Matemática

Estruturas Algébricas

Cleiton Batista Vasconcelos

1ª Edição
Ed UECE
Fortaleza
2019

Geografia

História

Educação Física

Química

Ciências Biológicas

Artes Plásticas

Computação

Física

Matemática

Pedagogia

Editora Filiada à

ASSOCIAÇÃO BRASILEIRA DAS EDITORAS UNIVERSITÁRIAS

Presidente da República
Jair Messias Bolsonaro
Ministro da Educação
Abraham Bragança de Vasconcellos Weintraub
Presidente da CAPES
Abilio Baeta Neves
Diretor de Educação a Distância da CAPES
Carlos Cezar Modernel Lenuzza
Governador do Estado do Ceará
Camilo Sobreira de Santana
Reitor da Universidade Estadual do Ceará
José Jackson Coelho Sampaio
Vice-Reitor
Hidelbrando dos Santos Soares
Pró-Reitora de Pós-Graduação
Nucácia Meyre Silva Araújo
Coordenador da SATE e UAB/UECE
Francisco Fábio Castelo Branco
Coordenadora Adjunta UAB/UECE
Eloísa Maia Vidal
Direção do CED/UECE
José Albio Moreira de Sales
Coordenação da Licenciatura em Matemática
Ana Carolina Costa Pereira
Coordenação de Tutoria da Licenciatura em Matemática
Gerardo Oliveira Barbosa
Editor da EdUECE
Erasmo Miessa Ruiz
Coordenadora Editorial
Rocylânia Isidio de Oliveira
Projeto Gráfico e Capa
Roberto Santos
Diagramador
Francisco Oliveira
Revisão Ortográfica
Fernanda Ribeiro

Editora da Universidade Estadual do Ceará – EdUECE
Av. Dr. Silas Munguba, 1700 – Campus do Itaperi – Reitoria – Fortaleza – Ceará
CEP: 60714-903 – Fone: (85) 3101-9893
Internet: www.uece.br – E-mail: eduece@uece.br

Secretaria de Apoio às Tecnologias Educacionais
Fone: (85) 3101-9962

Sumário

Apresentação

Capítulo 1

Operações Binárias

Objetivo

- Neste capítulo, apresentaremos o conceito de operação binária, exemplificando e demonstrando suas principais propriedades.

Introdução

Conhecemos, desde o primeiro segmento do Ensino Fundamental, o que se convencionou chamar de operações fundamentais nos números naturais: a adição, a subtração, a multiplicação e a divisão.

Dados dois números naturais, **m** e **n**, a adição associa a eles o número **m+n**, chamado soma ou total de **m** com **n**; a subtração associa a eles o número **m—n**, chamado de diferença entre **m** e **n**; a multiplicação, aos dois números, associa o número **mXn**[1], chamado de produto de **m** por **n**; e a divisão associa a eles o número **m/n**, chamado de quociente[2] entre **m** e **n**; todos tomados nesta ordem. Como já sabemos, enquanto a adição e a multiplicação de números naturais são sempre possíveis, isto é, dados dois números naturais é sempre possível encontrar um número natural que represente sua soma ou seu produto, o mesmo não ocorre quando se trata da subtração e da divisão. Por exemplo, a diferença 5—8 não é um número natural; o quociente 1/2 também não é um número natural. Ao estudarmos a adição e a multiplicação de números naturais, nos deparamos com suas propriedades.

Todos sabemos que, para efetuar a adição 3 + 4 + 5, podemos começar somando 3 + 4 e, em seguida, somarmos o resultado com o 5; ou podemos fazer, inicialmente, 4 + 5 = 9, para, em seguida, fazermos 3 + 9. O resultado, em ambos os casos, é 12. Sabemos também que essas duas maneiras de adicionar podem ser utilizadas na adição de quaisquer 3 números naturais. Também sabemos que, em 3X4 e em 4X3, embora a ordem dos fatores seja diferente, os dois produtos são iguais. Sabemos, ainda, que 0 adicionado com qualquer número natural dá sempre esse número natural e que o produto de 1 por qualquer número natural é esse número natural. Observando atentamente a adição e a multiplicação de números naturais, percebemos que a ideia que permeia essas operações é a de uma lei que associa a cada par de números

[1] O número m X n também pode ser indicado por m.n ou, simplesmente, mn. Usaremos indistintamente qualquer uma das três notações.
[2] O quociente m/n só faz sentido quando n é um número diferente se zero.

naturais, tomados em certa ordem, um número natural, não necessariamente diferente dos dois primeiros.

Essas idéias podem ser generalizadas para conjuntos e operações quaisquer, como veremos a seguir.

1. Operação Binária

Definição. Dado E, um conjunto não vazio, uma **operação binária**[3] definida em E ou, simplesmente, uma operação definida em E é uma lei * que associa a cada par ordenado (x,y) de elementos de E um e somente um elemento x*y, também de E.

Se * é uma operação definida em E, dizemos, também, que E é um conjunto munido de uma operação[4].

O elemento x*y é chamado o composto de x com y por estrela, nesta ordem. Os elementos x e y são chamados termos de x*y, sendo x o primeiro termo ou termo da esquerda e y o segundo termo ou termo da direita.

Exemplo 1.01. A adição e a multiplicação de números naturais são exemplos de operação binária sobre o conjunto N, dos números

naturais. Já a subtração e a divisão, por não poderem ser realizadas entre dois números naturais quaisquer, não são operações sobre o conjunto dos números naturais.

Exemplo 1.02. A subtração é uma operação quer no conjunto Z, dos números inteiros, quer no conjunto Q, dos números racionais.

Exemplo 1.03. Mesmo no conjunto Q, dos números racionais, a divisão não é uma operação. Não existe, em Q, o quociente 3/0, por exemplo.

Exemplo 1.04. A adição e a multiplicação de números complexos[5] são exemplos de operações em C, o conjunto dos números

complexos. De fato, se u = a+bi e v = c+di são números complexos, então sua soma u + v é definida como u + v = (a+c) + (b+d)i, que também é um número complexo. O produto de u por v é definido por u.v = (ac–bd) + (ab+cd)i e é também um número complexo.

Exemplo 1.05. Novamente, a divisão não é operação em C. Em C, não existe divisão por 0 (zero).

Exemplo 1.06. Em N, o conjunto dos números naturais, defina * por a*b = 2a + 3b. A lei * é uma operação em N. De fato, dados os

números naturais a e b, sempre é possível calcular 2a + 3b, e o resultado, além de ser univocamente determinado, é um número natural.

Exemplo 1.07. A adição de matrizes é uma operação no conjunto das ma-

[3]Uma operação binária em um conjunto E também é chamada de lei de composição interna em E. A palavra "binária" é para ressaltar que * opera sempre com dois elementos de cada vez.

[4]Um conjunto não vazio E, munido de uma operação * é dito uma ESTRUTURA ALGÉBRICA.

[5]Um número complexo é um número z da forma z = a + bi, em que a e b são números reais e i é um número imaginário tal que i2 = -1. Eles foram criados, possivelmente, para que toda equação do segundo grau tivesse duas raízes.

trizes quadradas de ordem 2, com entradas[6] reais. De fato, a soma de duas matrizes quadradas de ordem 2, com entradas reais, sempre está definida e é, ainda, uma matriz quadrada de ordem 2, com entradas reais.

Exemplo 1.08. A adição de polinômios não é uma operação no conjunto dos polinômios a uma indeterminada, com coeficientes inteiros e de grau 2. De fato, embora a adição de dois ou mais polinômios a uma indeterminada e com coeficientes inteiros seja ainda um polinômio a uma indeterminada e com coeficientes inteiros, quando adicionamos dois polinômios de grau 2 o resultado pode não ser um polinômio de grau 2. Como exemplo podemos citar os polinômios p(x) = 3x2+2x e q(x) = -3x2+2. Quando efetuamos p(x)+q(x) encontramos o polinômio f(x) = 2x + 2, que é de grau 1.[7]

Exemplo 1.09. A adição no conjunto 2N, dos números naturais pares, é uma operação em 2N. De fato, a soma de dois números pares sempre está definida e é um número par. Já o mesmo não ocorre no conjunto I, dos números naturais ímpares. A soma de dois números ímpares, apesar de sempre estar definida, não é um número ímpar.

Exemplo 1.10. Sejam E um conjunto e P(E) o conjunto das partes de E, isto é, o conjunto de todos os subconjuntos de E. A união e a interseção de conjuntos são operações em P(E). De fato, quando tomamos dois subconjuntos X e Y de E, a união $X \cup Y$ está definida para todos X e Y e é um subconjunto de E. Também a interseção $X \cap Y$ está definida para todos X e Y e é um subconjunto de E.

Exemplo 1.11. No conjunto E de todos os pontos de um plano α, definimos * como a lei que associa, aos pontos P e Q, o ponto médio

do segmento PQ. Então * é uma operação binária em E. De fato, dados dois pontos quaisquer, P e Q, de α, o segmento PQ está contido em α e, consequentemente, o ponto médio de PQ está em α. Aqui, estamos definindo o segmento PP e seu ponto médio como o próprio ponto P.

Operações definidas por meio de tabelas

Em geral, para definir uma operação binária em um conjunto finito, utilizamos uma tabela, como explicaremos a seguir.

Para maior simplicidade e melhor compreensão, vamos explicar o processo, definindo uma operação * no conjunto E = {a, b, c, d}. Na primeira linha da tabela colocaremos o símbolo da operação, seguido pelos elementos de E, dispostos em qualquer ordem. Assim, a primeira linha da tabela que queremos construir pode ser qualquer uma das que seguem:

*	a	b	c	d

Tabela 1

*	b	c	a	d

Tabela 2

*	d	a	c	b

Tabela 3

[6] Chamamos de entradas de uma matriz A = (aij) mXn cada um dos elementos aij desta matriz.

[7] O grau do polinômio p(x) = a0 + a1x + a2x2 + ... + anxn, na indeterminada x, é definido como o maior expoente r, da indeterminada x, tal que o coeficiente ar é não nulo. O grau do polinômio nulo — p(x) = 0 — não é definido. Muitas vezes, por questões de conveniência, usaremos definir o grau do polinômio nulo como sendo -1.

Na primeira coluna, debaixo da *, dispomos os elementos de E, na mesma ordem em que eles se encontram na primeira linha. Para a tabela 1 anterior, temos:

*	a	b	c	d
a				

*	a	b	c	d
a				
b				

*	a	b	c	d
a				
b				
c				
d				

Agora falta definirmos, para cada par ordenado (x,y) de elementos de E, o elemento x*y. Tal elemento tomará lugar na interseção da linha que inicia com o elemento x com a coluna que inicia com o elemento y. Por exemplo, nas três tabelas a seguir, temos os elementos a*c = b, b*d = a e d*c = d.

*	a	b	c	d
a			b	
b				
c				
d				

*	a	b	c	d
a				
b				a
c				
d				

*	a	b	c	d
a				
b				
c				
d				d

Assim, já definimos três dos dezesseis elementos. Os demais podem ser definidos, devendo-se observar, apenas, que o resultado de x*y só pode ser a, b, c ou d.

A seguir, temos as tabelas de três operações diferentes, definidas no conjunto E.

*	a	b	c	d
a	d	a	b	c
b	a	b	d	a
c	c	b	a	b
d	d	d	a	b

*	a	b	c	d
a	b	b	a	b
b	a	b	c	a
c	c	d	b	c
d	b	c	a	d

*	a	b	c	d
a	a	d	c	b
b	b	c	d	a
c	c	b	a	c
d	d	a	d	b

2. Propriedades das operações binárias

Comutatividade

Como sabemos, a adição e a multiplicação de números naturais são tais que 3 + 4 = 4 + 3 e 3X4 = 4X3.

Essas propriedades se generalizam para quaisquer dois números naturais e costumam ser resumidas por:

"a ordem das parcelas não altera a soma",

para a adição; ou

"a ordem dos fatores não altera o produto",

no caso da multiplicação.

Existem outras operações para as quais a ordem em que os termos aparecem não altera o composto, ou seja, chamando os termos de x e y e representando a operação binária por *, temos x*y = y*x. Como exemplo, podemos citar:

- no conjunto P(E), das partes de E, as operações de união e interseção de conjuntos;
- no conjunto R, dos números reais, a média aritmética (x*y é a média aritmética entre x e y) e a média geométrica (x*y é a média geométrica entre x e y).

Existem, também, operações para as quais a ordem dos termos altera o composto, ou seja, chamando os termos de x e y e representando a operação binária por *, temos $x*y \neq y*x$. Por exemplo:

- em Z, a subtração;
- em R, a operação binária definida por x*y = y.

Essas observações nos levam à seguinte definição.

Definição. Dizemos que uma operação binária *, definida em um conjunto não vazio E, é **comutativa** ou possui a (ou goza da) **propriedade comutativa** se, e somente se, vale o seguinte:

"$\forall$ x, y $\in$ E, x*y = y*x". 7

Associatividade

Ainda recorrendo à adição e à multiplicação de números naturais, observamos que 3 + (6 +8) = (3 + 6) + 8 e que 3X(6X8) = (3X6)X8.

Também como no caso anterior, essa propriedade se generaliza para 3 números naturais quaisquer. Ou seja, para adicionarmos (ou multiplicarmos) 3 números naturais, podemos começar pelos dois primeiros e a soma (o produto) destes adicionar ao (multiplicar com o) terceiro; ou podemos começar adicionando (multiplicando) o segundo e o terceiro e, depois, adicionarmos (multiplicarmos) o primeiro com (por) esse resultado.

