen}2\theta\\ &= \left(\cos^2\theta - \operatorname{sen}^2\theta\right)\cos\theta - 2\operatorname{sen}\theta\cos\theta\operatorname{sen}\theta\\ &= \left(\cos^2\theta - \left(1-\cos^2\theta\right)\right)\cos\theta - 2\cos\theta\left(1-\cos^2\theta\right)\\ &= 4\cos^3\theta - 3\cos\theta.\end{aligned}$$

Atividade 2

Você pode aplicar indução e o passo indutivo é dado por:

$$\begin{aligned}z^{n+1}-1 &= \left(z^{n+1}-z\right)+(z-1)\\ &= z\left(z^n-1\right)+(z-1)\\ &= z(z-1)+\left(z^{n-1}+z^{n-2}+\ldots+z+1\right)+(z-1)\\ &= (z-1)\left[z\left(z^{n-1}+z^{n-2}+\ldots+z+1\right)+1\right]\\ &= (z-1)\left(z^n+z^{n-1}+\ldots+z+1\right).\end{aligned}$$

Atividade Final 1

É só dividir por z^2.

Atividade Final 2

Observe as transformações: $z^2 - z + 1 + \frac{1}{z} + \frac{1}{z^2} = \left(z^2 - \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1$

$$\begin{aligned}&= \left(\left(z+\frac{1}{z}\right)^2 - 2\right) + \left(z+\frac{1}{z}\right) + 1\\ &= \left(z+\frac{1}{z}\right)^2 + \left(z+\frac{1}{z}\right) - 1\\ &= t^2 + t - 1.\end{aligned}$$

Portanto, a equação: $z^2 + z + 1 + \frac{1}{z} + \frac{1}{z^2} = 0$

se transforma em: $t^2 + t - 1 = 0$.

As primeiras equações polinomiais

AULA 20

Meta da aula

Apresentar alguns problemas clássicos que motivaram as estruturas algébricas modernas.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as raízes históricas de problemas que propiciaram grande desenvolvimento no campo da Álgebra.
- Descrever o processo de solução de equações polinomiais de segundo e terceiro graus.

INTRODUÇÃO

Dando continuidade aos problemas expostos na primeira aula, vamos descrever a solução das equações polinomiais de segundo e terceiro graus, ou seja, das equações quadráticas e cúbicas. Esses problemas fazem parte de uma discussão que motivou um grande desenvolvimento da Álgebra.

A EQUAÇÃO QUADRÁTICA

A equação quadrática geral pode ser dada por

$$ax^2 + bx + c = 0,$$

com coeficientes $a, b, c \in \mathbf{R}$ e $a \neq 0$. A idéia geral é obter as soluções dessa equação em função dos coeficientes e das operações mais simples. Na busca destas soluções, uma técnica importante é a aplicação de mudanças de variável, ou substituições, de modo que a equação original seja transformada numa equação bem mais simples e, portanto, mais fácil de ser resolvida.

Dividindo esta equação quadrática geral por a, obtemos

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0. \qquad (1.1)$$

Completando o quadrado dos termos em x, temos

$$x^2 + \frac{b}{a}x = \left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2},$$

e substituindo na equação 1.1, ficamos com

$$\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0,$$

ou, ainda,

$$\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2} = 0. \qquad (1.2)$$

Fazendo a mudança de variável $t = x + \frac{b}{2a}$, a equação 1.2 se transforma em $t^2 = \frac{b^2 - 4ac}{4a^2}$.

Observe que esta nova equação é quadrática em *t*, mas não possui um termo de primeiro grau na nova variável. Portanto, aplicando a substituição $t = x + \frac{b}{2a}$, obtivemos uma nova equação mais simples que a original. E ela é facilmente resolvida em *t*, apresentando as soluções

$$t = \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$

Substituindo de volta $t = x + \frac{b}{2a}$, obtemos

$$x + \frac{b}{2a} = \pm \frac{\sqrt{b^2 - 4ac}}{2a},$$

e, finalmente, as soluções

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a},$$

(1.3)

Observe que esta fórmula para a solução da equação quadrática é dada em função dos coeficientes *a*, *b* e *c* utilizando os operadores aritméticos +, –, x, ÷, e o operador raiz quadrada $\sqrt{\ }$. A solução da equação quadrática surgiu pela primeira vez com o renomado matemático muçulmano Al-Khwarizmi no século IX.

A EQUAÇÃO CÚBICA

Com um pouco mais de trabalho, podemos obter uma fórmula semelhante para a equação cúbica. A equação cúbica geral é dada por

$$ax^3 + bx^2 + cx + d = 0, \qquad (1.4)$$

com coeficientes $a, b, c, d \in \mathbf{R}$ e $a \neq 0$. Lembre que a idéia é aplicar mudanças de variáveis de modo a simplificar cada vez mais a equação. Para isso, começamos substituindo $t = x + \frac{b}{3a}$, ou seja, $x = t + \frac{b}{3a}$, na equação 1.4.

ATIVIDADE

1. Mostre que a equação 1.4 se transforma em

$$t^3 = pt + q, \qquad (1.5)$$

onde os novos coeficientes p e q são calculados em função dos coeficientes originais a, b, c e d.

A equação 1.5 é mais simples que a equação 1.4, mas ainda não podemos resolvê-la diretamente. O truque, agora, é aplicar a substituição $t = u + v$. Obtemos

$$(u+v)^3 = p(u+v) + q,$$

que pode ser reescrito como

$$3uv(u+v) + u^3 + v^3 = p(u+v) + q,$$

o que sugere a escolha

$$3uv = p \text{ e } u^3 + v^3 = q.$$

Assim, substituindo $v = p/3u$, na segunda equação anterior, obtemos

$$u^3 + \left(\frac{p}{3u}\right)^3 = q,$$

que pode ser reescrita como

$$\left(u^3\right)^2 - qu^3 + \left(\frac{p}{3}\right)^3 = 0.$$

Esta última equação é uma equação quadrática em u^3. E como v^3 satisfaz a mesma equação, as soluções são

$$u^3 = \frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3} \text{ e } v^3 = \frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}.$$

Assim, a solução da equação 1.5 é dada por

$$t = u + v = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$$

e, portanto,

$$x = t - \frac{b}{3a} = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} - \frac{b}{3a}$$

é a solução da equação cúbica geral $ax^3 + bx^2 + cx + d = 0$. Observe, mais uma vez, que esta fórmula é dada em função dos coeficientes a, *b*, *c* e *d* utilizando os operadores aritméticos +, —, X, ÷ e os operadores raiz quadrada $\sqrt{\ }$ e raiz cúbica $\sqrt[3]{\ }$. A solução da equação cúbica foi obtida pela primeira vez pelo matemático italiano del Ferro no século XVI. Ainda no século XVI, o matemático francês Viète descobriu que o problema da trisecção do ângulo, visto na Aula 1, é equivalente a uma equação cúbica.

