FUNDAMENTOS MATEMÁTICOS DA COMPUTAÇÃO

Vanessa Davanço

E-book 4

FAM ONLINE

Neste E-Book:

INTRODUÇÃO

Neste módulo, faremos uma incursão mais complexa e algébrica, ou seja, trataremos de álgebra e elementos de teoria dos números. A matemática do dia a dia é pautada por muitas definições e teorias com demonstrações algébricas e não numéricas. Toda essa teoria valida a matemática “numérica”, que aprendemos na escola, durantes os ensinos fundamental e médio.

Para estudantes de computação, é muito importante saber por que algumas coisas acontecem, pois, ao programar, coloca-se o formato algébrico em seus códigos, não o formato numérico. Vamos iniciar os estudos com álgebra e elementos de teoria de número.

ÁLGEBRA E ELEMENTOS DE TEORIA DE NÚMEROS

A matemática é cheia de detalhes e artifícios para conseguir alcançar um objetivo definido. Obviamente, esses artifícios precisam ser pautados por definições e regras reais. Às vezes, não conseguimos alcançar uma resposta pelos dados obtidos, mas conseguimos supor algum ponto de partida que nos possibilite alcançar a resposta almejada. Nesse sentido, a álgebra e os elementos de teoria de números se destacam para que possamos encontrar soluções com um embasamento teórico e, muitas vezes, com uso de demonstrações.

Indução

Para uma melhor compreensão sobre a indução, vamos começar falando do conceito de indução intuitivamente. Imagine uma escada infinita (Figura 1), da qual desejamos saber se seria possível alcançar todos os seus degraus. Podemos saber duas coisas:

Figura 1: *Escada infinita.* ***Fonte:*** *Elaboração Própria.*

1. Pode-se alcançar o primeiro degrau.

2. Se pudermos alcançar um determinado degrau, então podemos alcançar o próximo degrau da escada.

Então, conseguimos alcançar todos os degraus? Pela proposição (1), afirmamos que podemos alcançar o primeiro degrau da escada; em (2), afirmamos que se estamos no primeiro degrau, podemos ir para o segundo degrau. Aplicando o (2), sucessivamente, podemos chegar ao terceiro, quarto, quinto degraus e, dessa maneira, podemos concluir que chegaremos ao final da escada, ou seja, no infinito. Esta é a forma

intuitiva de como se chegar ao final da escada. Agora, vamos definir formalmente o conceito de indução.

O Princípio da Indução Matemática: a fim de demonstrar que $P(n)$ é verdadeira para todos os números inteiros n, em que $P(n)$ é uma função proposicional, devemos completar dois passos:

1. Verifica-se se $P(1)$ é verdadeira.

2. Mostra-se que a proposição condicional $P(n) \rightarrow P(n+1)$ é verdadeira para todos os números inteiros positivos n.

Exemplo 1: Mostre que, se n é um inteiro positivo, então

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

Resolução:

1. Verificando se *P(1)* é verdadeira:

Verificar se o primeiro termo é verdade, ou seja, se o primeiro dado da indução é 1, substituindo na fórmula final, o resultado será 1? Sendo assim, vamos verificar.

$$1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Portanto, o passo 1 verdadeiro.

2. $P(n) \rightarrow P(n+1)$, devemos verificar se $P(n)$ é válido. Sendo assim:

$$1 + 2 + \cdots + k = \frac{k.(k+1)}{2}$$

Devemos adicionar mais um termo, ou seja, de ambos os lados $(k+1)$, sendo assim:

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

Portanto, pela indução matemática, sabemos que $P(k)$ é verdade para todos os números inteiros positivos n.

Exemplo 2: Mostre que, se n^2 é a soma dos primeiros inteiros positivos ímpares.

Resolução: Vamos definir que $P(n) = 1 + 3 + 5 + \ldots + (2n\text{-}1) = n^2$, sendo assim, devemos seguir para os passos 1 e 2 e verificar se a afirmação é verdadeira.

1. Verificando se *P(1)* é verdadeira:

Verificar substituindo na função o valor 1, ou seja, $1 = 1^2$.

Portanto, o passo 1 é verdadeiro.

2. $P(n) \rightarrow P(n+1)$, vamos supor que $P(n)$ seja verdade, ou seja, $1 + 3 + 5 + \ldots + (2n\text{-}1) = n^2$.

Para o próximo passo, devemos provar que $P(n+1)$ é verdadeiro:

$$1 + 3 + 5 + \ldots + (2n\text{-}1) + [2(n+1)\text{-}1] = (n+1)^2$$

Para provar, devemos arrumar a equação. Sabe-se que $1 + 3 + 5 + \ldots + (2n\text{-}1) = n^2$, assim, podemos substituir na equação acima, resultando em:

$$n^2 + [2(n + 1)\text{-}1] = n^2 + (2n + 2 - 1)$$

$$= n^2 + 2n + 1$$

$$(n + 1)^2$$

Concluímos que a proposição é verdadeira.

