MATEMÁTICA DISCRETA

UNITAU digital

ANA CLARA DA MOTA

Ana Clara da Mota

Matemática Discreta

Taubaté 2022

Unitau-Reitoria
Rua Quatro de Março,432, Centro
Taubaté – São Paulo. CEP:12.020-270
Central de Atendimento:0800557255

Polo Taubaté – Sede
Rua Conselheiro Moreira de Barros, 203 - Centro
Taubaté – São Paulo. CEP:12.010-080
Telefones: Coordenação Geral: (12) 3621-1530
Secretaria: (12) 3622-6050

edUNITAU

EXPEDIENTE EDITORA

Sistema Integrado de Bibliotecas - SIBi/ UNITAU
Grupo Especial de Tratamento da Informação – GETI

M917m Mota, Ana Clara da
Matemática discreta [recurso eletrônico] / Ana Clara da Mota. – Dados eletrônicos. -- Taubaté : EdUnitau, 2022.

Formato: PDF
Requisitos do sistema: Adobe
Modo de acesso: world wide web

ISBN: 978-65-86914-56-6 (on-line)

1. Método indutivo. 2. Teoria dos números. 3. Conjunto. 4. Análise combinatória. 5. Funções. I. Título.

CDD – 511

Ficha catalográfica elaborada pela Bibliotecária Ana Beatriz Ramos – CRB-8/6318

Índice para Catálogo sistemático

Método indutivo – 511
Teoria dos números – 511
Conjunto – 511
Análise combinatória – 512
Funções – 512

Sumário

Recursos de Imersão:

Explorando ideias

Eu indico

Pensando juntos

Pípulas de conhecimento

Podcast

QRCode

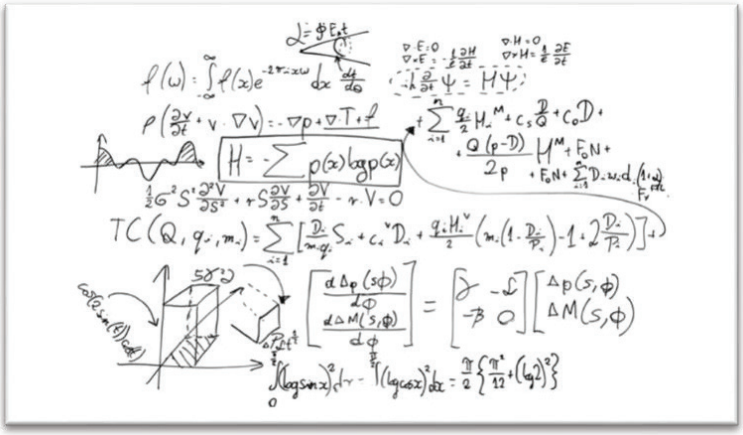
Matemática Discreta

Unidade I

Princípio da Indução Matemática

Nesta Unidade, você aprenderá a fazer demonstrações pelo método de indução matemática. Também estudará sobre os principais conceitos de Indução Matemática, o Princípio da Indução Finita, o axioma de Peano e sua importante utilização em demonstrações relativas a proposições dos números naturais. Para realizar esse estudo, terá acesso à fundamentação teórica que explica os mecanismos utilizados na prática.

Introdução



Nesta Unidade, você estudará o Princípio da Indução Matemática, um axioma empregado para a validação de resultados matemáticos que envolvem o conjunto dos números naturais e seus subconjuntos infinitos.

Para isso, os conceitos abordados serão os seguintes:

a) Principais conceitos de Indução Matemática;

b) O Princípio da Indução Finita;

c) O Axioma de Peano e a importante utilização desse axioma em demonstrações relativas a proposições dos números naturais.

Um tipo de pergunta que os conteúdos a serem estudados tentam responder é a seguinte: "Como podemos ter certeza da validade de certa propriedade para todos os números naturais?".

Na área da informática, conhecer sobre o Princípio da Indução Matemática pode ser importante ao realizar tarefas como provar que uma proposição vale para um grande número de casos, além de ajudar a compreender a noção do infinito em Matemática, crucial para o campo das tecnologias digitais.

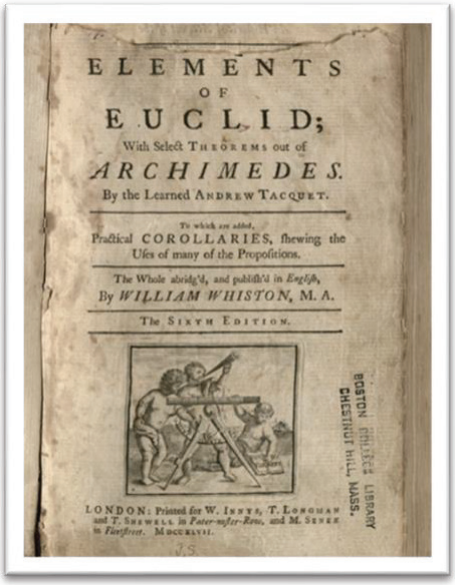
Por isso, dedique-se ao máximo, estude com afinco, acesse as atividades e os materiais complementares. Tudo isso ajudará você a construir os saberes necessários para consolidar seus conhecimentos em torno do Princípio da Indução Matemática.

VOCÊ SABE O QUE SÃO AXIOMAS?

São proposições aceitas como verdadeiras, sem demonstrações, e que servem de base para uma teoria.

Para se aprofundar mais em relação aos axiomas, acesse:
https://super.abril.com.br/mundo-estranho/qual-a-diferenca-entre-axioma-teoria-e-teorema/

1.1 Conceitos de Indução Finita



Os gregos foram os primeiros a utilizar as demonstrações matemáticas. Euclides (360 a.C./295 a.C.) e seu texto *Elementos*[1] exerceram papel importante no campo da ciência, por causa do desenvolvimento do método axiomático.

Atualmente, as demonstrações são, em sua maioria, postas de lado, e os resultados matemáticos costumam ser exibidos como verdades absolutas, sem questionamentos. Em alguns casos, as fórmulas são realizadas apenas por meio de deduções empíricas, ou seja, sem a realização de experimentos ou de outras formas de comprovação de resultados.

Assim, podemos nos perguntar: como podemos ter certeza da validade de certa propriedade em relação a todos os números naturais?

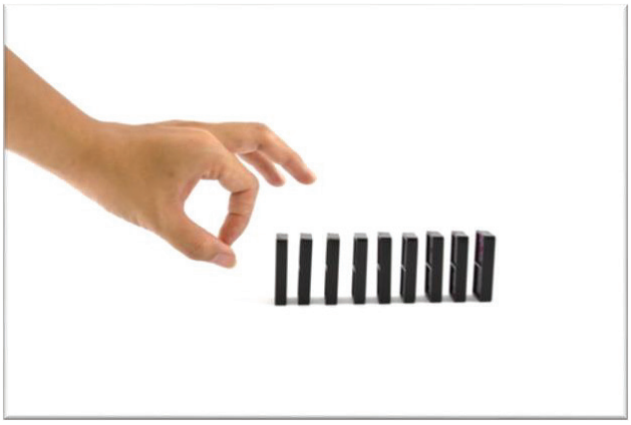
É bastante comum que utilizemos fórmulas como: "Se vale para ***e***, então, intuitivamente, vale para o todo.". Como você vai estudar nesta Unidade, em vários desses casos, o Princípio da Indução poderá ser aplicado.

O Princípio da Indução é um axioma e se configura como uma ferramenta de demonstração. Nesta Unidade, o objetivo é fundamentar teoricamente o Princípio da Indução e, principalmente, explorar a aplicação nas demonstrações relativas a proposições indexadas pelos números naturais.

Para saber mais sobre Euclides e a obra *Elementos*, acesse:

https://matematica.br/historia/euclides.html

[1] A imagem de reprodução do livro Elementos, de Euclides, que você vê nesta página, foi adaptada e está disponível em: https://www.maa.org/press/periodicals/convergence/mathematical-treasure-tacquets-euclid-and-archimedes. Acesso em: mar. 2021.



Você já deve ter ouvido falar em recordistas mundiais na categoria dominós enfileirados e derrubados por grupo, não é? Então, essa prática traduz, em essência, a ideia do Princípio da Indução Finita. A expressão "efeito dominó", comumente utilizada na Língua Portuguesa, apropria-se bem do significado do funcionamento da Indução Finita.

Imagine um modelo ideal de enfileiramento de dominós e pense que eles estão em um número infinito.

Nesse modelo, os dominós estão, entre si, a uma distância tal que, se um deles cai para frente, então, necessariamente derruba o seguinte.

Assim, se o primeiro dominó fosse derrubado, o que aconteceria?

Sem considerar o tempo que seria necessário para derrubar todos os dominós, a resposta a essa pergunta é bem intuitiva: todos os outros dominós cairiam também. Afinal, se supormos que um determinado dominó ficaria de pé, digamos o de posição k, $k \in Z$ e $k > 1$, teríamos que o dominó imediatamente anterior a este, o de posição k - 1, também teria ficado de pé, pois, se tivesse caído, por hipótese, derrubaria o de posição k que está logo à frente.

Procedendo assim, suficientemente e reiteradas vezes, concluiríamos que o primeiro dominó não teria sido derrubado, chegando, portanto, a um absurdo!

As reflexões sobre os dominós nos colocam diante do fato de que não podemos supor que algum dominó vai ficar de pé. Isso porque duas condições foram respeitadas: a primeira é a de que o dominó de posição $k = 1$ é derrubado, e a segunda é a de que, se um dominó cai, então, derruba o da frente.

Repare que as duas condições são igualmente necessárias, uma vez que, se apenas a primeira fosse verdadeira, nada nos garantiria que os demais dominós cairiam. E se somente a segunda fosse verdadeira, o processo de queda dos dominós poderia jamais iniciar.

O Princípio de Indução Matemática se assemelha ao raciocínio sobre os dominós, pois tem como objetivo provar que determinado resultado vale para todos os números naturais, ou para todos os naturais a partir de certo número dado.

Como já dito neste item, a ideia do enfileiramento de dominós revela a essência do Princípio da Indução Matemática. Vamos agora às formalidades.

1.2 A Generalização do primeiro princípio da indução

Antes de iniciarmos o tópico, é importante explicar que o que fazemos ao empregar o Princípio da Indução é aplicar um método chamado Método Indutivo à Indução Matemática, como um método dedutivo para demonstração de fatos sobre números naturais.

Há uma forma mais geral de apresentar o Primeiro Princípio da Indução.

Essa forma é importante, pois alguns problemas são provados somente para naturais a partir de certo ponto.

Seja P(n) uma proposição relativa a números naturais. Suponha que:

i. P(a) é verdadeira, e
ii. Se P(n) é verdadeira, para algum n, segue-se que P(n+1) também é verdadeira.

Então, P(n) é verdadeira para todos os números naturais iguais a ou maiores do que a.

Vejamos o problema abaixo:

Problema 1

Prove que $\forall n \geq 3, 2n + 1 < 2^n$

Demonstração:

a) Vejamos se a proposição P(a) é verdadeira nesse caso.
Substituindo o valor 3 na proposição, teremos: P(3): 2.3+1=7, que é menor do que $8=2^3$, que é verdadeira.

Segunda proposição:

b) Suponha que para algum n, P(n) é verdadeira.
Para (n+1), teremos a seguinte situação: $2(n+1) + 1 < 2^{n+1} \rightarrow 2(n+1) +1 < 2^n.2$.
(pelo problema: $2n + 1 < 2^n$, então, no lugar do 2n+1, substituiremos por 2^n);
então: $2^n + 2 < 2^n.2 = 2^{n+1}$.

Conclui-se, portanto, que P(n+1) é verdadeira.

Assim, por indução, a proposição está demonstrada.

1.3 Os axiomas de Peano

Enunciaremos, a seguir, os axiomas de Peano.

Foi o matemático italiano Giussepe Peano (1858-1932) que introduziu, pela primeira vez, os axiomas que caracterizam os números naturais e que levam o nome dele: os axiomas de Peano. Esses axiomas são os pilares de toda teoria dos números naturais.

O axioma, quando enunciado sob a forma de proposições, constitui a ferramenta para demonstrações relativas a números naturais. Demonstrações que se utilizam desse axioma são denominadas **Provas por Indução Finita** ou, simplesmente, **Provas por Indução.**

Considere primitivamente, isto é, sem a necessidade de ter definição, um conjunto N cujos elementos n são chamados de números naturais, e uma função chamada sucessor:

s: N → N, que leva n em (n + 1) denominado o sucessor de n.

A função sucessora satisfaz os seguintes axiomas:

i) s é injetiva – Se a ≠ b, então s(a) ≠ s(b) (números naturais distintos têm sucessores distintos);

ii) N – s(N) é um conjunto unitário (existe um único número natural, representado pelo símbolo 1, que não é sucessor de nenhum outro número natural);

iii) (Axioma da Indução) Se A ⊂ N, 1 ∈ A e $\forall a \in A$, ocorre também $a + 1 \in A$, então A = N (se um subconjunto tem o número 1 e tem a propriedade de possuir o sucessor de todos os elementos, então ele é o próprio N).

A partir daqui, vamos considerar que é sabido o que é um número natural, assim como as operações e as propriedades básicas, além da notação simbólica dos próprios elementos N={1, 2, 3, 4, 5, ...}.

Antes de enunciarmos o axioma (iii), em termos de proposições, vamos deixar bem claro o que é uma proposição relativa a números naturais e dar alguns exemplos.

Uma proposição ou sentença aberta P(n), que depende da variável n, é uma afirmação que pode ser verdadeira ou falsa toda vez que substituímos n por algum número natural.

Vejamos o exemplo de proposição em N:

Agora, o terceiro axioma de Peano pode também ser enunciado como a seguir.

Primeiro Princípio da Indução

Seja P(n) uma proposição relativa a números naturais.

Suponha que:

i. P(1) é verdadeira, e

ii. Se P(n) é verdadeira, para algum n, segue-se que P(n+1) também é verdadeira.

Então P(n) é verdadeira para todos os números naturais.

A fim de entendermos a equivalência entre essa forma de enunciado e a anterior, pense numa proposição P(n) com as características (i) e (ii) acima e tome o conjunto Y= {n; P(n) é verdadeira} $\subset N$.

Como P(1) é verdadeira, por (i), segue que 1A.

Por (ii), conclui-se, de imediato, que Y tem o sucessor de todos os seus elementos. Logo, Y = N.

Vejamos, agora, uma demonstração por indução.

Problema

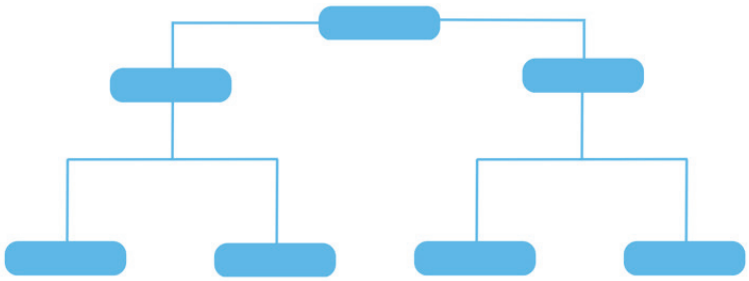
A árvore genealógica da família Pedrosa tem um aspecto bem singular. Cada pessoa tem sempre dois descendentes, e cada um dos dois descendentes tem sempre dois descendentes também, e assim sucessivamente.
Quantos descendentes terá a 3ª geração da família Pedrosa?
E a enésima geração?

Solução

Determinar o número de descendentes da 3ª geração é simples. Pode-se montar um gráfico, como a seguir, e se contarmos o número de descendentes de cada geração, teremos uma solução investigativa. Já para a segunda pergunta, a história é outra, não dá para simplesmente contar o número de descendentes, pois a pergunta exige uma resposta literal.

Veja, a seguir, as representações com resultados.

Figura 1 - Descendentes da 3ª geração da Família Pedrosa.



Fonte: elaborado pela autora, 2021.

Tabela1 - Descendentes da 3ª geração família Pedrosa.

GERAÇÃO	NÚMERO DE DESCENDENTES
Primeira	$2= 2^1$
Segunda	$4=2^2$
Terceira	$8=2^3$
.....	(...)

Fonte: elaborada pela autora, 2021.

A terceira geração terá oito descendentes.

Quanto à segunda pergunta, temos uma hipótese para a resposta: na enésima geração, teremos 2^n descendentes. Entretanto, isso tem que ser provado!

Então, faremos a demonstração por indução:

i. P(1) significa que a 1ª geração tem dois descendentes, o que é verdade, como se observa na Figura 1.

ii. Suponha que, para algum n, P(n) é verdadeira, isto é, a enésima geração tem 2n descendentes. Como, por hipótese, cada indivíduo tem sempre dois filhos, e uma geração qualquer sempre terá o dobro de indivíduos da geração anterior.

Logo, a geração de ordem (n+1) terá 2.2n = 2n+1 elementos.

Conclui-se, portanto, que P(n+1) é verdadeira e, assim, por indução, a proposição vale para qualquer número natural, o que significa que a enésima geração da família Pedrosa terá 2^n descendentes.

1.4 Aprendendo

Apresentamos alguns exemplos referentes à Unidade I.

Aproveite para refazê-los.

1. Qual será a soma dos n primeiros números naturais, ou seja, o valor da soma 1+2+3+4+5+ ...+ n é $\frac{n(n+1)}{2}$?

Solução: para termos a garantia desse resultado, precisamos usar o Princípio da Indução Finita.

Para isso, faremos os seguintes passos:

Passo 1 - Base de Indução (BI): para n = 1 é óbvio que 1 = 1(1 + 1)/2 .

Passo 2 - Hipótese de Indução (HI): suponha que o resultado vale para k > 1.