A equação geral de quarto grau é dada por

$$a_4x^3 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0,$$

de coeficientes $a_i \in \mathbf{R}, i = 0,1,2,3,4$ e $a_4 \neq 0$. Esta equação também pode ser resolvida em função dos coeficientes a*i* utilizando apenas os operadores aritméticos +, –, x, ÷ e o operador raiz quadrada $\sqrt{\ }$. Sua solução foi obtida pela primeira vez pelo matemático italiano Ferrari, também do século XVI.

O problema geral que se colocava, então, era o de resolver a equação polinomial de grau *n*,

$$a_nx^n + a_{n-1}x^{n-1} + \ldots + a_ix + a_0 = 0$$

em função dos coeficientes $a_i \in \mathbf{R}, i = 0,1,2,\ldots,n(a_n \neq 0)$, utilizando apenas os operadores aritméticos +, –, X, ÷ e os operadores de raiz $\sqrt{\ }$, $\sqrt[3]{\ }$, …, $\sqrt[n]{\ }$. Dizemos, quando isso é possível, que a equação é *solúvel por radicais*. Após a solução por radicais das equações de terceiro e quarto graus, no século XVI, um grande objetivo da Álgebra passou a ser a solução por radicais da equação geral de quinto grau. Devido à grande dificuldade desse problema, os matemáticos começaram a pensar na impossibilidade de tal solução. Somente no século XIX o matemático norueguês Abel e o matemático francês Galois conseguiram provar tal fato. Foi deste empreendimento que surgiram os conceitos de grupo, anel, corpo e dimensão, que possibilitaram controlar muitos aspectos de um processo de cálculo sem a necessidade de fato de efetuar estes cálculos.

CONCLUSÃO

A tentativa de resolver estes problemas clássicos, envolvendo equações polinomiais, motivou o surgimento das estruturas algébricas de anel, corpo e grupo. Pelo estudo das equações quadrática e cúbica e pelo que você desenvolveu nas atividades, você já deve ter notado como o trabalho com equações polinomiais envolve tantos cálculos algébricos. É importante que você se habitue com esse traquejo algébrico e até venha a apreciá-lo. Ele permeia todo o estudo da Álgebra.

A próxima atividade vai auxiliá-lo a praticar mais alguns cálculos algébricos.

ATIVIDADE FINAL

Mostre que a mudança de variável $t = x + \frac{b}{4a}$, ou $x = t - \frac{b}{4a}$, transforma a equação geral de quarto grau $ax^4 + bx^3 + cx^2 + dx + e = 0$ na equação de quarto grau $t^4 + pt^2 + qt + r = 0$, sem o termo cúbico, isto é, sem o termo em t^3. Calcule os coeficientes *p*, *q* e *r* em função dos coeficientes *a*, *b*, *c*, *d* e *e*.

RESPOSTAS

Atividade 1

Para desenvolver a expressão $x^3 = \left(t - \frac{b}{3a}\right)^3$, você poderá usar o produto notável

$$(a-b)^3 = a^3 - 3a^2b + 3ab^2 - b^3.$$

Observe que os termos quadráticos em *t* vão se cancelar.

Você deverá chegar às seguintes expressões:

$$p = \frac{b^2}{3a^2} - \frac{c}{a} \text{ e } q = -\frac{2b^3}{27a^3} + \frac{bc}{3a^2} - \frac{d}{a}.$$

Atividade Final

Para desenvolver a expressão $x^4 = \left(t - \frac{b}{4a}\right)^4$, você poderá usar o produto notável

$$(a-b)^4 = a^4 - 4a^3b + 6a^2b^2 - 4ab^3 = b^4.$$

Observe que os termos cúbicos em *t* irão se cancelar.

Você deverá chegar às seguintes expressões:

$$p = -\frac{3b^2}{8b^2} + \frac{c}{a}, q = \frac{b^3}{8a^3} + \frac{d}{a} \text{ e } r = \frac{3b^4}{256a^4} + \frac{b^2c}{16a^3} - \frac{bd}{4a^2} + \frac{e}{a}.$$

Não se assuste com a contabilidade dos coeficientes!

Teoria dos anéis – 1ª parte

AULA 21

Meta da aula

Descrever a estrutura algébrica de anel como uma generalização de determinadas propriedades dos números inteiros.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as propriedades que caracterizam um anel.
- Apresentar exemplos de anéis.
- Aplicar os axiomas de anel para justificar a unicidade de alguns de seus elementos.

Pré-requisito

Você precisará das propriedades do anel dos inteiros módulo n.

INTRODUÇÃO

Nesta aula, vamos dar início ao estudo formal da estrutura algébrica chamada anel. Vamos fazer isto revendo algumas propriedades já bem conhecidas dos números inteiros, que serão generalizadas para muitas outras situações. Aproveite!

NOSSO PRIMEIRO ANEL

Você sabe que o conjunto dos números inteiros

$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

é munido de duas operações, a adição (+) e a multiplicação (·), que satisfazem determinadas propriedades. Queremos ressaltar as seguintes propriedades satisfeitas por estas operações. Se $a, b, c, \in \mathbf{Z}$, temos:

Z1. A operação de adição é associativa: $(a+b)+c = a+(b+c)$.

Z2. A operação de adição é comutativa: $a+b = b+a$.

Z3. A operação de adição tem um elemento neutro, o número 0: $a+0 = 0+a = a$.

Z4. Todo número inteiro possui um simétrico: para todo inteiro a, existe outro inteiro $-a$, o elemento *oposto* de a, tal que $a+(-a)=(-a)+a = 0$.

Z5. A operação de multiplicação é associativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Z6. A operação de multiplicação é comutativa: $a \cdot b = b \cdot a$.

Z7. A operação de multiplicação tem um elemento neutro, o número 1: $a \cdot 1 = 1 \cdot a = a$.

Z8. As operações de multiplicação e adição satisfazem as leis distributivas: $a \cdot (b+c) = a \cdot b + a \cdot c$ e $(b+c) \cdot a = b \cdot a + c \cdot a$.

Acontece que estas propriedades são comuns a muitos outros conjuntos munidos de duas operações. Sendo assim, podemos nos abstrair dos casos particulares e tratar de uma estrutura algébrica geral, neste caso, chamada *anel*.

OS AXIOMAS QUE TODO ANEL TEM DE SATISFAZER

Definição 1

Um *anel (comutativo)* é um conjunto não-vazio A, munido de duas operações binárias, $+$ e $\cdot$, chamadas de uma *adição* e uma *multiplicação*, respectivamente, que satisfazem os seguintes axiomas ($a,b,c \in A$):

A1. A operação de adição é associativa: $(a+b)+c = a+(b+c)$.

A2. A operação de adição é comutativa: $a+b = b+a$.

A3. A operação de adição tem um elemento neutro: existe um elemento $0 \in A$, tal que $a+0 = 0+a = a$.

A4. Todo elemento de A possui um simétrico: para todo $a \in A$, existe um $a' \in A$, tal que, $a+a' = a'+a = 0$.

A5. A operação de multiplicação é associativa: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$.

A6. A operação de multiplicação é comutativa: $a\cdot b = b\cdot a$.