Embora essa também seja uma propriedade de outras operações binárias, como:

- a união e a interseção, no conjunto P(E), das partes do conjunto E;
- a composição de funções, no conjunto F(R,R), de todas as funções de R em R;

essa propriedade não é comum a todas as operações binárias, isto é, existem operações em que essa propriedade não vale. Por exemplo:

- a subtração, no conjunto Z, dos números inteiros (x*y = x – y);
- a potenciação no conjunto N, dos números naturais ($x*y = x^y$);
- a média aritmética, no conjunto R dos números reais (x*y é a média aritmética entre x e y).

Essas observações nos levam à seguinte definição.

Definição. Dizemos que uma operação * definida em um conjunto E é **associativa** ou possui a (ou goza da) **propriedade associativa** se, e somente, se, vale o seguinte:

"$\forall$ x, y, z $\in$ E, (x*y)*z = x*(y*z)".

Idenpotência

Observando as operações de união e interseção de conjuntos definidas no conjunto P(E), das partes de um conjunto E, percebe-se que:

- $X \cup X = X$, para todo X em P(E); e
- $X \cap X = X$, para todo X em P(E).

Observa-se também que essa não é uma propriedade válida para a adição nem para a multiplicação de números naturais pois, embora 0 + 0 = 0 e 1X1 = 1, esses são os únicos números naturais com essa propriedade.

Isso sugere a definição que segue.

Definição. Dizemos que uma operação * definida em um conjunto E é idempotente ou possui a (ou goza da) propriedade da idempotência se, e somente, se, vale o seguinte:

"$\forall$ x $\in$ E, (x*x) = x".

Parte fechada de um conjunto para uma operação binária

Considerando a adição, definida no conjunto dos números naturais, percebe-se, facilmente, que ao adicionarmos dois números pares, a soma é, ainda, um número par. Observa-se, também, que o mesmo não ocorre com os números ímpares. Por exemplo, ao adicionarmos os números ímpares 3 e 5 obtemos o número par 8. Na realidade, a soma de dois números ímpares é, sempre, um número par.

Assim, podemos dizer que a adição é uma operação definida no conjunto dos números pares, enquanto que, restrita ao conjunto dos números ímpares, não o é.

Essas observações nos conduzem às seguintes definições.

Sejam E um conjunto não vazio, * uma operação definida em E e A um subconjunto não vazio de E.

Definição. Dizemos que A é uma parte de E, fechada para a operação * ou, simplesmente, que A é fechado para a operação *, se, e somente se, vale o seguinte:

"$\forall$ x, y $\in$ A, x*y $\in$ A".

Neste caso, a operação *, definida em E, também é uma operação definida em A. Essa operação, definida em A, é chamada restrição de * ao conjunto A.

Exemplo 1.12. O subconjunto A = {-1, 0, 1}, do conjunto Z, dos números inteiros, é fechado para a multiplicação de números inteiros.

Exemplo 1.13. O subconjunto E = {1, i, -1, -i}, do conjunto C, dos números complexos, é fechado para a multiplicação de números complexos.

Potências de um elemento

Na adição de números naturais, convencionou-se escrever **n**×**a**, para representar a adição de **n** parcelas[8] iguais ao número natural **a**.

$$\text{“}n \times a = \underbrace{a + a + \ldots + a}_{n \text{ parcelas}}$$

Na multiplicação também se convencionou chamar de an, o produto de n fatores[9] iguais ao número natural a.

$$\text{“}a^n = \underbrace{a \times a \times \ldots \times a}_{n \text{ fatores}}\text{“}$$

Para uma operação binária associativa, convencionou-se denotar por a^n, o composto de n termos iguais ao elemento **a**. Convencionou-se, ainda, denotar o elemento **a** por a^1.

[8]Parcela é o nome que se dá a cada um dos termos da adição. Como operação binária, essa convenção só faz sentido para n número natural, maior do que ou igual a 2.

[9]Fator é o nome que se dá a cada um dos termos da multiplicação. Como na nota anterior, essa convenção só faz sentido para n número natural, maior do que ou igual a 2.

3. Elementos notáveis de um conjunto com operação binária

Assim como o 0 (zero), na adição de números naturais, e o 1 (um), na multiplicação de números naturais, possuem o que se convencionou chamar de propriedade do elemento neutro, alguns elementos de um conjunto com uma operação binária possuem propriedades especiais.

No que segue e até que se diga o contrário, E será um conjunto munido de uma operação binária *.

Definição. Um elemento e, pertencente ao conjunto E é dito ser um **elemento neutro** para a operação * se, e somente se, satisfaz o seguinte:

$$\text{“}e*x = x*e = x,\ \forall\ x \in E\text{”}.$$

Unicidade do elemento neutro. No caso de um conjunto com uma operação possuir um elemento neutro este elemento é único com essa propriedade. (Ver exercício resolvido 05)

Definição. Se E possui um elemento neutro e para a operação binária *, um elemento b, de E, é dito ser **simetrizável** para a operação * se, e somente se, satisfaz o seguinte:

$$\text{“}\exists\ b' \in E, \text{ tal que } b'*b = b*b' = e\text{”}.$$

O elemento b', quando existe, é chamado o **simétrico** de b para a operação *.

Somente existe unicidade para do simétrico de um elemento, se a operação for associativa.

Observe que, de acordo com a definição, a existência do simétrico de um elemento pressupõe a existência de um elemento neutro para a operação *.

Unicidade do elemento simétrico. Diferentemente do elemento neutro, é possível que um elemento de E possua mais de um simétrico. Entretanto, mostra-se que, no caso de operações associativas, o simétrico de um elemento, se existir, será único. (Ver exercícios resolvidos 06 e 07)

Definição. Um elemento a, pertencente ao conjunto E, é dito ser um elemento absorvente para a operação * se, e somente se, satisfaz o seguinte:

$$\text{“}a*x = x*a = a,\ \forall\ x \in E\text{”}.$$

Unicidade do elemento absorvente. Como no caso do elemento neutro, o elemento absorvente, quando existe, é único. (Ver exercício resolvido 08)

Definição. Um elemento c, pertencente ao conjunto E, é dito ser um elemento **idempotente** para a operação * se, e somente se, satisfaz o seguinte:

$$\text{“}x*x = x\text{”}.$$

Observe que se E possui elemento neutro para a operação *, este elemento também será idempotente para *.

4. Algumas palavras de advertência

Ao se definir uma operação * em um conjunto E, é importante estarmos atento às duas exigências que se seguem:

1. Exatamente um elemento deve ser associado a cada par ordenado de elementos de E.

   Não basta associar um elemento para a maioria dos pares ordenados de elementos de E. É importante que essa associação seja feita para todo par ordenado. Se não for assim, dizemos que * **não foi definida**.

   Não pode acontecer, também, de haver ambiguidade na definição do elemento associado a cada par . Se houver essa ambiguidade, dizemos que * **não está bem definida**.

2. Para cada par ordenado de elementos de E, o elemento associado deve estar em E.

   Não pode acontecer de o elemento associado a algum par de elementos de E não pertencer ao conjunto E. Se o elemento associado a algum par de elementos não pertencer ao conjunto E, dizemos que E **não é fechado** para *.

Síntese do Capítulo

1. Neste capítulo nós estudamos as operações binárias ou leis de composição interna em um conjunto não vazio E.
2. Vimos que, de acordo com sua definição, somente serão operações binárias aquelas leis que podem ser aplicadas a cada dois elementos do conjunto, sem exceção, e que obtém como resultado um e somente um elemento do próprio conjunto, composto de um elemento com o outro.
3. Estudamos as propriedades comutativa, associativa e idempotente das operações binárias.
4. Estudamos e aprendemos a encontrar alguns elementos notáveis das operações: elemento idempotente, elemento neutro e elemento simétrico.
5. Vimos que, enquanto o elemento neutro sempre é único, a unicidade do elemento simétrico só pode ser garantida para as operações associativas.

Leituras, filmes e sites

Aron Simis, p.1.

A natureza é pródiga em sistemas que guardam entre si, por diferentes que sejam, certos atributos comuns. A fim de expressar o que há de comum entre tais sistemas, é conveniente estabelecer alguma linguagem matemática mediante a qual se possam abstrair certas propriedades "mínimas" que permanecem válidas qualquer que seja o sistema particular em questão. Chega-se então à ideia de estrutura (ou conjunto estruturado) em Matemática.

Exercícios Resolvidos

RES1.01. Seja E o conjunto dos restos possíveis da divisão euclidiana de números inteiros, por 6. como sabemos, E={0, 1, 2, 3, 4, 5}. A tabela abaixo define uma operação * em E, chamada de **adição módulo 6.**

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Essa operação é associativa e comutativa, mas não é idempotente.

De fato, a operação não é idempotente, pois 2*2 = 4 2, por exemplo. A comutatividade é facilmente percebida a partir de uma análise mais atenta da tabela. Para a associatividade, basta observamos que nessa adição tomamos sempre o resto da divisão por 6. É como se fosse fazemos grupos de 6 e tomando as sobras. Assim, por exemplo, 5+5 = (5+1)+4 = 4. Assim, podemos efetuar (3+4)+5 fazendo 3+4 = (3+3)+1 = 1. E fazendo agora 1+5 = 0. Mas como estamos interessados na sobra que fica após agruparmos todas as unidades, podemos efetuar assim (3+4)+5 = (3+3)+(1+5) = 0. De maneira semelhante, podemos fazer 3+(4+5) = 3+[3+(1+5)], o que nos dá 3+(4+5) = (3+3)+(1+5) = 0. Esse processo pode ser generalizado, obtendo-se a associatividade da operação.

RES1.02. A subtração, no conjunto Z dos números inteiros, é uma operação que não é associativa, nem comutativa.

De fato, se considerarmos as subtrações

6 – (5 – 4) = 6 – 1 = 5 e (6 – 5) – 4 = 1 – 4 = -3, veremos que a operação de subtração não é associativa. Considerando as subtrações

5 – 4 = 1 = 5 e 4 – 5 = -1,

percebemos que não vale a comutatividade.

RES1.03. No conjunto dos números naturais, a operação * definida por a*b = 2a + 3b não é comutativa.

De fato,

2*3 = 2X2 + 3X3 = 4 + 9 = 13, enquanto

3*2 = 2X3 + 3X2 = 6 + 6 = 12.

RES1.04. Seja E o conjunto com quatro elementos, dado por E={0,1,a,b} e defina * em E de acordo com a seguinte tabela:

*	**0**	**1**	**a**	**b**
0	0	1	0	1
1	a	b	a	b
a	0	0	a	a
b	b	a	1	0

Observe que 1*0 = a e 0*1 = 1. Portanto, * não comutativa.

RES1.05. O elemento neutro de um conjunto E com operação binária

*, se existir, é único.

De fato, suponha que existam em E elementos neutros u e v. Como u é elemento neutro, temos que u*v = v e como v é elemento neutro, temos que u*v = u. Assim, teremos u = v.

RES1.06. É possível que um elemento de um conjunto E com operação binária *, possua mais de um simétrico.

De fato, sejam E = { a, b, c, d } e * a operação definida por:

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	b	a
d	d	a	a	b

Temos que a é o elemento neutro de * e como b*d=d*b=a e c*d=d*c=a, temos que b e c são simétricos de d.

RES1.07. Se em um conjunto E com operação binária *, a operação é associativa, então o simétrico de um dado elemento, se existir, é único.

De fato, sejam E um conjunto com operação *, com elemento neutro e, e u um elemento de E. Suponha que u' e v' são elementos de E tais que:

• u*v'= v'*u = e.

Temos as igualdades:

u' = e*u' = (v'*u)*u' = v'*(u*u') = v'*e = v',

que mostram que, se vale a associatividade, o simétrico de um elemento, se existir, é único.

RES1.08. Seja E um conjunto não vazio com operação binária * e suponha que em E exista um elemento absorvente, digamos u. Esse elemento é o único com essa propriedade.

De fato, suponha que v seja, também, elemento absorvente de E. Assim, devemos ter as igualdades:

• u*v = u, pois u é elemento absorvente;

• u*v = v, pois v é elemento absorvente. Daí, u = v, e o elemento absorvente é único.

RES1.09. No conjunto G de todas as funções f: R $\rightarrow$ R, defina a composição de funções reais por: Dados f,g: R $\rightarrow$ R, a composta de f com g é a função fog: R $\rightarrow$ R, dada por fog(x) = f(g(x)) para cada x $\in$ R.

Observe inicialmente que, se f e g são funções em G, então fog é uma função de G, univocamente determinada por f e g, pois, para cada número real x, fog(x) assume um valor e, desde que g(x) assume um único valor e para esse valor, f(g(x)) também assume um único valor, o valor de fog(x) é único. Assim, a composição de funções reais é uma operação em G.

Essa operação é associativa, mas não é comutativa.

De fato, temos que fo(goh): R → R e (fog)oh: R → R, possuem o mesmo domínio e o mesmo contradomínio. Além disso, temos que [fo(goh)](x) = f((goh)(x)) = f(g(h(x))) e ([fog]oh)(x) = [fog](h(x)) = f(g(h(x))), ou seja, as funções coincidem ponto a ponto. Assim, vale a associatividade.

Para mostrarmos que não vale a comutatividade da operação de composição, sejam as funções f: R → R e g: R → R, dadas por f(x) = 2x e g(x) = x + 5. Temos que

- (fog)x = f(g(x)) = f(x+5) = 2(x+5) = 2x + 10; e
- (gof)x = g(f(x)) = g(2x) = 2x + 5.