Passo 3 - Passagem de Indução (PI): devemos mostrar a validade do resultado para k + 1:

De fato, $1+2+3+\cdots+k+(k+1), \text{``}+(k+1) \overset{HI}{\Leftrightarrow} \frac{k(k+1)}{2}+(k+1)=\frac{k(k+1)+2(k+1)}{2}=\frac{(k+1)(k+2)}{2}=\frac{(k+1)(k+1)+1}{2}$, como queríamos mostrar.

Fique atento

Fique Atento: esse exemplo pode ser usado para obter a fórmula da soma dos n primeiros termos de uma progressão aritmética.

2. Prove que $1+3+5+\cdots+(2n-1)=n^2$, para todo $n \geq 1$.

Solução (utilizamos o Princípio da Indução para provar):

Passo 1 (BI): para n = 1 é obvio que vale, pois $1=1^2$.

Passo 2 (HI): supõe que o resultado vale para k≥ 1; então: $1 + 3+ 5 + ...+ (2k-1)=k^2$.

Passo 3 (PI): para (k + 1) $1 + 3 + 5 + ...+ (2k – 1) + [2(k+1) -1] \overset{HI}{\Leftrightarrow} k^2 + 2k + 1 = (k+1)^2$, como queríamos demonstrar.

3. Prove, por indução em n, que $2^{2n} - 1=4^n - 1$ é divisível por 3, para todo n ≥ 1.

Solução (utilizamos o Princípio da Indução para provar):

Passo 1 (BI): para n=1 é claro que vale, pois $2^{2.1}-1 = 4^1-1 \rightarrow 2^2-1=4-1 \rightarrow 3 = 3$ é divisível por 3.

Passo 2 (HI): supõe que é verdade para k ≥ 1; então: $4^k-1=3m$, com m inteiro. Assim, $4^k = 3m + 1$.

Passo 3 (PI): para k+1 temos que $4^{k+1}- 1= 4.4^k-1 \overset{HI}{\Leftrightarrow} 4 (3m + 1) – 1 = 3(4m+1)$, como queríamos demonstrar.

4. Prove que a soma das medidas dos ângulos internos de um polígono convexo de n lados é igual a (n - 2) 180º.

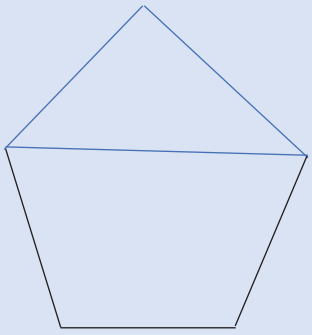
Solução (utilizamos o Princípio da Indução para provar):

Passo 1 (BI): para n = 3 vale o resultado, pois a soma dos ângulos internos de um triângulo é 180º = (3 - 2)180º.

Passo 2 (HI): supõe que a soma dos ângulos interno de um polígono convexo de l dados.

Passo 3 (PI): para l + 1, podemos decompor o polígono em dois: um com l lados e um triângulo, conforme figura abaixo:

Figura 3 — Decomposição de Polígono.



Fonte: elaborado pela autora, 2021.

Portanto. a soma dos ângulos internos de um polígono de l + 1 lados será igual a (l - 2)180º + 180º = (l + 1 - 2)180º.

5. Prove, por indução matemática, $2\ 1 + 2\ 2 + 2\ 3 + \ldots + 2n = n^2 + n$, para todo $n \geq 1$.

Solução:

Passo 1 (BI): para n = 1, 21 = 2 e $1^2 + 1 = 2$. O passo BI é verdadeiro.

Passo 2 (HI): se a fórmula é verdadeira para n = k, $k \geq 1$, então deve ser verdadeira para n = k+1.

Hipótese indutiva: $2\ 1 + 2\ 2 + 2\ 3 + \ldots + 2k = k^2 + k$

$= k(k + 1), k \geq 1.$

Passo 3 (PI): deve-se mostrar que: $2\ 1 + 2\ 2 + \ldots + 2k + 2(k + 1) = (k + 1)^2 + (k + 1)$

$= (k + 1)[(k + 1) + 1]$

$= (k + 1)(k + 2), k \geq 1.$

Sabe-se que:

$2\ 1 + 2\ 2 + \ldots + 2k + 2(k + 1) = k(k + 1) + 2(k + 1)$

$= k^2 + k + 2k + 2$

$= k^2 + 3k + 2$

$= (k + 1)(k + 2).$

6. Use a indução matemática para provar que a soma dos primeiros inteiros positivos ímpares é n^2.

Solução:

Seja P(n): podemos pensar na seguinte sentença: "A soma dos primeiros ímpares é n^2" ou: "$1 + 3 + 5 + \cdots + (2n - 1) = n^2$".

Passo1 (BI): comprovar P(1).

P(1) estabelece que $1 = 1^2$, o que é Verdadeiro.

Passo 2 (HI): mostrar que $P(k) \rightarrow P(k + 1)$ é Verdadeiro.

Suponha que P(k) é Verdadeiro para um k fixo, ou seja:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2 .$$

A partir disso, pensamos no Passo 3 (PI): queremos provar que P(k + 1) é Verdadeiro, ou seja:

$$1 + 3 + 5 + \cdots + (2k - 1) + [2(k + 1) - 1] = (k + 1)^2.$$

Uma vez que P(k) é Verdadeiro, o lado esquerdo acima fica:

$$k^2 + [2(k + 1) - 1] = k^2 + (2k + 2 - 1)$$
$$= k^2 + 2k + 1$$
$$= (k + 1)^2$$

Isso mostra que, efetivamente, P(k + 1) segue de P(k).

Assim, uma vez que P(1) e P(k) → P(k + 1) são Verdadeiras, independentemente da escolha de k, concluímos que é Verdade a proposição: ∀n P(n).

7. O número n·(n+1)·(n+2) é divisível por 6 para qualquer n∈N.

Solução:

Passo 1 (BI): verificaremos que a propriedade é válida para n_o=0.

0·(0+1)·(0+2)=0·1·2=0, logo o 0 é divisível por 6.

Passo 2 (HI): vamos assumir que o número n·(n+1)·(n+2) é divisível por 6 (vamos demonstrar que a propriedade é válida para n+1).

(n+1)(n+1+1)(n+1+2)

=(n+1)(n+2)(n+3)

A estratégia, nesse passo 3, sempre é a de encontrar a expressão do passo 2.

Então, vamos distribuir as multiplicações e ver se a encontramos:

(n+1)(n+2)(n+3)=

$=(n^2+2n+n+2)(n+3)=$

$=(n^2+3n+2)(n+3)=$

$=n^3+3n^2+3n^2+9n+2n+6=$

$=n^3+6n^2+11n+6$

O que, porém, essa expressão tem a ver com a do Passo 2?

Vamos voltar e distribui-la também para descobrir:

n·(n+1)·(n+2)=

$=n(n^2+2n+n+2)=$

$=n(n^2+2n+n+2)=$

$=n^3+3n^2+2n$

Ou seja, podemos separar a expressão do Passo 3 da seguinte forma:

$n^3+6n^2+11n+6=$

$=(n^3+3n^2+2n)+(3n^2+9n+6)=$

$=(n^3+3n^2+2n)+3(n^2+3n+2)$

Vamos fatorar de volta a parte $3(n^2+3n+2)$:

$(n^3+3n^2+2n)+3(n+1)(n+2)$

A parte (n^3+3n^2+2n) é divisível por 6, pois é consequência direta do Passo 2. E vemos que a parte $3(n+1)(n+2)$ também é, pois já é múltipla de 3; e se $(n+1)$ não for um número par, então $(n+2)$ é par.

Então, demonstramos que a propriedade também é válida para n+1 e, portanto, a hipótese inicial é válida.

Observemos, portanto, que há várias formas de pensar em provar sentenças em diversos conceitos matemáticos, utilizando o Princípio da Indução.

1.6 Síntese da Unidade

Nesta Unidade, estudamos o **Princípio da Indução Matemática** como ferramenta matemática de demonstração/prova de resultados.

Para isso, estudamos, em primeiro lugar, a fundamentação teórica sobre o tema, destacando, principalmente, o Método Indutivo aplicado a proposições indexadas pelos números naturais.

Vimos que esse Método permite a realização de uma experiência matemática completa, quanto à solução de problemas indutivos, uma vez que, realizada a investigação matemática e conjecturado determinado resultado, o passo final pode ser dado, comprovando-se o resultado, via indução, e reduzindo a zero qualquer dúvida a seu respeito.

Essa completude que a demonstração por Indução garante pode contribuir para a aquisição de significados matemáticos mais sólidos.

1.7 Para saber mais

Artigos científicos

LIMA, E. L. Indução Matemática – **Revista Eureka**. Disponível em: www.obm.org.br/export/sites/default/revista_eureka/.../inducao.doc. Acesso em: 08 jan. 2021.

HEFEZ, A**. Indução Matemática**. Obmep. Disponível em: http://server22.obmep.org.br:8080/media/servicos/recursos/296654.o. Acesso em: 08 jan. 2021.

Livro

HEFEZ, A. **Elementos de Aritmética**. São Paulo: SBM, 2011.

Unidade II

Teoria dos Números

Nesta Unidade, você estudará os tipos de dados e as instruções de entrada e saída em linguagem C; também poderá observar a contextualização dos processos de seleção e/ou tomada de decisão, durante a solução de um problema, e as estruturas de decisão, baseadas em um teste de condição (se ... então ... senão...), assim como as estruturas de decisão que dependem do valor de uma variável ou expressão (caso ...faça) e as estruturas de seleção/decisão em linguagem C.

Introdução

Fonte: br.freepik.com

Nesta Unidade, você conhecerá a Teoria dos Números, responsável por estudar as características e aplicações do que chamamos Números Inteiros, ou seja, dos números que não representam frações. Para isso, os conceitos que serão abordados são os seguintes: a) conjunto dos números inteiros, b) propriedades dos números inteiros, c) divisibilidade e números inteiros, d) números primos; e) Máximo divisor comum; f) Algoritmo de Euclides para o MDC e, por fim, g) Teorema Fundamental da Aritmética.

Certamente, você já estudou alguns desses conceitos ao longo de sua vida escolar. Assim, muitos dos temas aqui serão mais uma retomada do que a introdução de um novo conceito. Entendemos que essa retomada é bastante necessária para que a continuidade dos estudos neste curso possa se dar satisfatoriamente, por isso, dedique-se bastante à aprendizagem/retomada desses conceitos.

Estamos certos de que esses conceitos são muito importantes para a formação do(a) profissional da área da Tecnologia.

Não deixe de consultar as indicações de leitura e de outros materiais que aparecem ao longo do texto, pois são indicações selecionadas para que seu estudo seja ampliado e aprofundado.

2.1 A Teoria dos Números

Fonte: canva.com

A Teoria dos Números nasceu cerca de 600 anos antes de Cristo, quando Pitágoras e os seus discípulos começaram a estudar as propriedades dos números inteiros. Os pitagóricos realizavam verdadeiro culto místico ao conceito de número, considerando-o como essência das coisas. Acreditavam que tudo no universo estava relacionado com números inteiros ou com razões de números inteiros (em linguagem atual, números racionais). Na Antiguidade, a designação "número" aplicava- se somente aos inteiros maiores do que um.

O conceito de número tomou forma num longo desenvolvimento histórico. A origem e a formulação desse conceito ocorreram simultaneamente ao nascimento e ao desenvolvimento da Matemática. As atividades práticas do homem, por um lado, e as exigências internas da Matemática, por outro, determinaram o desenvolvimento do conceito de número.

A necessidade de contar objetos fez surgir o conceito de número Natural. Todas as nações que desenvolveram formas de escrita introduziram o conceito de número Natural e desenvolveram o sistema de contagem. O desenvolvimento subsequente do conceito de número prosseguiu, principalmente, devido ao próprio desenvolvimento da Matemática.

Os números negativos aparecem pela primeira vez na China antiga. No entanto, não aceitavam a ideia de um número negativo poder ser solução de uma equação.

As regras sobre grandezas eram já conhecidas através dos teoremas gregos sobre subtração, como por exemplo $(a - b)(c - d) = ac + bd - ad - bc$, mas os hindus converteram-nas em regras numéricas sobre números negativos e positivos.

Diofanto (Séc. III) operou facilmente com os números negativos. Eles apareciam constantemente em cálculos intermédios em muitos problemas do seu "Aritmetika". No entanto, havia certos problemas para os quais as soluções eram valores inteiros negativos, como, por exemplo, $4x + 20 = 4$.

Nessas situações, Diofanto limitava-se a classificar o problema como absurdo. Nos séculos XVI e XVII, muitos matemáticos europeus não apreciavam os números negativos e, se esses números apareciam nos seus cálculos, eles consideravam-nos falsos ou impossíveis.

2.2 Os conjuntos dos números inteiros

Fonte: br.freepik.com

Um número inteiro é aquele que pode ser escrito sem um elemento decimal. Não fazem parte dos números inteiros: as frações, os números decimais, os números irracionais e os complexos. Assim, os números inteiros, também chamados apenas de "inteiros", são:

$$..., -3, -2, -1, 0, 1, 2, 3,...$$

O conjunto dos inteiros é representado pela letra Z, como podemos ver abaixo:

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

Nesse conjunto Z, destacam-se os seguintes subconjuntos:

1) Conjunto Z* dos inteiros não nulos (≠0): $Z^* = \{x \in Z / x \neq 0\} = \{\pm 1, \pm 2, \pm 3, \pm 4, ..\}$

2) Conjunto Z_+ dos inteiros não negativos (≥0): $Z_+ = \{x \in Z / x \geq 0\} = \{0, 1, 2, 3, 4, ...\}$

3) Conjunto Z_- dos inteiros não positivos (≤0): $Z_- = \{x \in Z / x \leq 0\} = \{0,-1,-2,-3, -4, ...\}$

4) Conjunto Z^*_+ dos inteiros positivos (> 0): $Z^*_+ = \{x \in Z / x > 0\} = \{1, 2, 3, 4, 5, ...\}$

5) Conjunto Z_-^* dos inteiros negativos (< 0): $Z_-^* = \{x \in Z / x < 0\} = \{-1, -2, -3, -4, ...\}$

Os inteiros positivos são também denominados inteiros naturais e, por isso, o conjunto dos inteiros positivos é habitualmente designado pela letra N ($N = * Z_+$).

2.2.1 Propriedades dos números inteiros

Fonte: br.freepik.com

O conjunto Z dos inteiros, munido das operações de adição (+) e de multiplicação (.), apresenta as propriedades fundamentais. Essas propriedades são apresentadas a seguir. Considere que a, b e c são inteiros quaisquer, isto é, elementos de Z:

1) $a + b = b + a$ e $ab = ba$; (comutatividade)

2) $(a + b) + c = a + (b + c)$ e $(ab)\, c = a\, (bc)$; (associatividade)

3) $0 + a = a$ e $1.a = a$; (elemento neutro)

4) $–a = (-1)\, a$ e $a – a = a + (-a) = 0$; (elemento oposto e inverso multiplicativo)

5) $a\, (b + c) = ab + ac$; (distributiva)

6) $0.a = 0$, e se $ab = 0$, então $a = 0$ ou $b = 0$.

Também existe uma "relação de ordem" entre os inteiros, representada pelo sinal "< (menor que)", que apresenta as seguintes propriedades:

7) Se $a \neq 0$, então $a > 0$ ou $a < 0$;

8) Se $a < b$ e $b < c$, então $a < c$;

9) Se $a < b$, então $a + c < b + c$;

10) Se $a < b$ e $0 < c$, então $ac < bc$;

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

Dessas propriedades, podem ser deduzidas muitas outras propriedades dos inteiros. Vamos ver alguns exemplos de aplicação dessas propriedades:

Exemplo 1: Demonstrar: $- (a + b) = (-a) + (-b)$

Exemplo 2: Demonstrar que, se $x \neq 0$, então $0 < x^2$.

Solução: Neste caso, temos sucessivamente:

$-(a + b) = (-1)(a + b) =$ (Propriedade 4)

$= (-1)a + (-1)b =$ (Propriedade 5)

$= (-a) + (-b)$ (Propriedade 4)

Solução

Suponha que

1) Se $x \neq 0$, então $x < 0$ ou $0 < x$ (Propriedade 7)

2) Se $x < 0$, então $0.x < x.x$ (Propriedade 11)

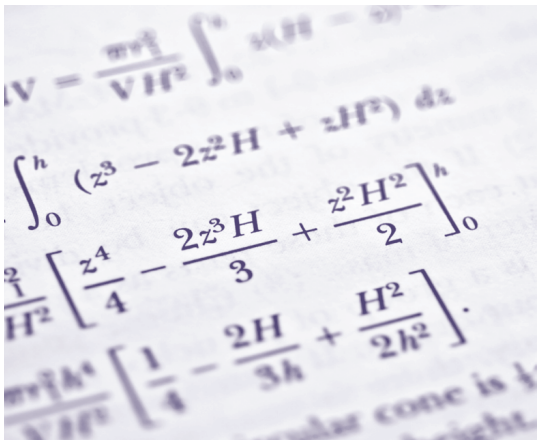
$0 < x^2$ (Propriedade 6)

3) Se $0 < x$, então $0.x < x.x$ (Propriedade 10)

$0 < x^2$ (Propriedade 6)

Observação: com o mesmo significado de $a < b$, escreve-se $b > a$. Indica-se, de modo abreviado, que $a < b$ ou $a = b$ por $a \leq b$. Por exemplo, temos $3 \leq 5$, porque $3 < 5$, e $3 \leq 3$, porque $3 = 3$. Com o mesmo significado de $a \leq b$, escreve-se $b \geq a$. Em lugar de $a \leq b$ e $b \leq c$ também se escreve $a \leq b \leq c$.

2.2.2 Teoria dos números e divisibilidade



Um conceito chave em Teoria dos Números é o conceito de divisibilidade. Existem muitos aspectos interessantes referentes à divisão de números inteiros. Antes que possam ser analisados, é necessário que conceitos básicos, como divisor e dividendo, estejam bem estabelecidos.