A7. A operação de multiplicação tem um elemento neutro: existe um elemento $e \in A$, $e \neq 0$, tal que $a\cdot e = e\cdot a = a$.

A8. As operações de multiplicação e adição satisfazem as leis distributivas: $a\cdot(b+c) = a\cdot b+a\cdot c$ e $(b+c)\cdot a = b\cdot a+c\cdot a$.

Observações:

1. Observe que, ao exigir que $+$ e $\cdot$ sejam operações binárias em A, já estamos exigindo que elas sejam *fechadas* em A, isto é, dados $a,b \in A$, então $a+b \in A$ e $a\cdot b \in A$. O elemento $a+b$ é chamado de *soma* (de a e b), e o elemento $a\cdot b$ é chamado de produto (de a e b).

2. Quando apenas o axioma A6 não for satisfeito, ou seja, quando a multiplicação não é comutativa, dizemos tratar-se de um *anel não-comutativo*. Em algumas situações, é conveniente tratar de estruturas, deste tipo. Mas, neste curso, trataremos apenas dos anéis comutativos. Por termos incluído o axioma A7, que trata do elemento neutro da multiplicação, alguns autores costumam chamar este anel de *anel comutativo com unidade*.

3. Devido à comutatividade das duas operações, os axiomas A3, A4, A7 e A8 poderiam conter apenas as seguintes igualdades:

A3: $a+0 = a$
A4: $a+a' = 0$
A7: $a \cdot e = a$
A8: $a \cdot (b+c) = a \cdot b + a \cdot c$

As igualdades restantes:

$0+a = a$; $a'+a = 0$; $e \cdot a = a$ e $(b+c) \cdot a = b \cdot a + c \cdot a$,

seguem como conseqüências dos axiomas de comutatividade A2 e A6.

4. O elemento neutro da adição é único: se $0' \in A$, é tal que $a+0' = 0'+a = a$, então:

$0' = 0+0' = 0$.

Vamos justificar estas igualdades usando os axiomas de anel. Temos:
$0' = 0+0'$ pelo axioma A3 para o elemento 0;
$0+0' = 0$ pelo axioma A3 para o elemento $0'$;
O elemento neutro da adição é chamado de *zero de A*.

5. O elemento simétrico é único: dado $a \in A$, seja $a'' \in A$, tal que $a+a'' = a''+a = 0$, então

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

Como o elemento simétrico é único, podemos ter uma notação especial para ele. Assim, denotamos por $-a$ o elemento simétrico de a, denotamos por $a-b$ a soma $a+(-b)$ e chamamos esta operação $(-)$ de *subtração*. O elemento $a-b$ é chamado de *diferença* de a e b.

6. O elemento neutro da multiplicação é único: se $e' \in A$ é tal que $a \cdot e' = e' \cdot a = a$, então

$e' = e \cdot e' = e$.

O elemento neutro da multiplicação é, muitas vezes, denotado por 1_A ou, simplesmente, por 1.

7. Denotamos um anel por $(A, +, \cdot)$. Quando as operações estiverem claras no contexto, então denotaremos o anel simplesmente por A.

ATIVIDADES

1. Justifique as igualdades apresentadas na observação 5 usando os axiomas de anel, assim como fizemos na observação 4.

2. Justifique as igualdades apresentadas na observação 6 usando os axiomas de anel, assim como fizemos na observação 4.

MUITOS EXEMPLOS DE ANÉIS

Vamos agora estudar alguns exemplos de anéis.

Exemplo 1

Seja $A = \mathbf{Z}$, com as operações usuais de adição e multiplicação. Então, como foi visto no início da aula, $(\mathbf{Z}, +, \cdot)$ é um anel.

Exemplo 2

Seja $A = \mathbf{Q}$, com as operações de adição e multiplicação de frações. Neste caso, $(\mathbf{Q}, +, \cdot)$ é um anel, já que os números racionais satisfazem aquelas mesmas propriedades iniciais dos números inteiros.

Exemplo 3

Seja $A = \mathbf{R}$, com as operações de adição e multiplicação de números reais. Neste caso, $(\mathbf{R}, +, \cdot)$ é um anel, já que os números reais também satisfazem as mesmas propriedades iniciais dos números inteiros.

Exemplo 4

Seja $A = \mathbf{C}$, o conjunto dos números complexos, com as operações de adição e multiplicação de números complexos. Neste caso, $(\mathbf{C}, +, \cdot)$ é um anel, já que os números complexos também satisfazem as mesmas propriedades iniciais dos números inteiros.

Exemplo 5

Seja n um inteiro positivo e $A = \mathbf{Z}_n$ o conjunto das classes de congruência módulo n. Com as operações de adição e multiplicação de classes de congruência, vistas no curso de Álgebra I, segue que $(\mathbf{Z}_n, +, \cdot)$ é um anel. Reveja a Aula 11 do seu curso de Álgebra I. O elemento neutro da adição é dado pela classe de congruência $\overline{0}$, e o elemento neutro da multiplicação é a classe de congruência $\overline{1}$. O elemento oposto da classe de congruência $\overline{a}$ é dado pela classe de congruência $\overline{(-a)}$.

Exemplo 6

Seja A o conjunto de todas as funções $f: \mathbf{R} \to \mathbf{R}$. Dadas $f, g \in A$, definimos a soma $f+g$ e o produto $f \cdot g$ por:

$$(f+g)(x) = f(x)+g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x), \; x \in \mathbf{R}.$$

Por exemplo, se $f(x) = x$ e $g(x) = 3x^2$, então $(f+g)(x) = x+3x^2$ e $(f \cdot g)(x) = 3x^2$. Com isso, definimos uma adição e uma multiplicação em A.

ATIVIDADE

3. Verifique que $(A, +, \cdot)$, apresentado no exemplo 6, é um anel em que o elemento neutro da adição é a função identicamente nula, $n(x) = 0$, e o elemento neutro da multiplicação é a função constante igual a 1, $e(x) = 1$.

_____

_____

Exemplo 7

Seja $\mathbf{N}=\{0,1,2,3,...\}$ o conjunto dos inteiros não-negativos (os *números naturais*). Então, com as operações usuais de adição e multiplicação, $(\mathbf{N}, +, \cdot)$ não é um anel, pois já não satisfaz o axioma A5. Por exemplo, o número $2 \in \mathbf{N}$ não tem simétrico em $\mathbf{N}$, isto é, não existe natural n tal que $2+n = 0$.

Exemplo 8

Sejam $(A, +, \cdot)$ e $(B, +, \cdot)$ dois anéis e $A \times B$ o produto cartesiano dos conjuntos A e B. Em $A \times B$, definimos as operações de adição e multiplicação por:

$(a,b)+(a',b')= (a+a',b+b')$
$(a\cdot b)\cdot(a',b')= (a\cdot a',b\cdot b')$.

ATIVIDADE

4. Verifique que $(A \times B, +, \cdot)$ é um anel, chamado *soma direta* de A e B e denotado por $A \times B$ ou $A \otimes B$. Determine quem são os elementos neutros da adição e da multiplicação e o elemento simétrico.