O que mostra que a composição de funções não é comutativa.

Atividades de avaliação

1. Seja P(E) o conjunto das partes de um conjunto qualquer E. Defina, em P(E), a operação * por X*Y = (X-Y)U(Y-X). Verifique se a operação * é:

a) comutativa;

b) associativa.

2. Seja E o conjunto dos pontos de um plano α. Defina uma operação binária *, em E, por "M*N é o simétrico de N em relação a M". Verifique se * é uma operação:

a) comutativa;

b) associativa;

c) idempotente.

3. No conjunto R dos números reais, defina a operação * por x*y = x + y + 1. Verifique se * é:

a) comutativa;

b) associativa;

c) idempotente.

4. Verifique se a composição de funções, no conjunto F(R,R), das funções de R em R, é uma operação:

a) comutativa;

b) associativa;

c) idempotente.

5. Verifique se a operação de divisão, definida em R – {0}, por a*b = a:b, é:

a) associativa;

b) comutativa.

[10] Copiado do livro A first course in abstract algebra de John B. Fraleigh.
[11] Adaptado do livro A first course in abstract algebra de John B. Fraleigh.

6. Verifique se a operação de exponenciação, definida em N por a*b = ab é:

a) associativa;

b) comutativa.

7. Determinar todos os pares (a,b), de números reais, para os quais a operação *, definida em R por x*y = ax + by, é:

a) associativa;

b) comutativa.

8. Verifique se são associativas as operações * definidas em R por:

a) x*y = 2xy

b) x*y = x + y + xy

9. . Verifique se são comutativas as operações * definidas em R por:

a) x*y = (x/2).(y/3)

b) x*y = x + y2

10. No conjunto R, dos números reais, define-se a operação * por a*b = máx{a,b} (que se lê: máximo entre a e b) cujo resultado é o maior dos dois números reais a e b. Por exemplo, 2*3 = 3, 5*3 = 5. Verifique se essa operação é:

a) associativa;

b) comutativa;

c) idempotente.

11. Verifique se, no conjunto dos números reais, a média aritmética é uma operação:

a) associativa;

b) comutativa;

c) idempotente.

12. Verifique se, no conjunto dos números reais, a média geométrica é uma operação:

a) associativa;

b) comutativa;

c) idempotente.

13. Mostre que A = {0, 1, -1} é uma parte fechada do conjunto dos números inteiros, para a multiplicação de números inteiros.

14. Mostre que o conjunto A = {1, i, -1, -i} é uma parte fechada do conjunto dos números complexos, para a multiplicação de números complexos.

15. Mostre que, no conjunto das matrizes quadradas de ordem 2, com entradas reais, a adição de matrizes é uma operação associativa e comutativa.

16. Mostre que a adição e a multiplicação de números complexos são operações comutativas e associativas.

17. Seja R* o conjunto de todos os números reais não nulos e defina em R* a operação * dada por a*b = |a|b.

a) Mostre que * é uma operação binária em R*;

b) Mostre que existe elemento neutro a esquerda para a operação *;

c) Mostre que todo elemento de R* é simetrizável à direita com esse elemento neutro.10

18. Seja S o conjunto consistindo de vinte pessoas todas com altura diferente umas das outras. Defina * em S por a*b = c, em que c é a pessoa mais baixa entre todos os que são mais altos do que a e b. Mostre que * não é uma operação binária em S.[11]

Referências

FRALEIGH, J.B. A first course in abstract algebra. Addison-Wesley: Japão, 1968

GONÇALVES, Adilson. Introdução à álgebra. Projeto Euclides. IMPA: Rio de Janeiro, 1979.

JACOBSON, N. Basic algebra. W. H. Freeman Company: San Francisco--USA, 1974.

NACHBIN, Leopoldo. Introdução à álgebra. McGraw-Hill do Brasil Ltda/Editora da UNB: Rio de Janeiro, 1971.

SIMIS, Aron. Introdução à álgebra. Monografias de Matemática 23. IMPA: Rio de Janeiro, 1977.

Capítulo 2

Definição e propriedades elementares

Objetivo

- Neste capítulo, apresentaremos o conceito de grupos, exemplificando e demonstrando suas principais propriedades.

Introdução

A adição no conjunto dos números naturais goza de certas propriedades como a associatividade e a comutatividade e possui elemento neutro. Pelo fato de a adição ser associativa em N, dizemos que o par (N,+) é exemplo de uma estrutura algébrica chamada SEMIGRUPO. Como, N possui elemento neutro para a adição, dizemos que a estrutura algébrica (N,+) é um monoide.

Também são exemplos de semigrupos as estruturas:

- (N,X), do conjunto dos números naturais com a multiplicação;
- (Z,+), do conjunto dos números inteiros com a adição;
- (Z,X), do conjunto dos números inteiros com a multiplicação; e
- (Q,+), do conjunto dos números racionais com a adição.

Por possuírem elemento neutro, todas essas estruturas listadas anteriormente também são exemplos de monoides.

No caso dos números inteiros e dos números racionais com a adição, cada elemento x do monoide (Z,+) e (Q,+) possui um elemento simétrico, indicado por –x, e também chamado de oposto de x. Dizemos, por isso, que (Z,+) e (Q,+) possuem a estrutura de grupo.

Assim, um grupo é um monoide cuja operação possui a propriedade do elemento simetrizável para todo elemento.

Essa estrutura de grupo está presente em muitos exemplos na Matemática, como veremos a seguir.

1. Grupos: definição e exemplos

Conforme mencionamos anteriormente, o que faz com que o monoide (Z,+) seja um grupo é o fato de todos os seus elementos serem simetrizáveis para a adição. Assim, podemos definir grupo como segue.

Definição. Um grupo é um par (G,*), em que G é um conjunto não vazio e * é uma operação binária em G, gozando das seguintes propriedades:

G1: * é associativa;

$$\forall\ a, b, c \in G,\ a*(b*c) = (a*b)*c$$

G2: G possui elemento neutro;

$$\exists\ e \in G;\ a*e = e*a = a,\ \forall\ a \in G$$

G3: Todo elemento de G é simetrizável.

$$\forall\ a \in G,\ \exists\ a' \in G;\ a*a' = a'*a = e$$

É bom que fique claro que na definição que o grupo é o par (G,*). Isso significa que um mesmo conjunto pode ser grupo com uma operação e não sê-lo com outra. Por exemplo, (Z,+) é um grupo, enquanto (Z,X) não o é. A mesma observação se aplica à operação. O par (Z,+) é um grupo, enquanto o par (N,+) não o é.

Assim, um grupo é um par (conjunto, operação).

Mesmo assim, muitas vezes nesse livro faremos referência ao grupo G, omitindo a operação *. Isso somente acontecerá quando não houver perigo de confusão.

Se além das propriedades G1, G2 e G3 a operação * possuir a propriedade comutativa, dizemos que (G,*) é um grupo abeliano[1] ou comutativo. Temos, portanto, a definição que segue.

Definição. Um grupo abeliano ou comutativo é um grupo (G,*) cuja operação goza da propriedade G4, a seguir

G4: * é comutativa

$$\forall\ a, b \in G,\ a*b = b*a$$

Exemplo 01. O exemplo mais simples de grupo é o par (Z,+) em que Z é o conjunto dos números inteiros e + é a operação de adição de números inteiros. Esse grupo é abeliano.

Exemplo 02. Também são grupos abelianos com a adição os pares (Q,+) e (R,+), em que Q e R são os conjuntos dos números racionais e dos números reais, respectivamente.

Exemplo 03. O conjunto dos números inteiros pares com a operação de adição de números inteiros é um grupo abeliano.

Exemplo 04. O conjunto das matrizes 3X2, com entradas inteiras munido da operação de adição de matrizes[2], definida posição a posição, é um grupo abeliano.

Exemplo 05. Na realidade, é um grupo abeliano o conjunto das matrizes do tipo m×n com entradas reais munido da operação de adição de matrizes.

[1] O nome abeliano é em homenagem ao matemático norueguês Niels Henrik Abel (1802-1829).

[2] Se $A = (a_{ij})_{mXn}$ e $B = (b_{ij})_{mXn}$, então $A + B = (a_{ij} + b_{ij})_{mXn}$.

Exemplo 06. Denotando por Zn[x] o conjunto formado pelo polinômio nulo e todos os polinômios de grau menor do que ou igual a n, temos que o par (Zn[x],⊗), em que ⊗ é a adição de polinômios, é um grupo abeliano.

Exemplo 07. Seja Z6 = {0, 1, 2, 3, 4, 5} o conjunto dos restos possíveis da divisão euclidiana de números inteiros, por 6. Como vimos no capítulo anterior, a tabela abaixo define uma operação em Z6, chamada de adição módulo 6 e que será indicada por +.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Vimos que essa operação é associativa e comutativa. Podemos perceber também que 0 é o elemento neutro dessa operação, uma vez que 0 + x = x (primeira linha de resultados) e x + 0 = x (primeira coluna de resultados), qualquer que seja o elemento x de Z_6. Observe ainda que cada elemento de Z_6 possui um simétrico para a operação *: 0' = 0, 1' = 5, 2' = 4, 3' = 3, 4' = 2 e 5' = 1. Assim, o par (Z_6,+) é um grupo abeliano.

Exemplo 2.08.De maneira semelhante ao que foi feito no exemplo anterior, para cada inteiro m, m > 1, o par (Zm,+) em que Zm é o conjunto Zm = {0, 1, 2, 3, 4,..., m-1} dos restos da divisão euclidiana por m e + é a adição módulo m é um grupo abeliano. Com isso, temos infinitos exemplos de grupos abelianos.

Grupos não abelianos

Todos os exemplos listados anteriormente foram de grupos abelianos, o que faz com que nos questionemos onde encontrar grupos não abelianos, se é que eles existem.

Vamos agora apresentar dois exemplos de grupos não abelianos.

Exemplo 2.09.O conjunto M2[R], das matrizes 2X2, invertíveis e com entradas reais, munido da multiplicação de matrizes é um grupo não abeliano, ou seja, o par (M_2[R],⊗), em que ⊗ é a multiplicação de matrizes, é um grupo não abeliano.

Inicialmente mostraremos o produto de matrizes 2X2 é uma operação associativa no conjunto de todas as matrizes 2X2.

Dadas as matrizes $A = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$, $B = \begin{bmatrix} e & g \\ f & h \end{bmatrix}$ e $C = \begin{bmatrix} k & n \\ m & o \end{bmatrix}$, temos que:

i) $A \otimes B = \begin{bmatrix} ae + cf & ag + ch \\ be + df & bg + dh \end{bmatrix}$;

ii) $(A \otimes B) \otimes C = \begin{bmatrix} (ae + cf)k + (ag + ch)m & (ae + cf)n + (ag + ch)o \\ (be + df)k + (bg + dh)m & (be + df)n + (bg + dh)o \end{bmatrix}$

$(A \otimes B) \otimes C = \begin{bmatrix} aek + cfk + agm + chm & aen + cfn + ago + cho \\ bek + dfk + bgm + dhm & ben + dfn + bgo + dho \end{bmatrix}$;

iii) $B \otimes C = \begin{bmatrix} ek + gm & en + go \\ fk + hm & fn + ho \end{bmatrix}$;

iv) $A \otimes (B \otimes C) = \begin{bmatrix} (ek + gm)a + (fk + hm)c & (en + go)a + (fn + ho)c \\ (ek + gm)b + (fk + hm)d & (en + go)b + (fn + ho)d \end{bmatrix}$

$A \otimes (B \otimes C) = \begin{bmatrix} aek + agm + cfk + chm & aen + ago + cfn + cho \\ bek + bgm + dfk + dhm & ben + bgo + dfn + dho \end{bmatrix}$.

Assim, o produto de matrizes 2X2 é uma operação associativa. Mostraremos agora que o produto de matrizes 2X2 é uma operação no conjunto M2[R] das matrizes invertíveis de ordem 2, ou seja, mostraremos que o produto de duas matrizes invertíveis de ordem 2 é uma matriz invertível de ordem 2. Na realidade, já sabemos que o produto de duas matrizes quadradas de ordem 2 é uma matriz quadrada de ordem 2. Assim, só precisamos mostrar que o produto de duas matrizes invertíveis é uma matriz invertível.

Sejam A e B matrizes invertíveis, com inversas A-1 e B-1.

A inversa da matriz A⊗B é a matriz B-1⊗A-1.

De fato, temos que

i) (A⊗B)⊗(B-1⊗A-1) = A⊗(B⊗B-1)⊗A-1 = A⊗(I)⊗A-1 = A⊗A-1 = I;

ii) (B-1⊗A-1)⊗(A⊗B) = B-1⊗(A-1⊗A)⊗B = B-1⊗(I)⊗B = B-1⊗B = I.

Assim, a operação de multiplicação de matrizes, restrita a M2[R] é uma operação associativa, com elemento neutro e tal que todo elemento é invertível. Em outras palavras, $(M_2[R], \otimes)$ é um grupo.

Observe que, se $A = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$, temos que:

i) $A \otimes B = \begin{bmatrix} 0 & 1 \\ 3 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 3 & 0 \end{bmatrix}$;

ii) $B \otimes A = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \otimes \begin{bmatrix} 2 & 3 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 7 & 6 \end{bmatrix}$.

E, portanto, $A \otimes B \neq B \otimes A$ e $(M_2[R], \otimes)$ é um grupo não abeliano.