SAIBA MAIS

Um exemplo simples que ilustra a Indução Matemática é o efeito dominó. Imagine uma fila sem fim de peças de dominó, na qual, ao derrubar a primeira peça, as próximas serão derrubadas uma após a outra.

Suponhamos que seja verdadeira as seguintes proposições:

1.A primeira peça é derrubada em direção as demais.

2.Se qualquer que seja a peça que estiver próxima da seguinte na fila, então, ao ser derrubada, derrubará a seguinte e assim consequentemente.

Concluímos, então, que:

• Com o item 1, a primeira peça será derrubada.

• Com o item 2, a segunda peça será derrubada.

• Com o item 3, a terceira peça será derrubada e assim sucessivamente...

Portanto, podemos generalizar que se o início é certo e se não existe nada para parar essa sequência, então sempre será correto.

Por que a indução é válida?

Podemos dizer que uma indução matemática é válida pela propriedade de ordenação para os inteiros positivos, ou seja, **todo conjunto não vazio do conjunto dos inteiros positivos tem um elemento mínimo**.

Devemos supor que exista um $P(1)$ que seja verdadeiro e que $P(n) \rightarrow P(n+1)$ também seja verdadeiro, sendo um n inteiro e positivo. Agora, devemos assumir que existe pelo menos um inteiro positivo que não faça parte do conjunto verdadeiro, ou seja, $P(n)$ tenha valor falso. Concluímos que é falso o conjunto dos números inteiros positivos no qual $P(n)$. Vamos denominá-lo de T um conjunto não vazio. Logo, pelo conjunto do ordenamento, dizemos que:

- O conjunto T tem um elemento mínimo (m): sabemos que $m \neq 1$, pois assumimos no início que $P(1)$ é verdade, com isso, o mínimo não pode ser 1. Contudo, se m for positivo e maior que 1, concluímos que m-1 é um inteiro positivo. Como m-1 pertence ao conjunto T, uma vez que ele é maior que m, sendo que m é mínimo. Então, $P(m\text{-}1)$ deve ser verdadeiro.

Como $P(m\text{-}1)$ é verdadeiro, verifica-se então que $P(n) \rightarrow P(n+1)$ também é verdadeiro, deste modo, chegamos a uma contradição: $P(m)$ é verdadeiro.

Portanto, $P(n)$ deve ser verdadeiro para todo inteiro positivo n.

Para que toda demonstração corresponda ao esperado, devemos usar a indução matemática passo a passo, desde o básico até o passo indutivo, com o intuito de não correr o risco de que algumas etapas sejam definidas de forma errada.

Recursão

Alguns conjuntos são difíceis de se definir explicitamente, mas às vezes são fáceis de se definir recursivamente. A recursão pode ser usada para definir sequências, funções e conjuntos.

Exemplo 3: A sequência de potências 3 é dada por $a_n = 3^n$.

Resolução: Podemos definir essa sequência também a partir do primeiro termo, $a_0 = 1$, e uma regra para encontrar o próximo termo poderia ser $a_{n+1} = 3a_n$ para n=0,1,2,3,...

Quando definimos um problema recursivamente, especificamos a forma como encontramos os próximos termos da sequência a partir do termo anterior, ou seja, não usamos a função definida no exemplo, mas sim a função que definimos como sendo a ideal para encontrar o termo subsequente.

Funções definidas recursivamente

Para definirmos uma função recursivamente, devemos defini-la em duas etapas:

1. Especificar o valor da função em zero.

2. Fornecer uma regra para encontrar seu valor em um número inteiro a partir do passo anterior.

Exemplo 4: A função f é definida recursivamente conforme:

$$f(0) = 1$$

$$f(n+1) = 2f(n) + 2$$

Encontre $f(1), f(2), f(3), f(4)$ e $f(5)$.

Resolução: A partir da definição dada no exemplo de forma recursiva, devemos calcular a sequência pedida no exemplo.

$$f(0+1) = f(1) = 2f(0) + 2 = 2.1 + 2 = 4$$

$$f(1+1) = f(2) = 2f(1) + 2 = 2.4 + 2 = 10$$

$$f(2+1) = f(3) = 2f(2) + 2 = 2.10 + 2 = 22$$

$$f(3+1) = f(4) = 2f(3) + 2 = 2.22 + 2 = 46$$

$$f(4+1) = f(5) = 2f(4) + 2 = 2.46 + 2 = 94$$

O problema continuaria fazendo a sequência dessa mesma forma até que chegasse ao fim do problema definido. Para o problema dado acima, temos

que $f(1) = 4, f(2) = 10, f(3) = 22, f(4) = 46$ e $f(5) = 94$.

