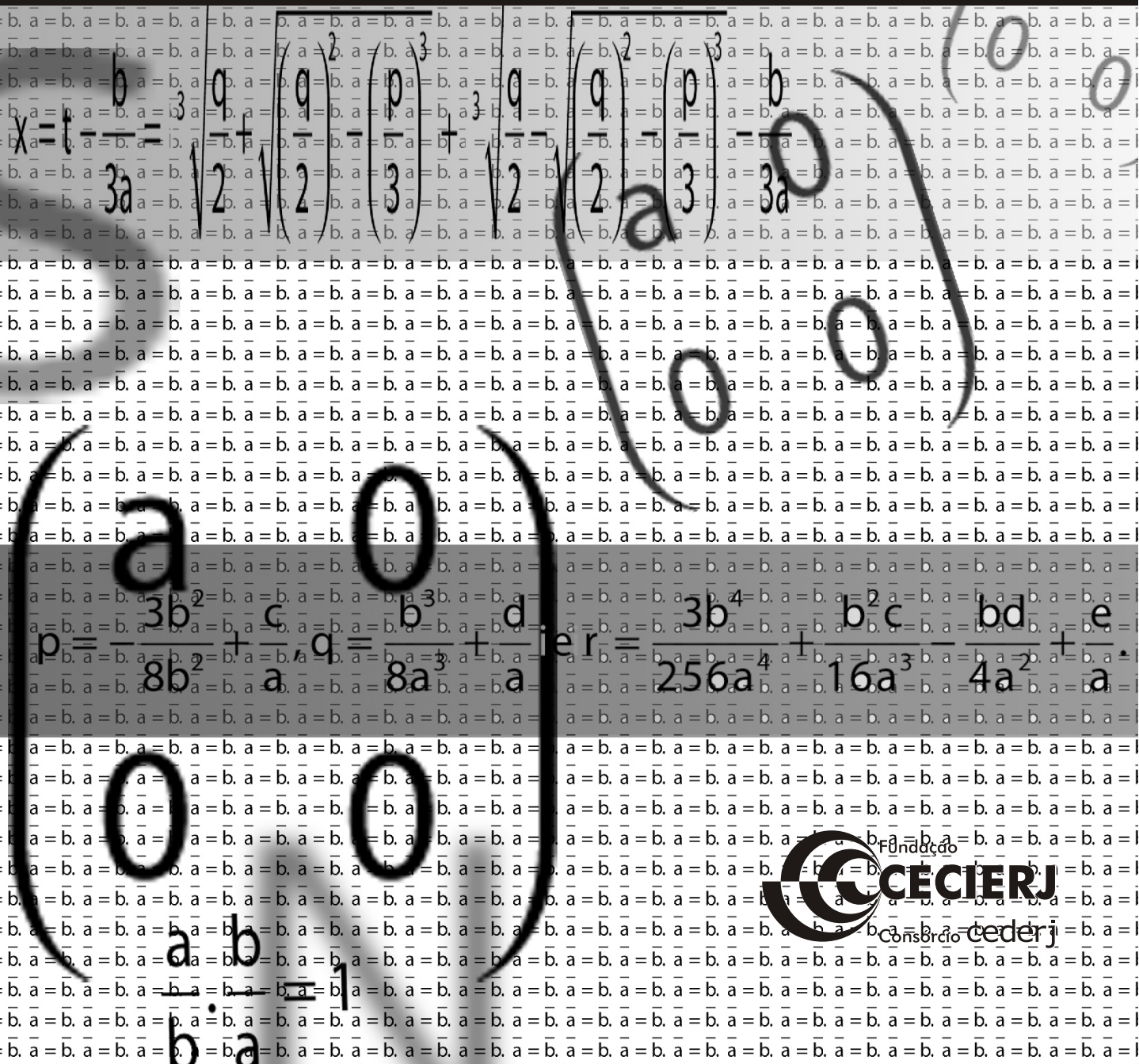
Hernando Bedoya
Ricardo Camelier

Volume único

Álgebra II



Fundação CECIERJ
Consórcio cederj

Fundação CECIERJ

Consórcio cederj

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

Álgebra II

Volume único

Hernando Bedoya

Ricardo Camelier

GOVERNO DO Rio de Janeiro

SECRETARIA DE CIÊNCIA E TECNOLOGIA

UAB UNIVERSIDADE ABERTA DO BRASIL

Ministério da Educação

BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Apoio:

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

Fundação Cecierj / Consórcio Cederj

Rua Visconde de Niterói, 1364 – Mangueira – Rio de Janeiro, RJ – CEP 20943-001
Tel.: (21) 2334-1569 Fax: (21) 2568-0725

Presidente
Masako Oya Masuda

Vice-presidente
Mirian Crapez

Coordenação do Curso de Matemática
UFF - Regina Moreth
UNIRIO - Luiz Pedro San Gil Jutuca

Material Didático

ELABORAÇÃO DE CONTEÚDO
Hernando Bedoya
Ricardo Camelier

COORDENAÇÃO DE DESENVOLVIMENTO INSTRUCIONAL
Cristine Costa Barreto

DESENVOLVIMENTO INSTRUCIONAL E REVISÃO
Zulmira Speridião
Marcelo Bastos Matos

COORDENAÇÃO DE LINGUAGEM
Cyana Leahy-Dios
Maria Angélica Alves

COORDENAÇÃO DE AVALIAÇÃO DO MATERIAL DIDÁTICO
Débora Barreiros

AVALIAÇÃO DO MATERIAL DIDÁTICO
Letícia Calhau

Departamento de Produção

EDITORA
Tereza Queiroz

COPIDESQUE
José Meyohas

REVISÃO TIPOGRÁFICA
Elaine Bayma
Marcus Knupp

COORDENAÇÃO DE PRODUÇÃO
Jorge Moura

PROGRAMAÇÃO VISUAL
Márcia Valéria de Almeida
Renata Borges
Sanny Reis

ILUSTRAÇÃO
Equipe Cederj

CAPA
Equipe Cederj

PRODUÇÃO GRÁFICA
Oséias Ferraz
Patricia Seabra

B412a
Bedoya, Hernando.
Álgebra II. v. único / Hernando Bedoya; Ricardo Camelier. – Rio de Janeiro: Fundação CECIERJ, 2010.
264p.; 19 x 26,5 cm.

ISBN: 85-7648-314-9

1. Álgebra. 2. Anéis quocientes. 3. Teorema de homomorfismo. 4. Polinômios. I. Camelier, Ricardo. II. Título.
CDD: 512

2010/1

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
Alexandre Cardoso

Universidades Consorciadas

UENF - UNIVERSIDADE ESTADUAL DO NORTE FLUMINENSE DARCY RIBEIRO
Reitor: Almy Junior Cordeiro de Carvalho

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

UFF - UNIVERSIDADE FEDERAL FLUMINENSE
Reitor: Roberto de Souza Salles

UFRJ - UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Reitor: Aloísio Teixeira

UFRRJ - UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
Reitor: Ricardo Motta Miranda

UNIRIO - UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
Reitora: Malvina Tania Tuttman

SUMÁRIO

AULA 1

Anéis quocientes

Meta da aula

Apresentar o desenvolvimento da estrutura algébrica de anel quociente.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Apresentar a relação de congruência módulo /.
- Identificar os passos que levam à caracterização de um anel quociente.
- Apresentar e demonstrar as primeiras propriedades operatórias da congruência módulo /.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos nas Aulas 21 a 23 do curso de Álgebra I. Você também vai precisar dos conceitos de ideal de $\mathbb{Z}$ e dos anéis dos inteiros módulo n, do seu curso de Álgebra I.

INTRODUÇÃO

Bem-vindo ao curso de Álgebra II. Aqui vamos estudar duas importantes e belíssimas estruturas algébricas: os anéis e os grupos. Estas teorias têm raízes em problemas muito longínquos que relativamente há pouco tempo foram resolvidos.

Nesta aula, vamos copiar a construção dos anéis dos inteiros módulo n, visto no seu curso de Álgebra I, para o caso geral de um anel A e de um ideal I de A. Portanto, é uma boa idéia rever as aulas daquele curso. Você perceberá uma idéia que é recorrente na matemática: a construção de uma estrutura abstrata geral seguindo os passos de um exemplo particular muito importante.

EXPANDINDO O CONCEITO DE CONGRUÊNCIA

Definição 1

Sejam A um anel e I um ideal de A. Definimos a seguinte relação binária em A:

$$a \equiv b \pmod{I} \Leftrightarrow b - a \in I$$

Dizemos, neste caso, que a e b são *congruentes módulo I*. Esta relação satisfaz às seguintes propriedades, que a tornam uma relação de equivalência.

Proposição 1

1. Propriedade Reflexiva

$a \equiv a \pmod{I}$

2. Propriedade Simétrica

Se $a \equiv b \pmod{I}$, $b \equiv a \pmod{I}$.

3. Propriedade Transitiva

Se $a \equiv b \pmod{I}$ e $b \equiv c \pmod{I}$, então $a \equiv c \pmod{I}$.

Demonstração

1. Basta observar que $a - a = 0 \in I$.

2. Como $a \equiv b \pmod{I}$, então $b - a \in I$. Assim, $a - b = -I$. $(b - a) \in I$, pela condição $I2$ de subanel. Logo, $b \equiv a \pmod{I}$. □

ATIVIDADE

1. Prove a propriedade transitiva da congruência módulo *I*.

GENERALIZANDO AS CLASSES DE CONGRUÊNCIA

Agora, que vimos que a congruência módulo I é uma relação de equivalência, sabemos que o anel A fica decomposto em classes de equivalência. São subconjuntos disjuntos, cuja união é todo o anel A, caracterizando o que chamamos de uma *partição* de A. Será neste conjunto de classes de equivalência que definiremos operações de adição e multiplicação, de modo a transformá-lo num anel.

Definição 2

Sejam A um anel, I um ideal de A, e $a \in A$. Definimos a *classe residual de a módulo I* (também chamada *classe de congruência de a módulo I*) como sendo o conjunto

$$\overline{\mathrm{a}} = \mathrm{a} + I = \{a + x \,|\, x \in I\}.$$

A próxima proposição afirma que as classes de congruência são exatamente as classes de equivalência da relação congruência módulo I.

Proposição 2

Sejam A um anel, I um ideal de A, e $a, b \in A$. Então $a \equiv b \pmod{I}$ se, e somente se, $\overline{a} = \overline{b}$.

Demonstração

($\Rightarrow$) Vamos provar a inclusão $\overline{a} \subset \overline{b}$. Como $a \equiv b \pmod{I}$, então $y = b - a \in I$. Assim, $a = b - y$. Agora, um elemento genérico de $\overline{a}$ é da forma $a + x$ com $x \in I$. Segue que:

$$\begin{aligned} a + x &= (b - y) + x \\ &= b + (x - y) \in \overline{b}, \end{aligned}$$

pois $x - y \in I$. A inclusão inversa, $\overline{b} \subset \overline{a}$, é análoga, e será uma atividade para você.

($\Leftarrow$) Temos $\overline{a} = \overline{b}$, então $b = b + 0 \in \overline{b} = \overline{a}$. Como $b \in \overline{a}$, existe $x \in I$, tal que $b = a + x$. Portanto, temos $b - a = x \in I$, ou seja, $a \equiv b \pmod{I}$. □

Vamos, agora, demonstrar a propriedade da partição que a congruência módulo I gera no anel A.

Proposição 3

1. Se $\overline{a} \cap \overline{b} \neq \emptyset$, então $\overline{a} = \overline{b}$.
2. $\bigcup_{a \in A} \overline{a} = A$.

Demonstração

1. Como $\overline{a} \cap \overline{b} \neq \emptyset$, existe um elemento $c \in \overline{a} \cap \overline{b}$. De $c \in \overline{a}$, temos que $c = a + x$ com $x \in I$. De $c \in \overline{b}$, temos que $c = b + y$, com $y \in I$. Logo, $b + y = a + x$, o que nos dá:

$$b - a = x - y \in I,$$

ou seja, $a \equiv b \pmod{I}$. Pela Proposição 2, segue que $\overline{a} = \overline{b}$.

2. Temos $a \in a$ para todo $a \in A$, então $A \subset \bigcup_{a \in A} \overline{a}$. Como, claramente, $\bigcup_{a \in A} \overline{a} \subset A$, então segue que $\bigcup_{a \in A} \overline{a} = A$. □

Denotamos por A/I o conjunto das classes residuais módulo I, ou seja, $A/I = \left\{ \overline{a} \middle| a \in A \right\}$.

O próximo passo é a definição das operações de adição e multiplicação em A/I.

Definição 3

Em A/I, definimos as seguintes operações:

Adição: $\overline{a} + \overline{b} = \overline{a + b}$;

Multiplicação: $\overline{a} \,.\, \overline{b} = \overline{a \,.\, b}$.

Observação

Como $\overline{a} = a + I$, uma outra notação muito utilizada para as operações de adição e multiplicação, definidas anteriormente, é:

$(a + I) + (b + I) = (a + b) + I$;

$(a + I) \,.\, (b + I) = (a \,.\, b) + I$.

A próxima proposição mostra que estas operações, em A/I, estão bem definidas, na medida em que não dependem dos representantes a e b das classes residuais $\overline{a}$ e $\overline{b}$, respectivamente.

Proposição 4

Se $\overline{a} = \overline{a_1}$ e $\overline{b} = \overline{b_1}$, então:

1. $\overline{a} + \overline{a} = a_1 + b_1$;
2. $a \,.\, b = a_1 \,.\, b_1$.

Demonstração

1. Se $\overline{a} = \overline{a_1}$, então, pela Proposição 2, $a \equiv a_1 \pmod{I}$, ou seja, $a_1 - a = x$, com $x \in I$. Analogamente, de $\overline{b} = \overline{b_1}$, segue que $b_1 - b = y$, com $y \in I$. Então,

$$\begin{aligned}(a_1 + b_1) - a + b &= (a_1 - a) + (b_1 - b) \\ &= x + y \in I,\end{aligned}$$

logo, $(a + b) \equiv (a_1 + b_1) \pmod{I}$, ou seja, $\overline{a + b} = \overline{a_1 + b_1}$. Portanto,

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{a_1 + b_1} = \overline{a_1} + \overline{b}_{1.}$$

2. Esta parte é um pouco mais trabalhosa, pois depende de um certo traquejo algébrico. Como anteriormente, se $\overline{a} = \overline{a_1}$, então $a_1 - a = x$, com $x \in I$, e, de $\overline{b} = \overline{b_1}$, segue que $b_1 - b = y$, com $y \in I$. Então,

$$\begin{aligned}(a_1 \,.\, b_1) - (a \,.\, b) &= (a_1 \,.\, b_1 - a \,.\, b_1) + (a \,.\, b_1 - a \,.\, b) \\ &= (a_1 - a).\, b_1 + a \,.\, (b_1 - b) \\ &= x \,.\, b_1 + a \,.\;\; y \in I,\end{aligned}$$

pois, $x \,.\, b_1 \in I$ e $a \,.\, y \in I$. Portanto, $(a \,.\, b) \equiv (a_1 \,.\, b_1) \pmod{I}$, ou seja, $\overline{a \,.\, b} = \overline{a_1 \,.\, b_1}$. Assim,

$$\overline{a} \,.\, \overline{b} = \overline{a \,.\, b} = \overline{a_1 \,.\, b_1} = \overline{a_1} \,.\, \overline{b}_1 \,. \;\square$$

Podemos, agora, completar nossa construção. Segue que $(A/I, +, \cdot)$ é um anel, chamado de *anel quociente,* ou *anel das classes residuais módulo I*, cujo zero é dado por $\overline{0}$ e cuja unidade é dada por $\overline{1}$.

Exemplo 1

Sejam $(\mathbf{Z}, +, .)$ o anel dos inteiros e I o ideal de $\mathbf{Z}$ dado por

$$\mathrm{I} = 12\mathbf{Z} = \{12\mathrm{k} \,|\, \mathrm{k} \in Z\}.$$

Então o anel $\mathbf{Z}/\mathrm{I} = \{a + I \,|\, a \in Z\}$ consiste em 12 elementos:

$$\begin{aligned}\mathbf{Z}/\mathrm{I} &= \{0 + I, 1 + I, 2 + I, \ldots, 11 + I\} \\ &= \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{11}\} \\ &= \mathbf{Z}_{12}\end{aligned}$$

que são as classes residuais módulo 12. Como 12 não é um número primo, então, por teorema dado no Volume III de Álgebra I, $\mathbf{Z}/I$ é anel, mas não é um domínio.

CONCLUSÃO

Se você achou esta aula mais abstrata, não se preocupe, pois ela é mesmo. Apesar de termos feito uma construção semelhante à que você fez no seu curso de Álgebra I, qualquer passagem de uma estrutura algébrica, como um anel, para uma estrutura quociente, como o anel quociente, requer um salto de abstração. Tenha paciência e insista na compreensão destes conceitos. Eles são importantes na Álgebra e serão utilizados ao longo de todo o curso de Álgebra II.

ATIVIDADE FINAL

1. Verifique que os axiomas de anel valem para $(A/I, +, \cdot)$.

RESUMO

A construção da relação de equivalência que consiste na congruência módulo I, é o primeiro passo da construção do anel quociente, feita por meio da introdução das operações de adição e multiplicação no conjunto das classes residuais módulo I. Tudo isto, seguindo a construção análoga que foi feita no seu curso de Álgebra I, para obter-se o anel dos inteiros módulo n.

RESPOSTAS

Atividade 1

De $a \equiv b \pmod{I}$, temos que $x = b - a \in I$. De $b \equiv c \pmod{I}$, temos $y = c - b \in I$. Então

$$\begin{aligned} c - a &= (c - b) + (b - a) \\ &= y + x \in I, \end{aligned}$$

ou seja, $a \equiv c \pmod{I}$.

Atividade Final

Percorra cada um dos axiomas que definem um anel, lembrando que os elementos neutros são $\overline{0}$ e $\overline{1}$. Por exemplo,

A1. Associatividade da Adição:

$$\begin{aligned} \overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b + c} \\ &= \overline{a + (b + c)} \\ &= \overline{(a + b) + c} \\ &= \overline{a + b} + \overline{c} \\ &= (\overline{a} + \overline{b}) + \overline{c}. \end{aligned}$$

AULA 2

Homomorfismos

Meta da aula

Apresentar o conceito de homomorfismo de anel e suas propriedades básicas.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Reconhecer um homomorfismo entre anéis.
- Apresentar e demonstrar as primeiras propriedades dos homomorfismos.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos nas Aulas 21 a 23 do curso de Álgebra I.

INTRODUÇÃO

As funções consideradas naturais entre duas estruturas algébricas do mesmo tipo, como os anéis, são aquelas que *preservam* as operações, ou seja, transformam uma soma de elementos no anel domínio na soma de suas imagens e transformam um produto de elementos no anel domínio no produto de suas imagens. Essas funções, chamadas de *homomorfismos*, serão o objeto do nosso interesse nesta aula.

Apesar de o conceito de homomorfismo ser muito natural, ele surgiu de forma muito gradual. O conceito de homomorfismo de grupos surgiu, pela primeira vez, em torno de 1830, o de homomorfismo de corpos em torno de 1870 e o de homomorfismo de anel somente em 1920.

HOMOMORFISMO DE ANÉIS

Definição 1

Dados dois anéis A e B, uma função $f : A \to B$ é chamada de um *homomorfismo* (*de anéis*) se para todo $a, b \in A$, vale:

H1. $f(a + b) = f(a) + f(b)$;
H2. $f(a \cdot b) = f(a) \cdot f(b)$;
H3. $f(1_A) = 1_B$ (ou, simplesmente, $f(1) = 1$).

Definição 2

Um homomorfismo $f : A \to B$ é chamado de um *isomorfismo* se for, também, uma bijeção. Nesse caso, dizemos que A e B são *isomorfos* e denotamos $A \approx B$.

Lembre que dois conjuntos A e B têm o mesmo número de elementos, ou seja, eles têm a mesma cardinalidade, se existe uma bijeção entre A e B. Assim, se A e B são isomorfos, então eles têm *exatamente* o mesmo número de elementos. Isso acontece porque se $f : A \to B$ é um isomorfismo, então, em particular, f é uma bijeção entre A e B.

Definição 3

O *núcleo* de um homomorfismo de anéis $f : A \to B$ é o conjunto

$$N(f) = \{x \in A \mid f(x) = 0_B\},$$

onde 0_B é o elemento neutro do anel B.

Vejamos agora dois dos exemplos mais simples de homomorfismo de anéis.

Exemplo 1

O exemplo mais simples de todos é o *homomorfismo identidade*. Dado um anel A, o homomorfismo identidade é definido pela função identidade em A, ou seja, $id : A \to A$, $id(a) = a$. Vamos verificar que a identidade é, de fato, um homomorfismo de anéis. Para isso, precisamos verificar os três axiomas de homomorfismos. Sejam $a, b \in A$, então

H1. $id(a + b) = a + b = id(a) + id(b)$;
H2. $id(a \cdot b) = a \cdot b = id(a) \cdot id(b)$;
H3. $id(1_A) = 1_A$.

Assim, id é um homomorfismo. Mais ainda, o homomorfismo identidade é bijetor, portanto, ele é também um exemplo de um isomorfismo. Vamos calcular seu núcleo. Nesse caso, $N(id) = \{x \in A \mid id(x) = 0_A\}$. Ou seja, queremos resolver a equação $id(x) = 0_A$. Como $id(x) = x$, a equação se transforma em $x = 0_A$, ou seja, sua única solução é $x = 0_A$, portanto, $N(id) = \{0_A\}$.

Exemplo 2

Seja $n \in \mathbf{Z}$, $n > 1$. Considere a função $f: \mathbf{Z} \to \mathbf{Z}_n$ definida por $f(a) = \overline{a}$, onde $\overline{a}$ é classe residual módulo n do inteiro a. Vamos verificar que f é um homomorfismo de anéis. De fato, dados $a, b \in \mathbf{Z}$, então

H1. $f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b)$;
H2. $f(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = f(a) \cdot f(b)$;
H3. $f(1) = \overline{1} = 1_{Zn}$.

Assim, f é um homomorfismo. Mais ainda, o homomorfismo f é sobrejetor, pois, dado $\overline{k} \in \mathbf{Z}_n$, então $f(k) = \overline{k}$. No entanto, f não é injetor, pois $f(0) = \overline{0}$ e $f(n) = \overline{n} = \overline{0}$, ou seja, $f(0) = f(n)$ com $n \neq 0$. Portanto, f não é um isomorfismo.

Vamos calcular, agora, o núcleo de f. Nesse caso, $N(f) = \{x \in \mathbf{Z} \mid f(x) = \overline{0}\}$. Ou seja, queremos resolver a equação $f(x) = \overline{0}$. Como $f(x) = \overline{x}$, a equação se transforma em $\overline{x} = \overline{0}$, e suas soluções são os inteiros múltiplos de n, portanto, $N(f) = n\mathbf{Z} = \{kn \mid k \in \mathbf{Z}\}$.

Vamos, agora estudar uma série de propriedades fundamentais sobre os homomorfismos.

Proposição 1

Seja $f : A \to B$ um homomorfismo de anéis. Temos:

1. $f(0_A) = 0_B$ (ou, simplesmente, $f(0) = 0$).
2. $f(-a) = -f(a)$ para todo $a \in A$.
3. $f(a - b) = f(a) - f(b)$, para todo $a, b \in A$.
4. $f(A)$ é um subanel de B, onde o conjunto *imagem de A*, $f(A)$, é definido por $f(A) = \{f(a) \mid a \in A\}$.
5. Se A' é um subanel de A, então $f(A')$ é um subanel de $f(A)$.
6. Se B' é um subanel de B, então $f^{-1}(B')$ é um subanel de A, onde o conjunto *imagem inversa de B*, $f^{-1}(B')$ é definido por $f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$.
7. Se I é um ideal de A, então $f(I)$ é um ideal de $f(A)$.
8. Se J é um ideal de B, então $f^{-1}(J)$ é um ideal de A.
9. $N(f)$ é um ideal de A.
10. Se f é um isomorfismo (ou seja, f é uma função bijetora), então $f^{-1} : B \to A$ é um homomorfismo de anéis e, portanto, é também um isomorfismo.

Demonstração

Algumas das demonstrações deixaremos como atividade para você. Demonstraremos algumas delas.

1. Temos

$$\begin{aligned} 0 + f(0) &= f(0) \\ &= f(0 + 0) \\ &= f(0) + f(0), \end{aligned}$$

e, cancelando $f(0)$ nos dois lados (lembre da lei do cancelamento), segue que

$$f(0) = 0.$$

2. Aplicando, inicialmente, a propriedade anterior, temos

$$\begin{aligned} 0 &= f(0) \\ &= f(a) + (-a)) \\ &= f(a) + f(-a), \end{aligned}$$

para todo $a \in A$. Logo, pela unicidade do elemento simétrico, segue que $f(-a) = -f(a)$.

3. Temos

$$\begin{aligned} f(a-b) &= f(a+(-b)) \\ &= f(a)+ f(-b), \\ &= f(a)+ (-f(b)), \text{ pela propriedade 2} \\ &= f(a) - f(b). \end{aligned}$$

4. Como $A \neq \emptyset$, segue que $f(A) \neq \emptyset$. Agora, dados $f(a)$, $f(b) \in f(A)$ e aplicando a propriedade 3, temos que

$$f(a) - f(b) = f(a-b) \in f(A),$$

e, também,

$$f(a) \,.\, f(b) = f(a \,.\, b) \in f(A).$$

Assim, pela Proposição 1 da Aula 5, segue que $f(A)$ é um subanel de B.

Tente você, agora, provar a próxima propriedade.

ATIVIDADE

1. Demonstre a propriedade 5, ou seja, prove que se A' é um subanel de A, então $f(A')$ é um subanel de $f(A)$.

6. Como $f(0_A) = 0_B$ e $0_B \in B'$, então $0_A \in f^{-1}(B')$ e, portanto, $f^{-1}(B') \neq \emptyset$. Agora, dados $a, b \in f^{-1}(B')$, então $f(a), f(b) \in B'$ e segue que

$$f(a - b) = f(a) - f(b) \in B',$$

pois B' é subanel de B. Portanto, $a - b \in f^{-1}(B')$. Também temos

$$f(a \cdot b) = f(a) \cdot f(b) \in B',$$

pois B' é subanel de B. Portanto, $a \cdot b \in f^{-1}(B')$. Assim, provamos que $f^{-1}(B')$ é um subanel de A.

É sua vez de praticar novamente.

ATIVIDADE

2. Demonstre a propriedade 7, ou seja, prove que se I é um ideal de A, então $f(I)$ é um ideal de $f(A)$.

_____

_____

_____

_____

_____

_____

_____

_____

8. Como $0_B \in J$ e $f(0_A) = 0_B$, então $0_A \in f^{-1}(J)$, e, portanto, $f^{-1}(J) \neq \emptyset$. Agora, dados $a, b \in f^{-1}(J)$, então $f(a), f(b) \in J$ e, assim, segue que

$$f(a + b) = f(a) + f(b) \in J,$$

pois J é um ideal de B. Portanto, $a + b \in f^{-1}(J)$. Por outro lado, sejam $a \in A$ e $b \in f^{-1}(J)$, então vale que $f(a) \in f(A)$ e $f(b) \in J$, e, como J é ideal de B e $f(A) \subset B$, temos $f(a) \cdot f(b) \in J$. Portanto,

$f(a \cdot b) = f(a) \cdot f(b) \in J$,

ou seja, $a \cdot b \in f^{-1}(J)$. Assim, concluímos que $f^{-1}(J)$ é um ideal de A.

9. Para mostrar que o núcleo é um ideal, usamos a propriedade anterior. De fato,

$$N(f) = \{x \in A \mid f(x) = 0_B\}$$
$$= f^{-1}(\{0_B\}),$$

e, como $\{0_B\}$ é um ideal de B, segue, pela propriedade 8, que $N(f)$ é um ideal de A. □

Assim, concluímos a demonstração da Proposição 1. Veja que deixamos as propriedades 5, 7 e 10 como atividades a serem desenvolvidas por você.

ATIVIDADE

3. Demonstre a propriedade 10 da Proposição 1, ou seja, prove que se f é um isomorfismo (ou seja, f é um homomorfismo bijetor), então $f^{-1}: B \to A$ é um homomorfismo de anéis.

Os homomorfismos são ricos em propriedades, e agora vamos ver algumas dessas propriedades relacionadas ao núcleo. As primeiras duas propriedades que seguem devem trazer à lembrança as propriedades equivalentes para o núcleo de uma transformação linear e para um homomorfismo de grupos.

Proposição 2

Seja $f : A \to B$ um homomorfismo de anéis e $N(f)$ o núcleo de f. Então,

1. $f(a) = f(b)$ se e somente se $b - a \in N(f)$.
2. f é injetora se e somente se $N(f) = \{0\}$.
3. Se A é um corpo, então f é injetora.

Demonstração

1. ($\Rightarrow$) Suponhamos que $f(b) = f(a)$ e vamos mostrar que $b - a \in N(f)$.

De fato, $f(a) = f(b)$ implica que $f(b) - f(a) = 0$. Assim, $f(b - a) = f(b) - f(a) = 0$, ou seja, $b - a \in N(f)$.

($\Leftarrow$) Reciprocamente, suponhamos que $b - a \in N(f)$ e vamos mostrar que $f(a) = f(b)$.

De fato, se $b - a \in N(f)$, então $f(b - a) = 0$. Assim, $f(b) - f(a) = f(b - a) = 0$, ou seja, $f(a) = f(b)$.

2. ($\Rightarrow$) Suponhamos, primeiramente, que f é injetora. Vamos mostrar que $N(f) = \{0\}$.

De fato, se f é injetora, considere $a \in N(f)$. Então $f(a) = 0$, e como $f(0) = 0$, segue que $f(a) = f(0)$. Como f é injetora, temos $a = 0$. Assim, $N(f) = \{0\}$.

($\Leftarrow$) Reciprocamente, suponha que $N(f) = \{0\}$. Vamos mostrar que f é injetora.

Se $f(a) = f(b)$, então, pela propriedade anterior, temos que $b - a \in N(f)$. Como estamos supondo que $N(f) = \{0\}$, segue que $b - a = 0$, ou seja, $a = b$, o que prova que f é injetora.

3. Suponhamos que A é corpo e seja $a \in A$ com $a \neq 0$. Então existe a^{-1}, o inverso multiplicativo de a, que satisfaz $a \,.\, a^{-1} = 1_A$. Assim,

$$f(a) \cdot f(a^{-1}) = f(a \cdot a^{-1}), \text{ pois } f \text{ é homomorfismo}$$
$$= f(1_A)$$
$$= 1_B \text{ , pois } f \text{ é homomorfismo.}$$

Portanto, concluímos que $f(a)$ é invertível e, em particular, $f(a) \neq 0$. Logo, $a \notin N(f)$ para todo $a \in A$ com $(a) \neq 0$, o que nos leva a concluir que $N(f) = \{0\}$. Pela propriedade anterior, segue que f é injetora.□

Exemplo 3

Vamos descrever um homomorfismo muito importante, chamado *homomorfismo canônico* (ou *homomorfismo projetor*). Seja A um anel e I um ideal de A. Seja $\pi : A \to A/I$, definida por $\pi(a) = \overline{a}$, onde $\overline{a} = a + I \in A/I$ é a classe residual de $a \in A$ módulo I. Vamos verificar, agora, que π é um homomorfismo de anéis. De fato, sejam $a, b \in A$, então

H1. $\pi(a + b) = \overline{a + b} = \overline{a} + \overline{b} = \pi(a) + \pi(b)$;
H2. $\pi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \pi(a) \cdot \pi(b)$;
H3. $\pi(1_A) = \overline{1}_A = 1_{A/I}$.

Assim, π é um homomorfismo. Mais ainda, o homomorfismo π é sobrejetor, pois para qualquer $\overline{a} \in A/I$ temos que $\pi(a) = \overline{a}$. Chamamos $\pi : A \to A/I$ de *homomorfismo canônico*.

Vejamos, agora, como se comportam os homomorfismos sob a operação de composição de funções.

Proposição 3

Sejam $g : A \to B$ e $f : B \to C$ dois homomorfismos de anéis. Então:

a) A composição $f \circ g : A \to C$ é um homomorfismo de anéis;

b) Se $A \approx B$ e $B \approx C$, então $A \approx C$, isto é, se A é isomorfo a B e B é isomorfo a C, então A é isomorfo a C.

A demonstração desta proposição faz parte das Atividades Finais da aula.

Para terminar esta aula, queremos enfatizar para você que os anéis isomorfos têm propriedades idênticas, e eles diferem apenas na apresentação de seus elementos. O que importa é que o isomorfismo preserva todas as propriedades entre tais anéis.

A Atividade Final é um desafio para você. Lembre-se de consultar os resultados apresentados. Leia várias vezes as demonstrações das propriedades e tente imitá-las. Tenha sempre papel e lápis à mão e, se for preciso, apague e reescreva quantas vezes for necessário. Achamos que se você entendeu bem esta aula, então terá capacidade de sobra para resolver essas atividades. Vamos lá!

ATIVIDADES FINAIS

1. Sejam A um anel e $a \in A - \{0\}$. Defina a função $f_a : A \to A$ por $f_a(x) = a \cdot x$.

a. Mostre que f_a é sobrejetora se e somente se a é invertível.

_____

_____

b. Mostre que se A é um domínio de integridade, então f_a é injetora.

_____

_____

c. f_a é um homomorfismo?

_____

_____

2. Prove a Proposição 3.

_____

_____

RESUMO

Nesta aula, foram apresentados os seguintes resultados:

i. O conceito de homomorfismo entre dois anéis *A* e *B*, ou seja, uma função $f : A \to B$ que para todo $a, b \in A$,

satisfaz:

H1. $f(a + b) = f(a) + f(b)$;

H2. $f(a \cdot b) = f(a) \cdot f(b)$;

H3. $f(1_A) = 1_B$ (ou, simplesmente, $f(1) = 1$).

ii. O conceito de isomorfismo, ou seja, um homomorfismo que também é uma bijeção.

iii. As propriedades apresentadas e demonstradas servem para verificar que os homomorfismos preservam algumas estruturas dos anéis.

iv. O conceito de núcleo de um homomorfismo, ou seja, o núcleo do homomorfismo $f : A \to B$ é o conjunto $N(f) = \{x \in A \mid f(x) = 0_B\}$. Algumas propriedades importantes dos homomorfismos são verificadas pelo comportamento do seu núcleo.

v. O homomorfismo projetor, ou seja, dado o anel *A* e *I* um ideal de *A*, é definido por $\pi : A \to A/I$, $\pi(a) = \overline{a}$ (lembre que $\overline{a} = a + I \in A/I$).

RESPOSTAS

Atividade 1

Como $A' \neq \emptyset$, segue que $f(A') \neq \emptyset$. Agora, dados $f(a)$, $f(b) \in f(A')$, temos, aplicando a propriedade 3,

$$f(a) - f(b) = f(a - b) \in f(A'),$$

e, também,

$$f(a) \cdot f(b) = f(a \cdot b) \in f(A').$$

Assim, pela Proposição 1 da Aula 5, segue que $f(A')$ é um subanel de $f(A)$.

Atividade 2

Como $0_A \in I$ e $0_B = f(0_A)$, então $0_B \in f(I)$, e, portanto, $f(I) \neq \emptyset$. Agora, dados $f(a)$, $f(b) \in f(I)$ então segue que

$$f(a) + (b) = f(a + b) \in f(I),$$

ou seja, $f(a) + (b) \in f(I)$. Vamos considerar, agora, $f(a) \in f(A)$ e $f(b) \in f(I)$, então, como $a \in A$, $b \in I$ I é ideal, temos $a \,.\, b \in I$. Portanto,

$$f(a) \,.\, (b) = f(a \,.\, b) \in f(I),$$

ou seja, $f(a) \,.\, (b) \in f(I)$. Assim, concluímos que $f(I)$ é um ideal de $f(A)$.

Atividade 3

Dados $x, y \in B$, sejam $a = f^{-1}(x)$ e $b = f^{-1}(y)$, ou seja, $f(a) = x$ e $f(b) = y$. Como f é um homomorfismo, sabemos que

$$f(a + b) = f(a) + f(b) \text{ e } f(a \,.\, b) = f(a) \,.\, f(b).$$

Temos, então, que

$$\begin{aligned} f^{-1}(x + y) &= f^{-1}(f(a) + f(b)), \text{ pela escolha de } x \text{ e } y \\ &= f^{-1}(f(a + b)), \text{ pois } f \text{ é homomorfismo} \\ &= a + b, \text{ pois } f^{-1} \circ f = id \\ &= f^{-1}(x) + f^{-1}(y). \end{aligned}$$

Lembre que id representa a função identidade. Temos, também,

$$\begin{aligned} f^{-1}(x \,.\, y) &= f^{-1}(f(a) \,.\, f(b)), \text{ pela escolha de } x \text{ e } y \\ &= f^{-1}(f(a \,.\, b)), \text{ pois } f \text{ é homomorfismo} \\ &= a \,.\, b, \text{ pois } f^{-1} \circ f = id \\ &= f^{-1}(x) \,.\, f^{-1}(y). \end{aligned}$$

Finalmente, como $f(1_A) = 1_B$ e f é bijetora, segue que $f^{-1}(1_B) = 1_A$. Concluímos, assim, que $f^{-1} : B \to A$ é um homomorfismo.

Atividade Final 1

a. (⇒) Suponha que f_a é sobrejetora. Vamos mostrar que *a* é invertível.

De fato, como f_a é sobrejetora, existe $a' \in A$ tal que $f_a(a') = 1_A$, isto é, $a \,.\, a' = 1_A$. Logo, a' é o elemento inverso de a, isto é, a é invertível.

(⇐) Reciprocamente, suponha que a é invertível. Vamos mostrar que f_a é sobrejetora.

Seja $b \in A$ um elemento qualquer. Temos que

$$\begin{aligned} f_a(a^{-1}.\, b) &= a \,.\, (a^{-1}.\, b), \text{ pela definição de } f_a \\ &= (a \,.\, a^{-1}) \,.\, b \\ &= 1_A \,.\, b, \text{ pois } a \text{ é invertível} \\ &= b. \end{aligned}$$

Mostramos, assim, que para qualquer que seja $b \in A$, existe $x = a^{-1} \,.\, b$ tal que $f_a(x) = a$. Portanto, concluímos que f_a é sobrejetora.

b. Vamos mostrar que f é injetora. Suponhamos que $f_a(x) = f_a(y)$, isto é, $a \,.\, x = a \,.\, y$. Logo, $a \,.\, x - a \,.\, y = 0$ e, portanto, $a \,.\, (x - y) = 0$. Como A é domínio de integridade e $a \neq 0$, segue que $x - y = 0$, isto é, $x = y$, o que prova que f_a é injetora.

c. f_a é homomorfismo somente no caso em que $a = 1_A$, pois

$$f_a(x \,.\, y) = a \,.\, (x \,.\, y)$$

e

$$f_a(x) \,.\, f_a(y) = a^2 \,.\, (x \,.\, y).$$

Para serem iguais, é necessário que $a = a^2$, isto é, $a = 1_A$.

Atividade Final 2

Vamos verificar os axiomas de homomorfismo para a composição $f \circ g$. Dados $a, b \in A$, temos

H1.

$(f \circ g)(a + b) = f(g(a + b))$, pela definição de composição

$= f(g(a) + g(b))$, pois g é homomorfismo;

$= f(g(a)) + f(g(b))$, pois f é homomorfismo;

H2.

$(f \circ g)(a \cdot b) = f(g(a \cdot b))$, pela definição de composição

$= f(g(a) \cdot g(b))$, pois g é homomorfismo;

$= f(g(a)) \cdot f(g(b))$, pois f é homomorfismo;

H3.

$(f \circ g)(1_A) = f(g(1_A))$, pela definição de composição

$= f(1_B)$, pois g é homomorfismo;

$= 1_C$, pois f é homomorfismo.

Assim, provamos que a composição $f \circ g$ é um homomorfismo de anéis.

b. Suponhamos que A é isomorfo a B e B é isomorfo a C. Queremos provar que A é isomorfo a C. Como $A \approx B$ e $B \approx C$, então existem isomorfismos $g : A \to B$ e $f : B \to C$. Como f e g são homomorfismos, então, pelo item a), $f \circ g : A \to C$ também é um homomorfismo. Agora, você sabe que se f e g são funções bijetoras, então a composição $f \circ g$ também é bijetora. Portanto, concluímos que $f \circ g : A \to C$ é um homomorfismo bijetor, ou seja, $f \circ g : A \to C$ é um isomorfismo de anéis. Assim, concluímos que $A \approx C$.

AULA 3

Teorema do homomorfismo

Metas da aula

Apresentar o teorema do homomorfismo de anéis e sua demonstração. Realizar outra demonstração do teorema do resto chinês.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Demonstrar o teorema do homomorfismo.
- Demonstrar que os anéis $\mathbf{Z}_n$ e Z/nZ são isomorfos.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos nas Aulas 21 a 23 de Álgebra I, e Aulas 1 e 2 deste curso.

INTRODUÇÃO

Todo homomorfismo gera um isomorfismo entre um anel quociente e o anel imagem do homomorfismo. Esse importante resultado será o tema desta aula. Como aplicação, vamos rever o teorema do resto chinês, visto no seu curso de Álgebra I, obtendo, agora, uma nova demonstração.

Vamos começar revendo a definição de isomorfismo de anéis, apresentada na aula anterior.

DEFINIÇÃO 1

Um homomorfismo $f : A \to B$ é chamado de um *isomorfismo* se for, também, uma bijeção. Nesse caso, dizemos que A e B são *isomorfos* e denotamos $A \approx B$.

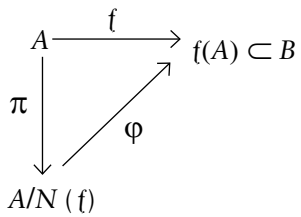
O resultado principal desta aula, o teorema do homomorfismo, é similar a um resultado correspondente sobre os homomorfismos de grupos, apresentado no curso de Álgebra I.

Lembre, da aula anterior, que dado o homomorfismo de anéis $f : A \to B$, então o conjunto imagem de A, $f(A)$, é um subanel de B e o núcleo de f, $N(f)$, é um ideal de A.

TEOREMA DO HOMOMORFISMO DE ANÉIS

Dado um homomorfismo $f : A \to B$ entre os anéis A e B, então existe um isomorfismo de anéis $\varphi : A/N(f) \to f(A)$ que satisfaz $f = \varphi \circ \pi$, onde $\pi : A \to A/N(f)$ é o homomorfismo canônico.

Representamos esse resultado pelo seguinte esquema.



$$A/N(f) \approx f(A)$$

É de suma importância que você acompanhe passo a passo todas as etapas desta demonstração. Ela é longa e será dividida em várias etapas para facilitar a sua compreensão. Para que você não se perca na argumentação, leia e releia com atenção cada uma de suas etapas. Certifique-se de que você entendeu cada passagem e faça suas próprias anotações, justificando as passagens que você considera mais difíceis. Vamos lá então!

Demonstração

Vamos dividir a demonstração em alguns passos.

1º Passo: Vamos definir uma função $\varphi : A/N(f) \to f(A)$, segundo o diagrama anterior.

Para isso, definimos $\varphi(\overline{a}) = f(a)$ para todo $\overline{a} = a + N(f) \in A/N(f)$. Então, precisamos provar que φ é, de fato, uma função bem definida, o que significa mostrar que se $\overline{a} = \overline{b}$, então $\varphi(\overline{a}) = \varphi(\overline{b})$, ou seja, se $\overline{a} = \overline{b}$, então $f(a) = f(b)$. Suponhamos, então, que $\overline{a} = \overline{b}$. Da aula anterior, sabemos que $N(f)$ é um ideal de A, logo, $a - b \in N(f)$ e, portanto, $f(a - b) = 0_B$. Assim,

$$f(a) - f(b) = f(a - b) = 0_B,$$

ou seja,

$$f(a) = f(b),$$

ou, equivalentemente, pela definição de φ, que $\varphi(\overline{a}) = \varphi(\overline{b})$. Concluímos, assim, que φ é, de fato, uma função de $A/N(f)$ em $f(A)$.

2º Passo: Vamos mostrar que φ é um homomorfismo. Para isso, basta verificar que φ satisfaz os axiomas de homomorfismo vistos na Aula 2.

Se $\overline{a}, \overline{b} \in A/N(f)$, temos:

H1.

$$\begin{aligned}\varphi(\overline{a} + \overline{b}) &= \varphi(a + b)\\ &= f(\overline{a + b}) \text{ pela definição de } \varphi\\ &= f(a) + f(b) \text{ pois } f \text{ é homomorfismo}\\ &= \varphi(a) + \varphi(b) \text{ pela definição } \varphi.\end{aligned}$$

H2.

$$\begin{aligned}\varphi(\overline{a} \,.\, \overline{b}) &= \varphi(a \,.\, b)\\ &= f(\overline{a \,.\, b}) \text{ pela definição de } \varphi\\ &= f(a) \,.\, f(b) \text{ pois } f \text{ é homomorfismo}\\ &= \varphi(\overline{a}) \,.\, \varphi(\overline{b}) \text{ pela definição } \varphi.\end{aligned}$$

H3.

$$\begin{aligned}\varphi(\overline{1}_A) &= f(1_A) \text{ pela definição de } \varphi\\ &= 1_A \text{ pois } f \text{ é homomorfismo.}\end{aligned}$$

Concluímos, assim, que a função φ é um homomorfismo entre os anéis $A/N(f)$ em $f(A)$.

3º Passo: Vamos provar, agora, que φ é uma função bijetora. Vamos começar provando que ela é injetora. Pela Proposição 2, item 2, da Aula 7, basta mostrar que $N(\varphi) = \{\overline{0}_A\}$. Seja $\overline{a} \in N(\varphi)$, então, pela definição de φ, $f(a) = \varphi(\overline{a}) = 0_B$, ou seja, $\overline{a} \in N(f)$. Portanto, $\overline{a} = a + N(f) = \overline{0}_A$. Isso prova que $N(\varphi) = \{\overline{0}_A\}$.

Caso você ache essa argumentação muito abstrata, vamos apresentar a demonstração clássica de injetividade, que consiste em provar que se $\varphi(\overline{a}) = \varphi(\overline{b})$, então $\overline{a} = \overline{b}$. De fato, se $\varphi(\overline{a}) = \varphi(\overline{b})$, temos que $f(a) = f(b)$, pela definição de φ, logo $f(a) - f(b) = 0$. Daí,

$$f(a - b) = f(a) - f(b) = 0,$$

e isso significa que $a - b \in N(f)$, ou seja, $\overline{a} = \overline{b}$. Pois, lembre que $a \in A/N(f)$.

Finalmente, φ é uma função sobrejetora, pois dado $y \in f(A)$ arbitrário, então existe $a \in A$ tal que $y = f(a)$ e, como $\varphi(\overline{a}) = f(a)$, segue que $y = \varphi(\overline{a})$.

Concluímos, assim, que a função $\varphi: A/N(f) \to f(A)$, definida por $\varphi(\overline{a}) = f(a)$, é um homomorfismo bijetor, ou seja, é um isomorfismo e, portanto, temos $A/N(f) \approx f(A)$.

Esperamos que você tenha apreciado a demonstração desse belo teorema. Uma conseqüência imediata do Teorema do Homomorfismo é:

Corolário 1

Se $f : A \to B$ é um homomorfismo sobrejetor, então $A/N(f)$ e B são anéis isomorfos, isto é, $A/N(f) \approx B$.

Demonstração

Como f é sobrejetora, temos $f(A) = B$ e, pelo teorema do homomorfismo, temos $A/N(f) \approx f(A)$. Portanto, concluímos que $A/N(f) \approx B$.

Corolário 2

Seja $n \in \mathbf{Z}$, $n > 0$. Então os anéis $\mathbf{Z}/n\mathbf{Z}$ e $\mathbf{Z}_n$ são isomorfos, isto é, $\mathbf{Z}/n\mathbf{Z} \approx \mathbf{Z}_n$.

A demonstração deste corolário você vai realizar, agora, como sua primeira atividade desta aula.

ATIVIDADE

1. Nesta atividade, você vai demonstrar o Corolário 2. Para isso, seja $f : Z \to Z_n$ a função dada por $f(a) = \overline{a}$, onde $\overline{a}$ é a classe residual de a módulo n. Mostre que:

a) f é um homomorfismo sobrejetor;

b) $N(f) = nZ$;

c) $\mathbf{Z}/n\mathbf{Z} \approx \mathbf{Z}_n$.

Agora, vamos utilizar o corolário anterior para provar o teorema do resto chinês.

TEOREMA DO RESTO CHINÊS

Sejam $m, n \in \mathbf{Z}$, $m, n > 0$, tais que mdc(m, n) = 1. Então os anéis $\mathbf{Z}_{mn}$ e $\mathbf{Z}_m \times \mathbf{Z}_n$ são isomorfos.

Lembre que $\mathbf{Z}_{mn} = \{[a]_{mn} \mid a \in \mathbf{Z}\}$ e $\mathbf{Z}_m \times \mathbf{Z}_n = \{([a]_m, [a]_n) \mid [a]_{mn} \in \mathbf{Z}_m$ e $[a]_n \in \mathbf{Z}_n\}$. Lembre, também, que dois inteiros m e n com mdc(m, n) = 1 são chamados de primos relativos (ou, primos entre si), o que significa que m e n não têm divisor primo comum.

Demonstração

Consideremos a função $f : Z \to \mathbf{Z}_m \times \mathbf{Z}_n$ definida por $f(a) = ([a]_m, [a]_n)$, onde $[a]_m$ e $[a]_n$ denotam as classes residuais de $a \in \mathbf{Z}$, módulo m e módulo n, respectivamente.

1º Passo: provar que *f* é um homomorfismo de anéis.

A demonstração desse fato é mais uma atividade proposta para você.

ATIVIDADE

2. Prove que função $f : Z \to Z_m \times Z_n$, definida por $f(a) = ([a]_m, [a]_n)$, é um homomorfismo de anéis.

Veja que propriedades você deve provar e tente adaptar as provas parecidas que já fizemos.

2º Passo: vamos mostrar que $N(f) = mn\mathbf{Z}$, onde $N(f)$ é o núcleo de f.

Vamos começar pela primeira inclusão: $N(f) \supset mn\mathbf{Z}$. Se $a \in mn\mathbf{Z}$, então a é múltiplo de mn, isto é, $mn \mid a$ (lembre que esse símbolo significa mn divide a). Como $m \mid mn$ e $n \mid mn$, temos que $m \mid a$ e $n \mid a$, ou seja, $[a]_m = [0]_m$ e $[a]_n = [0]_n$. Assim, $f(a) = ([a]_m, [a]_n) = ([0]_m, [0]_n) = 0_{Zm \times Zn}$. Isso significa que $a \in N(f)$.

Vamos provar, agora, a segunda inclusão: $N(f) \neq mn\mathbf{Z}$. Seja $a \in N(f)$, então $f(a) = ([a]_m, [a]_n) = 0_{Zm \times Zn} = ([0]_m, [0]_n)$. Daí, segue que $[a]_m = [0]_m$ e $[a]_n = [0]_n$. Logo, $m \mid a$ e $n \mid a$. Como $m \mid a$, $n \mid a$ e mdc(m,n) = 1 então, por propriedade conhecida do seu curso de Álgebra I, segue que $m \mid a$, ou seja, a é múltiplo de mn. Portanto, $a \in mn\mathbf{Z}$.

Concluímos assim, que $N(f) = mn\mathbf{Z}$.

3º Passo: vamos provar que $\mathbf{Z}_{mn} \approx f(\mathbf{Z})$.

Nos passos anteriores mostramos que $f : \mathbf{Z} \to \mathbf{Z}_m \times \mathbf{Z}_n$ é um homomorfismo com núcleo $N(f) = mn\mathbf{Z}$. Pelo Teorema do Homomorfismo, segue que $\mathbf{Z}/mn\mathbf{Z} \approx f(\mathbf{Z})$. Agora, pelo Corolário 2, segue que $\mathbf{Z}_{mn} \approx \mathbf{Z}/mn\mathbf{Z}$. Logo, pela Proposição 3 da Aula 7, segue que $\mathbf{Z}_{mn} \approx f(\mathbf{Z})$.

4º Passo: para finalizar, vamos mostrar que $f(Z) \to \mathbf{Z}_m \times \mathbf{Z}_n$.