_____

_____

_____

RESUMO

Os axiomas A1 a A8 caracterizam os anéis, a primeira das estruturas algébricas que estudaremos neste curso. Nas observações que seguem os axiomas de anel, já há algumas conseqüências simples, porém importantes, destes axiomas, como a unicidade dos elementos neutros e a unicidade do elemento simétrico.

RESPOSTAS

Atividade 1

$a''= 0+a''$ pelo axioma A3;

$0+a''= (a'+a)+a''$ pelo axioma A4 para o elemento a';

$(a'+a)+a''= a'+(a+a'')$ pelo axioma A1;

$a'+(a+a'')= a'+0$ pelo axioma A4 para o elemento a'';

$a'+0 = a'$ pelo axioma A3.

Atividade 2

$e'= e\cdot e'$ pelo axioma A7 para o elemento e;

$e\cdot e'= e$ pelo axioma A7 para o elemento e'.

Atividade 3

Basta você verificar que todos os axiomas de anel são satisfeitos.

Atividade 4

O elemento neutro da adição é $(0_A, 0_B)$, o elemento neutro da multiplicação é $(1_A, 1_B)$ e o elemento simétrico de (a, b) é $(-a, -b)$. Agora, basta você verificar que todos os axiomas de anel são satisfeitos.

Teoria dos anéis – 2ª parte

AULA 22

Meta da aula

Apresentar algumas propriedades operatórias básicas dos anéis e descrever tipos especiais de anéis, chamados domínios de integridade e corpos.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Conhecer algumas propriedades operatórias dos anéis.
- Compreender comportamentos diferentes de elementos de um anel quanto à operação de multiplicação.
- Aprender as estruturas algébricas de domínio de integridade e corpos.
- Analisar exemplos de domínios de integridade e corpos.

Pré-requisito

Você precisará das propriedades do anel dos inteiros módulo n, e dos conhecimentos de anéis desenvolvidos na aula anterior.

INTRODUÇÃO

Vamos iniciar esta aula vendo algumas propriedades características do anel dos números inteiros, que tornam os cálculos muito mais fáceis. Em seguida, vamos expandir o conceito de anel e obter duas novas estruturas algébricas.

PROPOSIÇÃO 1

Considere A um anel e $a, b \in A$. Então:

1. $a.0 = 0.a = 0$.
2. $a.(-b) = (-a).b = -(a.b)$.
3. $-(-a) = a$.
4. $(-a).(-b) = a.b$.

Demonstração

1. Você precisará ter em mãos os axiomas de anel apresentados na Aula 3. Veja que:

$a.0 = a.0 + 0$ pelo axioma A3;
$a.0 + 0 = a.0 + (a.0 + (-(a.0)))$ pelo axioma A4;
$a.0 + [a.0 + (-(a.0))] = [a.0 + a.0] + (-(a.0))$ pelo axioma A1;
$[a.0 + a.0] + (-(a.0)) = a.[0 + 0] + (-(a.0))$ pelo axioma A8;
$a.[0 + 0] + (-(a.0)) = a.0 + (-(a.0))$ pelo axioma A3;
$a.0 + (-(a.0)) = 0$ pelo axioma A4.

Assim, provamos que $a.0 = 0$.

2. Observe que:

$(-a).b = (-a).b + 0$ pelo axioma A3;
$(-a).b + 0 = (-a).b + [a.b + (-(a.b))]$ pelo axioma A4;
$(-a).b + [a.b + (-(a.b))] = [(-a).b + a.b] + (-(a.b))$ pelo axioma A1;
$[(-a).b + a.b] + (-(a.b)) = [(-a) + a].b + (-(a.b)$ pelo axioma A8;
$[(-a) + a].b + (-(a.b) = 0.b + (-(a.b))$ pelo axioma A4;
$0.b + (-(a.b)) = 0 + (-(a.b))$ pela propriedade 1;
$0 + (-(a.b)) = -(a.b)$ pelo axioma A3.

Portanto, provamos que $(-a).b = -(a.b)$.

3. Como $a + (-a) = 0$, a unicidade do elemento simétrico simplesmente diz que $-(-a) = a$.

4. Temos:

$(-a).(-b) = [(-a).b]$ pela propriedade 2;

$-[(-a).b] = -[(-a).b]$ novamente pela propriedade 2;

$-[(-a).b] = a.b$ pela propriedade.

Assim, provamos que $(-a).(-b) = a.b.\square$

ATIVIDADES

1. Faça as adaptações necessárias para provar o caso $0.a = 0$ na demonstração do item 1 da Proposição 1.

2. Faça as adaptações necessárias para provar o caso $a.(-b) = -(a.b)$ na demonstração do item 2 da Proposição 1.

3. Prove a lei distributiva para a subtração, isto é, prove que $a.(b - c) = a.b - a.c$.

EXISTEM DIFERENTES TIPOS DE ANÉIS!

Observe que a Proposição 1.1 afirma que, se a ou b for igual a zero, então $a.b = 0$. Agora, é interessante notar que existem anéis em que a multiplicação de elementos não-nulos resulta em um produto zero. Por exemplo, no anel $\mathbf{Z}_6$, temos $\overline{2} \,.\, \overline{3} = \overline{6} = \overline{0}$. Neste caso, dizemos que $\overline{2}$ e $\overline{3}$ são *divisores de zero*. Já não é o caso do anel $\mathbf{Z}$, pois, se $a \neq 0$ e $b \neq 0$, então $a.b \neq 0$, ou seja, o anel $\mathbf{Z}$ não tem divisores de zero.

Definição 1

Sejam A um anel e $a \in A$, $a \neq 0$. Dizemos que a é um *divisor de zero*, se existe $b \in A$, $b \neq 0$, tal que $a.b = 0$.

Definição 2

Um anel A é chamado de um *domínio de integridade*, se A não possui divisores de zero, isto é, se

$$a \neq 0 \text{ e } b \neq 0 \Rightarrow a.b \neq 0,$$

ou, equivalente,

$$a.b = 0 \Rightarrow a = 0 \text{ } ou \text{ } b = 0.$$

A lei do cancelamento para a multiplicação não vale, em geral, para os anéis, mas vale para os domínios de integridade.

PROPOSIÇÃO 2

Sejam A um domínio de integridade e $a,b,c \in A$. Se $a.b = a.c$ e $a \neq 0$, então $b = c$.

Demonstração

De $a.b = a.c$, segue que $a.b - a.c = 0$; logo, $a.(b - c) = a.b - a.c = 0$. Como A é domínio de integridade, $a = 0$ ou $b - c = 0$. Mas, por hipótese, $a \neq 0$; portanto, só resta a possibilidade $b - c = 0$, ou seja, $b = c$.□.