Fonte: canva.com

Definição: sejam a e b dois inteiros, com a ≠ 0. Diz-se que a divide b se, e somente se, existe um inteiro q tal que b = a.q.

Se a divide b, também se diz que a é divisor de b, que b é múltiplo de a, que a é um fator de b, ou que b é divisível por a.

Notação: a | b (a divide b)

Observação: se a | b, então - a | b

Teorema 1: quaisquer que sejam os inteiros a, b e c, tem-se:

1) a | 0 a 0, 1 | a e a | a a ≠ 0

2) Se a | 1, então a = 1

3) Se a | b e se c | d, então ac | bd

4) Se a | b e se b | c, então a | c

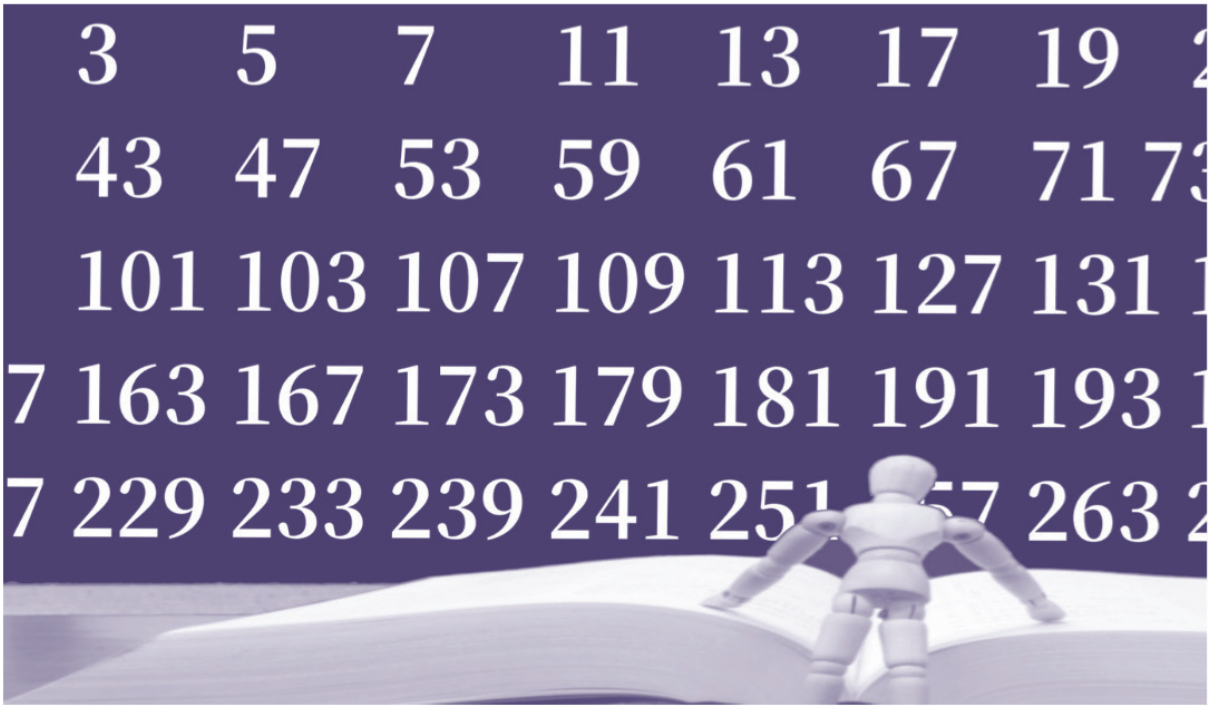
5) Se a | b e se b | a, então a = b

6) Se a | b com b ≠ 0, então | a | | b |

7) Se a | b e se a | c, então a | (bx + cy) para todo x e y em Z.

Teorema 2: se a e b são dois inteiros, com b > 0, então existem e são únicos os inteiros q e r que satisfazem às condições: a = bq + r e 0 ≤ r < b.

2.3 Números Primos



Fonte: canva.com

Definição 1: diz-se que um número positivo p > 1 é um número primo, ou apenas um primo, se, e somente se, 1 e p são seus únicos divisores positivos. De um inteiro maior do que 1 e que não é primo, diz-se composto.

Corolário 1: propriedade fundamental dos Números Primos. Se p é um primo tal que p | ab, então p | a ou p | b (podendo ser fator de ambos, a e b).

Observação: observe que esta propriedade necessária dos números primos é também suficiente para que um inteiro positivo n seja primo: pois, se n = k. s é composto (1< s≤ k < n) , temos n| k.s porém tanto n | k e n | s .

Corolário 2: Se p é um primo tal que p | $a_1a_2a_3$ ... a_n, então existe um índice k, com 1 ≤ k ≤ n tal que p | a_k.

Definição 2: Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ e $b \neq 0$). Diz-se que a e b são relativamente primos se, e somente se, o mdc (a,b) = 1.

Assim, por exemplo, são relativamente primos os inteiros: 2 e 5, -9 e 16, -27 e –35, pois, temos:

$$mdc(2,5) = mdc(-9,16) = mdc(-27,-35) = 1$$

Dois inteiros a e b relativamente primos admitem como **únicos divisores comuns 1 e –1**.

Teorema 3: Dois inteiros a e b, não conjuntamente nulos ($a \neq 0$ e $b \neq 0$), são primos entre si se, e somente se, existem inteiros x e y tais que ax + by = 1.

Demonstração:

(→) Se a e b são relativamente primos, então o mdc(a,b) = 1 e por conseguinte existem inteiros x e y tais que ax + by = 1.

(←) Reciprocamente, se existem inteiros x e y tais que ax + by = 1 e se o mdc(a,b) = d, então d | a e d | b. Logo, d | (ax + by) e d | 1, o que implica d = 1 ou mdc(a,b) =1, isto é, a e b são primos entre si.

Corolário 1: Se o mdc (a,b) = d, então o mdc (a/d , b/d) = 1.

Exemplo 1: mdc (-12,30) = 6 e mdc (-12/6 , 30/6) = mdc (-2,5) = 1.

Corolário 2: Se a | b e se o mdc (b,c) = 1, então o mdc (a, c) = 1.

Corolário 3: Se a | c, se b | c e se o mdc (a,b) = 1, então ab | c.

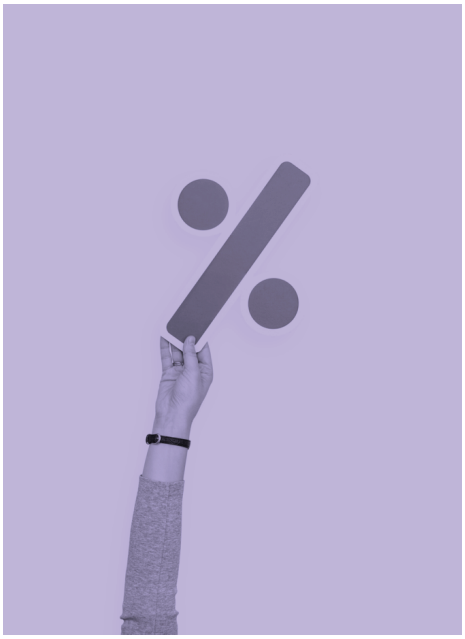
Observe-se que somente as condições a | c e b | c não implicam ab | c.

Assim, por exemplo, 6 | 24 e 8 | 24, mas 6.8 $\nmid$ 24 (o mdc (6,8) = 2 ≠ 1).

Corolário 4: Se mdc (a, b) = 1 = mdc (a, c), então o mdc (a, bc) = 1.

Corolário 5: Se o mdc (a, bc) = 1, então mdc (a, b) = 1 = mdc (a, c)

2.3.1 Máximo Divisor Comum



Fonte: br.freepik.com

Definição: sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se máximo divisor comum de a e b o inteiro positivo d ($d > 0$) que satisfaz às condições: 1) $d \mid a$ e $d \mid b$;

2) se $c \mid a$ e se $c \mid b$, então $c \leq d$.

Observe-se que, pela condição (1), d é um divisor comum de a e b, e pela condição (2), d é o maior dentre todos os divisores comuns de a e b.O máximo divisor comum de a e b indica-se pela notação mdc(a,b).

É imediato que o mdc(a,b) = mdc(b,a). Em particular:

(i) o mdc(0,0) não existe.

(ii) o mdc(a,1) = 1

(iii) se $a \neq 0$, então o mdc(a,0) = $|a|$

(iv) se $a \mid b$, então o mdc(a,b) = $|a|$

Assim, por exemplo:

mdc(8,1) = 1 mdc(-3,0) = $|-3| = 3$ mdc(-6,12) = $|-6| = 6$.

Exemplo 1: Sejam os inteiros a = 16 e b = 24. Os divisores comuns positivos de 16 e 24 são 1, 2, 4 e 8, e como o maior é 8, segue-se que o mdc (16,24) = 8.

Observa-se que mdc(-16,24) = mdc(16,-24) = mdc(-16,-24) = 8.

Exemplo 2: Sejam os inteiros a = -24 e b = 60. Os divisores comuns positivos de –24 e 60 são 1, 2, 3, 4, 6 e 12, e como o maior deles é 12, segue-se que o mdc (-24,60) = 12.

2.3.2 Algoritmo de Euclides para o MDC

Fonte: br.freepik.com

O livro VII, *Os Elementos de Euclides*, começa com o processo, hoje conhecido como algoritmo euclidiano, para achar o máximo divisor comum de dois ou mais números inteiros, e o usa para verificar se dois inteiros são primos entre si.

Começaremos com o seguinte lema:

Lema: Se a = bq + r, então o mdc(a,b) = mdc(b,r).

Demonstração:

Se o mdc(a,b) = d, então d | a e d | b, o que implica d | (a - bq) ou d | r, isto é, d é um divisor comum de b e r (d | b e d | r).

Por outro lado, se c é um divisor comum qualquer de b e r (c | b e c | r), então c | (bq + r) ou c | a, isto é, c é um divisor comum de a e b, o que implica c d. Assim sendo, o mdc(b,r) = d.

Algoritmo de Euclides

Fonte: br.freepik.com

Sejam a e b dois inteiros não conjuntamente nulos (a ≠ 0 ou b ≠ 0), cujo máximo divisor comum se deseja determinar. É imediato que:

(1) se a ≠ 0, então o mdc (a, 0) = | a |

(2) se a ≠ 0, então o mdc (a, a) = | a |

(3) se b | a, então o mdc (a, b) = | b |

Além disso, por ser mdc (a, b) = mdc (| a |, | b |), a determinação do mdc (a, b) reduz-se ao caso em que a e b são inteiros positivos distintos, por exemplo, com a > b, tais que b não divide a, isto é: a > b > 0 e b | a. Nessas condições, a aplicação repetida do algoritmo da divisão nos dará as igualdades:

$$a = bq_1 + r_1, 0 < r_1 < b$$

$$b = r_1q_2 + r_2, 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2$$

$$r_2 = r_3q_4 + r_4, 0 < r_4 < r_3 \text{ .....}$$

Como os restos r_1, r_2, r_3, r_4, ... são todos inteiros positivos tais que

$$b > r_1 > r_2 > r_3 > r_4 \text{ ....}$$

e existem apenas b – 1 inteiros positivos menores do que b, necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, isto é, finalmente, teremos:

$$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, r_{n-1} = 0$$

O último resto $r_n \neq 0$ que aparece nesta sequência de divisões é o máximo divisor comum procurado de a e b, isto é, o mdc (a,b) = r_n, visto que, pelo lema anterior, temos:

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \cdots = mdc(r_{n-2},r_{n-1}) = mdc(r_{n-1},r_n) = r_n$$

Esse processo prático para o cálculo do máximo divisor comum de dois inteiros positivos a e b é denominado Algoritmo de Euclides, ou processo das divisões sucessivas.

Geralmente, utilizamos o dispositivo prático no emprego do Algoritmo de Euclides, como podemos ver na tabela a seguir:

	q_1	q_2	q_3	....	q_n	q_{n-1}
a	b	r_1	r_2	...	r_{n-1}	r_n
$\mathbf{r_1}$	r_2	r_3	r_4	....	0	

Tabela 1: Algoritmo de Euclides

Que se traduz na seguinte REGRA:

Para se "achar" o mdc de dois inteiros positivos, divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente, até encontrar um resto nulo. O último resto não nulo é o máximo divisor comum procurado.

Exemplo: encontrar o mdc (963,657) pelo algoritmo de Euclides e a sua expressão como combinação linear de 963 e 657.

Solução:

Temos, sucessivamente:

963 = 657.1 + 306 657

= 306.2 + 45 306

= 45.6 + 36 45

= 36.1 + 9 36

= 9.4 + 0

	1	2	6	1	4
963	657	306	45	36	9
	306	45	36	9	0

Tabela 2: Algoritmo de Euclides

Portanto, o mdc (963,657) = 9 e a sua expressão como combinação linear de 963 e 657 se obtêm eliminando os restos 36, 45 e 306 entre as quatro primeiras igualdades anteriores, do seguinte modo:

9 = 45 – 36 = 45 – (306 – 45.6) =

= - 306 + 7.45 = - 306 + 7(657 – 306.2) =

= 7.657 – 15.306 = 7.657 – 15(963 – 657) =

= 963(-15) + 657.2

Isto é: 9 = mdc (963,657) = 963x + 657y onde x = -15 e y = 22.

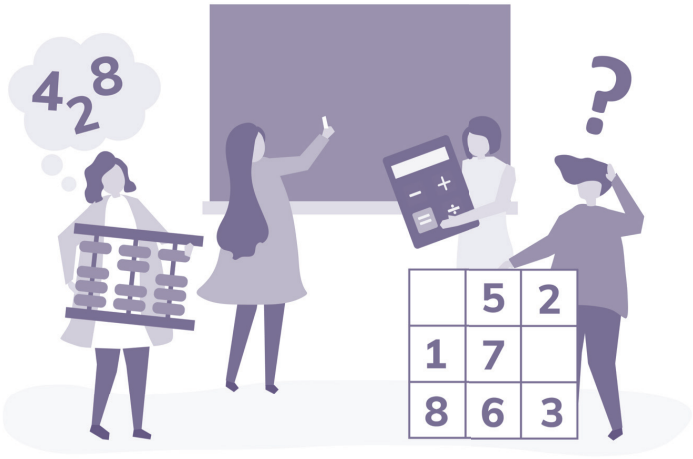
Essa representação do inteiro 9 = mdc (963,657) como combinação linear de 963 e 657 não é única.

Assim, por exemplo, somando e subtraindo o produto 963.657 ao segundo membro da igualdade: 9 = 963(-15) + 657.22; obtemos:

$$9 = 963(-15 + 657) + 657(22 - 963) = = 963.642 + 657(-941)$$

Essa é uma outra representação do inteiro 9 = mdc (963,657) como combinação linear de 963 e 657.

2.4 Teorema Fundamental da Aritmética



Fonte: br.freepik.com

Todo inteiro positivo n > 1 é igual a um produto de fatores primos.

Observação: esse teorema (como qualquer outro teorema chamado de "fundamental") não deveria ser aplicado sem a devida precaução. Existem inúmeros sistemas numéricos nos quais a fatoração não é única. Por exemplo, imagine um sistema que tenha apenas inteiros pares, com a adição e a multiplicação usual, e denominemos um número de

"e-primo", se ele não for o produto de dois outros números pares. Nesse caso, alguns "e-primos" são 2, 6, 10, 14, 18...

Observe que, nesse sistema, 36 tem duas fatorações diferentes: 6 x 6 e 2 x 18.

2.5 Síntese da Unidade

Nesta Unidade, vimos que qualquer número inteiro pode ser decomposto em fatores primos, que é um dos teoremas importantes da teoria dos números. Também vimos suas inúmeras aplicações.

Você aprendeu que esse teorema é conhecido como Teorema Fundamental da Aritmética, e trata-se do fato de que todo número composto pode ser escrito como produto de fatores primos.

Geralmente, aprendemos na escola um método para detectar os fatores primos de um número natural, que começa com a divisão do número pelo menor fator primo e o quociente dessa divisão pelo menor fator primo, e assim sucessivamente.

Em geral, a fatoração por primos não é uma tarefa fácil, por isso o algoritmo de Euclides é bem mais rápido para ser usado na computação manual. Outra consequência do teorema Fundamental da Aritmética é a possibilidade de achar o menor múltiplo comum a dois números inteiros positivos.

Tendo finalizado, então, esta Unidade, esperamos que você tenha compreendido e/ou relembrado conceitos fundamentais da Teoria dos Números, com a devida ênfase no Teorema Fundamental da Aritmética, de modo que esses saberes sirvam de subsídios para o estudo das próximas Unidades.

2.6 Para saber mais

Site

http://clubes.obmep.org.br/blog/teorema-fundamental-da-aritmetica/ Neste endereço, você acessa informações sobre o Teorema Fundamental da Aritmética, além de um

vídeo sobre o Teorema. Encontra, ainda, o algoritmo de Euclides para determinação do MDC.

Artigo

MAIER, R. R. **A teoria dos números**. Disponível em: https://www.mat.unb.br/~maierr/tnotas.pdf. Acesso em maio de 2021.

2.7 Praticando

Agora, é hora de praticar o que aprendemos sobre a Teoria dos Números. Vamos lá!

1. Em uma divisão inteira, o divisor é 12, o quociente é 5 e o resto é o maior possível. Qual é o dividendo?

2. Utilizando o algoritmo de Euclides, queremos saber o MDC de a = 600 e b = 252.

3. Explique:

a) O número 10 não é primo, por quê?

b) O número 5 é primo, por quê?

4. Agora vejamos a seguinte situação sobre divisão: queremos dividir por um número inteiro negativo. Por exemplo, se queremos saber o quociente e o resto da divisão inteira de 180 por −12, sabemos que 180 = (−1)15 (−1)12 + 0, sendo então o quociente de dividir 180 por −12 o número inteiro −15 e resto 0. A questão de o divisor ser um inteiro negativo foi resolvida. Agora a questão é... e se o dividendo for um número inteiro negativo? Como faremos? Explique utilizando o processo de divisão.