Muitas funções podem ser estudas por meio das definições de forma recursiva. Agora vamos analisar um exemplo clássico para a recursão, que é a função fatorial $F(n) = n!$

Exemplo 5: Encontre uma definição recursiva da função fatorial $F(n) = n!$

Resolução: Iniciemos a resolução especificando o valor inicial da função.

$$F(0) = 0! = 1$$

Devemos encontrar uma regra para $F(n+1)$ a partir de $F(n)$. Vamos defini-la da seguinte maneira:

$$F(n+1) = (n+1).F(n)$$

Na sequência, encontramos alguns valores para verificar se essa função definida será válida para a função fatorial.

$$F(1) = F(0+1) = (0+1).F(0) = 1.1 = 1$$

$$F(2) = F(1+1) = (1+1).F(1) = 2.1 = 2$$

$$F(3) = F(2+1) = (2+1).F(2) = 3.2 = 6$$

$$F(4) = F(3+1) = (3+1).F(3) = 4.6 = 24$$

$$F(5) = F(4+1) = (4+1).F(4) = 5.24 = 120$$

Seguindo a mesma função e tendendo ao infinito, podemos encontrar qualquer valor de permutação.

Observe que, na forma recursiva, precisamos saber sempre o valor do termo anterior.

Algoritmos definidos recursivamente

Vamos definir um algoritmo a partir de uma sequência definida em cada um dos exemplos propostos. Se pensarmos no Exemplo 5, sobre permutação, sabemos que é preciso seguir a sequência infinitamente até que seja definido um ponto de parada. Definição: Um algoritmo é chamado de recursivo se resolver um problema reduzindo-o a um mesmo problema com valores iniciais menores.

Exemplo 6: Encontre um algoritmo recursivo para computar $n!$ em que n é um número inteiro não negativo.

Resolução: Conforme estudado no Exemplo 5, definimos a seguinte função do segundo termo em diante $F(n+1) = (n+1).F(n)$.

Uma forma para construir esse algoritmo seria:

Procedure fatorial (n: número inteiro não negativo)

if n=0 then fatorial (n):=1

else fatorial (n):= fatorial(n-1)

Exemplo 7: Suponha uma sequência definida como:

1. $S_1 = 2$

2. $S_n = 2.S_{n-1}$ para $n \geq 2$.

Resolução: A seguir, mostra-se um algoritmo possível para a solução desse problema; porém, sabemos que, de acordo com a lógica do programador e com o tipo de programação, podemos ter vários algoritmos, sendo um deles:

```
function S(n)
if n=1 then
    S:=2
else
    S:=2*S(n-1)
endif
```

Dessa maneira, podemos tornar qualquer problema recursivo em um algoritmo.

Podcast 1

Grupos e semigrupos

Em relação à teoria de Grupos, a ideia básica é combinar dois elementos de um conjunto. Ao combinar esses dois elementos relacionados, apresenta-se um terceiro elemento que pertença ao mesmo conjun-

to dos outros dois elementos. A esse fato damos o nome de **operação binária**.

Definição: Seja B um conjunto não vazio. Uma operação binária sobre B é uma função * que associa a cada par ordenado $(a, b) \in B \times B$ um elemento $a^*b \in B$, representada por

$$*: B \times B \to B$$

$$(a, b) \mapsto a^*b$$

Conforme definido anteriormente, a cada relação do conjunto B com o conjunto B, teremos um novo elemento que também pertencerá a esse conjunto B.

Exemplo 8: Sejam os conjuntos N (conjunto dos números naturais com o zero), Z (conjunto dos números inteiros), Q (conjunto dos números racionais), R (conjunto dos números reais) e C (conjunto dos números complexos), dizemos que:

a) A adição sobre N, Z, Q, R ou C é uma operação binária.

b) A subtração sobre N, Z, Q, R ou C é uma operação binária.

c) A multiplicação sobre N, Z, Q, R ou C é uma operação binária.

d) A divisão sobre N, Z, Q e R é uma operação binária.

Definição de Grupo: Seja G um conjunto não vazio munido de uma operação *. Dizemos que G é um

grupo com respeito à operação * se, e somente se, acontece:

I) $\forall a, b \in G \Rightarrow a*b \in G$, ou seja, Lei Comutativa.

II) $\forall a, b, c \in G \Rightarrow a*(b*c) = (a*b)*c$, ou seja, Lei Associativa.