Como Z_{mn} e f(Z) são isomorfos, então $\mathbf{Z}_{mn}$ e $f(Z)$ têm o mesmo número de elementos. Sabemos que $\mathbf{Z}_{mn}$ tem $m \,.\, n$ elemento, portanto, $f(Z)$ também tem $m.n$ elementos. Mas, $f(\mathbf{Z}) \subset \mathbf{Z}_m \times \mathbf{Z}_n$. Como $\mathbf{Z}_m \times \mathbf{Z}_n$ também tem $m.n$ elementos, concluímos que $f(\mathbf{Z}) = \mathbf{Z}_m \times \mathbf{Z}_n$.

Dos passos anteriores, concluímos que $\mathbf{Z}_{mn} = \mathbf{Z}_m \times \mathbf{Z}_n$ sempre que mdc(m,n) = 1.

ATIVIDADE FINAL

Sejam $n, K \in Z, n, K > 0$. Seja $f : Z_{Kn} \to Z_n$ definida por $f([a]_{Kn}) = [a]_n$, onde $[a]_{Kn}$ e $[a]_n$ são as classes residuais de *a*, módulo k*n* e módulo *n*, respectivamente.

a) Mostre que f é um homomorfismo de anéis.

b) Mostre que $N(f) = nZ_{Km} = \{n \,.\, [x]_{Kn} \;\; [x]_{Kn} \in Z_{Kn}\}$.

c) Mostre que f é sobrejetora e conclua que os anéis $\mathbf{Z}_{Kn} / nZ_{Kn}$ e $\mathbf{Z}_n$ são isomorfos, isto é, $Z_{Kn} / nZ_{Km} \approx \mathbf{Z}_n$.

RESUMO

Nesta aula, você viu o importante teorema do homomorfismo, muitas vezes também chamado de teorema do isomorfismo. Esse teorema afirma que dado um homomorfismo de anéis $f : \boldsymbol{A} \to \boldsymbol{B}$, então os anéis $A/N(f)$ e $f(A)$ são isomorfos. Ele é um mecanismo de criação de isomorfismos e, assim, uma importantíssima ferramenta de comparação de anéis. Fizemos uma bela aplicação desse teorema quando provamos o teorema do resto chinês, que afirma que os anéis $\mathbf{Z}_{mn}$ e $\mathbf{Z}_m \times \mathbf{Z}_n$ são isomorfos sempre que mdc(m,n) = 1.

RESPOSTAS

Atividade 1

a) Para mostrar que f é homomorfismo, sejam $a, b \in \mathbf{Z}$, então

H1. $f(a + b) = \overline{a + b} = \overline{a} + \overline{b} = f(a) + f(b)$;

H2. $f(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = f(a) \cdot f(b)$;

H3. $f(1) = \overline{1} = 1_{Zn}$,

ou seja, f é um homomorfismo. Mais ainda, é um homomorfismo sobrejetor, pois, dado $a \in \mathbf{Z}_n$, temos $f(a) = \overline{a}$ com $a \in \mathbf{Z}$.

b) Para provar que os dois conjuntos são iguais, seja

$$\begin{aligned} a \in N(f) &\Leftrightarrow f(a) = \overline{0} \\ &\Leftrightarrow \overline{a} = \overline{0} \\ &\Leftrightarrow a \equiv 0 \pmod{n} \\ &\Leftrightarrow n \mid a \\ &\Leftrightarrow a \in n\mathbf{Z}. \end{aligned}$$

Assim, concluímos que $N(f) = n\mathbf{Z}$.

c) Sabendo que $f : \mathbf{Z} \to \mathbf{Z}_n$ é um homomorfismo sobrejetor, segue, agora, diretamente do corolário 1, que $\mathbf{Z}/N(f) \approx \mathbf{Z}_n$. E, como $N(f) = n\mathbf{Z}$, então, concluímos que $\mathbf{Z}/n\mathbf{Z} \approx \mathbf{Z}_n$.

Atividade 2

Precisamos verificar que $f : \mathbf{Z} \to \mathbf{Z}_m$ x $\mathbf{Z}_n$, definida por $f(a) = ([a]_m, [a]_n)$, satisfaz os três axiomas de homomorfismo.

H1.

$$\begin{aligned} f(\mathrm{a} + \mathrm{b}) &= ([\mathrm{a} + \mathrm{b}]_m, [\mathrm{a} + \mathrm{b}]_n), \text{ para todo } a, b \in \mathbf{Z} \\ &= ([a]_m + [b]_m, [a]_n + [b]_n) \\ &= ([a]_m + [a]_n) + [b]_m + [b]_n) \\ &= f(a) + f(b); \end{aligned}$$

H2.

$f(a \cdot b) = ([a \cdot b]_m , [a \cdot b]_n)$, para todo $a, b \in \mathbf{Z}$

$= ([a]_m . [b]_m , [a]_n . [b]_n)$

$= ([a]_m , [a]_n) + ([b]_m , [b]_n)$

$= f(a) . f(b);$

H3. $f(1) = ([1]_m , [1]_n) = 1_{Z_m \times Z_m}$.

Assim, concluímos que f é um homomorfismo de anéis.

Atividade Final

a) Vamos verificar que *f* satisfaz os axiomas de homomorfismo. Sejam $a, b \in Z$, então

H1.

$f([a]_{Kn} . [b]_{Kn}) = f([a + b]_m)$, para todo $a, b \in \mathbf{Z}$

$= [a + b]_n$, pela definição de f

$= [a]_n + [b]_n$

$= f(a) + f(b);$

H2.

$f([a]_{Kn} . [b]_{Kn}) = f([a . b]_{Kn})$ para todo $a, b \in \mathbf{Z}$

$= [a . b]_n$, pela definição de f

$= [a]_n . [b]_n$

$= f(a) . f(b);$

H3.

$f(1_{ZKn}) = f([1]_{Kn})$

$= [1]_n$, pela definição de f

$= 1_{Zn}$.

Assim, concluímos que f é um homomorfismo de anéis.

b) Vamos calcular o núcleo de f. Sabemos que $N(f) = \{[a]_{Kn} \in \mathbf{Z}_{Kn} \mid f([a]_{Kn}) = 0_{Zn} = [0]_n\}$. Temos

$$\begin{aligned} f([a]_{Kn}) = [0]_n &\Leftrightarrow [a]_n = [0]_n \\ &\Leftrightarrow a = nt,\ t \in \mathbf{Z} \\ &\Leftrightarrow [a]_{Kn} = n.[t]_{Kn} \\ &\Leftrightarrow [a]_{Kn} \in n\mathbf{Z}_{Kn}. \end{aligned}$$

Portanto, concluímos que $N(f) = n\mathbf{Z}_{Kn} = \{n\,.\,[x]_{Kn} \mid [x]_{Kn} \in \mathbf{Z}_{Kn}\}$.

c) Para mostrar que $f : \mathbf{Z}_{Kn} \to \mathbf{Z}_n$ é sobrejetora, basta observar que dado $[a]_n \in \mathbf{Z}_n$, então $f([a]_n) = [a]_n$. Agora, pelo Teorema do Homomorfismo, concluímos que $\mathbf{Z}_{Kn}/N(f) \approx \mathbf{Z}_n$ e, como $N(f) = n\mathbf{Z}_{Kn}$, temos $\mathbf{Z}_{Kn}/n\mathbf{Z}_{Kn} \approx \mathbf{Z}_n$.

AULA 4

Divisibilidade em anéis

Meta da aula

Apresentar a teoria básica de divisibilidade em anéis e o conceito de máximo divisor comum.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Operar com as propriedades básicas de divisibilidade.
- Operar com o conceito de máximo divisor comum.
- Demonstrar propriedades do máximo divisor comum.

Pré-requisito

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos nas Aulas 21 a 23 do curso de Álgebra I, e das Aulas 1 e 2 deste curso.

INTRODUÇÃO

Nesta aula, vamos imitar a teoria de divisibilidade desenvolvida para os números inteiros, agora, no contexto dos anéis. A sensação que você deve ter é a de uma repetição da construção dos conceitos de divisibilidade desenvolvidos no curso de Álgebra I.

Vamos começar apresentando a noção de divisor em um anel.

Definição 1

Sejam A um anel e $a, b \in A$. Dizemos que a *divide b*, e denotamos $a \mid b$, se existe um elemento $c \in A$ tal que $b = c \cdot a$. Nesse caso, dizemos também que a *é um divisor de b*, ou que *a é um fator de b*, ou que *b é um múltiplo de a*, ou, ainda, que *b é divisível por a*.

Se não existe um elemento c tal que $b = c \cdot a$, diremos que *a não divide b*, o que denotamos por $a \Phi b$.

Exemplo 1

No anel dos inteiros $\mathbf{Z}$, temos:

i. $4 \mid 12$, pois $12 = 3.4$;

ii. $(-5) \mid 35$, pois $35 = 7.(-5)$;

iii. $4 \mid 11$, pois não existe $c \in \mathbf{Z}$ tal que $11 = c \cdot 4$.

Exemplo 2

No anel $\mathbf{Q}$ dos números racionais, temos $4 \mid 7$, pois $7 = \frac{7}{4} \cdot 4$ e $\frac{7}{4} \in \mathbf{Q}$.

Exemplo 3

No anel $\mathbf{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$ dos inteiros módulo 8, temos:

i. $\overline{2} \mid \overline{6}$, pois $\overline{6} = \overline{3} \cdot \overline{2}$;

ii. $\overline{5} \mid \overline{2}$, pois $\overline{2} = \overline{2} \cdot \overline{5}$.

iii. $\overline{4} \mid \overline{7}$, pois você pode facilmente verificar que não existe $\overline{c} \in \mathbf{Z}_8$ tal que $\overline{7} = \overline{c} \cdot \overline{4}$.

Veremos, agora, uma seqüência de propriedades de divisibilidade num anel *A*. Observe que elas são semelhantes às propriedades sobre divisibilidade dos números inteiros.

Proposição 1

Sejam a, b, c, d,... elementos de um anel A. Então:

1. $a \mid a$ e $a \mid 0_A$, onde 0_A é o elemento neutro da adição de A.

2. Se u é um elemento invertível em A, então $u \mid a$. Em particular, $1_A \mid a$, onde 1_A é o elemento neutro da multiplicação de A.

3. Se $a \mid b$ e $b \mid c$, então $a \mid c$.

4. Se $a \mid b$, então $a \mid b \,.\, c$.

5. Se $a \mid b$ e $a \mid c$, então $a \mid (b + c)$ e $a \mid (b - c)$.

6. Se $a \mid b$ e $a \mid c$, então $a \mid (x \,.\, b + y \,.\, c)$, para todo $x, y \in A$.

7. Se $a \mid b$ e $c \mid d$, então $a \,.\, c \mid b \,.\, d$.

8. Se $a \mid (b + c)$ e $a \mid c$, então $a \mid c$.

Demonstração

Lembre que costumamos denotar 0_A por 0 e 1_A por 1, sempre que não houver risco de confusão.

1. Como $0 = 0 \,.\, a$ para todo a, então, da definição de divisibilidade, concluímos que $a \mid 0$. E, também, como $a = 1 \,.\, a$, concluímos que $a \mid a$.

2. Temos que

$$\begin{aligned} a &= a \,.\, 1 \\ &= a.\, (u^{-1}.\, u), \text{ pois } u \text{ é invertível} \\ &= (a \,.\, u^{-1}) \,.\, u. \end{aligned}$$

Como $a \,.\, u^{-1} \in A$, concluímos que a é múltiplo de u, o que significa que $u \mid a$. Em particular, como 1 é um elemento invertível de A, então $1 \mid a$. Essa última afirmação também pode ser facilmente verificada de modo direto, pois $a = a \,.\, 1$.

3. Supondo que $a \mid b$ e $b \mid c$, então existem elementos $s, t \in A$ tais que $b = s \,.\, a$ e $c = t \,.\, d$. Logo,

$$\begin{aligned} c &= t \,.\, b \\ &= t \,.\, (s \,.\, a), \text{ pois } b = s \,.\, a \\ &= (t \,.\, s) \,.\, a. \end{aligned}$$

Como $t \,.\, s \in A$, concluímos que c é múltiplo de a, o que prova que $a \mid c$.

Observe que nas provas das propriedades usamos somente a definição de divisibilidade e as propriedades de anel já conhecidas. Tente, agora, montar argumentos semelhantes para demonstrar a propriedade 4. Esta será a sua primeira atividade desta aula.

ATIVIDADE

1. Prove que se $a \mid b$, então $a \mid b \cdot c$.

Continuaremos, agora, com as demonstrações das outras propriedades. Observe, primeiramente, que a propriedade 5 é um caso particular da propriedade 6. Portanto, vamos primeiro provar a propriedade 6 e, depois, tirar como conseqüência a validade da propriedade 5. Observe que este tipo de argumento, ou seja, provar uma propriedade mais geral e tirar um caso particular como conseqüência, é muito comum na matemática.

6. Supondo que $a \mid b$ e $a \mid c$, então existem elementos $s, t \in A$ tais que $b = s \cdot a$ e $c = t \cdot a$. Assim, para todo $x, y \in A$, temos que

$$\begin{aligned} x \cdot b + y \cdot c &= x \cdot (s \cdot a) + y \cdot (t \cdot a), \text{ pois } b = s \cdot a \text{ e } c = t \cdot a \\ &= (x \cdot s) \cdot a + (y \cdot t) \cdot a \\ &= (x \cdot s + y \cdot t) \cdot a. \end{aligned}$$

Como $x, y, s, t \in A$ e A é um anel, então $x \cdot s + y \cdot t \in A$. Portanto, temos que $x \cdot b + y \cdot c$ é múltiplo de a, o que prova que $a \mid (x \cdot b + y \cdot c)$.

Vamos concluir a prova da propriedade 5.

5. Observe que, na propriedade 6, tomando $x = y = 1$, obtemos que $a \mid (b + c)$. Agora, tomando $x = 1$ e $y = -1$, obtemos $a \mid (b - c)$.

A próxima propriedade (a 7ª) será mais uma atividade para você. Tente imitar os argumentos usados anteriormente.

ATIVIDADE

2. Prove que se $a \mid b$ e $c \mid d$, então $a \cdot c \mid b \cdot d$.

Vamos, agora, demonstrar a última propriedade.

8. Supondo que $a \mid (b + c)$ e $a \mid b$, então existem elementos $s, t \in A$ tais que $b + c = s \cdot a$ e $b = t \cdot a$. Logo,

$$\begin{aligned} c &= (b + c) - b \\ &= s \cdot a - t \cdot a, \text{ pois } b + c = s \cdot a \text{ e } b = t \cdot a \\ &= (s - t) \cdot a \end{aligned}$$

Como $s - t \in A$, concluímos que c é múltiplo de a, o que prova que $a \mid c$. □

Lembre que no anel $\boldsymbol{Z}$ dos números inteiros vale uma propriedade que diz que se $a \mid b$ e $b \mid a$, então $b = a$ ou $b = -a$. Agora, observe que 1 e –1 são os únicos elementos invertíveis de $\boldsymbol{Z}$ e que $\boldsymbol{Z}$ é um domínio de integridade. Lembre, também, que um domínio de integridade é um anel que não tem divisores de zero, isto é, não existem elementos não-nulos a e b tais que $a \cdot b = 0$. Isso nos dá a motivação para a próxima propriedade.

Proposição 2

Sejam a e b dois elementos de um domínio de integridade A. Então, $a \mid b$ e $b \mid a$ se, e somente se, existir um elemento invertível $u \in A$, tal que $b = u \cdot a$.

Demonstração

($\Rightarrow$) Supondo que $a \mid b$ e $b \mid a$, vamos mostrar que existe um elemento invertível $u \in A$, tal que $b = u \cdot a$.

Como $a \mid b$ e $b \mid a$, então existem elementos u e t em A, tais que $b = u \cdot a$ e $a = t \cdot b$.

1º caso: $b = 0$. Nesse caso, temos $a = t \cdot b = t \cdot 0 = 0$, o que prova que $b = a = 1 \cdot a$. Veja que, nesse caso, podemos escolher $u = 1$, concluindo que $b = 1 \cdot a$, sendo 1 um elemento invertível.

2º caso: $b \neq 0$. Nesse caso, temos

$$\begin{aligned} b &= u \cdot a \\ &= u \cdot (t \cdot b), \text{ pois } a = t \cdot b \\ &= (u \cdot t) \cdot b. \end{aligned}$$

Como A é um domínio de integridade e $b \neq 0$, vale a lei do cancelamento em A (veja a Proposição 2 da Aula 4) para o elemento b, ou seja,

$$(u \,.\, t) \,.\, b = 1 \,.\, b \quad \text{e} \quad b \neq 0 \;\Rightarrow\; u \,.\, t = 1.$$

Como $u \,.\, t = 1$ e $t \in A$, concluímos que o elemento u é invertível. Daí, segue que $b = u \,.\, a$ com u invertível em A.

($\Leftarrow$) Agora, supondo que $b = u \,.\, a$, com u invertível em A, vamos provar que $a \mid b$ e $b \mid a$.

Como $b = u \,.\, a$, temos que b é múltiplo de a, ou seja, $a \mid b$. Agora, sendo u um elemento invertível de A, temos que

$$b = u \,.\, a \;\Rightarrow\; a = u^{-1} \,.\, b.$$

Como $u^{-1} \in A$, já que u é invertível, concluímos que a é múltiplo de b, ou seja, $b \mid a$. □

Em particular, você pode obter outra demonstração para a propriedade dos números inteiros mencionada anteriormente. Esta será sua próxima atividade.

ATIVIDADE

3. Use a Proposição 2 para provar que se a e b são dois números inteiros, tais que $a \mid b$ e $b \mid a$, então $b = a$ ou $b = -a$.

Definição 2

Dois elementos, a e b, de um anel A são chamados de *elementos associados* se existir um elemento invertível $u \in A$ tal que $b = u \,.\, a$.

Assim, podemos reescrever a Proposição 2 nessa nova linguagem.

Proposição 3

Em um domínio de integridade A, dois elementos a e b são associados se, e somente se, $a \mid b$ e $b \mid a$.

Vamos, agora, estender para um anel qualquer o conceito de máximo divisor comum, já conhecido do seu estudo do anel dos inteiros $\mathbf{Z}$. Daremos inicialmente a definição para dois elementos de um anel.

Definição 3

Sejam dois elementos, a e b, de um anel A; dizemos que um elemento, $d \in A$, é um *máximo divisor comum* de a e b se:

MDC1. d é um divisor comum de a e b, isto é, $d \mid a$ e $d \mid b$;

MDC2. todo divisor comum q de a e b também é divisor de d, isto é, se $q \mid a$ e $q \mid b$, então $q \mid d$.

Nesse caso, dizemos, simplesmente, que d é um *mdc* de a e b e denotamos $d = mdc(a, b)$.

A relação imediata que temos para dois máximos divisores comuns de a e b está contida na próxima propriedade.

Proposição 4

Sejam dois elementos, a e b, de um anel A com máximo divisor comum d. Um elemento $d_1 \in A$ é um máximo divisor comum de a e b se, e somente se, $d_1 \mid d$ e $d \mid d_1$.

Demonstração

($\Rightarrow$) Estamos supondo que d_1 é um mdc de a e b. Então, em particular, $d_1 \mid a$ e $d_1 \mid b$, isto é, d_1 é um divisor comum de a e b. Como d é um mdc de a e b, então temos que, por MDC2, $d_1 \mid d$.

Por outro lado, como d é um mdc de a e b, então, por MDC1 compreendemos que $d \mid a$ e $d \mid b$. E, agora, como d_1 é um mdc de a e b, então, por MDC2, temos $d \mid d_1$.

($\Leftarrow$) Estamos supondo, agora, que $d_1 \mid d$ e $d \mid d_1$. Queremos concluir que d_1 é um mdc de a e b.

Como d é um mdc de a e b, então $d \mid a$ e $d \mid b$. Agora, como $d_1 \mid d$, temos, pela Proposição 1.3, que $d_1 \mid a$ e $d_1 \mid b$, ou seja,

$$\begin{aligned} &d_1 \mid d \text{ e } d \mid a \Rightarrow d_1 \mid a \text{ e} \\ &d_1 \mid d \text{ e } d_1 \mid b \Rightarrow d_1 \mid b, \end{aligned}$$

portanto d_1 é um divisor comum de a e b. Agora, dado qualquer divisor q de a e b temos, por MDC2, que $q \mid d$. Da hipótese, temos que $d \mid d_1$. Assim, temos:

$$q \mid d \text{ e } d \mid d_1 \Rightarrow q \mid d_1,$$

ou seja, todo divisor q de a e b também é divisor de d_1. E, com isso, concluímos que d_1 também é um mdc de a e b. □

Num anel, elementos que se comportam do mesmo modo quanto à divisibilidade são chamados de elementos associados. A seguir veremos sua definição formal.

Veja, agora, como fica a relação entre dois máximos divisores comuns de dois elementos num domínio de integridade.

Proposição 5

Sejam dois elementos, a e b, de um domínio de integridade A com máximo divisor comum d. Um elemento, $d_1 \in A$, é um máximo divisor comum de a e b se, e somente se, d_1 é associado a d.

Demonstração

($\Rightarrow$) Estamos supondo que $d_1 \in A$ é um máximo divisor comum de a e b e queremos provar que d_1 é associado a d. Pela Proposição 3, temos que $d_1 \mid d$ e $d \mid d_1$, agora, pela Proposição 4, já que A é um domínio de integridade, segue que d_1 e d são elementos associados.

($\Leftarrow$)Supondo, agora, que d_1 é associado a d, então, pela Proposição 4, já que A é um domínio de integridade, temos $d_1 \mid d$ e $d \mid d_1$. Depois, pela Proposição 3, segue que d_1 é um máximo divisor comum de a e b. □

ATIVIDADE FINAL

Mostre que a relação binária no anel A, definida por $a \sim b \Leftrightarrow a$ é associado a b, é uma relação de equivalência.

RESUMO

Nesta aula, vimos o conceito de divisibilidade num anel A, em que dizemos que a divide b quando existe um elemento $c \in A$, tal que $b = c \cdot a$. Em seguida, vimos muitas propriedades de divisibilidade, todas elas generalizações de propriedades semelhantes aos números inteiros. Depois, vimos o conceito de máximo divisor comum, que é um divisor comum que é múltiplo de todos os demais divisores comuns, e de elementos associados, onde a e b são associados se existir elemento invertível $u \in A$, tal que $b = u \cdot a$.

RESPOSTAS

Atividade 1

Se $a \mid b$, então existe $S \in A$, tal que $b = s \,.\, a$. Assim,

$$\begin{aligned} b \,.\, c &= (s \,.\, a) \,.\, c, \text{ pois } b = s \,.\, a \\ &= s \,.\, (a \,.\, c) \\ &= s \,.\, (c \,.\, a) \\ &= (s \,.\, c) \,.\, a, \text{ múltiplo de } a, \end{aligned}$$

o que prova que $a \mid b \,.\, c$.

Atividade 2

Se $a \mid b$ e $c \mid d$, então existem elementos s e t no anel A, tais que $b = s \,.\, a$ e $d = t \,.\, c$. Logo,

$$\begin{aligned} b \,.\, d &= (s \,.\, a) \,.\, (t \,.\, c), \text{ pois } b = s \,.\, a \text{ e } d = t \,.\, c. \\ &= (s \,.\, t) \,.\, (a \,.\, c), \text{ múltiplo de } a \,.\, c, \end{aligned}$$

o que prova que $a \,.\, c \mid b \,.\, d$.

Atividade 3

Pela Proposição 2, como $a \mid b$, $b \mid a$ e $\boldsymbol{Z}$ é um domínio de integridade, então $b = u \,.\, a$ com u invertível em $\boldsymbol{Z}$. Como os únicos elementos invertíveis em $\boldsymbol{Z}$ são 1 e –1, segue que $b = a$ ou $b = -a$.

Atividade Final

A relação é reflexiva, isto é, $a \sim a$, pois $a = 1_A \,.\, a$ e o elemento 1_A é invertível.

A relação é simétrica, isto é, $a \sim b \Rightarrow b \sim a$, pois

a ~ b $\Rightarrow$ existe elemento invertível $u \in A$, tal que $b = u \,.\, a$.

$\Rightarrow a = u^{-1} \,.\, b =$ e u^{-1} é um elemento invertível

$\Rightarrow b \sim a$.

A relação é transitiva, isto é, $a \sim b$ e $b \sim c \Rightarrow a \sim c$, pois

$a \sim b$ e $b \sim c \Rightarrow b = u \,.\, a$ e $c = v \,.\, b$ com u e v elementos invertíveis

$\Rightarrow c = v \,.\, b = (v \,.\, u) \,.\, a$ com $v \,.\, u$ um elemento invertível

$\Rightarrow a \sim c$.

Assim, a relação "~" sendo reflexiva, simétrica e transitiva, faz dela uma relação de equivalência.

AULA 5

Introdução aos polinômios

Meta da aula

Apresentar o conceito de um polinômio com coeficientes num anel A.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Reconhecer um polinômio sobre um anel A.
- Determinar o grau de um polinômio.
- Determinar se um escalar é uma raiz de um polinômio.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos nas Aulas 21 a 23 do curso de Álgebra I, e da Aula 1 deste curso.

INTRODUÇÃO

Como todo estudante, você já deve ter visto expressões como

$$x + x^2,\ \ 5 + x^3,\ 17 + x^2 + 2x^3.$$

Essas expressões são conhecidas como polinômios, mais exatamente, polinômios de uma variável. Nesses exemplos, os coeficientes que aparecem pertencem ao corpo dos números reais.

Nesta aula, começaremos a estudar essas expressões num contexto mais geral, o que permitirá considerar os coeficientes dos polinômios pertencendo a um anel qualquer. Assim, nosso estudo abrangerá expressões tais como

$$\overline{3}x\ + \overline{5}x^2 \ \text{ com } \overline{3}, \overline{5} \in \mathbf{Z}_4 \text{ , por exemplo.}$$

Para estudarmos essas expressões, definiremos as operações de soma e produto de polinômios e veremos, nesse contexto, que o conjunto dos polinômios forma um anel, chamado um anel de polinômios.

Considere $(A, +, .)$ um anel. Lembre que isso significa um anel comutativo e com unidade ($1_A \in A$). No que se segue, a letra x denotará uma *variável* ou um *símbolo*.

DEFINIÇÃO 1

Um *polinômio* na variável x com *coeficientes* no anel A é uma soma da forma

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots$$

onde cada $a_i \in A$ e $a_i = 0$ para todo i suficientemente grande (e isso significa que existe $n \in \mathbf{N}$ tal que $a_i = 0$ para todo $i > n$).

Os escalares a_i são chamados de *coeficientes* do polinômio. Assim,

a_0 é o *coeficiente constante*;

a_1 é o *coeficiente do termo linear* x;

a_2 é o *coeficiente do termo quad*rático x^2;

a_3 é o *coeficiente do termo cúbico* x^3.

Como temos os coeficientes $a_1 = 0$ para todo $i > n$, podemos denotar o polinômio $a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots$ por

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n.$$

Exemplo 1

Isso significa que o polinômio $1 + 2x + 3x^2 + 1x^3 + 0x^4 + 0x^5 + 0x^6 + \ldots$ será denotado por

$$1 + 2x + 3x^2 + x^3 \text{ ou } f(x) = 1 + 2x + 3x^2 + x^3.$$

O polinômio cujos coeficientes são *todos* iguais a zero,

$$0 + 0x + 0x^2 + 0x^4 + 0x^5 + 0x^6 + \ldots,$$

chamado *polinômio nulo*, será denotado simplesmente por **0**. Observe, também, no caso a seguir, que a falta do termo x^2 em

$$f(x) = 4 + 2x - \frac{7}{3}x^3$$

significa que o coeficiente de x^2 é igual a zero, isto é, $a^2 = 0$.

DEFINIÇÃO 2

Denotamos o conjunto dos polinômios sobre o anel A por

$$A[x] = \{\text{Polinômios na variável } x \text{ com coeficientes em } A\}$$
$$= \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \mid a_i \in A \text{ e } n \in \mathbf{N}\}.$$

Exemplo 2

Temos

$$\mathbf{Z}[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \mid a_i \in \mathbf{Z} \text{ e } n \in \mathbf{N}\};$$
$$\mathbf{Q}[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \mid a_i \in \mathbf{Q} \text{ e } n \in \mathbf{N}\};$$
$$\mathbf{R}[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \mid a_i \in \mathbf{R} \text{ e } n \in \mathbf{N}\};$$
$$\mathbf{C}[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \mid a_i \in \mathbf{C} \text{ e } n \in \mathbf{N}\};$$
$$\mathbf{Z}_m[x] = \{\overline{a}_0 + \overline{a}_1x + \overline{a}_2x^2 + \overline{a}_3x^3 + \ldots + \overline{a}_nx^n \mid \overline{a}_i \in \mathbf{Z}_m \text{ e } n \in \mathbf{N}\}.$$

Assim, temos também

$p(x) = 1 + 2x + 3x^2 + x^3 \in \mathbf{Z}[x]$;

$f(x) = 4 + 2x - \frac{7}{3} x^3 \in \mathbf{Q}[x]$, mas $f(x) \notin \mathbf{Z}[x]$, pois $\frac{7}{3} \notin \mathbf{Z}$;

$g(x) = (3 + \sqrt{2}) - (1 + \sqrt{2}) x^3 \in \mathbf{R}[x]$, mas $g(x) \notin \mathbf{Q}[x]$, pois $3 + \sqrt{2} \notin \mathbf{Q}$;

$h(x) = (2 - i)x + (4 + 1)x^4 \in \mathbf{C}[x]$, mas $h(x) \notin \mathbf{R}[x]$, pois $2 - i \notin \mathbf{R}$.

Lembre que **C** representa o corpo dos números complexos, ou seja,

$$\mathbf{C} = \{a + bi \mid a, b \in \mathbf{C} \text{ e } i = \sqrt{-1}\}.$$

Algumas observações são muito importantes:

1. $A \subset A[x]$. Os elementos do anel A, em $A[x]$, fazem o papel dos *polinômios constantes*, $f(x) = a_0$ (com $a_1 = 0$ para todo $i > 0$).

2. Se A e B são anéis e $A \subset B$, então $A[x] \subset B[x]$.

Esta última observação consiste na sua primeira atividade.

ATIVIDADE

1. Prove que se A e B são anéis e $A \subset B$, então $A[x] \subset B[x]$.

Na teoria dos polinômios, o último termo não-nulo exerce um papel importante. É esse termo que vamos estabelecer na próxima definição.

DEFINIÇÃO 3

Seja A um anel e $f(x)$ um polinômio em $A[x]$ tal que

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n \quad \text{com} \quad a_n \neq 0 \quad \text{e} \quad n \geq 0.$$

Neste caso, dizemos que o polinômio $f(x)$ tem *grau n* e denotamos $gr(f) = n$. O coeficiente a_n é chamado de *coeficiente líder*. Em particular, quando o coeficiente líder for igual a 1,

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + x^n, \quad a_n = 1,$$

dizemos que $f(x)$ é um *polinômio mônico*. Observe, também, que não estamos definindo o grau do polinômio nulo.

Exemplo 3

a) O polinômio

$$f(x) = 1 + 2x + 3x^2 + x^3 \in \mathbf{Z}[x]$$

tem grau 3, $gr(f) = 3$. Observe que $f(x)$ é um polinômio mônico

b) O polinômio

$$p(x) = \overline{3} + \overline{4}x^2 + \overline{5}x^4 \in \mathbf{Z}_7[x]$$

tem grau 4, $gr(p) = 4$. Observe que $p(x)$ não é um polinômio mônico.

c) O polinômio

$$g(x) = (1 - i)x + 2ix^3 + x^5 \in \mathbf{C}[x]$$

tem grau 5, $gr(g) = 5$. Observe que $g(x)$ é um polinômio mônico.

Vamos estudar, agora, a igualdade de dois polinômios.

DEFINIÇÃO 4

Sejam $f(x)$ e $g(x)$ dois polinômios em $A[x]$, digamos,

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n.$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_mx^m.$$

Dizemos que os polinômios $f(x)$ e $g(x)$ *são iguais*, e denotamos $f(x) = g(x)$, se

$$a_i = b_i \text{ para todos os valores de } i.$$

Em particular, observe que se $gr\ (f) = n$ e $gr(g) = m$, então $n = m$. Assim, dois polinômios são iguais, se eles tiverem o mesmo grau e se seus coeficientes correspondentes forem iguais.

Exemplo 4

Os polinômios

$$f(x) = 1 + 2x + 3x^2 + x^3 \in \mathbf{Z}[x]$$

e

$$g(x) = 1 + 2x - 3x^2 + x^3 \in \mathbf{Z}[x]$$

não são iguais, pois $a_2 = 3 \neq -3 = b_2$. Já os polinômios

$$p(x) = 1 + 3x^2 + x^3 \in \mathbf{Z}[x]$$

e

$$q(x) = 1 + 0x + 3x^2 + x^3 \in \mathbf{Z}[x]$$

são iguais, pois todos os seus coeficientes correspondentes são iguais.

Você provavelmente já conhece os conceitos de valor de um polinômio e raiz ou zero de um polinômio. Vamos, então, relembrá-los.

DEFINIÇÃO 5

Dados um polinômio $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n \in A[x]$ e um escalar $\alpha \in A$, dizemos que

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + ... + a_n\alpha^n$$

é o *valor de f em* α. Como A é um anel e, portanto, fechado sob as operações de adição e multiplicação, então temos

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + ... + a_n\alpha^n \in A.$$

No caso em que $f(\alpha) = 0$, dizemos que α é uma *raiz* de f ou um *zero* de f *em* A.

Exemplo 5

Seja $f(x) = 3 + 2x - 5x^3 \in Z[x]$. O valor de $f(x)$ em $\alpha = 2$ é

$$\begin{aligned} f(2) &= 3 + 2 \,.\, 2 - 5 \,.\, 2^3 \\ &= 3 + 4 - 40 \\ &= -33. \end{aligned}$$

Então, temos $f(2) = -33$ e, em particular, $\alpha = 2$ não é uma raiz de $f(x)$. Agora, para $\alpha = 1$ temos o valor

$$\begin{aligned} f(1) &= 3 + 2 \,.\, 1 - 5 \,.\, 1^3 \\ &= 3 + 2 - 5 \\ &= 0. \end{aligned}$$

Portanto, já que $1 \in Z$, $\alpha = 1$ é uma raiz de $f(x)$ em Z.

Exemplo 6

Seja $g(x) = \overline{1} + \overline{2}x + \overline{2}x^2 \in Z_3[x]$, onde $Z_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ é o anel das classes residuais módulo 3. Os valores que $g(x)$ assume em Z_3 são:

$$\begin{aligned} g(\overline{0}) &= \overline{1} + \overline{2} \,.\, \overline{0} + \overline{2} \,.\, \overline{0}^2 \\ &= \overline{1} + \overline{0} + \overline{0} \\ &= 1 \in Z_3; \end{aligned}$$

$$\begin{aligned} g(\overline{1}) &= \overline{1} + \overline{2} \,.\, \overline{1} + \overline{2} \,.\, \overline{1}^2 \\ &= \overline{1} + \overline{2} + \overline{2} \\ &= \overline{5} \\ &= \overline{2} \in \mathbf{Z}_3; \end{aligned}$$

$$\begin{aligned} g(\overline{2}) &= \overline{1} + \overline{2} \,.\, \overline{2} + \overline{2} \,.\, \overline{2}^2 \\ &= \overline{1} + \overline{4} + \overline{8} \\ &= \overline{13} \\ &= \overline{1} \in \mathbf{Z}_3; \end{aligned}$$

Como $g(\overline{0}) \neq \overline{0}$, $g(\overline{1}) \neq \overline{0}$ e $g(\overline{2}) \neq \overline{0}$, então o polinômio $g(x) = \overline{1} + \overline{2}x + \overline{2}x^2 \in \mathbf{Z}_3[x]$ não tem raiz em $\mathbf{Z}_3$. Observe que $\propto = \overline{0}, \overline{1}, \overline{2}$ são as únicas possibilidades de raiz em $\mathbf{Z}_3$ e, uma vez descartadas estas, podemos concluir que o polinômio não tem raízes em $\mathbf{Z}_3$.

Exemplo 7

Seja $h(x) = 1 + x^2 \in \mathbf{R}[x]$. O valor de $h(x)$ no escalar $\alpha \in \mathbf{R}$ é dado pela expressão

$$\begin{aligned} h(\alpha) &= 1 + \alpha^2 \\ &= \alpha^2 + 1 \in \mathbf{R}. \end{aligned}$$

Sabemos que, dado $\alpha \in \mathbf{R}$, então $\alpha^2 \geq 0$. Assim,

$$\alpha^2 + 1 > 0,$$

isto é, a expressão $\alpha^2 + 1$ terá sempre um valor positivo e, portanto, nunca será igual a zero para qualquer que seja o valor de $\alpha \in \mathbf{R}$. Assim, concluímos que $h(\alpha) \neq 0$ para todo $\alpha \in \mathbf{R}$ e isso significa que o polinômio $h(\alpha) = 1 + x^2$ $\mathbf{R}[x]$ não possui raiz em $\mathbf{R}$. Dizemos que $h(x) \in \mathbf{R}[x]$ *não tem raízes reais*.

Por outro lado, temos

$$\mathbf{R} \subset \mathbf{C}$$

e, portanto,

$$\mathbf{R}[x] \subset \mathbf{C}[x].$$

Agora, dado $\boldsymbol{i} \in \mathbf{C}$, $\boldsymbol{i} = \sqrt{-1}$, temos

$$\begin{aligned} h(i) &= 1 + i^2 \\ &= 1 + (-1) \\ &= 0, \end{aligned}$$

ou seja, $\alpha = \boldsymbol{i}$ é uma raiz de $h(x) = 1 + x^2$ em $\mathbf{C}$. Dizemos que i é uma *raiz complexa* de $h(x)$. Veja, também, que $\alpha = -\boldsymbol{i}$ é outra raiz complexa de $h(x) = 1 + x^2$, já que

$$\begin{aligned} h(-i) &= 1 + (-i)^2 \\ &= 1 + (-1) \\ &= 0. \end{aligned}$$

Observe que o exemplo anterior teve o propósito de ressaltar o fato de quando falamos em raiz de um polinômio, devemos especificar o anel com o qual estamos trabalhando. Mais especificamente, dizer, simplesmente, "o polinômio $h(x) = 1 + x^2$ não tem raiz", consiste numa afirmação incompleta, pois vimos que este polinômio não tem raízes reais, mas tem raízes complexas.

Vamos ver, agora, uma propriedade muito simples, porém muito importante sobre raízes nulas de um polinômio.

Proposição 1

Seja o polinômio $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \in \boldsymbol{A}[x]$ com raiz nula, isto é, com $f(0) = 0$. Então o coeficiente constante é igual a zero, ou seja, $a_0 = 0$, e $f(x)$ é da forma

$$f(x) = a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n .$$

Demonstração

De $f(0) = 0$ segue que

$$a_0 + a_1 . 0 + a_2 . 0^2 + a_3 . 0^3 + \ldots + a_n . 0^n = 0,$$

o que nos dá

$$a_0 = 0.$$

Portanto, $f(\mathrm{x}) = a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n . \square$

ATIVIDADES FINAIS

1. Seja $f(x) = x^2 - 2 \in \mathbf{Q}[x]$. Use o fato de $\sqrt{2} \notin \mathbf{Q}$ para mostrar que $f(x)$ não tem raízes racionais. Verifique que $f(x)$ possui raízes reais e encontre essas raízes.

2. Determine o polinômio $f(x) \in \mathbf{R}[x]$, de 3º grau, que apresenta uma raiz nula e satisfaz a condição $f(x - 1) = f(x) + (2x)^2$ para todo x real.

3. Com o auxílio do polinômio obtido no exercício anterior, calcule a soma $2^2 + 4^2 + \ldots + (2n)^2$, onde $n \geq 1$ é um número natural.

RESUMO

O conceito de polinômio em uma variável é dado por:

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n ,$$

com coeficientes $a_0 , a_1 , a_2 , \ldots , a_n$ num anel A. O grau de um polinômio é o maior valor de n tal que $a_n \neq 0$. O conceito de raiz de um polinômio é um escalar $\alpha \in A$ tal que $f(\alpha) = 0$.

RESPOSTAS

Atividade 1

Dado o polinômio

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \in \boldsymbol{A}[x],$$

então os coeficientes $a_1 \in \boldsymbol{A}$ para $i = 0, 1, \ldots, n$. Como $\boldsymbol{A} \subset \boldsymbol{B}$, então cada $a_1 \in \boldsymbol{B}$, e isto significa que

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \in \boldsymbol{B}[x].$$

Portanto, provamos que $\boldsymbol{A}[x] \subset \boldsymbol{B}[x]$.

Atividade Final 1

Veja que

$$\begin{aligned} f(x) = 0 &\Leftrightarrow x^2 - 2 = 0 \\ &\Leftrightarrow x^2 = 2 \\ &\Leftrightarrow x = \pm\sqrt{2} \end{aligned}$$

Assim, as única raízes de $f(x)$ são os números reais $\sqrt{2}$ e $-\sqrt{2}$. Como $\sqrt{2} \notin \mathbf{Q}$, então $f(x)$ não tem raízes racionais. Mas $f(x)$ tem duas raízes reais, a saber, e.

Atividade Final 2

Como o polinômio $f(x)$ é de grau 3, então podemos escrever

$$f(x) = ax^3 + bx^2 + cx + d \text{ com } a, b, c, d \in \mathbf{R} \text{ e } a \neq 0.$$

Como $f(0) = 0$, temos, pela Proposição 1, que $d = 0$ e, assim,

$$f(x) = ax^3 + bx^2 + cx.$$

Agora, substituindo $x = 0$ em $f(x - 1) = f(x) + f(2x)^2$, obtemos

$$\begin{aligned} f(-1) &= f(0) + (2 \cdot 0)^2 \\ &= 0 + 0 \\ &= 0, \end{aligned}$$

isto é, $f(-1) = 0$. Portanto, –1 também é uma raiz de $f(x)$.

Substituindo $x = 1$ em $f(x - 1) = f(x) + (2x)^2$, obtemos

$$f(0) = f(1) + (2 \cdot 1)^2,$$

o que nos dá

$$\begin{aligned} f(1) &= f(0) - 2^2 \\ &= 0 - 4 \\ &= -4, \end{aligned}$$

isto é, $f(1) = -4$. Finalmente, substituindo $x = 2$ em $f(x - 1) = f(x) + (2x)^2$, obtemos

$$f(2 - 1) = f(2) + (2 \cdot 2)^2,$$

o que nos dá

$$\begin{aligned} f(2) &= f(1) + 4^2 \\ &= -4 - 16 \\ &= -20, \end{aligned}$$

isto é, $f(2) = -20$. Agora, substituindo $f(-1) = 0$, $f(1) = -4$ e $f(2) = -20$ em $f(x) = ax^3 + bx^2 + cx$, obtemos o sistema linear

$$\begin{cases} -a + b - c = 0 \\ a + b + c = -4 \\ 8a + 4b + 2c = -20, \end{cases}$$

cuja solução, usando as técnicas já aprendidas no curso de Álgebra Linear II, é

$$a = -\frac{4}{3},\ b = -2 \text{ e } c = -\frac{2}{3}.$$

Portanto, temos

$$f(x) = -\frac{4}{3}x^3 - 2x^2 - \frac{2}{3}x.$$

Atividade Final 3

De $f(x-1) = f(x) + (2x)^2$ temos a expressão $(2x)^2 = f(x-1) - f(x)$ que usaremos na soma $2^2 + 4^2 + \ldots + (2n)^2$. Temos:

$$\begin{aligned} 2^2 + 4^2 + \ldots + (2n)^2 &= (2 \,.\, 1)^2 + (2 \,.\, 2)^2 + \ldots + (2 \,.\, n)^2 \\ &= (f(0) - f(1)) + (f(1) - f(2)) + \ldots + (f(n-1) - f(n)) \\ &= f(0) - f(n). \end{aligned}$$

Agora, usando a expressão $f(x) = -\frac{4}{3}x^3 - 2x^2 - \frac{2}{3}x$ obtida na atividade anterior, temos:

$$\begin{aligned} 2^2 + 4^2 + \ldots + (2n)^2 &= f(0) - f(n) \\ &= 0 - (-\frac{4}{3}n^3 - 2n^2 - \frac{2}{3}n) \\ &= \frac{4}{3}n^3 + 2n^2 + \frac{2}{3}n. \end{aligned}$$

AULA 6

Operações com polinômios

Meta da aula

Apresentar as operações de adição e multiplicação de polinômios com coeficientes num anel A.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Calcular a soma de dois polinômios sobre um anel A.
- Calcular o produto de dois polinômios sobre um anel A.
- Determinar o grau do polinômio soma.
- Determinar o grau do polinômio produto.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I, e da introdução aos polinômios, na Aula 5.

INTRODUÇÃO

Lembra-se da aula passada? Vimos que se A é um anel, e isso significa um anel comutativo e com unidade ($1_A \in A$), então denotamos o conjunto dos polinômios sobre o anel A por $A[x]$, isto é,

$$A[x] = \{\text{polinômios na variável x com coeficientes em } A\}$$
$$= \{ a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n \ \big| a_i \in A \text{ e } n \in N\}.$$

Nesta aula, vamos definir as operações de adição e multiplicação em $A[x]$, ou seja, a soma e o produto de polinômios. Depois, veremos como o grau de um polinômio se comporta perante estas operações.

DEFINIÇÃO 1

Sejam $f(x)$ e $g(x)$ dois polinômios em $A[x]$, digamos,

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_mx^m.$$

Podemos supor, sem perda de generalidade, que $m \leq n$. Definimos as operações de adição e multiplicação de polinômios como segue.

1. *Adição de polinômios. O polinômio soma* $f(x) + g(x)$ é definido por

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_m + b_m)x^m + a_{m+1}x^{m+n} ... + a_nx^n$$
$$= c_0 + c_1x + c_2x^2 + c_3x^3 + ... + c_nx^n,$$

onde os novos coeficientes são dados por $c_K = a_K + b_K$ para cada $k = 1, 2, ..., n$. Observe que $b_K = 0$ para todo $k > m$.

Assim, para somarmos dois polinômios, simplesmente somamos os seus coeficientes correspondentes.

2. *Multiplicação de polinômios*. O *polinômio produto* $f(x) . g(x)$ é definido por

$$f(x) . g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + ... + c_{m+1}x^{m+n},$$

onde os coeficientes c_K são definidos por

$$c_0 = a_0b_0;$$
$$c_1 = a_0b_1 + a_1b_0;$$
$$c_2 = a_0b_2 + a_1b_1 + a_2b_0;$$
$$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0;$$
$$\vdots$$
$$c_K = a_0b_K + a_1b_{K-1} + a_2b_{K-2} + \ldots + a_Kb_0, \text{ para todo } k \leq m + n,$$

e onde estamos considerando que $b_K = 0$ para todo $k > m$ e $a_K = 0$ para todo $k > n$. Esta regra diz, simplesmente, que para formarmos o produto $f(x) \,.\, g(x)$, fazemos o produto de cada termo de $f(x)$ por cada termos de $g(x)$, usando a regra

$$(a_ix^i) \,.\, (b_ix^i) = a_ib_jx^{i+j}, \text{ para todo } i, j \geq 0$$

e, depois, agrupamos todos os termos que têm a mesma potência em x. Observe que a formação dos coeficientes c_K segue, simplesmente, a aplicação da lei distributiva.

Vejamos alguns exemplos.

Exemplo 1

Sejam $f(x) = 3 + 2x - x^2$ e $g(x) = 1 + 2x^2$ dois polinômios em $\boldsymbol{R}[x]$. O polinômio soma $f(x) + g(x)$ é dado por

$$\begin{aligned} f(x) + g(x) &= (3 + 2x - x^2) + (1 + 2x^2) \\ &= (3 + 1) + (2 + 0)x + (-1 + 2)x^2 \\ &= 4 + 2x + x^2. \end{aligned}$$

Já o polinômio produto $f(x) \,.\, g(x)$ é obtido como segue:

$f(x) \,.\, g(x) = (3 + 2x - x^2)(1 + 2x^2)$

$= (3 + 2x - x^2) \,.\, 1 + (3 + 2x - x^2) \,.\, 2x^2$; aplicando a lei distributiva

$= (3 + 2x - x^2) + (6x^2 + 4x^3 - 2x^4) \,.\, 2x^2$; aplicando a lei distributiva

$= 3 + 2x - 5x^2 + 4x^3 - 2x^4$; aplicando a soma de polinômios.

Vamos observar, no caso geral, que os polinômios $f(x) + g(x)$ e $f(x) \,.\, g(x)$ são, de fato, polinômios em $A[x]$. Como A é um anel e $a_K, b_K \in A$, então os coeficientes $c_K = a_K + b_K$ do polinômio soma $f(x) + g(x)$ pertencem a A, garantindo que $f(x) + g(x) \in A[x]$. Da mesma forma, cada coeficiente

$$c_K = a_0 b_K + a_1 b_{K-1} + a_2 b_{K-2} + \ldots + a_K b_0$$

do polinômio produto $f(x) \,.\, g(x)$ pertence a A, mais uma vez, garantindo que $f(x) \,.\, g(x) \in A[x]$.

ATIVIDADE

1. Calcule a soma e o produto dos polinômios $f(x) = \overline{2} + \overline{2}x^2 + x^3$ e $g(x) = \overline{1} + \overline{2}x$, em $Z_3[x]$.

_____

_____

_____

_____

Concluiremos esta aula estudando o comportamento do grau dos polinômios soma e produto. Para isso, vamos considerar que no anel A não ocorra que o produto de dois elementos não-nulos seja nulo, ou seja, que A é um domínio de integridade. Isso significa que dados $a, b \in A$ com $a \neq 0$ e $b \neq 0$, então $a \,.\, b \neq 0$, o que, em outras palavras, significa que o anel A não tem divisores de zero. Lembre, também, que o grau do polinômio

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_n x^n, \text{ com } a_0 \neq 0 \text{ e } n \geq 1,$$

é igual a n, o que denotamos por $gr(f) = n$. Observe, no Exemplo 1, que o grau do polinômio soma $f(x) + g(x)$ é igual a 2 e que o grau do polinômio produto $f(x) \,.\, g(x)$ é igual a 4.

Proposição 1

Seja A um domínio de integridade e sejam os polinômios $f(x), g(x) \in A[x]$, cujos graus são $gr(f) = n$ e $gr(g) = m$, com $m \leq n$. Então

1. $gr(f + g) \leq n = \max\{gr(f), gr(g)\}$;
2. $gr(f \cdot g) = n + m = gr(f), gr(g)$.

Demonstração

Sejam os polinômios $f(x)$ e $g(x)$ dados por

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n, \text{ com } a_n \neq 0,$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_mx^m, \text{ com } b_m \neq 0.$$

1. Assim, o polinômio soma é dado por

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_m + b_m)x^m + a_{m+1}x^{m+1} \ldots + a_nx^n$$
$$= c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_nx^n,$$

onde os novos coeficientes são dados por $c_K = a_K + b_K$ para cada $k = 1, 2, \ldots, n$. Observe que $b_K = 0$ para todo $k > m$.

Como $m \leq n$, então $b_K = 0$ e $a_K = 0$ para todo $k > n$, o que nos leva a $c_K = a_K + b_K = 0$ para todo $k > n$, e isto mostra que

$$gr(f + g) \leq n = \max\{gr(f), gr(g)\}.$$

Observe que no caso de $m < n$, temos então $b_n = 0$, o que nos dá

$$c_n = a_n + b_n = a_n \neq 0,$$

ou seja, concluímos que, neste caso, $gr(f + g) = n$, ou seja, vale a igualdade.

2. Agora, o polinômio produto é dado por

$$f(x) \,.\, g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_{m+n}x^{m+n}$$

onde os coeficientes são dados por $c_K = a_0b_K + a_1b_{K-1} + a_2b_{K-2} + \ldots + a_Kb_0$. Em particular, temos

$$\begin{aligned} c_{m+n} &= a_0b_{m+n} + a_1b_{m+n-1} + \ldots + a_{n-1}b_{m+1} + a_nb_m + a_{n+1}b_{m-1} + \ldots + a_{m+n}b_0 \\ &= a_0 \,.\, 0 + a_1 \,.\, 0 + \ldots + a_{n-1} \,.\, 0 + a_nb_m + 0 \,.\, b_{m-1} \ldots + 0 \,.\, b_0 \\ &= a_nb_m \neq 0, \end{aligned}$$

pois $b_K = 0$ para todo $k > m$, $a_K = 0$ para todo $k > n$ e $a_nb_m \neq 0$ porque $a_n \neq 0$, $b_m \neq 0$ e A é um domínio de integridade. Assim, concluímos que $gr(f \,.\, g) = n + m$. □

Observe que na prova de $gr(f + g) \leq \max\{gr(f), gr(g)\}$, na Proposição 1, não usamos a hipótese de A ser um domínio de integridade. Assim, esta propriedade vale para um anel A qualquer. Já não é o caso da segunda parte, $gr(f \,.\, g) = gr(f) + gr(g)$, em que usamos explicitamente a hipótese de A ser um domínio de integridade. Portanto, esta propriedade não é válida quando A não for um domínio de integridade. Veja a Atividade Final 2.