5. O número inteiro 26 é uma combinação linear de 6 e 10. Explique o porquê.

6. Mostre que 2 pode ser escrito como combinação linear de 6 e 10. A partir disso, mostre que todo número par pode ser expresso como combinação linear de 6 e 10.

7. Ache o quociente e resto da divisão inteira de 1.678 por −75.

Unidade III

Coleções e Relações

Nesta Unidade, você terá estudará sobre coleções e relações, conteúdos que abordarão os seguintes conceitos: definição de coleções, tipos de relações e relações de equivalência. Ainda em relação às coleções, abordaremos as ordenadas (listas) e as não ordenadas (conjuntos).

INTRODUÇÃO

Dando continuidade a nossos estudos, nesta unidade estudaremos sobre dois tipos de coleção: as ordenadas (listas) e as não ordenadas (conjuntos).

Para isso, abordaremos as definições desses conceitos, bem como realizaremos atividades práticas que reforcem a sua compreensão em relação ao funcionamento teórico-prático desses conceitos.

Ao final da Unidade, esperamos que você tenha se apropriado desses saberes e que se mostre capaz de concatená-los com os saberes já estudados até este momento, não apenas em nossa disciplina, mas no curso, como um todo.

Não deixe de consultar as indicações e sugestões que aparecem ao longo de todo a Unidade.

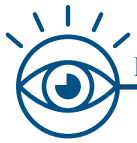
Bons estudos!

3.1 Conceituação de Coleções

3.1.1 Listas (ordenadas)

Uma lista é uma sequência ordenada de objetos.

Escrevemos uma lista abrindo um parêntese e apresentando, dentro do parêntese, os elementos da lista separados por vírgulas. Ao final, fecha-se o parêntese. Por exemplo: (1,2, Z) é uma lista cujo primeiro elemento é o número 1, o segundo elemento é o número 2 e o terceiro elemento é o conjunto dos inteiros.



Fique atento

A ordem em que os elementos figuram na lista é significativa. A lista (1, 2, 3) não é a mesma que a lista (3, 2, 1).

Uma lista pode conter elementos repetidos, como (3, 3, 2).

O número de elementos em uma lista é chamado de comprimento. Por exemplo, a lista (1, 1, 2, 1) tem comprimento quatro.

3.1.2. Contagem de listas de dois elementos

Uma lista de comprimento dois tem um nome especial: par ordenado.

Uma lista de comprimento zero é chamada lista vazia e se denota por ( ).

O que significa duas listas serem iguais?

Duas listas são iguais se tiveram o mesmo comprimento e se os elementos nas posições correspondentes nas duas listas forem iguais. As listas (a, b, c) e (t, y, z) são iguais se e somente se a = t, b = y e c = z.

Outra expressão que os matemáticos usam para listas é **upla.**

Uma lista de n elementos é conhecida como uma **n-upla (ênupla).** As listas estão presentes em toda a Matemática e além dela. Um ponto no plano costuma ser especificado por um par ordenado de números reais (x, y). Um número natural, quando escrito em notação-padrão, é

uma lista de algarismos. Podemos encarar o número 172 como a lista (1, 7, 2). Uma palavra é uma lista de letras. Um identificador em um programa de computador é uma lista de letras e algarismos (em que o primeiro elemento da lista é uma letra).

→ Agora, vamos abordar questões do tipo: "quantas listas podemos formar?"

Exemplo: suponha que estamos interessados em realizar uma lista de dois elementos, na qual os valores da lista podem ser quaisquer dos quatro algarismos 1, 2, 3 e 4. Quantas listas são possíveis?

A abordagem mais direta para responder a essa pergunta consiste em escrever todas as possibilidades.

(1, 1); (1, 2); (1, 3); (1, 4); (2, 1); (2, 2); (2, 3); (2, 4); (3, 1); (3, 2); (3, 3); (3, 4); (4, 1); (4, 2); (4, 3); (4, 4). Há 16 listas.

Generalizando um pouco mais esse exemplo, suponha que desejamos saber o número de listas de dois elementos em que há n escolhas possíveis para cada valor da lista. Pode-se admitir que os elementos possíveis fossem os inteiros de 1 a n. Como anteriormente, organizamos todas as listas possíveis em uma tabela, ou quadro.

(1, 1) (1, 2) ...(1, n)

(2, 1) (2, 2) ...(2, n)

.....

(n, 1) (n , 2) ... (n, n).

A primeira linha contém todas as listas que começam com 1; a segunda linha, as que começam com 2; e assim por diante. Há n linhas ao todo. Cada linha tem exatamente n listas. Há, pois, n x n = n^2 listas possíveis.

Quando uma lista é formada, as opções para a segunda posição podem ser diferentes das opções para a primeira posição.

Por exemplo, uma refeição como uma lista de dois elementos, consistindo em uma entrada e uma sobremesa. O número possível de entradas pode ser diferente do número de sobremesas. Então: quantas listas de dois elementos são possíveis quando há n escolhas para o primeiro elemento e m escolhas para o segundo elemento?

Suponha que os elementos possíveis na primeira posição da lista sejam os inteiros l a n, e que os elementos possíveis na segunda posição sejam os inteiros l a m.

Construímos uma tabela de todas as possibilidades como foi feito anteriormente:

(1, 1) (1, 2) ... (1, m)

(2, 1) (2, 2) ... (2, m)

.....

(n, 1) (n, 2) • (n, m).

Há n linhas (para cada primeira escolha possível), e cada linha contém m valores. Assim, o número possível de tais listas é m + m + ... + m = m x n.

Às vezes, os elementos de uma lista verificam propriedades especiais. Em particular, a escolha do segundo elemento pode depender de qual seja o primeiro elemento. Suponha, por exemplo, que se queira contar o número de listas diferentes de dois elementos que podemos formar com os inteiros 1 a 5, em que os dois números da lista devem ser diferentes.

Por hipótese, contaremos (3, 2) e (2, 5), mas não (4, 4). Escrevem-se todas as listas possíveis: (1, 2); (1, 3); (1, 4); (1, 5); (2, 1); (2, 3); (2, 4); (2, 5); (3, 1); (3, 2); (3, 4); (3, 5); (4, 1); (4, 2); (4, 3); (4, 5); (5, 1); (5, 2); (5, 3); (5, 4). Como no exemplo anterior, inicia-se com todas as listas possíveis que começam com 1; em seguida, as listas que começam com 2; e assim por diante, de modo que haja cinco linhas. Há, pois, cinco linhas. Note que cada linha contém exatamente 5-1= 4 listas. Assim, o número de listas é 5 x 4 = 20.

Teorema (Princípio da Multiplicação): considerem listas de dois elementos em que há n escolhas para o primeiro elemento e, para cada uma dessas escolhas, há m escolhas do segundo elemento. Então, o número de tais listas é n x m.

Exemplo 1: as iniciais de uma pessoa constituem uma lista formada pelas iniciais de seu primeiro e seu último nome. Por exemplo, as iniciais do autor são AM. De quantas maneiras podemos dispor as iniciais do nome de uma pessoa? De quantas maneiras podemos dispor essas iniciais de maneira que as letras sejam diferentes? A primeira questão pede o número de listas de dois elementos em que há 26 escolhas para cada elemento. Há 26^2 listas. A segunda questão pede o número de listas de dois elementos em que há 26 escolhas para o primeiro elemento e,

para cada uma dessas escolhas, 25 escolhas do segundo elemento. Há, pois, 26 x 25 de tais listas.

Exemplo 2: uma microempresa tem dez membros e deseja eleger um como presidente e um como vice-presidente. De quantas maneiras é possível preencher os dois postos? Podemos reformular esse exemplo como uma situação de contagem de lista: quantas listas de duas pessoas podemos formar, nas quais as duas pessoas na lista são escolhidas de uma coleção de dez candidatos, e a mesma pessoa não pode ser escolhida duas vezes? Há dez escolhas para o primeiro elemento da lista. Para cada escolha do primeiro elemento (para cada presidente), há nove escolhas possíveis para o segundo elemento da lista (o vice-presidente). Pelo princípio da multiplicação, há 10 x 9 possibilidades.

Exemplo 3. (voltemos ao Exemplo 2): Temos uma microempresa com dez membros e se deseja eleger uma diretoria composta por um presidente, um vice-presidente, um secretário e um tesoureiro. De quantas maneiras podemos fazer essa escolha (admitindo que nenhum membro da microempresa possa preencher dois cargos)? Haverá dez escolhas para presidente. Nove escolhas para o vice-presidente, então, 10 x 9 maneiras de preencher os dois primeiros postos. Preenchidos estes, há oito maneiras de preencher o próximo posto (secretário), havendo (10 x 9) x 8 maneiras de preencher os três primeiros postos. Por fim, preenchidos os três postos, há sete maneiras de escolher o tesoureiro; há, pois (10 X 9 x 8) x 7 maneiras de selecionar a chapa de dirigentes.

Quando se admitem repetições, temos n escolhas para o primeiro elemento da lista, n escolhas para o segundo elemento da lista e assim por diante, até n escolhas para o último elemento da lista. Ao todo, há n x n x ... x n = n^k listas possíveis. As listas sem repetições por vezes são chamadas permutações.

3.2 Conjuntos (não-ordenados)

Um conjunto é uma coleção de objetos, sem repetição e não ordenada. Determinado objeto é, ou não é, elemento de um conjunto – um objeto não pode figurar em um conjunto "mais de uma vez". Não há ordem para os elementos de um conjunto. A maneira mais simples de especificar um conjunto consiste em listar seus elementos entre chaves. Por exemplo, {2, 3, 4,5} é um conjunto com exatamente três elementos, ou membros: os inteiros 2 e 3 e o racional. Nenhum outro objeto está no conjunto. Todos os conjuntos a seguir são o mesmo conjunto: {3, 2, 4,5}; {4,5, 2, 3}; {2, 4,5, 3}.

Não interessa a ordem em que se listam os elementos nem se repetem um elemento. Tudo o que importa é: quais objetos são elementos do conjunto e quais não o são. Nesse exemplo, exatamente três objetos são elementos do conjunto; nenhum outro objeto é.

Um objeto pertencente a um conjunto é chamado elemento do conjunto. A pertinência a um conjunto é denotada pelo símbolo Є. A notação x Є A significa que o objeto x é elemento do conjunto A. Por exemplo, 2 Є {2, 3, 4,5} é verdadeiro, mas 5 $não$ Є {2, 3, 4,5} é falso. Na última hipótese, podemos escrever 5 não Є {2, 3, 4,5}; a notação x $não$ Є A significa que x não é elemento de A. E se pronuncia "é membro de", ou "é elemento de", ou "está em", "pertence a".

O número de elementos em um conjunto A se denota por $|A|$. A cardinalidade de A nada mais é que o número de objetos no conjunto. A cardinalidade do conjunto {2, 3, 4,5} é 3. A cardinalidade de Z é infinita. Dizemos também que $|A|$é o tamanho do conjunto A. Diz-se que um conjunto é finito se sua cardinalidade é um inteiro (isto é, é finita). Caso contrário, dizemos que o conjunto é infinito. O conjunto vazio é o conjunto desprovido de elementos. O conjunto vazio pode ser denotado por { }, ou o símbolo especial ∅. A afirmação "x Є ∅" é falsa, qualquer que seja o objeto que x possa representar. A cardinalidade do conjunto vazio é zero (isto é, |∅ | = 0).

3.2.1 Relações entre conjuntos

Definição (Relação em, entre conjuntos): seja R uma relação e sejam os conjuntos A e B. Dizemos que R é uma relação sobre A desde que R ⊂ A X A; e dizemos que R é uma relação de A para B se R ⊂ A x B.

Exemplo: sejam A = (1, 2, 3 ,4} e B = {4, 5 , 6, 7}.

Sejam R = {(1, 1), (2, 2), (3, 3), (4, 4)}, S= {(1, 2), (3, 2)}, T = {(1, 4), (1, 5), (4, 7)}. Todos esses conjuntos são relações: • R é uma relação sobre A. Note que é a relação de igualdade em A. • S é uma relação sobre A. • T é uma relação de A para B. Note que os elementos 2, 3 ∈ A e 6 ∈ B.

Dados dois conjuntos A e B não vazios, chama-se de relação binária de A e B a qualquer subconjunto de A X B ou a qualquer elemento do conjunto, e indica-se por R.

Exemplo: sejam A = {a, b} e B = {x, y, s}, tem-se que:

A X B = {(a, x), (a, y), (a, s), (b, x), (b, y), (b, s)}. Qualquer subconjunto (parte) de A X B é uma relação binária de A e B ou entre A e B, logo: R = {(a, x), (b, x), (b, s)} ⊂ A X B é uma relação binária.

3.2.2 Contagem de subconjuntos

Primeiramente, revisando a definição (subconjunto): sejam os conjuntos A e B. Dizemos que A é subconjunto de B se, e somente se, todo elemento de A também for elemento de B. A notação A ⊂ B significa que A é subconjunto de B.

Contagem de subconjuntos: quantos subconjuntos tem um conjunto?

Considere o exemplo: quantos subconjuntos tem o conjunto A = {1,2,3}?

A maneira mais fácil de resolver é listar todas as possibilidades. Como $|A| = 3$, qualquer subconjunto de A pode ter de zero a três elementos. Podem-se organizar todas as possibilidades como:Tabela 1: Lista de possibilidades

Número de elementos	Subconjuntos	Número
0	∅	1
1	{1}, {2}, {3}	3
2	{1,2}, {1,3}, {2,3}	3
3	{1,2,3}	1
TOTAL		**8**

Portanto, {1, 2, 3} tem oito subconjuntos.

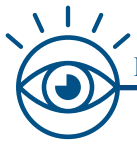
Teorema: Seja A um conjunto finito. O número de subconjuntos de A é $2^{|A|}$.

3.2.3 Conjunto potência

Um conjunto pode ser elemento de outro conjunto. Por exemplo, {1, 2, {3,4}} é um conjunto com três elementos: o número 1, o número 2 e o conjunto {3,4}.

Exemplo especial deste caso é o chamado conjunto potência de um conjunto.

Definição (conjunto potência): seja A um conjunto. O conjunto potência de A é o conjunto de todos os subconjuntos de A.

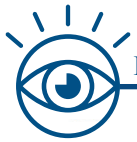


Fique atento

Por exemplo, o conjunto potência de {1, 2, 3} é o conjunto { ∅, {1}, {2}, {3}, {1, 2}, {1, 3 }, {2, 3}, {1, 2, 3}} O conjunto potência de A se denota por 2^A.

3.3. Relações

As relações permeiam toda a matemática. Intuitivamente, uma relação é uma comparação entre dois objetos. Os dois objetos estão, ou não, relacionados de acordo com alguma regra. Por exemplo, menor que (<) é uma relação definida nos inteiros. Alguns pares de números, como (2, 8), satisfazem a relação menor que (pois 2 < 8), mas outros pares de números não a satisfazem, como (10, 3), pois 10 não é < 3.



Fique atento

Há outras relações definidas sobre os inteiros, como divisibilidade, maiores que, igualdade etc. Além disso, há relações sobre outros tipos de objetos. Podemos, por exemplo, perguntar se um par de conjuntos satisfaz a relação ⊂.

3.3.1 Definição (Relação): uma relação é um conjunto de pares ordenados

Por exemplo, R ={(1,2), (1,3), (3,0)} é uma relação. O conjunto de pares ordenados é uma listagem completa de todos os pares de objetos que "satisfazem" a relação. Essa relação nos diz que, para a relação R, 1 está relacionado com 2, 1 está relacionado com 3 e 3 está relacionado com 0, e, para quaisquer outros objetos, x e y, x não está relacionado com y. Podemos escrever (l, 2) ∈ *R*, (1, 3) ∈ R, (3, 0) ∈ R, (4, 3) não ∈ *R* isso significa que (1, 2), (1, 3) e (3, 0) estão relacionados por R, mas (4, 3) não está. Embora se trate de uma maneira formalmente correta de expressar esses fatos, não é como mostramos. Ficará como: 1 R 2, 1 R 3, 3 R 0.

Em outras palavras, os símbolos x R y significam (x, y) ∈ R. Ou seja, “x está relacionado com y pela R”, ou, “x está relacionado com y”.

Domínio e Imagem de uma relação:

Domínio – sejam os conjuntos A e B e a relação R ⊂ A X B; chama-se domínio de R e indica-se por D(R) o conjunto dos elementos de A que estão na relação. Isto é, D(R) ⊂ A.

Imagem: sejam os conjuntos A e B e a relação R ⊂ A X B; chama-se imagem de R e indica-se por Im(R) o conjunto de B que está na relação. Isto é, Im(R) ⊂ B.

3.3.2 Tipos de relações

3.3.2.1 Reflexiva

Seja R uma relação definida em um conjunto A. Se, para todo x ∈ A, temos x R x; dizemos que R é reflexiva.

Exemplo: Considere a relação = (igualdade) sobre os inteiros. Ela é reflexiva (qualquer inteiro é igual a si mesmo).

3.3.2.2 Simétrica

Seja R uma relação definida em um conjunto A. Se, para todo x, y ∈ A, temos x R y =>y R x; dizemos que R é simétrica.

Exemplo: Considere a relação = (igualdade) sobre os inteiros. Ela é simétrica, pois se x = y, então y=x.

3.3.2.3 Transitiva

Seja R uma relação definida em um conjunto A. Se, para todo x, y, z ∈ A, tem-se: x R y e y R z) => x R z, dizemos que R é transitiva.

Exemplo: Considere a relação = (igualdade) sobre os inteiros. Ela é transitiva, pois se x = y e y = z, então devemos ter x = z.