III) $\exists e \in G , \forall a \in G \Rightarrow a*e = e*a = a$, ou seja, Existência do Elemento Neutro.

IV) $\exists a^{-1} \in G , \forall a \in G \Rightarrow a*a^{-1} = a^{-1}*a = e$, ou seja, a Existência do Elemento Oposto.

Nessa definição,

I) diz que o conjunto G deve ser fechado com relação à operação *, ou seja, em uma operação realizada no Grupo G com a operação *, resultará em outro elemento de G.

II) mostra que * é uma operação associativa, ou seja, os elementos relacionados à operação * podem ser relacionados sem a necessidade de parênteses, pois a ordem não importa.

III) mostra a exigência de um elemento neutro.

IV) garante que todo elemento $a \in G$ possua operação * um elemento inverso $a^{-1} \in G$.

Note que, para ter um grupo, precisamos que o conjunto seja um conjunto não vazio e que exista uma operação sobre ele definida como *; podemos usar uma notação de grupo com a operação *, sendo $\langle G, * \rangle$. Nada impede de apenas falar G é um grupo definido pela operação *.

Exemplo 9: O conjunto $\langle Q, + \rangle$, $\langle R, + \rangle$ e $\langle C, + \rangle$ são grupos com a operação usual de adição, com o elemento neutro sendo 0, e o elemento oposto de x é -x.

Exemplo 10: O conjunto Z, munido da operação subtração, não caracteriza um grupo, pois esse grupo não possui um elemento neutro, ou seja, não existe e-$x = x$.

Exemplo 11: O conjunto $Q\{0\} = \{r \in Q / r \neq 0\}$ é um grupo em relação à operação usual de produto de números racionais $\langle Q, . \rangle$.

Exemplo 12: O conjunto $\langle R^*, . \rangle$ e $\langle C^*, . \rangle$ são grupos com a operação usual de multiplicação, com o elemento neutro sendo 1, e o elemento oposto de x é o $\frac{1}{x}$.

Exemplo 13: O conjunto N, munido da operação potenciação *, dada por $A*b = a^b$, não é um grupo, ou seja, tomando como exemplo $(2 * 3)*4 \neq 2 * (3 * 4)$.

$$(2 * 3)*4 = (2^3)^4 = 4096$$

$$2 * (3 * 4) = (3^4)^2 = 6561$$

Portanto, não é grupo.

Definição: Dizemos que um grupo $\langle G, * \rangle$ é abeliano ou comutativo se, e somente se, * é uma operação comutativa.

Exemplo 14: Para todo $x, y \in Z$, temos que $x + y = y + x$, ou seja, $\langle Z, + \rangle$ é um grupo aditivo abeliano. Da mesma forma, os grupos $\langle Q, + \rangle$, $\langle R, + \rangle$ e $\langle C, + \rangle$ com a operação adição são grupos abelianos.

Definição de semigrupo: Sejam G um grupo e S semigrupo não vazio de G. Dizemos que S é um semigrupo de G e denotamos por $S \leq G$, se, e somente se, S é um grupo com a operação binária de G.

Observação: {e} e G são semigrupos triviais de G.

Definição: Dizemos que S é um semigrupo próprio ou não trivial de G e denotamos por S<G, se H é um semigrupo de G com S≠G e S≠ $\{e\}$.

Exemplo 15: Observa-se facilmente:

1. $Z < Q < R$ com relação à operação usual da adição.

2. $Q^* < R^*$ e $R^+ < R^*$ com relação à operação usual de multiplicação.

3. O conjunto de todos os números pares é um semigrupo de $\langle Z, + \rangle$.

Na definição a seguir, demonstramos uma forma em que se pode determinar um subconjunto S de G sem ter que mostrar que esse conjunto S também é um grupo com a operação definida em G.

Definição: Se S é um subconjunto de um grupo $\langle G, * \rangle$, então, S é um semigrupo de G se, e somente se, as seguintes acontecem:

I) $e \in S$; ou seja, Elemento Neutro de S.

II) $\forall a \in S \Rightarrow a^{-1} \in S$; ou seja, fechado para o Elemento Inverso.

III) $\forall a, b \in S \Rightarrow a^*b \in S$, ou seja, fechado para a operação.

Demonstração: Vamos provar a ida da definição, ou seja, vamos supor que $S \leq G$, provando que as condições i, ii e iii são satisfeitas. Se e_s é um elemento neutro de H, então $e_s{}^*e_s = e_s$, logo $e^*e_s = e_s$, e $e \in S$.