Exemplo 2

Sejam os polinômios $f(x) = \bar{1} + x$ e $g(x) = x$ em $\mathbf{Z}_2[x]$. Vamos calcular a soma e o produto destes polinômios e, também, seus graus.

Para o polinômio soma, temos

$$\begin{aligned} f(x) + g(x) &= (\bar{1} + x) + x \\ &= (\bar{1} + \bar{0}) + (\bar{1} + \bar{1})x \\ &= \bar{1} + \bar{2}x \\ &= \bar{1} + \bar{0}x; \text{ pois } \bar{2} = \bar{0} \text{ em } \mathbf{Z}_2 \\ &= \bar{1} \in \mathbf{Z}_2[x] \end{aligned}$$

Veja que $gr(f + g) = 0 < 1 = \max\{gr(f), gr(g)\}$.

Para o polinômio produto, temos

$$\begin{aligned} f(x) \,.\, g(x) &= (\bar{1} + x) \,.\, x \\ &= \bar{1} \,.\, x + x \,.\, x; \text{ aplicando a lei distributiva} \\ &= x + x^2 \in \mathbf{Z}_2[x] \end{aligned}$$

Observe que $gr(f \,.\, g) = 2 = 1 + 1 = gr(f) + gr(g)$. Com isso, concluímos o Exemplo 2.

ATIVIDADES FINAIS

1. Calcule a soma e o produto, e seus respectivos graus, dos polinômios $f(x) = 3x + 2x^2$ e $g(x) = 1 + x$, em $\mathbf{Z}[x]$.

2. Encontre um exemplo de um anel A e de polinômios $f(x), g(x) \in A[x]$, para os quais não vale a igualdade $gr(f \,.\, g) = gr(f) + gr(g)$. Observe que A não pode ser um domínio de integridade.

RESUMO

A soma e o produto dos polinômios

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_mx^m,$$

supondo $m \leq n$, são dados por

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_m + b_m)x^m + a_{m+1}x^{m+1} \ldots + a_nx^n$$
$$= c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_nx^n$$

e

$$f(x) \cdot g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_{m+n}x^{m+n},$$

onde os coeficientes c_K são definidos por

$$c_0 = a_0b_0;$$
$$c_1 = a_0b_1 + a_1b_0;$$
$$c_2 = a_0b_2 + a_1b_1 + a_2b_0;$$
$$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0;$$
$$\vdots$$
$$c_K = a_0b_K + a_1b_{K-1} + a_2b_{K-2} + \ldots + a_Kb_0, \text{ para todo } k \leq m + n.$$

Valem as propriedades $gr(f + g) \leq \max\{gr(f), gr(g)\}$ e $gr(f \cdot g) = gr(f) + gr(g)$, sendo que esta última apenas quando o anel A é um domínio de integridade.

RESPOSTAS COMENTADAS

Atividade 1

Para o polinômio soma, temos

$$\begin{aligned} f(x) + g(x) &= (\bar{2} + \bar{2}x^2 + x^3) + (\bar{1} + \bar{2}x) \\ &= (\bar{2} + \bar{1}) + (\bar{0} + \bar{2})x + (\bar{2} + \bar{0})x^2 + (\bar{1} + \bar{0})x^3 \\ &= \bar{3} + \bar{2}x + \bar{2}x^2 + x^3 \\ &= \bar{0} + \bar{2}x + \bar{2}x^2 + x^3; \text{ pois } \bar{3} = 0 \text{ em } Z_3 \\ &= \bar{2}x + \bar{2}x^2 + x^3 \in Z_3[x]. \end{aligned}$$

Calculando o polinômio produto, temos

$f(x) \cdot g(x) = (\overline{2} + \overline{2}x^2 + x^3) + (\overline{1} + \overline{2}x)$

$= (\overline{2} + \overline{2}x^2 + x^3) \cdot \overline{1} + (\overline{2} + \overline{2}x^2 + x^3) \cdot \overline{2}x$; aplicando a lei distributiva

$= (\overline{2} + \overline{2}x^2 + x^3) + (\overline{4}x + \overline{4}x^3 + \overline{2}x^4)$; aplicando a lei distributiva

$= (\overline{2} + \overline{0}) + (\overline{0} + \overline{4})x + (\overline{2} + \overline{0})x^2 + (\overline{1} + \overline{4})x^3 + (\overline{0} + \overline{2})x^4$; aplicando a soma de polinômios

$= \overline{2} + \overline{4}x + \overline{2}x^2 + \overline{5}x^3 + \overline{2}x^4$

$= \overline{2} + \overline{1}x + \overline{2}x^2 + \overline{2}x^3 + \overline{2}x^4$; pois $\overline{4} = \overline{1}$ e $\overline{5} = \overline{2}$ em Z_3

$= \overline{2} + x + \overline{2}x^2 + \overline{2}x^3 + \overline{2}x^4 \in Z_3[x]$.

Atividade Final 1

Para o polinômio soma, temos

$f(x) + g(x) = (3x + 2x^2) + (1 + x)$

$= (0 + 1) + (3 + 1)x + (2 + 0)x^2$

$= 1 + 4x + 2x^2 \in Z[x]$.

Veja que $gr(f + g) = 2 = \max\{gr(f), gr(g)\}$.

Calculando o polinômio produto, temos

$f(x) \cdot g(x) = (3x + 2x^2)(1 + x)$

$= (3x + 2x^2) \cdot 1 + (3x + 2x^2) \cdot x$; aplicando a lei distributiva

$= (3x + 2x^2) + (3x^2 + 2x^3)$; aplicando a lei distributiva

$= (3 + 0)x + (2 + 3)x^2 + (0 + 2)x^3$; aplicando a soma de polinômios

$= 3x + 5x^2 + 2x^3 \in Z[x]$.

Observe que $gr(f \cdot g) = 3 = 2 + 1 = gr(f) + gr(g)$.

Atividade Final 2

Sejam os polinômios $f(x) = \overline{1} + \overline{2}x$ e $g(x) = \overline{2}x$ em $Z_4[x]$. Calculando o polinômio produto, temos

$f(x) \cdot g(x) = (\overline{1} + \overline{2}x) \cdot \overline{2}x$

$= \overline{1} \cdot \overline{2}x + \overline{2}x \cdot \overline{2}x$; aplicando a lei distributiva

$= \overline{2}x + \overline{4}x^2$

$= \overline{2}x + \overline{0}x^2$; pois $\overline{4} = \overline{0}$ em Z_4

$= \overline{2}x \in Z_4[x]$.

Veja que $gr(f \,.\, g) = 1 < 2 = 1 + 1 = gr(f) + gr(g)$. Observe que Z_4 não é um domínio de integridade, pois contém divisores de zero $(\overline{2} \,.\, \overline{2} = \overline{0})$.

AULA 7

Anéis de polinômios

Meta da aula

Apresentar a estrutura de anel para o conjunto dos polinômios com coeficientes num anel A.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar a natureza de um anel de polinômios.
- Determinar as condições para que um anel de polinômios seja um domínio de integridade.
- Determinar que um anel de polinômios nunca é um corpo.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I, e dos conhecimentos sobre os polinômios das Aulas 5 e 6.

INTRODUÇÃO

Vimos nas aulas anteriores que se A é um anel, comutativo e com unidade ($1_A \in A$), então denotamos o conjunto dos polinômios sobre o anel A por $A[x]$, isto é,

$$A[x] = \{\text{polinômios na variável } x \text{ com coeficientes em } A\}$$
$$= \{a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \mid a_i \in A \text{ e } n \in \mathbf{N}\}.$$

Depois, definimos as operações de adição e multiplicação de polinômios e vimos como o grau de um polinômio se comporta perante estas operações.
Nesta aula, vamos provar que $A[x]$, munido destas operações, tem a estrutura de um anel. Vamos relembrar, da aula passada, as definições de soma e produto de polinômios.

DEFINIÇÃO 1

Sejam $f(x)$ e $g(x)$ dois polinômios em $A[x]$, digamos,

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_mx^m.$$

Podemos supor, sem perda de generalidade, que $m \leq n$. Definimos as operações de adição e multiplicação de polinômios como segue.

1. *Adição de polinômios*. O *polinômio soma* $f(x) + g(x)$ é definido por

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + a_2)x^2 + \ldots + (a_m + a_m)x^m + a_{m+1}x^{m+1} + \ldots + a_nx^n$$
$$= c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_nx^n,$$

onde os novos coeficientes são dados por $c_K = a_K + b_K$ para cada $k = 1, 2, \ldots, n$ e $b_K = 0$ para todo $k > m$.

Assim, para somarmos dois polinômios, simplesmente somamos os seus coeficientes correspondentes.

2. *Multiplicação de polinômios*. O *polinômio produto* $f(x)\,.\,g(x)$ é definido por

$$f(x)\,.\,g(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_{m+n}x^{m+n},$$

onde os coeficientes c_K são definidos por

$c_0 = a_0b_0$;

$c_1 = a_0b_1 + a_1b_0$;

$c_2 = a_0b_2 + a_1b_1 + a_2b_0$;

$c_3 = a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0$;

$\vdots$

$c_K = a_0b_K + a_1b_{K-1} + a_2b_{K-2} + \ldots + a_Kb_0 = \sum_{i=0}^{k} a_ib_{K-i}$ para todo $k \leq m + n$,

e onde estamos considerando que $b_K = 0$ para todo $k > m$, e $a_K = 0$ para todo $k > n$. Esta regra diz, simplesmente, que, para formarmos o produto $f(x)\,.\,g(x)$, fazemos o produto de cada termo de $f(x)$ por cada termos de $g(x)$, usando a regra

$$(a_ix^i)\,.\,(b_jx^i) = a_ib_jx^{i+j} \text{ para todo } i, j \geq 0,$$

e, depois, agrupamos todos os termos que têm a mesma potência em x. Observe que a formação dos coeficientes c_K segue, simplesmente, a aplicação da lei distributiva.

Vamos, agora, enunciar o resultado principal desta aula.

Teorema 1

Dado um anel A, o conjunto dos polinômios $A[x]$, munido das operações de adição e multiplicação de polinômios, é um anel.

Chamamos $A[x]$ um *anel de polinômios*. Nas aulas que seguem, estudaremos muitas propriedades desses anéis.

A demonstração deste teorema é longa e consiste em verificarmos, um a um, os axiomas de anel. Antes de prosseguir na leitura desta aula, não deixe de rever esses axiomas, que estão na Aula 3.

Demonstração

Primeiramente, vamos observar que a adição e a multiplicação de polinômios são operações binárias em $A[x]$, ou seja, dados os polinômios $f(x), g(x) \in A[x]$ temos que

$$f(x) + g(x) \in A[x] \quad \text{e} \quad f(x) \,.\, g(x) \in A[x].$$

De fato, sejam $f(x), g(x), h(x) \in A[x]$ dados por

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n,$$

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_mx^m$$

e $$h(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_1x^1.$$

Observe que

$$a_K = 0 \text{ para todo } k > n;$$
$$b_K = 0 \text{ para todo } k > m \quad \text{e}$$
$$c_K = 0 \text{ para todo } k > l.$$

Podemos supor, sem perda de generalidade, que $l \leq m \leq n$. Portanto, temos

$$a_K = 0,\ b_K = 0 \text{ e } c_K = 0 \quad \text{para todo } k > n,$$

e podemos escrever

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n,$$

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_nx^n$$

e $$h(x) = c_0 + c_1x + c_2x^2 + c_3x^3 + \ldots + c_nx^n \,.$$

Vamos, agora, demonstrar a validade de cada um dos oito axiomas de anel para $A[x]$. Observe atentamente que em cada uma destas demonstrações, usaremos a hipótese de A ser um anel.

1. A adição de polinômios é associativa. De fato,

$$[f(x) + g(x)] + h(x) = [(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_n + b_n)x^n] + (c_0 + c_1x + c_2x^2 + \ldots + c_nx^n)$$
$$= [(a_0 + b_0) + c_0] + [(a_1 + b_1) + c_1]\,x + [(a_2 + b_2) + c_2]x^2 + \ldots + [(a_n + b_n) + c_n]x^n$$
$$= [a_0 + (b_0 + c_0)] + [a_1\ \ (b_1 + c_1)]x + [a_2 + (b_2 + c_2)]x^2 + \ldots + [a_n + (b_n + c_n)]x^n$$
$$= (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) + [(b_0 + c_0) + (b_1 + c_1)x + (b_2 + c_2)x^2 + \ldots + (b_n + c_n)x^n]$$
$$= [f(x) + [g(x) + h(x)].$$

Você deve observar que uma condição para que as igualdades acima sejam verdadeiras é que a adição seja associativa em A. Isto é verdade, pois estamos supondo que A é um anel.

2. A adição de polinômios é comutativa, pois,

$$f(x) + g(x) = (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \ldots + b_nx^n)$$
$$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_n + b_n)x^n$$
$$= (b_0 + a_0) + (b_1 + a_1)x + (b_2 + a_2)x^2 + \ldots + (b_n + a_n)x^n$$
$$= g(x) + f(x).$$

Novamente, vemos que, nas igualdades anteriores, usamos o fato de a adição no anel A ser comutativa.

3. O elemento neutro da adição em $A[x]$ é o polinômio nulo que pode ser escrito como

$$N(x) = 0 + 0x + 0x^2 + 0x^3 + \ldots + 0x^n \in A[x].$$

Assim, temos

$$\begin{aligned} f(x) + N(x) &= (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) + (0 + 0x + 0x^2 + \ldots + 0x^n) \\ &= (a_0 + 0) + (a_1 + 0)x + (a_2 + 0)x^2 + \ldots + (a_n + 0)x^n \\ &= a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \\ &= f(x). \end{aligned}$$

Analogamente, temos $N(x) + f(x) = f(x)$, pois a adição de polinômios é comutativa no anel A.

Note que o elemento neutro da adição em $A[x]$ é o mesmo neutro aditivo em A.

4. O polinômio simétrico de $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ é o polinômio

$$-f(x) = -a_0 - a_1x - a_2x^2 - a_3x^3 - \ldots - a_nx^n,$$

pois,

$$\begin{aligned} f(x) + (-f(x)) &= (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) + (-a_0 - a_1x - a_2x^2 - \ldots - a_nx^n) \\ &= (a_0 - a_0) + (a_1 - a_1)x + (a_2 - a_2)x^2 + \ldots + (a_n - a_n)x^n \\ &= 0 + 0x + 0x^2 + \ldots + 0x^n \\ &= N(x). \end{aligned}$$

Analogamente, temos $(-f(x)) + f(x) = N(x)$, pois como já foi observado, a adição é comutativa em $A[x]$. Vemos que é fundamental a aplicação dos axiomas de anel para os coeficientes a_i, b_i e c_i.

A seguinte propriedade a ser demonstrada, a associatividade da multiplicação, possui uma prova um pouco mais delicada. Antes de demonstrá-la, você está convidado a realizar a primeira atividade desta aula. Nela se verificará como funciona, na prática, essa propriedade associativa na multiplicação.

ATIVIDADE

1. Sejam os seguintes polinômios em $\mathrm{IR}[x]$:

$$f(x) = 2x^2 + 1$$
$$g(x) = x^2 - x$$
$$h(x) = x + 4$$

Verifique se a propriedade associativa da multiplicação é válida no caso dos polinômios $f(x)$, $g(x)$ e $h(x)$, isto é,

$$[f(x) \,.\, g(x)] \,.\, h(x) = f(x) \,.\, [g(x) \,.\, h(x)].$$

Prosseguimos com a verificação da validade dos axiomas de anel para $A[x]$.

5. A multiplicação de polinômios é associativa. De fato,

$$\begin{aligned}
[f(x) \,.\, g(x)] \,.\, h(x) &= \left[\left(\sum_{k=0}^{n} a_k x^k\right).\left(\sum_{k=0}^{n} b_k x^k\right)\right].\left(\sum_{i=0}^{n} c_k x^k\right) \\
&= \left[\sum_{k=0}^{n}\left(\sum_{i=0}^{k} a_{k-i} b_i\right)x^k\right].\left(\sum_{k=0}^{n} c_k x^k\right) \\
&= \sum_{k=0}^{n}\left(\sum_{s=0}^{k}\left(\sum_{i=0}^{s} a_{s-i} b_i\right)c_{k-s}\right)x^k \\
&= \sum_{k=0}^{n}\left(\sum_{s=0}^{k}\left(\sum_{i=0}^{s} a_{s-i} b_i c_{k-s}\right)\right)x^k \\
&= \sum_{k=0}^{n}\left(\sum_{i=0}^{s}\left(\sum_{s=0}^{k} a_{s-i} b_i c_{k-s}\right)\right)x^k \\
&= \sum_{k=0}^{n}\left(\sum_{i=0}^{s} a_{s-i}\left(\sum_{s=0}^{k} b_i c_{k-s}\right)\right)x^k \\
&= \left(\sum_{k=0}^{n} a_k x^k\right).\left(\sum_{k=0}^{n}\left(\sum_{s=0}^{k} b_i c_{k-s}\right)x^k\right) \\
&= \left(\sum_{k=0}^{n} a_k x^k\right).\left[\left(\sum_{k=0}^{n} b_k x^k\right).\left(\sum_{i=0}^{n} c_k x^k\right)\right] \\
&= f(x).\big[g(x).h(x)\big].
\end{aligned}$$

Realizaremos mais uma atividade, para entendermos melhor a próxima propriedade a ser demonstrada.

ATIVIDADE

2. Considere os seguintes polinômios em IR[x]:

$$f(x) = \sqrt{2}x + 3$$

$$g(x) = 2x^2 - \sqrt{3}$$

Verifique se a propriedade comutativa da multiplicação é satisfeita neste caso particular, isto é,

$$f(x) \,.\, g(x) = g(x) \,.\, f(x).$$

Procedemos, agora, à demonstração da propriedade comutativa da multiplicação para qualquer par de polinômios com coeficientes no anel A.

6. A multiplicação de polinômios é comutativa. De fato,

$$\begin{aligned} f(x) \,.\, g(x) &= \left(\sum_{k=0}^{n} a_k x^k\right).\left(\sum_{k=0}^{n} b_k x^k\right) \\ &= \sum_{k=0}^{n} \left(\sum_{i=0}^{n} a_i b_{k-i}\right) x^k \\ &= \sum_{k=0}^{n} \left(\sum_{i=0}^{n} a_{k-i} b_i\right) x^k \\ &= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} b_i a_{k-i}\right) x^k \\ &= \left(\sum_{k=0}^{n} b_k x^k\right).\left(\sum_{k=0}^{n} a_k x^k\right) \\ &= g(x).f(x). \end{aligned}$$

7. O elemento neutro da multiplicação é o polinômio constante $e(x) = 1 \in A[x]$. Pois,

$$\begin{aligned} f(x) \,.\, e(x) &= \left(\sum_{k=0}^{n} a_k x^k\right).1 \\ &= \left(\sum_{k=0}^{n} a_k x^k\right) \\ &= f(x). \end{aligned}$$

Analogamente para $e(x) \,.\, f(x) = f(x)$, pois a multiplicação de polinômios é comutativa.

Novamente, observe que os elementos neutros da multiplicação em A e em $A[x]$ coincidem.

Para concluirmos que $A[x]$ é, de fato, um anel comutativo com unidade, resta verificar que a adição e a multiplicação de polinômios satisfazem a propriedade distributiva. Antes de demonstrarmos essa propriedade, convidamos você a desenvolver a seguinte atividade:

ATIVIDADE

3. Dados os seguintes polinômios com coeficientes reais:

$$f(x) = x^2 - 1$$

$$g(x) = 2x^2 - x$$

$$h(x) = x + 2,$$

mostre que a propriedade distributiva é válida para os polinômios dados acima, ou seja, mostre que

$$[f(x) + g(x)] \,.\, h(x) = f(x) \,.\, h(x) + g(x) \,.\, h(x)$$

Vamos verificar, agora, que essa propriedade é sempre satisfeita em qualquer polinômio.

8. A adição e a multiplicação de polinômios satisfazem a lei distributiva, pois,

$$\begin{aligned}
[f(x) + g(x)] \,.\, h(x) &= \left[\left(\sum_{k=0}^{n} a_k x^k\right) + \left(\sum_{k=0}^{n} b_k x^k\right)\right] . \left(\sum_{i=0}^{n} c_k x^k\right) \\
&= \left(\sum_{k=0}^{n} (a_k + b_k) x^k\right) . \left(\sum_{i=0}^{n} c_k x^k\right) \\
&= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} (a_i + b_i) c_{k-i}\right) x^k \\
&= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} (a_i c_{k-i} + b_i c_{k-i})\right) x^k \\
&= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} (a_i c_{k-i}) + \sum_{i=0}^{k} (b_i c_{k-i})\right) x^k \\
&= \sum_{k=0}^{n} \left(\sum_{i=0}^{k} (a_i c_{k-i})\right) x^k + \sum_{k=0}^{n} \left(\sum_{i=1}^{k} (b_i c_{k-i})\right) x^k \\
&= \left(\sum_{k=0}^{n} a_k x^k\right) . \left(\sum_{i=0}^{n} c_k x^k\right) + \left(\sum_{k=0}^{n} b_k x^k\right) . \left(\sum_{i=0}^{n} c_k x^k\right) \\
&= f(x) . h(x) + g(x) . h(x).
\end{aligned}$$

Convem observar que, tanto na Atividade 3 como na Propriedade 8, também é válida a igualdade:

$$h(x) \cdot [f(x) + g(x)] = h(x) \cdot f(x) + h(x) \cdot g(x),$$

pois a multiplicação de polinômios é comutativa.

Assim, as oito condições que caracterizam um anel são válidas. Podemos concluir, portanto, que se A é um anel (comutativo e com unidade), então $A[x]$, munido de suas operações de adição e multiplicação, também é um anel (comutativo e com unidade). E assim o teorema fica demonstrado.

Algumas observações se tornam pertinentes. Elas são conseqüências das observações que fizemos ao longo da prova do Teorema 1. Achamos que vale a pena serem destacadas aqui, por serem de grande importância.

1. Temos que $A \subset A[x]$, pois os elementos de A correspondem aos polinômios constantes de $A[x]$.

2. Se A não for comutativo, isto é, se a multiplicação em A não é comutativa, então $A[x]$ também não será comutativo.

3. Se A não tiver unidade, ou seja, o elemento neutro da multiplicação, então $A[x]$ também não terá unidade.

4. Se A for um domínio de integridade, então $A[x]$ também será um domínio de integridade. A demonstração desse fato será colocada como uma atividade para você.

ATIVIDADE

4. Prove que se *A* é um domínio de integridade, então $A[x]$ também é um domínio de integridade.

Vamos prosseguir com outras observações relevantes:

5. Se A for um corpo, então $A[x]$ é um domínio de integridade. De fato, se A é um corpo, então A é domínio de integridade e, pela observação anterior, $A[x]$ também será domínio de integridade.

6. Mesmo sendo A um corpo, $A[x]$ não é um corpo. A demonstração desse fato fará parte de sua Atividade Final.

ATIVIDADES FINAIS

1. Prove que o polinômio $f(x) = x$ não possui inverso multiplicativo.

2. Faça uso da atividade anterior para provar que se A é qualquer anel, então $A[x]$ não é um corpo.

RESUMO

Nesta aula, você viu que $A[x]$, munido das operações de adição e multiplicação de polinômios, é um anel (comutativo com unidade), denominado anel de polinômios com coeficientes no anel A (comutativo com unidade). Aprendeu também que $A[x]$ é um domínio de integridade, no caso de A ser um domínio de integridade. Finalmente, observou que $A[x]$ jamais será corpo, mesmo sendo A um corpo. Em particular IR[x] não é corpo, somente um domínio de integridade.

RESPOSTAS COMENTADAS

Atividade 1

Procedamos a fazer as multiplicações requeridas:

$$\begin{aligned}[f(x)g(x)]h(x) &= [(2x^2 + 1)(x^2 - x)](x + 4)\\ &= (2x^4 - 2x^3 + x^2 - x)(x - 4)\\ &= 2x^5 + 6x^4 - 7x^3 + 3x^2 - 4x.\end{aligned}$$

Por outro lado, temos

$$\begin{aligned}f(x)[g(x)h(x)] &= (2x^2 + 1)[(x^2 - x)(x + 4)]\\ &= (2x^2 + 1)(x^3 + 3x^2 - 4x)\\ &= 2x^5 + 6x^4 - 7x^3 + 3x^2 - 4x.\end{aligned}$$

Assim, observe que a igualdade $[f(x)g(x)]\ h(x) = f(x)[g(x)h(x)]$ é válida.

Atividade 2

De fato, temos que

$$\begin{aligned}f(x)g(x) &= (\sqrt{2}x + 3)(2x^2 - \sqrt{3})\\ &= 2\sqrt{2}x^3 + 3x^2 - \sqrt{6}x - 3\sqrt{3}.\end{aligned}$$

Por outro lado,

$$\begin{aligned}g(x)f(x) &= (2x^2 - \sqrt{3})(\sqrt{2}x + 3)\\ &= 2\sqrt{2}x^3 + 3x^2 - \sqrt{6}x - 3\sqrt{3}.\end{aligned}$$

Provando assim que a igualdade $f(x)g(x) = g(x)f(x)$ é válida.

Atividade 3

Temos que

$$[f(x) + g(x)] \,.\, h(x) = [(x^2 - 1)(2x^2 - 1)](x + 2)$$

$$= (3x^2 - 2)(x + 2)$$

$$= 3x^3 + 6x^2 - 2x - 4.$$

Por outro lado,

$$f(x)h(x) + g(x)h(x) = (x^2 - 1)(x + 2) + (2x^2 - 1)(x + 2)$$

$$= (x^3 + 2x^2 - x - 2) + (2x^3 + 4x^2 - x - 2)$$

$$= 3x^3 + 6x^2 - 2x - 4,$$

o que mostra que os polinômios $f(x)$, $g(x)$ e $h(x)$ satisfazem a propriedade distributiva.

Atividade 4

Vamos supor que *A* é um domínio de integridade, o que significa que dados *a*, *b* ∈ *A*, então

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

ou, equivalentemente,

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

Sejam, agora, $f(x)$ e $g(x)$ dois polinômios não-nulos em $A[x]$, digamos

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \text{, com } a_n \neq 0$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_mx^m \text{, com } b_m \neq 0.$$

O termo de mais alto grau do polinômio produto $f(x) \,.\, g(x)$ é dado por $a_nb_mx^{n+m}$. Como *A* é um domínio de integridade e $a_n \neq 0$ e $b_m \neq 0$, então $a_nb_m \neq 0$, o que garante que $f(x) \,.\, g(x)$ é um polinômio não-nulo. Assim, concluímos que o produto de dois polinômios não-nulos é um polinômio não-nulo. Portanto, provamos que $A[x]$ é um domínio de integridade.

Atividade Final 1

Vamos supor, por contradição, que exista um polinômio não-nulo $g(x)$ tal que

$$f(x) \,.\, g(x) = 1,$$

o que significa que $f(x) \,.\, g(x)$ é o polinômio constante $e(x) = 1$. Daí, temos que

$$gr(f \,.\, g) = gr(1) = 0,$$

e, portanto, como $gr(f \,.\, g) = 1 + gr(g)$, temos

$$1 + gr(g) = 0,$$

o que é impossível, já que $gr(g) \geq 0$. Assim, concluímos que não existe polinômio não-nulo $g(x)$ tal que

$$f(x) \,.\, g(x) = 1,$$

ou seja, o polinômio $f(x) = x$ não é invertível.

Atividade Final 2

Vimos, na Atividade Final anterior, que o polinômio $f(x) = x$ é não-nulo e não é invertível. Se o anel $A[x]$ fosse um corpo, seria necessário que $f(x) = x$, sendo não-nulo, fosse invertível. Portanto, o anel $A[x]$ não é um corpo.

AULA 8

Divisão de polinômios

Meta da aula

Apresentar o algoritmo de divisão de polinômios com coeficientes num corpo A.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar o algoritmo de divisão de polinômios.
- Executar cálculos de divisão de polinômios.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I, e dos conhecimentos sobre os polinômios das Aulas 5 a 7.

INTRODUÇÃO

Nas aulas anteriores, estudamos as operações de adição e multiplicação de polinômios com coeficientes num anel A. Vimos que o conjunto dos polinômios com coeficientes num anel A, denotado por $A[x]$, munido das operações anteriores, é também um anel.

Nesta aula, vamos tratar o problema da divisão de um polinômio por outro polinômio. Veremos que esta divisão nos dá informação sobre as raízes de um polinômio.

Vamos iniciar revendo, do seu curso de Ensino Médio, o algoritmo da divisão de polinômios. Depois, vamos enunciar e provar a propriedade da divisão de polinômios.

Exemplo 1

Vamos fazer a divisão do polinômio $f(x) = x^5 + 2x^3 + x + 1$ pelo polinômio $g(x) = 2x^3 + 2$. Podemos realizar uma analogia com o algoritmo da divisão dos números inteiros. Iniciamos montando o esquema da divisão:

$$\begin{array}{l|l} x^5 + 2x^3 + x + 1 & 2x^3 + 2 \\ \hline & \\ & \end{array}$$

O primeiro passo consiste em multiplicar o polinômio $2x^3 + 2$ pelo polinômio $\frac{1}{2}x^2$, obtendo o polinômio $x^5 + x^2$, de modo a igualar o grau e o coeficiente líder de $x^5 + 2x^3 + x + 1$:

$$\begin{array}{l|l} x^5 + 2x^3 + x + 1 & 2x^3 + 2 \\ \cline{2-2} x^5 + x^2 & \\ & \frac{1}{2}x^2 \end{array}$$

O segundo passo consiste em subtrair o polinômio $x^5 + x^2$ do polinômio $x^5 + 2x^3 + x + 1$, obtendo o polinômio $2x^3 - x^2 + x + 1$:

$$\begin{array}{l|l} x^5 + 2x^3 + x + 1 & 2x^3 + 2 \\ \cline{2-2} x^5 + x^2 & \\ \cline{1-1} 2x^3 - x^2 + x + 1 & \frac{1}{2}x^2 \end{array}$$

O terceiro passo consiste em multiplicar o polinômio $2x^3 + 2$ pelo polinômio constante 1, obtendo o mesmo polinômio $2x^3 + 2$, de modo a igualar o grau e o coeficiente líder de $2x^3 - x^2 + x + 1$:

$$\begin{array}{l|l} x^5 + 2x^3 + x + 1 & 2x^3 + 2 \\ \hline x^5 + x^2 & \\ \hline 2x^3 - x^2 + x + 1 & \frac{1}{2}x^2 + 1 \\ 2x^3 + 2 & \\ \hline & \end{array}$$

O quarto passo consiste em subtrair o polinômio $2x^3 + 2$ do polinômio $2x^3 - x^2 + x + 1$, obtendo o polinômio $-x^2 + x - 1$:

$$\begin{array}{l|l} x^5 + 2x^3 + x + 1 & 2x^3 + 2 \\ \hline x^5 + x^2 & \\ \hline 2x^3 - x^2 + x + 1 & \frac{1}{2}x^2 + 1 \\ 2x^3 + 2 & \\ \hline -x^2 + x - 1 & \end{array}$$

O quinto passo consiste em verificar que o grau do último polinômio obtido, $-x^2 + x - 1$, é menor que o grau do polinômio divisor $2x^3 + 2$. Sendo assim, encerramos o processo de divisão, obtendo o polinômio quociente $q(x) = \frac{1}{2}x^2 + 1$ e o polinômio resto $r(x) = -x^2 + x - 1$, que resumimos pela equação:

$$x^5 + 2x^3 + x + 1 = \left(\frac{1}{2}x^2 + 1\right).\left(2x^3 + 2\right) + \left(-x^2 + x - 1\right),$$

ou, ainda,

$$f(x) = q(x)g(x) + r(x) \text{ com } gr(r(x)) < gr(g(x)).$$

Observe que os dois polinômios iniciais, $f(x) = x^5 + 2x^3 + x + 1$ e $g(x) = 2x^3 + 2$, pertencem a $\mathbf{Z}[x]$, mas não é verdade que os dois polinômios obtidos pelo processo, $q(x) = \frac{1}{2}x^2 + 1$ e $r(x) = -x^2 + x - 1$, pertencem a $\mathbf{Z}[x]$, já que $\frac{1}{2}x^2 + 1 \notin \mathbf{Z}[x]$. Isso acontece porque o conjunto $\mathbf{Z}$ dos números inteiros não é um corpo. Agora, considerando esses mesmos dois polinômios em outro contexto: $f(x) = x^5 + 2x^3 + x + 1$ e $g(x) = 2x^3 + 2$ pertencendo a $\mathbf{Q}[x]$, então é verdade que os dois

polinômios obtidos, $q(x) = \frac{1}{2}x^2 + 1$ e $r(x) = -x^2 + x - 1$, pertencem a $\boldsymbol{Q}[x]$. Isto acontece porque $\boldsymbol{Q}$ é um corpo.

Por isso, ao considerar a divisão de polinômios em $\boldsymbol{A}[x]$, consideraremos que $\boldsymbol{A}$ seja um corpo. O processo de divisão descrito no Exemplo 1 é chamado de *algoritmo da divisão*.

Pratique, agora, o algoritmo da divisão de polinômios nesta atividade.

ATIVIDADE

1. Dados os polinômios $f(x) = 6x^6 + 7x^5 + 8x^4 + 1$ e $g(x) = x^4 + x + 1$ em $\boldsymbol{R}[x]$, obtenha os polinômios quociente e resto da divisão de $f(x)$ por $g(x)$.

Podemos, agora, enunciar o resultado geral sobre divisão de polinômio.

_____

_____

_____

_____

TEOREMA 1 (ALGORITMO DA DIVISÃO DE POLINÔMIOS)

Sejam $\boldsymbol{A}$ um corpo e $f(x), g(x) \in \boldsymbol{A}[x]$ dois polinômios com g(x) não-nulo, então existem polinômios $q(x), r(x) \in \boldsymbol{A}[x]$ tais que

$$f(x) = q(x)\, g(x) + r(x) \text{ com } gr(r(x)) < gr(r(x)) \text{ ou } r(x) = 0.$$

Antes de iniciarmos a demonstração, vejamos algumas observações:

1. Veja a semelhança deste resultado com o algoritmo da divisão em $\boldsymbol{Z}$: dados $a, b \in \boldsymbol{Z}$, com b > 0, então existem $q, r \in \boldsymbol{Z}$ tais que

$$a = qb + r \text{ com } 0 \leq r < b.$$

Lembre-se da terminologia usada: a é o *dividendo*, b é o *divisor*, q é o *quociente* e r é o *resto*. Lembre-se, também, de que a equação $a = qb + r$ é representada pelo esquema da divisão

$$\begin{array}{l|l} a & b \\ \hline r & q \end{array}$$

2. Analogamente, na propriedade da divisão para polinômios, o polinômio $f(x)$ é chamado de *dividendo*, $g(x)$ é o *divisor*, $q(x)$ é o *quociente* e $r(x)$ é polinômio *resto*. Também representamos a equação $f(x) = q(x)g(x) + r(x)$ de forma esquemática:

$$\begin{array}{l|l} f(x) & g(x) \\ \hline r(x) & q(x) \end{array}$$

3. Se o resto for o polinômio nulo, $r(x) = 0$, temos

$$f(x) = q(x)g(x),$$

e dizemos que o polinômio $g(x)$ *divide* o polinômio $f(x)$ em $A[x]$, e denotamos isso por $g(x) \mid f(x)$. Nesse caso, também dizemos que $g(x)$ é um *divisor* de $f(x)$, ou que $g(x)$ é um *fator* de $f(x)$, ou, ainda, que $f(x)$ é um *múltiplo* de $g(x)$ em $\boldsymbol{A}[x]$.

4. A forma de provarmos a existência dos polinômios $q(x)$ e $r(x)$ será construindo um algoritmo para calculá-los. Este algoritmo, que é simplesmente uma generalização do processo aplicado no Exemplo 1, será recursivo, o que significa que seu passo principal será aplicado repetidas vezes. O algoritmo fará esta repetição, obtendo uma seqüência de polinômios restos $r(x)$, até que o grau de $r(x)$ seja menor que o grau do polinômio divisor $g(x)$ ou até que $r(x) = 0$.

Demonstração

Lembre-se de que queremos encontrar polinômios $q(x)$ e $r(x)$, em $\boldsymbol{A}[x]$, que satisfaçam

$$f(x) = q(x)g(x) + r(x) \text{ com } gr(r(x)) < gr(g(x)) \text{ ou } r(x) = 0.$$

Vamos dividir nossa argumentação em três casos.

1º caso: $f(x)$ é o polinômio nulo, isto é, $f(x) = 0$.

Neste caso, escolhemos $q(x) = r(x) = 0$ e, assim, obtemos

$$\begin{aligned} f(x) &= 0 \\ &= 0 \cdot g(x) + 0 \\ &= q(x)g(x) + r(x), \end{aligned}$$

ou seja, temos

$$f(x) = q(x)g(x) + r(x) \text{ com } r(x) = 0,$$

garantindo a condição da divisão.

2º caso: $f(x)$ é um polinômio não-nulo com $gr(f(x)) < gr(g(x))$.

Agora, escolhendo $q(x) = 0$ e $r(x) = f(x)$, temos

$$\begin{aligned} f(x) &= 0 + f(x) \\ &= 0 \cdot g(x) + f(x) \\ &= q(x)g(x) + r(x) \end{aligned}$$

com

$$gr(r(x)) = gr(f(x)) < gr(g(x)).$$

Portanto, temos

$$f(x) = q(x)g(x) + r(x) \text{ com } gr(r(x)) < gr(g(x)),$$

garantindo, outra vez, a condição da divisão.

3º caso: $f(x)$ é um polinômio não-nulo com $gr(f(x)) \geq gr(g(x))$.

Neste caso, vamos construir uma seqüência de restos, $r_1(x)$, $r_2(x)$, ... , $r_k(x)$, que satisfaçam

$$gr(f(x)) > gr(r_1(x)) > gr(r_2(x)) > \ldots > gr(r_{k-1}(x)) > gr(r_k(x))$$

com

$$gr(r_k(x)) < gr(g(x)) \text{ ou } r_k(x) = 0.$$

Para isso, sejam

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$$

e

$$g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + \ldots + b_mx^m,$$

com $a_n \neq 0$, $b_m \neq 0$ e $m \leq n$ (que é a condição $gr(f(x)) \geq gr(g(x))$.
Para obter o primeiro resto $r_1(x)$, definimos

$$r_1(x) = f(x) - \frac{a_n}{b_m}\, x^{n-m}\, g(x).$$

Como $\boldsymbol{A}$ é corpo, então $\frac{a_n}{b_m} \in \boldsymbol{A}$, o que garante que

$$r_1(x) = f(x) - \frac{a_n}{b_m}\, x^{n-m}\, g(x) \in \boldsymbol{A}[x].$$

Lembre-se de que o quociente $\frac{a_n}{b_m}$ significa o produto $a_n \,.\, b_m^{-1}$, isto é, $\frac{a_n}{b_m} = a_n \,.\, b_m^{-1}$.

Controlando apenas os últimos coeficientes de $f(x)$ e $g(x)$, temos que

$$\begin{aligned}
r_1(x) &= f(x) - \frac{a_n}{b_m}\, x^{n-m}\, g(x) \\
&= \left(\ldots + a_{n-1}x^{n-1} + a_nx^n\right) - \frac{a_n}{b_m}\, x^{n-m}\left(\ldots + b_{m-1}x^{m-1} + b_mx^m\right) \\
&= \left(\ldots + a_{n-1}x^{n-1} + a_nx^n\right) - \left(\ldots + \frac{a_nb_{m-1}}{b_m}x^{n-m}x^{m-1} + \frac{a_nb_m}{b_m}x^{n-m}x^m\right) \\
&= \left(\ldots + a_{n-1}x^{n-1} + a_nx^n\right) - \left(\ldots + \frac{a_nb_{m-1}}{b_m}x^{n-1} + a_nx^n\right) \\
&= \ldots + \left(a_{n-1} - \frac{a_nb_{m-1}}{b_m}\right)x^{n-1} + \left(a_n - a_n\right)x^n \\
&= \ldots + \left(a_{n-1} - \frac{a_nb_{m-1}}{b_m}\right)x^{n-1} + 0\,.\,x^n \\
&= \ldots + \left(a_{n-1} - \frac{a_nb_{m-1}}{b_m}\right)x^{n-1},
\end{aligned}$$

o que mostra que $r_1(x) = 0$, o polinômio nulo, ou

$$gr(r_1(x)) \leq n - 1 < n = gr(f(x)).$$

Observe que o efeito da multiplicação $\frac{a_n}{b_m} x^{n-m} . g(x)$ foi de eliminar o termo de mais alto grau de $f(x)$ na diferença

$$r_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x).$$

Portanto, escolhendo o polinômio quociente

$$q_1(x) = \frac{a_n}{b_m} x^{n-m},$$

temos

$$f(x) = \frac{a_n}{b_m} x^{n-m} g(x) + r_1(x)$$

$$= q_1(x)g(x) + r_1(x),$$

com

$$gr(r_1(x)) < gr(f(x)) \text{ ou } r_1(x) = 0.$$

Vamos resumir este *passo principal*: se $g(x)$ é um polinômio não-nulo e $f(x)$ é um polinômio com $gr(f(x)) \geq gr(f(x))$, ambos em $\boldsymbol{A}[x]$, então existem polinômios $q_1(x)$ e $r_1(x)$, também em $\boldsymbol{A}[x]$, tais que

$$f(x) = q_1(x)g(x) + r_1(x) \text{ com } gr(r_1(x)) < gr(f(x)) \text{ ou } r_1(x) = 0.$$

Caso tenhamos $gr(r_1(x)) < gr(g(x))$ ou $r_1(x) = 0$, então a condição da divisão está satisfeita e interrompemos o processo.

Caso contrário, teremos $r_1(x) \neq 0$ e $gr(r_1(x)) \geq gr(g(x))$. Assim, aplicaremos o passo principal aos polinômios $g(x)$ e $r_1(x)$, obtendo novos polinômios $q_2(x)$ e $r_2(x)$, ambos em $A[x]$, tais que

$$r_1(x) = q_2(x)g(x) + r_2(x) \text{ com } gr(r_2(x)) < gr(r_1(x)) \text{ ou } r_2(x) = 0.$$

Caso tenhamos, agora, $gr(r_2(x)) < gr(g(x))$ ou $r_2(x) = 0$, então interrompemos o processo e observamos que

$$\begin{aligned} f(x) &= q_1(x)g(x) + r_1(x) \\ &= q_1(x)g(x) + (q_2(x)g(x) + r_2(x)) \\ &= (q_1(x) + q_2(x))g(x) + r_2(x) \\ &= q(x)g(x) + r_2(x), \end{aligned}$$

onde o polinômio quociente é

$$q(x) = q_1(x) + q_2(x),$$

satisfazendo, portanto, a condição da divisão.

Caso contrário, teremos $r_2(x) \neq 0$ e $gr(r_2(x)) \geq gr(g(x))$. Então, aplicaremos outra vez o passo principal aos polinômios $g(x)$ e $r_2(x)$, obtendo novos polinômios $q_3(x)$ e $r_3(x)$, ambos em $\boldsymbol{A}[x]$, tais que

$$r_2(x) = q_3(x)g(x) + r_3(x) \text{ com } gr(r_3(x)) < gr(r_2(x)) \text{ ou } r_3(x) = 0.$$

Caso tenhamos, agora, $gr(r_3(x)) < gr(g(x))$ ou $r_3(x) = 0$, então interrompemos o processo e observamos que

$$\begin{aligned} f(x) &= (q_1(x) + q_2(x))g(x) + r_2(x) \\ &= (q_1(x) + q_2(x))\mathrm{g}(x) + (q_3(x)g(x) + r_3(x)) \\ &= (q_1(x) + q_2(x) + q_3(x))g(x) + r_3(x) \\ &= q(x)g(x) + r_3(x), \end{aligned}$$

onde o polinômio quociente é

$$q(x) = q_1(x) + q_2(x) + q_3(x),$$

satisfazendo, portanto, a condição da divisão.

Caso contrário, continuaremos aplicando o passo principal, obtendo uma seqüência de restos, $r_1(x)$, $r_2(x)$, ... , $r_k(x)$, todos em $A[x]$, com graus estritamente decrescentes,

$$gr(k_{k-1}(x)) < gr(r_{k-2}(x)) < ... < gr(r_1(x)) < gr(f(x)),$$

o que garante, para certo valor de k, que

$$gr(r_k(x)) < gr(g(x)) \text{ ou } r_k(x) = 0.$$

Neste momento, interrompemos o processo e observamos que

$$\begin{aligned} f(x) &= (q_1(x) + q_2(x) + q_3(x))g(x) + r_3(x) \\ &= ... \\ &= (q_1(x) + q_2(x) + ... + q_k(x))g(x) + r_k(x) \\ &= q(x)g(x) + r_k(x), \end{aligned}$$

onde o polinômio quociente é soma

$$q(x) = q_1(x) + q_2(x) + ... + q_k(x) \in A[x],$$

dos polinômios $q_1(x)$, $q_2(x)$, ... , $q_k(x)$, obtidos em cada aplicação do passo principal. Assim, finalmente, fica satisfeita a condição da divisão. Observe que o polinômio resto é dado por $r_k(x)$.

ATIVIDADES FINAIS

1. A divisão de um polinômio $f(x)$ por $x^2 - x$ resulta no quociente $6x^2 + 5x + 3$ e resto $-7x$. Calcule o resto da divisão de $f(x)$ por $2x^2 + 1$.

2. Dividindo-se o polinômio $f(x) = x^5 + ax^4 + bx^2 + cx + 1 \in \boldsymbol{R}[\mathrm{x}]$ por $x - 1$, obtém-se resto igual a 2. Dividindo-se $f(x)$ por $x + 1$, obtém-se resto igual a 3. Sabendo que $f(x)$ é divisível por $x - 2$, determine o polinômio $f(x)$.

RESUMO

Nesta aula, você estudou a propriedade da divisão de polinômios, que afirma que dados $f(x)$, $g(x) \in A[x]$ com $g(x)$ não-nulo. Então existem polinômios $q(x)$, $r(x) \in A[x]$ tais que

$$f(x) = q(x)g(x) + r(x) \text{ com } gr(r(x)) < gr(r(x)) < gr(g(x)) \text{ ou } r(x) = 0.$$

RESPOSTAS COMENTADAS

Atividade 1

Aplicando o algoritmo da divisão, temos

$$\begin{array}{r|l}
6x^6 + 7x^5 + 8x^4 + 1 & x^4 + x + 1 \\
\cline{2-2}
6x^6 + 6x^3 + 6x^2 & 6x^2 + 7x + 8 \\
\cline{1-1}
7x^5 + 8x^4 - 6x^3 - 6x^2 + 1 & \\
7x^5 + 7x^2 - 7x & \\
\cline{1-1}
8x^4 - 6x^3 - 13x^2 - 7x + 1 & \\
8x^4 + 8x + 8 & \\
\cline{1-1}
-6x^3 - 13x^2 - 15x - 7 &
\end{array}$$

Como

$$gr(-6x^3 - 13x^2 - 15x - 7) = 3 < 4 = gr(x^4 + x + 1),$$

então o polinômio quociente é

$$q(x) = 6x^2 + 7x + 8$$

e o polinômio resto é

$$r(x) = -6x^3 - 13x^2 - 15x - 7.$$

De outra forma, temos

$$\begin{aligned} f(x) &= 6x^6 + 7x^5 + 8x^4 + 1 \\ &= q(x)g(x) + r(x) \\ &= (6x^2 + 7x + 8)(x^4 + x + 1) + (-6x^3 - 13x^2 - 15x - 7). \end{aligned}$$

Atividade Final 1

Temos que

$$\begin{aligned} f(x) &= (6x^2 + 5x + 3)(x^2 - x) - 7x \\ &= 6x^4 - x^3 - 2x^2 - 10x. \end{aligned}$$

Fazendo a divisão de $f(x)$ por $2x^2 + 1$, obtemos

$$\begin{array}{l|l} 6x^4 - x^3 - 2x^2 - 10x & 2x^2 + 1 \\ \hline 6x^4 + 3x^2 & 3x^2 - \frac{1}{2}x - \frac{5}{2} \\ \hline -x^3 - 5x^2 - 10x & \\ -x^3 - \frac{1}{2}x & \\ \hline -5x^2 - \frac{19}{2}x & \\ -5x^2 - \frac{5}{2}x & \\ \hline -\frac{19}{2}x + \frac{5}{2} & \end{array}$$

e, portanto, o resto da divisão de $f(x)$ por $2x^2 + 1$ é o polinômio linear $-\frac{19}{2}x + \frac{5}{2}$.

Atividade Final 2

Dividindo $f(x)$ por $x - 1$, temos

$$f(x) = q_1(x)(x - 1) + 2.$$

Daí, segue que $f(1) = q_1(1)(1 - 1) + 2 = 2$. Substituindo $f(1) = 2$ em $f(x) = x^5 + ax^4 + bx^2 + cx + 1$, obtemos

$$1^5 + a.\ 1^4 + b\ .\ 1^2 + c\ .\ 1 + 1 = 2$$

$$a + b + c = 0.$$

Dividindo $f(x)$ por $x + 1$, temos

$$f(x) = q_2(x)(x + 1) + 3.$$

Assim, temos que $f(-1) = q_2(-1)((-1) + 1) + 3 = 3$. Substituindo $f(-1) = 3$ em $f(x) = x^5 + ax^4 + bx^2 + cx + 1$, obtemos

$$(-1)^5 + a.\ (-1)^4 + b.(-1)^2 + c.\ (-1) + 1 = 3$$

$$a + b - c = 3.$$

Como $f(x)$ é divisível por $x - 2$, então $f(x) = q_3(x)(x - 2)$, o que nos dá $f(2) = 0$. Substituindo $f(2) = 0$ em $f(x) = x^5 + ax^4 + bx^2 + cx + 1$, obteremos

$$2^5 + a.2^4 + b.2^2 + c.2 + 1 = 0$$

$$16a + 4b + 2c = -33.$$

Resolvendo o sistema

$$\begin{cases} a + b + c = 0 \\ a + b - c = 3 \\ 16a + 4a + 2c = -33 \end{cases}$$

cuja solução é $a = -3$, $b = \frac{9}{2}$ e $b = -\frac{3}{2}$. Portanto, o polinômio $f(x)$ é dado por

$$f(x) = x^5 - 3x^4 + \frac{9}{2}x^2 - \frac{3}{2}x + 1.$$

Propriedades da divisão de polinômios

AULA 9

Meta da aula

Apresentar propriedades da divisão de polinômios.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as propriedades fundamentais da divisão de polinômios.
- Identificar o algoritmo de divisão de polinômios para polinômios lineares.
- Executar cálculos de divisão de polinômios por polinômios lineares.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I, e dos conhecimentos sobre os polinômios das Aulas 5 a 8.

INTRODUÇÃO

Na aula anterior, estudamos o algoritmo da divisão de um polinômio com coeficientes de um corpo A. Nesta aula, vamos obter algumas conseqüências deste importante teorema. Vamos, portanto, rever seu enunciado e alguns conceitos importantes.

TEOREMA 1 (ALGORITMO DA DIVISÃO DE POLINÔMIOS)

Sejam A um corpo e $f(x), g(x) \in \boldsymbol{A}[x]$ dois polinômios com $g(x)$ não-nulo. Então existem polinômios $q(x), r(x) \in \boldsymbol{A}[x]$ tais que

$$f(x) = q(x)g(x) + r(x) \text{ com } gr(r(x)) < gr(g(x)) \text{ ou } r(x) = 0.$$

Observações

1. Na propriedade da divisão para polinômios, o polinômio $f(x)$ é chamado de *dividendo*, $g(x)$ é o *divisor*, $q(x)$ é o quociente e $r(x)$ é polinômio *resto*. Também representamos a equação $f(x) = q(x)g(x) + r(x)$ de forma esquemática:

$$\begin{array}{l|l} f(x) & g(x) \\ \hline r(x) & q(x) \end{array}$$

2. Se o resto for o polinômio nulo, $r(x) = 0$, temos

$$f(x) = q(x)g(x),$$

e dizemos que o polinômio $g(x)$ *divide* o polinômio $f(x)$ em $\boldsymbol{A}$[x], e denotamos isso por $g(x) \mid f(x)$.