Vamos agora para o anel $\mathbf{Z}_9$. Veja que $2 \cdot 5 = 10 = 1$, ou seja, como $2 \cdot 5 = 1$, dizemos que $\overline{2}$ e $\overline{5}$ são *elementos invertíveis* de $\mathbf{Z}_9$. Já não é o caso de 6. Não existe nenhum elemento de $\mathbf{Z}_9$ que, multiplicado por $\overline{6}$, seja igual a 1. Neste caso, dizemos que o elemento $\overline{6}$ não é invertível. Na verdade, $\overline{6}$ é um divisor de zero, pois $6 \cdot 3 = 18 = 0$.

Definição 3

Sejam A um anel e $a \in A$. Dizemos que a é um *elemento invertível*, se existe $b \in A$, tal que $a.b = 1$. Neste caso, dizemos que b é um *elemento inverso* de a. Como o elemento inverso é único, podemos denotá-lo por a^{-1}. Daí, temos $a.a^{-1} = a^{-1}.a = 1$.

ATIVIDADE

4. Prove que o elemento inverso é único, isto é, prove que, se $a.b = 1$ e $a.b' = 1$, então $b = b'$. Prove também que, se a é invertível, então $(a^{-1})^{-1} = a$.

Exemplo 1

Em todo anel A, os elementos 1 e -1 são invertíveis, pois $1.1 = 1$ e $(-1).(-1) = 1$, pela Proposição 1.4. O zero não é invertível, pois, pela Proposição 1.1, $0.a = 0$ para todo $a \in A$.

Exemplo 2

Os únicos elementos invertíveis do anel $\mathbf{Z}$ são 1 e -1.

PROPOSIÇÃO 3

Um elemento $\overline{a}$ do anel $\mathbf{Z}_n$, das classes residuais módulo n, é invertível, se e somente se mdc(a,n) = 1.

Demonstração

Esta propriedade já foi demonstrada na Aula 12 do curso de Álgebra I, mas é tão importante, que vamos repeti-la aqui.

($\Rightarrow$) Se $\overline{a} \in \mathbf{Z}_n$ é invertível, então existe $\overline{b} \in \mathbf{Z}_n$, tal que $\overline{a}.\overline{b} = \overline{1}$, ou seja, $\overline{a}\,\overline{b} = \overline{1}$, o que significa que $ab = 1(\text{mod}n)$, e daí segue que $ab - 1 = kn$, assim, $ab - kn = 1$.

Se $d = \text{mdc}(a,n)$, então $d \mid a$ e $d \mid n$; logo, $d \mid (ab - Kn)$, ou seja, $d \mid 1$. Portanto, $d = 1$.

($\Leftarrow$) Se mdc $(a,n) = 1$, então, pela propriedade do MDC, existem inteiros r e s, tal que $ra + sn = 1$. Logo, $ar - 1 = (-s)n$, ou seja, $ar = 1(\text{mod}n)$. Desta forma, $\overline{ar} = \overline{1}$ e daí $\overline{a}\,.\,\overline{r} = \overline{1}$, ou seja, $\overline{a}$ é invertível.□

Exemplo 3

Os elementos invertíveis do anel $\mathbf{Z}_6$, pela Proposição 3, são $\overline{1}$ e $\overline{5}$. Já os elementos invertíveis do anel $\mathbf{Z}_9$ são $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{7}$ e $\overline{8}$.

Exemplo 4

Para todo primo p, os elementos invertíveis do anel $\mathbf{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\}$ são, pela Proposição 3, todos os elementos não nulos $\overline{1}, \overline{2}, ..., \overline{p-1}$ de $\mathbf{Z}_p$.

Exemplo 5

Todo elemento não-nulo do anel $\mathbf{Q}$, dos números racionais, é invertível, pois, se $\frac{a}{b} \in \mathbf{Q} - \{0\}$, então $\frac{a}{b}.\frac{b}{a} = 1$. Também nos anéis $\mathbf{R}$, dos números reais, e $\mathbf{C}$, dos números complexos, todo elemento não-nulo é invertível. Aliás, isto motiva a próxima definição.

Definição 4

Um anel A é chamado de *corpo*, se todo elemento não-nulo de A é invertível.

Exemplo 6

Os anéis **Q**, **R** e **C** são corpos. Agora, o anel **Z** é um domínio de integridade, mas não é um corpo.

Exemplo 7

Pelo que vimos no Exemplo 5, o anel $\mathbf{Z}_p$ é um corpo para todo p primo. Como $\mathbf{Z}_p$ só tem um número finito de elementos, dizemos que é um *corpo finito*.

PROPOSIÇÃO 4

Todo corpo é um domínio de integridade.

Demonstração

Sejam A um corpo e a,$b \in A$, com $a.b = 0$.

Se $a = 0$, então não há mais o que provar.

Se $a \neq 0$, então a é um elemento invertível de A e

$$b = 1.b = (a^{-1}.\ a).b = a^{-1}.(a.b) = a^{-1}.0 = 0,$$

o que prova que A é um domínio de integridade. □

ATIVIDADE

5. Justifique as igualdades na seqüência $b = 1.b = (a^{-1}.\ a).b = a^{-1}.(a.b) = a^{-1}.0 = 0$, da demonstração da Proposição 4, utilizando os axiomas de anel, a definição de corpo e as propriedades vistas anteriormente.

Exemplo 8

Se n não é primo, então o anel $\mathbf{Z}_n$ não é sequer um domínio de integridade. Pois, se n não é primo, então existem inteiros a e b, $1 < a < n$ e $1 < b < n$, tal que $n = ab$. Portanto,

$$a \,.\, b = ab = n = 0,$$

ou seja, a e b são divisores de zero de $\mathbf{Z}_n$.

Os exemplos 4 e 8 são tão importantes, que podemos resumi-los no seguinte teorema:

TEOREMA 1

O anel $\mathbf{Z}_n$ é um corpo, se, e somente se, n é primo. Mais ainda, se n não é primo, então o anel $\mathbf{Z}_n$ não é um domínio de integridade.

CONCLUSÃO

É natural que você encontre uma certa dificuldade para se sentir à vontade com os conceitos apresentados nesta aula. Afinal, tratamos de muitas sutilezas e isso requer amadurecimento matemático. Não tenha receio de ler e reler esta aula algumas vezes. A cada releitura alguma dúvida ficará esclarecida. Não tenha receio, também, de procurar seu tutor para esclarecer alguma passagem que resista em permanecer obscura. Mas lembre que é pela insistência que você vai vencer muitas das dificuldades na Matemática. Saiba, também, que a Matemática tem muita elegância e diversão. Nós autores achamos os assuntos tratados nesta aula muito elegantes e esperamos que você, também, venha a apreciá-los.

RESUMO

Algumas propriedades importantes de anéis fazem com que a parte operatória de anéis seja muito parecida com a do anel dos números inteiros. Os conceitos de domínio de integridade e corpo são muito importantes, e há uma variedade de exemplos e propriedades. Certifique-se de que os exemplos estejam claros na sua mente. Esperamos que você tenha tanto prazer no estudo desta aula quanto nós tivemos ao escrevê-la.