Exemplo 2.10.Seja G o conjunto de todas as funções $f: R \to R$, dadas por $f(x) = ax+b$, com $a,b \in R$ e $a \neq 0$. Geometricamente, G é o conjunto de todas as retas do plano cartesiano R^2, com coeficiente angular não nulo, ou seja, das retas que não são verticais em relação aos eixos coordenados. O par (G,o), em que o é a operação de composição de funções, é um grupo não abeliano.

Observe inicialmente que, se f e g são funções em G, então fog também é uma função de G e, portanto, a operação o é uma operação em G. De fato, dados $f: R \to R$ e $g: R \to R$ elementos de G, então existem números reais a, b, c e d, com a e c não nulos, tais que $f(x) = ax+b$ e $g(x) = cx+d$. Assim, a função $fog: R \to R$ é dada por $(fog)(x) = f(g(x)) = f(cx+d) = a(cx+d)+b = acx+ adb$ e pertence a G, uma vez que ac 0.

O elemento neutro de (G,*) é a função identidade $id: R \to R$, dada por $id(x) = x$.

De fato, se $f: R \to R$ é um elemento de G, dado por $f(x) = ax+b$, então $(idof)(x) = id(f(x)) = id(ax+b) = ax+b = f(x)$; por outro lado, $(foid)(x) = f(id(x)) = f(x)$.

O simétrico da função $f: R \to R$ de G, dada por $f(x) = ax+b$ é a função $f^{-1}: R \to R$ de G, dada por $f^{-1}(x) = x -$.

De fato, temos que:

- $(f^{-1}of)(x) = f^{-1}(f(x)) = f^{-1}(ax+b) = \frac{1}{a}(ax+b) - \frac{b}{a} = x + \frac{b}{a} - \frac{b}{a} = x = id(x)$; e
- $(fof^{-1})(x) = f(f^{-1}(x)) = f(\frac{1}{a}x - \frac{b}{a}) = a(\frac{1}{a}x - \frac{b}{a}) + b = x - b + b = x = id(x)$.

Mostrando que o par (G,o) é um grupo.

Para mostrar que (G,o) não é abeliano, basta considerarmos as funções de G, dadas por $f(x) = 2x$ e $g(x) = x+5$. Temos que:

- $(fog)(x) = f(g(x)) = f(x+5) = 2(x+5) = 2x+10$; e
- $(gof)(x) = g(f(x)) = g(2x) = 2x+5$.

Logo o grupo (G,o) não é abeliano.

2. Propriedades elementares

Os grupos (G,*) possuem certas propriedades que serão enunciadas e provadas a seguir, na forma de proposição.

Proposição 01. Unicidade do elemento neutro

O elemento neutro de um grupo (G,*) é único.

Prova

Sejam e_1 e e_2 elementos neutros de um grupo (G,*).

Sendo e_1 elemento neutro, temos que $e_1*e_2 = e_2$. E sendo e_2 elemento neutro, temos $e_1*e_2 = e_1$. Das igualdades anteriores, temos que $e_1 = e_2$ e, portanto, o elemento neutro de um grupo é único.

Proposição 02. Unicidade do elemento simétrico

O elemento simétrico de um elemento g de um grupo (G,*) é único.

Prova

Sejam (G,*) um grupo, e o elemento neutro de (G,*), g um elemento de G e g_1 e g_2 elementos simétricos de g.

Sendo g_1 simétrico de g, temos que $g_1*g = e$. Sendo g_2 simétrico de g, temos que $g*g_2 = e$.

Assim, $g_1 = g_1*e = g_1*(g*g_2) = (g_1*g)*g_2 = e*g_2 = g_2$ e, portanto, o simétrico de g é único.

Dessa proposição e do fato que se e é o elemento neutro de um grupo (G,*), então e*e = e, concluímos que o simétrico do elemento neutro de um grupo (G,*) é o próprio elemento neutro, isto é, e' = e.

Proposição 03. Lei do cancelamento

Se a, b e c são elementos de um grupo (G,*), tais que a*b = a*c, então b = c.

Prova

Como todos os elementos de um grupo (G,*) são simetrizáveis, existe a' em G tal que a'*a = e, em que e é o elemento neutro de (G,*).

Operando à esquerda ambos os membros da igualdade a*b = a*c com a', teremos a'*(a*b) = a'*(a*c). Usando a associatividade e o fato de a' ser o simétrico de a, teremos (a'*a)*b = (a'*a)*c, ou ainda, b = c. Provando o resultado.

Proposição 04. Existência e unicidade da solução de equações

Sejam a e b elementos de um grupo (G,*).

(i) A equação a*X = b tem solução e esta é única.

(ii) A equação X*a = b tem solução e esta é única.

Prova

Consideremos a equação a*X = b no grupo (G,*).

Como todo elemento de G é simetrizável, temos que existe a' $\in$ G, simétrico de a. Assim, operando à esquerda ambos os membros da igualdade com a', teremos

a*X = b a'*(a*X) = a'*b (a'*a)*X = a'*b e*X = a'*b

X = a'*b,

que é a única solução da equação, pois se u e v fossem soluções de a*X = b, teríamos a*u = b e a*v = b e, consequentemente, teríamos a*u = a*v. Operando à esquerda ambos os membros da igualdade por a', o simétrico de a, teremos

a'*(a*u) = a'*(a*v) (a'*a)*u = (a'*a)*v e*u = e*v

u = v.

Para a equação X*a = b, o processo é totalmente semelhante ao que fizemos e será deixado como exercício.

Proposição 05. O simétrico do simétrico

Sejam (G,*) um grupo, a um elemento de G e a' o seu simétrico. Temos que (a')' = a.

Prova

Por definição, o simétrico de um elemento g de um grupo (G,*) é o elemento g' tal que g*g' = g'*g = e, em que e é o elemento neutro de (G,*).

Fazendo a' = g, como a'*a = a*a' = e, temos g*a = a*g = e. Portanto a é o simétrico de g, ou melhor, a é o simétrico de a'. Em símbolos, (a')' = a. Como queríamos demonstrar.

Proposição 06. O simétrico do composto

Sejam (G,*) um grupo e a e b elementos de G. O simétrico de a*b é b'*a', ou melhor, (a*b)' = b'*a'.

Prova

Por definição, devemos mostrar que, se e é o elemento neutro de (G,*), então (b'*a')*(a*b) = (a*b)*(b'*a') = e.

Temos que

(i) (b'*a')*(a*b) = b'*(a'*a)*b = b'*(e)*b = (b'*e)*b = b'*b = e;

(ii) (a*b)*(b'*a') = a*(b*b')*a' = a*(e)*a' = (a*e)*a' = a*a' = e. O que mostra que (a*b)' = b'*a'.

Proposição 07. O elemento idempotente

Em um grupo (G,*), se x $\in$ G é tal que x*x = x, então x = e.

Prova

Sabemos que x = x*e. Assim, a igualdade x*x = x nos fornece a igualdade x*x = x*e. Pela lei do cancelamento, temos que x = e. Provando o resultado.

3. Grupos finitos com 1, 2 ou 3 elementos

Na definição de grupos, foi exigido que o conjunto G seja um conjunto não vazio. Assim G deve ter pelo menos um elemento. Nos vários exemplos estudados, vimos que em um grupo (G,*) o conjunto G pode ser finito ou infinito. Isto nos leva às seguintes definições.

Definição. Dizemos que um grupo (G,*) é um grupo finito se o conjunto G for um conjunto finito. Caso contrário, isto é, se o conjunto G for infinito, dizemos que o grupo (G,*) é um grupo infinito.

Definição. Dizemos que o grupo (G,*) é um grupo finito de ordem n, se o conjunto G possui n elementos.

Assim, a ordem de um grupo finito (G,*) é a cardinalidade, ou o número de elementos, do conjunto G.

Escrevemos |G| ou o(G), que se lê: ordem de G, para indicar a ordem do grupo (G,*). Assim, se o grupo (G,*) é finito e G possui n elementos, escrevemos |G| = n ou o(G) = n. Se o grupo (G,*) for infinito, escrevemos |G| = ∞ ou o(G) = ∞.

Grupos de ordem 1

Seja G = { a } um conjunto com um elemento.

A única operação possível de ser definida em G é a operação * tal que a*a = a.

Com essa operação em G, o par (G,*) é um grupo de ordem 1. De fato,

- a operação * é associativa, pois a*(a*a) = (a*a)*a = a (o único resultado possível);
- (G,*) possui elemento neutro, que é o próprio a;
- e todo elemento de (G,*), que é somente o a, possui simétrico; no caso, o próprio a.

Assim, a menos da natureza do elemento de G, existe um único grupo finito de ordem 1, ou melhor, existe uma única estrutura possível para um grupo de ordem 1.

Grupos de ordem 2

*	e	a
e	e	a
a	a	

Seja G = {e, a} um conjunto com dois elementos.

Vamos tentar definir uma operação * em G tal que o par (G,*) seja um grupo.

Como um grupo deve ter um elemento neutro, vamos escolher e para ser o elemento neutro de (G,*).

Assim, já temos que e*e = e, e*a = a e a*e = a, faltando determinar apenas o valor de a*a.

Como * deve ser uma operação em G, devemos ter a*a = e ou

a*a = a.

*	e	a
e	e	a
a	a	e

Observemos que a igualdade a*a = a não é possível, uma vez que, sendo a = a*e, teríamos a igualdade a*a = a*e e, pela lei do cancelamento (proposição 03, anterior), teríamos a = e. Assim, o conjunto G teria um único elemento.

Logo, só podemos ter a*a = e, completando a tabela.

Notemos que:

(i) * é uma operação em G;

(ii) e é o elemento neutro de G para a operação *; e

(iii) todo elemento de G é simetrizável: cada elemento é seu próprio simétrico.

Portanto, para que (G,*) seja um grupo, devemos mostrar que * é associativa. Para tanto, observemos os dezesseis resultados a seguir:

1) e*(e*e) = e*e = e
(e*e)*e = e*e =e

2) e*(e*a) = e*a = a
(e*e)*a = e*a = a

3) e*(a*e) = e*a = a
(e*a)*e = a*e = a

4) e*(a*a) = e*e = e
(e*a)*a = a*a = e

5) a*(e*e) = a*e = a
(a*e)*e = a*e = a

6) a*(e*a) = a*a = e
(a*e)*a = a*a = e

7) a*(a*e) = a*a = e
(a*a)*e = e*e = e

8) a*(a*a) = a*e = a
(a*a)*a = e*a = a

Assim, novamente, a menos da natureza dos elementos de G, existe uma única estrutura possível para um grupo de ordem 2, que pode ser resumida como segue:

(i) um dos elementos é o elemento neutro; e

(ii) o outro elemento é seu próprio inverso.

Grupos de ordem 3

*	e	a	b
e	e	a	b
a	a		
b	b		

Seja G = {e, a, b} um conjunto com três elementos.

Como nos casos anteriores, vamos tentar definir uma operação * em G, tal que o par (G,*) seja um grupo.

Inicialmente, escolheremos e para ser o elemento neutro de (G,*) e, portanto, já temos os cinco resultados: e*e = e, e*a = a*e = a, e e*b = b*e = b

Vamos encontrar um a um os outros resultados da tabela, iniciando com a*b.

Existem 3 possíveis valores para a*b, quais sejam: e, a, b.

Observe que não podemos ter a*b =a, pois neste caso teríamos

a*b = a*e, que nos daria b = e; o que é absurdo.

Também não podemos ter a*b = b, pois neste caso deveríamos ter a = e, o que também seria absurdo.

Assim, só podemos ter a*b = e, preenchendo mais uma lacuna na tabela.

*	e	a	b
e	e	a	b
a	a		e
b	b	e	

De maneira semelhante, devemos ter b*a = e.

Preenchendo mais uma lacuna.

Para determinarmos o valor de a*a, basta observarmos que esse valor não pode ser a, pois teríamos a = e, nem pode ser e, em virtude da igualdade b*a = e, que forçaria a igualdade a = b, que não ocorre. Assim, devemos ter a*a = b.

Por argumentos semelhantes, chegamos à conclusão que b*b = a, completando definitivamente a tabela.

Novamente, temos que:

(i) * é uma operação em G;

(ii) e é o elemento neutro de G para a operação *; e

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(iii) todo elemento de G é simetrizável: o simétrico de e é o próprio e, o simétrico do a é o b, e o simétrico do b é o a.

Portanto, para que (G,*) seja um grupo, devemos mostrar que * é associativa. Essa prova será deixada como exercício.

Assim, concluímos que a menos da natureza dos elementos de G, existe uma única estrutura possível para um grupo de ordem 3, que pode ser resumida como segue:

(i) um dos elementos é o elemento neutro; e

(ii) dos dois elementos restantes, um é o simétrico do outro.

Grupos de ordem maior do que 3

Vimos que, a menos da natureza dos elementos do conjunto G, existe apenas uma estrutura para os grupos de ordem 1, 2 ou 3.

Nessa expressão "existe apenas uma estrutura" está embutida a ideia de **isomorfismo** que será estudada posteriormente.

No caso de ordem 4, mostraremos que existem apenas duas estruturas: a do Z_4 e a do grupo de Klein; o mesmo ocorrendo no caso de ordem 6: a do Z_6 e a do grupo das permutações de 3 elementos. Para o caso da ordem 5, existe apenas uma estrutura que é a do Z_5.

Na realidade, mostraremos que para cada número primo positivo p, existe apenas uma estrutura de grupos que é a do Zp.

Síntese do Capítulo

Leituras, filmes e sites

Leopoldo Nachbin, p.48.