Podemos generalizar esta última observação na seguinte definição.

DEFINIÇÃO 1

Sejam A um anel e $f(x), g(x) \in \boldsymbol{A}[x]$ dois polinômios com $g(x)$ não-nulo. Dizemos que o polinômio $g(x)$ *divide* o polinômio $f(x)$ em $\boldsymbol{A}[x]$, caso haja um polinômio $q(x) \in \boldsymbol{A}[x]$ tal que

$$f(x) = q(x)g(x),$$

e denotamos isso por $g(x) \mid f(x)$. Nesse caso, também dizemos que $g(x)$ é um *divisor* de $f(x)$, ou que $g(x)$ é um fator de $f(x)$, ou, ainda, que $f(x)$ é um *múltiplo* de $g(x)$ em $\boldsymbol{A}[x]$.

Quando $f(x)$ se expressa como um produto de polinômios,

$$f(x) = p_1(x)p_2(x) \ldots p_n(x),$$

dizemos que o produto $p_1(x)p_2(x) \ldots p_n(x)$ é uma fatoração de $f(x)$ e, portanto, cada polinômio $p_k(x)$ é um fator de $f(x)$.

Exemplo 1

Veja que, em $\boldsymbol{Z}[x]$, o polinômio $g(x) = x^2 + 1$ divide o polinômio $f(x) = x^4 - x^3 + 2x^2 - x + 1$, pois

$$x^4 - x^3 + 2x^2 - x + 1 = (x^2 - x + 1)(x^2 + 1).$$

ATIVIDADES

1. Aplique o algoritmo da divisão de polinômios e verifique que o polinômio $f(x) = x^4 - x^3 + 2x^2 - x + 1$ é divisível por $g(x) = x^2 + 1$ em $\boldsymbol{R}[x]$.

2. Verifique que o polinômio $g(x) = x^2 + x + \overline{1}$ + divide $f(x) = x^4 - x^2 + \overline{1}$ em $\boldsymbol{Z}_2[x]$.

PROPOSIÇÃO 1 (PROPRIEDADES DA DIVISÃO DE POLINÔMIOS)

Sejam A um anel e polinômios $f(x)$, $g(x)$, $h(x) \in A[x]$.

1. Se $h(x) \mid f(x)$ e $h(x) \mid g(x)$, então $h(x) \mid (f(x) + g(x))$ e $h(x) \mid (f(x) - g(x))$.

2. Se $h(x) \mid f(x)$, então $h(x) \mid f(x)g(x)$.

3. $h(x) \mid f(x)$, $h(x) \mid g(x)$ e $p(x)$, $q(x) \in A[x]$, então $h(x) \mid (p(x)f(x) + q(x)g(x))$.

4. Se $h(x) \mid f(x)$ e $f(x) \mid g(x)$, então $h(x) \mid g(x)$.

Demonstração

Durante a demonstração, usaremos somente as definições anteriores. É muito importante que você reconheça as propriedades aplicadas em cada passo.

1. Como $h(x) \mid f(x)$ então existe $q(x) \in A[x]$ tal que $f(x) = q(x)h(x)$. Analogamente, como $f(x) \mid g(x)$ existe $p(x) \in A[x]$ tal que $g(x) = p(x)h(x)$. Assim,

$$\begin{aligned} f(x) + g(x) &= q(x)h(x) + p(x)h(x) \\ &= (q(x) + p(x))h(x). \end{aligned}$$

Como $q(x) + p(x) \in A[x]$, temos que $h(x)$ divide $f(x) + g(x)$, ou seja, $h(x) \mid (f(x) + g(x))$. Analogamente, temos

$$\begin{aligned} f(x) - g(x) &= q(x)h(x) - p(x)h(x) \\ &= (q(x) - p(x))h(x). \end{aligned}$$

Assim, $f(x) - g(x)$ é múltiplo de $h(x)$, ou seja, $h(x) \mid (f(x) - g(x))$.

2. Novamente, como $h(x) \mid f(x)$, existe $q(x) \in A[x]$ tal que $f(x) = q(x)h(x)$. Multiplicando por $g(x)$ ambos os lados desta última igualdade, temos

$$\begin{aligned} f(x)g(x) &= (q(x)h(x))g(x) \\ &= (q(x)g(x))h(x). \end{aligned}$$

Como $q(x)g(x) \in \boldsymbol{A}[x]$, temos que $f(x)g(x)$ é múltiplo de $h(x)$, ou seja, $h(x) \mid f(x)g(x)$.

3. Pela Proposição 1.2, se $h(x) \mid f(x)$, então $h(x) \mid p(x)f(x)$, e se $h(x) \mid g(x)$, então $h(x) \mid q(x)g(x)$. Agora, pela Proposição 1.1, concluímos que $h(x) \mid (p(x)f(x) + q(x)g(x))$.

4. Como $h(x) \mid f(x)$, existe $q(x) \in \boldsymbol{A}[x]$ tal que $f(x) = q(x)h(x)$. Analogamente, como $f(x) \mid g(x)$, existe $p(x) \in \boldsymbol{A}[x]$ tal que $g(x) = p(x)f(x)$. Assim,

$$\begin{aligned} g(x) &= p(x)f(x) \\ &= (q(x)h(x))f(x). \\ &= (q(x)f(x))h(x). \end{aligned}$$

E, daí, concluímos que $h(x)$ divide $g(x)$, ou seja, $h(x) \mid g(x)$.

Vamos rever também o conceito de raiz ou zero de um polinômio.

Você lembra o que significa um escalar α ser raiz de um polinômio $f(x)$? Na aula passada, introduzimos este conceito e vamos revê-lo agora.

DEFINIÇÃO 2

Sejam A um anel e um polinômio $f(x) \in \boldsymbol{A}[x]$. Dizemos que $\alpha \in \boldsymbol{A}$ é uma *raiz* ou um *zero* de $f(x)$ em $\boldsymbol{A}$ se $f(\alpha) = 0$.

Vejamos, a seguir, alguns exemplos.

Exemplo 2

Seja $f(x) = x^4 - x^3 - x + 1 \in \boldsymbol{Z}[x]$, temos que $\alpha = 1$ é uma raiz de $f(x)$ em $\boldsymbol{Z}$, pois

$$f(1) = 1^4 - 1^3 - 1 + 1 = 0.$$

Analogamente, $\alpha = \overline{1} \in \boldsymbol{Z}_5$ é raiz de $f(x) = x^3 + \overline{2}x^2 + \overline{2} \in \boldsymbol{Z}_5[x]$, pois

$$f(\overline{1}) = (\overline{1})^3 + \overline{2}(\overline{1})^2 + \overline{2} = \overline{5} = \overline{0},$$

observando que as operações são realizadas em $\boldsymbol{Z}_5$.

Verifique, agora, na sua próxima atividade, o que curiosamente ocorre.

ATIVIDADE

3. Com respeito ao Exemplo 2, aplique o algoritmo da divisão de polinômios e verifique que o polinômio linear $p(x) = x - 1$ divide o polinômio $f(x) = x^4 - x^3 - x + 1$.

Esse comportamento de o polinômio linear $x - \alpha$ dividir um polinômio $f(x)$ sempre que α for uma raiz de $f(x)$, e, reciprocamente, é uma importante propriedade dos polinômios. Além disso, é também conseqüência da propriedade da divisão de polinômios.

PROPOSIÇÃO 2

Sejam $\boldsymbol{A}$ um corpo, $f(x) \in \boldsymbol{A}[x]$ um polinômio e $\alpha \in \boldsymbol{A}$ um escalar. Então, existe um polinômio $q(x) \in \boldsymbol{A}[x]$ tal que

$$f(x) = (x - \alpha)q(x) + f(\alpha).$$

Demonstração

Aplicando o algoritmo da divisão aos polinômios $f(x)$ e $g(x) = x - \alpha$, temos que existem polinômios $q(x), r(x) \in \boldsymbol{A}[x]$ tais que

$$f(x) = q(x)(x - \alpha) + r(x) \text{ com } gr(r(x)) < gr(x - \alpha) \text{ ou } r(x) = 0.$$

Como $gr(r(x)) < gr(x - \alpha) = 1$, segue que $gr(r(x)) = 0$, ou seja, $r(x)$ é um polinômio constante, digamos, $r(x) = a \in \boldsymbol{A}$. Temos, assim, a seguinte igualdade polinomial

$$f(x) = q(x)(x - \alpha) + a.$$

Substituindo $x = \alpha$ na igualdade acima, temos que

$$\begin{aligned} f(\alpha) &= q(\alpha)(\alpha - \alpha) + a \\ &= 0 + a \\ &= a. \end{aligned}$$

Logo, temos que

$$f(x) = (x - \alpha)q(x) + f(\alpha)$$

Segue uma importante conseqüência desta proposição.

COROLÁRIO 1 (PROPRIEDADE DO FATOR LINEAR)

Sejam $\boldsymbol{A}$ um corpo, $f(x) \in \boldsymbol{A}[x]$ um polinômio e $\alpha \in \boldsymbol{A}$ um escalar. Então α é uma raiz de $f(x)$ se e somente se $(x - \alpha) \mid f(x)$.

Demonstração

Da igualdade $f(x) = (x - \alpha)q(x) + f(\alpha)$, temos que

α é uma raiz de $f(x) \Leftrightarrow f(\alpha) = 0 \Leftrightarrow f(x) = (x - \alpha)q(x) \Leftrightarrow (x - \alpha) \mid f(x)$.

Observação

Veja que na demonstração do Corolário 1, na implicação $(x - \alpha) \mid f(x) \Rightarrow f(\alpha) = 0$ não é necessário usar o fato de que $\boldsymbol{A}$ é um corpo. Portanto, esta parte vale para um anel qualquer. Somente na implicação $f(\alpha) = 0 \Rightarrow (x - \alpha) \mid f(x)$ usamos a propriedade da divisão de polinômios, onde é preciso supor que $\boldsymbol{A}$ é um corpo.

Vamos, agora, desenvolver um algoritmo especial para a divisão de um polinômio qualquer por um polinômio linear do tipo $p(x) = x - \alpha$.

ALGORITMO DE BRIOT-RUFFINI

Sejam um corpo $\boldsymbol{A}$, $f(x) \in \boldsymbol{A}[x]$ um polinômio e $\alpha \in \boldsymbol{A}$ um escalar. Pela Proposição 2, existe um polinômio $q(x) \in \boldsymbol{A}[x]$ tal que

$$f(x) = (x - \alpha)q(x) + r, \text{ com } r = f(\alpha).$$

Observando a igualdade polinomial anterior, vemos que se n é o grau de $f(x)$, então o grau de $q(x)$ é $n - 1$. Denotando o polinômio $f(x)$ por

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n,$$

então queremos encontrar os coeficientes $b_0, b_1, ..., b_{n-1} \in \boldsymbol{A}$ tais que

$$q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_{n-1}x^{n-1}.$$

O algoritmo de Briot-Ruffini consiste em obter os coeficientes $b_0, b_1, ..., b_{n-1}$ de $q(x)$ em função dos coeficientes $a_0, a_1, ..., a_n$ e do escalar α. Nestas condições, veremos que

$$\begin{aligned}
b_{n-1} &= a_n \\
b_{n-2} &= b_{n-1} \cdot \alpha + a_{n-1} \\
b_{n-3} &= b_{n-2} \cdot \alpha + a_{n-2} \\
&\vdots \\
b_1 &= b_2 \cdot \alpha + a_2 \\
b_0 &= b_1 \cdot \alpha + a_1 \\
r &= b_0 \cdot \alpha + a_0
\end{aligned}$$

Podemos representar os coeficientes anteriores por meio do seguinte esquema:

a_n	a_{n-1}	a_{n-2}	...	a_2	a_1	a_0	α
b_{n-1}	b_{n-2}	b_{n-3}	...	b_1	b_0	r	

Antes de demonstrarmos as fórmulas anteriores, veremos um exemplo de como este algoritmo funciona.

Exemplo 3

Vamos obter a divisão do polinômio $f(x) = x^4 - x^3 - x + 1$ pelo polinômio linear $x - 2 \in \boldsymbol{R}[x]$. Observe que os coeficientes de $f(x)$ são $a_4 = 1$, $a_3 = -1$, $a_2 = 0$, $a_1 = -1$ e $a_0 = 1$, e o escalar $\alpha = 2$. Portanto,

o polinômio quociente será da forma $f(x) = b_3x^3 + b_2x^2 + b_1x + b_0$.

O primeiro passo consiste em montar o esquema:

Coeficientes de $f(x)$

1	–1	0	–1	1	2

Como o coeficiente $b_3 = a_4 = 1$, o segundo passo consiste em abaixar o primeiro coeficiente de $f(x)$ para a linha de baixo, obtendo o primeiro coeficiente de $q(x)$.

1	–1	0	–1	1	2
1					

Pelas igualdades do algoritmos de Briot-Ruffini, o próximo passo consiste em obter o coeficiente b_2 de $q(x)$, multiplicando o último coeficiente obtido, b_3, por $\alpha = 2$ e, depois, somando este produto ao coeficiente a_3 de $f(x)$, isto é, $b_2 = b_3 \cdot \alpha + a_2$. Assim, o próximo coeficiente é $b_2 = 1 \cdot 2 + (-1) = 1$:

1	–1	0	–1	1	2
1	1				

Continuando o procedimento, temos que

$$\begin{aligned} b_1 &= b_2 \cdot \alpha + a_2 \\ &= 1 \cdot 2 + 0 \\ &= 2. \end{aligned}$$

Representamos isso por:

1	–1	0	–1	1	2
1	1	2			

Analogamente,

$$\begin{aligned} b_0 &= b_1 \cdot \alpha + a_1 \\ &= 2 \cdot 2 + (-1) \\ &= 3. \end{aligned}$$

1	–1	0	–1	1	2
1	1	2	3		

E, finalmente, o resto é dado por

$$\begin{aligned} r &= b_0 \,.\, \alpha + a_0 \\ &= 3 \,.\, 2 + 1 \\ &= 7. \end{aligned}$$

Coeficiente de $f(x)$	$\rightarrow$	1	-1	0	-1	1 | 2
Coeficiente de $q(x)$	$\rightarrow$	1	1	2	3	7 |
						$\uparrow$ resto

Lembre, também, que outra forma de encontrar o resto r é pela igualdade

$$r = f(2) = 2^4 - 2^3 - 2 + 1 = 7.$$

Portanto, o resultado é

quociente: $q(x) = x^3 + x^2 + 2x + 3$

e

resto: $r = 7$,

ou seja,

$$x^4 - x^3 - x + 1 = (x^3 + x^2 + 2x + 3)(x - 2) + 7.$$

ATIVIDADE

4. Use o algoritmo de Briot-Ruffini para verificar que o polinômio linear $p(x) = x - 1$ divide o polinômio $f(x) = x^4 - x^3 - x + 1$.

Faremos, agora, a demonstração do algoritmo de Briot-Ruffini.

DEMONSTRAÇÃO DO ALGORITMO DE BRIOT-RUFFINI

Lembre que $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$ e que queremos encontrar um polinômio $q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_{n-1}x^{n-1} \in \boldsymbol{A}[x]$ e um resto $r \in \boldsymbol{A}$ tal que

$$f(x) = q(x)(x - \alpha) + r.$$

Lembre, também, que o nosso problema consiste em obter os coeficientes $b_0, b_1, ..., b_{n-1}$ e r em função dos coeficientes $a_0, a_1, ..., a_n$ e de α.

Como $f(x) = q(x)(x - \alpha) + r$, temos

$$a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n = (b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_{n-1}x^{n-1})(x - \alpha) + r$$
$$= (r - \alpha b_0) + (b_0 - \alpha b_1)x + (b_1 - \alpha b_2)x^2 + ... + (b_{n-2} - \alpha b_{n-1})x^{n-1} + b_{n-1}x^n$$

e, da igualdade de polinômios, segue que

$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= b_{n-2} - \alpha b_{n-1} \\ a_{n-2} &= b_{n-3} - \alpha b_{n-2} \end{aligned}$$

$$\begin{aligned} a_2 &= b_1 - \alpha b_2 \\ a_1 &= b_0 - \alpha b_1 \\ a_0 &= r - \alpha b_0. \end{aligned}$$

Invertendo estas equações, obtemos,

$$\begin{aligned} b_{n-1} &= a_n \\ b_{n-2} &= b_{n-1} \cdot \alpha + a_{n-1} \\ b_{n-3} &= b_{n-2} \cdot \alpha + a_{n-2} \end{aligned}$$

$$\begin{aligned} b_1 &= b_2 \cdot \alpha + a_2 \\ b_0 &= b_1 \cdot \alpha + a_1 \\ r &= b_0 \cdot \alpha + a_0. \end{aligned}$$

Estas são as equações desejadas.

Exemplo 4

Neste exemplo, faremos sucessivas aplicações do algoritmo de Briot-Ruffini. Observe que 1 e –1 são raízes de $f(x) = x^4 - 1$, pois $f(1) = 0$ e $f(-1) = 0$. Fazemos, inicialmente, a divisão de $x^4 - 1$ por $x - 1$ e, em seguida, por $x + 1$.

Coeficiente de $f(x)$ $\rightarrow$	1	0	0	0	– 1	1
Coeficiente de $q_1(x)$ $\rightarrow$	1	1	1	1	0	

↑
resto

Observe que o primeiro polinômio quociente é $q_1(x) = x^3 + x^2 + x + 1$. Como $q_1(-1) = 0$, temos que $q_1(x)$ é divisível por $x + 1$. Aplicamos, novamente, o algoritmo de Briot-Ruffini, dividindo $q_1(x)$ por $x + 1$. Temos,

coeficientes de $f(x)$ $\rightarrow$	1	0	0	0	– 1	1
coeficientes de $q_1(x)$ $\rightarrow$	1	1	1	1	0	– 1
coeficientes de $q_2(x)$ $\rightarrow$	1	0	1	0		

↑
resto

O segundo quociente é $q_2(x) = x^2 + 1$. Assim,

$$\begin{aligned} f(x) &= x^4 - 1 \\ &= (x^3 + x^2 + x + 1)(x - 1) \\ &= (x^2 + 1)(x + 1)(x - 1). \end{aligned}$$

ATIVIDADES FINAIS

1. Se dividirmos um polinômio $f(x) \in \boldsymbol{R}[x]$ por $x - 2$, o resto será 13 e se dividirmos $f(x)$ por $x - 2$, o resto será 5. Supondo que $r(x)$ é o resto da divisão de $f(x)$ por $x^2 - 4$, calcule $r(1)$.

2. Sejam ***A*** um corpo $a, b \in A$ e $f(x) \in A[x]$. Prove que se $f(a) = f(b) = 0$ e $a \neq b$, então $(x - a)(x - b) \mid f(x)$.

RESUMO

Num corpo ***A***, se $f(x) \in A[x]$ for um polinômio e $\alpha \in A$, um escalar, então existirá um polinômio $q(x) \in A[x]$ tal que

$$f(x) = (x - \alpha)q(x) + f(\alpha),$$

isto é, o resto da divisão de $f(x)$ por $x - \alpha$ é $r = f(\alpha)$. Como conseqüência, temos que $f(\alpha) = 0$ se, e somente se, $x - \alpha$ dividir $f(x)$.

O algoritmo de Briot-Ruffini afirma que para um polinômio $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n \in A[x]$ e um escalar α num corpo ***A***, os coeficientes do polinômio quociente $q(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + ... + b_{n-1}x^{n-1} \in A[x]$ e o resto $r \in A$, da divisão de $f(x)$ por $x - \alpha$, isto é, tais que

$$f(x) = q(x)(x - \alpha) + r,$$

são dados por

$$\begin{aligned}
b_{n-1} &= a_n \\
b_{n-2} &= b_{n-1} \cdot \alpha + a_{n-1} \\
b_{n-3} &= b_{n-2} \cdot \alpha + a_{n-2} \\
&\vdots \\
b_1 &= b_2 \cdot \alpha + a_2 \\
b_0 &= b_1 \cdot \alpha + a_1 \\
r &= b_0 \cdot \alpha + a_0 .
\end{aligned}$$

RESPOSTAS COMENTADAS

Atividade 1

Aplicando o algoritmo da divisão de polinômios, obtemos

$$\begin{array}{r|l} x^4 - x^3 + 2x^2 - x + 1 & x^2 + 1 \\ \cline{2-2} x^4 - x^2 & x^2 - x + 1 \\ \cline{1-1} -x^3 + x^2 - x + 1 & \\ -x^3 - x & \\ \cline{1-1} x^2 + 1 & \\ x^2 + 1 & \\ \cline{1-1} 0 & \end{array}$$

Daí, vemos que o quociente é $q(x) = x^2 - x + 1$ e o resto é o polinômio nulo $r(x) = 0$.

Atividade 2

Aplicando o algoritmo da divisão de polinômios, agora em $Z_2[x]$,

$$\begin{array}{r|l} x^4 + x^2 + \overline{1} & \\ x^4 + x^3 + x^2 & x^2 + x + \overline{1} \\ \cline{2-2} x^3 + \overline{1} & x^2 + x + \overline{1} \\ \cline{1-1} x^3 + x^2 + x & \\ x^2 + x + \overline{1} & \\ \cline{1-1} x^2 + x + \overline{1} & \\ 0 & \\ \cline{1-1} & \end{array}$$

Daí, vemos que o quociente é $q(x) = x^2 - x + \overline{1}$ e o resto é o polinômio nulo $r(x) = \overline{0}$.

Atividade 3

Aplicando o algoritmo da divisão de polinômios, obtemos

$$\begin{array}{r|l} x^4 - x^3 - x + 1 & x - 1 \\ \cline{2-2} x^4 - x^3 & x^3 - 1 \\ \cline{1-1} -x + 1 & \\ -x + 1 & \\ \cline{1-1} 0 & \end{array}$$

Daí, vemos que o resto da divisão é o polinômio nulo e, portanto, $x - 1$ divide $f(x) = x^4 - x^3 - x + 1$. Observe que o polinômio quociente é $q(x) = x^3 - 1$.

Atividade 4

Aplicando o algoritmo de Briot-Ruffini, obtemos

$$\begin{array}{lccccc|c} \text{coeficientes de } f(x) \rightarrow & 1 & -1 & 0 & -1 & 1 & 1 \\ \cline{1-7} \text{coeficientes de } q(x) \rightarrow & 1 & 0 & 0 & -1 & 0 & \\ & & & & & \uparrow & \\ & & & & & \text{resto} & \end{array}$$

Daí, vemos que o resto da divisão é zero e, portanto, $x - 1$ divide $f(x) = x^4 - x^3 - x + 1$. Observe que o polinômio quociente é $q(x) = x^3 - 1$.

Atividade Final 1

Quando dividimos $f(x)$ por $x - 2$, obtemos resto 13, isto é, $f(x) = q_1(x)(x - 2) + 13$. Observe que $f(2) = 13$.

Dividindo $f(x)$ por $x + 2$, obtemos resto 5, isto é, $f(x) = q_2(x)(x + 2) + 5$. Novamente, observe que $f(-2) = 5$.

Quando dividimos $f(x)$ por $x^2 - 4$, obtemos

$$f(x) = q(x)(x^2 - 4) + r(x), \text{ com } gr(r(x)) < 2 \text{ ou } r(x) = 0.$$

Assim, temos $r(x) = ax + 0$ com $a, b \in \boldsymbol{R}$.

De $f(2) = 13$, obtemos

$$\begin{aligned} 13 &= f(2) \\ &= q(2)(2^2 - 4) + (a.2 + b) \\ &= 2a + b, \end{aligned}$$

ou seja, temos $2a + b = 13$.

De $f(-2) = 5$, obtemos

$$\begin{aligned} 5 &= f(-2) \\ &= q(-2)((-2)^2 - 4) + (a \,.\, (-2) + b) \\ &= -2a + b, \end{aligned}$$

ou seja, temos $-2a + b = 5$.

Resolvendo o sistema

$$\begin{cases} 2a + b = 13 \\ -2a + b = 5, \end{cases}$$

obtemos $a = 2$ e $b = 9$, o que nos dá $r(x) = 2x + 9$. Portanto, $r(1) = 11$.

Atividade Final 2

Dividindo o polinômio $f(x)$ por $(x - a)(x - b)$, obtemos

$f(x) = q(x)(x - a)(x - b) + r(x)$, com $gr(r(x)) < 2$ ou $r(x) = 0$.

Portanto, temos $r(x) = cx + d$ com $c, d \in \boldsymbol{A}$.

Como $f(a) = 0$ temos

$$\begin{aligned} 0 &= f(a) \\ &= q(a)(a - a)(a - b) + (c \,.\, a + d) \\ &= ac + d, \end{aligned}$$

ou seja, $ac + d = 0$.

Como $f(b) = 0$ temos

$$\begin{aligned} 0 &= f(b) \\ &= q(b)(b-a)(b-b) + (\mathrm{c} \,.\, b + d) \\ &= bc + d, \end{aligned}$$

ou seja, $bc + d = 0$.

Temos, assim, o sistema

$$\begin{cases} ac + d = 0 \\ bc + d = 0 \end{cases}$$

Subtraindo $bc + d = 0$ de $ac + d = 0$, obtemos

$$\begin{aligned} (ac + d) - (bc + d) &= 0 - 0 \\ ac + bc &= 0 \\ (a - b) \,.\, c &= 0. \end{aligned}$$

Como ***A*** é um corpo e $a - b \neq 0$, então resta $c = 0$. Substituindo esse valor em $ac + d = 0$, obtemos $d = 0$, o que nos dá $r(x) = 0$, isto é, $r(x)$ é o polinômio nulo. Portanto,

$$f(x) = q(x)(x - a)(x - b),$$

o que significa que $(x - a)(x - b) \,|\, f(x)$ em $A[x]$.

AULA 10

Sobre raízes de polinômios

Meta da aula

Apresentar alguns resultados importantes sobre as raízes de polinômios.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Realizar uma pesquisa sobre raízes de polinômios.
- Identificar o conceito de multiplicidade de uma raiz.
- Identificar as possíveis raízes racionais de um polinômio com coeficientes inteiros.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I, e dos conhecimentos sobre os polinômios das Aulas 5 a 9.

INTRODUÇÃO

Nas aulas anteriores estudamos várias propriedades da divisão de polinômios. Uma das mais importantes foi a propriedade do fator linear, pois ela fornece informação sobre a quantidade máxima de raízes de um polinômio. Por isso, vamos começar revendo esta propriedade.

PROPOSIÇÃO 1 (PROPRIEDADE DO FATOR LINEAR)

Sejam A um corpo, $f(x) \in A[x]$ um polinômio e $\alpha \in A$ um escalar. Então α é uma raiz de $f(x)$ se e somente se $(x - \alpha) \mid f(x)$ em $A[x]$.

É relevante o número máximo de vezes que esse polinômio linear $x - \alpha$ divide $f(x)$. A esse conceito chamamos multiplicidade da raiz α.

Definição 1

Sejam A um corpo e $\alpha \in A$ uma raiz do polinômio $f(x) \in A[x]$. Chamamos *multiplicidade* da raiz α ao inteiro positivo m tal que

$$(x - \alpha)^m \mid f(x) \text{ e } (x - \alpha)^{m+1} \Phi f(x),$$

portanto, ao número máximo de vezes que o polinômio linear $x - \alpha$ divide $f(x)$.

Isto também pode ser posto da seguinte forma:

$$f(x) = (x - \alpha)^m q(x) \text{ com } q(\alpha) \neq 0.$$

Dizemos, ainda, que uma raiz é *simples* quando sua multiplicidade for igual a 1 e que a raiz é *múltipla* quando sua multiplicidade for maior que 1. Dizemos, também, que a raiz é dupla ou, então, *tripla*, quando sua multiplicidade for igual a 2 ou a 3, respectivamente.

Exemplo 1

Dado o polinômio $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in R[x]$, então 1 é raiz de $f(x)$, pois

$$\begin{aligned} f(1) &= 1^4 - 2 \cdot 1^3 + 2 \cdot 1^2 - 2 \cdot 1 + 1 \\ &= 1 - 2 + 2 - 2 + 1 \\ &= 0 \end{aligned}$$

Vamos calcular a multiplicidade desta raiz. Aplicando Briot-Ruffini duas vezes, obtemos

1	–2	2	–2	1	1
1	–1	1	–1	0	
1	0	1	0		

e, portanto,

$$f(x) = (x^2 + 1)(x - 1)(x - 1)$$
$$= (x - 1)^2(x^2 + 1).$$

Como 1 não é raiz de $q(x) = x^2 + 1$, pois $q(1) = 2 \neq 0$, então a multiplicidade da raiz 1 é igual a 2, ou seja, 1 é uma raiz dupla de $f(x)$.

Uma conseqüência importante da propriedade do fator linear afirma que um polinômio de grau n tem, no máximo, n raízes.

PROPOSIÇÃO 2 (QUANTIDADE MÁXIMA DE RAÍZES DE UM POLINÔMIO)

Sejam A um corpo e $f(x) \in A[x]$ um polinômio de grau n. Então, $f(x)$ tem, no máximo, n raízes em A, sendo que cada raiz é contada um número de vezes igual à sua multiplicidade.

Demonstração

Sejam $\alpha_1, \alpha_2, ..., \alpha_\kappa \in A$ todas as raízes distintas de $f(x)$, isto é, sem contar suas multiplicidades.

1º passo: Seja m_1 a multiplicidade da raiz α_1, isto é,

$$f(x) = (x - \alpha_1)^{m1}\, q_1(x) \text{ com } q_1(\alpha_1) \neq 0,$$

onde $q_1(x) \in A[x]$.

2º passo: Como $f(\alpha_2) = 0$, então

$$(\alpha_2 - \alpha_1)^{m1}\, q_1(\alpha_2) = 0.$$

Como estamos supondo que $\alpha_1 \neq \alpha_2$, temos que $\alpha_2 - \alpha_1 \neq 0$. Logo, $q_1(\alpha_2) = 0$, isto é, α_2 também é uma raiz de $q_1(x)$.

Seja m_2 a multiplicidade da raiz α_2, isto é,

$$q_1(x) = (x - \alpha_2)^{m2}\, q_2(x) \text{ com } q_2(\alpha_2) \neq 0.$$

Portanto,

$$\begin{aligned} f(x) &= (x - \alpha_1)^{m1} q_1(x) \\ &= (x - \alpha_1)^{m1} (x - \alpha_2) q_1(\alpha_2) \end{aligned}$$

com $q_2(\alpha_1) \neq 0$ e $q_2(\alpha_2) \neq 0$.

Procedendo assim, sucessivamente, obtemos

$$f(x) = (x - \alpha_1)^{m1}(x - \alpha_2)^{m2} \ldots (x - \alpha_k)^{mk}\, q_k(x)$$

com $q_k(\alpha_1) \neq 0$, $q_k(\alpha_2) \neq 0$, , $q_k(\alpha_k) \neq 0$.

Contando as raízes com suas multiplicidades temos $m_1 + m_2 + \ldots + m_k$ raízes e

$$m_1 + m_2 + \ldots + m_k \leq + m_1 + m_2 + \ldots + m_k + gr(q_k(x)) = gr(f(x)) = n.$$

Exemplo 2

Considere o polinômio do Exemplo 1, $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \boldsymbol{R}[x]$. Como $\boldsymbol{R}[x] \subset \boldsymbol{C}[x]$, podemos supor que $f(x) = x^4 - 2x^3 + 2x^2 - 2x + 1 \in \boldsymbol{C}[x]$. No exemplo anterior, vimos que

$$f(x) = (x - 1)^2 (x^2 + 1).$$

Mas, em $\mathbf{C}[x]$, vale que

$$x^2 + 1 = (x + i)(x - i),$$

onde $i = \sqrt{-1}$. Então $f(x)$ pode ser escrito como

$$f(x) = (x - 1)^2 (x + i)(x - i).$$

Portanto, $f(x)$ tem 4 raízes complexas: 1, 1, $-i$ e i. Observe que uma delas, a raiz 1, é uma raiz dupla, enquanto $-i$ e i são raízes simples. Observe que, em $\boldsymbol{R}$, o polinômio $f(x)$ possui uma única raiz e ela é de multiplicidade dois.

Exemplo 3

O polinômio $f(x) = x^4 + x^3 - x - 1 \in \boldsymbol{R}[x]$ tem, no máximo, 4 raízes reais. Observe que 1 e –1 são raízes de $f(x)$. Aplicando Briot-Ruffini duas vezes, temos

1	1	0	–1	–1	1
1	2	2	1	0	–1
1	1	1	0		

logo,
$$f(x) = (x^3 + 2x^2 + 2x + 1)(x - 1)$$
$$= (x^2 + x + 1)(x + 1)(x - 1).$$

Como $q(x) = x^2 + x + 1$ não tem raízes reais, pois $\Delta = 1^2 - 4.\ 1\ .\ 1 = -3 < 0$, então $f(x)$ tem somente duas raízes reais, a saber, 1 e –1. Observe que ambas têm multiplicidade 1. No entanto, considerando $f(x) = x^4 + x^3 - x - 1$ em $\mathbf{C}[x]$, então $f(x)$ tem 4 raízes complexas. Veja que as raízes complexas de $q(x) = x^2 + x + 1$ são

$$\frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3}\, i}{2}.$$

Assim,

$$q(x) = x^2 + x + 1 = (x - \frac{-1 - \sqrt{3}\, i}{2})(x - \frac{-1 + \sqrt{3}\, i}{2}),$$

e $f(x)$ se escreve como

$$f(x) = (x - \frac{-1 - \sqrt{3}\, i}{2})(x - \frac{-1 + \sqrt{3}\, i}{2})(x + 1)(x - 1).$$

Observe que todas as quatro raízes complexas $f(x)$ são raízes simples.

ATIVIDADE

1. a. Aplicando o algoritmo de Briot-Ruffini, encontre todas as raízes reais de $f(x) = x^4 - 1 \in \boldsymbol{R}[x]$ e determine suas multiplicidades. Depois, considerando $f(x) = x^4 - 1 \in \boldsymbol{C}[x]$, obtenha também suas raízes complexas com suas multiplicidades.

1. b. Calcule as raízes de $f(x) = x^4 + \overline{1} \in \boldsymbol{Z}_2[x]$ e determine suas multiplicidades.

Vamos enunciar, agora, o resultado mais importante sobre raízes de polinômios com coeficientes complexos, o Teorema Fundamental da Álgebra. Ele garante que todo polinômio não-constante de coeficientes complexos tem, ao menos, uma raiz complexa.

TEOREMA FUNDAMENTAL DA ÁLGEBRA

Sejam $\boldsymbol{C}$ o corpo dos números complexos e $f(x) \in \boldsymbol{C}[x]$ um polinômio não-constante. Então, existe um valor $\alpha \in \boldsymbol{C}$ tal que $f(\alpha) = 0$, ou seja, $f(x)$ admite raiz complexa.

Como conseqüência, se $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n$ é um polinômio de coeficientes complexos de grau $n \geq 1$, então $f(x)$ tem n raízes complexas, $\alpha_1, \alpha_2, \ldots, \alpha_n \in \boldsymbol{C}$, contando suas multiplicidades, e $f(x)$ se decompõe em um produto de fatores lineares em $\boldsymbol{C}[x]$,

$$f(x) = a_n(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Observações

1. É curioso que o chamado Teorema Fundamental da Álgebra não se prove somente com técnicas algébricas, pois todas as demonstrações conhecidas deste teorema envolvem o conceito não algébrico de continuidade; conceito esse, da área de Análise. Portanto, a demonstração deste teorema está fora do escopo deste curso.

2. Observe que o Teorema Fundamental da Álgebra afirma que um polinômio de grau n, em $\mathbf{C}[x]$, possui n raízes complexas. Infelizmente, ele não informa como obter essas raízes, o que, em geral, é um problema muito difícil. Na Aula 2 vimos como determinar as raízes de polinômios de graus 2 e 3 em função dos seus coeficientes. Não é muito difícil obter fórmulas similares para as raízes de um polinômio de grau 4. No entanto, se o grau do polinômio for maior ou igual a 5, então, em geral, não existe fórmula que expresse suas raízes em função de seus coeficientes.

Um outro resultado, interessante para um curso introdutório como este, é a seguinte propriedade usada para determinar as possíveis raízes racionais de um polinômio com coeficientes inteiros.

PROPOSIÇÃO 3 (PROPRIEDADE DAS RAÍZES RACIONAIS)

Sejam $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \in \mathbf{Z}[x]$ um polinômio de grau $n \geq 1$ e $\alpha = \frac{p}{q}$ uma raiz racional de $f(x)$ com $p, q \in \mathbf{Z}$, q > 0 e $mdc\,(p, q) = 1$. Então, $p \mid a_0$ e $q \mid a_n$.

Demonstração

Como $f(p/q) = f(\alpha) = 0$ temos

$$a_0 + a_1\left(\frac{p}{q}\right) + a_2\left(\frac{p}{q}\right)^2 + a_3\left(\frac{p}{q}\right)^3 + \cdots + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + a_n\left(\frac{p}{q}\right)^n = 0$$

Multiplicando esta equação por q^n, obtemos

$$a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + a_3p^3q^{n-3} + \ldots + a_{n-1}p^{n-1}q + a_np^n = 0.$$

Vamos reescrever esta equação de duas formas. Primeiro, fatoramos p das últimas n parcelas, obtendo

$$a_0q^n + (a_1q^{n-1} + a_2pq^{n-2} + a_3p^2q^{n-3} + \ldots + a_{n-1}p^{n-2}q + a_np^{n-1})\,p = 0,$$

o que nos dá

$$a_0q^n = -(a_1pq^{n-1} + a_2pq^{n-2} + a_3p^2p^{n-3} + \ldots + a_{n-1}p^{n-2}q + a_np^{n-1})p,$$

que é um múltiplo de p. Portanto, $p \mid a_0 q^n$. Agora, como mdc $(p, q) = 1$, então $p \mid a_0$. Analogamente, fatoramos q das primeiras n parcelas de

$$a_0 q^n + a_1 p q^{n-1} + a_2 p^2 q^{n-1} + a_3 p^3 q^{n-3} + \ldots + a_{n-1} q^{n-1} q + a_n p^n = 0,$$

obtendo

$$(a_0 q^{n-1} + a_1 p q^{n-2} + a_2 p^2 q^{n-3} + a_3 p^3 q^{n-4} + \ldots + a_{n-1} p^{n-1}) q + a_n p^n = 0$$

o que nos dá,

$$a_n q^n = -(a_0 q^{n-1} + a_1 p q^{n-2} + a_2 p^2 q^{n-3} + a_3 q^3 q^{n-4} + \ldots + a_{n-1} p^{n-1}) q,$$

que é múltiplo de q. Portanto, $q \mid a_n p^n$. Novamente, como mdc $(p, q) = 1$, então $q \mid a_n$. Concluímos, assim, a prova da proposição.

Exemplo 4

Vamos determinar todas as raízes racionais do polinômio $f(x) = 2x^4 - 5x^3 - 2x^2 - 4x + 3$. Aplicando o critério da raiz racional, se $\alpha = \frac{p}{q}$ for uma raiz racional de $f(x)$ com mdc $(p, q) = 1$, então

$$p \mid 3 \text{ e } q \mid 2.$$

Portanto, $p \in \{-3, -1, 1, 3\}$ e $q \in \{1, 2\}$. Logo, os candidatos a raiz racional de $f(x)$ são

$$\alpha = \frac{p}{q} \in \left\{1, -1, 3, -3, \frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}\right\}.$$

Agora, é preciso checar estas possibilidades anteriores. Facilmente vemos que

$f(1) = -6 \neq 0$, $f(-1) = 12 \neq 0$, $f(-3) = 294 \neq 0$, $f(3) = 0$ e $f(1/2) = 0$.

Como 3 e 1/2 são raízes de $f(x)$, podemos aplicar Briot-Ruffini duas vezes, obtendo

2	– 5	– 2	– 4	3	3
2	1	1	– 1	0	1/2
2	2	2	0		

Isto nos dá a fatoração

$$f(x) = 2x^4 - 5x^3 - 2x^2 - 4x + 3$$
$$= (2x^2 + 2x + 2)(x - 3)(x - \frac{1}{2}).$$

Como o polinômio quadrático $g(x) = 2x^2 + 2x + 2$ não tem raízes reais, pois $\Delta = 2^2 - 4.\ 2\ .\ 2 = -12$, então, em particular, também não possui raízes racionais. Portanto, as raízes racionais de $f(x)$ são 3 e $\frac{1}{2}$. Assim, a decomposição de $f(x)$ em $\boldsymbol{R}[x]$ e em $\boldsymbol{Q}[x]$ é

$$f(x) = (2x^2 + 2x + 2)(x - 3)(x - \frac{1}{2}).$$

É interessante considerar $f(x) = 2x^4 - 5x^3 - 2x^2 - 4x + 3$ como um polinômio em $\boldsymbol{C}[x]$. Neste caso, as raízes complexas de $g(x) = 2x^2 + 2x + 2$ são

$$\frac{-1 \pm \sqrt{-3}}{2} = \frac{-1 \pm \sqrt{3}\, i}{2}\ .$$

Assim, a decomposição de $f(x)$ em $\boldsymbol{C}[x]$ é

$$f(x) = 2(x - \frac{-1 - \sqrt{3}\, i}{2})(x - \frac{-1 + \sqrt{3}\, i}{2})(x - 3)(x - \frac{1}{2}).$$

Lembre que se $\alpha = a + bi \in \mathbb{C}$, então seu *conjugado complexo* é o número $\overline{\alpha} = a - bi \in \boldsymbol{C}$. Por exemplo, se $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ então $\overline{\alpha} = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$. Assim, é interessante notar que as raízes complexas de $f(x)$ aparecem em pares de conjugados complexos. Isto é uma característica de todo polinômio com coeficientes reais. Vamos enunciar mais esta propriedade.

PROPOSIÇÃO 4 (PROPRIEDADE DAS RAÍZES CONJUGADAS)

Sejam $f(x) \in \boldsymbol{R}[x]$ e $\alpha \in \boldsymbol{C}$ uma raiz de $f(x)$, então $\overline{a}$ também é uma raiz de $f(x)$.

A demonstração desta proposição será parte de sua atividade final. Convidamos você a aplicar os resultados anteriores na próxima atividade.

ATIVIDADE

2. Determine todas as raízes do polinômio $f(x) = x^4 - 3x^2 - 4$ sabendo que $\alpha = i$ é uma raiz.

ATIVIDADES FINAIS

1. Prove a Proposição 4 sobre a propriedade das raízes conjugadas.

2. Seja $f(x) = ax^3 + bx^2 + cx + d \in A[x]$ um polinômio de grau 3, com A um corpo, e raízes α_1, α_2 e α_3. Mostre que

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = -\dfrac{b}{a} \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = \dfrac{c}{a} \\ \alpha_1\alpha_2\alpha_3 = -\dfrac{d}{a} \end{cases}.$$

3. Sendo 1 e $1 + 2i$ raízes do polinômio $f(x) = x^3 + ax^2 + bx + c$, em que a, b e c são números reais, então calcule o polinômio $f(x)$.

RESUMO

Nesta aula, você foi apresentado a vários resultados interessantes sobre as raízes de um polinômio.

Primeiramente, apresentamos conceito de multiplicidade de uma raiz α de um polinômio $f(x)$, ou seja o inteiro positivo m, tal que $(x - \alpha)^m \mid f(x)$ e $(x - \alpha)^{m+1} \Phi f(x)$, ou, equivalentemente, tal que

$$f(x) = (x - \alpha)^m q(x) \text{ com } q(\alpha) \neq 0.$$

Observamos, também, que o número de raízes de um polinômio, contadas com sua multiplicidade, não pode ultrapassar o grau do polinômio.

Vimos o Teorema Fundamental da Álgebra. Ele afirma que todo polinômio não-constante de coeficientes complexos admite ao menos uma raiz complexa.

Apresentamos um critério que permite obter as possíveis raízes racionais de um polinômio de coeficientes inteiros, a saber, se $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_nx^n \in \boldsymbol{Z}[x]$ for um polinômio de grau $n \geq 1$ e $\alpha = \frac{p}{q}$ for uma raiz racional de $f(x)$ com $p, q \in \boldsymbol{Z}$, $q > 0$ e $\text{mdc}(p, q) = 1$, então $p \mid a_0$ e $q \mid a_n$.

Finalmente, apresentamos a propriedade sobre polinômios com coeficientes reais que afirma que se $f(x) \in \boldsymbol{R}[x]$ e $\alpha = C$ for uma raiz de $f(x)$, então $\overline{\alpha}$, o conjugado complexo de α, também será uma raiz de $f(x)$.

RESPOSTAS COMENTADAS

Atividade 1

a. O polinômio $f(x) = x^4 - 1 \in R[x]$ tem, no máximo, 4 raízes reais. Facilmente vemos que 1 e –1 são raízes de $f(x)$. Aplicando Briot-Ruffini duas vezes, temos

1	0	0	0	–1	1
1	1	1	1	0	–1
1	0	1	0		

ou seja,

$$f(x) = (x^2 + 1)(x + 1)(x - 1).$$

Como $q(x) = x^2 + 1$ não tem raízes reais, então $f(x)$ tem somente duas raízes reais, a saber, 1 e -1. Veja que estas raízes são simples, ou seja, de multiplicidade 1.

Considerando $f(x) = x^4 - 1 \in C[x]$, pelo Teorema Fundamental da Álgebra, sabemos que $f(x)$ tem 4 raízes complexas. Duas delas, 1 e -1, já são conhecidas. As outras duas são as raízes complexas de $q(x) = x^2 + 1$, a saber i e $-i$. Assim,

$$q(x) = (x + i)(x - i),$$

e $f(x)$ se fatora em

$$f(x) = (x + i)(x - i)(x + 1)(x - 1).$$

Observe que todas as raízes complexas de $f(x)$ são raízes simples.

b. Como estamos trabalhando em Z_2, vemos que $\overline{1}$ é uma raiz de $f(x) = x^4 + \overline{1} \in Z_2[x]$, pois

$$\begin{aligned} f(\overline{1}) &= (\overline{1})^4 + \overline{1} \\ &= \overline{1} + \overline{1} \\ &= \overline{2} \\ &= \overline{0}. \end{aligned}$$

Aplicando Briot-Ruffini três vezes,

$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{0}$	
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{0}$		
$\overline{1}$	$\overline{1}$	$\overline{0}$			

obtemos, assim,

$$\begin{aligned} f(x) &= x^4 + \overline{1} \\ &= (x^3 + x^2 + x + \overline{1})(x - \overline{1}) \\ &= (x^2 + \overline{1})(x - \overline{1})(x - \overline{1}) \\ &= (x + \overline{1})(x - \overline{1})(x - \overline{1})(x - \overline{1}). \end{aligned}$$

Como $-\overline{1} = \overline{1}$ em Z_2, podemos escrever

$$\begin{aligned} f(x) &= (x + \overline{1})(x - \overline{1})(x - \overline{1})(x - \overline{1}) \\ &= (x + \overline{1})(x + \overline{1})(x + \overline{1})(x + \overline{1}) \\ &= (x + \overline{1})^4. \end{aligned}$$

Atividade 2

Como $f(i) = 1 - 3 \cdot (-1) - 4 = 0$ e o polinômio $f(x) = x^4 - 3x^2 - 4$ tem coeficientes reais, então $-i$ também é raiz de $f(x)$. Aplicando Briot-Ruffini duas vezes,

1	0	-3	0	-4	i
1	i	-4	$-4i$	0	$-i$
1	0	-4	0		

obtemos

$$\begin{aligned} f(x) &= (x + i)(x - i)(x^2 - 4) \\ &= (x + i)(x - i)(x + 2)(x - 2). \end{aligned}$$

Portanto, as raízes de $f(x) = x^4 - 3x^2 - 4$ são $\pm i$ e ± 2, todas raízes simples. Observe que se não fosse dada a informação sobre a raiz complexa i, poderíamos ter aplicado o critério da raiz racional, obtendo que 2 e -2 são raízes de f(x). Logo, aplicando Briot-Ruffini para estas raízes, obtemos

$$\begin{aligned} f(x) &= (x^2 + 1)(x + 2)(x - 2) \\ &= (x + i)(x - i)(x + 2)(x - 2). \end{aligned}$$

Atividade Final 1

Lembre que se $\beta, \alpha \in C$ e $\overline{\alpha}$ e $\overline{\beta}$ são seus conjugados complexos, então

$$\overline{\alpha\beta} = \overline{\alpha} \ . \ \overline{\beta},$$

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$$

e

$$\alpha = \overline{\alpha} \iff \alpha \in \boldsymbol{R}.$$

Seja, agora, $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$ com $a_K \in \boldsymbol{R}$ para todo $\boldsymbol{k}$. Se $\alpha \in C$ é uma raiz de $f(x)$ então

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + ... + a_n\alpha^n = 0.$$

Aplicando o conjugado complexo na igualdade acima, temos

$$\overline{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + ... + a_n\alpha^n} = \overline{0}.$$

Logo,

$$\overline{a_0} + \overline{a_1\alpha} + \overline{a_2\alpha^2} + \overline{a_3\alpha^3} + ... + \overline{a_n\alpha^n} = 0$$

$$\overline{a_0} + \overline{a_1}\,\overline{\alpha} + \overline{a_2}\,\overline{\alpha^2} + \overline{a_3}\,\overline{\alpha^3} + ... + \overline{a_n}\,\overline{\alpha^n} = 0$$

$$a_0 + a_1\overline{\alpha} + a_2\overline{\alpha^2} + a_3\overline{\alpha^3} + ... + a_n\overline{\alpha^n} = 0$$

pois, cada $a_K \in \boldsymbol{R}$. A igualdade acima significa que $f(\overline{\alpha}) = 0$, isto é, $\overline{\alpha}$ também é raiz de $f(x)$.

Atividade Final 2

Se $f(x) = ax^3 + bx^2 + cx + d$ um polinômio de grau 3 com raízes α_1, α_2 e α_3, então, aplicando Briot-Ruffini três vezes, obtemos

$$\begin{aligned} f(x) &= ax^3 + bx^2 + cx + d \\ &= a(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \\ &= a\left(x^3 - (\alpha_1 + \alpha_2 + \alpha_3)x^2 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3\right) \\ &= ax^3 - a(\alpha_1 + \alpha_2 + \alpha_3)x^2 + a(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x - a\alpha_1\alpha_2\alpha_3. \end{aligned}$$

Comparando os coeficientes da primeira e da última expressão, obtemos

$$\begin{aligned} -a(\alpha_1+\alpha_2+\alpha_3) &= b \\ a(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) &= c \\ -a\alpha_1\alpha_2\alpha_3 &= d, \end{aligned}$$

e, portanto,

$$\begin{cases} \alpha_1+\alpha_2+\alpha_3 = -\dfrac{b}{a} \\ \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 = \dfrac{c}{a} \\ \alpha_1\alpha_2\alpha_3 = -\dfrac{d}{a}. \end{cases}$$

3. Como $1+2i$ é raiz de $f(x)$ e $f(x)$ tem coeficientes reais, então $1-2i$ também é raiz de $f(x)$. Logo, pelo resultado do exercício anterior, com $\alpha_1 = 1$, $\alpha_2 = 1+2i$ e $\alpha_3 = 1-2i$, temos que

$$\begin{cases} 1+(1+2i)+(1-2i) = -\dfrac{a}{1} \\ 1(1+2i)+1\ \ (1-2i)+(1+2i)(1-2i) = \dfrac{b}{1} \\ 1(1+2i)(1-2i) = -\dfrac{c}{1}. \end{cases}$$

Portanto,

$$\begin{cases} a = -3 \\ b = 7 \\ c = -5. \end{cases}$$

Assim, $f(x) = x^3 - 3x^2 + 7x - 5$.

AULA 11

Polinômios irredutíveis

Meta da aula

Apresentar o conceito de polinômios irredutíveis e algumas de suas propriedades.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Definir o conceito de polinômio irredutível.
- Identificar polinômios irredutíveis de grau 1, 2 e 3.
- Identificar certos tipos polinômios irredutíveis de coeficientes inteiros.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I, e dos conhecimentos sobre os polinômios estudados nas Aulas 5 a 10.