3.3.2.4 Relação de Equivalência

À medida que prosseguirmos com o estudo da matemática discreta, vamos encontrar várias relações. Certas relações apresentam forte semelhança com a relação de igualdade. Um bom

exemplo (da geometria) é a relação “é congruente com” (em geral denotada por ≅) no conjunto dos triângulos. Aproximadamente, triângulos são congruentes se têm exatamente a mesma forma. Os triângulos congruentes não são iguais (por exemplo, podem estar em partes diferentes do plano), mas, em certo sentido, funcionam como triângulos iguais. Por quê? O que há de especial com ≅, que faz que atue como igualdade? Dos tipos listados no item 3.3.2, ≅ é reflexiva, simétrica e transitiva.

Definição (Relação de equivalência): Seja R uma relação em um conjunto A. Dizemos que R é uma relação de equivalência se R é reflexiva, simétrica e transitiva.

Exemplo: Considere a relação = (igualdade) sobre os inteiros. Como sabemos que a relação de = é reflexiva, simétrica e transitiva, logo R é de equivalência.

A relação de equivalência a seguir desempenha papel fundamental na teoria dos números.

Definição1 (Congruência módulo n): Seja n um inteiro positivo. Dizemos que os inteiros x e y são congruentes módulo n e escrevemos x ≡ y (mód. n), se n/x-y. Isto é, em outras palavras, x ≡ y (mód. n) se e somente se x e y diferem por um múltiplo de n.

Exemplos:

3 ≡ 13 (mód. 5) porque 3 - 13 = -10 é múltiplo de 5.

4 ≡ 4 (mód. 5) porque 4 - 4 = 0 é múltiplo de 5.

16 $\not\equiv$ 3 (mód. 5) porque 16 - 3 = 13 não é múltiplo de 5.

Em geral, abreviamos para mód. a palavra módulo.

Definição 2 (Classe de equivalência): Seja R uma relação de equivalência em um conjunto A e seja a ∈A. A classe de equivalência de a, denotada por [a], é o conjunto de todos os elementos de A relacionados com a (pela R); isto é, [a] ={x ∈ A/ x R a}.

Exemplo: Considere a relação de equivalência congruência mód. 2. O que é [1]? Por definição, [1] = {x ∈Z / x = 1 (mód. 2)} Este é o conjunto de todos os inteiros x, de modo que 2|(x — 1), isto é, x — 1 = 2k para algum k, de modo que x = 2k+ 1, isto é, x é ímpar. O conjunto [1] é o conjunto dos números ímpares.

Agora, para seu conhecimento, seguem várias proposições que descrevem as características importantes das classes de equivalência.

Proposição 1: seja R uma relação de equivalência em um conjunto A e seja a ∈ A. Então a ∈ [a].

Proposição 2: seja R uma relação de equivalência em um conjunto A, e sejam a, b ∈ A. Então, a R b se e somente se [a] = [b].

Proposição 3: seja R uma relação de equivalência em um conjunto A e sejam a, x, y ∈ A. Se x, y ∈ [a], então x R y.

3.4 Síntese da Unidade

Nesta Unidade , abordamos a contagem de listas de objetos. O instrumento central é o princípio da multiplicação. Uma fórmula geral é desenvolvida para a contagem de listas de comprimento k de elementos selecionados de um universo de n elementos com ou sem repetição.

Introduzimos o conceito de conjunto e a notação x ∈A. Apresentamos a notação representativa de um conjunto {x ∈ A/ ...}. Discutimos os conceitos de conjunto vazio (∅), subconjunto (⊂). Fizemos uma distinção entre conjunto finito e conjunto infinito, e apresentamos a notação |A| para a cardinalidade de A. Consideramos o problema da contagem do número de subconjuntos de um conjunto finito e definimos o conjunto potência de um conjunto, 2^A.

Para finalizar, formalizamos que a relação de equivalência é uma relação em um conjunto, a qual é reflexiva, simétrica e transitiva. Discutimos uma relação de equivalência importante: a congruência módulo em n em Z. Desenvolvemos a noção de classes de equivalência e discutimos várias propriedades das classes de equivalência.

Esperamos que os conteúdos tenham sido apropriados por você, de modo a colaborar com a sua formação em relação a esta disciplina.

3.5 Para saber mais

Teoria dos números – Relação de equivalência e conjunto quociente. Disponível em: https://www.youtube.com/watch?v=y0DhBchRQ10. Acesso em: 06 abr. 2021

Conjuntos e relações. Disponível em: http://mtm.ufsc.br. Acesso em: 06 abr. 2021

Teoria dos conjuntos. Disponível em: https://www.todamateria.com.br Acesso em: 06 abr. 2021

Congruência módulo m. Disponível em: https://www.youtube.com/watch?v=wpiaznK6U2Y Acesso em: 06 abr. 2021

3.6 Aprendendo e Praticando

1. Sejam A={a, b, c, d} e B={w, x, t, u, k} e a relação: R= {(a, x), (a, y), (c, t), (d, k)}, qual é o D(R) e o Im(R)?

Solução: D(R)= {a, c, d} e Im(R) = {x, y, t, k}

2. Sejam A=B=N= {0, 1, 2, 3, 4, ...} e a relação: R= {(x, y)/ y = 2x, ∀ x∈ n}, qual é o D(R) e Im(R)?

Solução: D(R) = {todos os x} = N e a Im(R) = {0, 2, 4, 6, 8, ...} = {pares}.

3. Seja A={a, b}, B ={c}, C = {1, 2}. Obter A X B X C.

Solução: AX B X C={(a, c, 1), (a, c, 2), (b, c, 1), (b, c, 2)}.

4. Seja A = {0, 1, 2, 3} e a relação R = < (menor que). Ela é uma relação transitiva?

Solução: R = {(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)} é transitiva, pois: x<y e y< z então x < z, isto é: 0 < 1 e 1 < 2 então 0 < 2.

5. Verifique se R é simétrica, sendo A = {retas coplanares} e R = paralelismo ou x R y = x //y.

Solução: Se r // s então s//r, logo a relação é simétrica.

6. Verifique se a relação a/b (a divide b) é reflexiva, sendo A={1, 2, 3, 4, 5}. Mostre quem é o R.

Solução: Ela é reflexiva, pois x/x, $\forall x \in A$. A relação será: R= {(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 2), (2, 3), (2, 4), (3, 3), (4, 4), (5, 5)}.

7. Seja A = {retas coplanares} e R = // (paralelismo); mostre que a relação é de equivalência.

Solução: a) reflexiva: r // r, $\forall r \in A$. b) simétrica: r // s então s // r, ∀ r ≠ s. c) transitiva: r //s e s // t, então r // t. Logo, o paralelismo é uma relação de equivalência.

8. Mostre que 352 ≡ 9997mód. 5.

Solução: 5/9997 – 352, então: 5/ 9645, logo é verdadeiro.

9. Mostre que 3 $\equiv$ 12 mód. 2.

Solução: 2/ 12 -3 $\rightarrow$ 2/9 a diferença não é divisível por 2.

10. Mostre que 20 $\not\equiv$ 17 mód. 5.

Solução: É verdade, pois o resto da divisão de 20 por 5 é 0, enquanto 17 deixa resto 2 na divisão por 5.

Unidade IV

Contagem

Nesta Unidade, os objetivos específicos são conhecer e aplicar os princípios básicos de contagem, notação fatorial, permutações e combinações, além do Princípio de Inclusão – Exclusão. Aplicaremos as ideias de relação a problemas de contagem, procurando contar o número de classes de quivalência, quando todas elas apresentam o mesmo tamanho. Encontraremos frequentemente problemas do tipo “de quantas maneiras diferentes podemos...”, além de aprofundar saberes teóricos ligados ao tema desta Unidade.

Introdução

Nesta Unidade, estudaremos um dos princípios básicos da Matemática presente no nosso dia a dia, de maneiras simples, mas que pode assumir dimensões importantes dentro do campo da Matemática Discreta: as contagens.

Para isso, aprenderemos sobre o conceito de contagem e seus princípios básicos, descobrir o quão próximos estão dos princípios da multiplicação para, em seguida, aprofundarmo-nos em relação aos tipos de arranjo, combinação e permutação e sobre o princípio da exclusão-inclusão, de modo a oferecer um percurso completo de informações sobre o tema desta unidade de ensino.

Ao final desta Unidade, esperamos que você tenha se apropriado dos saberes aqui apresentados, pois são de extrema importância para o profissional da área da Tecnologia da Informação.

Bons estudos!

4.1 Princípios básicos de contagem

Contagem

A necessidade de calcular o número de possibilidades existentes nos chamados jogos de azar é o que levou ao desenvolvimento da Análise Combinatória, parte da Matemática que estuda os métodos de contagem.

Esses estudos foram iniciados no século XVI, pelo matemático italiano Niccollo Fontana (1500-1557), conhecido como Tartaglia. Depois, vieram os franceses Pierre de Fermat (1601-1665) e Blaise Pascal (1623-1662). A Análise Combinatória visa desenvolver métodos que permitam contar – de uma forma indireta – o número de elementos de um conjunto, estando esses elementos agrupados sob certas condições.

Princípio básico de contagem ou Princípio fundamental da contagem (PFC):

Se determinado acontecimento ocorre em n etapas diferentes, e se a primeira etapa pode ocorrer de k_1 maneiras diferentes, a segunda, de k_2 maneiras diferentes, e assim sucessivamente, então o número total T de maneiras de ocorrer o acontecimento é dado por: $T = k_1 . k_2 . k_3 . \ldots . k_n$.

4.1.2 Notação Fatorial

Definição

Denominamos fatorial de um inteiro não negativo n ($n \geq 0$) o inteiro que se indica por n!, e tal que:

$$n! = \begin{cases} 1, se\ n = 0\ ou\ n = 1 \\ n(n-1)(n-2)\ldots.3.2.1\ se\ n \geq 2 \end{cases}$$

Assim, por exemplo:

$$8! = 8.7.6.5.4.3.2.1 = 40320$$

Exemplo 1: escrever, usando o símbolo de fatorial, o produto dos n primeiros inteiros positivos pares e o produto dos n primeiros inteiros positivos ímpares.

Solução: os n primeiros inteiros positivos pares são: 2, 4, 6, ... , 2n – 2, 2n.

Isto é: 2.1, 2.2, 2.3, ..., 2. (n – 1), 2n

Portanto: 2, 4, 6, ..., 2n – 2, 2n = 2^n (1.2.3... (n -1).n) = 2^n . n!.

Os n primeiros inteiros positivos ímpares são: 1, 3, 5, ..., (2n – 3), (2n – 1).

Portanto:

$$1, 3, 5, \ldots, (2n-3), (2n-1) = \frac{1,3,5,\ldots,(2n-3),(2n-1)2n}{2,4,6,\ldots,2n-2,2n} = \frac{2n}{2^n n!}.$$

Exemplo 2: calcular a soma: 1.1! + 2.2 ! + 3.3! + ... + n.n!.

Solução: tomemos a igualdade: k.k! = (k + 1)! – k! e nela façamos sucessivamente k = 1, 2, 3,..., n, o que dá: 1.1! = 2! - 1; 2.2! = 3! – 2!; 3.3! = 4! – 3!; ... , n.n! = (n + 1)! – n!.

Somando ordenadamente todas essas n igualdades e simplificando, obtemos: 1.1! + 2.2! + 3.3! + n.n!= (n + 1)! – 1.

4.2 Permutação e Combinação

4.2.1 Permutação

Podemos considerar a permutação simples como um caso particular de arranjo, em que os elementos formarão agrupamentos que se diferenciarão somente pela ordem. As permutações simples dos elementos A, B e C são: ABC, ACB, BAC, BCA, CAB, CBA. Para determinarmos o número de agrupamentos de uma permutação simples utilizamos a expressão: P = n!. Lembrando: **n! = n.(n-1).(n-2).(n-3).** ... .3.2.1.

Exemplo 1: quantos anagramas podemos formar com a palavra RATO?
Solução: podemos variar as letras de lugar e formar vários anagramas, formulando um caso de permutação simples. P = 4! = 24 possibilidades. Seriam:

RATO	RAOT	ROAT	ROTA	RTAO	RTOA
ARTO	AROT	AORT	AOTR	ATRO	ATOR
TARO	TAOR	TOAR	TORA	TRAO	TROA
ORTA	ORAT	OATR	OART	OTAR	OTRA

Exemplo 2: de quantas maneiras distintas podemos organizar as modelos: Ana, Carlita, Manuela, Paloma e Sofia para a produção de um álbum de fotografias promocionais?

Solução: o número de posições possíveis é 120.

Note que o princípio a ser utilizado na organização das modelos será o da permutação simples, pois formaremos agrupamentos que se diferenciarão somente pela ordem dos elementos.

$$\mathbf{P= n!}$$

$$P = 5!$$

$$P = 5.4.3.2.1$$

$$P = 120$$

Portanto, o número de posições possíveis é 120.

Exemplo 3: de quantas maneiras distintas podemos colocar em fila indiana seis homens e seis mulheres:

a) em qualquer ordem.

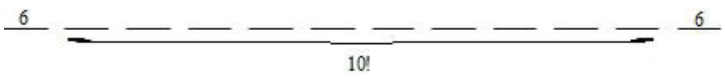
Solução: podemos organizar as 12 pessoas de forma distinta, portanto, utilizamos 12! = 12.11.10.9.8.7.6.5.4.3.2.1=479.001.600 possibilidades.

b) iniciando com homem e terminando com mulher.

Solução: ao iniciarmos o agrupamento com homem e terminarmos com mulher, teremos:

Seis homens aleatoriamente na primeira posição.

Seis mulheres aleatoriamente na última posição.



P = (6.6).10!= 36.10!

P = 130.636.800 possibilidades

4.2.2. Combinação

A combinatória é o ramo da matemática que trata de contagem. Problemas de contagem são importantes sempre que temos recursos finitos.

Exemplos:

- Quanto espaço de armazenamento um banco de dados usa?
- Quantos usuários uma determinada configuração de servidor pode suportar?

Problemas de contagem se resumem, muitas vezes, em determinar o número de elementos em algum conjunto finito.

Exemplos:

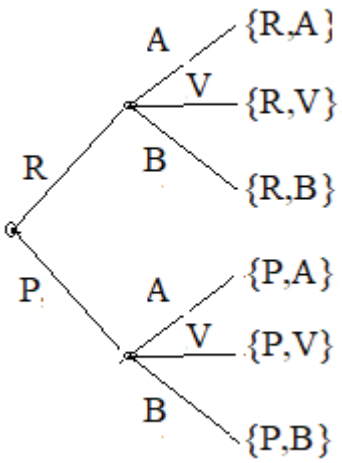
- Quantas linhas tem uma tabela-verdade com n letras de proposição?
- Quantos subconjuntos tem um conjunto com n elementos?

O Princípio da Multiplicação: muitos problemas de contagem podem ser resolvidos a partir de uma árvore de possibilidades.

Exemplo 1: uma criança pode escolher uma entre duas balas, uma rosa e outra preta, e um entre três chicletes, um amarelo, outro verde e outro branco. Quantos conjuntos diferentes a criança pode ter?

Solução: podemos resolver o problema separando a escolha dos doces em duas etapas sequenciais: escolher primeiro a bala e depois o chiclete. Percebe-se que existem 2 x 3= 6 possibilidades: {R,A}, {R,V}, {R,B}, {P,A}, {P,V} e {P,B}.

Mesmo que a sequência de eventos fosse trocada, o número de possibilidades seria o mesmo (3x2=6). O exemplo anterior ilustra o fato de que o número total de resultados possíveis para uma sequência de eventos pode ser obtido multiplicando-se o número de possibilidades do primeiro evento pelo número do segundo.



4.2.3 Árvore de possibilidades

A generalização do Princípio da Multiplicação

Se existem n_1 resultados possíveis para um primeiro evento e n_2 para o segundo, então existem $n_1.n_2$ resultados possíveis para a sequência dos dois eventos.

Árvores de Decisão

Árvores, como aquela apresentada no exemplo da escolha dos doces, que ilustram o número de possibilidades de um evento baseado em uma série de escolhas possíveis são chamadas de árvores de decisão.

Árvores regulares são aquelas em que os números de resultados possíveis em qualquer nível da árvore (ramificação) são os mesmos em todo o nível, como a do exemplo mostrado. Do exemplo anterior, dos doces, no primeiro nível há duas possibilidades R ou P, no segundo nível, três possibilidades para cada ramificação, A, V ou B.

Árvores menos regulares podem ser usadas para resolver problemas de contagem, nos quais a multiplicação não se aplica.

Exemplo 2: a última parte do seu número de telefone tem 04 dígitos. Quantos desses números de quatro dígitos existem?

Solução: a sequência de tarefas é --> escolher o primeiro, depois o segundo, o terceiro e, finalmente, o quarto.

O primeiro pode ser escolhido entre 0 e 9, ou seja, 10 dígitos; então, há 10 possibilidades para a primeira opção.

As seguintes também terão, cada uma, 10 opções. Usando o princípio da multiplicação, devemos multiplicar essas possibilidades para cada tarefa.

10 . 10 . 10 . 10 = 10.000 números diferentes.

Se um elemento não puder ser usado de novo (não são permitidas repetições), o número de possibilidades é afetado.

O Princípio da Adição

Suponha que queremos selecionar uma sobremesa entre três tortas e quatro bolos. De quantas maneiras isso pode ser feito?

Temos 02 eventos, um com 03 resultados possíveis e outro com 04. No entanto, não temos uma sequência de dois eventos possíveis, já que somente uma sobremesa será escolhida. O número de escolhas possíveis será o número total de possibilidades que temos: 3+4=7. Isso ilustra o Princípio da Adição.

Tipos de Combinatória

O princípio fundamental da contagem pode ser usado em grande parte dos problemas relacionados com contagem. Entretanto, em algumas situações, seu uso torna a resolução muito trabalhosa.

Por isso, usamos algumas técnicas para resolver problemas com determinadas características. Basicamente, há três tipos de agrupamentos: arranjos, combinações e permutações.