ATIVIDADES FINAIS

1. Determine todos os divisores de zero de $\mathbb{Z}_{16}$.

2. Determine os inversos de todos os elementos invertíveis de $\mathbb{Z}_8$.

3. Prove que, se p é primo, então os únicos elementos de $\mathbb{Z}_p$ que são seus próprios inversos, ou seja, $\overline{a} \,.\, \overline{a} = \overline{1}$, são $\overline{1}$ e $\overline{p-1}$.

RESPOSTAS

Atividade 1

$0.a = 0.a + 0$ pelo axioma A3;

$0.a + 0 = 0.a + (0.a + (-(0.a)))$ pelo axioma A4;

$0.a + [0.a + (-(0.a))] = [0.a + 0.a] + (-(0.a))$ pelo axioma A1;

$[0.a + 0.a] + (-(0.a)) = [0 + 0].a + (-(0.a))$ pelo axioma A8;

$[0 + 0].a + (-(0.a)) = 0.a + (-(0.a))$ pelo axioma A3;

$0.a + (-(0.a)) = 0$ pelo axioma A4.

Atividade 2

$a.(-b) = a.(-b) + 0$ pelo axioma A3;

$a.(-b) + 0 = a.(-b) + [a.b + (-(a.b))]$ pelo axioma A4;

$a.(-b) + [a.b + (-(a.b))] = [a.(-b) + a.b] + (-(a.b))$ pelo axioma A1;

$[a.(-b) + a.b] + (-(a.b)) = a.[(-b) + b] + (-(a.b))$ pelo axioma A8;

$a.[(-b) + b] + (-(a.b)) = a.0 + (-(a.b))$ pelo axioma A4;

$a.0 + (-(a.b)) = 0 + (-(a.b))$ pela propriedade 1;

$0 + (-(a.b)) = -(a.b)$ pelo axioma A3.

Atividade 3

Se os axiomas e as propriedades anteriores já estão claros para você, então você já pode resumir sua argumentação:

$$\begin{aligned} a.(b - c) &= a.\,[b + (-c)] \\ &= a.b + a.(-c) \\ &= a.b + (-(a.c)) \\ &= a.b - a.c. \end{aligned}$$

Atividade 4

Você consegue identificar a propriedade aplicada em cada igualdade?

$$\begin{aligned} b' &= 1.b' \\ &= (a.b).b' \\ &= (b.a).b' \\ &= b.(a.b') \\ &= b.1 \\ &= b. \end{aligned}$$

Agora,como $(a^{-1}).a = a.(a^{-1}) = a$, segue, pela unicidade do elemento inverso, que $(a^{-1})^{-1} = a$.

Atividade 5

Temos:

$b = 1.b$ pelo axioma A7;
$1.b = (a^{-1} - a).b$ pois a é um elemento não-nulo do corpo A;
$(a^{-1}.a).b = a^{-1}.(a.b)$ pelo axioma A5;
$a^{-1}.(a.b) = a^{-1}.0$ pela hipótese $a.b = 0$;
$a^{-1}.0 = 0$ pela proposição 1.1.

Atividade Final 1

Divisores de zero de $\mathbf{Z}_{16}$: $\overline{2}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{10}$, $\overline{12}$, $\overline{14}$.

Atividade Final 2

Elementos invertíveis de Z_8: $\overline{1}$ (com inverso $\overline{1}$), $\overline{3}$ (com inverso $\overline{3}$), $\overline{5}$ (com inverso $\overline{5}$) e $\overline{7}$ (com inverso $\overline{7}$).

Atividade Final 3

Se $\overline{a}.\overline{a} = \overline{1}$, então $\overline{a.a} = \overline{1}$, isto é, $a^2 \equiv 1 \pmod{p}$ e, portanto, $p \mid (a^2-1)$. Como $a^2 - 1 = (a-1)(a+1)$, então $p \mid (a-1)(a+1)$. Agora, como p é primo, então $p \mid (a-1)$ ou $p \mid (a+1)$.

Se $p \mid (a-1)$, então $a \equiv 1 \pmod{p}$, o que significa que $a = 1$.

Se $p \mid (a+1)$, então

$$a \equiv (-1) \pmod{p}$$
$$\equiv (p-1) \pmod{p},$$

e $a \equiv (p-1) \pmod{p}$ significa que $\overline{a} = \overline{p-1}$.

Subanéis e ideais

AULA 23

Meta da aula

Apresentar duas subestruturas algébricas contidas num anel, conhecidas por subanel e ideal.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Reconhecer as estruturas algébricas subanel e ideal.
- Identificar as propriedades que caracterizam um subanel e um ideal.
- Apresentar exemplos de subanéis e ideais.
- Apresentar e demonstrar algumas propriedades operatórias dos subanéis.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis desenvolvidos nas Aulas 21 e 22. Você também vai precisar dos conceitos de ideal de Z e dos anéis dos inteiros módulo *n*.

INTRODUÇÃO

Quando você estudou as estruturas algébricas de espaço vetorial você viu que a existência das subestruturas de subespaço vetorial enriqueceu a compreensão destas estruturas. De forma análoga, estudando o conceito de subanel e ideal, poderemos compreender melhor a estrutura algébrica de anel. Nesta aula, você será apresentado a estas duas subestruturas de um anel.

Definição 1

Seja $(A, +, \cdot)$ um anel. Um subconjunto não-vazio S, $S \subset A$, é chamado um *subanel* de A, se $(S, +, \cdot)$ é um anel sem unidade.

!

Dizer que $(S, +, \cdot)$ é um anel sem unidade significa que o axioma A7 da definição de anel não está sendo considerado, ou seja, não estamos exigindo a existência do elemento neutro da multiplicação. Reveja a definição de anel na Aula 3 e as observações que se seguem.
Lembre que, nos casos das estruturas de espaço vetorial e de grupo, temos um critério simples para determinar se um subconjunto não-vazio é um subespaço ou um subgrupo. Vamos estabelecer, também, um critério simples para determinar se um subconjunto não-vazio de um anel é um subanel.

PROPOSIÇÃO 1

Seja S um subconjunto não-vazio de um anel $(A, +, \cdot)$. Então S é um subanel de A se, e somente se, para todo $a,b \in S$, temos

S1. $a–b \in S$; e

S2. $a \cdot b \in S$.

Desta forma, basta que S seja fechado para a diferença e para o produto.

Demonstração

($\Rightarrow$) Se S é um subanel de A, então $(S, +, \cdot)$ é um anel. Logo, é imediato que $a–b \in S$ e $a \cdot b \in S$ para todo a, b $\in S$.

($\Leftarrow$) Vamos verificar que $(S, +, \cdot)$ satisfaz os axiomas de anel, com exceção do axioma A7 da existência do elemento neutro da multiplicação. Já sabemos, por S2, que S é fechado com respeito à multiplicação. Vamos verificar inicialmente que S é fechado com respeito à adição.

Primeiramente, temos $0 \in S$. Pois, como $S \neq \emptyset$, existe um elemento $a \in S$ e $0=a–a \in S$, pela condição S1.

Além disto, para todo elemento $a \in S$, como já sabemos que $0 \in S$, temos que $-a = 0-a \in S$.