Sendo $\langle S, * \rangle$ um grupo, então podemos falar que S é fechado com relação à operação *, ou seja, $\forall a, b \in S \Rightarrow a^*b \in S$. Também temos que $\forall a \in S \Rightarrow a^{-1} \in S$. Assim, verificamos se todas as condições estão satisfeitas.

Agora, devemos provar a volta, ou seja, vamos supor que as condições i, ii e iii sejam satisfeitas e devemos provar que S é um semigrupo de G. De fato, temos que $H \neq 0$, pois em i) temos a existência do elemento neutro. Já em ii) podemos falar que S possui inverso e iii) declara que S é fechado em relação a operação *, sendo que essa operação é a mesma do grupo G, seguindo que * é uma operação associativa. Com isso, podemos concluir que S é um grupo.

Temos ainda a seguinte definição, segundo a qual podemos utilizá-la ao invés da anterior.

Definição: Se S é um subconjunto de um grupo $\langle G, * \rangle$, então S é um semigrupo de G se, e somente se, acontece:

IV) $S \neq 0$

V) $\forall a, b \in S \Rightarrow a^*b^{-1} \in S$

Exemplo 16: O conjunto $S = \{1,2,3, \dots\}$ é um semi-grupo em relação à operação de soma usual.

Resolução: Como o conjunto $M = \{0,1,2,3, \dots\}$ é um monóide em relação à operação de soma usual, na qual $e = 0$ é o elemento neutro de M.

O conjunto $G = Z = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ é um grupo em relação à operação de soma usual, na qual $e = 0$ é o elemento neutro de G e sua inversa é $n^{-1} = -n$. Podemos chamar esse grupo de $\langle Z, + \rangle$ para lembrar o conjunto considerado, nesse caso, como o conjunto Z e a operação considerada +.

Exemplo 17: O conjunto $R_+ = \{x \in R \,/\, x > 0\}$ é um semigrupo em relação à operação de soma.

Exemplo 18: O conjunto $\langle N, +, * \rangle$, ou seja, o conjunto dos naturais com a soma e multiplicação usual é um semigrupo.

Exemplo 19: Considere o grupo $\langle R^*, . \rangle$ e $R_+^* = \{x \in R / x > 0\}$. Afirmamos que R_+^* é um semi-grupo de R^*.

Resolução:

Como 1>0 temos que $1 \in R_+^*$, ou seja, $R_+^* \neq 0$.

Para todo $b \in R_+^*$, temos que b>0.

Portanto $b^{-1} = \frac{1}{b} > 0$ e

$\forall a, b \in R_+^* \Rightarrow a > 0 \; e \; ab^{-1} > 0 \Rightarrow ab^{-1} \in R_+^*$.

Assim R_+^* é um semigrupo de R^*.

Homomorfismo de grupos e aplicações

Definição: Sejam $\langle G, * \rangle$ e $\langle S, \oplus \rangle$ grupos.

1. Uma aplicação $f: G \to S$ é um homomorfismo se, e somente se, $\forall a, b \in G, f(a*b) = f(a) \oplus f(b)$.

2. Uma aplicação $f: G \to S$ é um homomorfismo se, e somente se, f é um homomorfismo bijetor. Assim, podemos dizer que G e S são grupos isomorfos, $G \cong S$.

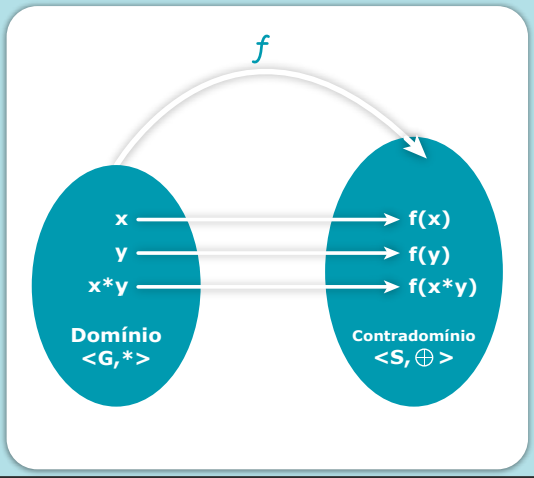

Figura 2: *Esboço de homomorfismo.* ***Fonte:*** *Elaboração Própria*

Exemplo 20: Sejam $G = \langle R, + \rangle$ e $H = \langle R_+^*, . \rangle$. Defina a aplicação $f: G \to S$ por $f(x) = 3^x$. A aplicação f assim definida é um isomorfismo.