Arranjos: os agrupamentos dos elementos dependem da ordem e da natureza de tais elementos. Para obter o arranjo simples de *n* elementos tomados, p a p (p ≤ n), utiliza-se a seguinte expressão: $N_{n,p}= \frac{n!}{(n-p)!}$.

Como exemplo de arranjo, podemos pensar na votação para escolher um representante e um vice-representante de uma turma com 20 estudantes. O mais votado será o representante, e o segundo mais votado, o vice-representante. Dessa forma, de quantas maneiras distintas a escolha poderá ser feita? Observe que, nesse caso, a ordem é importante, visto que altera o resultado: $A_{20,2}= \frac{20!}{(20-2)!} = \frac{20.19.18!}{18!} = 20.19 = 380$. Logo, o arranjo pode ser feito de **380** maneiras diferentes.

Combinações: são subconjuntos em que a ordem dos elementos não é importante, entretanto, são caracterizadas pela natureza desses elementos. Assim, para calcular uma combinação simples de n elementos tomados p a p (p ≤ n), utiliza-se a seguinte expressão: $C_{n,p} = \frac{n!}{p!(n-p)!}$.

A fim de exemplificar, podemos pensar na escolha de 3 membros para formar uma comissão organizadora de um evento, dentre as 10 pessoas que se candidataram.
De quantas maneiras distintas essa comissão poderá ser formada?

Solução: note que, ao contrário dos arranjos, nas combinações, a ordem dos elementos não é relevante. Isso quer dizer que escolher Pedro, Joana e Joaquim é equivalente a escolher Joana, Pedro e Joaquim.

$$C_{10,3}=\frac{10!}{3!(10-3)!}=\frac{10!}{3!7!}=\frac{10.9.8.7!}{3.2.1.7!}=\frac{10.9.8}{6}=120.$$

Observe que, para simplificar os cálculos, transformamos o fatorial de 10 em produto, mas conservamos o fatorial de 7, pois, dessa forma, é possível simplificar com o fatorial de 7 do denominador. Assim, existem 120 maneiras distintas de formar a comissão.

4.3 Princípio de Inclusão-Exclusão

O Princípio de Inclusão e Exclusão é uma generalização do princípio aditivo.

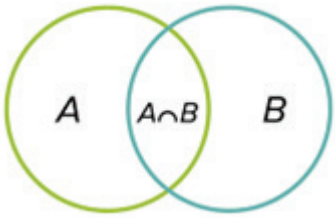
Um dos tópicos desta Unidade é a obtenção de uma fórmula para contar o número de elementos de uma união finita de vários conjuntos finitos, não necessariamente disjuntos. Tal fórmula é denominada **princípio de inclusão e exclusão**. Vamos validar essa fórmula e, em seguida, abordaremos diversas aplicações desse resultado.

Dado um conjunto finito A e um conjunto finito B, vamos denotar por n(A) o número de elementos de A, e n(B) o número de elementos de B.

Proposição 1. Considere A e B conjuntos finitos.

Então: $n(A \cup B) = n(A) + n(B) - n(A \cap B)$.

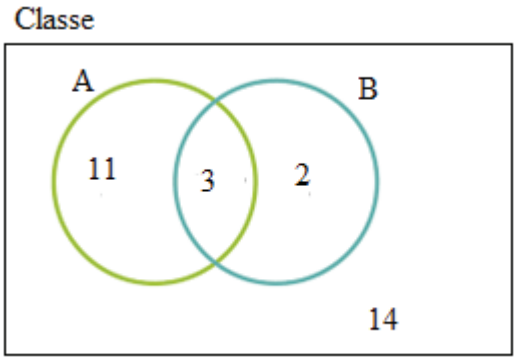
Ilustramos a ideia no Diagrama de Venn.



Exemplo: Numa classe de 30 estudantes, 14 falam inglês, 5 falam alemão e 3 falam inglês e alemão. Quantos alunos falam pelo menos uma língua dentre inglês e alemão?

Solução: vamos definir: A= conjunto formado pelos estudantes que falam inglês; B= conjunto formado pelos estudantes que falam alemão; $A \cap B$= conjunto formado pelos estudantes que falam inglês e alemão.

Temos que $n(A) = 14$, $n(B) = 5$ e $n(A \cap B) = 3$. Observe que: $n(A \cup B) = n(A) + n(B) - n(A \cap B) = 14 + 5 - 3 = 16$. Quando somamos 14 com 5, contando duas vezes os alunos que falam ambas as línguas, aqueles estudantes que se encontram em $A \cap B$, ou seja, os que falam inglês e alemão.



Representação do problema em Diagrama de Venn. Observe que os 14 alunos fora dos grupos A e B não falam nem alemão e nem inglês.

Proposição 2. Considere três conjuntos A, B e C, tais que A, B e C são finitos. Então: $n(A \cup B \cup C) = n(A)+n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$.

4.4 Síntese da Unidade

Nesta Unidade, você estudou uma parte da Matemática denominada **Análise Combinatória.**

Vimos que a Análise Combinatória visa desenvolver métodos que permitam contar – de uma forma indireta – o número de elementos de um conjunto, estando esses elementos agrupados sob certas condições.

Questões de contagem aparecem com frequência em Estatística, Física, Química, Biologia, Informática e em várias outras áreas do conhecimento. A ideia básica da combinatória é desenvolver técnicas para quantificar objetos de um dado conjunto finito sem a necessidade de listar todos os seus elementos.

Aprendemos, ainda, que algumas dessas técnicas consistem em dividir um problema maior em três pequenos problemas similares e que o princípio da inclusão e exclusão é uma ferramenta de grande utilidade na resolução de problemas de contagem.

Nos problemas de combinatória, os métodos mais utilizados são o Princípio Multiplicativo, o Princípio Aditivo, os Arranjos, as Permutações e as Combinações. Diferentes técnicas podem ser aplicadas a um mesmo problema. Dessa forma o princípio da inclusão e exclusão pode ser uma ferramenta facilitadora na resolução de diversos problemas combinatórios.

Ao chegar ao final desta Unidade, esperamos que o seu percurso de aprendizagem tenha sido satisfatório e de grande crescimento para você. Agora, consulte os materiais extra indicados na seção “Para saber mais”, bem como realize as atividades da seção Aprendendo e Praticando, para reforçar os saberes teóricos estudados até aqui.

4.5 Para Saber Mais

Princípio Fundamental da Contagem. Disponível em: https://www.youtube.com/watch?v=3dm6pq6akQI. Acesso em: 24 abr. 2021.

Análise Combinatória. Princípios Aditivos e Multiplicativos. Disponível em: https://www.youtube.com/watch?v=2dtHUK54j0c. Acesso em: 24 abr. 2021.

4.6 Aprendendo

1) Sejam os conjuntos A ={1, 2, 3, 4, 5}, B = {0, 2, 4, 6, 8} e C = {0, 3 ,4, 5, 6, 7, 8, 9}. Determinemos as interseções: A ∩ B = {2, 4}; A ∩ C = {3, 4, 5}; B ∩ C = {0, 4, 6, 8}; A ∩ B ∩ C = {4}.

Façamos, agora, a união dos três conjuntos: A ∪ B ∪ C = {1, 2, 3, 4, 5} ∪ {0, 2, 4, 6, 8}∪ {0, 3, 4, 5, 6, 7, 8, 9}= {0, 0, 1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 6, 6, 7, 8, 8, 9}

Retirando as repetições (interseções) dois a dois, ou seja, os elementos 0, 2, 3, 4, 5, 6, 8, obtemos: A ∪ B ∪ C = {0, 1, 2, 3, 5, 6, 7, 8, 9}.

Podemos notar que o elemento 4 que é a interseção entre os três conjuntos foi retirado totalmente da união, assim sendo, ele precisa ser incluído novamente, daí teremos:

A ∪ B ∪ C = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} possui 10 elementos.

Então, a fórmula para determinar a cardinalidade de elementos da união de três conjuntos é: $n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C) = 5 + 5 + 8 - 2 - 3 - 4 + 1 = 10$ elementos.

2) Numa classe de 30 estudantes, 14 falam inglês, 5 falam alemão e 7 falam francês. Sabendo-se que 3 falam inglês e alemão, 2 falam inglês e francês, 2 falam francês e alemão e que 1 fala as três línguas, determinar o número de elementos dos que falam pelo menos uma destas três línguas.

Solução: para resolver este problema podemos utilizar o princípio de inclusão – exclusão. Primeiro chamaremos de I o conjunto dos estudantes que falam inglês, A o conjunto dos estudantes que falam alemão e F o conjunto dos estudantes que falam francês. Temos: n(I) = 14; n(A) = 5; n(F) = 7; $n(I \cap A) = 3; n(I \cap F) = 2; n(A \cap F) = 2$ *e* $n(I \cap A \cap F) = 1$.

Dessa forma: $n(I \cup A \cup F) = n(I) + n(A) + n(F) - n(I \cap A) - n(I \cap F) - n(A \cap F) + n(I \cap A \cap F)$ = 14 + 5 + 7 – 3 – 2 – 2 + 1 = 20.

Portanto, temos que 20 estudantes falam pelo menos um dos idiomas.

3) Quantas senhas com 4 algarismos diferentes podemos escrever com os algarismos 1, 2, 3, 4, 5, 6, 7, 8, e 9?

Solução: Usando o princípio fundamental da contagem: como no enunciado informa que são diferentes os algarismos temos a situação: 9 para os algarismos das unidades; 8 para os algarismos das dezenas; 7 para os algarismos das centenas e 6 para o algarismo do milhar. Assim, o número de senhas será dado por: 9. 8. 7. 6 = 3024 senhas.

4) De quantas maneiras diferentes 6 amigos podem se sentar em um banco para tirar uma foto?

Solução: usando a fórmula de permutação, pois todos os elementos farão parte da foto. Note que a ordem que faz diferença.

$P_6 = 6! = 6. 5. 4. 3. 2. 1 = 720$ maneiras de 6 amigos se sentarem para tirar uma foto.

5) Quantas comissões de 4 elementos podemos formar com 20 estudantes de uma turma?

Solução: note que, como para uma comissão a ordem não faz diferença, usaremos a fórmula de combinação para calcular:

$$C_{20,4} = \frac{20!}{4!(20-4)!} = \frac{20!}{4!(16)!} = \frac{20.19.18.17.16!}{4.3.2.1.16!} = \frac{20.19.18.17}{4.3.2.1} = \frac{116280}{24} = 4845 \text{ comissões.}$$

6) Determine o número de anagramas

a) existentes na palavra FUNÇÃO:

Solução: cada anagrama consiste na reorganização das letras que compõem uma palavra. No caso da palavra FUNÇÃO temos 6 letras que podem ter suas posições modificadas. Para encontrar o número de anagramas basta calcular: $P_6 = 6! = 6.5.4.3.2.1 = 720$.

b) existentes na palavra FUNÇÃO desde que as vogais A e O apareçam juntas nessa ordem (ÃO):

Solução: se as letras A e O devem aparecer juntas como ÃO, então podemos interpretá-las como se fosse uma só letra: assim, temos que calcular P_5: $P_5 = 5! = 5.4.3.2.1 = 120$. Desta forma, existem 120 possibilidades de anagramas da palavra FUNÇÃO, mantendo em todos eles o final ÃO.

7) Uma equipe de trabalho é formada por 6 mulheres e 5 homens. Eles pretendem se organizar em grupo de 6 pessoas, com 4 mulheres e 2 homens, para compor uma comissão. Quantas comissões podem ser formadas?

Solução: para formar a comissão se deve escolher 4 das 6 mulheres ($C_{6,4}$) e 2 dos 5 homens ($C_{5,2}$). Pelo princípio fundamental da contagem multiplicamos estes números:

$$C_{6,4}.\ C_{5,2} = \frac{6!}{4!(6-4)!}.\frac{5!}{2!(5-2)!} = \frac{6!}{4!2!}.\frac{5!}{2!3!} = \frac{6.5.4!}{4!2.1}.\frac{5.4.3!}{2.1.3!} = \frac{30}{2}.\frac{20}{2} = 150$$

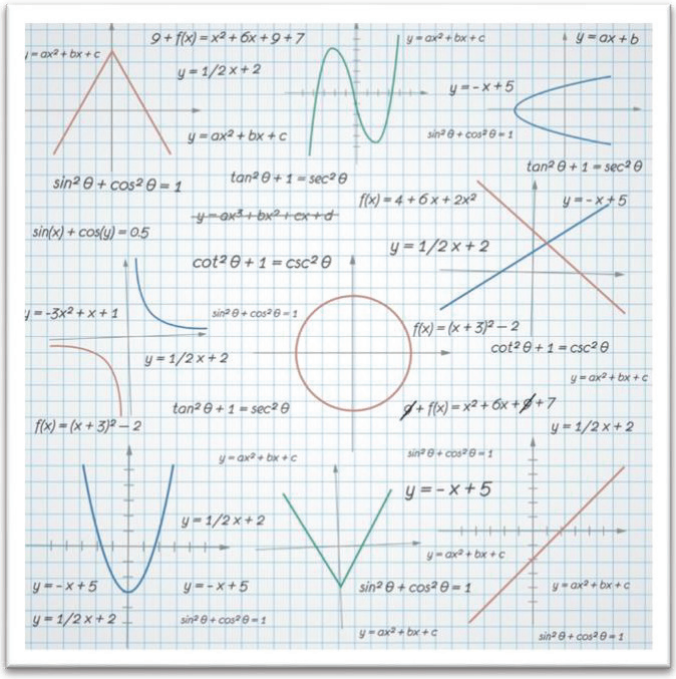
Assim, podem ser formadas 150 comissões com 6 pessoas e com, exatamente, 4 mulheres e 2 homens.

Unidade V

Funções

Nesta Unidade, estudaremos uma classe particular de relações chamadas funções. Estudaremos as funções chamadas discretas, que são aquelas que relacionam um conjunto enumerável como outro. Há várias aplicações na área de computação, como por exemplo: algoritmos são funções, compiladores são funções e outras mais aplicações. Iniciaremos com a definição, tipos de funções, funções inversas e funções compostas.

Introdução



Nesta Unidade, estudaremos uma classe particular de relações chamadas FUNÇÕES. De modo especial, as funções chamadas DISCRETAS, que são aquelas que relacionam um conjunto enumerável com outro conjunto enumerável.

Estudaremos as principais propriedades e os tipos de funções, como: **a) a função injetora**, também chamada de injetiva: um tipo de função que apresenta elementos correspondentes em outra; **b) a função sobrejetora**, também chamada de sobrejetiva: um tipo de função matemática que relaciona elementos de duas funções; **c) a função bijetora**, também chamada de bijetiva: um tipo de função matemática que relaciona elementos de duas funções; **d) a função inversa**, ou invertível: um tipo de função bijetora, ou seja, ela é sobrejetora e injetora ao mesmo tempo; **e) a função composta**, também chamada de função de função: um tipo de função matemática que combina duas ou mais variáveis. Sendo assim, ela envolve o conceito de proporcionalidade entre duas grandezas, e que ocorre por meio de uma só função.

São várias as aplicações das Funções na área da Ciência da Computação: Analisadores dos Compiladores; Criptografia de dados; Compressão de dados; Geração de Chave de Armazenamento, entre outros. Por isso, sugerimos que estude com bastante empenho os conteúdos apresentados.

Bons estudos!

5.1 Definições e propriedades das funções

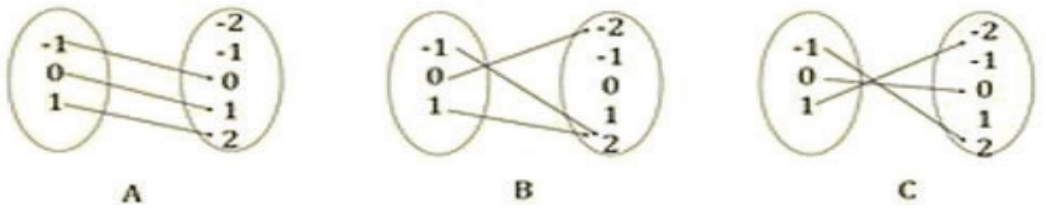
Intuitivamente: função é uma relação especial entre dois conjuntos, na qual todo elemento do primeiro conjunto deve ter, obrigatoriamente, elemento associado no segundo conjunto, e cada elemento do primeiro conjunto só pode ter um e apenas um elemento associado no segundo conjunto.

Formal: sejam A e B quaisquer dois conjuntos não vazios. A relação f de A para B é chamada uma função se para todo a ∈ A existe um único b ∈ B tal que (a, b) ∈ f, e se lê: "f é função de A em B". Em símbolos: f: A→B.

Para todo a ∈ Dom(f), f(a) (ou seja, o conjunto dos "f relativos" de a) contém apenas um elemento.

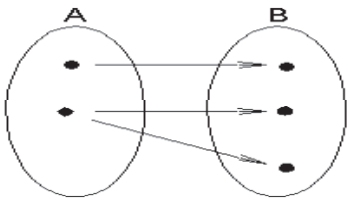
Exemplos

1) Diagramas de Venn representando Funções



Fonte: http://matimage.blogspot.com

2) Diagrama de Venn que não representa Função



Observações

– Se f(a)={b}, escreve-se f(a)=b;

– O valor a é chamado de argumento da função, e f(a) é chamado valor de f para o argumento a.

Exemplos

Sejam A={1, 2, 3, 4} e B={a, b, c, d, e} e seja f={(1,a), (2,b), (3,d), (4,d)}. Assim, os conjuntos dos f relativos de x para cada x ∈ A são: f(1)={a}, f(b)={2}, f(3)={d}, f(4)={d}.