INTRODUÇÃO

Vamos estudar, nesta aula, o conceito de polinômios que não se decompõem como um produto de outros polinômios. Estes são os polinômios irredutíveis. Eles são, na teoria dos polinômios, o análogo dos números primos no anel dos inteiros Z. Não se esqueça de que os números primos não se decompõem como um produto de inteiros positivos diferentes de 1 e dele mesmo; portanto, durante o desenvolvimento dos conceitos e das propriedades, lembre-se sempre da teoria dos números primos.

DEFINIÇÃO 1

Seja K um corpo, dizemos que $f(x) \in K[x]$ é um polinômio *irredutível sobre K*, ou *irredutível* em $K[x]$, se seus únicos divisores em $K[x]$ são os polinômios constantes e os múltiplos constantes dele mesmo, ou seja, se $g(x) \in K[x]$ é tal que

$$g(x) \mid f(x) \Rightarrow g(x) = c \text{ ou } g(x) = d\,f(x) \text{ onde } c \text{ e } d \text{ são constantes.}$$

Dizemos que $f(x)$ é *redutível em* $K[x]$, quando ele não for irredutível, ou seja, quando existirem polinômios $g(x)$, $h(x) = K(x)$ tais que

$$f(x) = g(x)h(x) \text{ com } gr(g(x)) < gr(h(x)) \text{ e } gr(f(x)).$$

Exemplo 1

Considere o polinômio $f(x) = x^2 - 2$ em $\mathbf{Q}[x]$. Como $f(x)$ é um polinômio de grau 2, se ele fosse redutível em $\mathbf{Q}[x]$, existiria um polinômio linear $ax + b$ em $\mathbf{Q}$[x], tal que $(ax + b) \mid f(x)$. Como o polinômio $ax + b$ tem raiz $-\frac{b}{a} \in \mathbf{Q}$, então $f(x)$ teria também uma raiz racional. Mas, sabemos que as possíveis raízes racionais de $f(x)$ são 2 e –2. Testando estas possibilidades, vemos que

$$f(2) = f(-2) = 2 \neq 0.$$

Assim, $f(x)$ não tem raízes racionais; logo, ele não pode ser escrito como o produto de dois polinômios de grau 1 em $\mathbf{Q}[x]$ e, portanto, é irredutível em $\mathbf{Q}[x]$.

Por outro lado, como $\pm\sqrt{2} \in R$, então $f(x)$ é redutível em $\boldsymbol{R}[x]$, pois podemos escrever

$$f(x) = x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$$

Logo, $f(x)$ é o produto de dois polinômios de grau um em $\boldsymbol{R}$[x].

Para compreender melhor o conceito de irredutibilidade de polinômios, vamos considerar a seguinte definição.

DEFINIÇÃO 2

Dizemos que um corpo $\boldsymbol{B}$ é uma *extensão* do corpo $\boldsymbol{A}$ se $\boldsymbol{A} \subset \boldsymbol{B}$.

Assim, por exemplo, o corpo $\boldsymbol{R}$ dos números reais é uma extensão do corpo $\boldsymbol{Q}$ dos números racionais. O corpo $\boldsymbol{C}$ dos números complexos é uma extensão tanto de $\boldsymbol{R}$ quanto de $\boldsymbol{Q}$.

Veja que na Definição 1 tratamos de um polinômio irredutível *sobre* $\boldsymbol{K}$, e não somente de um polinômio irredutível. Isto se deve ao fato do um polinômio poder ser irredutível sobre um corpo $\boldsymbol{K}$, porém redutível sobre um corpo L que seja uma extensão de $\boldsymbol{K}$. No Exemplo 1, vimos que $f(x) = x^2 - 2$ é irredutível em $\boldsymbol{Q}[x]$, mas é redutível em $\boldsymbol{R}[x]$.

ATIVIDADE

1. Verifique se o polinômio $f(x) = x^2 + 4$ é irredutível em $\boldsymbol{Q}[x]$, $\boldsymbol{R}[x]$ e $\boldsymbol{C}[x]$.

O próximo exemplo mostra que para verificar se um polinômio $f(x)$, de grau três, é irredutível sobre um corpo K basta verificar se $f(x)$ possui raízes em K.

Exemplo 2

Considere o polinômio $f(x) = x^3 + \overline{3}x + \overline{2} \in Z_5[x]$. Vejamos se $f(x)$ é irredutível em $Z_5[x]$. Se isso não acontecer, ou seja, se, $f(x)$ for redutível em $Z_5[x]$, então existe um polinômio $g(x) \in Z_5[x]$, de grau dois, e um polinômio $ax + b \in Z_5[x]$, de grau um, tal que

$$f(x) = (ax + b)g(x).$$

Observe que o polinômio linear $ax + b \in Z_5[x]$ tem uma raiz $-b \cdot a^{-1} \in Z_5$. Portanto, $f(x)$ é redutível em $Z_5[x]$ se, e somente se, $f(x)$ possuir uma raiz $a \in Z_5$. Verificando os valores de $f(x)$ para cada elemento de $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$, temos

$$f(\overline{0}) = (\overline{0})^3 + \overline{3} \cdot \overline{0} + \overline{2} = \overline{2} \neq \overline{0};$$
$$f(\overline{0}) = (\overline{1})^3 + \overline{3} \cdot \overline{1} + \overline{2} = \overline{6} = \overline{1} \neq \overline{0};$$
$$f(\overline{2}) = (\overline{2})^3 + \overline{3} \cdot \overline{2} + \overline{2} = \overline{16} = \overline{1} \neq \overline{0};$$
$$f(\overline{3}) = f(\overline{-2}) = (\overline{-2})^3 + \overline{3}.(\overline{-2}) + \overline{2} = \overline{-12} = \overline{3} \neq \overline{0};$$
$$f(\overline{4}) = f(\overline{-1}) = (\overline{-1})^3 + \overline{3}.(\overline{-1}) + \overline{2} = \overline{-2} = \overline{3} \neq \overline{0}.$$

Concluímos, assim, que $f(x) = x^3 + \overline{3}x + \overline{2}$ não possui raízes em $Z_5[x]$. Portanto, $f(x)$ não é redutível em $Z_5[x]$, ou seja, $f(x)$ é irredutível em $Z_5[x]$.

Veja que esses dois exemplos nos fornecem um critério para saber se um polinômio $f(x)$, de grau dois ou três, é irredutível sobre um corpo K. Basta verificar se $f(x)$ possui raízes em K. Este critério torna-se prático sempre que o corpo K for finito e com poucos elementos, ou quando pudermos restringir os candidatos a raiz a uns poucos elementos, como no caso da propriedade das raízes racionais, vista na Aula 15. Com isso podemos caracterizar a irredutibilidade de todos os polinômios de graus 1, 2 e 3. Lembre que estamos considerando K um corpo. Mais precisamente temos:

Proposição 1 (Irredutibilidade de polinômios de grau 1, 2 e 3)

Sejam K um corpo e $K[x]$ o anel de polinômios. Então,

1. Todo polinômio $f(x) \in K[x]$, de grau 1, é irredutível em $K[x]$.

2. Seja $f(x) \in K[x]$ um polinômio de grau 2 ou 3. Então, $f(x)$ é irredutível em $K[x]$ se, e somente se, $f(x)$ não possuir raízes em K. Equivalentemente, $f(x)$ é redutível em $K[x]$ se, e somente se, $f(x)$ possuir alguma raiz em K.

Demonstração

1. Seja $f(x) \in K[x]$ de grau 1. Se $f(x)$ fosse redutível em $K[x]$, existiriam polinômios $f(x), h(x) \in K[x]$ tais que

$$f(x) = g(x)h(x) \text{ com } gr(g(x)) < gr(g(x)) = 1 \text{ e } gr(h(x)) < gr(f(x)) = 1.$$

Portanto, teríamos que

$$gr(g(x)) = gr(h(x)) = 0,$$

ou seja, $g(x)$ e $h(x)$ seriam polinômios constantes, o que tornaria a igualdade $f(x) = g(x)h(x)$ impossível, já que, de um lado, temos um polinômio de grau um e, do outro, teríamos um polinômio de grau 0. Assim, concluímos que todo polinômio de grau um é irredutível num corpo K.

2. Seja $f(x) \in K[x]$ de grau 2 ou 3.

Suponhamos, primeiramente, que $f(x)$ seja redutível em $K[x]$. Como $f(x)$ tem grau 2 ou então existe um polinômio $ax + b \in K[x]$, de grau um, e um polinômio $g(x) \in K[x]$, também de grau um quando $f(x)$ tem grau 2, ou de grau 2 quando $f(x)$ tem grau 3, tal que

$$f(x) = (ax + b)g(x).$$

Veja que o polinômio linear $ax + b \in K[x]$ tem uma raiz $-b \cdot a^{-1} \in K$. Como $(ax + b) \mid f(x)$, concluímos que $-b \cdot a^{-1} \in K$ também é raiz de $f(x)$. Observe que, neste passo, é fundamental que K seja um corpo

($\Leftarrow$) Vamos supor, agora, que $f(x)$ possua uma raiz $\alpha \in K$. Então, pela propriedade do fator linear, vista na Aula 15, teremos que $(x - \alpha) \mid f(x)$. Logo, existe $g(x) \in K[x]$ tal que

$f(x) = (x - \alpha)g(x)$ com $g(x - \alpha) = 1 < gr(f(x))$ e $gr(f(x)) = 1$ ou $2 < gr(f(x))$.

Portanto, $f(x)$ é redutível em $K[x]$.

Na verdade, podemos generalizar um pouco a parte ($\Leftarrow$) da demonstração anterior. Tente você provar esta generalização na próxima atividade.

ATIVIDADE

2. Prove que se $f(x) \in K[x]$ for um polinômio de grau maior que um e tiver uma raiz em K, então $f(x)$ é redutível em $K[x]$. Ou, equivalentemente, se é irredutível em $K[x]$, então $f(x)$ não possui raízes em K.

_____

_____

_____

_____

Observação

A recíproca do resultado da atividade é falsa, ou seja, é falso em geral que se $f(x)$ é redutível em $K[x]$, então $f(x)$ tem uma raiz em K. Um contra-exemplo pode ser dado pelo polinômio $f(x) = x_4 - 4 \in Q[x]$. Como

$$f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2),$$

então $f(x)$ é redutível em $Q[x]$ e, no entanto, as raízes de $f(x)$ não são racionais, pois $\pm\sqrt{2}, \pm\sqrt{2i} \notin Q$.

Exemplo 3

Verifique se o polinômio $f(x) = x^3 - 4$ é irredutível em $\mathbf{Q}[x]$, $\mathbf{Q}[x]$ e $\mathbf{C}[x]$. Veja que na busca por raízes reais, temos que

$$f(x) = 0 \Leftrightarrow x^3 = 2 \Leftrightarrow x = \sqrt[3]{2}.$$

Portanto, $\sqrt[3]{2}$ é a única raiz real de $f(x) = x^3 - 2$. Como $\sqrt[3]{2} \notin \mathbf{Q}$, então, pela Proposição 1.2, segue que $f(x) = x^3 - 2$ é irredutível em $\mathbf{Q}[x]$. No entanto, como $\sqrt[3]{2} \in \mathbf{R} \subset \mathbf{C}$, então segue que é redutível em $\mathbf{R}[x]$ e em $\mathbf{C}[x]$. Aliás, você lembra como se prova que $\sqrt[3]{2} \notin \mathbf{Q}$?

Exemplo 4

Vamos determinar todos os polinômios irredutíveis de grau 2 em $\mathbf{Z}_2[x]$. Estes polinômios são da forma

$$x^2 + ax + b \text{ com } a, b \in \mathbf{Z}_2.$$

Como $\mathbf{Z}_2 = \{\overline{0}, \overline{1}\}$ só tem dois elementos, podemos escrever todos estes polinômios:

$$x^2,\ x^2 + x,\ x^2 + \overline{1} \text{ e } x^2 + x + \overline{1}.$$

Isto é, só existem 4 polinômios de grau 2 em $\mathbf{Z}_2[x]$. Destes, o único que não possui raiz em $\mathbf{Z}_2$ é $x^2 + x + \overline{1}$. Assim, $x^2 + x + \overline{1}$ é o *único* polinômio irredutível de grau 2 em $\mathbf{Z}_2[x]$.

Antes de enunciar a sua próxima atividade, lembremos o que é um polinômio mônico. Dizemos que o polinômio

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

é *mônico* se seu coeficiente líder for igual 1, isto é, se $a_n = 1$, ou seja, se

$$f(x) = x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0.$$

Agora sim, convidamos a resolver a sua terceira atividade; uma dica que damos para você é usar um argumento similar ao usado no Exemplo 4.

ATIVIDADE

3. Determine todos os polinômios mônicos irredutíveis de grau 2 em $Z_3[x]$.

_____

_____

_____

_____

Antes de continuar com a nossa teoria, vejamos mais um exemplo:

Exemplo 5

Vamos determinar se o polinômio $g(x) = x^4 - 6x^2 + 8 \in \boldsymbol{Q}[x]$ é irredutível ou não em $\boldsymbol{Q}[x]$.

Vejamos, primeiramente, se ele tem raízes racionais. Sabemos que as possíveis raízes racionais de $g(x)$ são $\{\pm 1, \pm 2, \pm 4, \pm 8\}$. Verificamos rapidamente que $g(-1) \neq 0$, e $g(2) = g(-2) = 0$. Isto é, 2 e –2 são raízes de $g(x)$. Assim, em particular, $g(x)$ é redutível em $\boldsymbol{Q}[x]$. Agora, aplicando duas vezes Briot-Ruffini, temos

1	0	–6	0	8	2
1	2	–2	–4	0	–2
1	0	–2	0		

o que nos dá

$$\begin{aligned} g(x) &= x^4 - 6x^2 + 8 \\ &= (x + 2)(x - 2)(x^2 - 2). \end{aligned}$$

Assim, escrevemos $g(x)$ como um produto de polinômios irredutíveis em $\boldsymbol{Q}[x]$. Veremos, mais adiante, que isto é um fato geral no anel de polinômios $\boldsymbol{K}[x]$.

Vamos continuar procurando critérios para decidir sobre a irredutibilidade de polinômios. O seguinte critério é muito útil para determinar se certos polinômios com coeficientes inteiros são irredutíveis sobre $\boldsymbol{Q}$.

Proposição 6 (Critério de Irredutibilidade de Eisenstein)

Sejam $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_2x^2 + a_1x + a_0 \in \mathbf{Z}[x]$ e um número primo p tal que p divide cada coeficiente a_i, para $i = 1, 2, 3, ..., n - 1$; p não divide a_n e p^2 não divide a_0. Então $f(x)$ é irredutível em $\mathbf{Q}[x]$.

Antes de dar alguns exemplos onde mostraremos a utilidade deste critério, achamos pertinente fazer algumas observações.

O Critério de Einsenstein diz que se os coeficientes de um polinômio $f(x) \in \mathbf{Z}[x]$ satisfazem certas condições para um primo p, então ele não pode ser escrito como o produto de dois polinômios em $\mathbf{Q}[x]$, com grau menor que o grau de $f(x)$. Podemos usar este critério no caso de o polinômio $f(x)$ ter coeficientes racionais. Para isso, observe que se

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_2x^2 + a_1x + a_0 \in \mathbf{Q}[x],$$

então podemos achar um inteiro d e um polinômio $g(x) \in \mathbf{Z}[x]$ tais que

$$d \,.\, f(x) = g(x) \text{ com } gr(g(x)) = gr(f(x)).$$

Podemos, então, aplicar o critério de Einsenstein aos coeficientes de $g(x)$. E, obviamente, se $g(x)$ for irredutível em $\mathbf{Q}[x]$, então $f(x)$ também será irredutível em $\mathbf{Q}[x]$. O seguinte exemplo mostra a utilidade deste critério.

Exemplo 6

Vejamos que o polinômio $f(x) = x^4 + 4x - 2$ é irredutível sobre $\mathbf{Q}$. De fato, tomando o primo 2, vemos que 2 não divide o coeficiente $a_4 = 1$, divide os coeficientes $a_3 = 0$, $a_2 = 0$, $a_1 = 4$ e $a_0 = -2$, mas $2^2 = 4$ não divide o coeficiente $a_0 = -2$. Portanto, pelo critério de Eisenstein, temos que $f(x)$ é irredutível em $f(x)$ em $\mathbf{Q}[x]$. Em particular, $f(x)$ não tem raiz racional. Observe que a aplicação do critério independe do grau do polinômio $f(x)$.

O próximo exemplo mostra que, em caso de não existir um primo p satisfazendo as condições do critério, então não podemos concluir nada a respeito da irredutibilidade $f(x)$.

Exemplo 7

O polinômio $f(x) = x^2 + 1$ é irredutível em $\mathbf{Q}[x]$ e não existe nenhum inteiro primo p satisfazendo as condições do critério. Por outro lado, o polinômio $f(x) = x^2 - 1$ é redutível em $\mathbf{Q}[x]$ e também não existe um primo p que satisfaça as condições do critério.

Você deve lembrar que no início da aula dissemos que os polinômios irredutíveis num corpo $\boldsymbol{K}$ tem um comportamento análogo aos números primos p no anel dos inteiros $\boldsymbol{Z}$. Uma das propriedades mais importantes dos números primos diz que qualquer inteiro positivo n pode ser escrito como um produto de números primos. Pois bem, uma propriedade análoga também vale no anel $\boldsymbol{K}[x]$.

Teorema 1

Sejam $\boldsymbol{K}$ um corpo e $f(x) \in \boldsymbol{K}[x]$ um polinômio não constante, então existem polinômios irredutíveis, $P_1(x)$, $P_2(x)$, ... , $P_n(x)$, em $\boldsymbol{K}[x]$ tais que

$$f(x) = P_1(x) \, . \, P_2(x) ... \, P_n(x).$$

Esta igualdade é conhecida como a Decomposição de $f(x)$ em polinômios *irredutíveis*.

Exemplo 8

Vamos expressar os seguintes polinômios como um produto de irredutíveis em $\boldsymbol{K}[x]$.

1. $f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2)$ em $\mathbf{Q}[x]$.
2. $f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x^2 + 2)$ em $\boldsymbol{R}[x]$.
3. $f(x) = x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x^2 + \sqrt{2})(x^2 - \sqrt{2})$ $= (x - \sqrt{2})(x - \sqrt{2})(x - \sqrt{2}i)(x + \sqrt{2}i)$ em $\mathbf{C}[x]$.

Para finalizar esta aula, convidamos você a realizar as seguintes atividades finais.

ATIVIDADES FINAIS

1. Determine todos os polinômios irredutíveis de grau 3 em $Z_2[x]$.

2. Mostre que $f(x) = x^5 - 9x^3 + 9x - 6$ é irredutível em $Q[x]$.

3. Escreva o polinômio $f(x) = x^5 + x^4 + x^2 - \overline{1}$ como um produto de polinômios irredutíveis em $Z_2[x]$.

RESUMO

Nesta aula, vimos que $f(x) \in K[x]$ é um polinômio *irredutível* sobre ***K***, ou *irredutível* em $K[x]$, se seus únicos divisores em $K[x]$ forem os polinômios constantes e os múltiplos constantes dele mesmo, ou seja, se

$$g(x) \mid f(x) \text{ com } g(x) \in K[x] \Rightarrow g(x) = c \text{ constante ou } g(x) = c\, f(x).$$

Dizemos que $f(x)$ é *redutível em* $K[x]$ quando ele não for irredutível, ou seja, quando existirem polinômios $g(x)$, $g(x) \in K[x]$ tais que

$$f(x) = g(x)h(x) \text{ com } gr(g(x)) < gr(f(x)) \text{ e } gr(h(x)) < gr(f(x)).$$

Vimos que quando o grau do polinômio é 1, 2 ou 3, determinar a irredutibilidade de um polinômio é bastante fácil. Mais precisamente, temos que:

1. Todo polinômio $f(x) \in K[x]$, de grau 1, é irredutível em $K[x]$.

2. Se $f(x) \in K[x]$ tem grau 2 ou 3, então $f(x)$ será irredutível em $K[x]$ se, e somente se, $f(x)$ não possuir raízes em K ou, equivalentemente, $f(x)$ será redutível em $K[x]$ se, e somente se, $f(x)$ possuir alguma raiz em K.

Depois, apresentamos um critério para estudar a irredutibilidade de certos polinômios com coeficientes racionais. É o chamado Critério de Eisenstein, que diz que se

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \in Z[x]$$

e existe um número primo p tal que p divide cada coeficiente a_i, para $i = 1, 2, 3, \ldots, n-1$, p não divide a_n e p^2 não divide a_0, então $f(x)$ é irredutível em $Q[x]$.

Finalmente, apresentamos um resultado que afirma que qualquer polinômio não constante com coeficientes num corpo K pode ser escrito como um produto de polinômios irredutíveis.

RESPOSTAS COMENTADAS

Atividade 1

Como

$$f(x) = x^2 + 4$$

$$= (x - 2i)(x + 2i),$$

então as raízes de $f(x)$ são $\pm 2i$. Como $\pm 2i \notin R$ e, portanto, $\pm 2i \notin Q$, então segue que $f(x)$ é irredutível em $Q[x]$ e $R[x]$. Como mostra a decomposição anterior, $f(x)$ é redutível em $C[x]$.

Atividade 2

Vamos supor que $f(x)$ possui uma raiz $\alpha \in Z$ e que $gr(f(x)) = n > 1$. Então, pela propriedade do fator linear, vista na Aula 10, temos que $(x - \alpha) \mid f(x)$. Logo, existe $g(x) \in K[x]$, polinômio não constante, tal que

$f(x) = (x - \alpha)g(x)$ com $gr(x - \alpha) = > 1\ n = gr(f(x))$ e $gr(g(x)) = n - 1 < n = gr(f(x))$.

Portanto, $f(x)$ é redutível em $K[x]$.

Atividade 3

Estes polinômios são da forma

$$x^2 + ax + b \text{ com } a, b \in Z_3.$$

Como $Z_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ só tem três elementos, podemos escrever todos estes polinômios:

x^2, $x^2 + x$, $x^2 + \overline{1}$, $x^2 + \overline{2}x$, $x^2 + \overline{2}$, $x^2 + x + \overline{1}$, $x^2 + \overline{2}x + \overline{1}$, $x^2 + x + \overline{2}$ e $x^2 + \overline{2}x + \overline{2}$.

Destes, você pode verificar que $x^2 + \overline{1}$, $x^2 + x$, $\overline{2}$ e $x^2 + \overline{2}x + \overline{2}$ não possuem raiz em Z_3. Logo, estes são os polinômios mônicos irredutíveis de grau 2 em $Z_3[x]$.

Atividade Final 1

Vamos determinar todos os polinômios irredutíveis de grau 3 em $Z_2[x]$. Estes polinômios são da forma

$$x^3 + ax^2 + bx + x^2 \text{ com } a, b, c \in Z_2.$$

Como $Z_2 = \{\overline{0}, \overline{1}\}$ só tem dois elementos, podemos escrever todos estes polinômios:

x^3, $x^3 + x^2$, $x^3 + x$, $x^3 + \overline{1}$, $x^3 + x^2 + x$, $x^3 + x^2 + \overline{1}$, $x^3 + x + \overline{1}$, e $x^3 + x^2 + x + \overline{1}$.

Isto é, existem 8 polinômios de grau 3 em $Z_2[x]$. Destes, os únicos que não possuem raiz em Z_2 são $x^3 + x^2 + \overline{1}$ e $x^3 + x + \overline{1}$. Assim, $x^3 + x^2 + \overline{1}$ e $x^3 + x + \overline{1}$ são os únicos polinômios irredutíveis de grau 3 em $Z_2[x]$.

Atividade Final 2

O primo 3 divide os coeficientes $a_4 = 0$, $a_3 = -9$, $a_1 = 9$, e $a_3 = -6$, mas $3^2 = 9$ não divide o coeficiente $a_0 = -6$. Portanto, pelo critério de Eisenstein, segue a irredutibilidade de $f(x)$ em $Q[x]$. Em particular, $f(x)$ não tem raiz racional.

Atividade Final 3

Como $f(\overline{1}) = f(\overline{1}) + (\overline{1}) + (\overline{1}) + \overline{1} = \overline{4} = \overline{0}$, então $(x - \overline{1}) \mid f(x)$. Aplicando Briot-Ruffini, temos

$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{1}$
$\overline{1}$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{0}$	

o que significa que

$$\begin{aligned} f(x) &= x^5 + x^4 + x^2 + \overline{1} \\ &= (x - \overline{1})(x^4 + x + \overline{1}) \end{aligned}$$

Denotando $g(x) = x^4 + x + x^2 + \overline{1}$, temos

$$g(\overline{0}) = (\overline{0}) + \overline{0} + \overline{1} = \overline{1} \neq \overline{0} \text{ e } g(\overline{1}) = (\overline{1})^4 + \overline{1} + \overline{1} = \overline{3} = \overline{1} \neq \overline{0},$$

portanto, não existe polinômio linear que divida $g(x)$. Assim, se $g(x)$ for redutível em $Z_2[x]$, então a decomposição será da forma

$$g(x) = x^4 + x + \overline{1} = (x^2 + ax + \overline{1})(x^2 + bx + \overline{1}).$$

Desenvolvendo o produto da direita, temos

$$\begin{aligned} x^4 + x + \overline{1} &= (x^2 + ax + \overline{1})(x^2 + bx + \overline{1}) \\ &= x^4 + (a + b)x^3 + (ab + \overline{1} + \overline{1})x^2 + (a + b)x + \overline{1} \\ &= x^4 + (a + b)x^3 + (ab + \overline{0})x^2 + (a + b)x + \overline{1} \\ &= x^4 + (a + b)x^3 + abx^2 + (a + b)x + \overline{1}, \end{aligned}$$

e, igualando os coeficientes, temos

$$\begin{cases} a + b = \overline{0} \\ ab = \overline{0} \\ a + b = \overline{1} \end{cases}$$

De $a + b = \overline{0}$ e $a + b = \overline{1}$, temos uma contradição. Logo, concluímos que $g(x)$ é irredutível em $\mathbb{Z}_2[x]$ e, portanto, a decomposição de $f(x)$ em um produto de polinômios irredutíveis em $\mathbb{Z}_2[x]$ é dada por

$$\begin{aligned} f(x) &= x^5 + x^4 + x^2 + \overline{1} \\ &= (x - \overline{1})(x^4 + x + \overline{1}). \end{aligned}$$

Introdução aos grupos

AULA 12

Meta da aula

Apresentar o conceito de grupo.

objetivos

Ao final desta aula, você deverá ser capaz de:

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

Pré-requisito

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I.

INTRODUÇÃO

Em Álgebra I e até a Aula 11, estudamos diversos aspectos da estrutura algébrica chamada de anel, mais particularmente, dos anéis comutativos e com unidade. Você deve se lembrar de que desenvolvemos o conceito de anel querendo generalizar o anel dos números inteiros e, assim, generalizamos muitas das suas propriedades algébricas. Vimos que a noção de anel nos permitiu desenvolver de uma forma muito elegante a teoria dos polinômios.

A teoria dos anéis pressupõe a ação de duas operações binárias, num conjunto não-vazio A, satisfazendo uma certa quantidade de axiomas. Vamos, agora, estudar a ação de apenas uma operação binária, sobre um conjunto não-vazio G, satisfazendo alguns daqueles axiomas. Esta nova estrutura algébrica é o que chamaremos de grupo. A estrutura de grupo é matematicamente relevante, porque ela aparece com muita freqüência em muitas áreas da Matemática e na natureza.

Nesta aula vamos, inicialmente, estabelecer os conceitos iniciais de grupos e, em seguida, estudar uma quantidade de exemplos.

DEFINIÇÃO 1 (DEFINIÇÃO DE GRUPO)

Um *grupo* é um conjunto não-vazio G, munido de uma operação binária (denotada, geralmente, por $\cdot$ ou $+$) que satisfaz os seguintes axiomas:

G1. A operação é *associativa*: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$;

G2. A operação tem um *elemento neutro*: existe um elemento $e \in G$, tal que $a \cdot e = e \cdot a = a$, para todo $a \in G$;

G3. Todo elemento de G possui um *elemento inverso*: para todo $a \in G$, existe um $a' \in G$, tal que, $a \cdot a' = a' \cdot a = e$.

Observações

1. Observe que ao exigir que a operação $\cdot$ seja uma operação binária em G, já estamos exigindo que ela seja *fechada* em G, isto é, dados $a, b \in G$, então $a \cdot b \in C$.

2. O elemento neutro é único: se $e' \in G$ é tal que $a \cdot e' = e' \cdot a = a$, então $e' = e$. Pois,

$e' = e \cdot e'$; usando que e é um elemento neutro.
$= e$; usando que e' é um elemento neutro.

O elemento neutro do grupo também é, muitas vezes, denotado por e_G , quando queremos ressaltar o grupo G; por 1 ou 1_G, quando a operação é uma multiplicação; e por 0 ou 0_G, quando a operação é uma adição. Nesse último caso, é costume denotar a operação por +.

3. O elemento inverso é único: dado $a \in G$, seja $a" \in G$, tal que $a \cdot a" = a" \cdot a = e$, então $a" = a'$. Pois,

$a" = e \cdot a"$; usando que e é um elemento neutro.
$= (a' \cdot a) \cdot a"$; usando que a' é um elemento inverso de a.
$= a' \cdot (a \cdot a")$; usando que a operação é associativa.
$= a' \cdot e$; usando que $a"$ é um elemento inverso de a
$= a'$; usando que e é o elemento neutro.

Como o elemento inverso é único, podemos denotá-lo por a^{-1}. Daí, temos $a \cdot a^{-1} = a^{-1} \cdot a = e$.

4. Denotamos um grupo por $(G, \cdot)$ ou $(G, +)$, dependendo de como consideramos a operação, uma multiplicação ou uma adição. Quando a operação estiver clara no contexto, então denotaremos o grupo simplesmente por G. Também, muitas vezes, denotamos o produto $a \cdot b$ simplesmente por ab.

Veja dois exemplos iniciais.

Exemplo 1

Seja $(\mathbf{Z}, +, \cdot)$ o anel dos números inteiros. Então, dos axiomas satisfeitos pela operação de adição, temos que $(\mathbf{Z}, +)$ é um grupo. O elemento neutro é 0 e o inverso aditivo de $a \in \mathbf{Z}$ é o elemento simétrico $-a$.

Exemplo 2

Seja $(\boldsymbol{Z}_n, +, \cdot)$ o anel das classes residuais módulo n. Então, dos axiomas satisfeitos pela operação de adição das classes residuais, temos que $(\boldsymbol{Z}_n, +)$ é um grupo. O elemento neutro é $\overline{0}$ e o inverso aditivo de é $a \in \boldsymbol{Z}_n$ é o elemento simétrico $-a$.

Vejamos duas propriedades básicas de grupos.

Proposição 1

Sejam $\boldsymbol{G}$ um grupo e $a, b, c \in \boldsymbol{G}$.

1. A equação $a \cdot x = b$ admite uma única solução em G, a saber, $x = a^{-1} \cdot b$.
2. $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.
3. (Lei do Cancelamento) Se $a \cdot b = a \cdot c$, então $b = c$.
   Se $b \cdot a = c \cdot a$, então $b = c$.

Demonstração

1. Observe, inicialmente, que $x = a^{-1} \cdot b$ é uma solução de $a \cdot x = b$, pois

$$\begin{aligned} a \cdot x &= a \cdot (a^{-1} \cdot b); \text{ pela definição de } x \\ &= (a \cdot a^{-1}) \,.\, b; \text{ pelo axioma } G1 \\ &= e \cdot b; \text{ pelo axioma } G3 \\ &= b; \text{ pelo axioma } G2 \end{aligned}$$

Agora, a solução é única, pois dada qualquer solução $y \in G$, temos

$$\begin{aligned} a \cdot y = b \;&\Rightarrow\; a^{-1} \cdot (a \cdot y) = a^{-1} \,.\, \text{b; multiplicando por } a^{-1} \\ &\Rightarrow\; (a^{-1} \cdot a) \cdot y = a^{-1} \,.\, \text{b; pelo axioma } \boldsymbol{G}1 \\ &\Rightarrow\; e \cdot y = \text{a}^{-1} \cdot b; \text{ pelo axioma } \boldsymbol{G}3 \\ &\Rightarrow\; y = a^{-1} \cdot \text{b; pelo axioma } \boldsymbol{G}2 \end{aligned}$$

2. Observe que $b^{-1}.\, a^{-1}$ satisfaz o axioma do elemento inverso para $a \cdot b$:

$$\begin{aligned} (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= a \cdot (b \cdot b^{-1}) \,.\, a^{-1}; \text{ pelo axioma G1} \\ &= a \cdot e \cdot a^{-1}; \text{ pelo axioma G3} \\ &= (a \cdot e) \cdot a^{-1}; \text{ pelo axioma G1} \\ &= a \cdot a^{-1}; \text{ pelo axioma G2} \\ &= e; \text{ pelo axioma G3.} \end{aligned}$$

Faça, como sua primeira atividade desta aula, a demonstração de $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$.

ATIVIDADE

1. Prove que $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$, justificando cada igualdade usada.

_____

_____

_____

Assim, provamos que $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e$. Logo, pela unicidade do elemento inverso, temos que $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

3. Temos

$$\begin{aligned} b &= e \cdot b; \text{ pelo axioma } G2 \\ &= (a^{-1} \cdot a) \cdot b; \text{ pelo axioma } G3 \\ &= a^{-1} \cdot (a \cdot b); \text{ pelo axioma } G1 \\ &= a^{-1} \cdot (a \cdot c); \text{ pela hipótese} \\ &= (a^{-1} \cdot a) \cdot c; \text{ pelo axioma } G1 \\ &= e \cdot c; \text{ pelo axioma } G3 \\ &= c; \text{ pelo axioma } G2. \end{aligned}$$

Portanto, provamos que $b = c$.

ATIVIDADE

2. Prove a segunda parte da lei do cancelamento, ou seja, prove que se $b \cdot a = c \cdot a$, então $b = c$.

_____

_____

_____

Vamos ver, agora, duas definições muito importantes.

DEFINIÇÃO 2 (GRUPO ABELIANO)

Um grupo G é chamado de grupo *abeliano* (ou, grupo *comutativo*) se $a \cdot b = b \cdot a$ para todo $a, b \in G$.

Observe que se G é um grupo abeliano, então $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. Prove isso como sua próxima atividade.

ATIVIDADE

3. Prove que se G é um grupo abeliano, então $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

_____

_____

_____

DEFINIÇÃO 3 (GRUPO FINITO)

Um grupo G é chamado de grupo *finito*, quando G contiver um número finito de elementos. Neste caso, a *ordem* de G|, denotada por |G|, é o número de elementos de G. Quando G *não* é um grupo finito, dizemos que G é um grupo de *ordem infinita*, ou seja, isto ocorre quando o grupo G contém infinitos elementos.

Vamos aos exemplos.

Exemplo 3

Como a operação de adição dos números inteiros é comutativa, então ($\mathbf{Z}$, +) é um grupo abeliano. Veja que ($\mathbf{Z}$, +) é um grupo de ordem infinita, pois $\mathbf{Z}$ contém uma quantidade infinita de elementos.

Exemplo 4

Como a operação de adição das classes residuais módulo n é comutativa, então $(\mathbf{Z}_n, +)$ é um grupo abeliano. Veja que $(\mathbf{Z}_n, +)$ é um grupo finito, pois $\mathbf{Z}_n = \{\overline{0}, \overline{1},..., \overline{n-1}\}$ contém uma quantidade finita de elementos, a saber, $(\mathbf{Z}_n, +)$ é um grupo de ordem n. Denotamos isso por $| \mathbf{Z}_n | = n$.

Exemplo 5

Observe que $(Z, \cdot)$ o conjunto dos números inteiros munido da operação de multiplicação não forma um grupo, pois o axioma G3, do elemento inverso, não é satisfeito. Por exemplo, o número inteiro 2 não possui inverso multiplicativo, isto é, não existe inteiro a tal que $2 \cdot a = 1$.

ATIVIDADE

4. Prove que (Q, +) o conjunto dos números racionais munido da operação de adição é um grupo abeliano de ordem infinita.

Exemplo 6

De um modo geral, se $(A, +, \cdot)$ é um anel, então $(A, +)$ é um grupo abeliano. A correspondência entre os axiomas de anel e os de grupo é como segue:

A1 $\leftrightarrow$ G1
A3 $\leftrightarrow$ G2
A4 $\leftrightarrow$ G3
A2 $\leftrightarrow$ Condição de grupo abeliano

No entanto, em geral, $(\boldsymbol{A}, \cdot)$ não é um grupo. E se $A^* = A - \{0_A\}$, mesmo $(\boldsymbol{A}^*, \cdot)$, em geral, não é um grupo. Como mostra o Exemplo 5, $(\boldsymbol{Z}, \cdot)$ e $(\boldsymbol{Z}^*, \cdot)$ não são grupos, pois o axioma G3 não é satisfeito.

Exemplo 7

Temos que $(\boldsymbol{Q}^*, \cdot)$, o conjunto dos números racionais não-nulos munido da operação de multiplicação, é um grupo abeliano de ordem infinita. Pois, como $(\boldsymbol{Q}, +, \cdot)$ é um corpo, então, dos axiomas satisfeitos pela operação de multiplicação, temos que $(\boldsymbol{Q}^*, \cdot)$ é um grupo abeliano. O elemento neutro é 1 e o elemento inverso de $\frac{a}{b} \in \boldsymbol{Q}^*$ é o elemento $\frac{b}{a} \in \boldsymbol{Q}^*$. Como $\boldsymbol{Q}^*$ é um conjunto infinito, segue que $(\boldsymbol{Q}, \cdot)$ é um grupo de ordem infinita.

Exemplo 8

De um modo geral, se $(\boldsymbol{A}, +, \cdot)$ é um corpo e $\boldsymbol{A}^* = \mathrm{A} - \{0_A\}$, então $(\boldsymbol{A}^*, \cdot)$ é um grupo abeliano. A correspondência entre os axiomas de anel e os de grupo é como segue:

A5 $\leftrightarrow$ G1
A7 $\leftrightarrow$ G2 (Veja que, $e = 1_A$.)
Condição de corpo (todo elemento não-nulo é invertível) $\leftrightarrow$ G3
A6 $\leftrightarrow$ Condição de grupo abeliano

Observe que, mesmo que (A, +, ·) seja um corpo, (A, ·) não é um grupo. Pois, como $0_A \in \boldsymbol{A}$, então

$$0_A \cdot 1_A = 0_A \neq 1_A$$

e, portanto, o axioma G2 não é satisfeito.

Exemplo 9

Dado o anel $(\boldsymbol{Z}_n, +, \cdot)$, seja $\boldsymbol{Z}^{\times}_n = \{\overline{a} \in \boldsymbol{Z}_n \mid mdc(a, n) = 1\}$. Então, $(\boldsymbol{Z}^{\times}_n, \cdot)$ é um grupo abeliano de ordem finita. Vamos verificar os axiomas.

G1. Como $(\mathbf{Z}_n, +, \cdot)$ é anel, então já sabemos que a operação de multiplicação de classes residuais é associativa.

G2. Como $\overline{1} \in \mathbf{Z}^{\times}_n$, esse é o elemento neutro: $\overline{a} \,.\, \overline{1} = \overline{1} \,.\, \overline{a} = \overline{a}$.

G3. Sabemos, da Álgebra I, que $\overline{a} \in \mathbf{Z}_n$ é um elemento invertível se, e somente se, $mdc(a, n) = 1$. Portanto, todo elemento $a \in \mathbf{Z}_n$ é invertível.

Grupo abeliano: como a operação de multiplicação de classes residuais é comutativa, segue que $(\mathbf{Z}^{\times}_n, \cdot)$ é um grupo abeliano.

Grupo finito: Como $\mathbf{Z}_n$ é um conjunto finito, então $\mathbf{Z}^{\times}_n$ também é. Logo, $(\mathbf{Z}^{\times}_n, \cdot)$ é um grupo finito.

Exemplo 10

Se p for um número primo então $\mathbf{Z}^{\times}_p = \{\overline{a} \in \mathbf{Z}_p \mid mdc(a, p) = 1\} = \{\overline{1},..., \overline{p-1}\}$. Portanto, $(\mathbf{Z}^{\times}_p, \cdot)$ é um grupo abeliano finito de ordem $|\mathbf{Z}^{\times}_p| = p - 1$.

Observação

Vamos desenvolver a notação clássica para as potências de $a \in G$, onde G é um grupo. Temos:

$a^0 = e$, o elemento neutro de $\mathbf{G}$,

$a^n = a \,.\, a^{n-1} = a^{n-1}.\, a$, n inteiro e $n \geq 1$;

$a^{-n} = (a^{-1})n$, n inteiro e $n \geq 1$.

Nestas condições, vale que

$$a^{m+n} = a^m \,.\, a^n$$

e

$$a^{mn} = (a^m)^n, \text{ para todos os inteiros } m \text{ e } n.$$

ATIVIDADES FINAIS

1. Seja G um grupo. Prove que a equação $x \cdot a = b$ admite uma única solução em G, a saber, $x = b \cdot a^{-1}$.

2. Seja G um grupo. Dado $a \in G$, prove que $(a^{-1})^{-1} = a$.

RESUMO

Nesta aula vimos a importantíssima noção de grupo. Vimos que se G for um conjunto não-vazio munido de uma operação binária $\cdot$, então $(G, \cdot)$ será um grupo se os três axiomas:

G1. A operação for *associativa*: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, para todo $a, b, c \in G$;

G2. A operação tiver um *elemento neutro*: existe um elemento $e \in G$, tal que $a \cdot e = e \cdot a = a$, para todo $a \in G$;

G3. Todo elemento de G possuir um *elemento inverso*: para todo $a \in G$, existe um $a' \in G$, tal que, $a \cdot a' = a' \cdot a = e$.

O grupo G é abeliano se $a \cdot b = b \cdot a$ para todo $a, b \in G$. E, também, o grupo G é finito se G for um conjunto finito.

Vimos, também, muitos exemplos e algumas propriedades iniciais sobre os grupos.

RESPOSTAS COMENTADAS

Atividade 1

Temos que

$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b$; pelo axioma $G1$

$= b^{-1} \cdot e \cdot b$; pelo axioma $G3$

$= (b^{-1} \cdot e) \cdot b$; pelo axioma $G1$

$= b^{-1} \cdot b$; pelo axioma $G2$

$= e$; pelo axioma $G3$.

Atividade 2

Temos

$b = b \cdot e$; pelo axioma $G2$

$= b \cdot (a \cdot a^{-1})$; pelo axioma $G3$

$= (b \cdot a) \cdot a^{-1}$; pelo axioma $G1$

$= (c \cdot a) \cdot a^{-1}$; pelo hipótese

$= c \cdot (a \cdot a^{-1})$; pelo axioma $G1$

$= c \cdot e$; pelo axioma $G3$

$= c$; pelo axioma $G2$.

Portanto, provamos que $b = c$.

Atividade 3

Basta observar que

$(b \cdot a)^{-1} = b^{-1} \cdot a^{-1}$; pela proposição 1.2

$= a^{-1} \cdot b^{-1}$; pela comutatividade da operação.

Atividade 4

Como $(\mathbb{Q}, +, \cdot)$ é um anel, então, dos axiomas satisfeitos pela operação de adição, temos que $(\mathbb{Q}, +)$ é um grupo abeliano. O elemento neutro é 0 e o inverso aditivo de $\frac{a}{b} \in \mathbb{Q}$ é o elemento simétrico $\frac{-a}{b} \in \mathbb{Q}$. Como $\mathbb{Q}$ é um conjunto infinito, segue que $(\mathbb{Q}, +)$ é um grupo de ordem infinita.

Atividade Final 1

Observe, inicialmente, que $x = b \cdot a^{-1}$ é uma solução de $x \cdot a = b$, pois

$x \cdot a = (b \cdot a^{-1}) \cdot a$; pela definição de x

$= b \,.\, (a^{-1} \cdot a)$; pelo axioma $G1$

$= b \cdot e$; pelo axiona $G3$

$= b$; pelo axioma $G2$.

Agora, a solução é única, pois dada qualquer solução $y \in G$, temos

$y \cdot a = b \;\Rightarrow\; (y \cdot a) \cdot a^{-1} = b \,.\, a^{-1}$; multiplicando por a^{-1}

$\Rightarrow\; y \,.\, (a \cdot a^{-1}) = b \,.\, a^{-1}$; pelo axioma $G1$

$\Rightarrow\; y \,.\, e = b \,.\, a^{-1}$; pelo axioma $G3$

$\Rightarrow\; y = b \,.\, a^{-1}$; pelo axioma $G2$.

Atividade Final 2

Da equação $a \,.\, a^{-1} = a^{-1} \,.\, a = e$, segue que o elemento a faz o papel de um elemento inverso de a^{-1}. Logo, pela unicidade do elemento inverso, segue que $(a^{-1})^{-1} = a$.

Mais exemplos de grupos

AULA 13

Meta da aula

Apresentar exemplos importantes de grupos.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as propriedades que caracterizam um grupo.
- Reconhecer exemplos importantes de grupos.

Pré-requisitos

Você vai precisar dos conhecimentos desenvolvidos em Álgebra I e na Aula 12.

INTRODUÇÃO

O conceito de grupo se tornou tão importante na Matemática devido à identificação dessa estrutura algébrica em tantas áreas diferentes da própria Matemática e de outras ciências. Nesta aula, vamos estudar exemplos importantes de grupos vindos de diferentes áreas da Matemática.

Vamos iniciar retomando um exemplo da aula anterior que ressalta o conceito de tabela de multiplicação de um grupo. A tabela de multiplicação explicita todos os produtos de dois elementos do grupo e, portanto, define completamente a operação do grupo.

Exemplo 1

Considere $Z_5^x = \{\bar{a} \in Z_5 \mid mdc(a,5) = 1\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$. Vimos, na aula anterior, que $(Z_5, \cdot)$ é um grupo abeliano finito de ordem 4. Sua tabela de multiplicação é dada pelo esquema a seguir:

$\times$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Contamos as linhas a partir da primeira linha abaixo do símbolo $\times$ e contamos as colunas a partir da primeira coluna à direita de $\times$. Assim, o elemento situado na segunda linha e na terceira coluna é o valor $\bar{1}$, que representa o produto $\bar{2} \cdot \bar{3}$. Portanto, a leitura que fazemos é $\bar{2} \cdot \bar{3} = \bar{1}$. Da terceira linha e quarta coluna, temos $\bar{3} \cdot \bar{4} = \bar{2}$.

Exemplo 2

Considere $Z_8^x = \{\bar{a} \in Z_8^x \mid mdc(a, 8) = 1\} = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Sabemos que $(Z_8^x, .)$ é um grupo abeliano finito de ordem 4. Sua tabela de multiplicação é dada pelo esquema abaixo:

$\times$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

Observe neste exemplo, curiosamente, que todo elemento é o seu próprio inverso: $\bar{1} \cdot \bar{1} = \bar{1}$, $\bar{3} \cdot \bar{3} = \bar{1}$, $\bar{5} \cdot \bar{5} = \bar{1}$ e $\bar{7} \cdot \bar{7} = \bar{1}$.

Exemplo 3

O *grupo das permutações de 3 elementos:* S_3. Denotamos por S_3 o conjunto de todas as bijeções de {1, 2, 3}, ou seja,

$S_3 = \{\sigma:\{1, 2, 3\} \to \{1, 2, 3\} | \ \sigma \text{ é uma bijeção}\}$.

Lembre-se de que uma permutação de um conjunto é, exatamente, uma bijeção desse conjunto. Assim, cada bijeção $\sigma:\{1, 2, 3\} \to \{1, 2, 3\}$ representa uma permutação de {1, 2, 3}. Por exemplo, uma destas permutações tem como valores: $\sigma(1) = 2$, $\sigma(2) = 3$ e $\sigma(3) = 1$. É usual, em Álgebra, representar uma permutação da seguinte forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}.$$

Assim, a permutação cujos valores são $\sigma(1) = 2$, $\sigma(2) = 3$ e $\sigma(3) = 1$ é representada por

$$\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}.$$

A operação que consideraremos em S_3 é a composição de funções. Como a composição de duas bijeções é uma nova bijeção, essa operação está bem definida em S_3. Lembre que composição de funções é definida da seguinte forma: dadas duas bijeções de S_3, $\sigma, \eta \in S_3$, então a composição $\sigma \circ \eta$: {1, 2, 3} → {1, 2, 3} é definida por

$\sigma \circ \eta(i) = \sigma \circ (\eta(i))$ para i = 1, 2, 3.

Geralmente, denotamos $\sigma \circ \eta$ simplesmente por $\sigma\eta$ e chamamos esta operação de uma *multiplicação* em S_3. Dizemos que $\sigma\eta$ é o produto de σ por η. Por exemplo, dadas as permutações

$$\sigma = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix} \text{ e } \eta = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix};$$

então, o produto $\sigma\eta$ é dado por

$$\sigma\eta = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}\begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix}.$$

Caso você não tenha compreendido o resultado final, lembre-se de que, como a operação é a composição de funções, ela deve ser realizada da direita para a esquerda. Por exemplo, da permutação η temos: $\eta:1\to1$ e, da permutação σ temos: $\sigma:1\to2$. Portanto, para a permutação $\sigma\eta$ temos: $\sigma\eta:1\to1\to2$, ou seja, $\sigma\eta:1\to2$. Assim, o cálculo completo de $\sigma\eta$ é dado por:

$\sigma\eta:1\to1\to2;$
$\sigma\eta:2\to3\to1;$
$\sigma\eta:3\to2\to3;$

o que nos dá o resultado final

$$\sigma\eta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

ATIVIDADE

1. Faça o produto inverso $\eta\sigma$ para as permutações anteriores

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \eta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Você deve ter obtido o seguinte resultado:

$$\eta\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Observe que

$$\eta\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma\eta,$$

portanto, esta operação de multiplicação em S_3 não é comutativa.

O elemento neutro da operação de composição de funções é a função identidade. Neste caso, em S_3, o elemento neutro é representado pela permutação

$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

Veja também que, como o conjunto {1, 2, 3} tem 3 elementos, então, existem 3! = 6 bijeções possíveis de {1, 2, 3}. Logo, S_3 tem 6 elementos, a saber,

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Na próxima atividade, vamos mostrar que S_3 é gerada pelas duas permutações seguintes:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

ATIVIDADE

2. Denotando por α e β as duas permutações anteriores, mostre que

a. $\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$;

b. $\alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$;

c. $\beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$;

d. $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$;

e. $\beta\alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$;

f. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta\alpha^2$.

Portanto, S_3 pode ser escrito como

$S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$.

Na aula anterior, vimos o conceito de grupo abeliano, ou seja, um G que satisfaz a propriedade comutativa: $a \cdot b = b \cdot a$ para todo $a, b \in G$. Vejamos, agora, o conceito de grupo não-abeliano.

DEFINIÇÃO 1 (GRUPO NÃO-ABELIANO)

Um grupo G é chamado *não-abeliano* se G não satisfizer a propriedade comutativa, ou seja, se existirem $a, b \in G$ tais que $a \cdot b \neq b \cdot a$.

Podemos, agora, enunciar o resultado que buscamos, nosso primeiro exemplo de grupo não-abeliano.

Proposição 1

Conforme as notações anteriores, $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$, munido da operação de composição de funções, é um grupo não-abeliano finito de ordem 6.

Demonstração

Primeiramente, observe que já que uma permutação é uma bijeção e a composição de duas bijeções é outra bijeção, então, a operação está bem definida. Vamos, agora, verificar os axiomas.

G1. Como a composição de funções é associativa, então, a operação em S_3 é associativa.

G2. O elemento neutro da composição de funções é a função identidade, que é representada, em S_3, pela permutação $I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$.

G3. Dada uma bijeção, o elemento inverso é representado pela sua função inversa.

Na Atividade 3, você será convidado a determinar o elemento inverso de cada elemento de S_3.

Por fim, observe que a operação em S_3 não é comutativa, pois como vimos na Atividade 2,

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \alpha\beta.$$

Portanto, S_3 é um grupo não-abeliano.