Resolução: Verificamos que, para todo $a, b \in R_+^*$, temos:

I) A aplicação f é um homomorfismo, ou seja,

$$f(a.b) = 3^{a.b} = 3^a + 3^b = f(a) + f(b)$$

II) A aplicação f é injetora, ou seja,

$$\forall a, b \in G, \qquad f(a) = f(b) \rightarrow 3^a = 3^b \rightarrow a = b$$

III) A aplicação f é sobrejetora, ou seja,

$$\forall b \in H, \exists a = \log_2 b \in G / f(a) = 2^{\log_2 b} = b$$

Portanto, f é um isomorfismo.

Exemplo 21: Sejam $G = \langle R, + \rangle$ e $S = \langle R_+^*, . \rangle$. Defina a aplicação $f: S \rightarrow G$ por $f(x) = \log(x)$. A aplicação f assim definida é um homomorfismo.

Resolução: Verificamos que, para todo $a, b \in R_+^*$, temos:

$$f(a.b) = \log(a.b) = \log(a) + \log(b) = f(a) + f(b)$$

Portanto, encontramos que $f(a.b) = f(a) + f(b)$, ou seja, um homomorfismo.

Definição: Seja G um grupo.

1. Uma aplicação $\theta: G \rightarrow G$ é um endomorfismo se, e somente se, θ é um homomorfismo.

2. Uma aplicação $\theta: G \rightarrow G$ é um automorfismo se, e somente se, θ é um isomorfismo.

Exemplo 22: A aplicação $\theta: \langle R, + \rangle \rightarrow \langle R, + \rangle$ definida por $\theta(x) = x^2$, não é um automorfismo.

Resolução: Conforme definição, temos que um automorfismo é um isomorfismo, logo, devemos verificar se a função é um isomorfismo:

$$\theta(x+y) = (x+y)^2 \neq x^2 + y^2$$

Portanto, $\theta(x+y) \neq \theta(x) + \theta(y)$ não é um automorfismo.

Exemplo 23: A aplicação $\theta: \langle R, . \rangle \to \langle R, . \rangle$, definida por $\theta(x) = x^2$ é um automorfismo.

Resolução: Conforme definição, temos que um automorfismo é um isomorfismo, logo, devemos verificar se a função é um isomorfismo:

$$\theta(x.y) = (x.y)^2 = x^2.y^2 = \theta(x).\theta(y)$$

Portanto, $\theta(x.y) = \theta(x).\theta(y)$ é um automorfismo

Exemplo 24: A aplicação $\theta: \langle Z \times Z, + \rangle \to \langle Z \times Z, + \rangle$, definida por $f(x,y) = (x\text{-}y, 0)$ é um endomorfismo.

Resolução: Conforme definição, temos que um endomorfismo é um homomorfismo, logo, devemos

$$f(x+z, y+t) = (x+z-y-t, 0) = (x-y, 0) + (-y-t, 0) = f(x,y) + f(z,t)$$

Portanto, $f(x,y)$ é um endomorfismo.

Definição: Sejam G e S grupos, e $f: G \to S$ um homomorfismo. Então:

1. $f(e_G) = e_S$, elemento neutro em que $e_G \in G$ e $e_S \in S$.

2. $f(a^{-1}) = f(a)^{-1}, \forall a \in G$.

3. $f(a^n) = f(a)^n$, $\forall n \in Z$.

Demonstração: Sejam e_G e e_S os respectivos elementos neutros de G e S. Se $a \in G, n \in Z$ e $f: G \to S$, é um homomorfismo, então:

1. $f(e_G) = e_S$. De fato, $f(e_G . e_G) = f(e_G).f(e_G)$. Logo, como $f(e_G) \in S$, pela definição, temos que $f(e_G) = e_S$.

2. $f(a^{-1}) = f(a)^{-1}$. De fato, $f(a).f(a^{-1}) = f(a.a^{-1}) = f(e_G) = e_S$. Pela unicidade do elemento inverso, temos que $f(a^{-1}) = f(a)^{-1}$.

3. $f(a^n) = f(a)^n$. De fato,

$$f(a^n) = f(\underbrace{aa \dots a}_{n\ vezes}) = \underbrace{f(a)f(a) \dots . f(a)}_{n\ vezes} = f(a)^n$$

Os algebristas não fazem distinção entre grupos isomorfos, ou seja, não se preocupam com a natureza dos elementos que compõem os grupos. No entanto, preocupam-se com a forma com que eles são operados. Portanto, com esse intuito, não se faz distinção entre os grupos cíclicos infinitos e o grupo aditivo dos inteiros, conforme a seguinte definição.

Definição: Todo grupo cíclico é isomorfo ao grupo aditivo dos inteiros.

Definição: Seja G um grupo cíclico finito de ordem n. Então, $G \cong Z_n$.