– Como existe um conjunto f(x), para todos os elementos x ∈ A, e

– Como cada conjunto f(x) para x ∈ A tem um único valor, então f é **UMA FUNÇÃO.**

Exemplos

1) Seja X={1, 5, Q, Queijo}, Y={2, 5, 7, r, Maria} e f: X→Y tem se f={(1, 2), (5, 7), (Q, r),(Queijo, r)}. Então, Dom(f) = X, Im(f) = {2, 7, r} e f(1) = 2, f(5) = 7, f(Q) = r e f(Queijo) = r.
2) Seja X = Y = R (reais) e $f(x)=x^2+2$. Então, Dom(f) = R, Im(f)⊆R os valores de f(x) estão contidos em uma parábola.
3) Seja X = Y = R (reais) e $f(x)=x^{1/2}$. Então, f não é uma função já que a condição de unicidade é violada, pois a cada valor de x correspondem dois valores de y ∈ R.

Observações

– Sabemos que nem todos os possíveis subconjuntos de A X B constituem-se em funções de A em B.

– O número de funções que podemos obter dos subconjuntos do produto cartesiano A X B é B^A.

Exemplo

Seja A={a, b, c} e B={0, 1}. Então A X B={(a, 0), (a, 1), (b, 0), (b, 1), (c, 0), (c, 1)}. Existem 2^6 subconjuntos de A X B, porém apenas 2^3 subconjuntos definem funções de A em B.

1. f1={(a, 0), (b, 0), (c, 0)}
2. f2={(a, 0), (b, 0), (c, 1)}
3. f3={(a, 0), (b, 1), (c, 0)}
4. f4={(a, 0), (b, 1), (c, 1)}
5. f5={(a, 1), (b, 0), (c, 0)}
6. f6={(a, 1), (b, 0), (c, 1)}
7. f7={(a, 1), (b, 1), (c, 0)}
8. f8={(a, 1), (b, 1), (c, 1)}

5.2 Tipos de Funções

5.2.1 Função Injetiva ou Injetora

Uma função f de A em B é dita de um-para-um, ou injetora, se e somente se f(a) ≠f(b) sempre a ≠ b.

Uma função f de A em B (f: A →B) é injetora se elementos diferentes de A apresentam imagens diferentes em B.

$$\forall\, x_1, x_2 \in A,\ (x_1 \neq x_2) \rightarrow f(x_1) \neq f(x_2).$$

Exemplos

1) Determine se a função $f(x)=x^2$, dos inteiros para os inteiros, é injetora.

Solução

A função $f(x)=x^2$ não é injetora, pois por exemplo $1 \neq -1$ mas $f(1) = f(-1) = 1$.

2) Determine se a função $f(x) = x+1$, dos inteiros para os inteiros, é injetora.

Solução A função $f(x) = x+1$ é injetora, pois sempre $x \neq y$, $x+1 \neq y+1$.

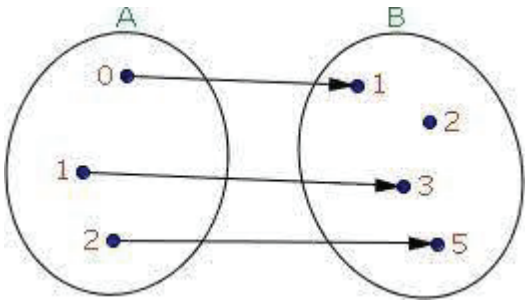


Diagrama de Venn – Função Injetora

5.2.2 Função Sobrejetiva ou Sobrejetora

Uma função f de A em B é chamada sobrejetora se, e somente se, para todo $b \in B$ existe um elemento $a \in A$ tal que $f(a) = b$.

Uma função f de A em B (f: A →B) é sobrejetora se todos os elementos de B são imagens dos elementos de A.

$$\forall\, b \in B,\ \exists\, a \in A \mid (a, b) \in f.$$

Exemplos

1) Determine se a função $f(x)=x^2$, dos inteiros para os inteiros, é sobrejetora.

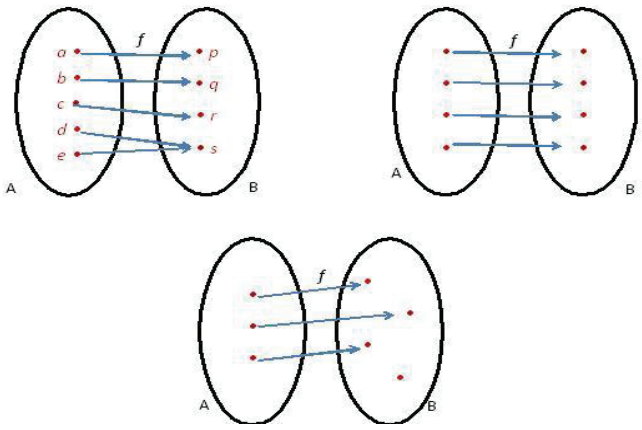
Solução

A função $f(x)=x^2$ não é sobrejetora, pois, por exemplo para $f(x) = -1$, não existe x tal que $x^2 = -1$.

2) Determine se a função f(x) = x+1, dos inteiros para os inteiros, é sobrejetora.

Solução

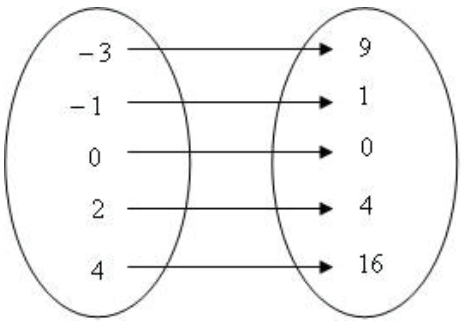
A função f(x) = x+1 é sobrejetora, pois para todo inteiro y existe um inteiro x tal que x+1 = y.



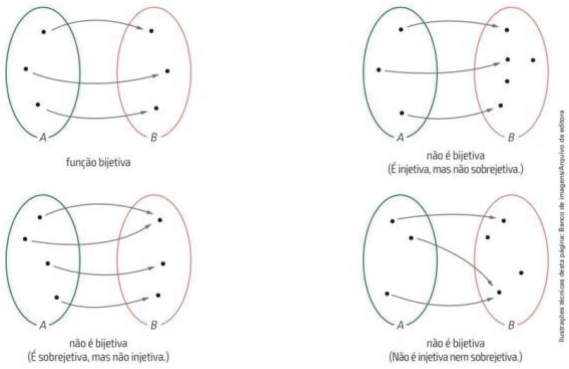
Diagramas de Venn – Função Sobrejetora

5.3 Função Bijetiva ou Bijetora

Uma função f de A em B é chamada bijetora se, e somente se, ela for injetora e sobrejetora simultaneamente.



Função Bijetora



Diagramas de Venn – representação de diagramas bijetoras e não bijetoras

5.3.1 Função Inversa

Definição: seja f: A →B uma função bijetora. A função inversa de f é a função que associa a um elemento b ∈ B o elemento único de a ∈ A tal que f(a)=b.

A função inversa de f é denotada por f^{-1}; portanto $f^{-1}(b) = a$ quando f(a)=b.

Uma função bijetora é chamada de inversível, ou invertível.

Exemplos

1) Seja f a função de {a, b, c} em {1, 2, 3} tal que f(a) = 2, f(b) = 3, f(c) = 1. Verifique se a função f é inversível e, em caso afirmativo, determine a sua inversa.

Solução

A função f é inversível, pois é bijetora e a função f^{-1} é: $f^{-1}(1)=c$, $f^{-1}(2)=a$, $f^{-1}(3)=b$.

2) Seja f a função de Z para Z com f(x)=x2. Esta função é inversível?

Solução

Como f(-1) = f(1) = 1, f NÃO É injetora.

Se uma f^{-1} fosse definida, ela teria de associar dois elementos a 1. Isso violaria a condição de unicidade. Logo, f NÃO É inversível.

O domínio de f é o conjunto imagem de g, e o conjunto imagem de f é o domínio de g. Quando queremos, a partir da sentença y=f(x), obter a sentença de $f^{-1}(x)$, devemos realizar os seguintes passos:

1º) Isolamos x na sentença y=f(x);
2º) Pelo fato de ser usual a letra x como símbolo da variável independente, trocamos x por y e y por x.

Por exemplo, para obter a função inversa de f: IR→IR definida por y=2x+1, devemos:

1º) Isolar x em y=2x+1. Assim y=2x+1→y-1=2x→ x=(y-1)/2;
2º) Trocar x por y e y por x: y=(x-1)/2.

Portanto, a função inversa de f é: $f^{-1}(x)=(x-1)/2$.

5.3.2 Função Composta

Definição: dados os conjuntos A, B e C, e as funções f de A em B definida por y=f(x) e g de B em C definida por z = g(y). Chama-se função composta de g com f, a função h=g o f, de A em C, definida por z = g(f(x)).

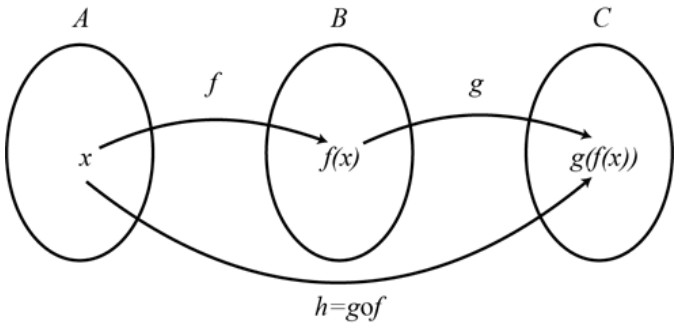


Diagrama de Venn – Função Composta

Exemplo

Seja f a função do conjunto {a, b, c} para ele mesmo, tal que f(a) = b, f(b) = c e f(c) = (a). Seja g a função do conjunto {a, b, c} para o conjunto {1, 2, 3}, tal que g(a) = 3, g(b) = 2, g(c) = 1. Determine a composição de g e f, e a composição de f e g.

Solução

A composição de gof é definida como:

gof(a) = g(f(a)) = g(b)=2; gof(b) = g(f(b)) = g(c) = 1; gof(c) = g(f(c)) = g(a)=3

Não existe a composição de fog. POR QUÊ?

Observações: só existirá a função composta gof de X em Z se o contradomínio de f for um subconjunto do domínio de g. A composição de funções NÃO É comutativa, isto é: fog ≠ g o f.

5.4 Síntese da Unidade

Toda função é uma relação binária de A em B, portanto toda função é um conjunto de pares ordenados. Geralmente, existe uma sentença aberta y = f(x) que expressa a lei mediante a qual, dado x Є A, determina-se y Є B, tal que (x, y) Є f, então f = {(x, y) / x Є A e y Є B e y = f(x)}. Isto significa que, dados os conjuntos A e B, a função f tem a lei de correspondência y = f(x). Vimos que, dada a função f de A em B, consideram-se as retas horizontais por (0, y) com y Є B:

1º) se nenhuma reta corta o gráfico mais de uma vez, então f é injetora;

2º) se toda reta corta o gráfico, então f é sobrejetora;

3º) se toda reta corta o gráfico em um só ponto, então f é bijetora.

Como consequência dos tipos de funções, podemos ter a seguinte condição: se duas funções f de A em B e g de B em C são sobrejetoras, então a função composta gof de A em C é também sobrejetora. A função será injetora se cada elemento diferente do domínio de f tem como imagem elemento distinto do contradomínio.

Pelo que acabamos de ver, a função f leva x até y, enquanto a função g leva y até x. A função g:B→A recebe o nome de **função inversa** de f e é indicada por f^{-1}. Para que uma função f admita a inversa f^{-1} é necessário que ela seja bijetora. Se f não for bijetora, ela não possuirá inversa.

Nesta Unidade, estudamos as principais propriedades e os tipos de funções, como:

a) A função injetora, também chamada de injetiva: um tipo de função que apresenta elementos correspondentes em outra. Assim, dada uma função f (f: A → B), todos os elementos da primeira têm como imagem elementos distintos de B. No entanto, não há dois elementos distintos de A com a mesma imagem de B.

b) A função sobrejetora, também chamada de sobrejetiva: um tipo de função matemática que relaciona elementos de duas funções. Na função sobrejetora, todo elemento do contradomínio de uma é imagem de pelo menos um elemento do domínio de outra. Em outras palavras, numa função sobrejetora o contradomínio é sempre igual ao conjunto imagem.

c) A função bijetora, também chamada de bijetiva: um tipo de função matemática que relaciona elementos de duas funções. Desse modo, os elementos de uma função A possuem correspondentes em uma função B. Importante notar que elas apresentam o mesmo número de elementos em seus conjuntos.

d) A função inversa, ou invertível: um tipo de função bijetora, ou seja, ela é sobrejetora e injetora ao mesmo tempo. Recebe esse nome porque, a partir de uma dada função, é possível inverter os elementos correspondentes de outra. Em outros termos, a função inversa cria funções a partir de outras. Sendo assim, os elementos de uma função A possuem correspondentes em outra função B.

e) A função composta, também chamada de função de função: um tipo de função matemática que combina duas ou mais variáveis. Sendo assim, ela envolve o conceito de proporcionalidade entre duas grandezas, e que ocorre por meio de uma só função.

São várias as aplicações das funções na área da Ciência da Computação: Analisadores dos Compiladores; Criptografia de dados; Compressão de dados; Geração de Chave de Armazenamento, entre outros. Por isso, sugerimos que estude com bastante empenho os conteúdos apresentados.

5.5 Para Saber Mais

Funções. Disponível em: https://www.youtube.com/watch?v=r8gj2eqAIOQ. Acesso em 25 de abril de 2021.

Funções. Disponível em: https://midia.atp.usp.br/plc/plc0001/impressos/plc0001_02.pdf. Acesso em 25 de abril de 2021.

5.6 Aprendendo e praticando

1) Sejam X={1, 2, 3}, Y={p, q} e Z={a, b}. Sejam também f: X →Y dada por f={(1, p), (2, p), (3, q)} e g:Y →Z dada por g={(p, b), (q, b)}. Ache gof.

Solução: gof={(1, b), (2, b), (3, b)}.

2) Seja X={1, 2, 3} e sejam f, g, h e s funções de X em X definidas como: f={(1, 2), (2, 3), (3, 1)}; g={(1, 2), (2, 1), (3, 3)}; h={(1, 1), (2, 2), (3, 1)}; s={(1, 1), (2, 2), (3, 3)}. Determine:

a) fog={(1, 3), (2, 2), (3, 1)}; b) gof={(1, 1), (2, 3), (3, 2)}; c) fohog={(1, 3), (2, 2), (3, 2)};

d) sog={(1, 2), (2, 1), (3, 3)}; e) gos={(1, 2), (2, 1), (3, 3)}; f) sos={(1, 1), (2, 2), (3, 3)};

g) fos={(1, 2), (2, 3), (3, 1)}.

3) Seja N o conjunto dos números naturais incluindo o zero. Determine quais das seguintes funções são injetoras, sobrejetoras ou bijetoras:

a) f:(N →N) f(j)=j2+2; b) f:(N →N) f(j)={0 se j for ímpar e 1 se j for par}; c) f:(N →{0,1}) f(j)={0 se j for ímpar e 1 se j for par}

4) Determine se a função f(x)=x+1, dos inteiros para os inteiros, é bijetora.

Solução: A função f(x)=x+1 é bijetora, pois é injetora e sobrejetora.

5) Seja f(x)=x+2, g(x)=x-2 e h(x)=3x para x ∈R. Determine:

a) fog={(x, x) | x ∈ R}; b) gof={(x, x) | x ∈ R}; c) fof={(x, x+4) | x ∈ R}; d) gog={(x, x-4) | x ∈ R}; e) foh={(x, 3x+2) | x ∈ R}; f) hof={(x, 3x+6) | x ∈ R}; g) hog={(x, 3x-6) | x ∈ R}; h) fohog={(x, 3x-4) | x ∈ R}.

6) Dada a função y = $\frac{x-1}{x+2}$, x ≠ -2, obtenha f-1(-1).

Solução: sabemos que y = $\frac{x-1}{x+2}$ e devemos isolar x nessa igualdade:

y(x + 2) = x – 1

y(x + 2) – x = -1

$yx + 2y - x = -1$

$x(y - 1) = -1 - 2y$

$x = \frac{-1-2y}{y-1}$

$x = -\frac{1+2y}{y-1}$

$x = \frac{1+2y}{1-y}$;

Trocando x por y e y por x, teremos: $y = \frac{1+2x}{1-x}$, ou seja, $f^{-1} = \frac{1+2x}{1-x}$.

Para $f^{-1}(-1) = \frac{1+2(-1)}{1-(-1)} = \frac{1-2}{1+1} = \frac{-1}{2}$.

7) Considere as seguintes funções: f(x) = x - 4 e g(x) = 5x + 1. Qual é o valor da função composta g(f(3))?

(x) -4 ( ) -2 ( )0 ( ) 4 ( )2

8) Considere as funções f:[0,+∞] ⟶ [0,+ ∞] e g: R⟶R, definidas por f(x) = x2 e g(x) = x2.

É correto afirmar que

a) g é bijetora.
b) f é bijetora.
c) f é injetora e g é sobrejetora.
d) f é sobrejetora e g é injetora.

Resposta correta: alternativa b)

9) Considere os conjuntos A = {(1,2), (1,3), (2,3)} e B = {1, 2, 3, 4, 5}, e seja a função f: A → B tal que f (x,y) = x + y.

É possível afirmar que f é uma função

a) injetora.
b) sobrejetora.
c) bijetora.
d) par.
e) ímpar.

Resposta correta: alternativa a)

Unidade VI
Estruturas Algébricas

Nesta Unidade, estudaremos estruturas algébricas, ou seja, conjuntos associados a uma ou mais operações sobre o conjunto que satisfazem certas proposições (axiomas). Você se deparará com conceitos como de grupo, semi-grupo, corpo, espaço vetorial, entre outros. A intenção nesta unidade é introduzir as noções dessas estruturas algébricas. Abordaremos os seguintes temas: grupos, isomorfismos de grupos, subgrupos, anel e corpo, além de suas definições e propriedades.

Introdução

A ideia, ao estudarmos uma estrutura algébrica, é obter resultados que valham no contexto mais geral possível e que englobem exemplos importantes.