Os grupos tiveram a sua origem na teoria das substituições devida, em parte, aos trabalhos de Lagrange. O verdadeiro iniciador deste capítulo da Álgebra, no entanto, foi Galois. O desenvolvimento da teoria dos grupos era, então, condicionado por suas aplicações à teoria das equações algébricas. Mais tarde, os trabalhos de Sophus Lie mostraram a importância dos grupos em certos aspectos das equações diferenciais, abrindo caminho para a teoria dos chamados grupos de Lie; e as ideias de Felix Klein sobre a conveniência de se considerar a geometria como o estudo de propriedades invariantes por grupos de transformações determinadas vieram ampliar o campo de atuação do conceito de grupo. Em sua forma axiomática, esta envolve dois aspectos: os grupos aditivos e os multiplicativos. Os primeiros... constituem, a menos da notação, um caso particular dos segundos.

Cleiton Batista Vasconcelos

Outra caracterização para um grupo (G,*)

Seja (G,*) um conjunto G munido de uma operação.

É possível que tenhamos e*x, para todo elemento x de G, mas que exista algum x, $x \in G$, tal que $x*e \neq x$. Assim, de acordo com nossa definição, esse elemento e não é elemento neutro. De maneira semelhante, é possível que tenhamos x*e = x, para todo elemento x em G, mas não se tenha e*x = x, para algum x, $x \in G$.

E, novamente, e não pode ser elemento neutro, conforme nossa definição anterior.

Tabela 1

*	e	a	b	c
e	e	a	b	c
a	a	b	e	a
b	c	b	e	a
c	b	c	a	b

Tabela 2

&	e	a	b	c
e	e	b	c	e
a	a	c	e	b
b	b	b	e	a
c	c	c	a	b

As tabelas 1 e 2 das operações * e &, anteriores, exemplificam o que foi mencionado aqui.

De fato, para a operação * da tabela 1, temos que e*e = e, e*a = a, e*b = b e e*c = c, mas, por exemplo, b*e = c. Assim, e é elemento neutro pela esquerda, mas não é elemento neutro pela direita; enquanto para a operação &, temos que e&e = e, a&e = a, b&e = b e c&e = c, e e&a = b, o que mostra que e é elemento neutro pela esquerda, mas não é elemento neutro pela direita.

O que vimos anteriormente pode ser consolidado nas seguintes definições.

Elemento neutro à direita

*	e	a	b	c
e	e			
a	a			
b	b			
c	c			

Definição. Dizemos que um elemento e de um conjunto G munido de uma operação * é elemento neutro à esquerda para essa operação, se e*a = a, qualquer que seja o elemento a, a $\in$ G.

Definição. Dizemos que um elemento e de um conjunto G munido de uma operação * é elemento neutro à direita para essa operação, se a*e = a, qualquer que seja o elemento a, a $\in$ G.

Elemento neutro à esquerda

*	e	a	b	c
e	e	a	b	c
a				
b				
c				

Assim, na definição de grupo, o elemento neutro é elemento neutro à direita e à esquerda, simultaneamente.

De maneira semelhante, em um conjunto G munido de uma operação *, dado um elemento a, a$\in$G, podemos definir simétrico à direita de a e simétrico à esquerda de a, conforme percebemos a seguir. Mas, antes, é bom mencionarmos que nas definições de elemento simétrico à esquerda e de elemento simétrico à direita faremos referência a um elemento neutro. Esse elemento neutro pode ser somente à esquerda, somente à direita, ou ambos: à esquerda e à direita.

Definição. Em um conjunto não vazio G munido de uma operação *, com elemento neutro e, um elemento a, a$\in$G, é dito simetrizável à esquerda se existe a' em G, tal que a'*a = e. O elemento a' é dito simétrico à esquerda de a para a operação *.

Definição. Em um conjunto não vazio G munido de uma operação *, com elemento neutro e, um elemento a, a$\in$G, é dito simetrizável à esquerda

se existe a' em G, tal que a'*a = e. O elemento a' é dito simétrico à esquerda de a para a operação *.

Nosso objetivo nesse texto é dar uma definição aparentemente "mais fraca" de grupo na qual o elemento neutro e o simétrico de cada elemento serão substituídos por elemento neutro à esquerda e elemento simétrico à esquerda ou elemento neutro à direita e elemento simétrico à direita.

Veremos que essa definição não tem nada de mais fraca, sendo, na realidade, equivalente à anterior.

Definição. Um grupo é um par (G,*) em que G é um conjunto não vazio e * é uma operação em G, gozando das seguintes propriedades:

G1': * é associativa;

G2': existe $e \in G$, tal que $e*a = a$, $\forall a \in G$;

G3': dado $a \in G$, existe $a' \in G$, tal que $a'*a = e$.

Mostraremos que esta definição é equivalente à anterior, provando que esse elemento neutro à esquerda e o simétrico à esquerda serão obrigatoriamente elemento neutro à direita e simétrico à direita, respectivamente.

O elemento neutro à esquerda é, também, elemento neutro à direita

Denotemos por e esse elemento neutro à esquerda, por a um elemento qualquer de G e por a' o simétrico à esquerda de a. Queremos mostrar que a*e = a.

Fazendo a*e = u, temos

- $a*e = u \Rightarrow a'*(a*e) = a'*u \Rightarrow (a'*a)*e = a'*u \Rightarrow e*e = a'*u$

De onde se conclui que a'*u = e, e como a'*a = e, temos a'*u = a'*a.

Como todo elemento de G possui simétrico pela esquerda e como a' é elemento de G, temos que a' possui simétrico pela esquerda, digamos, a''.

Assim, temos as seguintes igualdades:

- a'*u = a'*a

a''*(a'*u) = a''*(a'*a) (a''*a')*u = (a''*a')*a e*u = e*a

Portanto, a*e = a, provando que e, o elemento neutro pela esquerda, é, também, elemento neutro pela direita.

O elemento simétrico pela esquerda é, também, elemento simétrico pela direita

Denotemos por e o elemento neutro pela esquerda (o qual já foi demonstrado ser elemento neutro pela direita), por a um elemento qualquer de G e por a' o simétrico à esquerda de a.

Queremos mostrar que a' também é elemento simétrico de a pela direita, isto é, queremos mostrar que a*a' = e.

Fazendo a*a' = u, temos que

• a*a' = u ⇒ a'*(a*a') = a'*u ⇒ (a'*a)*a' = a'*u ⇒ e*a' = a'*u

De onde se conclui que a'*u = a' e, consequentemente, a'*u = a'*e.

Como todo elemento de G possui elemento simétrico pela esquerda, denotando por a'' o simétrico de a', temos que:

• a'*u = a'*e

a''*(a'*u) = a''*(a'*e)

(a''*a')*u = (a''*a')*e

e*u = e*e

u = e.

Assim, a*a'= a'*a = e, provando que o simétrico pela esquerda é também simétrico pela direita.

Logo, essa definição "mais fraca" de grupo é equivalente à definição anterior.

Exercícios resolvidos

1. O par (Q+,*), em que Q+ é o conjunto de todos os números racionais positivos e * é a operação em Q+ definida por a*b = , é um grupo abeliano.

De fato, observemos inicialmente que * é uma operação em Q+ uma vez que o produto de dois números racionais positivos sempre existe e que o quociente entre esse produto e 2 é um número racional positivo univocamente determinado. Vamos agora determinar o elemento neutro de Q+ para a operação.

Denotando por u esse elemento, devemos ter a*u = = a e u*a = = a, para cada elemento a de Q+. As duas igualdades

somente serão possíveis se a = 0 ou se u = 2. Como a ∈ Q+ e, portanto, a 0, devemos ter u = 2. Assim, 2 é o elemento neutro de (Q+,*). Vamos mostrar agora que todo elemento de Q+ é simetrizável para a operação *. Dado a ∈ Q+, denotemos por a' o simétrico de a. Assim, devemos ter a*a' = a'*a = 2, ou seja, = 2. Dessa última igualdade, como a 0, temos

a' = . Com isso mostramos que (Q+,*) é um grupo. E desde que a multiplicação de números racionais é comutativa, o grupo (Q+,*) é abeliano.

2. Definindo no conjunto Z×Z, de todos os pares ordenados de números inteiros, a operação de adição de pares ordenados por: $(a,b)\otimes(c,d) = (a+c,b+d)$, em que a adição dentro dos parêntesis é a adição de números inteiros, o par $(Z\times Z,\otimes)$ é um grupo abeliano.

   De fato,

3. O conjunto R dos números reais munido da operação * dada por $a*b = a + b - 3$ é um grupo abeliano.

Inicialmente devemos mostrar que * é realmente uma operação binária em R, ou seja, que * pode ser aplicada a quaisquer dois elementos de R, que o composto a*b de quaisquer dois elementos a e b de R é um elemento de R e que é univocamente determinado por a e b. Isso de fato ocorre, pois dados dois elementos a e b de R sua soma a+b existe e está em R; e se subtrairmos 3 unidades de a+b, o resultado ainda está em R. Além disso, o número a+b-3 é univocamente determinado por a e b. Assim, * é uma operação em R, mostrando a primeira parte.

Observemos agora que * é uma operação associativa, pois

- $a*(b*c) = a*(b+c-3) = a + (b+c-3) - 3 = a+b+c-6$; e
- $(a*b)*c = (a+b-3)*c = (a+b-3) + c - 3 = a+b+c-6$.

O elemento neutro de (R,*), se existir, deve ser um elemento u, $u\in R$, tal que $a*u = u*a = a$, $\forall a\in R$. Assim, de $a*u = a$, temos $a+u-3 = a$, o que nos dá $u = 3$; e de $u*a = a$, temos $u+a-3 = a$, o que nos dá, também, $u = 3$. Assim, se (R,*) tiver elemento neutro, esse deve ser o 3.

Para concluirmos que 3 é o elemento neutro de (R,*), basta observarmos que:

(i) $3\in R$;

(ii) $3*a = 3+a-3 = a$;

(iii) $a*3 = a+3-3 = a$.

Portanto, 3 é o elemento neutro de (R,*).

Para concluirmos que (R,*) é um grupo, basta mostrarmos que todo elemento de R é simetrizável para a operação *. Assim, dado $a\in R$, para que a seja simetrizável, devemos ter:

(i) $a*a' = 3 \Rightarrow a+a'-3 = 3 \Rightarrow a' = 6 - a$;

(ii) $a'*a = 3 \Rightarrow a'+a-3 = 3 \Rightarrow a' = 6 - a$.

Assim, se o número real a for simetrizável para a operação *, devemos ter $a' = 6 - a$.

Para concluirmos que todo elemento a de R é simetrizável para a operação *, basta observarmos que:

(i) $6-a\in R$;

(ii) a*(6-a) = a+(6-a)-3 = 3;

(iii) (6-a)*a=(6-a)+a-3=3.

Portanto todo elemento a de (R,*) é simetrizável e seu simétrico é 6-a.

Do que foi feito, concluímos que (R,*) é um grupo.

Finalmente, basta mostrarmos que (R,*) é abeliano, ou seja, que * é comutativa. Para tanto, observemos que, dados os números reais a e b, temos que a*b = a+b-3 = b+a-3 = b*a, uma vez que a adição de números reais é comutativa.

Logo (R,*) é um grupo abeliano.

Atividades de avaliação

1. O conjunto M_{3X2} das matrizes 3X2, com entradas inteiras munido da operação de adição de matrizes, definida posição a posição, é um grupo abeliano. Determine seu elemento neutro e o simétrico de um elemento genérico de M_{3X2}.
2. Denotando por $Z_n[x]$ o conjunto formado pelo polinômio nulo e todos os polinômios de grau menor do que ou igual a n, temos que o par $(Zn[x],\rightarrow)$, em que • é a adição de polinômios, é um grupo abeliano. Determine seu elemento neutro e o simétrico de um elemento genérico de Zn[x].
3. Seja Z_4 = {0, 1, 2, 3} o conjunto dos restos possíveis da divisão euclidiana de números inteiros, por 4. Como vimos, Z4 munido da adição módulo 4 é um grupo abeliano. Construa a tabela da adição módulo 4 e determine o elemento neutro do grupo e o simétrico de cada elemento de $(Z_4,+)$.
4. Sejam a e b elementos de um grupo (G,*). Mostre que a equação X*a = b tem solução e esta é única.
5. Sejam a, b e c elementos de um grupo (G,*). Mostre que (a*b'*c)' = c'*b*a'.
6. Seja G = {e, a, b} um conjunto com três elementos. Defina em G a operação * dada pela tabela ao lado. Mostre que * é associativa determinando os 54 resultados necessários.

Referências

DOMINGUES, H. H. Álgebra moderna. Atual: São Paulo, 2003

FRALEIGH, J.B. A first course in abstract algebra. Addison-Wesley: Japão, 1968

GONÇALVES, Adilson. Introdução à álgebra. Projeto Euclides. IMPA: Rio de Janeiro, 1979.

JACOBSON, N. Basic algebra. W. H. Freeman Company: San Francisco--USA, 1974.

MONTEIRO, L. H. J. Iniciação às estruturas algébricas. Série Professor No 6. Nobel: São Paulo, 1979.

NACHBIN, Leopoldo. Introdução à álgebra. McGraw-Hill do Brasil Ltda/Editora da UNB: Rio de Janeiro, 1971.

SIMIS, Aron. Introdução à álgebra. Monografias de Matemática 23. IMPA: Rio de Janeiro, 1977.

Capítulo 3

Alguns exemplos importantes

Objetivo

- Neste capítulo, apresentaremos alguns exemplos importantes de grupos. Iniciamos com a retomada do grupo dos restos módulo m; em seguida trabalhamos os grupos simétricos Sn; para finalizarmos com os grupos diedrais, ou grupos das rotações dos polígonos regulares, Dn. representação geométrica dos grupos Dn.