ATIVIDADE

3. Construa a tabela de multiplicação do grupo S_3 e identifique o elemento inverso de cada elemento de S_3.

Exemplo 4

Seja $GL_2(\mathbf{R})$ o conjunto das matrizes quadradas de ordem 2 invertíveis com elementos em **R**, isto é,

$$GL_2(\mathbf{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \, a, b, c, d \in \mathbf{R} \text{ e } ad - bc \neq 0 \right\}.$$

Em $GL_2(\mathbf{R})$, consideramos a operação de multiplicação de matrizes. Do curso de Álgebra Linear, sabemos que o produto de matrizes invertíveis é uma matriz invertível e, portanto, a operação de multiplicação de matrizes está bem definida em $GL_2(\mathbf{R})$. Já sabemos, também, que a multiplicação de matrizes é associativa e, assim, o axioma da associatividade em $GL_2(\mathbf{R})$ já fica automaticamente satisfeito. O elemento neutro é dado pela matriz identidade,

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

e o elemento inverso da matriz $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $GL_2(\mathbf{R})$ é dado pela conhecida fórmula do seu curso de Álgebra Linear,

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Também é fácil ver que $GL_2(\mathbf{R})$ é um conjunto infinito, já que

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \; a \neq 0$$

é um conjunto infinito de matrizes invertíveis, pois

$$\det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a \neq 0.$$

Portanto,

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{R}) \text{ para todo } a \neq 0$$

Assim, temos o seguinte resultado:

Proposição 2

$GL_2(\mathbf{R})$, munido da operação de multiplicação de matrizes, é um grupo infinito não-abeliano.

Na próxima atividade, você irá mostrar que o grupo $GL_2(\mathbf{R})$ é não-abeliano.

ATIVIDADE

4. Mostre que a operação de multiplicação de matrizes em $GL_2(\mathbf{R})$ não é comutativa. Para isso, você deverá encontrar duas matrizes A, B $\in GL_2(\mathbf{R})$ tais que $AB \neq BA$.

Exemplo 5

O *grupo das simetrias do triângulo eqüilátero:* D_3. Vamos estudar, agora, um grupo formado por transformações geométricas estudadas no curso de Álgebra Linear II. Trata-se de um grupo de transformações que mantém o triângulo eqüilátero da **Figura 13.1** invariante, ou seja, que transforma o triângulo eqüilátero nele mesmo. Vamos considerar que o lado BC é perpendicular ao eixo-x e a origem O é o baricentro do triângulo ABC. Portanto, nestas condições, as transformações do triângulo nele mesmo são compostas pela função identidade, por algumas rotações em torno da origem e por certas reflexões. Vamos descrever cada uma dessas transformações.

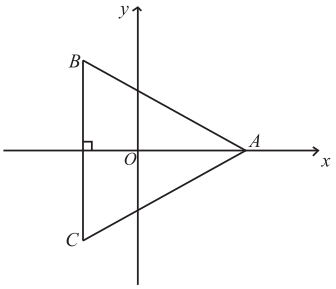


Figura 13.1: Triângulo eqüilátero.

Vamos denotar o triângulo ABC da **Figura 13.1** por Δ. As transformações que estamos procurando são da forma T: $\mathbf{R}^2 \to \mathbf{R}^2$ com $T(\Delta) = \Delta$.

Inicialmente, a função identidade, I: $\mathbf{R}^2 \to \mathbf{R}^2$, claramente mantém o triângulo Δ invariante, ou seja, $I(\Delta) = \Delta$, como ilustra a figura a seguir.

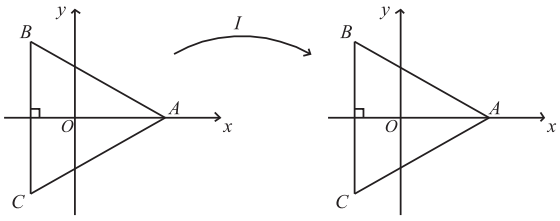


Figura 13.2: A transformação identidade.

Depois, a rotação de 120°, ou $2\pi/3$ radianos, em torno da origem, também deixa o triângulo Δ invariante. Retomando a notação do curso de Álgebra Linear II, denotamos por $R = R_{2\pi/3}$ esta rotação. Portanto, temos $R = R_{2\pi/3} : \mathbf{R}^2 \to \mathbf{R}^2$ com $R(\Delta) = \Delta$, como ilustra a **Figura 13.3**.

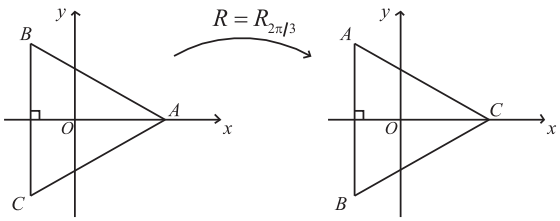


Figura 13.3: A rotação $R = R_{2\pi/3}$.

O mesmo acontece com a rotação de 240°, ou $4\pi/3$ radianos, em torno da origem. Considerando a operação de composição de funções, temos:

$$R_{4\pi/3} = R_{2\pi/3} \circ R_{2\pi/3} = R^2.$$

Assim, esta rotação satisfaz $R^2 = R_{4\pi/3} : \mathbf{R}^2 \to \mathbf{R}^2$ com $R^2(\Delta) = \Delta$. A **Figura 13.4** ilustra essa transformação.

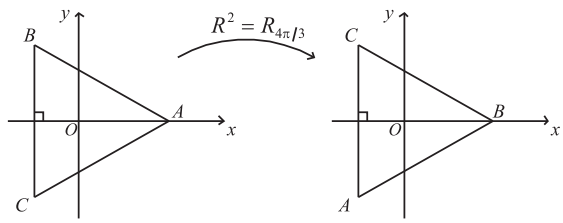


Figura 13.4: A rotação $R^2 = R_{4\pi/3}$.

Observe que, aplicando a rotação $R = R_{2\pi/3}$ mais uma vez, obtemos a função identidade:

$$R^3 = R^2R = R_{4\pi/3} \circ R_{2\pi/3} = R_{6\pi/3} = R_{2\pi} = I.$$

Outro tipo de transformação que mantém o triângulo eqüilátero invariante são as reflexões do plano em torno das retas mediatrizes do triângulo. Denotamos estas retas por r_1, r_2 e r_3, como indica a **Figura 13.5**. Observe que a reta mediatriz r_1 coincide com o eixo-x.

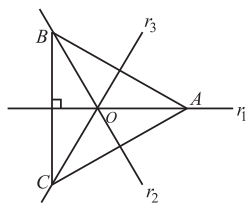


Figura 13.5: As retas mediatrizes do triângulo eqüilátero.

Denotamos por F:$\mathbf{R}^2 \to \mathbf{R}^2$ a reflexão em torno do eixo-x. Assim, temos F(Δ) = Δ. A **Figura 13.6** ilustra essa transformação.

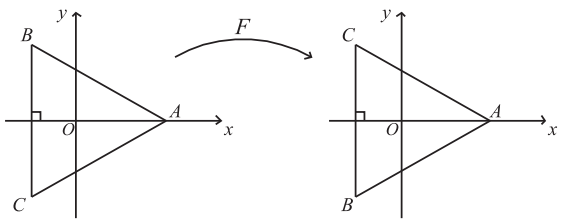


Figura 13.6: A reflexão *F* em torno do eixo-x.

Observe que, aplicando a reflexão F mais uma vez, obtemos $F^2 = F \circ F = I$. Aplicando a composição $FR = F \circ R$, obtemos exatamente a reflexão em torno da reta mediatriz r_2, como indica a **Figura 13.7**.

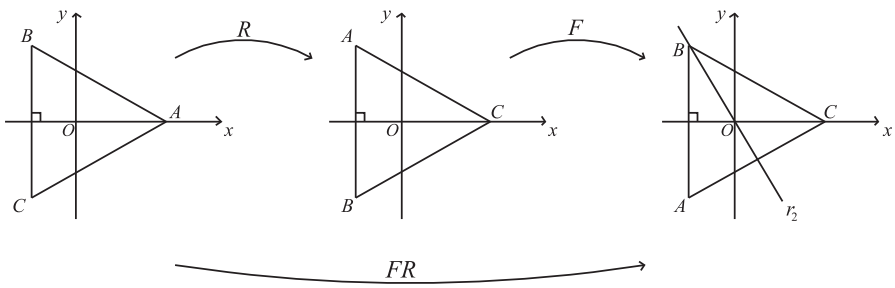


Figura 13.7: Rotação R seguida da reflexão F.

Assim, a reflexão em torno da reta mediatriz r_2 pode ser representada por FR^2: $\mathbf{R}^2 \to \mathbf{R}^2$ com FR(Δ) = Δ. Novamente, temos $(FR)^2 = I$.

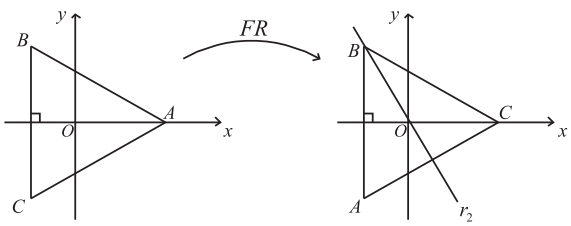


Figura 13.8: A reflexão *FR* em torno da reta mediatriz r_2.

Analogamente, aplicando a composição $FR^2 = F \circ R^2$, obtemos a reflexão em torno da reta mediatriz r_3, como indica a **Figura 13.9**. Assim, essa reflexão satisfaz $FR^2 : \mathbf{R}^2 \to \mathbf{R}^2$ com $FR^2(\Delta) = \Delta$ e $(FR^2)^2 = I$.

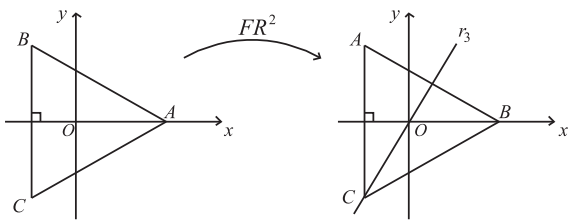


Figura 13.9: A reflexão FR^2 em torno da reta mediatriz r_3.

Denotamos por D_3 o conjunto dessas seis simetrias do triângulo eqüilátero:

$D_3 = \{I, R, R^2, F, FR, FR^2\}$.

Assim, munindo o conjunto D_3 com a operação de composição de funções, obtemos o grupo das simetrias do triângulo eqüilátero.

Proposição 3

Com as notações anteriores, $D_3 = \{I, R, R^2, F, FR, FR^2\}$, munido da operação de composição de funções, é um grupo não-abeliano finito de ordem 6.

Na próxima atividade, você será convidado a mostrar que D_3 é um grupo não-abeliano.

ATIVIDADE

5. Mostre que $RF = FR^2$ e, portanto, $RF \neq FR$. Conclua que D_3 é um grupo não-abeliano.

Em nosso último exemplo desta aula, vamos estabelecer que o produto cartesiano de dois grupos também tem uma estrutura de grupo.

Exemplo 6

Sejam $(G, \cdot)$ e $(H, *)$ dois grupos. Vamos considerar o produto cartesiano $G \times H$ munido da seguinte operação:

$(a_1, b_1) \otimes (a_2, b_2) = (a_1 \cdot a_2, b_1 * b_2)$ para $a_1, a_2 \in G$ e $b_1, b_2 \in H$.

O elemento neutro dessa operação será $(e_G, e_H) \in G \times H$, onde e_G e e_H são os elementos neutros de G e H, respectivamente, e o elemento inverso de $(a, b) \in G \times H$ é dado por (a^{-1}, b^{-1}). Nessas condições, temos o seguinte resultado:

Proposição 4

Com as notações anteriores, temos que $(G \times H, \otimes)$ é um grupo chamado *produto exterior* de G e H.

ATIVIDADES FINAIS

1. Construa a tabela de multiplicação do grupo D_3 e identifique o elemento inverso de cada elemento de D_3.

2. Construa a tabela de multiplicação do grupo $Z_4^x \times Z_4^x$, onde Z_4^x é o grupo multiplicativo dos elementos invertíveis de Z_4. Depois, identifique o elemento inverso de cada elemento de $Z_4^x \times Z_4^x$.

RESUMO

Nesta aula, estudamos os grupos multiplicativos $(Z_5^x, \cdot)$ e $(Z_8^x, \cdot)$. Eles são grupos finitos e abelianos. Depois, estudamos o grupo $\{S_3 = I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ das permutações do conjunto {1, 2, 3}. Esse grupo é finito e não-abeliano. No exemplo seguinte, estudamos o grupo $GL_2(\mathbf{R})$ das matrizes invertíveis de ordem com elementos em **R**. Esse grupo é infinito e não-abeliano. No exemplo seguinte, estudamos o grupo $D_3 = \{I, R, R^2, F, FR, FR^2\}$ das simetrias do triângulo eqüilátero. Esse grupo também é finito e não-abeliano. Por fim, vimos o produto exterior $G \times H$ dos grupos G e H.

RESPOSTAS

Atividade 1

O produto

$$\eta\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

é dado por

$\eta\sigma : 1 \to 2 \to 3;$

$\eta\sigma : 2 \to 3 \to 2;$

$\eta\sigma : 3 \to 1 \to 1.$

Portanto, temos

$$\eta\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Atividade 2

Temos:

a. $\alpha^2 = \alpha \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$

b. $\alpha^3 = \alpha^2 \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$;

c. $\beta^2 = \beta \cdot \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I$;

d. $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$;

e. $\beta\alpha^2 = \beta \cdot \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$;

f. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta\alpha^2$.

Atividade 3

Queremos completar a seguinte tabela:

$\times$	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I						
α						
α^2						
β						
$\beta\alpha$						
$\beta\alpha^2$						

Efetuamos os produtos da tabela acima e identificamos os resultados com os elementos de $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$. Por exemplo,

$\alpha \cdot \beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \beta$.

Assim, obtemos a seguinte tabela de multiplicação:

$\times$	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	I	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	I	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	I	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	I	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	I

Podemos observar que os pares de elementos inversos são

$I \leftrightarrow I$; $\alpha \leftrightarrow \alpha^2$; $\beta \leftrightarrow \beta$; $\beta\alpha \leftrightarrow \beta\alpha$; $\beta\alpha^2 \leftrightarrow \beta\alpha^2$.

Atividade 4

Temos de encontrar duas matrizes invertíveis que não satisfaçam a propriedade comutativa. Existem infinitas possibilidades e, como vamos apresentar aqui apenas uma delas, é bem provável que a sua resposta seja diferente desta. Para isso, considere as matrizes

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL_2(R).$$

Temos os seguintes produtos:

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

e

$$BA = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Como

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

temos, então, que $AB \neq BA$, ou seja, essas matrizes não satisfazem a propriedade comutativa.

Atividade 5

Aplicando a composição RF = R F , veja que obtemos exatamente a reflexão em torno da reta mediatriz r3 , como mostra a **Figura 13.10.**

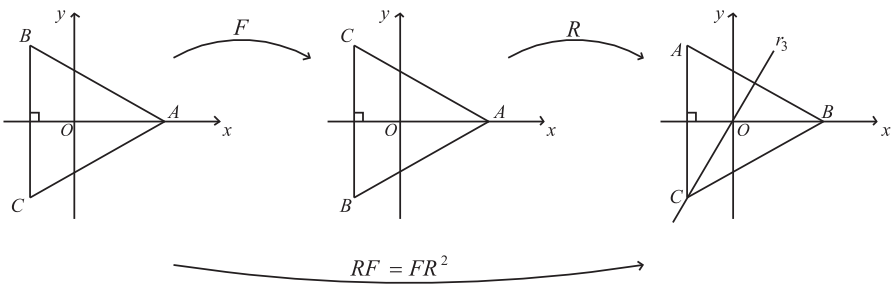


Figura 13.10: A composição *RF* é igual à reflexão FR^2 em torno da reta mediatriz r_3.

Portanto, temos que $RF = FR^2$. Como FR é a reflexão em torno da reta mediatriz r_2, temos reflexões diferentes $FR^2 \neq FR$. Logo, $RF \neq FR$. Em particular, como o par R e F não satisfaz a propriedade comutativa, isso nos diz que D_3 é um grupo não-abeliano.

Atividade Final 1

Queremos completar a seguinte tabela:

×	*I*	*R*	R^2	*F*	*FR*	FR^2
I						
R						
R^2						
F						
FR						
FR^2						

Efetuamos os produtos da tabela acima e identificamos os resultados com os elementos de $D_3 = \{I, R, R^2, F, FR, FR^2\}$. Para isso, você pode usar as relações $R^3 = I$, $F^2 = I$ e $RF = FR^2$. Por exemplo, podemos calcular o produto $R \cdot FR$:

$R \cdot FR = (RF)R$, pois a operação é associativa;

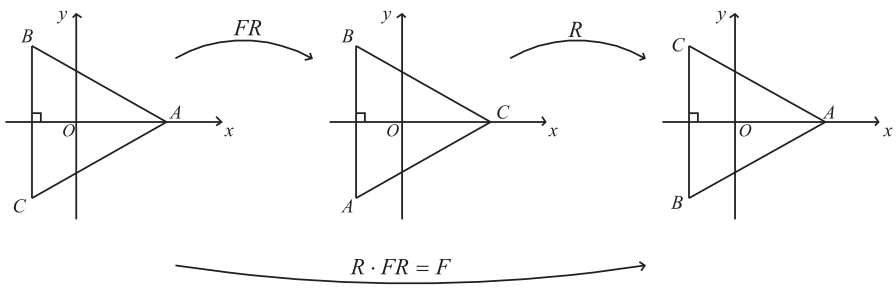
$= (FR^2)R$, pois $RF = FR^2$;

$= F \cdot R^3$, pois a operação é associativa;

$= F \cdot I$, pois $R^3 = I$;

$= F$, pois I é o elemento neutro.

Também podemos obter esse resultado geometricamente:



Assim, obtemos a seguinte tabela de multiplicação:

$\times$	I	R	R^2	F	FR	FR^2
I	I	R	R^2	F	FR	FR^2
R	R	R^2	I	FR^2	F	FR
R^2	R^2	I	R	FR	FR^2	F
F	F	FR	FR^2	I	R	R^2
FR	FR	FR^2	F	R^2	I	R
FR^2	FR^2	F	FR	R	R^2	I

Podemos observar que os pares de elementos inversos são

$I \leftrightarrow I$; $R \leftrightarrow R^2$; $F \leftrightarrow F$; $FR \leftrightarrow FR$; $FR^2 \leftrightarrow FR^2$.

Atividade Final 2

Temos que $Z_4^x = \{\bar{a} \in Z_4 \mid mdc\,(a, 4) = 1\} = \{1, 3\}$. Então,

$Z_4 \times Z_4 = \{(1, 1), (1, 3), (3, 1), (3, 3)\}$.

Veja que a operação em $Z_4 \times Z_4$ é dada por

$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$.

Por exemplo,

$(1, 3) \,.\, (3, 3) = (1 \,.\, 3, 3 \,.\, 3) = (3, 1)$.

Operando dessa forma, obtemos a seguinte tabela de multiplicação:

$\times$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{3})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{3})$
$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{3})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{3})$
$(\bar{1}, \bar{3})$	$(\bar{1}, \bar{3})$	$(\bar{1}, \bar{1})$	$(\bar{3}, \bar{3})$	$(\bar{3}, \bar{1})$
$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{1})$	$(\bar{3}, \bar{3})$	$(\bar{1}, \bar{1})$	$(\bar{1}, \bar{3})$
$(\bar{3}, \bar{3})$	$(\bar{3}, \bar{3})$	$(\bar{3}, \bar{1})$	$(\bar{1}, \bar{3})$	$(\bar{1}, \bar{1})$

Como o elemento neutro de $Z_4^x \times Z_4^x$ é $(\bar{1}, \bar{1})$, podemos observar que cada elemento de $Z_4^x \times Z_4^x$ é seu próprio inverso:

$(\bar{1}, \bar{1}) \leftrightarrow (\bar{1}, \bar{1})$; $(\bar{1}, \bar{3}) \leftrightarrow (\bar{1}, \bar{3})$; $(\bar{3}, \bar{1}) \leftrightarrow (\bar{3}, \bar{1})$; $(\bar{3}, \bar{3}) \leftrightarrow (\bar{3}, \bar{3})$.

Subgrupos e grupos cíclicos

AULA 14

Meta da aula

Apresentar os conceitos de subgrupo e de subgrupo cíclico.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as propriedades que caracterizam um subgrupo.
- Apresentar exemplos de subgrupos.
- Identificar as propriedades que caracterizam um grupo cíclico.
- Apresentar exemplos de subgrupos cíclicos.

Pré-requisitos

Você vai precisar dos conhecimentos sobre anéis e ideais, desenvolvidos em Álgebra I e nas Aulas 12 e 13.

INTRODUÇÃO

Nas duas aulas anteriores, desenvolvemos o conceito de grupo e estudamos vários exemplos. Você deve ter notado que vimos alguns exemplos de grupos contidos em outro grupo maior. Por exemplo, o grupo (**Z**, +), dos números inteiros com a operação de adição, está contido no grupo (**Q**, +) dos números racionais com a operação de adição. Da mesma forma, (**Q**, +) está contido em (**R**, +) que, por sua vez, está contido em (**C**, +). Esta é a importante noção de subgrupo.

É relevante observar que, quando dizemos que o grupo (**Z**, +) está contido no grupo (**Q**, +), queremos dizer não só que um conjunto é subconjunto do outro, $\mathbf{Z} \subset \mathbf{Q}$, mas também que a operação de adição (+) entre dois números inteiros, a e b, produz o mesmo resultado $a + b$ que na situação em que a e b são vistos como elementos do grupo (**Q**, +). Assim, não podemos dizer que o grupo multiplicativo ($\mathbf{Q}^*$, ·) está contido no grupo aditivo (**R**, +), pois, apesar de $\mathbf{Q}^* \subset \mathbf{R}$, as operações $a \cdot b$ em ($\mathbf{Q}^*$, ·) e $a + b$ em (**R**, +) dão resultados diferentes para os mesmos $a, b \in \mathbf{Q}$. Por exemplo, $1 \cdot 1 = 1$ e $1 + 1 = 2$. Portanto, para que um grupo seja um subgrupo de outro grupo, vamos exigir não só que um conjunto esteja contido no outro mas, também, que suas operações coincidam nos elementos que são comuns aos dois conjuntos.

DEFINIÇÃO 1 (SUBGRUPO)

Sejam $(G, \cdot)$ um grupo e H um subconjunto não-vazio de G. Dizemos que H é um subgrupo de G se H, munido da operação · do grupo G, for um grupo, ou seja, se $(H, \cdot)$ for um grupo.

Veja que a operação · já é associativa em G, logo, ela já satisfaz a propriedade associativa para os elementos de H. Portanto, as propriedades a serem satisfeitas para que H seja um subgrupo de G são dadas pelos seguintes axiomas.

SG1. H é fechado pela operação de G, isto é, $a \cdot b \in H$ para todo $a, b \in H$.

SG2. $e_G \in H$.

SG3. Se $a \in H$ então $a^{-1} \in H$.

Se H é subgrupo de G, então denotamos $H < G$ e, caso contrário, denotamos $H \quad G$.

Observação

Dado o grupo G, então $\{e_G\}$ e G são subgrupos de G, chamados *subgrupos triviais* de G. Se H é um subgrupo de G, diferente de $\{e_G\}$ e G, então dizemos que H é um subgrupo próprio de G.

Exemplo 1

Pelas nossas observações iniciais, temos a seguinte seqüência de subgrupos:

$$(\mathbf{Z}, +) < (\mathbf{Q}, +) < (\mathbf{R}, +) < (\mathbf{C}, +) .$$

No entanto, $(\mathbf{Q}^*, \cdot)$ não é subgrupo de $(\mathbf{R}, +)$, já que a operação de $(\mathbf{Q}^*, \cdot)$ não é a mesma que a de $(\mathbf{R}, +)$. Mas é verdade que

$$(\mathbf{Q}^*, \cdot) < (\mathbf{R}^*, \cdot) < (\mathbf{C}^*, \cdot) .$$

Assim como temos critérios que facilitam verificar se um subconjunto de um espaço vetorial é um subespaço vetorial ou se um subconjunto de um anel é um subanel, temos, também, um critério que facilita verificar se um subconjunto de um grupo é um subgrupo. É o que vamos fazer a seguir.

Proposição 1 (Critério do Subgrupo)

Seja H um subconjunto não-vazio de um grupo G. Então, H é um subgrupo de G se, e somente se, $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

Demonstração

($\Rightarrow$) Vamos supor, inicialmente, que H é um subgrupo de G. Queremos provar que $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

Assim, sejam $a, b \in H$. Temos

$$a, b \in H \Rightarrow b^{-1} \in H \quad \text{pela propriedade SG3 de subgrupo}$$
$$\Rightarrow a \cdot b^{-1} \in H \quad \text{pela propriedade SG1 de subgrupo,}$$

e, assim, provamos o que queríamos, ou seja, que $a \cdot b^{-1} \in H$ para todo $a, b \in H$.

($\Leftarrow$) Nossa hipótese, agora, é que $a \cdot b^{-1} \in H$ para todo $a, b \in H$. Queremos provar que H é subgrupo de G, ou seja, que H satisfaz as propriedades SG1 a SG3. Vamos provar primeiro a validade de SG2, depois SG3 e, por fim, SG1.

SG2. Como $H \neq \emptyset$, existe um elemento $a \in H$. Daí, temos

$$a \in H \ \Rightarrow \ e_G = a \cdot a^{-1} \in H \quad \text{pela hipótese com } b = a\,.$$

SG3. Seja $x \in H$. Como já sabemos que $e_G \in H$, então,

$$x, e_G \in H \ \Rightarrow \ x^{-1} = e_G \cdot x^{-1} \in H \text{ pela hipótese com } a = e_G \text{ e } b = x.$$

SG1. Sejam $x, y \in H$. Pela propriedade SG3, sabemos que $y^{-1} \in H$. Portanto, temos

$$x, y^{-1} \in H \Rightarrow x \cdot y = x \cdot (y^{-1})^{-1} \in H \text{ pela hipótese com } a = x \text{ e } b = y^{-1}.$$

Concluímos, assim, que H é um subgrupo de G.

Observação

Quando G for um grupo aditivo, $(G, +)$, e H um subconjunto não-vazio de G, a condição $a \cdot b^{-1} \in H$ se transformará em

$$a - b \in H,$$

já que $-b$ é o elemento inverso de b. Assim, nesse caso, temos

$$H < G \quad \Leftrightarrow \quad a - b \in H \ \text{ para todo a, } b \in H\,.$$

ATIVIDADE

1. Dado o grupo aditivo $(\mathbf{Z}, +)$, mostre que $n\mathbf{Z} = \{kn \mid k \in Z\}$ é um subgrupo de Z para todo inteiro $n > 1$.

Exemplo 2

Seja $D_3 = \{I, R, R^2, F, FR, FR^2\}$ o grupo das simetrias do triângulo eqüilátero visto na Aula 18. Então

$$H_1 = \{I, R, R^2\} \text{ e } H_2 = \{I, F\}$$

são subgrupos de D_3. Isso é imediato pela aplicação do critério do subgrupo.

Exemplo 3

Considere o grupo $(\mathbf{Z}_4, +)$. Vamos mostrar que $H = \{\bar{0}, \bar{2}\}$ é o único subgrupo próprio de $\mathbf{Z}_4$. Se H for outro subgrupo próprio de $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, então, teremos $\bar{1} \in H$ ou $\bar{3} \in H$. Caso seja $\bar{1} \in H$, então, aplicando SG1, teremos

$$\bar{2} = \bar{1} + \bar{1} \in H\,; \ \bar{3} = \bar{2} + \bar{1} \in H \quad e \quad \bar{0} = \bar{3} + \bar{1} \in H\,,$$

e, portanto, teríamos $H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbf{Z}_4$, o que é uma contradição, já que H é subgrupo próprio de $\mathbf{Z}_4$.

Caso seja $\bar{3} \in H$, então, aplicando SG3, teremos

$$\bar{1} = -\bar{3} \in H\,,$$

e, pelo argumento anterior, teríamos novamente que $H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbf{Z}_4$, que é a mesma contradição. A conclusão, portanto, é que $H = \{\bar{0}, \bar{2}\}$ é o único subgrupo próprio de $\mathbf{Z}_4$.

Vamos desenvolver, agora, um importante tipo de subgrupos, que são os subgrupos gerados por um único elemento.

DEFINIÇÃO 2 (SUBGRUPO GERADO POR UM ELEMENTO)

Sejam $(G, \cdot)$ um grupo e $a \in G$. Definimos as *potências* de a:

$$\begin{aligned} a^0 &= e_G \\ a^n &= a^{n-1} \cdot a \quad \text{se } n \in \mathbf{Z}, n \geq 1 \\ a^n &= (a^{-1})^{-n} \quad \text{se } n \in \mathbf{Z}, n < 0 . \end{aligned}$$

Denotamos por $< a >$ o conjunto de todas as potências de a, ou seja,

$$< a > = \{a^n \mid n \in \mathbf{Z}\} .$$

Veremos, a seguir, que este conjunto é um subgrupo de G, chamado *subgrupo gerado* por a. Dizemos, também, que a é um gerador de $<a>$.

Quando G for um grupo aditivo, $(G, +)$, então as potências de a serão, na verdade, os múltiplos de a:

$$\begin{cases} 0a = 0_G \\ na = (n-1)\, a + a \quad \text{se } n \in \mathbf{Z}, n \geq 1 \\ na = (-n)(-a) \quad \text{se } n \in \mathbf{Z}, n < 0 , \end{cases}$$

e o subgrupo gerado por a se escreve como

$$< a > = \{na \mid n \in \mathbf{Z}\}.$$

Proposição 2 (O subgrupo gerado por *a*)

Sejam $(G, \cdot)$ um grupo e $a \in G$. Então $< a >$ é um subgrupo de G.

Demonstração

Vamos aplicar o critério do subgrupo. Sejam $a^n, a^k \in < a >$ dois elementos, então

$$a^n \cdot (a^k)^{-1} = a^n \cdot a^{-k} = a^{n-k} \in < a > ,$$

o que prova que $< a >$ é um subgrupo de G.

Exemplo 4

Dado o grupo (Z, +), então $n\mathbf{Z} = \{kn \mid k \in \mathbf{Z} = < n >\}$. Em particular, $2\mathbf{Z} = < 2 >$. Veja, também, que $\mathrm{Z} = < 1 >$.

Exemplo 5

Considere o grupo $(\mathbf{Z}_4, +)$ do Exemplo 3. Então $H = \{\overline{0}, \overline{2}\} = < 2 >$. Veja aqui, também, que $\mathbf{Z}_4 = < \overline{1} >$.

Grupos, como $\mathbf{Z}$ ou $\mathbf{Z}_4$, que são gerados por apenas um elemento, são muito importantes e têm uma nomenclatura especial.

DEFINIÇÃO 3 (GRUPO CÍCLICO)

Um grupo G é chamado grupo cíclico se $= G = < a >$ para algum $a \in G$, ou seja, G é gerado por um elemento. Neste caso, dizemos que a é um gerador de G.

Observação

Se G é um grupo cíclico, então o gerador de G, isto é, o elemento $a \in G$ tal que $G = < a >$, em geral, não é único. Por exemplo, $\mathbf{Z}_4 =< \overline{1} >$ e $\mathbf{Z}_4 = < \overline{3} >$.

Exemplo 6

Considere o grupo $(\mathbf{Z}_n, +)$, onde $n > 1$ é um inteiro. Então $\mathbf{Z}_n = < \overline{1} >$, e, portanto, Z_n é um grupo cíclico.

ATIVIDADE

2. Determine se os grupos multiplicativos $(\mathbf{Z}^{x}_{5}, .)$ e $(\mathbf{Z}^{x}_{8}, .)$ são grupos cíclicos. Caso algum deles seja um grupo cíclico, determine seus geradores.

_____

_____

_____

_____

_____

Para terminar esta aula, vamos enunciar um resultado que diz, no fundo, que todo grupo cíclico é uma cópia de $(\mathbf{Z}, +)$ ou uma cópia de algum $(\mathbf{Z}_n, +)$. Para isso precisamos definir o conceito de ordem de um elemento.

DEFINIÇÃO 4 (ORDEM DE UM ELEMENTO)

Seja G um grupo e seja $a \in G$. Se o subgrupo $< a >$ for finito, então dizemos que a *ordem de a*, denotada por ord(a), é o número de elementos de $< a >$, ou seja, é igual à ordem de $< a >$. Agora, se $< a >$ for um grupo infinito, então dizemos que a *ordem de a* é *infinita*.

Observação

1. Para o elemento neutro e de um grupo G, temos $< e > = \{e\}$ e, portanto, $ord(e) = 1$. Para qualquer outro elemento $a \in G$ $(a \neq e)$, temos $\text{ord}(a) = > 1$.
2. Se G é um grupo cíclico com gerador a, $G = < a >$, então $\text{ord}(a) = |G|$.

Exemplo 7

Considere o grupo aditivo $\mathbf{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Pela observação anterior, já sabemos que $\text{ord}(\overline{0}) = 1$. Agora,

$< \overline{1} > = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbf{Z}_4$; $< \overline{2} > = \{\overline{0}, \overline{2},\}$; $< \overline{3} > = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbf{Z}_4$,

de onde concluímos que

$\text{ord}(\overline{1}) = 4$; $\text{ord}(\overline{2}) = 2$ $\text{ord}(\overline{3}) = 4$

ATIVIDADE

3. Determine a ordem dos elementos dos grupos multiplicativos $(\mathbf{Z}_5^x, .)$ e $(\mathbf{Z}_8^x, .)$.

Podemos enunciar, agora, o resultado mais importante deste capítulo.

TEOREMA 1

Seja G um grupo e seja $a \in G$.

1. Se a for um elemento de ordem finita n, então n será o menor inteiro positivo que satisfaz $a^n = e_G$. Mais ainda, $< a > = \{e, a, a^2, ..., a^{n-1}\}$.
2. Se a for um elemento de ordem infinita, então $a^n \neq e_G$ para todo inteiro $n \neq 0$. Mais ainda, $< a > = \{..., a^{-2}, a^{-1}, e, a, a^2, ...\}$ e todas as potências de a serão distintas.

CARACTERIZAÇÃO DOS GRUPOS CÍCLICOS

Futuramente vamos definir o conceito de isomorfismo de grupos de modo muito semelhante ao que foi feito para os isomorfismos de espaços vetoriais e para os isomorfismos de anéis. Isso significa que dois grupos serão isomórficos quando um for uma cópia algébrica do outro.

Assim, se G for um grupo cíclico com gerador a, ou seja, $G = < a >$, então o teorema anterior diz que teremos dois casos a considerar:

1. Se a for um elemento de ordem finita n, então $G = \{e, a, a^2, ..., a^{n-1}\}$ e G será isomórfico a $\mathbf{Z}n$.

2. Se a for um elemento de ordem infinita, então $G = \{..., a^{-2}, a^{-1}, e, a, a^2, ...\}$, com todas as potências de a distintas, e G será isomórfico a $\mathbf{Z}$.

Observação

Como conseqüência da caracterização dos grupos cíclicos, temos que todo grupo cíclico é abeliano.

No entanto, a recíproca é falsa, ou seja, nem todo grupo abeliano é um grupo cíclico. Por exemplo, o grupo multiplicativo $\mathbf{Z}^{\times}_{8}$, é abeliano, mas, como você provou na Atividade 2, ele não é um grupo cíclico.

ATIVIDADES FINAIS

1. Determine se o grupo multiplicativo $\mathbf{Z}^{\times}_{7} = \{\overline{a} \in \mathbb{Z}_7 \mid mdc\,(a, 7) = 1\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ é cíclico. Caso seja, determine seus geradores.

_____

_____

_____

_____

2. Determine se o grupo S_3, das permutações de 3 objetos, é cíclico. Caso seja, determine seus geradores.

_____

_____

_____

_____

_____

RESUMO

Nesta aula, vimos o conceito de subgrupo. Vimos que um subconjunto não-vazio H de um grupo G é um subgrupo de G se satisfizer os seguintes axiomas:

SG1. H é fechado pela operação de G, isto é, $a \cdot b \in H$ para todo $a, b \in H$.

SG2. $e_G \in H$.

SG3. Se $a \in H$ então $a^{-1} \in H$.

Depois, vimos o conceito de um subgrupo gerado por um elemento $a \in G$, que o subconjunto $< a > = \{a^n \mid n \in \mathbf{Z}\} \subset G$. Vimos que a ordem do elemento $a \in G$ é a ordem do subgrupo $< a >$. Em seguida, vimos que um grupo G é um grupo cíclico se existir $a \in G$ tal que $G = < a >$. Nesse caso, dizemos que o elemento a é um gerador do grupo G.

Por fim, vimos o importante teorema que diz que se G é um grupo e $a \in G$, então:

1. Se a for um elemento de ordem finita n, então n será o menor inteiro positivo que satisfaz $a^n = e_G$. Mais ainda, $< a > = \{e, a, a^2, ..., a^{n-1}\}$;
2. Se a for um elemento de ordem infinita, então $a^n \neq e_G$ para todo inteiro $n \neq 0$. Mais ainda, $< a > = \{..., a^{-2}, a^{-1}, e, a, a^2, ...\}$ e todas as potências de a serão distintas.

RESPOSTAS COMENTADAS

Atividade 1

Pelo critério do subgrupo, basta verificar que $a - b \in n\mathbf{Z}$ para todo $a, b \in n\mathbf{Z}$. Como $a, b \in n\mathbf{Z}$, então existem $k, m \in \mathbf{Z}$ tais que $a = kn$ e $b = mn$. Assim,

$$a - b = kn - mn = (k - m)n \in n\mathbf{Z} ,$$

e, portanto, $n\mathbf{Z}$ é um subgrupo de $\mathbf{Z}$.

Atividade 2

Vamos considerar, inicialmente, $\mathbf{Z}^x_5 = \{\overline{a} \in \mathbf{Z}_5 | \ mdc(a, 5) = 1\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Considerando as potências de $\overline{2} \in \mathbf{Z}^x_5$, temos:

$$(\overline{2})^1 = \overline{2};\ \ (\overline{2})^2 = \overline{4};\ (\overline{2})^3 = \overline{3};\ \ (\overline{2})^4 = \overline{1},$$

o que mostra que $\mathbf{Z}^x_5 = < \overline{2} >$, ou seja, $\mathbf{Z}^x_5$ é um grupo cíclico. Mais ainda, não só o elemento $\overline{2}$ é um gerador de $\mathbf{Z}^x_5$, o elemento $\overline{3}$ também é, pois

$$(\overline{3})^1 = \overline{3};\ \ (\overline{3})^2 = \overline{4};\ (\overline{3})^3 = \overline{2};\ \ (\overline{3})^4 = \overline{1},$$

e, portanto, $\mathbf{Z}^x_5 = < \overline{3} >$. Mas, $\overline{4}$ não é gerador de $\mathbf{Z}^x_5$, pois

$$(\overline{4})^1 = \overline{4};\ \ (\overline{4})^2 = \overline{1};\ (\overline{4})^3 = \overline{4};\ \ (\overline{4})^4 = \overline{1};\ ...,$$

ou seja, $< \overline{4} > = \{\overline{1}, \overline{4}\}$, que é um subgrupo próprio de $\mathbf{Z}^x_5$.

No caso de $\mathbf{Z}^x_8 = \{\ a \in \mathbf{Z}_8 | \ mdc(a, 8) = 1\} = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, temos

$$(\overline{3})^1 = \overline{3};\ \ (\overline{3})^2 = \overline{1};\ (\overline{3})^3 = \overline{3};\ \ (\overline{3})^4 = \overline{1};\ ...,$$
$$(\overline{5})^1 = \overline{5};\ \ (\overline{5})^2 = \overline{5};\ (\overline{5})^3 = \overline{5};\ \ (\overline{5})^4 = \overline{1};...,$$

e

$$(\overline{7})^1 = \overline{7};\ \ (\overline{7})^2 = \overline{7};\ (\overline{7})^3 = \overline{7};\ \ (\overline{7})^4 = \overline{1},... \ .$$

Portanto, temos

$$< \overline{3} > = \{\overline{1}, \overline{3}\}\ ,\quad < \overline{5} > = \{\overline{1}, \overline{5}\} \text{ e } \quad < \overline{7} > = \{\overline{1}, \overline{7}\},$$

ou seja, todos subgrupos próprios de $\mathbf{Z}^x_8$. Assim, $\mathbf{Z}^x_8$ não é um grupo cíclico.

Atividade 3

Considere $\mathbf{Z}^x_5$. Já sabemos que $\text{ord}(\overline{1}) = 1$. Agora, dos cálculos feitos na atividade anterior, temos

$$< \overline{2} > = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \mathbf{Z}^x_5;\quad < \overline{3} > = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \mathbf{Z}^x_5;\quad < \overline{4} > = \{\overline{1}, \overline{4}\}\ ,$$

de onde concluímos que

$$\text{ord}(\overline{2}) = 4;\quad \text{ord}(\overline{3}) = 4 \quad \text{e} \quad \text{ord}(\overline{4}) = 2.$$

Seja, agora, $\mathbb{Z}_8^x = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. Já sabemos que $ord(\overline{1}) = 1$. Também, dos cálculos feitos na atividade anterior, temos

$$< \overline{3} > = \{\overline{1}, \overline{3}\}\ , \quad < \overline{5} > = \{\overline{1}, \overline{5}\} \text{ e } \quad < \overline{7} > = \{\overline{1}, \overline{7}\},$$

de onde concluímos que

$$ord(\overline{3}) = 2; \quad ord(\overline{5}) = 2 \quad \text{e} \quad ord(\overline{7}) = 2.$$

Observe que, como os elementos $\overline{3}$, $\overline{5}$ e $\overline{7}$ são seus próprios inversos em $\mathbb{Z}_8^x$, então eles são de ordem $\overline{2}$.

Atividade Final 1

Calculando as potências dos elementos de $\mathbb{Z}_7^x = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6},\}$ e aplicando o Teorema 1, obtemos

$$(\overline{2})^1 = \overline{2}; \quad (\overline{2})^2 = \overline{4}; \quad (\overline{2})^3 = \overline{1} \quad \Rightarrow \quad ord(\overline{2}) = 3;$$

$$(\overline{3})^1 = \overline{3}; \quad (\overline{3})^2 = \overline{2}; \quad (\overline{3})^3 = \overline{6}; \quad (\overline{3})^4 = \overline{4}; \quad (\overline{3})^5 = \overline{5}; \quad (\overline{3})^6 = \overline{1} \quad \Rightarrow \quad ord(\overline{3}) = 6$$

$$(\overline{4})^1 = \overline{4}; \quad (\overline{4})^2 = \overline{2}; \quad (\overline{4})^3 = \overline{1} \quad \Rightarrow \quad ord(\overline{4}) = 3$$

$$(\overline{5})^1 = \overline{5}; \quad (\overline{5})^2 = \overline{4}; \quad (\overline{5})^3 = \overline{6}; \quad (\overline{5})^4 = \overline{2}; \quad (\overline{5})^5 = \overline{3}; \quad (\overline{5})^6 = \overline{1} \quad \Rightarrow \quad ord(\overline{5}) = 6$$

e

$$(\overline{6})^1 = \overline{6}; \quad (\overline{6})^2 = \overline{1}; \quad \Rightarrow \quad ord(\overline{6}) = 2$$

Portanto, como $\mathbb{Z}_7^x = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ é um grupo de ordem 6 e temos dois elementos também de ordem 6, então segue que $\mathbb{Z}_7^x$ é um grupo cíclico com

$$\mathbb{Z}_7^x = < \overline{3} > = < \overline{5} >,$$

ou seja, $\mathbb{Z}_7^x$ tem os geradores $\overline{3}$ e $\overline{5}$.

Atividade Final 2

Na Aula 18, vimos que $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ com

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad \beta \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Pelos cálculos, também feitos naquela aula, e aplicando o Teorema 1, temos

$$(\alpha)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad \alpha^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad \alpha^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \quad \Rightarrow \quad \text{ord}(\alpha) = 3 ;$$

$$(\alpha^2)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad (\alpha^2)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad (\alpha^2)^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \quad \Rightarrow \quad \text{ord}(\alpha) = 3 ;$$

$$(\beta)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad \beta^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \quad \Rightarrow \quad \text{ord}(\beta) = 2 ;$$

$$(\beta\alpha)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; \quad (\beta\alpha)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \quad \Rightarrow \quad \text{ord}(\beta\alpha) = 2 ;$$

e

$$(\beta\alpha^2)^1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad (\beta\alpha^2)^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = I \quad \Rightarrow \quad \text{ord}(\beta\alpha^2) = 2 ;$$

Como S_3 é um grupo de ordem 6 e todos os seus elementos têm ordem menor que 6, então segue que S_3 não é um grupo cíclico.

O Teorema de Lagrange

AULA 15

Meta da aula

Apresentar o Teorema de Lagrange
e suas conseqüências.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar as condições do Teorema de Lagrange.
- Demonstrá-lo.
- Apresentar suas conseqüências.

Pré-requisitos

Você vai precisar dos conhecimentos
sobre grupos das Aulas 11 a 13.

INTRODUÇÃO

Um problema muito estudado e bastante difícil na teoria dos grupos é a determinação de todos os subgrupos, de um grupo *G*. Uma forma de encarar esse problema seria considerar todos os subconjuntos de G que contenham o elemento neutro e, então, verificar se satisfazem as condições de subgrupo. No entanto, esta abordagem não é nada prática. Por exemplo, se um grupo G tiver 6 elementos, então o número de subconjuntos contendo o elemento neutro será $2^5 = 32$. Já se *G* tiver 10 elementos, então o número de subconjuntos contendo o elemento neutro será $2^9 = 516$. Se *G* fosse um grupo infinito, então teríamos que levar em consideração uma infinidade de subconjuntos de *G*.

No entanto, quando o grupo *G* for finito, teremos um importante resultado que permitirá reduzir enormemente o número de subconjuntos de *G* que podem ser subgrupos. Trata-se do Teorema de Lagrange, que afirma que se *H* for um subgrupo do grupo finito *G*, então a ordem de *H* dividirá a ordem de *G*. No caso de o grupo *G* ter 6 elementos, então basta considerar os subconjuntos contendo a unidade com 1, 2, 3 e 6 elementos, que são os divisores de 6. Como os subconjuntos de 1 e 6 elementos, nesse caso, são os subgrupos triviais, então basta considerar os subconjuntos contendo a unidade com 2 e 3 elementos. Dentre esses estarão os demais candidatos a subgrupos do grupo ***G***. Veja que, assim, reduzimos enormemente a busca inicial.

!

Lembre-se de que o número de subconjuntos contidos num conjunto com *n* elementos é 2^n.
Por exemplo, o conjunto A = {a, b} possui $2^2 = 4$ subconjuntos a saber {a}, {b}, {a, b} e Φ, onde Φ é o conjunto vazio.

Observe que no caso de G ser um grupo com 6 elementos, o número de subconjuntos contendo o elemento é $2^{6-1} = 2^5 = 32$, pois o elemento neutro é comum em todos os subconjuntos.

TEOREMA DE LAGRANGE

Sejam *G* um grupo finito e *H* um subgrupo de *G*. Então, a ordem de *H* divide a ordem de *G*.

Observações

1. Em linguagem mais simbólica, o Teorema de Lagrange afirma que, se *G* for um grupo finito e $H < G$, então $|H| \mid |G|$.

2. Atenção, a recíproca do Teorema de Lagrange é falsa, ou seja, em geral não é verdade que se um inteiro *m* dividir $|G|$ então *G* terá um subgrupo *H* de *G* com $|H| = m$.

Exemplo 1

Sabemos que $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$, com

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

é um grupo de ordem 6 e, portanto, seus subgrupos só podem ter ordem 1, 2, 3 e 6.

ATIVIDADE

1. Encontre subgrupos de S_3 de ordem 2 e 3.

Para demonstrar o Teorema de Lagrange precisaremos de um novo conceito, o de classe lateral. Futuramente, as classes laterais também serão fundamentais para a construção dos grupos quocientes.

Definição 1 (Classe Lateral)

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, chamamos de uma *classe lateral* (*à esquerda*) ao conjunto

$$aH = \{a \,.\, h \mid h \in H\}.$$

Observação

1. Se G for um grupo aditivo, então denotaremos a classe lateral aH por

$$a + H = \{a + h \mid h \in H\}.$$

2. Se e for o elemento neutro do grupo G, então $eH = H$. Mais ainda, $a \in aH$ para todo $a \in G$.

3. O conceito de *classe lateral à direita* é definido de modo análogo; é o subconjunto de G definido por

$$Ha = \{h \,.\, a \mid h \in H\},$$

onde H é um subgrupo de G e $a \in G$. No entanto, nesta última aula, não trabalharemos com as classes laterais à direita.

Sua próxima atividade desta aula será justificar a observação 2, anterior.

ATIVIDADE

2. Seja e o elemento neutro do grupo G e seja H um subgrupo de G. Mostre que:

a. $eH = H$;

b. $a \in aH$ para todo $a \in G$.

Exemplo 2

Vamos calcular as classes laterais do subgrupo $H = \{I, \beta\}$ de $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$. Estaremos usando a tabela de multiplicação de S_3, vista na Aula 18:

x	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	I	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	I	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	I	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	I	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	I

Assim, temos:

$$\alpha H = \alpha\{I,\beta\} = \{\alpha I, \alpha\beta\} = \{\alpha, \beta\alpha^2\};$$
$$\alpha^2 H = \alpha^2\{I,\beta\} = \{\alpha^2 I, \alpha^2\beta\} = \{\alpha^2, \beta\alpha\};$$
$$\beta H = \beta\{I,\beta\} = \{\beta I, \beta^2\} = \{\beta, I\} = H;$$
$$\beta\alpha H = \beta\alpha\{I,\beta\} = \{(\beta\alpha)I,\ (\beta\alpha)\beta\} = \{\beta\alpha, \alpha^2\} = \alpha^2 H;$$
$$\beta\alpha^2 H = \beta\alpha^2\{I,\beta\} = \{(\beta\alpha^2)I,\ (\beta\alpha^2)\beta\} = \{\beta\alpha^2, \alpha\} = \alpha H.$$

Observe que as classes laterais distintas, nesse caso, são H, αH e $\alpha^2 H$.

Vamos provar, agora, algumas propriedades sobre as classes laterais. Estas propriedades tornarão a demonstração do Teorema de Lagrange extremamente simples.

Proposição 1 (Propriedades das Classes Laterais)

Sejam G um grupo finito, H um subgrupo de G e $a, b \in G$.

1. $aH = bH$ se, e somente se, $b^{-1}. a \in H$.

2. Se $aH \cap bH \neq \emptyset$, então $aH = bH$, ou, equivalentemente, se $aH \neq bH$, então $aH \cap bH = \emptyset$.

3. Todas as classes laterais têm $|H|$ elementos, isto é, $|aH| = |H|$ para todo $a \in G$.

4. Existem elementos $a_1, a_2, ..., a_k \in G$, com $a_1 = e_G$, tal que

$$G = a_1 H \cup a_2 H \cup ... \cup a_k H,$$

e a união é disjunta.

Demonstração

1. ($\Rightarrow$) Vamos supor, primeiramente, que $aH = bH$. Queremos provar que $b^{-1} . a \in H$.

Sabemos que $a \in aH = bH$, logo, existe $h \in H$, tal que $a = b . h$. Portanto,

$$\begin{aligned} b^{-1} . a &= b^{-1} . (b . h); \text{ pois } a = b . h \\ &= (b^{-1} . b) . h \\ &= e . h \\ &= h \in H. \end{aligned}$$

($\Leftarrow$) Vamos, agora, supor que $b^{-1} . a \in H$. Queremos provar que $aH = bH$.

Vamos provar, inicialmente, a inclusão $aH \subset bH$. Como $b^{-1} \cdot a \in H$, então existe $h_1 \in H$, tal que $b^{-1} \cdot a = h_1$. Portanto, $a = b \cdot h_1$. Seja, agora, $a \cdot h \in aH$, um elemento genérico de aH, com $h \in H$. Então, temos

$$\begin{aligned} a \cdot h &= (b \cdot h_1) \cdot h; \text{ pois } a = b \cdot h_1 \\ &= b \cdot (h_1 \cdot h). \end{aligned}$$

Como H é subgrupo e $h, h_1 \in H$, então $h_1 \cdot h \in H$ e, portanto,

$$a \cdot h = b \cdot (h_1 \cdot h) \in bH.$$

Daí, segue que $a \cdot h \in bH$, para todo $h \in H$, ou seja, $aH \subset bH$. A inclusão contrária, $bH \subset aH$, é completamente análoga à anterior e será uma atividade para você. Portanto, segue que $aH = bH$.