Por fim, para todo $a, b \in S$, como $-b \in S$, então $a+b = a-(-b) \in S$, pela condição S1. Deste modo, S é fechado com respeito à adição. Vamos verificar os axiomas:

A1. Como a operação de adição é associativa em A, $S \subset A$ e S é fechado com respeito à adição, então ela continua associativa em S. Dizemos que S herda a associatividade da adição de A.

A2. Analogamente, S herda a comutatividade da adição de A.

A3. O zero está em S, como vimos anteriormente. As propriedades do zero são naturalmente herdadas de A.

A4. O elemento simétrico está em S, como já foi visto. As propriedades do elemento simétrico também são herdadas de A.

A5. Como S é fechado com respeito à multiplicação, segue que S herda a associatividade da multiplicação de A.

A6. Analogamente, S herda de A a comutatividade da multiplicação.

A7. Como S é fechado pelas duas operações, então S herda a propriedade distributiva de A. □

Vamos aos exemplos.

Exemplo 1

Se $(A, +, \cdot)$ é um anel, então $\{0\}$ e A são subanéis de A, chamados de subanéis triviais de A. Observe que o subanel $\{0\}$ não possui unidade, isto é, $1 \notin \{0\}$, enquanto A é um subanel com unidade, isto é, $1 \in A$.

Exemplo 2

$\mathbf{Z}$ é um subanel de $\mathbf{Q}$ com unidade.

Exemplo 3

$\mathbf{Q}$ é um subanel de $\mathbf{R}$ com unidade.

Exemplo 4

$2\mathbf{Z}$ é um subanel de $\mathbf{Z}$. Lembre que $2\mathbf{Z} = \{2k \mid k \in \mathbf{Z}\}$ é o conjunto dos números pares. Neste caso, $2\mathbf{Z}$ é um anel sem unidade, isto é, $1 \notin 2\mathbf{Z}$.

Exemplo 5

$n\mathbf{Z}$ é um subanel de $\mathbf{Z}$. Lembre que $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$, n inteiro e $n>1$, é o conjunto dos múltiplos de n. Aqui, também, $n\mathbf{Z}$ é um anel sem unidade, isto é, $1 \notin n\mathbf{Z}$.

ATIVIDADE

1. Use a Proposição 1 para verificar que são subanéis os exemplos 2 a 5.

UNIDADES DIFERENTES!

O próximo exemplo ilustra como a questão do elemento neutro no subanel pode ser complicada. Veremos um exemplo de um anel e de um subanel com unidade onde a unidade do subanel é diferente da unidade do anel!

Exemplo 6

Seja $(A, +, \cdot)$ o anel das matrizes diagonais reais de ordem 2, com as operações usuais de adição e multiplicação de matrizes, isto é,

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \; a,b \in \mathbf{R} \right\}.$$

Temos que A é um anel onde o zero é a matriz nula

$$N = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

e a unidade é a matriz

$$I_A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Seja, agora, o subconjunto

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \; a \in \mathbf{R} \right\}.$$

Então, $(S, +, \cdot)$ é um subanel de A cuja unidade é dada pela matriz

$$I_S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

que é diferente de I_A.

ATIVIDADE

2. Com relação ao exemplo 6, mostre que $(S, +, \cdot)$ é um subanel de A com unidade I_S.

TUDO VOLTA AO NORMAL NUM DOMÍNIO DE INTEGRIDADE

Este último exemplo nos faz pensar um pouco, pois unidades diferentes num anel e num subanel não é exatamente a situação mais desejada. No entanto, veremos que esse comportamento estranho não acontece quando o anel não possui divisor de zero, ou seja, quando o anel é um domínio de integridade. Veja as próximas propriedades.

PROPOSIÇÃO 2

Num domínio de integridade $(A, +, \cdot)$, as únicas soluções da equação $x^2 = x$ são 0 e 1.

Demonstração

De $x^2 = x$, temos $x^2 - x = 0$. Agora, como

$$x^2 - x = x \cdot x - x \cdot 1 = x \cdot (x - 1),$$

segue que $x \cdot (x-1) = 0$. Como A é um domínio de integridade, então temos que $x=0$ ou $x-1 = 0$, ou seja, temos $x = 0$ ou $x = 1$.□

PROPOSIÇÃO 3

Sejam A um domínio de integridade, com elemento neutro 1_A, e B um subanel de A, com elemento neutro 1_B. Então $1_B = 1_A$.

Demonstração

Como 1_B é elemento neutro de B, então $(1_B)^2 = 1_B \cdot 1_B = 1_B$ e $1_B \neq 0$. Portanto, considerando 1_B como elemento de A, temos que 1_B é uma solução não-nula de $x^2 = x$. Como A é um domínio de integridade, pela Proposição 2, segue que $1_B = 1_A$. □

GENERALIZANDO O CONCEITO DE IDEAL

Lembre que, no início do curso, você estudou os ideais do anel **Z**. Vamos, agora, estender o conceito de ideal para um anel qualquer. O objetivo do estudo dos ideais é a construção do aparato algébrico que nos possibilitará obter os anéis quocientes. Para construirmos os anéis quocientes, precisamos construir classes de equivalência nas quais podemos definir operações de adição e multiplicação. Daí a necessidade de introduzir o conceito de ideal. Será justamente a estrutura de ideal, com suas propriedades características, que possibilitará a construção dos anéis quocientes, tudo muito parecido com o que foi feito na construção dos inteiros módulo n.

Definição 2

Seja $(A, +, \cdot)$ um anel. Um subconjunto não-vazio I, $I \subset A$, é chamado de um *ideal* de A se satisfaz as seguintes propriedades:

$I1$. Se $a, b \in I$, então $a + b \in I$;
$I2$. Se $a \in A$ e $b \in I$, então $a \cdot b \in I$.

Exemplo 7

Se A é um anel, então $\{0\}$ e A são ideais de A, chamados de *ideais triviais* de A. Os ideais não-triviais de A são chamados de *ideais próprios* de A.

Exemplo 8

Considere o subanel $2\mathbf{Z}$ do anel dos inteiros $\mathbf{Z}$. $2\mathbf{Z}$ é, então, um ideal próprio de $\mathbf{Z}$. De um modo geral, o conjunto $n\mathbf{Z}$, dos múltiplos de n, $n > 1$, é um ideal próprio de $\mathbf{Z}$, chamado de *ideal gerado por n*.

ATIVIDADE

3. Mostre que $n\mathbf{Z}$ é um ideal de $\mathbf{Z}$.

Exemplo 9

Seja A um anel. Dado $a \in A$, o subconjunto

$$\langle a \rangle = \{t \cdot a \mid t \in A\}$$

é um ideal de A, chamado *ideal gerado por a*.

Exemplo 10

Seja A um anel. Dados $a, b \in A$, o subconjunto

$$\langle a,b \rangle = \{t \cdot a + s \cdot b \mid t,s \in A\}$$

é um ideal de A.