Introdução

Alguns grupos merecem destaque especial por serem de fundamental importância para a teoria dos grupos ou por apresentarem propriedades que os diferenciam dos demais.

Dentre esses grupos destacamos o grupo dos restos módulo m, o Z_m já estudado anteriormente, os grupos simétricos Sn ou grupo das permutações de n elementos; e o n-grupo diedral Dn ou grupo das rotações dos polígonos regulares de n lados.

Esses grupos serão apresentados e ou retomados de forma bem detalhada nesse capítulo.

O grupo dos restos módulo m

Para cada inteiro m, m> 1, por grupo de restos módulo m entendemos o grupo $(Z_m,\oplus)$, em que Zm é o conjunto cujos elementos são 0, 1, 2, 3,..., m-1 e a operação $\oplus$ é definida como segue:

"Dados a, b $\in$ G, a$\oplus$b é o resto da divisão de a+b (adição em Z) por m".

Assim, Z6, por exemplo, é o conjunto Z6 = {0, 1, 2, 3, 4, 5} e, de acordo com a definição da operação $\oplus$, teremos:

- $3\oplus4=(7)6=1$;
- $5\oplus4=(9)6=3$;
- $2\oplus3=(5)6=5$;

em que os símbolos $(x)_6$ significam, para cada x, o resto da divisão de x por 6; Z5 é o conjunto Z5 ={0,1,2,3,4} e a operação $\oplus$ étal que:

- $3 \oplus 4 = (7)5 = 2$;
- $5 \oplus 2 = (7)5 = 3$;
- $2 \oplus 3 = (5)6 = 0$;

e, neste caso, o símbolo $(x)5$ representa o resto da divisão de x por 5.

As tabelas a seguir definem as operações em Z_5 e Z_6. $(Z5, \oplus)$ $(Z6, \oplus)$

$(Z_5, \oplus)$

⊕	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(Z_6, \oplus)$

⊕	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Definida como resto da divisão de uma adição em Z, por m, $\oplus$, que será chamada de adição módulo m ou simplesmente adição, é obviamente uma operação em Zm. De fato,

(1) A adição $\oplus$ é fechada em Zm, pois 0, 1, 2, 3, ..., m-1 são os únicos restos possíveis na divisão por m. Assim, quando adicionamos dois elementos de Zm, o resultado se encontra em Zm.

(2) Dados quaisquer dois elementos de Zm, digamos a e b, sempre é possível calcular $a \oplus b$.

e, além disso,

(3) O resultado da adição de a com b, $a \oplus b$, é único, uma vez que o resto da divisão de a+b por m é único.

Para mostrarmos que o par $(Zm, \oplus)$ é realmente um grupo, devemos mostrar que:

(1) A operação $\oplus$ é associativa;

(2) Em $(Zm, \oplus)$ temos elemento neutro;

(3) Todo elemento de Zm é simetrizável para a operação $\oplus$.

Observemos inicialmente que 0 é o elemento neutro de $(Zm, \oplus)$, pois se a é elemento de Zm, então

(i) $0 \oplus a = (0+a)m = (a)m = a$;

(ii) $a \oplus 0 = (a+0)m = (a)m = a$.

Observemos ainda que, se $a \in Zm$, então $0 \leq a \leq m-1$ e, consequentemente, $1 \leq m-a \leq m$.

- Se $1 \leq m\text{-}a < m$, então $m\text{-}a \leq Zm$ e
- $(m\text{-}a)\oplus a = (m–a+a)m = (m)m = 0$;
- $a\oplus(m\text{-}a) = (a+m\text{-}a)m = (m)m = 0$.

Consequentemente, m-a é o simétrico de a.

- Se m-a = m, então a = 0 e o simétrico de 0 é 0.

Assim, se $a\in Z_m$, então ou a = 0 e é seu próprio simétrico ou $a \neq 0$ e seu simétrico é m-a. Em qualquer caso, se $a\in Z_m$, então a é simetrizável para a operação $\oplus$.

Para mostrarmos que $(Z_m,\oplus)$ é um grupo, basta mostramos que $\neq$ é associativa. Essa demonstração será deixada para você fazer, como exercício.

Exercício 3.1. Mostre que a operação $\oplus$, definida anteriormente, é associativa.

Exercício 3.2. Mostre que a operação $\oplus$, definida anteriormente, é comutativa.

Os exercícios 3.1 e 3.2 anteriores, juntamente com o que já havia sido feito, nos permitem afirmar que o par $(Z_m, \oplus)$ é um grupo abeliano (comutativo), qualquer que seja o inteiro m, com m > 1.

Exercício 3.3. Considere o grupo $(Z_m, \oplus)$, em que m = 6. Mostre que é possível obter todos os elementos de Zm a partir de adições sucessivas do elemento 1. Assim: $1\oplus1$, $1\oplus1\oplus1$, $1\oplus1\oplus1\oplus1$, ... Que outros elementos de Z6 possuem esta propriedade?

Exercício 3.4. Faça o que se pede no exercício 3.3 para os grupos $(Z5, \oplus)$ e $(Z6, \oplus)$.

Exercício 3.5. Mostre que os únicos subconjuntos de $(Z5, \oplus)$ que são fechados para a adição $\oplus$ são {0} e Z5.

Exercício 3.6. Determine todos os subconjuntos de $(Z6, \oplus)$ que são fechados para a adição $\oplus$.

1. Os grupos simétricos ou grupos de permutações

Na teoria dos grupos, uma permutação em um conjunto não vazio A é qualquer bijeção $f: A \rightarrow A$. Se A = {1, 2, 3, ..., n} o conjunto de todas as permutações em A é denotado por Sn.

Munido da operação de composição de funções, o conjunto Sn possui a estrutura de grupo, ou seja, o par (Sn,o), em que 'o' representa a operação de composição de funções, é um grupo: o grupo das permutações de n elementos ou o grupo simétrico de ordem n!.

O grupo (S2,o) das permutações de 2 elementos ou o grupo simétrico de ordem 2

As permutações em A = {1, 2} são as funções f, g: A → A, dadas por f(1) = 1, f(2) = 2 – ou seja, a função identidade – e g(1) = 2 e g(2) = 1. Na teoria dos grupos essas funções são representadas por

f: e g: , em que a linha de cima, ou primeira linha,

representa o domínio e a linha de baixo, ou segunda linha, representa o contradomínio da função; em cada coluna temos o elemento (primeira linha) e sua imagem pela função (segunda linha).

Para determinarmos efetivamente a operação 'o', basta preenchermos a tabela 1 ao lado.

Tabela 1

o	f	g
f		
g		

Como f é a função identidade, temos que a primeira linha e a primeira coluna da tabela devem ser preenchidas como na tabela 2, ao lado.

Tabela 2

o	f	g
f	f	g
g	f	

Por fim, resta calcular a composta de g com, ou seja, a função gog.

Temos que:

- gog(1) = g(g(1)) = g(2) = 1; e
- gog(2) = g(g(2)) = g(1) = 2.

E, assim, gog = f, completando a tabela (tabela 3). Observemos que, mesmo sem calcular efetivamente gog, poderíamos ter completado a tabela, lembrando que em um grupo cuja operação é definida em uma tabela, não podemos ter elementos repetidos nem nas linhas nem nas colunas. Assim, a única maneira possível de completarmos a tabela era com a função f no espaço vazio da tabela 2.

Tabela 3

o	f	g
f	f	g
g	g	f

Grupo simétrico de ordem 2

Exercício 3.7. Justifique porque na tabela da operação de um grupo não podemos ter elementos iguais nem nas linhas nem nas colunas.

Exercício 3.8. Calcule efetivamente, pela definição de função composta, fof, fog, gof e gog.

O grupo (S3,o) das permutações de 3 elementos ou o grupo simétrico de ordem 6

As permutações em A = {1, 2, 3} são em número de 6 e são dadas por: e: , f1: , f2: , g1: , g2: e g3: , em que, novamente, a linha de cima (primeira linha) representa o domínio e a linha de baixo (segunda linha) representa o contradomínio e, além disso, em cada coluna, temos o elemento do domínio (primeira linha) e sua imagem pela função (segunda linha).

O conjunto das seis funções anteriores é denotado por S3 e, portanto, $S3 = \{e, f_1, f_2, g_1, g_2, g_3\}$.

A tabela da operação de composição entre as funções de S3 se encontra a seguir.

o	e	f1	f2	g1	g2	g3
e	e	f1	f2	g1	g2	g3
f1	f1	f2	e	g3	g1	g2
f2	f2	e	f1	g2	g3	g1
g1	g1	g2	g3	e	f1	f2
g2	g2	g3	g1	f2	e	f1
g3	g3	g1	g2	f1	f2	e

Grupo (S3,o)
Grupo simétrico de ordem 3!

Nos quadros a seguir, mostramos como podem ser calculadas algumas composições de permutações do S3. No primeiro quadro, tomamos os elementos 1, 2 e 3 do domínio, aplicamos g1 a cada um deles e, em seguida, ao resultado, aplicamos f1, obtendo a permutação g3; no segundo quadro, aos elementos 1, 2 e 3 do domínio, aplicamos g3 e, em seguida, aos resultados obtidos, aplicamos g2, obtendo a permutação f1.

$$f_1 o g_1: \quad \overset{g1}{1 \longrightarrow 1} \overset{f1}{\longrightarrow 2} \qquad f_1 o g_1: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = g_3$$
$$ \quad 2 \longrightarrow 3 \longrightarrow 1$$
$$ \quad 3 \longrightarrow 2 \longrightarrow 3$$

$$g_2 o g_3: \quad \overset{g3}{1 \longrightarrow 2} \overset{g2}{\longrightarrow 2} \qquad g_2 o g_3: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_1$$
$$ \quad 2 \longrightarrow 1 \longrightarrow 3$$
$$ \quad 3 \longrightarrow 3 \longrightarrow 1$$

Observe que, de acordo com a tabela, e é o elemento neutro de (S3,o) e g1, g2 e g3 são seus próprios simétricos ou inversos: g1'=g1, g2'=g2 e g3'=g3. Além disso, f1'=f2 e, consequentemente, f2'=f1.

A associatividade da operação ‘o’, que sendo aceita até o momento, será provada, de maneira mais geral, na proposição seguinte:

Proposição 3.9. A composição de funções é uma operação associativa.

Prova

Sejam f, g e h funções.

Para os valores de x em que faz sentido falarmos na composição dessas funções, temos que:

- [fo(goh)](x) = f[(goh)(x)] = f[g(h(x))]; e
- [(fog)oh](x) = (fog)(h(x)) = f[g(h(x))]. Provando o resultado.

Observe que (S_2,o) é um grupo comutativo, enquanto (S_3,o) não o é. Na realidade, podemos mostrar que, se n >2, então (Sn,o) é um grupo não abeliano.

Esse resultado será mostrado na próxima seção.

Exercício 3.10. Calcule efetivamente todos os elementos da tabela de (S_3,o).

Exercício 3.11. Escolha três coleções com três elementos de S3, todos diferentes da identidade, e mostre que vale a associatividade, determinando o valor de cada composta.

Exercício 3.12. Analisando a tabela de (S3,o), determine todos os pares de elementos que comutam entre si.

Exercício 3.13. Determine um subconjunto de S3 que seja fechado para a operação de composição em S3 e que possua mais de um elemento. Observe que H = {e} é parte fechada de S3 para a composição de permutações e, além disso, H é um grupo com essa operação.

O grupo (Sn,o) das permutações de n elementos ou o grupo simétrico Sn

Também para n > 3, é possível construir o grupo das permutações (Sn,o). Neste caso, Sn é o conjunto de todas as permutações no conjunto An = {1, 2, 3, ..., n}.

Assim, são elementos de S4, entre outras, as seguintes permutações: ,,;

$$\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}, \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

são elementos de S5, as seguintes permutações:

$$\begin{pmatrix}1&2&3&4&5\\1&2&4&3&5\end{pmatrix}, \begin{pmatrix}1&2&3&4&5\\5&3&1&2&4\end{pmatrix}, \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}, , ,....$$

entre outras.

De maneira geral, o grupo (Sn,o) possui n! elementos e como dissemos anteriormente, para n ≥ 3, esse grupo não é abeliano.

Você saberia dizer quantos elementos possui o grupo (S4,o)? E o grupo (S_5,o)?

Esse fato será provado na proposição a seguir.

Proposição 3.14. Se n ≥ 3, então (Sn,o) é não comutativo. Prova

Sejam A = {1, 2, 3, 4, ..., n}, com n ≥ 3, e f e g permutações em A, tais que f(1) = 3, f(2) = 1, g(1) = 2 e g(3) = 3.

Temos que:

(a) fog(1) = f(g(1)) = f(2) = 1; e

(b) gof(1) = g(f(1)) = g(3) = 3.

Assim, fog ≠ gof e, assim, Sn,o) não é abeliano, se n ≥ 3. Provando o resultado.

Exercício 3.15. Mostre que a ordem de (Sn,o) ou o número de elementos de Sn é n!.

Exercício 3.16. Qual é o elemento neutro de (S4,o)? E de (S5,o)? De maneira geral, qual o elemento neutro de (Sn,o)?

Exercício 3.17. Escolha 5 (cinco) elementos de (S4,o) e determine seus inversos.

Exercício 3.18. Escolha 5 (cinco) elementos de (S5,o) e determine seus inversos.

Exercício 3.19. Exiba um elemento de (S10,o), diferente do elemento neutro, que seja seu próprio inverso.