ATIVIDADE

3. Prove que se $b^{-1} \cdot a \in H$, então $bH \subset aH$.

2. Se $aH \cap bH \neq \emptyset$, então existe $g \in aH \cap bH$. Portanto, $g \in aH$ e $g \in bH$. Daí, segue que existem $h_1, h_2 \in H$ tais que $g = a \cdot h_1$ e $g = b \cdot h_2$, ou seja, $a \cdot h_1 = b \cdot h_2$. Assim, temos

$$\begin{aligned} a \cdot h_1 = b \cdot h_2 &\Rightarrow (a \cdot h_1) \cdot h_1^{-1} = (b \cdot h_2) \cdot h_1^{-1} \\ &\Rightarrow a = b \cdot (h_2 \cdot h_1^{-1}) \\ &\Rightarrow b^{-1} \cdot a = b^{-1} \cdot (b \cdot h_2 \cdot h_1^{-1}) \\ &\Rightarrow b^{-1} \cdot a = h_2 \cdot h_1^{-1}. \end{aligned}$$

Como H é subgrupo e $h_1, h_2 \in H$, então $h_2 \,.\, h_1^{-1} \in H$ e, portanto, $b^{-1} \,.\, a = h_2 \,.\, h_1^{-1} \in H$. Assim, pela propriedade 1 que acabamos de provar, segue que $aH = bH$.

3. Lembre-se de que, para provar que dois conjuntos têm o mesmo número de elementos, precisamos mostrar que existe uma bijeção entre estes conjuntos.

Considere a função $f : H \to aH$ definida por $f(h) = a \,.\, h$. Vamos provar que esta função é bijetora. Pela própria definição de aH, já vemos que $\text{Im}(f) = aH$, ou seja, que f é sobrejetora.

Para provar que f é injetora, sejam $h_1, h_2 \in H$ tais que $f(h_1) = f(h_2)$. Queremos concluir que $h_1 = h_2$. Assim, temos

$$\begin{aligned} f(h_1) = f(h_2) \quad &\Rightarrow \quad a \,.\, h_1 = a \,.\, h_2 \\ &\Rightarrow \quad a^{-1} \,.\, (a \,.\, h_1) = a^{-1} \,.\, (a \,.\, h_2) \\ &\Rightarrow \quad (a^{-1} \,.\, a) \,.\, h^{-1} = (a^{-1} \,.\, a) \,.\, h_2 \\ &\Rightarrow \quad h_1 = h_2. \end{aligned}$$

o que prova que f é, de fato, injetora. Portanto, como f é uma bijeção, então aH e H têm o mesmo número de elementos, isto é, $|aH| = |H|$.

4. Como $a \in aH$, existem elementos $a_1, a_2, \ldots, a_k \in G$, com $a_1 = e_G$, tal que $G = a_1H \cup a_2H \cup \ldots \cup a_KH$. E, como cada duas classes laterais coincidem ou são disjuntas, a união $G = a_1H \cup a_2H \cup \ldots \cup a_kH$ pode ser considerada uma união disjunta.

Exemplo 3

Dado o subgrupo $H = \{I, \beta\}$ de $S_3 = \{I, \alpha, \alpha^2, \beta\alpha, \beta\alpha^2\}$, vamos obter elementos $a_1, a_2, \ldots, a_k \in S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ tal que $S_3 = a_1H \cup a_2H \cup \ldots \cup a_KH$ seja uma união disjunta.

Vimos, no Exemplo 2, que as classes laterais distintas, nesse caso, são

$$H = \{I, \beta\},\ \alpha H = \{\alpha, \beta\alpha^2\} \text{ e } \alpha^2 H = \{\alpha, \beta\alpha^2\}.$$

Então, podemos escolher $a_1 = I$, $a_2 = \alpha$ e $a_3 = \alpha^2$, e temos que

$$S_3 = H \cup \alpha H \cup \alpha^2 H$$

é uma união disjunta.

Estamos, agora, em condições de completar a demonstração do Teorema de Lagrange.

Demonstração do Teorema de Lagrange

Pela Proposição 1.4, sabemos que existem $a_1, a_2, ..., a_k \in G$, com $a_1 = e_G$, tal que

$$G = a_1H \cup a_2H \cup a_2H \cup .... \cup a_kH,$$

e a união é disjunta. Como a união é disjunta, o número de elementos de G é igual à soma do número de elementos de cada classe lateral da união, ou seja,

$$|G| = |a_1H| + |a_2H| + ... + |a_kH|.$$

Agora, pela Proposição 1.3, sabemos que

$$|a_iH| = |H| \text{ para todo } i = 1, 2, ..., k.$$

Fazendo as devidas substituições na equação anterior, temos

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + ... + |a_kH| \\ &= |H| + |H| + ... + |H|; \ (k \text{ parcelas}) \\ &= k\,|H|. \end{aligned}$$

Portanto, $|G| = k|H|$ com k um inteiro positivo, ou seja, $|H|$ divide $|G|$.

Observe como esta demonstração ficou extremamente simples. Isso não quer dizer que o Teorema de Lagrange é fácil de ser provado, significa, simplesmente, que todo o trabalho duro foi feito anteriormente, neste caso, na Proposição 1. Agora, o Teorema de Lagrange tem conseqüências importantes e muito elegantes. Vamos a elas!

COROLÁRIO 1

Sejam G um grupo finito e $a \in G$, então a ordem de a divide a ordem de G, isto é, ord(a)||G|.

Demonstração

O subgrupo gerado por a, $<a>$, é um subgrupo do grupo finito G. Logo, pelo Teorema de Lagrange, temos que |$<a>$|||G|. Mas, como por definição, a ordem do elemento a é a ordem do subgrupo gerado por a, ou seja, ord(a) = |$<a>$|, segue que ord(a)||G|.

COROLÁRIO 2

Sejam G um grupo finito de ordem n e $a \in G$, então $a^n = e_G$.

Demonstração

Seja m a ordem do elemento a. De acordo com o Corolário 1, $m \mid n$, ou seja, existe um inteiro k, tal que $n = km$. Vimos, na aula passada, que a ordem m de a é o menor inteiro positivo, tal que $a^m = e_G$. Assim,

$$a^n = a^{mk} = (a^m)^k = (e_G)^k = e_G.$$

O próximo corolário do Teorema de Lagrange é especialmente elegante.

COROLÁRIO 3

Todo grupo de ordem primo é cíclico.

Demonstração

Seja G um grupo de ordem primo p. Como p > 1, então existe $a \in G$ com $a \neq e_G$. Agora, como $a \neq e_G$, então ord(a) > 1. Por outro lado, pelo Corolário 1, ord(a)||G|, ou seja, ord(a) | p. Mas, como p é primo, então seus únicos divisores positivos são 1 e p e, como ord(a) >*1*. Assim, só resta a possibilidade ord(a) = p. Isto significa que o subgrupo $<a>$ gerado por a tem o mesmo número de elementos que G e, como $<a> \subset G$, segue que $<a>$ = G, ou seja, G é um grupo cíclico.

Temos, agora, uma demonstração muito simples do Pequeno Teorema de Fermat.

COROLÁRIO 4 (PEQUENO TEOREMA DE FERMAT)

Sejam p um número primo e a um inteiro tal que a não divide p. Então $a^{p-1} \equiv 1 (\text{mod } p)$.

Demonstração

Vimos, na Aula 17, que

$$Z_p^{\times} = \{\overline{k} \in Z_p \mid mdc(k, p) = 1\} = \{\overline{1}, \ldots, \overline{p-1}\}$$

é um grupo multiplicativo com $|Z_p^{\times}| = p - 1$. Como $a \Phi p$ e p é primo, então $mdc(a, p) = 1$ e, portanto, $\overline{a} \in Z_p^{\times}$. Logo, pelo Corolário 2,

$$(\overline{a})^{p-1} = \overline{1},$$

o que significa que $a^{p-1} \equiv 1 \pmod{p}$.

A demonstração anterior pode ser generalizada para obter, agora, uma demonstração extremamente simples do importante teorema de Euler. Lembre, da Aula 17, que

$$Z_n^{\times} = \{\overline{a} \in Z_n \mid mdc(a,n) = 1\}$$

é um grupo multiplicativo finito. Sua ordem é denotada por $\varphi(n)$, onde

$$\varphi(n) = \left| \{k \in Z \mid 1 \leq k < n \text{ e } mdc(k, n) = 1\} \right|$$

é a *função de Euler*, ou seja, $\varphi(n)$ é o número de inteiros k, tais que $1 \leq k < n$ e $mdc(k, p)$. Veja que no caso de um número primo p, temos

$$\begin{aligned} \varphi(p) &= \left| \{k \in Z \mid 1 \leq k < p \text{ e } mdc(k, p) = 1\} \right| \\ &= \left| \{1, 2, \ldots, p-1\} \right| \\ &= p - 1. \end{aligned}$$

COROLÁRIO 4 (TEOREMA DE EULER)

Sejam $n > 1$ um número inteiro e a um inteiro, tal que $mdc(a, n) = 1$. Então $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Observe que o Pequeno Teorema de Fermat é o caso particular do Teorema de Euler em que n é um primo p. A demonstração do Teorema de Euler será uma atividade final para você.

ATIVIDADES FINAIS

1. a. Calcule todas as classes laterais distintas do subgrupo $H = \{I, \alpha, \alpha^2\}$ de $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$.

b. Obtenha elementos $a_1, a_2, \ldots, a_k \in S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$, tal que $S_3 = a_1H \cup a_2H \cup \ldots \cup a_KH$ seja uma união disjunta.

2. Prove o Teorema de Euler.

RESUMO

O importante Teorema de Lagrange afirma que se G é um grupo finito e $H < G$, então $|H| \mid |G|$. Para provar esse teorema, foi preciso introduzir o conceito de classe lateral (à esquerda), ou seja, o conjunto $aH = \{a \,.\, h \mid h \in H\}$, onde $H < G$ e $a \in G$. Depois, vimos várias conseqüências do Teorema de Lagrange:

1. Se G for um grupo finito e $a \in H$, então $\text{ord}(a) \mid |G|$.
2. Se G for um grupo finito com $|G| = n$ e $a \in G$, então $a^n = e_G$.
3. (Pequeno Teorema de Fermat) Se p for primo e $a \Phi p$, então $a^{p-1} \equiv 1 (\text{mod } p)$.
4. (Teorema de Euler) Se $n > 1$ for inteiro e $mdc(a, n) = 1$, então $a^{\varphi(n)} \equiv 1 \ (\text{mod } n)$.

RESPOSTAS COMENTADAS

Atividade 1

Como $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in S_3$ tem ordem 2, já que $\beta^2 = I$, então

$$<\beta> = \{I, \beta\}$$

será um subgrupo de S_3 de ordem 2. Agora, como $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ tem ordem 3, já que $\alpha^3 = I$, então

$$< \alpha > = \{I, \alpha, \alpha^2\}$$

será um subgrupo de S_3 de ordem 3.

Atividade 2

a. Basta observar que $e \,.\, h = h$, para todo $h \in H$. Daí,

$$eH = \{e \,.\, h \mid h \in H\}$$

$$= \{h \mid h \in H\}; \textit{pois } e \,.\, h = h$$

$$= H.$$

b. Como $e \in H$, então $a = a \,.\, e \in aH$.

Atividade 3

Como $b^{-1}.\, a \in H$, então existe $h_1 \in H$, tal que $b^{-1}.\, a = h_1$. Portanto, $a = b \,.\, h_1$ e, daí, $b = a \,.\, h_1^{-1}$. Seja, agora, $b \,.\, h \in bH$, um elemento genérico de bH, com $h \in H$. Assim,

$$b \,.\, h = (a \,.\, h_1^{-1}) \,.\, h; \text{ pois } b = a \,.\, h_1^{-1}.$$

$$= a \,.\, (a \,.\, h_1^{-1}).$$

Como H é subgrupo e $h, h_1 \in H$, então $h_1^{-1} \,.\, h \in H$ e, portanto,

$$b \,.\, h = a\,(h_1^{-1} \,.\, h) \in aH.$$

Daí, segue que $b, h \in aH$, para todo $h \in H$, ou seja, $bH \subset aH$.

Atividade Final 1

a. Pela tabela de multiplicação de S_3,

x	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	I	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	I	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	I	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	I	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	I

temos:

$$\alpha H = \alpha\{I, \alpha, \alpha^2\} = \{\alpha I, \alpha^2, \alpha^3\} = \{\alpha, \alpha^2, I\} = H;$$
$$\alpha^2 H = \alpha^2\{I, \alpha, \alpha^2\} = \{\alpha^2 I, \alpha^3, \alpha^4\} = \{\alpha^2, I, \alpha\} = H;$$
$$\beta H = \beta\{I, \alpha, \alpha^2\} = \{\beta I, \beta\alpha, \beta\alpha^2\} = \{\beta, \beta\alpha, \beta\alpha^2\};$$
$$\beta\alpha H = \beta\alpha\{I, \alpha, \alpha^2\} = \{(\beta\alpha)I, (\beta\alpha)\alpha, (\beta\alpha)\alpha^2\} = \{\beta\alpha, \beta\alpha^2, \beta\} = \beta H;$$
$$\beta\alpha^2 H = \beta\alpha^2\{I, \alpha, \alpha^2\} = \{(\beta\alpha^2)I, (\beta\alpha^2)\alpha, (\beta\alpha^2)\alpha^2\} = \{\beta\alpha^2, \beta, \beta\alpha\} = \beta H.$$

Observe que as classes laterais distintas, nesse caso, são H e βH.

b. Vimos, na parte *a* Atividade Final 1, que as classes laterais distintas são

$$H = \{I, \alpha, \alpha^2\} \text{ e } \beta H = \{\beta, \beta\alpha, \beta\alpha^2\}.$$

Então, por exemplo, podemos escolher $a_1 = I$ e $a_2 = \beta$, e temos que

$$S_3 = H \cup \beta H$$

é uma união disjunta.

Atividade Final 2

Como $mdc(a, n) = 1$, então $\bar{a} \in Z^{\times}_n$. Agora, $Z^{\times}_n$ é um grupo de ordem $\varphi(n)$ e, portanto, pelo Corolário 2, temos $(\bar{a})^{\varphi(n)} = \bar{1}$, o que significa que $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$.

Classes laterais e o grupo quociente

AULA 16

Meta da aula

Apresentar os conceitos de classes laterais à esquerda e classes laterais à direita, suas propriedades, e o conceito de grupo quociente.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Identificar e calcular classes laterais.
- Identificar em que condições uma operação se torna bem definida no conjunto das classes laterais à esquerda.
- Identificar as características de um grupo quociente.

Pré-requisitos

Você vai precisar dos conhecimentos sobre grupos das Aulas 12 a 15.

INTRODUÇÃO

Na aula anterior apresentamos e provamos o Teorema de Lagrange. Ele é um dos teoremas mais importantes da teoria dos grupos e afirma que a ordem de todo subgrupo divide a ordem do grupo finito. Para provar o Teorema de Lagrange, foi preciso introduzir o conceito de classe lateral de um grupo. Mais precisamente, vimos os conceitos de classe lateral à esquerda e classe lateral à direita. Na demonstração do Teorema de Lagrange foi necessário trabalhar apenas com as classes laterais à esquerda. No entanto, um dos objetivos desta aula é a construção dos grupos quocientes que desempenham, em teoria dos grupos, um papel análogo aos anéis quocientes em teoria dos anéis. Na construção dos grupos quocientes será necessário lidar com subgrupos em que as classes laterais à esquerda e à direita são iguais. Estes subgrupos são chamados de subgrupos normais e serão nosso objeto de estudo na próxima aula.

Vamos iniciar revendo os conceitos de classe lateral à esquerda e à direita.

DEFINIÇÃO 1 (CLASSE LATERAL)

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, chamamos de uma *classe lateral à esquerda de G com respeito a H* ao conjunto

$$aH = \{a \,.\, h \mid h \in H\}.$$

De modo análogo, chamamos de *classe lateral à direita de G com respeito a H* ao conjunto

$$Ha = \{h \cdot a \mid h \in H\}.$$

Observações

1. Se G é um grupo aditivo, então denotamos a classes laterais aH e Ha por

$$a + H = \{a + h \mid h \in H\}$$

e

$$H + a = \{h + a \mid h \in H\},$$

respectivamente.

2. Se e é o elemento neutro do grupo G, vimos que $eH = He = H$. Mais ainda, $a \in aH$ e $a \in Ha$ para todo $a \in G$.

Exemplo 1

Seja G o grupo aditivo dos números inteiros, ou seja, o grupo $(Z, +)$. Considere, agora, o subgrupo

$$H = 4Z = \{4t \mid t \in Z\}$$

dos múltiplos de 4. Vamos calcular todas as classes laterais à esquerda de H. Já sabemos, pela Observação 2, que

$$0 + H = H + 0 = H.$$

Agora, veja que

$$1 + H = \{1 + h \mid h \in H\} = \{1 + 4t \mid t \in Z\}$$

consiste em todos os inteiros que deixam resto 1 na divisão por 4. Da mesma forma,

$$2 + H = \{2 + h \mid h \in H\} = \{2 + 4t \mid t \in Z\}$$

consiste em todos os inteiros que deixam resto 2 na divisão por 4, e

$$3 + H = \{3 + h \mid h \in H\} = \{3 + 4t \mid t \in Z\}$$

consiste em todos os inteiros que deixam resto 3 na divisão por 4. Pelo Algoritmo da Divisão em $\mathbf{Z}$, o resto da divisão de qualquer inteiro por 4 só pode ser 0, 1, 2 ou 3. Assim, todo inteiro pertence a uma das classes laterais $H = 0 + H$, $1 + H$, $2 + \mathrm{H}$ ou $3 + H$. Portanto,

$$H = 0 + H,\ 1 + H,\ 2 + H \text{ e } 3 + H$$

são as únicas classes laterais à esquerda de $H = 4\mathbf{Z}$ em $\mathbf{Z}$.

ATIVIDADE

1. Mostre que $H = H + 0, H + 1, H + 2$ e $H + 3$ são as únicas classes laterais à direita de $H = 4Z$ em $(Z, +)$.

Como você observou na Atividade 1, $H + 1$ consiste nos inteiros que deixam resto 1 na divisão por 4, $H + 2$ consiste nos inteiros que deixam resto 2 na divisão por 4 e $H + 3$ consiste nos inteiros que deixam resto 3 na divisão por 4, segue que

$0 + H = H + 0 = H$; $1 + H = H + 1$; $2 + H = H + 2$ e $3 + H = H + 3$.

Ou seja, as classes laterais à esquerda e à direita são iguais, sempre que obtidas com o mesmo elemento,

$$a + H = H + a \text{ para todo } a \in Z.$$

No entanto, nem sempre isto acontece, como veremos no próximo exemplo.

Exemplo 2

Seja G o grupo $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ das permutações de 3 elementos, onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

e seja $H = \{ I, \beta \}$. Para fins de consulta, lembre-se de que a tabela de multiplicação do grupo S_3 é dada por

x	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	I	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	I	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	I	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	I	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	I

No Exemplo 2 da Aula 20, vimos que apenas três classes laterais à esquerda com respeito a H, que são:

$$IH = \{I,\ \beta\} = H;\ \alpha H = \{\alpha, \beta\alpha^2\};\ \alpha^2 H = \{\alpha^2, \beta\alpha\};$$

pois, as demais são cópias das já obtidas:

$$\beta H = \{\beta, I\} = H;\ \beta\alpha H = \{\beta\alpha, \alpha^2\} = \alpha^2 H;\ \beta\alpha^2 H = \{\beta\alpha^2, \alpha\} = \alpha H.$$

Observe que temos três classes laterais à esquerda distintas: H, aH e $\alpha^2 H$. Na próxima atividade, você vai calcular as classes laterais à direita com respeito à H.

ATIVIDADE

2. Mostre que as classes laterais à direita com respeito a $H = \{I,\ \beta\}$, em S_3, são

$$HI = \{I,\ \beta\} = H;\ H\alpha = \{\alpha, \beta\alpha\};\ H\alpha^2 = \{\alpha^2, \beta\alpha^2\};$$

Observe que temos três classes laterais à esquerda distintas: H, $H\alpha$ e $H\alpha^2$. Comparando as classes laterais à esquerda com as classes laterais à direita, temos

$$\alpha H = \{\alpha, \beta\alpha^2\} = H\alpha^2 \text{ e } \alpha^2 H = \{\alpha^2, \beta\alpha\} = \alpha H.$$

Portanto, temos que

$$\alpha H \neq H\alpha \text{ e } \alpha^2 H \neq H\alpha^2,$$

diferente do que ocorreu no exemplo anterior, ou seja, encontramos elementos $a \in S_3$ tais que

$$aH \neq Ha.$$

Nas seguintes proposições, vamos relembrar algumas propriedades fundamentais das classes laterais. Estas propriedades já foram estudadas na aula passada.

PROPOSIÇÃO 1 (PROPRIEDADES DAS CLASSES LATERAIS À ESQUERDA)

Sejam G um grupo, H um subgrupo de G e $a, b \in G$.

1. $aH \neq bH$ se, e somente se, $b^{-1} \cdot a \in H$.

2. Se $aH \cap bH \neq \emptyset$, então $aH = bH$. Ou, equivalentemente, se $aH \neq bH$, então $aH \cap bH = \emptyset$.

3. Se G é um grupo finito, então todas as classes laterais têm $|H|$ elementos, isto é, $|aH| = |H|$ para todo $a \in G$. Em outras palavras, todas as classes laterais à esquerda têm o mesmo número de elementos.

4. Se G é um grupo finito, então existem elementos $a_1, a_2, ..., a_k \in G$, com $a_1 = e_G$, tal que

$$G = a_1H \cup a_2H \cup ... \cup a_kH,$$

e a união é disjunta.

Uma propriedade idêntica, com uma demonstração análoga, vale para as classes laterais à direita.

PROPOSIÇÃO 2 (PROPRIEDADES DAS CLASSES LATERAIS À DIREITA)

Sejam G um grupo, H um subgrupo de G e $a, b \in G$.

1. $Ha = Hb$ se, e somente se, $a \cdot b^{-1} \in H$.

2. Se $Ha \cap Hb \neq \emptyset$, então, $Ha = Hb$. Ou, equivalentemente, se $Ha \neq Hb$, então $Ha \cap Hb \neq \emptyset$.

3. Se G é um grupo finito, então todas as classes laterais têm $|H|$ elementos, isto é, $|Ha| = |H|$ para todo $a \in G$. Em outras palavras, todas as classes laterais à direita têm o mesmo número de elementos.

4. Se G é um grupo finito, então existem elementos $a_1, a_2, ..., a_2 \in G$ com $a_1 = e_G$, tal que

$$G = Ha_1 \cup Ha_2 \cup ... \cup Ha_k,$$

e a união é disjunta.

Uma conseqüência destas propriedades é que existem o mesmo número de classes laterais à esquerda e à direita, mesmo que não sejam iguais, no sentido de que existam elementos $a \in G$ tais que

$$aH \neq Ha.$$

No entanto, um caso especial e muito importante é quando elas coincidem, ou seja, quando

$$aH = Ha \quad \text{para todo } a \in G.$$

Neste caso, poderemos fazer a construção dos chamados grupos quocientes que são semelhantes aos anéis quocientes já estudados anteriormente. Na verdade, veremos que a condição $aH = Ha$, para todo $a \in G$, permitirá definir uma operação binária no conjunto

$$G/H = \{aH \mid a \in G\}$$

das classes laterais que fará deste conjunto um grupo, chamado grupo quociente. Mas isto é uma longa história que só terminará na próxima aula.

DEFINIÇÃO 2 (CONJUNTO DAS CLASSES LATERAIS)

Sejam G um grupo e H um subgrupo de G. Denotamos por

$$G/H = \{aH \mid a \in G\}$$

o *conjunto das classes laterais à esquerda com respeito a H*.

Exemplo 3

Seja G o grupo $(\mathbf{Z}, +)$ e $H = 4\mathbf{Z} = \{4t \mid t \in \mathbf{Z}\}$. Pelo que vimos no Exemplo 1, as únicas classes laterais à esquerda com respeito a $H = 4\mathbf{Z}$ são $H = 0 + H$, $1 + H$, $2 + H$ e $3 + H$. Logo,

$$G/H = \{H, 1 + H, 2 + H, 3 + H\}$$

ou ainda, particularizando a notação para este exemplo, temos

$$Z/4Z = \{4Z, 1 + 4Z, 2 + 4Z, 3 + 4Z\}.$$

Exemplo 4

Seja G o grupo $S_3 = \{I, \alpha, \alpha^2\beta, \beta\alpha, \beta\alpha^2\}$ das permutações de 3 elementos, onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{e} \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

e seja o subgrupo $H = \{I, \alpha, \alpha^2\}$. Usando a tabela de multiplicação de S_3, contida no Exemplo 2, temos que

$$IH = I\{I,\ \alpha,\ \alpha^2\} = \{II,\ I\alpha,\ I\alpha^2\} = \{I,\ \alpha,\ \alpha^2\} = H;$$
$$\alpha H = \alpha\{I,\ \alpha,\ \alpha^2\} = \{\alpha I,\ \alpha\alpha,\ \alpha\cdot\alpha^2\} = \{\alpha,\ \alpha^2,\ I\} = H;$$
$$\alpha^2 H = \alpha^2\{I,\ \alpha,\ \alpha^2\} = \{\alpha^2 I,\ \alpha^2\cdot\alpha, \alpha\cdot\alpha^2\} = \{\alpha^2,\ I, \alpha\} = H;$$
$$\beta H = \beta\{I,\ \alpha,\ \alpha^2\} = \{\beta I,\ \beta\alpha,\ \beta\alpha^2\} = \{\beta,\ \beta\alpha,\ \beta\alpha^2\};$$
$$(\beta\alpha)\mathrm{H} = (\beta\alpha)\{\mathrm{I},\ \alpha,\ \alpha^2\} = \{\beta\alpha\cdot\mathrm{I},\ \beta\alpha\cdot\alpha,\ \beta\alpha\cdot\alpha^2\} =$$
$$\{\beta\alpha,\ \beta\alpha^2,\ \beta\} = \beta H;$$
$$(\beta\alpha^2)H = (\beta\alpha^2)\{I,\ \alpha,\ \alpha^2\} = \{\beta\alpha^2\cdot I,\ \beta\alpha^2\cdot\alpha,\ \beta\alpha^2\cdot\alpha^2\} =$$
$$\{\beta\alpha^2,\ \beta,\ \beta\alpha\} = \beta H.$$

Portanto,

$$G/H = \{H,\ \beta H\}.$$

ATIVIDADE

3. Mostre que as classes laterais à direita com respeito a $H = \{I, \alpha, \alpha^2\}$, em S_3, são iguais às respectivas classes laterais à esquerda, calculadas no Exemplo 4.

Nosso projeto, agora, é construir uma operação binária no conjunto das classes laterais $G/H = \{aH \mid a \in G\}$ de modo a torná-lo um grupo. A forma natural de definirmos uma operação binária em G/H será reproduzir o que foi feito para os anéis quocientes. Vamos formalizar estas idéias.

DEFINIÇÃO 2 (OPERAÇÃO EM G/H)

Sejam G um grupo e H um subgrupo de G. Definimos a seguinte operação no conjunto das classes laterais $G/H = \{aH \mid a \in G\}$:

$$aH \,.\, bH = (ab)H \text{ para todo } aH, bH \in G/H.$$

No entanto, precisamos saber se esta operação está bem definida, ou seja, se ela independe da escolha dos representantes a e b das classes laterais aH e bH, respectivamente. Nesta primeira etapa, vamos provar que se as classes laterais à esquerda e à direita coincidem, isto é, se

$$aH = Ha \text{ para todo } a \in G,$$

então a operação binária acima estará, de fato, bem definida em G/H.

Proposição 3

Sejam G um grupo e H um subgrupo de G tal que $aH = Ha$ para todo $a \in G$. Se $aH = a_1H$ e $bH = b_1H$, com $a, a_1, b, b_1 \in G$, então

$$aH \cdot bH = a_1H \cdot b_1H,$$

ou, equivalentemente,

$$abH = a_1b_1H.$$

Isto significa que a operação em G/H não depende dos representantes a e b escolhidos nas classes laterais aH e bH.

Demonstração

Para concluir que $(ab)H = (a_1b_1)H$, provaremos as duas inclusões $(ab)H \subset (a_1b_1)H$ e $(a_1b_1)H \subset (ab)H$.

Seja $abh \in (ab)H$, $h \in H$, um elemento genérico de abH. Vamos provar que $abh \in (a_1b_1)H$. Como $a \in aH = a_1H$, então existe $h_1 \in H$ tal que $a = a_1h_1$. Analogamente, de $b \in bH = b_1H$, existe $h_2 \in H$ tal que $b = b_1h_2$. Agora, é aqui o ponto crucial, como $Hb_1 = b_1H$ e $h_1b_1 \in Hh_1$, então, existe $h_3 \in H$ tal que $h_1b_1 = b_1h_3$. Logo, juntando todas estas informações, temos

$$\begin{aligned} abh &= (a_1h_1)(b_1h_2)h; \ \textit{pois}\ a = a_1h_1 \text{ e } b = b_1h_2 \\ &= a_1(h_1b_1)h_2h; \ \text{pela lei associativa} \\ &= a_1(b_1h_3)h_2h; \ \text{pois } h_1b_1 = b_1h_3 \\ &= a_1b_1(h_3h_2h); \ \text{pela lei associativa} \\ &= a_1b_1h_4 \in a_1b_1H; \ \text{pois } h_4 = h_3h_2h \in H. \end{aligned}$$

Isto prova que $abh \in (a_1b_1)H$ e, portanto, que $(ab)H \subset (a_1b_1)H$. A inclusão contrária, $(a_1b_1)H \subset (ab)H$, é feita de modo análogo e será uma de suas atividades finais.

Exemplo 5

Seja G o grupo $(\mathbf{Z}, +)$ e $\boldsymbol{H} = 4\mathbf{Z} = \{4t \mid t \in \mathbf{Z}\}$. Pelo que vimos no Exemplo 3,

$$G/H = Z/4Z = \{4Z,\ 1+4Z,\ 2+4Z,\ 3+4Z\}.$$

Lembre, do curso de Álgebra I, que

$$4Z = 0+4Z = \overline{0}; 1+4Z = \overline{1}\ ; 2+4Z = \overline{2}, 3+4Z = \overline{3}.$$

Logo,

$$Z/4Z = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\}.$$

Como

$$a+4Z = 4Z+a$$

para todo $a \in \mathbf{Z}$, então, pela Proposição 3, a operação binária está bem definida em $\mathbf{Z}/4\mathbf{Z}$. Mais precisamente, temos que

$(a+4Z)+(b+4Z)=(a+b)+4Z$ para todo $a, b \in Z$,

ou, equivalentemente,

$$\overline{a}+\overline{b}=\overline{a+b} \quad \text{para todo } a, b \in \mathbf{Z}.$$

A tabela desta operação, em $\mathbf{Z}/4\mathbf{Z}$, é dada por

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$

Podemos, agora, concluir a construção do grupo quociente.

Teorema 1 (O Grupo Quociente)

Sejam G um grupo e H um subgrupo de G tal que $aH = Ha$ para todo $a \in G$. Então G/H, munido da operação definida em G/H, é um grupo. Chamamos este grupo de *grupo quociente de G com respeito a H*.

Em particular, $eH = H$ é o elemento neutro do grupo e $a^{-1}H$ é o elemento inverso de aH. Denotamos isto por

$$e_{G/H} = e_G H = H \quad \text{e} \quad (aH)^{-1} = a^{-1}H$$

Demonstração

Como $aH = Ha$ para todo $a \in G$, então, pela Proposição 3, a operação de G/H está bem definida. Vamos verificar os axiomas de grupo para $(G/H, .)$.

$G1$. A operação é associativa:

$$\begin{aligned} aH \cdot (bH \,.\, cH) &= aH \cdot (bc)H \\ &= (a(bc))H \\ &= ((ab)c)H; \text{ pela associatividade em } G \\ &= (ab)H \,.\, cH \\ &= (aH \,.\, bH) \cdot cH. \end{aligned}$$

$G2$. O elemento neutro é $eH = H$ com e o elemento neutro de G:

$$aH \,.\, eH = (ae)H = aH \text{ e } eH \,.\, aH = (ea)H = aH.$$

Denotamos este elemento por $e_{G/H} = e_{GH} = H$.

$G3$. O elemento inverso de $aH \in G/H$ é $a^{-1}H$:

$$aH \cdot a^{-1}H = (aa^{-1})H = eH \text{ e } a^{-1}H \,.\, aH = (a^{-1}a)H = eH.$$

Denotamos este elemento por $(aH)^{-1} = a^{-1}H$.

Exemplo 6

Seja G o grupo $(\mathbf{Z}, +)$ e $H = 4Z = \{4t \mid t \in Z\}$. Como vimos no Exemplo 5,

$$G/H = Z/4Z = \{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3}\}$$

é um grupo quociente cujo elemento neutro é $e_{G/H} = 0 + 4Z = \bar{0}$. Observe que ele coincide com o grupo $(\mathbf{Z}_4, +)$ das classes residuais módulo 4.

ATIVIDADES FINAIS

1. Seja G o grupo $S_3 = \{I,\ \alpha,\ \alpha^2,\ \beta,\ \beta\alpha,\ \beta\alpha^2\}$ das permutações de 3 elementos, onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

e seja o subgrupo $H = \{I, \alpha, \alpha^2\}$. Conclua que a operação em G/H está bem definida e monte a tabela de operação do grupo quociente.

2. Sejam G um grupo, H um subgrupo de G e $a, b \in G$. Mostre que $Ha = Hb$ se, e somente se, $a \cdot b^{-1} \in H$.

3. Sejam G um grupo e H um subgrupo de G tal que $aH = Ha$ para todo $a \in G$. Se $aH = a_1H$ e $bH = b_1H$, com $a, a_1, b, b_1 \in G$, então prove que $(a_1b_1)H \subset (ab)H$.

RESUMO

Nesta aula revimos os conceitos de classe lateral à esquerda e classe lateral à direita:

$$aH = \{a \cdot h \mid h \in H\} \text{ e } Ha = \{h \cdot a \mid h \in H\}.$$

Em seguida, vimos as propriedades das classes laterais à esquerda e das classes laterais à direita:

1. $aH = bH$ se, e somente se, $b^{-1} \cdot a \in H$.
2. Se $aH \cap bH \neq \emptyset$, então $aH = bH$. Ou, equivalentemente, se $aH \neq bH$, então, $aH \cap bH \neq \emptyset$.
3. Se G é um grupo finito então, todas as classes laterais têm $|H|$ elementos, isto é, $|aH| = |H|$ para todo $a \in G$.
4. Se G é um grupo finito, então existem elementos $a_1, a_2, \ldots, a_k \in G$ com $a_1 = e_G$, tal que

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH,$$

e a união é disjunta.

5. $Ha = Hb$ se, e somente se, $a \cdot b^{-1} \in H$.

6. Se $Ha \cap Hb \neq \emptyset$, então, $Ha = Hb$. Ou, equivalentemente, se $Ha \neq Hb$, então $Ha \cap Hb = \emptyset$.

7. Se G é um grupo finito, então todas as classes laterais têm $|H|$ elementos, isto é, $|Ha| = |H|$ para todo $a \in G$.

8. Se G é um grupo finito, então existem elementos $a_1, a_2, ..., a_k \in G$, com $a_1 = e_G$, tal que

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k,$$

e a união é disjunta.

Depois, vimos que no conjunto das classes laterais à esquerda,

$$G/H = \{aH \mid a \in G\},$$

podemos definir a operação

$$aH.bH = (ab)H \text{ para todo } aH,\ bH \in G/H$$

Em seguida, vimos que esta operação está bem definida sempre que $aH = Ha$ para todo $a \in G$, isto é, se as classes laterais à esquerda e à direita coincidem. Neste caso, construímos o grupo quociente G/H.

RESPOSTAS COMENTADAS

Atividade1

Pela Observação 2, já sabemos que

$$0 + H = H + 0 = H$$

Agora, veja que

$$H + 2 = \{h + 2 \mid h \in H\} = \{4t + 2 \mid t \in Z$$

consiste em todos os inteiros que deixam resto 1 na divisão por 4. Da mesma forma,

$$H + 2 = \{h + 2 \mid h \in H\} = \{4t + 2 \mid t \in Z\}$$

consiste em todos os inteiros que deixam resto 2 na divisão por 4, e

$$H + 3 = \{h + 3 \mid h \in H\} = \{4t + 3 \mid t \in Z\}$$

consiste em todos os inteiros que deixam resto 3 na divisão por 4. Pelo Algoritmo da Divisão em Z, o resto da divisão de qualquer inteiro por 4 só pode ser 0, 1, 2 ou 3. Assim todo inteiro pertence a uma das classes laterais $H = H + 0$, $H + 1$, $H + 2$ ou $H + 3$. Portanto,

$$H = H + 0, H + 1, H + 2 \text{ e } H + 3$$

são as únicas classes laterais à direita de $H = 4Z$ em Z.

Atividade 2

Usando a tabela de multiplicação de S_3, temos

$HI = \{I, \beta\}I = \{H, \beta I\} = \{I, \beta\} = H;$
$H\alpha = \{I, \beta\}\alpha = \{I\alpha, \beta\alpha\} = \{\alpha, \beta\alpha\};$
$H\alpha^2 = \{I, \beta\}\alpha^2 = \{I\alpha^2, \beta\alpha^2\} = \{\alpha^2, \beta\alpha^2\};$
$H\beta = \{I, \beta\}\beta = \{I\beta, \beta^2\} = \{\beta, I\} = H;$
$H\beta\alpha = \{I, \beta\}\beta\alpha = \{I \,.\, \beta\alpha, \beta \,.\, \beta\alpha\} = \{\beta\alpha, \alpha\} = H\alpha;$
$H\beta a^2 = \{I, \beta\}\beta\alpha^2 = \{I \,.\, \beta\alpha^2, \beta \,.\, \beta\alpha^2\} = \{\beta\alpha^2, \alpha^2\} = H\alpha^2.$

Assim, obtemos somente três classes laterais distintas: H, $H\alpha$ e $H\alpha^2$.

Atividade 3

Usando a tabela de multiplicação de S_3, contida no Exemplo 2, vamos calcular todas as classes laterais:

$H\alpha = \{I,\ \alpha,\ \alpha^2\}\alpha = \{I \cdot \alpha,\ \alpha \cdot \alpha,\ \alpha^2 \cdot \alpha\} = \{\alpha,\ \alpha^2,\ I\} = \alpha H = H;$
$H\alpha^2 = \{I,\ \alpha,\ \alpha^2\}\alpha^2 = \{I \cdot \alpha^2,\ \alpha \cdot \alpha^2,\ \alpha^2 \cdot \alpha^2\} = \{\alpha^2,\ \mathrm{I},\ \alpha\} =$
$\alpha^2 H = H;$
$H\beta = \{I,\ \alpha,\ \alpha^2\}\beta = \{I \,.\, \beta,\ \alpha.\beta,\ \alpha^2.\beta\} = \{\beta,\ \beta\alpha^2,\ \beta\alpha\} = \beta H;$
$H(\beta\alpha) = \{I,\ \alpha,\ \alpha^2\}(\beta\alpha) = \{I \cdot \beta\alpha,\ \alpha \cdot \beta\alpha,\ \alpha^2 \cdot \beta\alpha\} = \{\beta\alpha,\ \beta,\ \beta\alpha^2\} =$
$(\beta\alpha)H = \beta H;$
$H(\beta\alpha^2) = \{I,\ \alpha,\ \alpha^2\}(\beta\alpha^2) = \{I \cdot \beta\alpha^2,\ \alpha \cdot \beta\alpha^2,\ \alpha^2 \cdot \beta\alpha^2\} =$
$\{\beta\alpha^2,\ \beta\alpha, \beta\} = (\beta\alpha^2)H = \beta H.$

Atividade Final 1

Vimos, na Atividade 3, que $aH = Ha$ para todo $a \in S_3$. Portanto, pela Proposição 3, a operação em G/H está bem definida. Temos que

$$G/H = \{H, \beta H\},$$

A tabela da operação em G/H é dada por

X	H	βH
H	H	βH
βH	βH	H

pois, $\beta H \cdot \beta H = \beta^2 H = IH = H$

onde H é o elemento neutro de G/H.

Atividade Final 2

($\Rightarrow$) Vamos supor, primeiramente, que $Ha = Hb$. Queremos provar que $a \,.\, b^{-1} \in H$. Sabemos que $a \in Ha = Hb$, logo, existe $h \in H$ tal que $a = h \,.\, b$. Portanto,

$$\begin{aligned} a.b^{-1} &= (h.b) \cdot \mathrm{b}^{-1}\,;\ \text{pois } a = h.b \\ &= h \cdot (b\,.b^{-1}) \\ &= h\,.\,e \\ &= h \in H. \end{aligned}$$

($\Leftarrow$) Vamos, agora, supor que $a \,.\, b^{-1} \in H$. Queremos provar que $Ha = Hb$.

Vamos provar, inicialmente, a inclusão $Ha \subset Hb$. Como $a \,.\, b^{-1} \in H$, então, existe $h_1 \in H$ tal que $a \,.\, b^{-1} = h_1$. Portanto, $a = h_1 \,.\, b$. Seja, agora, $h \,.\, a \in Ha$, $h \in H$, um elemento genérico de Ha. Então, temos

$$\begin{aligned} h.a &= h \cdot (h_1 \cdot b)\,;\ \text{pois } a = h_1 \cdot b \\ &= (h.h_1) \cdot \mathrm{b}. \end{aligned}$$

Como H é subgrupo e $h, h_1 \in H$, então $h_1 \,.\, h \in H$ e, portanto,

$$h.a = (h.h_1) \cdot b \in Hb.$$

Daí, segue que $h \cdot a \in Hb$ para todo $h \in H$, ou seja, $Ha \subset Hb$. A inclusão contrária, $Hb \subset Ha$, é completamente análoga à anterior. Portanto, segue que $Ha = Hb$.

Atividade Final 3

Seja $a_1 b_1 h_1 \in (a_1 b_1)H$, $h \in H$, um elemento genérico de $a_1 b_1 H$. Vamos provar que $a_1 b_1 h_1 \in (ab)H$. Como $a_1 \in a_1 H = aH$, então existe $h_1 \in H$ tal que $a_1 = ah_1$. Analogamente, de $b_1 \in b_1 H = bH$, existe $h_2 \in H$ tal que $b_1 = bh_2$. Agora, é aqui o ponto crucial, como $Hb = bH$ e $h_1 h \in Hb$, então existe $h_3 \in H$ tal que $h_1 b = bh_3$. Logo, juntando todas estas informações, temos

$$\begin{aligned} a_1 b_1 h &= (ah_1)(bh_2)h; \text{ pois } a_1 = ah_1 \text{ e } b_1 = bh_2 \\ &= a(h_1 b)h_2 h; \text{ pela lei associativa} \\ &= a(bh_3)h_2 h; \text{ pois } h_1 b = bh_3 \\ &= ab(h_3 h_2 h); \text{pela lei associativa} \\ &= abh_4 \in abH; \text{ pois } h_4 = h_3 h_2 h \in H. \end{aligned}$$

Isto prova que $a_1 b_1 h \in (ab)H$ e, portanto, que $(a_1 b_1)H \subset (ab)H$.

Subgrupos normais

AULA 17

Meta da aula

Apresentar os subgrupos normais e os grupos quocientes de um grupo dado.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Aplicar a conceituação dos subgrupos normais.
- Determinar as condições para que um dado subgrupo seja normal.
- Construir o grupo quociente.Você vai precisar dos conhecimentos sobre grupos das Aulas 12 a 14.

Pré-requisitos

Você vai precisar dos conhecimentos sobre grupos das Aulas 12 a 16.

INTRODUÇÃO

Na aula anterior, encontramos uma classe de subgrupos especiais N de um grupo G que satisfaz a condição

$$gN = Ng \text{ para todo } g \in G.$$

Estes subgrupos são especiais porque, nesse caso, podemos definir uma operação binária no conjunto das classes laterais

$$G/N = \{gN \mid g \in G\}.$$

definida por

$$aN.bN = (ab)N.$$

tornando o conjunto G/N num grupo, chamado grupo quociente.

A necessidade da condição $gN = Ng$, para todo $g \in G$, apareceu para que pudéssemos resolver o problema da ambigüidade da representação das classes laterais. O problema consiste no fato de que existem muitas formas de se escrever a classe lateral aN. Por exemplo, uma outra forma de se escrever esta classe lateral é axN para qualquer $x \in N$. Aliás, você pode provar isto na Atividade 1.

ATIVIDADE

1. Sejam G um grupo e N um subgrupo de G. Prove que aN para todo $x \in N$.

Analogamente, para a classe lateral bN, podemos escrever $bN = byN$ para todo $y \in N$. Assim, o nosso problema é saber se a definição da operação binária em G/N,

$$aN.bN = (ab)N.$$

depende ou não da forma como representamos as classes laterais, isto é, se depende de representarmos a classe lateral *aN* por *aN* mesmo ou por *axN* para algum $x \in N$. É isto o que queremos dizer quando afirmamos que a operação binária está bem definida em *G/N*. Na aula passada provamos que se $gN = Ng$ para todo $g \in G$, então, de fato, a operação binária em *G/N* está bem definida. Mais precisamente, provamos a seguinte propriedade.

Proposição 1

Sejam G um grupo e N um subgrupo de G, tal que $gN = Ng$ para todo $g \in G$. Se $aN = a_1N$ e $bN = b_1N$, com $a, a_1, b, b_1 \in G$, então,

$$aN.bN = a_1N.b_1N,$$

ou, equivalentemente,

$$(ab)N = (a_1b_1)N.$$

Os subgrupos N para os quais a operação binária em G/N está bem definida recebe uma denominação especial.

DEFINIÇÃO 1 (SUBGRUPO NORMAL)

Um subgrupo N de um grupo G é chamado de um subgrupo normal de G se $gN = Ng$ para todo $g \in G$.

Existe outra caracterização de subgrupo normal muito usada. Para descrevê-la precisamos considerar o seguinte conjunto. Sejam H um subconjunto do grupo G e $a \in G$. Definimos o subconjunto aHa^{-1} de G por

$$aHa^{-1} = \{aha^{-1} \mid h \in H\}.$$

Daí, temos a seguinte propriedade

Proposição 2

Sejam G um grupo, H um subgrupo de G e $a \in G$.

1. aHa^{-1} é um subgrupo de G.
2. $aH = Ha$ se, e somente se, $aHa^{-1} = H$.

Demonstração

1. Lembre que, pelo critério do subgrupo visto na Aula 19, basta provar que

$xy^{-1} \in aHa^{-1}$ para todo $x, y \in aHa^{-1}$.

Como $x, y \in aHa^{-1}$, então existem $h_1, h_2 \in H$, tais que $x = ah_1a^{-1}$ e $y = ah_2a^{-1}$. E também, como H é subgrupo de G, então $h_3 = h_1h_2^{-1} \in H$. Juntando tudo, temos

$$
\begin{aligned}
xy^{-1} &= (ah_1a^{-1})(ah_2a^{-1})^{-1}; \text{pois } x = ah_1\text{a}^{-1} \text{ e } y = ah_2a^{-1} \\
&= (ah_1a^{-1})(ah_2^{-1}a^{-1}); \text{ por propriedade do elemento inverso} \\
&= ah_1(a^{-1}a)h_2^{-1}a^{-1}; \quad \text{pela lei associativa} \\
&= ah_1e_Gh_2^{-1}a^{-1}; \quad \text{por propriedade do elemento inverso} \\
&= \text{a}(h_1h_2^{-1})a^{-1}; \quad \text{por propriedade do elemento neutro} \\
&= ah_3a^{-1} \in aHa^{-1}; \quad \text{pois } h_3 = h_1h_2^{-1} \in H.
\end{aligned}
$$

Portanto, aHa^{-1} é um subgrupo de G.

2. ($\Rightarrow$) Vamos supor que $aH = Ha$. Queremos provar que $aHa^{-1} = H$. Vamos começar provando a inclusão $aHa^{-1} \subset H$. Dado $x \in aHa^{-1}$, existe $h_1 \in H$, tal que $x = ah_1a^{-1}$. Como $aH = Ha$, existe $h_1 \in H$, tal que $ah_1 = h_2a$. Assim, temos

$$
\begin{aligned}
x &= ah_1a^{-1}; \quad \text{pois } x = ah_1a^{-1} \\
&= (ah_1)a^{-1}; \quad \text{pela lei associativa} \\
&= (h_2a)a^{-1}; \quad \text{pois } ah_1 = h_2a \\
&= h_2(aa^{-1}); \quad \text{pela lei associativa} \\
&= h_2e_G; \quad \text{por propriedade do elemento neutro} \\
&= h_2 \in H.
\end{aligned}
$$

Portanto, provamos que $aHa^{-1} \subset H$. A inclusão $H \subset aHa^{-1}$ será uma atividade para você.

($\Leftarrow$) Vamos supor, agora, que $aHa^{-1} \subset H$ e vamos provar a inclusão $aH \subset Ha$. Dado $x \in aH$, existe $h \in H$, tal que $x = ah$. Como $xa^{-1} = aha^{-1} \in aHa = H$, então existe $h_1 \in H$, tal que $xa^{-1} = h_1$ e, portanto, $x = h_1a \in Ha$. Assim, temos $aH \subset Ha$.

A inclusão contrária, $Ha \subset aH$, é feita de forma análoga. Dado $x \in Ha$, existe $h \in H$, tal que $x = ha$. Como

$$xa^{-1} = (ha)a^{-1} = h(aa^{-1}) = h \in H = aHa,$$

então existe $h_1 \in H$, tal que $xa^{-1} = ah_1a^{-1}$ e, portanto,

$$x = (xa^{-1})a = (ah_1a^{-1})a = (ah_1)(a^{-1}a) = ah_1 \in aH$$

Assim, temos $Ha \subset aH$. □

ATIVIDADE

2. Sejam G um grupo e H um subgrupo de G que satisfaz $aH \subset Ha$. Prove que $H \subset aHa^{-1}$.

Portanto, pela parte 2 da Proposição 2, a outra caracterização de subgrupo normal fica clara.

DEFINIÇÃO 2 (SUBGRUPO NORMAL)

Um subgrupo N de um grupo G é chamado de um subgrupo normal de G se $gNg^{-1} = N$ para todo $g \in G$.

A próxima propriedade fornece um critério que facilita verificar se um subgrupo N é um subgrupo normal de G. Esta propriedade mostra que basta verificar a inclusão $gNg^{-1} \subset N$ para todo $g \in G$.

Proposição 3 (Critério do Subgrupo Normal)

Sejam G um grupo e N um subgrupo de G. Então N é um subgrupo normal de G, se, e somente se, $gNg^{-1} = N$ para todo $g \in G$.

Demonstração

($\Rightarrow$) Se N é um subgrupo normal de G, então, pela Definição 2, $gNg^{-1} = N$ para todo $g \in G$. Portanto, segue imediatamente que $gNg^{-1} \subset N$ para todo $g \in G$.

($\Leftarrow$) Temos de provar que $gNg^{-1} = N$ para todo $g \in G$. Como já sabemos, por hipótese, que $gNg^{-1} \subset N$, então basta provar que $N \subset gNg^{-1}$ para todo $g \in G$. Seja $a \in N$ um elemento qualquer. Como N é subgrupo, então $a^{-1} \in N$. Logo, $g^{-1}a^{-1}g \in g^{-1}Ng$ e como, por hipótese, $g^{-1}Ng \subset N$, segue que $g^{-1}a^{-1}g \in N$. Novamente, como N é subgrupo, então $(g^{-1}a^{-1}g)^{-1} \in N$, ou seja,

$$b = g^{-1}ag = (g^{-1}a^{-1}g)^{-1} \in N$$

De $g^{-1}ag = b$ segue imediatamente que $a = gbg^{-1} \in gNg^{-1}$. Portanto, provamos que $N \subset gNg^{-1}$, o que termina a demonstração de que N é um subgrupo normal de G. □

Observação

O critério do subgrupo normal pode ser reescrito da seguinte forma: N é um subgrupo normal de G se, e somente se, $gxg^{-1} \in N$ para todo $x \in N$ e para todo $g \in G$.

Vamos, agora, ver alguns exemplos.

Exemplo 1

Seja G um grupo. Então os subgrupos triviais de G, $N_1 = \{e_G\}$ e $N_2 = G$, são subgrupos normais de G.