Exemplo 25: A aplicação θ: $\langle Z_5^*, . \rangle \rightarrow \langle Z_5^*, . \rangle$, definida por $f(x) = \overline{2} = 2^k$, é um grupo cíclico gerado por $\overline{2}$.

Resolução: Primeiramente, vamos entender como funciona esse grupo $f(x) = \overline{2}$, no conjunto $\langle Z_5^*, . \rangle \rightarrow \langle Z_5^*, . \rangle$. Como n=5, temos uma variação desse conjunto de 0 a 4, denominado de conjunto das classes de restos módulo n, que é definida como

$$\bar{x}.\bar{y} = \overline{x.y}$$

Ou seja,

$$\overline{0}.\overline{1} = \overline{0}$$

$$\overline{1}.\overline{2} = \overline{2}$$

$\overline{2}.\overline{3} = \overline{1}$, ou seja, 2.3=6, porém o resto é 5, então, $\overline{2}.\overline{3} = \overline{1}$ e assim sucessivamente.

O grupo gerado será definido conforme $G = [x] = \{x^k / k \in Z\}$.

Após as devidas explicações, retornamos ao exemplo, o grupo cíclico gerado por $\overline{2}$ será:

$$[\overline{2}] = \left\{\overline{2^0}, \overline{2^1}, \overline{2^2}, \overline{2^3}\right\} = \{\overline{1}, \overline{2}, \overline{4}, \overline{3}\} = Z_5^*$$

Pode-se observar que, para provar que dois grupos G e S são isomorfos, basta seguir os passos dados a seguir. Obviamente, a ordem não precisa ser respeitada, pois os dados são ordenados da seguinte maneira:

I) Defina uma aplicação $f: G \rightarrow S$.

II) Mostre que *f* é injetora.

III) Mostre que *f* é sobrejetora.

IV) Mostre que *f* é um homomorfismo.

FIQUE ATENTO

Pensando igual a um algebrista, quando precisamos mostrar que dois conjuntos não são isomorfos, podemos encontrar alguma propriedade algébrica que será preservada pela existência do isomorfismo entre esses dois grupos que queremos demonstrar, mas que satisfaz apenas em um dos dois grupos envolvidos. Por exemplo, se tivermos dois grupos e eles forem isomorfos, e um dos grupos for abeliano, então, pela definição, o outro também precisa ser um grupo abeliano, ou seja,

Definição: Sejam G e S grupos, e $f: G \to S$ um isomorfismo. Se G é abeliano, então, S é abeliano.

Definição: Sejam G e H grupos, S um semigrupo de G, e $f: G \to H$ um homomorfismo. Então, $f(S)$ é um subgrupo de H. Sendo assim, $Im(f) = F(G)$ é um semigrupo de H.

Definição: Sejam G e H grupos e $f: G \to H$ um homomorfismo. Se f é injetiva, então $G \cong Im(f)$.

Definição: Seja G um grupo cíclico gerado por a. Se $\theta: G \to H$ é um homomorfismo de grupos, então $\forall x \in G, \theta(x)$ é completamente determinado por $\theta(a)$.

Definição: Sejam G e H e V grupos. Se $g: G \to H$ e $f: H \to V$ são homomorfismo, então $f \circ g: G \to V$ é um homomorfismo.

Definição: Se $f: G \to H$ é um isomorfismo, então, $f^{-1}: H \to G$ também é um isomorfismo.

Definição: Seja G e H grupos, e $f: G \to H$ um homomorfismo, então, definimos o núcleo de f, denotado por $N(f)$, conforme:

$$N(f) = \{x \in G \,/\, f(x) = e_H\}$$

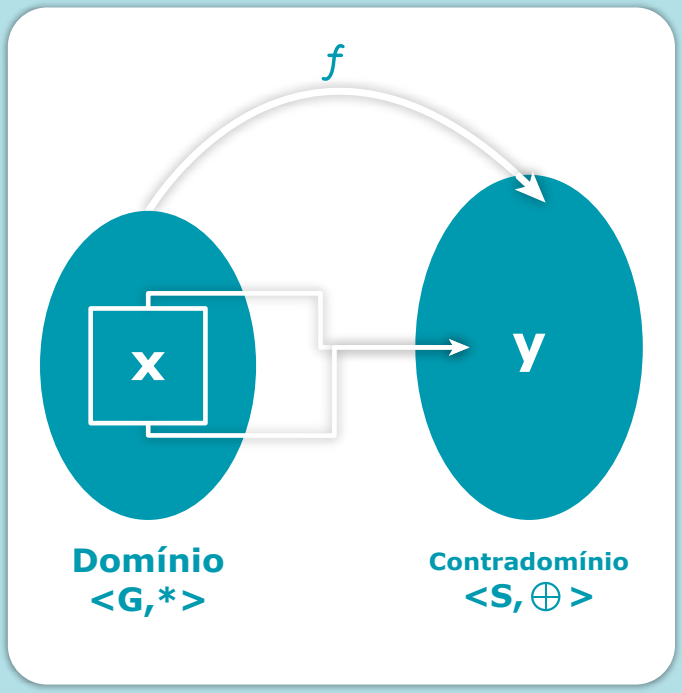

Figura 3: *Núcleo de um homomorfismo.* ***Fonte:*** *Elaboração Própria.*

Exemplo 26: Seja $\theta: Z \to Z$, definida por $\theta(x) = 3x, \forall x \in Z$, é um homomorfismo.

Resolução: Usando a definição, precisamos encontrar um valor para a função que seja o elemento neutro da função e esse será o núcleo. Sendo assim,

$$N(\theta) = \{x \in Z \,/\, \theta(x) = 0 = \{x \in Z \,/\, 3x = 0\} = \{0\}$$

Definição: Seja $f: G \to H$ um homomorfismo, então:

1. $N(f)$ é um semigrupo de G.
2. f é injetora se, e somente se, $N(f) = \{e_G\}$.

Exemplo 27: Conforme o Exemplo 24, observamos que a aplicação $\theta: Z \to Z$, definida por $\theta(x) = 3x, \forall x \in Z$, é um homomorfismo, cujo núcleo é $N(f) = \{0\}$. Essa função será injetiva.

Resolução: Usando as definições, podemos observar que, quando a aplicação é um homomorfismo com núcleo $N(f) = \{0\}$, temos que a função será injetiva, ou seja, para cada elemento do domínio, temos apenas uma indicação no contradomínio.

Podcast 2

CONSIDERAÇÕES FINAIS

Neste módulo, apresentamos a álgebra para que se possa utilizá-la em programações, ao lançar mão do que foi exposto da matemática pura, ou seja, o motivo das definições matemáticas. Um programa bem estruturado e com menos rodeios tem um custo computacional muito menor do que programas com vários ifs.

Quanto mais uso de álgebra pura em seus problemas do dia a dia, mais bem estruturado ficará suas programações, portanto, recomendamos o bom uso dessas informações na carreira profissional.

SÍNTESE

FUNDAMENTOS MATEMÁTICOS DA COMPUTAÇÃO

Neste módulo, abordamos a álgebra e os elementos algébricos. Em seguida, passamos pela matemática pura a fim de compreender quais são as características de regras de **funções, relações, núcleo e imagem** de uma **função**. Dessa forma, estudamos os seguintes tópicos:

- **Indução.**
- **Recursão.**
- **Funções Definidas Recursivamente.**
- **Algoritmos Definidos Recursivamente.**
- **Grupos e Semigrupos.**
- **Homomorfismo de Grupos e Aplicações.**

Referências Bibliográficas & Consultadas

DAGHLIAN, J. **Lógica e álgebra de boole**. 4. ed. São Paulo: Atlas, 2011 [Minha Biblioteca].

GERSTING, J. **Fundamentos matemáticos para a ciência da computação:** um tratamento moderno de matemática discreta. 7. ed. Rio de Janeiro: LTC, 2004 [Minha Biblioteca].

MENEZES, P. B. **Matemática discreta para computação e informática.** Porto Alegre: Sagra Luzzatto, 2005.

PAIL, D. B.; TRAMUNT, A. I. **Fundamentos Linguísticos e Computação**. Porto Alegre: EdiPUCRS, 2015 [Biblioteca Virtual].

PANONCELI, D. M. **Análise Matemática.** São Paulo. Editora InterSaberes, 2017 [Biblioteca Virtual].

ROSEN, Kenneth H. **Matemática Discreta e suas Aplicações**.6. ed. Porto Alegre: AMGH. 2010.

SIMÕES-PEREIRA, J.M.S. **Grafos e redes: teoria e algoritmos básicos**. Rio de Janeiro: Editora Rio de Janeiro, 2013 [Biblioteca Virtual].

STEIN, C.; DRYSDALE, R. L.; BOGART, K. **Matemática Discreta para ciência da computação**. São Paulo: Pearson Education do Brasil, 2013 [Biblioteca virtual].

TOCCI, R. J.; WIDMER, N. S.; MOSS, G. L**. Sistemas digitais: princípios e aplicações**. 11. ed. São Paulo: Pearson Prentice Hall, 2011 [Biblioteca Virtual].

WEBER, R. F. **Fundamentos de** arquitetura de computadores. 4. ed. Porto Alegre: Bookman, 2012 [Minha Biblioteca].


fam
ONLINE