Um polígono regular de n lados possui n eixos de simetria. Aliás, essa é uma propriedade que serve para caracterizar os polígonos regulares, ou seja, se um polígono de n lados possui n eixos de simetria, então o polígono é regular.

2. Os grupos diedrais ou grupos de rotações

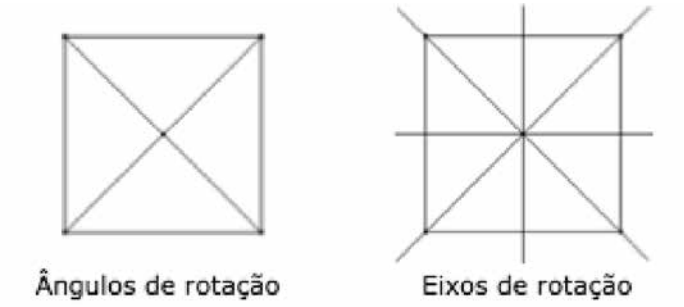
Até o momento, todos os grupos estudados apresentaram natureza algébrica. Nenhum deles foi voltado a outro ramo da Matemática. Agora iremos apresentar um "grupo geométrico", ou melhor, um grupo de natureza geométrica. Na realidade, trata-se de uma visão geométrica de grupos de permutações.

Em todo polígono regular de n lados é possível efetuarmos n rotações planas em torno de seu centro, cada uma dessas rotações possuindo ângulo de rotação de 360o/n. Além dessas rotações planas, é possível efetuarmos n rotações espaciais em torno de seus eixos de simetria.

Por exemplo, em um triângulo equilátero podemos efetuar 3 rotações planas em torno de seu centro, correspondendo a ângulos de 0o, 120o e 240o, e 3 rotações espaciais, em torno de seus eixos de simetria, perfazendo um total de 6 rotações.

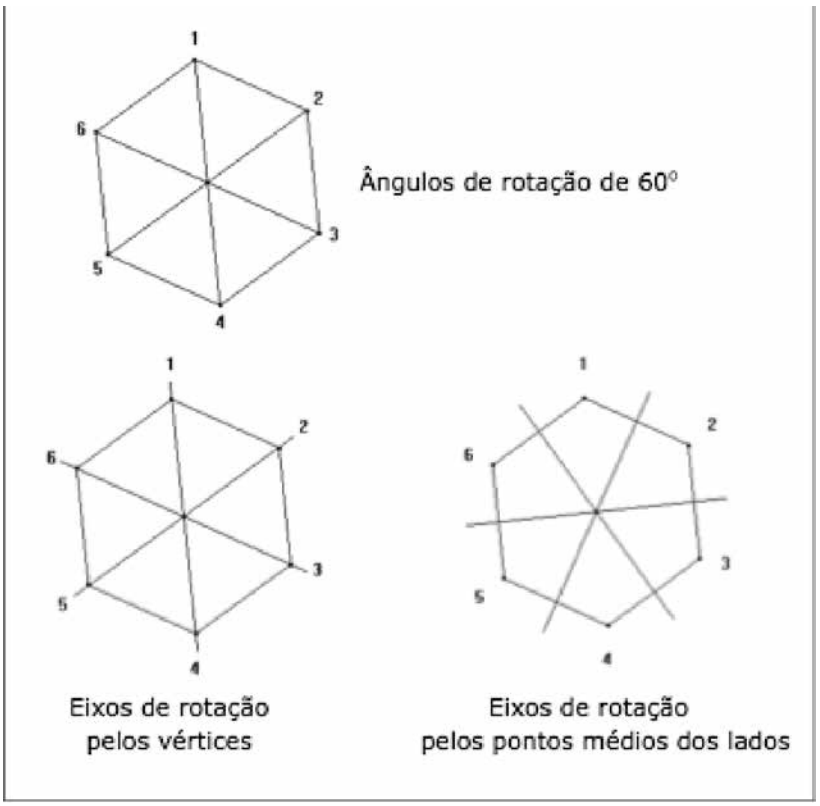
O conjunto das rotações do triângulo equilátero é denotado por D3. Em um quadrado podemos efetuar 4 rotações planas em torno de seu centro, correspondendo a ângulos de 90o, e 4 rotações espaciais em torno de seus eixos de simetria, perfazendo um total de 8 rotações.

Nas figuras abaixo podemos ver os eixos de simetria e os ângulos de rotação de um quadrado.



Ângulos de rotação Eixos de rotação

Nas figuras abaixo podemos ver os eixos de simetria e os ângulos de rotação de um hexágono regular.



De maneira geral, em todo polígono regular de n lados é possível efetuamos n rotações planas, correspondendo a ângulos de 360o/n, e n rotações espaciais em torno dos seus n eixos de simetria, perfazendo um total de 2n simetrias. O conjunto dessas 2n simetrias é denotado por D_n.

Cada uma dessas 2n rotações pode ser caracterizada ou pelo ângulo de rotação, no caso das rotações no plano, ou pelo eixo de simetria em torno do qual ela foi realizada, no caso das rotações espaciais.

Exercício 3.20. Numere os vértices do quadrado e veja a posição dos vértices após cada uma das rotações planas em torno do seu centro. Desenhe a figura obtida ao final.

Exercício 3.21. Idem para as rotações espaciais.

Exercício 3.22. Numere os vértices do hexágono regular e veja a posição dos vértices após cada uma das rotações planas em torno do seu centro. Desenhe a figura obtida ao final.

Exercício 3.23. Idem para as rotações espaciais.

Exercício 3.24. Numere os vértices do triângulo equilátero e veja a posição dos vértices após cada uma das rotações planas em torno do seu centro. Desenhe a figura obtida ao final.

Exercício 3.25. Idem para as rotações espaciais.

Exercício 3.26. Repita o exercício 3.20 para o pentágono, determinando seus ângulos de rotação.

Exercício 3.27. Repita o exercício 3.21 para o pentágono.

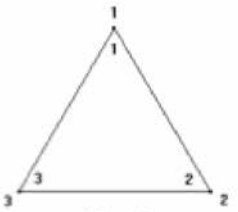


Figura 1

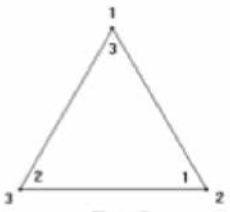


Figura 2

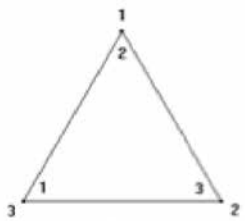


Figura 3

O 3-grupo diedral

Na figura 1 ao lado, temos um triângulo equilátero de vértices 1, 2 e 3 — os numerais internos —, enquanto os numerais externos representam as posições de cada vértice. Assim, o vértice 1 se encontra na posição 1; o vértice 2 se encontra na posição 2; e o vértice 3 se encontra na posição 3.

Na figura 2, o mesmo triângulo sofreu uma rotação de 120o em torno de seu centro, de tal forma que o vértice 1 passou a ocupar a posição 2; o vértice 2 ocupa a posição 3; e o vértice 3 ocupa a posição 1.

Na figura 3, o triângulo da figura 1 sofreu uma rotação de 240o em torno de seu centro, passando os vértices 1, 2 e 3 a ocuparem as posições 3, 1 e 2, respectivamente.

Pensando a figura 1 como uma rotação de 0o ou de 360o do triângulo original em torno de seu centro, essas são as três rotações planas do triângulo equilátero em torno de seu centro.

Essas rotações podem ser "traduzidas" na forma de funções/permutações do conjunto {1, 2, 3} nele mesmo, em que o domínio representa os três vértices e a imagem de cada vértice é a posição que ele ocupa na rotação.

Assim, as figuras 1, 2 e 3 anteriores podem ser representadas pelas seguintes permutações, em que os numerais da primeira linha representam

os vértices do triângulo e o numeral logo abaixo de cada vértice representa a posição que tal vértice ocupa.

Quadro das rotações planas do triângulo equilátero em torno de seus eixos de simetria, representadas por meio de permutações.

$$e: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$p_1: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$p_2: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Além das três rotações planas descritas anteriormente, os triângulos equiláteros ainda possuem mais três rotações, agora espaciais, em torno de seus eixos de simetria.

A figura a seguir mostra os três eixos de simetria do triângulo, cada um correspondente a uma das três posições que os vértices podem ocupar.

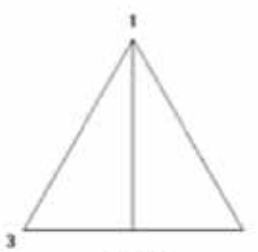


Figura 4

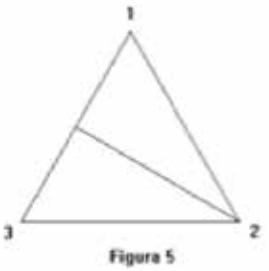


Figura 5

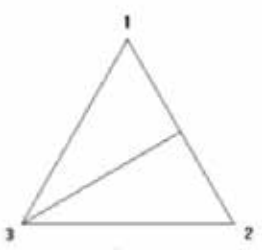
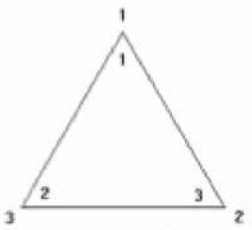
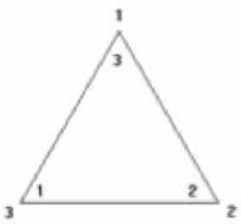
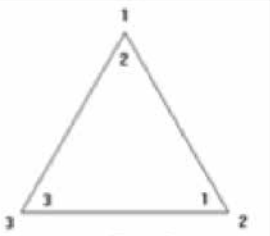


Figura 6

Chamando de E1, E2 e E3 os eixos correspondentes às posições 1, 2 e 3, respectivamente, as rotações do triângulo da figura 1, em torno de E1, E2 e E3 podem ser visualizadas nas figuras 7, 8 e 9, a seguir.

Rotação em torno de E1	Rotação em torno de E2	Rotação em torno de E3
 Figura 7	 Figura 8	 Figura 9

De maneira semelhante ao que foi feito com as rotações planas, as rotações espaciais podem ser representadas por permutações do conjunto {1, 2, 3}, como no quadro a seguir.

Quadro das rotações espaciais do triângulo equilátero em torno de seus eixos de simetria, representadas por meio de permutações.

$$e_1: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$e_2: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

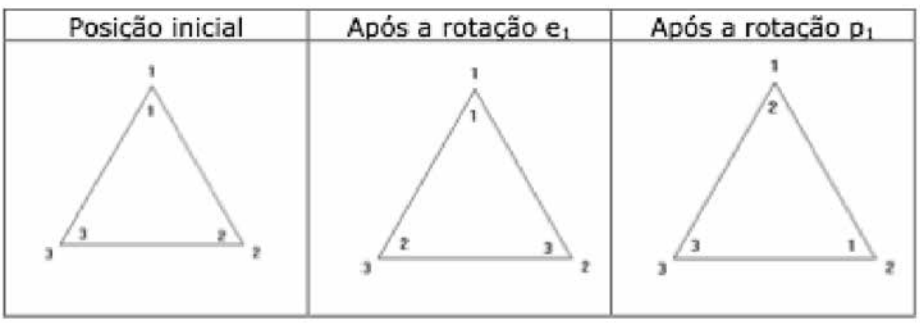
$$e_3: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Observe que essas são as seis permutações possíveis para 3 objetos. Assim, o conjunto dessas permutações, munido com a operação de composição de funções é o grupo (S3,o).

A composição de rotações

Trabalhando de forma mais geométrica, é possível definir no conjunto das seis rotações do triângulo equilátero a operação de composição de rotações, como segue: Se f e g são duas rotações do triângulo equilátero, a composta de f com g é indicada por fog e definida como a rotação que obtemos quando efetuamos no triângulo original, ou seja, no triângulo na posição inicial, primeiramente a rotação g e, em seguida, a rotação f.

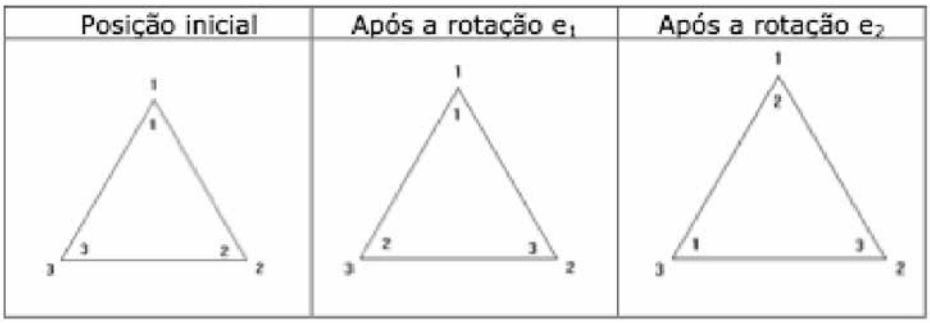
Exemplo 3.28. Calculando geometricamente a composta p1oe1, obtemos a rotação e3, conforme se percebe da sequência de figuras a seguir:



Exemplo 3.29. Calculando algebricamente a composta p1oe1, obtemos a rotação e3, conforme podemos perceber:

- p1oe1(1) = p1(1) = 2;
- p1oe1(2) = p1(3) = 1;
- p1oe1(3) = p1(2) = 3.