De fato, para $N_1 = \{e\}$, como e é o único elemento de N_1, então

$$g^{-1}eg = g^{-1}g = e \in N_1$$

e, portanto, temos $gN_1g^{-1} \subset N_1$ para todo $g \in G$. Pela Proposição 3, isto prova que $N_1 = \{e_G\}$ é um subgrupo normal de G.

A prova de que $N_2 = G$. é um subgrupo normal de G faz parte da próxima atividade desta aula.

ATIVIDADE

3. Seja G um grupo. Mostre que G é um subgrupo normal de G.

Exemplo 2

Seja G um grupo abeliano, então todo subgrupo N de G é normal. De fato, para quaisquer $x \in N$ e $g \in G$ temos que

$$g^{-1}xg = xg^{-1}g, \text{ pois G é abeliano}$$
$$= x \in N$$

Portanto, temos $gNg^{-1} \subset N$ para todo $g \in G$, o que prova que N é subgrupo normal de G.

Exemplo 3

Seja G o grupo $S_3 = \{1, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ das permutações de 3 elementos, onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

e seja o subgrupo $N = \{I, \alpha, \alpha^2\}$. Vimos, no Exemplo 4 e na Atividade 3, ambos na Aula 21, que $gN = Ng$ para todo $g \in S_3$. Portanto, N é um subgrupo normal de S_3.

Exemplo 4

Seja o subgrupo $H = \{I, \beta\}$ de S_3. Como

$$\alpha H = \alpha\{I, \beta\} = \{\alpha I, \alpha\beta\} = \{\alpha, \beta\alpha^2\}, \text{ onde } \alpha\beta = \beta\alpha^2, ,$$

e

$$H\alpha = \{I, \beta\}\alpha = \{I\alpha, \beta\alpha\} = \{\alpha, \beta\alpha\} \neq \alpha H,$$

segue que $H = \{I, \beta\}$ não é subgrupo normal de S_3.

Voltando à nossa discussão inicial, vimos que se N é um subgrupo normal, então a operação binária definida em G/N está bem definida. Na verdade, a condição $gNg^{-1} \subset N$, para todo $g \in G$, é não só suficiente como é também necessária para que a operação binária em G/N esteja bem definida. Vejamos a discussão a seguir.

Dados $a, b \in G$ e $x, y \in N$ arbitrários, então ax e a representam a mesma classe lateral aN, isto é, $aN = axN$ e, similarmente, para a classe lateral $b^{-1}N$, temos que $b^{-1}N = b^{-1}yN$. Assim, a operação binária em G/N está bem definida se, e somente se,

$$ab^{-1}N = (ax)(b^{-1}y)N \text{ para todo } a, b \in G \text{ e para todo } x, y \in N.$$

Veja que esta igualdade vale se, e somente se

$$ab^{-1}N = (ax)(b^{-1}y)N \text{ para todo } a, b \in G \text{ e } x, y \in N,$$

e, portanto,

$$N = bxb^{-1}yN = bxb^{-1}N \text{ para todo } b \in G \text{ e } x \in N,$$

Assim, a operação binária em G/H está bem definida se, e somente, se

$$bxb^{-1} \in N \text{ para todo } b \in G \text{ e } x \in N.$$

Resumindo, temos que os subgrupos N do grupo G que satisfazem a propriedade $bxb^{-1} \in N$ para todo $b \in G$ e para todo $x \in N$

são os subgrupos para os quais o conjunto quociente G/N é um grupo. Estes grupos são muito importantes e são os grupos quocientes vistos no final da aula passada. Vamos retomar as definições com a nova nomenclatura de subgrupo normal.

TEOREMA 1 (O GRUPO QUOCIENTE)

Sejam G um grupo e N um subgrupo normal de G. Então G/N, munido da operação definida em G/N, é um grupo. Chamamos este grupo de *grupo quociente de G módulo N*.

Em particular, $eN = N$ é o elemento neutro do grupo e $a^{-1}N$ é o elemento inverso de aN. Denotamos isto por

$$e_{G/N} = e_G N = N \text{ e } (aN)^{-1} = a^{-1}N .$$

Vamos apresentar outros exemplos sobre subgrupos normais.

Exemplo 5

Retornando ao subgrupo $N = \{I, \alpha, \alpha^2\}$ de $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$, vimos no Exemplo 3 que N é um subgrupo normal de S_3. No Exemplo 4 da Aula 16, vimos que o grupo quociente S_3/N é dado por

$$S_3/N = \{N, \beta N\} .$$

A seguinte atividade é muito importante para entendermos a noção de subgrupo normal.

ATIVIDADE

4. Calcule todos os subgrupos normais de S_3.

Apresentaremos agora alguns resultados sobre o grupo quociente.

Proposição 4

Sejam G um grupo e N um subgrupo normal de G. Então:

1. Se G é um grupo abeliano, então o grupo quociente G/N é um grupo abeliano.

2. Se G é um grupo cíclico, então o grupo quociente G/N é um grupo cíclico.

Demonstração

1. Sejam aN e bN duas classes laterais em G/N. Temos que

$$\begin{aligned}(aN)\cdot(bN) &= abN, && \text{pela definição da operação en G/N}\\ &= baN, && \text{pois G é abeliano}\\ &= (bN)\cdot(aN).\end{aligned}$$

Concluímos, assim, que G/N é um grupo abeliano também.

2. Suponhamos, agora, que G é um grupo cíclico gerado pelo elemento $x \in G$. Isto é, qualquer elemento de G é uma potência de x. Afirmamos que a classe lateral xN é gerador do grupo G/N. De fato, seja $aN \in G/N$ com $a \in G$, então podemos escrever $a = x^k$ para algum $k \in Z$. Assim,

$$aN = x^k N = (xN)^k \text{ para algum } k \in Z,$$

o que mostra que G/N é um grupo cíclico. □

Vejamos mais alguns exemplos de grupos quocientes.

Exemplo 6

Como $\mathbf{Z}$ é um grupo aditivo abeliano, então o subgrupo $N = 4\mathbf{Z}$, dos inteiros múltiplos de 4, é um grupo normal de $\mathbf{Z}$. Assim, o grupo quociente $\mathbf{Z}/4\mathbf{Z}$ é formado pelos quatro elementos

$$4\mathbf{Z} = 0 + 4\mathbf{Z},\ 1 + 4\mathbf{Z},\ 2 + 4\mathbf{Z} \text{ e } 3 + 4\mathbf{Z}$$

Não é difícil ver que $\mathbf{Z}/4\mathbf{Z}$ é um grupo cíclico gerado por $1 + 4\mathbf{Z}$. Assim, $\mathbf{Z}/4\mathbf{Z}$ é um grupo isomorfo com $\mathbf{Z}4$.

O exemplo anterior é um caso particular do seguinte exemplo.

Exemplo 7

Sabemos que se $n \in \mathbf{Z}$, então o subgrupo

$$n\mathbf{Z} = \{nt \mid t \in \mathbf{Z}\}$$

é um subgrupo normal do grupo aditivo **Z**. Sabemos também que existem n classes laterais de $n\mathbf{Z}$ em **Z**, a saber,

$$0 + n\mathbf{Z} = n\mathbf{Z},\ 1 + n\mathbf{Z},\ 2 + n\mathbf{Z}\ldots\ldots\ (n\text{-}1) + n\mathbf{Z}\ .$$

Como o grupo aditivo **Z** é cíclico, gerado pelo elemento 1, temos que o grupo quociente $\mathbf{Z}/n\mathbf{Z}$ também é cíclico e é gerado pela classe lateral $1 + nZ$. Sendo um grupo cíclico de ordem n, temos que $\mathbf{Z}/n\mathbf{Z}$ é isomorfo a $\mathbf{Z}n$. Num abuso de notação, muitas vezes escrevemos

$$\frac{\mathbf{Z}}{n\mathbf{Z}} = \mathbf{Z}_n .$$

Exemplo 8

Considere o grupo abeliano

$$\mathbf{Z}_4 \times \mathbf{Z}_6 = \{(x, y) \mid x \in \mathbf{Z}_4 \ \text{ e } \ y \in \mathbf{Z}_6\}.$$

Com a operação definida por

$(a,b) \oplus (c,d) = (a + c, b, + d)$ para todo $a, c \in \mathbf{Z}_4$ e $b, d \in \mathbf{Z}_6$.

Seja N o subgrupo cíclico de $\mathbf{Z}_4$ x $\mathbf{Z}_6$ gerado pelo elemento $(\bar{0}, \bar{1})$, isto é,

$$N = \left\{K(\bar{0}, \bar{1})K \in \mathbf{Z}\right\}.$$

Atenção para não se confundir com a notação: observe que a primeira componente de $(\bar{0}, \bar{1})$ é $\bar{0} \in \mathbf{Z}_4$ e que a segunda componente de $(\bar{0}, \bar{1})$ é $\bar{1} \in \mathbf{Z}_6$. Assim, temos

$$0(\bar{0}, \bar{1}) = e_{Z_4 \times Z_6} = (\bar{0}, \bar{0});$$
$$1(\bar{0}, \bar{1}) = (\bar{0}, \bar{1});$$
$$2(\bar{0}, \bar{1}) = (\bar{0}, \bar{1}) \oplus (\bar{0}, \bar{1}) = (\bar{0} + \bar{0}, \bar{1} + \bar{1}) = (\bar{0}, \bar{2})$$
$$3(\bar{0}, \bar{1}) = 2(\bar{0}, \bar{1}) \oplus (\bar{0}, \bar{1}) = (\bar{0}, \bar{2}) \oplus (\bar{0}, \bar{1}) = (\bar{0} + \bar{0}, \bar{2} + \bar{1}) = (\bar{0}, \bar{3});$$
$$4(\bar{0}, \bar{1}) = 3(\bar{0}, \bar{1}) \oplus (\bar{0}, \bar{1}) = (\bar{0}, \bar{3}) \oplus (\bar{0}, \bar{1}) = (\bar{0} + \bar{0}, \bar{3} + \bar{1}) = (\bar{0}, \bar{4});$$
$$5(\bar{0}, \bar{1}) = 4(\bar{0}, \bar{1}) \oplus (\bar{0}, \bar{1}) = (\bar{0}, \bar{4}) \oplus (\bar{0}, \bar{1}) = (\bar{0} + \bar{0}, \bar{4} + \bar{1}) = (\bar{0}, \bar{5});$$
$$6(\bar{0}, \bar{1}) = 5(\bar{0}, \bar{1}) \oplus (\bar{0}, \bar{1}) = (\bar{0}, \bar{5}) \oplus (\bar{0}, \bar{1}) = (\bar{0} + \bar{0}, \bar{5} + \bar{1}) = (\bar{0}, \bar{6}) = (\bar{0}, \bar{0}).$$

Logo,

$$N = \{k(\bar{0}, \bar{1}) \mid k \in \mathbf{Z}\}$$
$$= \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{0}, \bar{2}), (\bar{0}, \bar{3}), (\bar{0}, \bar{4}), (\bar{0}, \bar{6})\}.$$

Sendo $\mathbf{Z}_4$ x $\mathbf{Z}_6$ abeliano, temos que N é um subgrupo normal e $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$ um grupo abeliano. Sabemos que todas as classes laterais de N são disjuntas, possuem a mesma cardinalidade de N, no caso, 6 elementos cada, e sua união é todo o grupo G, de ordem 24. Logo, existem somente 4 classes laterais de N, ou seja, o grupo quociente $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$ em ordem 4.

Assim, os 4 elementos de $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$ são

$$(\bar{0}, \bar{0}) \oplus N = N;\ (\bar{1}, \bar{0}) \oplus N;\ (\bar{2}, \bar{0}) \oplus N \text{ e } (\bar{3}, \bar{0}) \oplus N.$$

Na próxima atividade desta aula, você estará encarregado de verificar que $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$ é um grupo cíclico gerado por $(\bar{1}, \bar{0}) \oplus N$. Podemos, assim, concluir que $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$ é um grupo isomorfo ao grupo $\mathbf{Z}_4$.

ATIVIDADES FINAIS

1. Verifique que $(\bar{1}, \bar{0}) \oplus N;$ é gerador do grupo $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$. Apresente o elemento inverso de cada elemento do grupo.

2. Sejam $H \subset K$ subgrupos normais de um grupo G. Verifique que:

a) H é um subgrupo normal de K.

b) O grupo K/H é um subgrupo normal do grupo G/H.

RESUMO

Nesta aula estudamos uma classe especial de subgrupos de um grupo G, são os chamados subgrupos normais, mais precisamente, dizemos que um um subgrupo N é normal em G se $gNg^{-1} = N$ para todo $g \in G$, ou, equivalentemente, se $gN = Ng$ para todo $g \in G$.

Estes subgrupos são importantes pois, nesse caso, o conjunto das classes laterais de N em G é um grupo, chamado do grupo quociente de H e que foi denotado por G/H.

RESPOSTAS COMENTADAS

Atividade 1

Na Proposição 1 da Aula 21, vimos que $aN = bN$ se, e somente se, $a^{-1} \cdot b \in N$. Nesse caso, teremos

$aN = bN$ se, e somente se, $a^{-1} \cdot b \in N$.

Assim, temos $a^{-1} \cdot (ax) = (a^{-1}a) \cdot x$; pela lei associativa

$= e_G \cdot x$

$= x \in N$; pois $x \in N$.

Portanto, provamos que $a^{-1} \cdot (ax) \in N$ e, conseqüentemente, que aN = axN para todo x∈N.

Atividade 2

Seja h∈H um elemento qualquer. Vamos provar que $h \in aHa^{-1}$. Como, existe $h_1 \in H$ tal que ha = ah_1. Portanto,

$h = he_G$; por propriedade do elemento neutro

$= h(aa^{-1})$; por propriedade do elemento inverso

$= (ha)a^{-1}$; pela lei associativa

$= (ah_1)a^{-1}$; pois $ha = ah_1$

$= ah_1a^{-1} \in aHa^{-1}$.

Portanto, provamos que $H \subset aHa^{-1}$.

Atividade 3

Dado $a \in G$ um elemento qualquer, então

$$gag^{-1} \in G \text{ para todo } g \in G.$$

Isto prova que $gGg^{-1} \subset G$ para todo $g \in G$ e, portanto, temos que G é um subgrupo normal de G.

Atividade 4

Lembre que, pelo Teorema de Lagrange, a ordem de um subgrupo H divide a ordem do grupo G. Como $|S_3| = 6$, os subgrupos de $S_3 = \{1, \alpha, \alpha_2, \beta, \beta\alpha, \beta\alpha^2\}$ só podem ter ordem 1, 2, 3 ou 6. Assim, temos as seguintes possibilidades:

Se $|H| = 1$, o subgrupo só pode ser o subgrupo trivial $H_1 = \{1\}$;

Se $|H| = 2$, como S_3 tem três elementos de ordem 2, a saber, $\beta, \beta\alpha, \beta\alpha^2$, então os subgrupos de ordem 2 são $H_2 = \{I, \beta\}$, $H_3 = \{I, \beta\alpha\}$ e $H_4 = \{I, \beta\alpha^2\}$;

Se $|H| = 3$, como S_3 tem 2 elementos de ordem 3, a saber, $\alpha = \alpha^2$, então o único subgrupo de ordem 3 é $H_5 = \{1, \alpha, \alpha^2\}$;

Se $|H| = 6$, o subgrupo só pode ser o subgrupo trivial $H_6 = S_3$.

Dos seis subgrupos citados anteriormente e dos exemplos vistos nesta aula, sabemos que os subgrupos triviais, $H_1 = \{1\}$; e $H_6 = S_3$, e o subgrupo $H_5 = \{1, \alpha, \alpha^2\}$ são subgrupos normais, enquanto o subgrupo $H_2 = \{I, \beta\}$ não é subgrupo normal. Assim como fizemos no Exemplo 4, vamos verificar que $H_3 = \{I, \beta\alpha\}$ e $H_4 = \{I, \beta\alpha^2\}$ não são subgrupos normais. Lembre, da Aula 15, que a tabela de multiplicação de S_3 é dada por

x	1	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
1	1	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	1	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	1	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	1	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	1	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	1

Assim temos que

$$\alpha H_3 = \alpha\{I,\ \beta\alpha\} = \{\alpha I,\ \alpha(\beta\alpha)\} = \{\alpha,\ \beta\}$$

e

$$H_3\alpha = \{I,\ \beta\alpha\}\alpha = \{I\alpha,\ (\beta\alpha)\alpha\} = \{\alpha,\ \beta\alpha^2\} \neq \alpha H_3 .$$

Logo, $H_3 = \{I,\ \beta\alpha\}$ não é subgrupo normal de S_3. De modo análogo, temos

$$\alpha H_4 = \alpha\{I,\ \beta\alpha^2\} = \{\alpha I,\ \alpha(\beta\alpha^2)\} = \{\alpha,\ \beta\alpha\}$$

e

$$H_4\alpha = \{I,\ \beta\alpha^2\}\alpha = \{I\alpha,\ (\beta\alpha^2)\alpha\} = \{\alpha,\ \beta\} \neq \alpha H_4$$

Logo, $H_4 = \{I,\ \beta\alpha^2\}$ também não é subgrupo normal de S_3.

Concluindo, os subgrupos normais de S_3 são $H_1 = \{I\}$, $H_5 = \{I, \alpha, \alpha^2\}$ e $H_6 = S_3$.

Atividade Final 1

Vimos, no Exemplo 8, que

$$\frac{\mathbf{Z}_4 \times \mathbf{Z}_6}{N} = \{N, (\overline{1}, \overline{0}) \oplus N, (\overline{2}, \overline{0}) \oplus N, (\overline{3}, \overline{0}) \oplus N\}.$$

Para simplificar a notação, denotaremos

$$\overline{(a, b)} = (a, b) \oplus N ,$$

assim, temos

$$\frac{\mathbf{Z}_4 \times \mathbf{Z}_6}{N} = \{\overline{(\overline{0}, \overline{0})}, \overline{(\overline{1}, \overline{0})}, \overline{(\overline{2}, \overline{0})}, \overline{(\overline{3}, \overline{0})}\}$$

Vamos verificar que $\overline{(\overline{1}, \overline{0})} = (\overline{1}, \overline{0}) \oplus N$; é um gerador de $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$:

$$1\overline{(\overline{1}, \overline{0})} = \overline{(\overline{1}, \overline{0})};$$

$$2\overline{(\overline{1}, \overline{0})} = [(\overline{1}, \overline{0}) \oplus N] + [(\overline{1}, \overline{0}) \oplus N] = (\overline{2}, \overline{0}) \oplus N = \overline{(\overline{2}, \overline{0})};$$

$$3\overline{(\overline{1}, \overline{0})} = 2\overline{(\overline{1}, \overline{0})} + \overline{(\overline{1}, \overline{0})} = [(\overline{2}, \overline{0}) \oplus N] + [(\overline{1}, \overline{0}) \oplus N] = (\overline{3}, \overline{0}) \oplus N = \overline{(\overline{3}, \overline{0})}$$

$$4\overline{(\overline{1}, \overline{0})} = 3\overline{(\overline{1}, \overline{0})} + \overline{(\overline{1}, \overline{0})} = [(\overline{3}, \overline{0}) \oplus N] + [(\overline{1}, \overline{0}) \oplus N] = (\overline{4}, \overline{0}) \oplus N = \overline{(\overline{0}, \overline{0})}$$

Portanto, $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$; é um grupo cíclico gerado por $\overline{(\overline{1}, \overline{0})} = (\overline{1}, \overline{0}) \oplus N$.

Agora, para obter os elementos inversos dos elementos de $(\mathbf{Z}_4 \times \mathbf{Z}_6)/N$;, temos:

- $\overline{(\bar{0}, \bar{0})} + \overline{(\bar{0}, \bar{0})} = \overline{(\bar{0}, \bar{0})}$, logo $\overline{(\bar{0}, \bar{0})}$ é seu próprio inverso;
- $\overline{(\bar{1}, \bar{0})} + \overline{(\bar{3}, \bar{0})} = \overline{(\bar{0}, \bar{0})}$, logo $\overline{(\bar{1}, \bar{0})}$ e $\overline{(\bar{3}, \bar{0})}$ são inversos um do outro;
- $\overline{(\bar{2}, \bar{0})} + \overline{(\bar{2}, \bar{0})} = \overline{(\bar{0}, \bar{0})}$, logo $\overline{(\bar{2}, \bar{0})}$ é seu próprio inverso.

Atividade Final 2

a) Sejam $h \in H$ e $k \in K$. Temos que

$khk^{-1} \in H$, pois $k \in K \subset G$ e *H* é normal em *G*.

Assim, provamos que $kHk^{-1} \subset H$ para todo $k \in K$. Logo, pelo critério do subgrupo normal, segue que *H* é subgrupo normal de *K*.

b) Sejam $kH \in K/H$ e $gH \in G/H$. Temos que

$$(gH) \cdot (kH) \cdot (gH)^{-1} = (gH) \cdot (kH) \cdot (g^{-1}H) = (gkg^{-1})H$$

Como *K* é normal em *G* e $k \in K$, então $ghg^{-1} \in K$ para todo $k \in K$ e para todo $g \in G$. Assim, temos que

$$(gH) \cdot (kH) \cdot (gH)^{-1} = (gkg^{-1})H \in K/H$$

para todo $k \in K$ e para todo $g \in G$. Portanto, pelo critério do subgrupo, segue que K/H é subgrupo normal de G/H.

Homomorfismos de grupos

AULA 18

Meta da aula

Apresentar o conceito de homomorfismo de grupo e suas propriedades básicas.

objetivos

Ao final desta aula, você deverá ser capaz de:

- Reconhecer e conceituar um homomorfismo de grupos.
- Apresentar e demonstrar várias propriedades dos homomorfismos de grupos.
- Apresentar e calcular importantes exemplos de homomorfismos de grupos.

Pré-requisitos

Você vai precisar dos conhecimentos sobre grupos das Aulas 12 a 17.

INTRODUÇÃO

Apresentaremos nesta aula o conceito de homomorfismo de grupos. Lembre que na Aula 2 estudamos o conceito de homomorfismo de anéis e muitas de suas propriedades. Como aconteceu naquela aula, em que vimos também o conceito de isomorfismo de anéis, veremos aqui o conceito de isomorfismo de grupos. Os isomorfismos são muito importantes porque eles permitem a identificação entre grupos aparentemente muito diferentes. Lembre que um homomorfismo de anéis é uma função entre dois anéis que preserva as operações destes anéis. Analogamente, um homomorfismo de grupos é uma função entre dois grupos que preserva a operação destes grupos. Vamos às definições.

DEFINIÇÃO 1 (HOMOMORFISMO DE GRUPOS)

Dados dois grupos G e H, uma função $f : G \to H$ é chamada de um *homomorfismo* (*de grupos*) se

$$f(a \,.\, b) = f(a) \,.\, f(b) \text{ para todo } a, b \in G$$

Observações

1. Observe que a operação que aparece em $f(a \,.\, b)$ é a do grupo G, enquanto a operação que aparece em $f(a) \,.\, f(b)$ é a operação do grupo H.

2. Lembre que a condição

$$f(a \,.\, b) = f(a) \,.\, f(b) \text{ para todo } a, b \in G$$

significa que *f preserva as operações* dos grupos G e H. Para simplificar a notação, muitas vezes escrevemos esta condição sem denotar explicitamente a operação:

$$f(ab) = f(a)\, f(b) \text{ para todo } a, b \in G$$

DEFINIÇÃO 2 (ISOMORFISMO DE GRUPOS)

Um homomorfismo de grupos $f : G \to H$ é chamado de um *isomorfismo* (*de grupos*) se for, também, uma bijeção. Nesse caso, dizemos que os grupos G e H são *isomorfos* e denotamos $G \approx H$.

Se $f: G \to H$ é um isomorfismo do grupo G nele mesmo, dizemos que f é um *automorfismo* de G.

Observação

Lembre que dois conjuntos G e H têm o mesmo número de elementos, ou seja, eles terão a mesma cardinalidade, se existir uma bijeção entre G e H. Assim, se G e H forem grupos isomorfos, então eles terão *exatamente* o mesmo número de elementos. Isso acontece porque se $f: G \to H$ for um isomorfismo, então, em particular, f será uma bijeção entre G e H.

DEFINIÇÃO 3 (NÚCLEO DE UM HOMOMORFISMO)

O *núcleo* de um homomorfismo de grupos $f: G \to H$ é o conjunto

$$N(f) = \{x \in G \mid f(x) = e_H\},$$

onde e_H é o elemento neutro do grupo H.

Vejamos, agora, dois dos exemplos mais simples de homomorfismos de grupos.

Exemplo 1

Dados os grupos G e H, consideremos a função constante $f: G \to H$ dada por

$$f(x) = e_H \text{ para todo } x \in G,$$

onde e_H é o elemento neutro do grupo H. É fácil verificar que f é um homomorfismo de grupos, pois

$$\begin{aligned} f(a.b) &= e_H \\ &= e_H . e_H \\ &= f(a)f(b), \end{aligned}$$

para todo $a, b \in G$. Podemos, também, facilmente calcular o seu núcleo. Como $f(x) = e_H$ para todo $x \in G$, então

$$N(f) = \{x \in G \mid f(x) = e_H\} = G.$$

Portanto, o núcleo de f é todo o grupo G, o maior subgrupo possível de G.

Exemplo 2

Dado um grupo G, o homomorfismo *identidade de G* é definido pela função identidade em G, ou seja, $id : G \to G$, $id(a) = a$ para todo $a \in G$. É fácil verificar que a identidade é, de fato, um homomorfismo de grupos. Temos que

$$id(a \,.\, b) = a \,.\, b = id(a) \cdot id(b),$$

para todo $a, b \in G$, o que prova facilmente o que queríamos. Como a identidade é uma bijeção em G, então $id : G \to G$ é, na verdade, um isomorfismo do grupo G. Seu núcleo também pode ser calculado simplesmente. Observe que

$$id(x) = e_G \;\Rightarrow\; x = e_G,$$

logo,

$$N(f) = \{x \in G \mid f(x) = e_G\} = \{e_G\}.$$

Portanto, o núcleo do homomorfismo identidade *id* é o subgrupo trivial $\{e_G\}$, o menor subgrupo possível de G.

Exemplo 3

Sejam $G = (\boldsymbol{R}, +)$ o grupo aditivo dos números reais e $H = (\boldsymbol{R}_+^*, .)$ o grupo multiplicativo dos números reais positivos. Considere a função $f : G \to H$ definida por

$$f(x) = 2^x \quad \text{para todo} \quad x \in \boldsymbol{R}.$$

Vamos verificar que f é um homomorfismo de grupos. Dados $y, x \in \boldsymbol{R}$, temos

$$f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y).$$

Assim, temos que f preserva as operações dos grupos e, portanto, é um homomorfismo. Como a função exponencial $f(x) = 2^x$ é uma bijeção entre $\boldsymbol{R}$ e $\boldsymbol{R}_+^*$, então f é um isomorfismo de grupos. Vamos calcular seu núcleo. Como $e_H = 1$, temos que

$$f(x) = 1 \Leftrightarrow 2^x = 1 \Leftrightarrow x = 0 = e_G.$$

Portanto, o núcleo de f é o subgrupo trivial $N(f) = \{0\}$.

Vamos à nossa primeira atividade.

ATIVIDADE

1. Sejam $G = (\boldsymbol{Z}, +)$ o grupo aditivo dos números inteiros e $H = (\boldsymbol{Z}_n, +)$ o grupo aditivo dos inteiros módulo n. Considere a função $f : G \to H$ definida por

$$f(a) = \overline{a} \text{ para todo } a \in \boldsymbol{Z}.$$

Mostre que f é um homomorfismo sobrejetor e calcule o seu núcleo.

Vamos, agora, estudar algumas propriedades dos homomorfismos.

Proposição 1

Seja $f : G \to H$ um homomorfismo de grupos. Então,

1. $f(e_G) = eH$
2. $f(a)^{-1} = f(a^{-1})$
3. Se N é um subgrupo de G, então $f(N)$ é um subgrupo de H. Em particular, $\text{Im}(f) = f(G)$ é um subgrupo de H.
4. $N(f)$ é um subgrupo normal de G.
5. f é injetora se, e somente se, $N(f) = \{e_G\}$.
6. Se f for bijetora, então $f^{-1} : H \to G$ será um homomorfismo de grupos.

Demonstração

1. Temos que

$$\begin{aligned} f(e_G) &= f(e_G \,.\, e_G)\ ;\ \text{pois}\ \ e_G = e_G \,.\, e_G \\ &= f(e_G)\cdot f(e_G);\ \ \text{pois}\ f\ \text{Øhomomorfismo.} \end{aligned}$$

Multiplicando ambos os lados da equação $f(e_G)\,.\,f(e_G) = f(e_G)$ por $f(e_G)^{-1}$, obtemos

$$(f(e_G)\cdot f(e_G))\cdot f(e_G)^{-1} = f(e_G)\cdot f(e_G)^{-1},$$

e como $f(e_G)\cdot f(e_G)^{-1} = e_H$, então temos

$$f(e_G) = e_H.$$

2. Vemos que

$$\begin{aligned} f(a)\cdot f(a^{-1}) &= f(a\,.\,a^{-1});\ \ \text{pois}\ f\ \text{Øhomomorfismo} \\ &= f(e_G);\ \ \text{pois}\ \ a\,.\,a^{-1} = e_G \\ &= e_H;\ \ \text{pela propriedade anterior.} \end{aligned}$$

Analogamente, $f(a^{-1})\cdot f(a) = e_H$. Logo, pela unicidade do elemento inverso, segue que $f(a)^{-1} = f(a^{-1})$.

3. Sejam $x,\ y \in f(N)$. Vamos provar que $x\,.\,y^{-1} \in f(x)$. Como $x \in f(N)$, existe $a \in N$ tal que $f(a) = x$ e como $y \in f(N)$, existe $a \in N$ tal que $f(b) = x$. Como N é subgrupo, então $a\,.\,b^{-1} \in N$. Assim, temos que

$$\begin{aligned} x\,.\,y^{-1} &= f(a)\cdot f(b)^{-1};\ \ \text{pois}\ \ \ x = f(a)\ \ \text{e}\ \ \ y = f(b) \\ &= f(a)\cdot f(b^{-1});\ \ \text{pois}\ \ f(b)^{-1} = f(b^{-1}) \\ &= f(a\,.\,b^{-1});\ \ \text{pois}\ f\ \text{Øhomomorfismo} \\ &= f(a\,.\,b^{-1}) \in f(N);\ \ \text{pois}\ \ \ a\,.\,b^{-1} \in N. \end{aligned}$$

Portanto, pelo critério do subgrupo, temos que $f(N)$ é subgrupo de H. Em particular, como $\text{Im}(f) = f(G)$, então $\text{Im}(f)$ é um subgrupo de H.

4. Vamos, primeiramente, provar que $N(f)$ é um subgrupo de G. Dados $a\,.\,b^{-1} \in N(f)$, queremos mostrar que $a\,.\,b^{-1} \in f(N)$. Como $a\,.\,b \in N(f)$, então $f(a) = f(b) = e_H$. Assim,

$$\begin{aligned} f(a \,.\, b^{-1}) &= f(a)\cdot f(b^{-1}) \;;\; \text{pois } f \text{ Øhomomorfismo} \\ &= f(a)\cdot f(b)^{-1};\; \text{pois } f(b^{-1}) = f(b)^{-1} \\ &= e_H \cdot e_H^{-1};\; \text{pois } f(a) = f(b) = e_H \\ &= e_H . \end{aligned}$$

De $f(a \,.\, b^{-1}) = e_H$, temos que $a \,.\, b^{-1} \in N(f)$, o que prova que $N(f)$ é um subgrupo de G. Para provar que $N(f)$ é um subgrupo normal de G, sejam $a \in N(f)$ e $g \in G$. Vamos mostrar que $g \,.\, a \,.\, g^{-1} \in N(f)$. Como $a \in N(f)$, então $f(a) = e_H$. Assim,

$$\begin{aligned} f(g \,.\, a \,.\, g^{-1}) &= f(g)\cdot f(a)\cdot f(g^{-1});\; \text{pois } f \text{ Øhomomorfismo} \\ &= f(g)\cdot e_H \cdot f(g)^{-1};\; \text{pois } f(a) = e_H \text{ e } f(g^{-1}) = f(g)^{-1} \\ &= f(g)\cdot f(g)^{-1} \\ &= e_H . \end{aligned}$$

Portanto, de $f(g \,.\, a \,.\, g^{-1}) = e_H$, temos que $g \,.\, a \,.\, g^{-1} \in N(f)$. Logo, pelo critério do subgrupo normal, segue que $N(f)$ é um subgrupo normal de G.

5. ($\Rightarrow$)Vamos supor que f seja injetora. Queremos provar que $N(f) = \{e_G\}$. Dado $a \in N(f)$, então

$$f(a) = e_H = f(e_G),$$

e, como f é injetora, segue que $a = e_G$. Daí, concluímos que $N(f) = \{e_G\}$.

($\Leftarrow$) Vamos supor agora que $N(f) = \{e_G\}$. Queremos provar que f é injetora. Dados $a, b \in N$ tais que $f(a) = f(b)$, vamos mostrar que $a = b$. Temos

$$\begin{aligned} f(a \,.\, b^{-1}) &= f(a)\cdot f(b^{-1});\; \text{pois } f \text{ Øhomomorfismo} \\ &= f(a)\cdot f(b)^{-1};\; \text{pois } f(b^{-1}) = f(b)^{-1} \\ &= f(a)\cdot f(a)^{-1};\; \text{pois } f(b) = f(a) \\ &= e_H . \end{aligned}$$

De $f(a \,.\, b^{-1}) = e_H$, temos que $a \,.\, b^{-1} \in N(f)$. Como $N(f) = \{e_G\}$, então $a \,.\, b^{-1} = e_G$ e, multiplicando por b dos dois lados, temos $a = b$, de onde concluímos que f é injetora.

6. Sejam $x, y \in H$. Vamos mostrar que $f^{-1}(x \,.\, y) = f^{-1}(x) \,.\, f^{-1}(y)$. Sejam $a = f^{-1}(x)$ e $b = f^{-1}(y)$, então $f(a) = x$ e $f(b) = y$. Assim,

$$\begin{aligned} f^{-1}(x \,.\, y) &= f^{-1}(f(a) \cdot f(b)); \text{ pois } x = f(a) \text{ e } y = f(b) \\ &= f^{-1}(f(a \,.\, b)); \text{ pois } f \text{ Øhomomorfismo} \\ &= a \,.\, b; \text{ pois } f^{-1} \circ f = id \\ &= f^{-1}(x) \cdot f^{-1}(y); \text{ pois } a = f^{-1}(x) \text{ e } b = f^{-1}(y). \end{aligned}$$

Logo, f^{-1} é um homomorfismo de grupos.

O próximo exemplo formaliza uma identificação entre os grupos S_3 e D_3, observada na Aula 13.

Exemplo 4

Seja o grupo $S_3 = \{I, \alpha, \alpha^2, \beta, \beta\alpha, \beta\alpha^2\}$ das permutações de 3 elementos, onde

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

e seja o grupo $D_3 = \{I, R, R^2, F, FR, FR^2\}$ das simetrias do triângulo eqüilátero, da **Figura 18.1** visto na Aula 13,

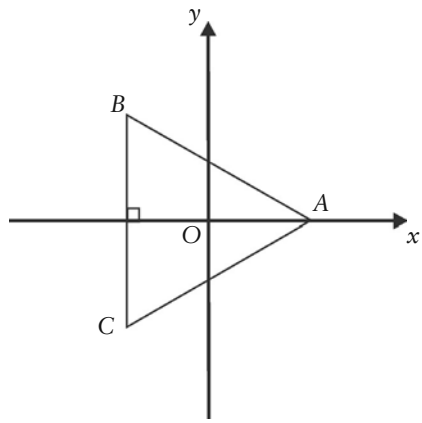


Figura 18.1: Triângulo eqüilátero ABC.

onde $R = R_{2\pi/3}$ é a rotação de $2\pi/3$ radianos em torno da origem e F é a reflexão com respeito ao eixo-x.

Observe a semelhança nas tabelas de multiplicação destes dois grupos. A menos de uma diferença de notação, as duas tabelas são idênticas!

x	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
I	I	α	α^2	β	$\beta\alpha$	$\beta\alpha^2$
α	α	α^2	I	$\beta\alpha^2$	β	$\beta\alpha$
α^2	α^2	I	α	$\beta\alpha$	$\beta\alpha^2$	β
β	β	$\beta\alpha$	$\beta\alpha^2$	I	α	α^2
$\beta\alpha$	$\beta\alpha$	$\beta\alpha^2$	β	α^2	I	α
$\beta\alpha^2$	$\beta\alpha^2$	β	$\beta\alpha$	α	α^2	I

x	I	R	R^2	F	FR	FR^2
I	I	R	R^2	F	FR	FR^2
R	R	R^2	I	FR^2	F	FR
R^2	R^2	I	R	FR	FR^2	F
F	F	FR	FR^2	I	R	R^2
FR	FR	FR^2	F	R^2	I	R
FR^2	FR^2	F	FR	R	R^2	I

Portanto, é natural definirmos a seguinte bijeção entre S_3 e D_3:

$$f : S_3 \to D_3, \text{ onde}$$

$f(I) = I$; $f(\alpha) = R$; $f(\alpha^2) = R^2$: $f(\beta) = F$; $f(\beta\alpha) = FR$; $f(\beta\alpha^2) = FR^2$.

Assim, pelas semelhanças entre as tabelas acima, é fácil ver que

$$f(a \,.\, b) = f(a) \cdot f(b)$$

para todo $a, b, \in S_3$. Logo, f é um homomorfismo bijetor e, portanto, um isomorfismo entre S_3 e D_3, o que denotamos por $S_3 \approx D_3$.

Vamos à nossa próxima atividade. Este é um importante exemplo de automorfismo de grupo.

ATIVIDADE

2. Sejam G um grupo e $g \in G$. Considere a aplicação $i_g : G \to G$ definida por $i_g(x) = gxg^{-1}$. Mostre que i_g é um isomorfismo do grupo G nele mesmo, ou seja, um automorfismo do grupo G.

Vamos finalizar esta aula apresentando um dos exemplos mais importantes de homomorfismo de grupos. Graças a ele temos o importante teorema do homomorfismo para grupos.

Exemplo 5 (O homomorfismo canônico)

Sejam G um grupo e H um subgrupo normal de G. Considere a aplicação entre G e o grupo quociente G/H, $\pi : G \to G/H$, definida por $\pi(a) = aH$. Vamos verificar que π é um homomorfismo de grupo. Dados $a, b \in G$, temos

$$\begin{aligned}\pi(a \,.\, b) &= (a \,.\, b)H \\ &= aH \,.\, bH \\ &= \pi(a) \cdot \pi(b).\end{aligned}$$

Portanto, π é um homomorfismo de grupos, chamado homomorfismo canônico.

Proposição 2

Sejam G um grupo e H um subgrupo normal de G. Seja $\pi : G \to G/H$, $\pi(a) = aH$, o homomorfismo canônico. Então,

1. π é um homomorfismo sobrejetor;
2. $N(\pi) = H$.

Demonstração

1. Seja $aH \in G/H$, $a \in G$, um elemento arbitrário do grupo quociente G/H. Então, da própria definição do homomorfismo canônico, temos que $\pi(a) = aH$, donde concluímos que π é, de fato, sobrejetor.

2. Temos que

$$\begin{aligned}a \in N(\pi) &\Leftrightarrow \pi(a) = e_{G/H} \\ &\Leftrightarrow \pi(a) = \mathrm{H};\ \text{pois } e_{G/H} = e_G H = H \\ &\Leftrightarrow aH = H;\ \text{pois } \pi(a) = aH \\ &\Leftrightarrow a \in H.\end{aligned}$$

E isso prova que $N(\pi) = H$

Observação

1. É importante ressaltar que o homomorfismo canônico é uma função sobrejetora, mas, em geral, não é injetora. Pois, se H é um subgrupo normal do grupo G, diferente do subgrupo trivial $\{e_G\}$, então,

dada qualquer classe lateral $aH \in G/H$, existe $b \in G$, $b \neq a$, tal que $bH = aH$. Assim, temos

$$\pi(b) = bH = aH = \pi(a).$$

E isso prova que o homomorfismo canônico $\pi : G \to G/H$ não é uma função injetora.

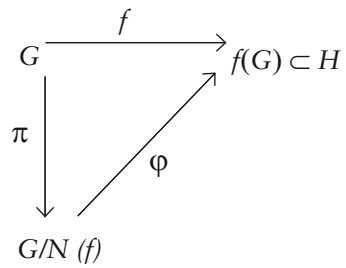
2. O homomorfismo da Atividade 1, $f : Z \to Z_n$, definido por $f(a) = \overline{a}$ para todo $a \in Z$, é um importante exemplo de homomorfismo canônico.

3. Na próxima aula provaremos o teorema do homomorfismo para grupos que tem o seguinte enunciado.

Teorema do Homomorfismo para Grupos

Dado um homomorfismo de grupos $f : G \to H$, então existe um isomorfismo de grupos $\varphi : G/N(f) \to f(G)$ que satisfaz $f : \varphi \circ \pi$, onde $\pi : G \to G/N(f)$ é o homomorfismo canônico.

Representamos esse resultado pelo seguinte esquema.



$G/N(f) \approx f(G)$

ATIVIDADES FINAIS

1. a) Sejam $(Z, +)$ o grupo aditivo dos números inteiros e $f : \mathbf{Z} \to \mathbf{Z}$ um homomorfismo de $\mathbf{Z}$ em $\mathbf{Z}$. Mostre que $f(n) = f(1) \cdot n$ para todo $n \in \mathbf{Z}$.

b) Mostre que todo automorfismo do grupo aditivo $\mathbf{Z}$ é da forma $x \to x$ ou $x \to -x$, para todo $x \in \mathbf{Z}$.

2. a) Sejam $(Z_n, +)$ o grupo aditivo dos inteiros módulo n e $f : Z_n \to Z_n$ um homomorfismo de Z_n em Z_n. Mostre que $f(\overline{a}) = f(\overline{1}) \cdot \overline{a}$ para todo $\overline{a} \in Z_n$.

b) Mostre que todo automorfismo de Z_n é da forma $\overline{x} \to \overline{a} \cdot \overline{x}$, com $\overline{a} \in Z_n^x$.

RESUMO

Nesta aula vimos o conceito de homomorfismo de grupos onde, dados dois grupos G e H, uma função $f: G \to H$ é chamada de um *homomorfismo* (*de grupos*) se

$$f(a \,.\, b) = f(a) \,.\, f(b) \text{ para todo } a, b \in G$$

Se, ainda, f é uma bijeção, então dizemos que $f: G \to H$ é um *isomorfismo* dos grupos G e H e denotamos $G \approx H$.

Para $f: G \to H$ um homomorfismo de grupos, vimos as seguintes propriedades:

1. $f(e_G) = e_H$
2. $f(a)^{-1} = f(a^{-1})$
3. Se N for um subgrupo de G, então $f(N)$ será um subgrupo de H. Em particular, $\mathrm{Im}(f) = f(G)$ é um subgrupo de H.
4. $N(f)$ é um subgrupo normal de G.
5. f é injetora se, e somente se, $N(f) = \{e_G\}$.
6. Se f for bijetora, então $f^{-1}: H \to G$ for um homomorfismo de grupos.

Por fim, vimos o importante exemplo do homomorfismo canônico. Dados G um grupo e H um subgrupo normal de G, o homomorfismo canônico é definido por $\pi: H \to G/H$ com $\pi(a) = aH$.

RESPOSTAS COMENTADAS

Atividade 1

É fácil ver que f é um homomorfismo, pois, dados $a, b \in Z$, temos

$$\begin{aligned} f(ab) &= \overline{ab} \\ &= \overline{a} \,.\, \overline{b} \\ &= f(a) \cdot f(b). \end{aligned}$$

O homomorfismo f é sobrejetor, pois, dado $\overline{a} \in Z_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$, $a \in Z$, então $f(a) = \overline{a}$. Quanto ao núcleo de f, temos

$$\begin{aligned} a \in N(f) &\Leftrightarrow f(a) = \overline{0} \\ &\Leftrightarrow \overline{a} = \overline{0} \\ &\Leftrightarrow a \equiv 0 (\mathrm{mod}\, n) \\ &\Leftrightarrow a \in nZ. \end{aligned}$$

Logo, o núcleo de f é formado pelos múltiplos de n, ou seja, $N(f) = nZ$.

Atividade 2

Vamos verificar primeiro que $ig : G \to G$ é um homomorfismo de grupos. Dados $a, b \in G$, temos que

$$\begin{aligned} i_g(ab) &= g(ab)g^{-1}; \text{pois } f \text{ Øhomomorfismo} \\ &= g(ae_G b)g^{-1} \\ &= g(ag^{-1}gb)g^{-1};\ \text{pois}\ e_G = g^{-1}g \\ &= (gag^{-1})(gbg^{-1}) \\ &= i_g(a)\cdot i_g(b). \end{aligned}$$

Portanto, ig é um homomorfismo de grupos. Agora vamos verificar que i_g é sobrejetora. Dado $b \in G$, queremos encontrar $a \in G$ tal que $i_g(a) = b$, ou seja, queremos que $gag^{-1} = b$. Resolvendo esta equação para a, obtemos $a = g^{-1}bg$. Assim, tomando $a = g^{-1}bg$, temos

$$\begin{aligned} i_g(a) &= i_g(g^{-1}bg);\ \text{pois}\ a = g^{-1}bg \\ &= g(\mathrm{g}^{-1}bg)g^{-1} \\ &= (gg^{-1})b(gg^{-1});\ \text{pela associatividade} \\ &= e_G b e_G;\ \text{pois}\ gg^{-1} = e_G \\ &= b. \end{aligned}$$

Portanto, temos que i_g é sobrejetora. Finalmente, para verificar que i_g é injetora, vamos calcular seu núcleo. Temos que

$$\begin{aligned} a \in N(i_g) &\Leftrightarrow i_g(a) = e_G \\ &\Leftrightarrow gag^{-1} = e_G \\ &\Leftrightarrow ga = e_G g = g;\ \text{multiplicando direita por g} \\ &\Leftrightarrow a = g^{-1}g;\ \text{multiplicando esquerda por g}^{-1} \\ &\Leftrightarrow a = \mathrm{e}_G;\ \text{pois}\ g^{-1}g = e_G. \end{aligned}$$

O cálculo anterior nos diz que $N(i_g) = \{e_G\}$ e, portanto, pela Proposição 1, segue que i_g é injetora. Então, como $i_g : G \to G$ é um homomorfismo bijetor, temos que i_g é um automorfismo de G.

Atividade Final 1

a) 1º caso: $n \geq 0$.

Vamos provar por indução que $f(n) = f(1) \,.\, n$ para todo $n \in N$.

Base: $n = 0$

Como $f : Z \to Z$ é um homomorfismo, então, pela Proposição 1, já sabemos que $f(0) = 0$. Logo,

$$f(0) = 0 = f(1) \,.\, 0 \,.$$

Hipótese de indução: $n = K$

Vamos supor que $f(K) = f(1) \,.\, K$.

Tese de indução: $n = K + 1$

Vamos provar que $f(k+1) = f(1) \cdot (k+1)$. Temos

$$\begin{aligned} f(k+1) &= f(k) + f(1); \quad \text{pois f Øum homomorfismo} \\ &= f(1) \cdot k + f(1); \quad \text{pela hip tese de indu ª o} \\ &= f(1) \cdot (k+1). \end{aligned}$$

Logo, pelo 1º Princípio da Indução, segue que $f(n) = f(1).\, n$ para todo $n \geq 0$.

1º caso: $n < 0$.

Seja $m = -n > 0$. Pelo 1º caso, temos que $f(m) = f(1).\, m$. Como $n = -m$, temos

$$\begin{aligned} f(n) &= f(-m) \\ &= -f(m); \quad \text{pela Proposi ª o 1} \\ &= -(f(1) \cdot m); \quad \text{pelo } 1^{\text{o}} \text{ caso} \\ &= f(1) \cdot (-m) \\ &= f(1) \cdot n. \end{aligned}$$

Portanto, provamos que $f(n) = f(1) \,.\, n$ para todo $n \in Z$.

b) Seja $f : Z \to Z$ um automorfismo de Z. Pelo item a, já sabemos que

$$f(x) = f(1) \cdot x \quad \text{para todo } x \in Z.$$

Como f é uma bijeção de Z, então existe $k \in Z$, tal que

$$f(k) = 1,$$

ou seja,

$$f(1) \,.\, k = 1.$$

Como $f(1)$ e k são números inteiros, temos apenas as possibilidades

$$f(1) = k = 1 \text{ ou } f(1) = k = -1.$$

Portanto, como $f(x) = f(1) \,.\, x$, temos apenas as duas possibilidades

$$f(x) = x \text{ para todo } x \in Z,$$

ou

$$f(x) = -x \text{ para todo } x \in Z.$$

Atividade Final 2

a) Dado $\overline{a} \in Z_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ podemos considerar $0 \le a < n-1$. Se $a = 0$, então já sabemos, pela Proposição 1, que $f(\overline{0}) = \overline{0}$. Agora, podemos supor que $0 < a < n-1$ e, portanto,

$$\overline{a} = \overline{1} + \overline{1} + \cdots + \overline{1} \quad (a \text{ parcelas}).$$

Usando que f é homomorfismo, temos

$$\begin{aligned} f(\overline{a}) &= f(\overline{1} + \overline{1} + \cdots + \overline{1}); \text{ pois } \overline{a} = \overline{1} + \overline{1} + \cdots + \overline{1} \ (n \text{ parcelas}) \\ &= f(\overline{1}) + f(\overline{1}) + \cdots + f(\overline{1}); \text{ pois } f \text{ Øhomomorfismo } (n \text{ parcelas}) \\ &= f(\overline{1}) \cdot (\overline{1} + \overline{1} + \cdots + \overline{1}); \ (n \text{ parcelas}) \\ &= f(1) \cdot \overline{a}; \text{ pois } \overline{a} = \overline{1} + \overline{1} + \cdots + \overline{1} \ (n \text{ parcelas}). \end{aligned}$$

b) Seja, agora, $f : Z_n \to Z_n$ um automorfismo de Z_n. Já sabemos, pelo item a, que

$$f(\overline{x}) = f(\overline{1}) \cdot \overline{x} \text{ para todo } \overline{x} \in Z_n.$$

Como f é uma bijeção de Z_n, então existe $\overline{b} \in Z_n$ tal que

$$f(\overline{b}) = \overline{1}$$

ou seja,

$$f(\overline{1}) \,.\, \overline{b} = \overline{1}.$$

Então, $f(\bar{1})$ e $\bar{b}$ são elementos invertíveis de Z_n, ou seja, $f(\bar{1}), \bar{b} \in Z_n^x$. Assim, denotando $\bar{a} = f(\bar{1})$, temos

$$f(\bar{x}) = f(\bar{1}) \cdot \bar{x} = \bar{a} \,.\, \bar{x} \quad \text{com} \quad \bar{x} \in Z_n^x \ .$$

Álgebra II

Referências

GONÇALVES, Adilson. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1999. (Projeto Euclides-IMPA.)

IEZZ, Gelson et al. *Fundamentos da matemática elementar*. São Paulo: Atual, 1993. v. 6.

Aulas 12 e 13

GARCIA, Arnaldo; LEQUAIN, Yves. *Álgebra*: um curso introdutório. [s.l: s.n.], 2004. (Projeto Euclides - IMPA.)

GONÇALVES, Adilson. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1999. (Projeto Euclides-IMPA.)

Aula 14

GONÇALVES, Adilson. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1999. (Projeto Euclides-IMPA.)

IEZZ, Gelson et al. *Fundamentos da matemática elementar*. São Paulo: Atual, 1993. v. 6.

Aula 15

GARCIA, Arnaldo; LEQUAIN, Yves. *Álgebra*: um curso introdutório. [s.l: s.n.], 2004. (Projeto Euclides - IMPA.)

GONÇALVES, Adilson. *Introdução à álgebra*. Rio de Janeiro: IMPA, 1999. (Projeto Euclides-IMPA.)

ISBN 85-7648-314-9
9 788576 483144

UENF
Universidade Estadual
do Norte Fluminense

UERJ
UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO

Universidade Federal Fluminense
UFF

UFRJ

Universidade Federal Rural
do Rio de Janeiro

UNIRIO

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

GOVERNO DO
Rio de Janeiro
SECRETARIA DE
CIÊNCIA E TECNOLOGIA

UAB
UNIVERSIDADE
ABERTA DO BRASIL

Ministério
da Educação

BRASIL
UM PAÍS DE TODOS
GOVERNO FEDERAL