CONCLUSÃO

Dentro de um anel há uma variedade de subestruturas algébricas. Elas tendem a causar uma grande confusão mental e, caso isso tenha ocorrido, você não deve se assustar. À medida que o tempo for passando e sua mente matemática for amadurecendo, você começará a perceber como estas subestruturas vão se encaixando. Neste caso, você verá que os conceitos de subanel e ideal serão fundamentais para as construções que faremos a seguir.

ATIVIDADES FINAIS

1. Sejam R e S subanéis de um anel $(A, +, \cdot)$. Prove que $R \cap S$ também é um subanel de A.

2. Seja A um anel e $a \in A$. Mostre que $<a> = \{t \cdot a \mid t \in A\}$ é um ideal de A.

3. Seja A um anel e $a, b \in A$. Mostre que $<a,b> = \{t \cdot a + s \cdot b \mid t,s \in A\}$ é um ideal de A.

4. Sejam A um anel e I um ideal de A. Mostre que $I = A$ se, e somente se, I contém um elemento invertível de A.

5. Sejam A um anel e I um ideal de A. Mostre que A é um corpo se, e somente se, os seus únicos ideais são $\{0\}$ e o próprio A.

RESUMO

Os conceitos de subanel e ideal são estruturais. Os subanéis têm uma estrutura mais rígida quando o anel é um domínio de integridade. O conceito de ideal de um anel é uma generalização do conceito de ideal de $\mathbb{Z}$ e voltaremos a utilizá-lo na próxima aula.

RESPOSTAS

Atividade 1

$\mathbb{Z}$ é um subconjunto não-vazio de $\mathbb{Q}$ e é fechado para a subtração e o produto, logo, pela Proposição 1, $\mathbb{Z}$ é um subanel de $\mathbb{Q}$. Além disso, $\mathbb{Z}$ é um subanel com unidade, pois $1 \in \mathbb{Z}$.

Q é um subconjunto não-vazio de R e é fechado para a subtração e o produto, logo, pela Proposição 1, $\mathbb{Q}$ é um subanel de $\mathbb{R}$. $\mathbb{Q}$ é, também, um subanel com unidade, pois $1 \in \mathbb{Q}$.

$2\mathbb{Z}$ é um subconjunto não-vazio de $\mathbb{Z}$ e é fechado para a subtração e o produto, pois

S1. $2a–2b = 2(a–b) \in 2\mathbb{Z}$;

S2. $2a \cdot 2b = 2(2ab) \in 2\mathbb{Z}$.

Logo, pela Proposição 1, $2\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Observe que $2\mathbb{Z}$ é um subanel sem unidade, pois $1 \notin 2\mathbb{Z}$.

$n\mathbb{Z}$ é um subconjunto não-vazio de $\mathbb{Z}$ e é fechado para a subtração e o produto, pois

S1. $na–nb = n(a–b) \in n\mathbb{Z}$;

S2. $na \cdot nb = n(nab) \in n\mathbb{Z}$.

Logo, pela Proposição 1, $n\mathbb{Z}$ é um subanel de $\mathbb{Z}$. Observe que $n\mathbb{Z}$ é um subanel sem unidade, pois $1 \notin n\mathbb{Z}$.

Atividade 2

S é um subconjunto não-vazio de A e é fechado para a subtração e o produto, pois

S1. $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-b & 0 \\ 0 & 0 \end{pmatrix} \in S$;

S2. $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in S$.

Logo, pela Proposição 1, S é um subanel de A. Observe que S é um subanel com unidade $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, pois

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \text{ e } \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

Atividade 3

$n\mathbf{Z}$ é um subconjunto não-vazio de $\mathbf{Z}$ e é fechado para a adição e o produto, pois

I1. $na+nb=n(a+b) \in n\mathbf{Z}$;

I2. $a \cdot nb=n(ab) \in n\mathbf{Z}$.

Logo, $n\mathbf{Z}$ é um ideal de $\mathbf{Z}$.

Atividade Final 1

$R \cap S$ é não-vazio, pois $0 \in R \cap S$. Dados $a,b \in R \cap S$, temos $a,b \in R$ e $a,b \in S$. Logo,

S1. $a-b \in R$ e $a-b \in S$, e, portanto, $a-b \in R \cap S$;

S2. $a \cdot b \in R$ e $a \cdot b \in S$, e, portanto, $a \cdot b \in R \cap S$.

Logo, pela Proposição 1, $R \cap S$ é um subanel de A.

Atividade Final 2

$\langle a \rangle$ é não-vazio, pois $a \in \langle a \rangle$. Agora, $\langle a \rangle$ é fechado para a adição e o produto, pois

I1. $ta + sa = (t+s)a \in \langle a \rangle$;

I2. $b \cdot sa = (tb) \cdot a \in \langle a \rangle$, para todo $b \in A$.

Logo, $\langle a \rangle$ é um ideal de A.

Atividade Final 3

$\langle a,b \rangle$ é não-vazio, pois $a,b \in \langle a,b \rangle$. Agora, $\langle a,b \rangle$ é fechado para a adição e o produto, pois

I1. $(t_1a+s_1b) + (t_2a+s_2b) = (t_1+t_2)a + (s_1+s_2)b \in \langle a,b \rangle$;

I2. $c(ta+sb) = (ct)a+(cs)b \in \langle a,b \rangle$, para todo $c \in A$.

Logo, $\langle a,b \rangle$ é um ideal de A.

Atividade Final 4

($\Longrightarrow$) Como $I = A$, então é imediato que $1 \in A = I$.

($\Longleftarrow$) Como $1 \in I$, então, para todo $a \in A$, temos $a = a \cdot 1 \in I$. Logo, $I = A$.

Atividade Final 5

($\Longrightarrow$) Seja *I* um ideal de A com $I \neq \{0\}$. Então, existe $a \in I$ com $a \neq 0$. Como $a \neq 0$ e A é um corpo, então existe a^{-1} e $1 = a^{-1} \cdot a \in I$. Logo, pela Atividade Final 4, temos $I = A$, ou seja, provamos que se I é um ideal de A e $I \neq \{0\}$, então a única possibilidade que resta é $I = A$. Assim, A só tem os ideais triviais.

($\Longleftarrow$) Seja $a \in A$ com $a \neq 0$. Queremos mostrar que o elemento a é invertível. Pela Atividade Final 2, $\langle a \rangle$ é um ideal de A. Como $a \neq 0$, então $\langle a \rangle \neq \{0\}$, e como, por hipótese, A só admite os ideais triviais, então, segue que $\langle a \rangle = A$. Portanto, $1 \in A = \langle a \rangle$, logo, existe $t \in a$ tal que $1 = t \cdot a$, isto é, o elemento a é invertível. Portanto, A é um corpo.

Álgebra I

Referências

Você vai gostar de acompanhar os assuntos tratados aqui no livro:

HEFEZ, Abramo. *Curso de Álgebra*. Rio de Janeiro: IMPA, 1997. Coleção Matemática Universitária, v. 1.

HEFEZ, Abramo. *Curso de Álgebra.* Rio de Janeiro: IMPA, 1993. Coleção Matemática Universitária, v.1.