Exemplo 3.30. Calculando geometricamente a composta e2oe1, obtemos a rotação p2, conforme se percebe da sequência de figuras a seguir:



Exemplo 3.31. Calculando algebricamente a composta p1oe1, obtemos a rotação p2, conforme podemos perceber:

e2oe1(1) = e2(1) = 3;

e2oe1(2) = e2(3) = 1;

e2oe1(3) = e2(2) = 2.

Definição 3.32. O conjunto das rotações do triângulo equilátero, munido da composição de rotações é um grupo chamado 3-grupo diedral e é indicado por D3.

Exercício 3.33. Complete a tabela do 3-grupo diedral.

O n-grupo diedral

Tudo o que foi feito para o triângulo equilátero pode ser feito para o quadrado, obtendo-se assim, o 4-grupo diedral.

De maneira mais geral, quando trabalhamos de forma semelhante com um polígono regular de n lados, obtemos o n-grupo diedral Dn, ou grupo das rotações planas e espaciais desse polígono.

Observe que, como todo polígono regular de n lados possui 2n rotações – n planas em torno do centro e n espaciais em torno dos seus eixos de simetria –, a ordem de Dn é 2n. Observe ainda que os elementos de Dn podem ser pensados como permutações de n objetos, ou seja, elementos de Sn.

Assim, Dn é uma parte de Sn que é um grupo com a operação de composição de rotações. E como D3 possui 2X3 (=6) elementos e S3 possui 3! (=6) elementos os grupos D3 e S3 são o mesmo grupo, apenas com visões diferentes: em D3, a visão é geométrica; em S3, a visão é algébrica.

Desde que, se n > 3, temos 2Xn n!, o caso n = 3 é o único caso em que Sn = Dn.

Exercício 3.34. Construa a tabela completa do 4-grupo diedral.

Exercício 3.35. Escolha 5 (cinco) elementos de D5 e determine seus inversos.

Exercício 3.36. Como S5 possui 120 elementos e D5 possui apenas 10 elementos, determine 5 (cinco) elementos de S5 que não pertencem a D5.

DOMINGUES, H. H. Álgebra moderna. Atual: São Paulo, 2003

FRALEIGH, J.B. A first course in abstract algebra. Addison-Wesley: Japão, 1968

GONÇALVES, Adilson. Introdução à álgebra. Projeto Euclides. IMPA: Rio de Janeiro, 1979.

JACOBSON, N. Basic algebra. W. H. Freeman Company: San Francisco--USA, 1974.

MONTEIRO, L. H. J. Iniciação às estruturas algébricas. Série Professor No 6. Nobel: São Paulo, 1979.

NACHBIN, Leopoldo. Introdução à álgebra. McGraw-Hill do Brasil Ltda/Editora da UNB: Rio de Janeiro, 1971.

SIMIS, Aron. Introdução à álgebra. Monografias de Matemática 23. IMPA: Rio de Janeiro, 1977.

Capítulo 4

Isomorfismos de Grupos

Objetivo

- Neste capítulo, apresentaremos uma primeira noção de isomorfismo de grupos para que possamos entender certas afirmações que foram feitas ao longo dos capítulos anteriores.

Você sabe dizer precisamente o que isso significa?

Introdução

Nos capítulos anteriores nós dissemos que existe uma e apenas uma estrutura para um grupo de ordem 3.

Assim, as duas tabelas a seguir, dos grupos (G,*) e (H,o), definem o mesmo grupo.

Na realidade os grupos apresentam diferenças bem visíveis. A primeira delas está na natureza dos elementos: os elementos de G são letras, enquanto os de H são numerais; a segunda é o símbolo e o nome do símbolo utilizado para a operação: em G, a operação é representada por uma estrela ou um asterisco; em H, a operação é representada por uma bola.

Mas se substituirmos na tabela do grupo G as letras e, a e b por 0, 1 e 2, respectivamente, essa tabela fica como a que se encontra ao lado e, agora, G e H diferem apenas pelo símbolo da operação.

Trocando a * da operação de G pela □ da operação de H, os grupos passam a ser o mesmo grupo.

Note que, com essa substituição, os numerais 0, 1 e 2, elementos de H, passaram a desempenhar "os papeis" das letras e, a e b, elementos de G, mantendo os mesmos valores dos compostos em H, mostrando que G e H diferem somente pela natureza dos elementos de cada conjunto. Dizemos, por isso, que G e H são isomorfos.

É esse conceito que será mais bem trabalhado no que segue.

Essa substituição feita ao final da introdução pode ser pensada, matematicamente, como a existência de uma função f: G $\rightarrow$ H, injetora e sobrejetora e que preserva as operações de ambos os grupos, ou seja, uma bijeção f: G $\rightarrow$ H, tal que

f(x*y) = f(x)of(y).

De fato, a função definida é tal que f(e) = 0, f(a) = 1 e f(b) = 2 e, portanto é uma bijeção. Além disso, f possui essa propriedade explicitada anteriormente.

Os exemplos a seguir, servem para entendermos o que significa essa propriedade:

• f(e*b) = f(b) = 2, e

f(e)of(b) = 0o2 = 2,

mostrando que f(e*b) = f(e)of(b);

• f(a*b) = f(e) = 0, e

f(a)of(b) = 1o2 = 0,

mostrando que f(a*b) = f(a)of(b);

• f(a*a) = f(b) = 2, e

f(a)of(a) = 1o1 = 2,

mostrando que f(a*a) = f(a)of(a).

Exercício 4.1. Mostre que vale o resultado para os demais compostos de (G,*).

Mais precisamente, a definição de isomorfismo é dada como segue.

Definição 4.2. Dados os grupos (G,*) e (H,o), um isomorfismo de G em H é uma função f: G $\rightarrow$ H com as seguintes propriedades:

i) f é injetora;

ii) f é sobrejetora;

iii) f(x*y) = f(x)of(y).

Notação
Usaremos a notação G □ H para indicar que o grupo G é isomorfo ao grupo H.

Exemplo 4.3. A função identidade, f: Z $\rightarrow$ Z, dada por f(x) = x é um isomorfismo de (Z,+) em (Z,+). De fato, f é sobrejetora e injetora e, além disso, temos que f(x+y) = x+y = f(x) + f(y).

Exemplo 4.4. Na realidade, a função identidade de um grupo qualquer nele mesmo é um isomorfismo de grupos.

Exemplo 4.5. A função f, do grupo aditivo dos restos módulo 4, no grupo multiplicativo dos restos módulo 5, f: (Z4,+) $\rightarrow$ (Z5,•), dada por f(0) = 1, f(1) = 3, f(2) = 4, f(3) = 2, é um isomorfismo de (Z4,+) em (Z5,•). A função f é, obviamente, uma bijeção. Por meio de poucas contas é possível mostrar que f(x+y) = f(x)of(y), quaisquer que sejam os elementos x e y de Z4.

Exercício 4.6. Faça as contas e verifique que a função do exemplo 4.5 é realmente um isomorfismo de grupos.

Exemplo 4.7. A função f-1, do grupo multiplicativo (Z5,•) no grupo aditivo (Z4,+), inversa da função do exemplo 4.5, é um isomorfismo de (Z5,•) em (Z4,+).

Exercício 4.8. Faça as contas e verifique que a função f-1 do exemplo 4.7 é realmente um isomorfismo de grupos.

Da definição anterior, temos que todo isomorfismo de grupos é uma função injetora e sobrejetora, ou seja, uma função bijetora.

Você já sabe que se f: G $\rightarrow$ H é uma função injetora e sobrejetora, então existe uma função injetora e sobrejetora f-1: H $\rightarrow$ G, definida por

"f-1(y) = x se, e somente se, f(x) = y" e chamada de função inversa de f.

Assim, se f: G $\rightarrow$ H é um isomorfismo de grupos (do grupo G no grupo H), então sua inversa f-1: H $\rightarrow$ G, é uma função injetora e sobrejetora.

Essa observação, juntamente com o exemplo 4.7 e o exercício 4.8, nos leva à seguinte pergunta:

"A função f^{-1} inversa de um isomorfismo de grupos f é, também, um isomorfismo de grupos?"

Ou seja,

"Será que f-1(uov) = f-1(u)*f-1(v), $\forall$ u,v $\in$ H?"

A resposta a essa pergunta é sim: a inversa de um isomorfismo de grupos é, ainda, um isomorfismo de grupos, conforme demonstraremos na proposição a seguir.

Proposição 4.9. Sejam (G,*) e (H,o) grupos e f: G $\rightarrow$ H um isomorfismo de grupos. A função f-1: H $\rightarrow$ G, inversa de f é um isomorfismo de grupos.

Prova

Como f^{-1}: H $\rightarrow$ G é injetora e sobrejetora, basta mostrarmos que f^{-1}(uov) = f^{-1}(u)*f^{-1}(v), quaisquer que sejam os elementos u e v de H.

Sejam f^{-1}(u) = x, f^{-1}(v) = y e f^{-1}(uov) = z.

Temos, pela definição de f^{-1}, que f(x) = u, f(y) = v e f(z) = uov e, portanto

- f^{-1}(uov) = f^{-1}(f(x)*f(y))

e como f é um isomorfismo, temos que

- f^{-1}(uov) = f^{-1}(f(x)of(y)) = f^{-1}(f(x*y)) = x*y,

em que a última igualdade é decorrente da definição da função f-1.

Mas, x = f^{-1}(u) e y = f^{-1}(v), o que nos dá

- f^{-1}(uov) = f^{-1}(u)of^{-1}(v).

Assim, f^{-1} é um isomorfismo de grupos. Provando o resultado.

Se existe um isomorfismo do grupo (G,*) no grupo (H,o), ou simplesmente de G em H, dizemos que G é isomorfo a H. Pela proposição 4.9, se G é isomorfo a H, então H é isomorfo a G.

Assim, ao invés de dizer que o grupo G é isomorfo ao

grupo H (G é isomorfo a H) ou que o grupo H é isomorfo

ao grupo G (H é isomorfo a G), dizemos que os grupos G e H são isomorfos, ou que G e H são grupos isomorfos, sem nos preocuparmos com a ordem em que os grupos aparecem.

Exemplo 4.10. O grupo aditivo dos números reais, (R,+) é isomorfo ao grupo (R+,•), em que R+ é o conjunto dos números reais positivos e • é a multiplicação de números reais. De fato, a função f: $R \rightarrow R+$, dada por f(x) = exp(x) = ex, é um isomorfismo de (R,+) em (R+,•). Note que:

i) f é injetora, pois se f(x) = f(y), então ex = ey e, consequentemente, x = y;

ii) f é sobrejetora, pois se u $\in$ R+, então ln(u), o logaritmo natural de u, é tal que f(ln(u)) = elnu = u;

iii) $f(x + y) = e^{x+y} = e^x \bullet e^y = f(x) \bullet f(y)$.

De acordo com o que foi feito até agora, podemos pensar intuitivamente que se o grupo G é isomorfo ao grupo H, então G é apenas uma renomeação dos elementos de H e, portanto, ao elemento eH, elemento neutro de do grupo H, corresponde o elemento eG, elemento neutro do grupo G.

Nessa perspectiva mais intuitiva, os resultados que seguem são óbvios, entretanto, é possível demonstrá-los matematicamente, de forma mais rigorosa, e isso é o que faremos no que segue.

Dados os grupos G e H, e denotando por eG e eH os elementos neutros de G e de H, respectivamente, temos o seguinte resultado:

Proposição 4.11. Se f é um isomorfismo de G em H, então f(eG) = eH.

Prova

Como f é um isomorfismo de grupos, temos que

• f(eG) = f(eG*eG) = f(eG).f(eG).

Assim, f(eG) é solução, em H, da equação X2 = X. E desde que em um grupo a única solução dessa equação é eH, temos que f(eG) = eH.

Provando o resultado.

Para os elementos a e a', o simétrico de a, de um grupo G, temos o seguinte resultado:

Proposição 4.12. Se f é um isomorfismo de G em H, então f(a') = [f(a)]'.
Prova

Como f é um isomorfismo de grupos, temos que

- f(a').f(a) = f(a'.a) = f(eG) = eH;
- f(a).f(a') = f(a.a') = f(eG) = eH. Assim, por definição, f(a') = [f(a)]'.

Provando o resultado.

Exemplo 4.13. O isomorfismo do exemplo 4.5, do grupo aditivo dos restos módulo 4, (Z4,+), no grupo multiplicativo dos restos módulo 5, (Z5,□), é dado por f(0) = 1, f(1) = 3, f(2) = 4, f(3) = 2. Observe que 0 e 1 são, respectivamente, os elementos neutros de (Z4,+) e (Z5,□), e f(0) = 1. Além disso, temos, por exemplo, que 1' = 3, f(1') = f(3) = 2 e [f(1)]' = [3]' = 2. Como afirmam as proposições anteriores.

Leituras, filmes e sites

Atividades de avaliação

Atividades de avaliação

Referências

DOMINGUES, H. H. Álgebra moderna. Atual: São Paulo, 2003

FRALEIGH, J.B. A first course in abstract algebra. Addison-Wesley: Japão, 1968

GONÇALVES, Adilson. Introdução à álgebra. Projeto Euclides. IMPA: Rio de Janeiro, 1979.

JACOBSON, N. Basic algebra. W. H. Freeman Company: San Francisco--USA, 1974.

MONTEIRO, L. H. J. Iniciação às estruturas algébricas. Série Professor No 6. Nobel: São Paulo, 1979.

NACHBIN, Leopoldo. Introdução à álgebra. McGraw-Hill do Brasil Ltda/Editora da UNB: Rio de Janeiro, 1971.

SIMIS, Aron. Introdução à álgebra. Monografias de Matemática 23. IMPA: Rio de Janeiro, 1977.