Do ponto de vista da Álgebra, um polinômio não deve ser visto como um objeto isolado, mas, antes, como um elemento de um conjunto de polinômios, em que os elementos possam ser somados e, também, multiplicados, resultando em uma estrutura chamada anel de polinômios.

No contexto dessa Unidade, faz sentido, portanto, falarmos em soma e em produto de matrizes, de polinômios e de funções, embora tais objetos não sejam números. Isso se dá porque tais objetos podem ser organizados em conjuntos munidos de uma ou mais operações binárias, o que dá a cada um desses conjuntos uma estrutura algébrica.

Podemos, então, estudar tais estruturas de modo abstrato, sem fazer referência à natureza dos elementos do conjunto, obtendo resultados que valem em diferentes contextos. E é isso que faremos nesta Unidade.

Para isso, estudaremos as estruturas algébricas mais básicas, como grupos, anéis e corpos.

Esperamos que, ao fim desta Unidade, você se mostre capaz de trabalhar com esses saberes de forma autônoma.

Bons estudos!

6.1 Tipos Especiais de Dados

Neste tópico, estudaremos uma primeira estrutura algébrica, chamada estrutura de grupo. Por serem os objetos matemáticos adequados para se quantificar a noção de simetria, os grupos encontram aplicações na Geometria (fundamentação da geometria via grupos de transformações, grupos de Lie, ladrilhamentos), na Química (estrutura dos orbitais atômicos, ligação química, estrutura cristalográfica das moléculas), na Física (mecânica quântica) e na Biologia (estrutura icosaédrica dos vírus). Trata-se, portanto, de uma noção matemática de fundamental importância.

Um magma (também chamado grupoide) é um conjunto não vazio N dotado de uma operação binária $N \times N \longrightarrow N$. denotada (produto) e satisfazendo a seguinte propriedade:

Fechamento: para quaisquer $a, b \in N$: $(a.b) \in N$.

Exemplos

1: soma nos reais.

2: multiplicação de matrizes reais.

Contraexemplos

1: soma nos reais excluindo o zero $(a + (-a) = 0)$.

2: conjunto de funções complexas, com produto interno em um intervalo fechado (resultado é um número).

Um grupo é um conjunto $G \neq \emptyset$, no qual está definida uma operação $*$ que satisfaz as seguintes propriedades:

⇒ $*$ É associativa, ou seja, $x * (y * z) = (x * y) * z, \forall x, y, z \in G$
⇒ $*$ Admite elemento neutro, ou seja, $\exists e \in G$ tal que $x * e = e * x = x, \forall x \in G$
⇒ Para cada elemento $x \in G, \exists x^{-1} \in G$ tal que $x * x^{-1} = x^{-1} * x = e$

Além disso, se $*$ for comutativa, então o grupo G é denominado comutativo ou abeliano.

Exemplos

⇒ O conjunto dos inteiros Z com a adição usual é um grupo.
⇒ O conjunto dos números reais não nulos R^* com a operação de multiplicação usual é um grupo.

6.1.1 Isomorfismo e homomorfismo de grupos

Um isomorfismo de um grupo G em um grupo J é um homomorfismo de G em J que também é uma função bijetora. Se existir um isomorfismo de G em J, então dizemos que G e J são isomorfos, e denotamos isso por $G \simeq J$.

Exemplo

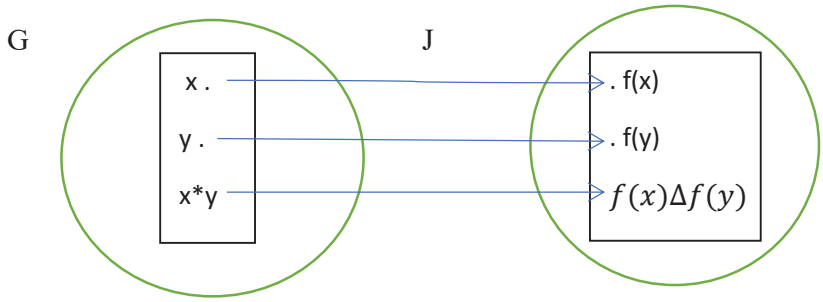
A função $f(x) = \log(x)$ é um isomorfismo de $G = (R^*_+, .\cdot)$ em $J = (R, +)$, porque:

⇒ $f: R^*_+ \longrightarrow R$, $f(x) = \log(x)$ é bijetora.

⇒ Para quaisquer x, y ∈ R^*_+, temos: f(x, y) = log(x.y) = log(x) + log(y) = f(x) + f(y).

Homomorfismo de grupos Δ

Uma função f de um grupo (G, ∗) em um grupo (J, Δ) chama-se um homomorfismo quando f(x∗y) = f(x)Δf(y), ∀x, y ∈ G.

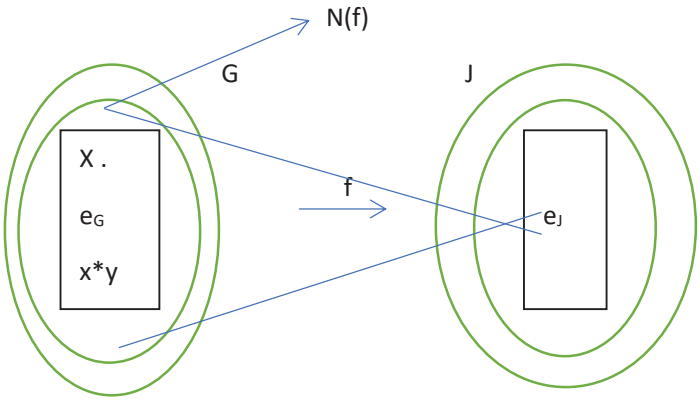


Exemplo

⇒ Se G = J = (Z, +), então f : G → J, f(x) = 2x é um homomorfismo de grupos, porque f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y), ∀x, y ∈ G.

Núcleo de um homomorfismo

Se f: G → J for um homomorfismo de grupos, o núcleo de f , denotado por N(f), é o conjunto de todos os elementos do domínio G cujas imagens através de f são iguais ao elemento neutro de J: N(f) = {x ∈ G | f(x) = e_J}.



Exemplos

⇒ Seja f : (Z, +) → (R, +), f(x) = 2x. O elemento neutro do contradomínio de f é o 0 (zero). Se x ∈ N(f), então f(x) = 0 ⇒ 2x = 0 ⇒ x = 0. Logo, o núcleo de f é formado apenas pelo 0 (zero), isto é, N(f) = {0}.

Sejam G = (Q*, .), J = (R*, .), f: G → J, f(x) = x^2. O elemento neutro de J é o 1 (um). Se x ∈ N(f), então devemos ter f(x) = 1, ou seja, $x^2 = 1 \Rightarrow x = \pm 1$. Logo, N(f) = {−1, 1}.

Isomorfismo de grupos

Um isomorfismo de um grupo G em um grupo J é um homomorfismo de G em J, que também é uma função bijetora. Se existir um isomorfismo de G em J, então dizemos que G e J são isomorfos, e denotamos isso por $G \simeq J$.

Exemplo

A função $f(x) = \log(x)$ é um isomorfismo de $G = (R^*_+, .)$ em $J = (R, +)$, porque:

- $\Rightarrow$ $f : R^*_+ \to R$, $f(x) = \log(x)$ é bijetora;
- $\Rightarrow$ Para quaisquer $x, y \in R^*_+$ temos: $f(x.y) = \log(x.y) = \log(x) + \log(y) = f(x) + f(y)$.

6.1.2 Subgrupos

Neste item, estudaremos subconjuntos de grupos que também são grupos (subgrupos), e veremos que um subgrupo pode ser usado para definir uma relação de equivalência sobre o grupo que o contém. Em um determinado caso especial que vamos estudar, poderá ser dada uma estrutura de grupo ao conjunto das classes de equivalência dessa relação.

Definição: seja $(G, *)$ um grupo. Um subconjunto não vazio $H \subset G$ que seja fechado com relação à operação $*$ é denominado um subgrupo de G quando $(H, *)$ também for um grupo.

Exemplos

- $\Rightarrow$ $H = (Q, +)$ é um subgrupo de $G = (R, +)$
- $\Rightarrow$ O conjunto H dos inteiros pares com a operação de adição usual é um subgrupo de $G = (Z, +)$.
- $\Rightarrow$ O conjunto $H = (R^*_+, .)$ dos números reais positivos com a operação de multiplicação usual é um subgrupo de $G = (R^*, .\cdot)$
- $\Rightarrow$ O conjunto $N = (R^*_-, .\cdot)$ dos reais negativos com a multiplicação não é subgrupo de $G = (R^*, .\cdot)$, porque N não é fechado com relação à multiplicação.

Observações

1. Dizemos que X é parte fechada de A com relação à operação $*$ quando $\forall x, y \in X \Rightarrow x * y \in X$.
2. Tábua de uma operação: a tábua de uma operação $*$ definida sobre um conjunto finito $A = \{a_1, a_2, \cdots, a_n\}$ é uma tabela onde o resultado da operação $a_i * a_j$ é colocado na i-ésima linha e j-ésima coluna.

Exemplo de tábua ou tabela de operação

Seja a operação * definida no conjunto {a, b, c, e}.

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

6.2 Grupos Comutativos ou Abelianos

Além das propriedades mencionadas na definição de grupo, se $*$ for comutativa, então o grupo G é denominado comutativo ou abeliano.

6.2.1 Anel – Definição

Agora, estudaremos estruturas algébricas que têm duas operações definidas sobre elas, lembrando que uma operação sobre um conjunto é uma maneira de combinar dois elementos desse conjunto, produzindo um terceiro. O estudo de anéis, como objeto abstrato, veio da observação de que muitos conjuntos com os quais trabalhamos frequentemente têm duas operações definidas sobre eles, e com propriedades semelhantes, como, por exemplo, o conjunto dos inteiros, o conjunto dos números reais, o conjunto das matrizes quadradas, o conjunto dos polinômios etc.
Esses exemplos citados têm uma soma e uma multiplicação definidas em cada um deles, e são grupos comutativos com relação à soma. Além disso, a soma e a multiplicação se relacionam através da propriedade que chamamos de distributividade. Esses fatos levaram à seguinte definição.

Definição
Seja $A \neq \emptyset$ um conjunto com duas operações: uma adição (+) e uma multiplicação ($\cdot$). Dizemos que $(A, +, \cdot)$ é um anel quando:

$\Rightarrow$ A é um grupo abeliano com relação à adição:
$\forall x, y, z \in A, x + (y + z) = (x + y) + z \circ \forall x, y \in A, x + y = y + x \circ$
Existe $0 \in A$ tal que $x + 0 = x, \forall x \in A$
Para todo $x \in A$, existe $(-x) \in A$ tal que $x + (-x) = 0$

$\Rightarrow$ A multiplicação é associativa: $\forall x, y, z, (x \cdot y) \cdot z = x \cdot (y \cdot z)$.
$\Rightarrow$ A multiplicação é distributiva com relação à adição:
$x.(y + z) = x.y + x.z$ e $(x + y).z = x. z + y. z$ para quaisquer $x, y, z \in A$.

Exemplos

⇒ O conjunto dos números inteiros é um anel com relação às operações de adição e de multiplicação de inteiros usuais.

⇒ Também são anéis os seguintes conjuntos numéricos: (Q, +, .·), (R, +, .·) e (C, +, .·).

⇒ Sendo n um inteiro positivo, o conjunto dos múltiplos de n, nZ= {nk | k ∈ Z}, é um anel com as operações de adição e de multiplicação usuais dos inteiros.

⇒ Dado n > 1 um inteiro, o conjunto Mn×n(Z) das matrizes quadradas n × n com elementos em Z é um anel com relação à adição e à multiplicação de matrizes definidas de forma usual.

6.2.2 Propriedades

Subanéis

Seja (A, +, .·) um anel e S≠∅ um subconjunto de A.
Dizemos que S é um subanel de A quando (S, +, .·) também for um anel com as operações de A restritas ao conjunto S.

Exemplos

⇒ O conjunto dos múltiplos de 2, 2Z, é um subanel de Z com as operações de adição e multiplicação de inteiros usuais.

⇒ Em geral, (nZ, +, . ·) é um subanel de (Z, +, .·) para qualquer inteiro positivo n.

A proposição a seguir fornece um critério bastante útil para determinar se um conjunto S ≠ ∅ é subanel de um anel A.

Proposição
Sejam (A, +, .·) e S ≠ ∅ um subconjunto de A.
Então, S é um subanel de A se, e somente se, S for fechado com relação à subtração e à multiplicação de A, ou seja, se, e somente se, x − y ∈ S e x.y ∈ S para quaisquer x, y ∈ S.

Observação
Em um anel A, a diferença x−y de dois elementos x, y ∈ A é definida como sendo x − y = x + (−y).

Exemplo
Consideremos no anel A = (M2×2(R), +, .·) o conjunto S = $\{\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \mid x, y \in Q\}$.

⇒ É claro que S ≠ ∅ porque, por exemplo, $\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} \in S$.

⇒ Além disso, dados dois elementos quaisquer de S, M = $\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}$ e N = $\begin{pmatrix} z & 0 \\ t & 0 \end{pmatrix}$, temos que M − N = $\begin{pmatrix} x-z & 0 \\ y-t & 0 \end{pmatrix} \in S$ e M.N = $\begin{pmatrix} xz & 0 \\ yt & 0 \end{pmatrix} \in S$.

⇒ Usando a Proposição anterior, concluímos que S é um subanel de A.

Anéis comutativos

Um anel $(A, +, .\cdot)$ é denominado comutativo se a sua multiplicação for comutativa, ou seja, se $x.y = y.x, \forall x, y \in A$.

Exemplos

⇒ O anel dos inteiros $(Z, +, .\cdot)$ é um anel comutativo, porque $x.y = y.x, \forall x, y \in Z$.

⇒ Também são comutativos os seguintes anéis: Q, R, C com as operações usuais de adição e de multiplicação definidas em cada um desses conjuntos.

⇒ Dado $n > 1$ um inteiro, o anel $(Mn\times n(R), +, .\cdot)$ das matrizes quadradas $n\times n$ com elementos não é comutativo.

Anéis com unidade

Um anel com unidade é um anel A cuja multiplicação tem um elemento neutro, denotado por $1A$ ou simplesmente por 1, é denominado a unidade do anel.

Exemplos

⇒ O número 1 é a unidade dos anéis $(Z, +, .\cdot)$, $(Q, +, .\cdot)$,$(R, +, .\cdot)$ e $(C, +, .\cdot)$. Logo, esses são exemplos de anéis com unidade.

⇒ Sendo n um inteiro maior do que 1, o anel $(nZ, +, .\cdot)$ não tem unidade.

Anéis de integridade

Um anel comutativo com unidade A é denominado anel de integridade quando $\forall x, y \in A, x.y = 0 \Rightarrow x = 0$ ou $y = 0$.

Definição

Dizemos que $x \neq 0$ e $y \neq 0$ em um anel A são divisores próprios de zero quando $x.y = 0$.

Observação

De acordo com as definições anteriores, um anel de integridade é um anel comutativo com unidade que não tem divisores próprios do zero.

Exemplos

⇒ No anel dos inteiros Z, se $x, y \in Z$ são tais que $x.y = 0$, então temos que $x = 0$ ou $y = 0$. Logo, Z é um anel de integridade.

⇒ Também são anéis de integridade: Q, R e C.

⇒ Em $A = M2\times 2(Z)$, consideremos os elementos $X = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ e $Y = \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}$. X e Y não são matrizes nulas, no entanto $X.Y = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Logo, X e Y são divisores próprios do zero, e A não é anel de integridade.

6.3 Corpo

Um anel comutativo com unidade K é denominado um corpo se todo elemento não nulo de K tiver inverso multiplicativo, ou seja, $\forall x \in K, x \neq 0 \Rightarrow \exists x^{-1} \in K$ tal que $x.x^{-1} = 1$.

Exemplos

⇒ Os anéis Q, R e C são exemplos de corpos (com as operações de adição e multiplicação usuais).

⇒ Z não é um corpo, porque nem todo elemento de Z tem inverso multiplicativo. Por exemplo, $2 \in Z$, e não existe $y \in Z$ tal que $2.y = 1$.

⇒ Se p for um inteiro primo positivo, então Zp é um corpo.

6.3.1 Propriedades

Proposição

Todo corpo é um anel de integridade.

Observação

A recíproca da proposição anterior não é válida, ou seja, nem todo anel de integridade é um corpo. O exemplo mais conhecido dessa situação é o anel dos inteiros Z.

Proposição

Todo anel de integridade finito é um corpo.

Homomorfismos de anéis

Uma função $f: A \rightarrow B$ de um anel A em um anel B é denominada homomorfismo de anéis quando forem verificadas as duas seguintes propriedades:

- $\forall x, y \in A, f(x + y) = f(x) + f(y)$;
- $\forall x, y \in A, f(x \cdot y) = f(x) \cdot f(y)$

Exemplo

Sejam $A = R$, $B = R \times R$ e a função $f: A \rightarrow B$, $f(x) = (0, x)$.

⇒ Se $x, y \in R$, então $f(x + y) = (0, x + y) = (0, x) + (0, y) = f(x) + f(y)$

⇒ Temos também: $f(x.y) = (0, x.y) = (0, x).(0, y) = f(x).f(y)$.

Logo, f é um homomorfismo do anel A no anel B.

Seja $f : A \rightarrow B$ um homomorfismo de anéis. São válidas as seguintes propriedades:

⇒ $f(-x) = -f(x), \forall x \in A$

⇒ $f(x - y) = f(x) - f(y), \forall x, y \in A$

⇒ Se S é um subanel de A, então f(S) é um subanel de B

⇒ Se f for uma função sobrejetora e A possuir unidade 1A, então o mesmo acontece com B e a unidade de B é $1B = f(1A)$

⇒ Se f for sobrejetora, A tiver unidade e x for invertível (com relação à multiplicação), então f(x) também é invertível e $f(x^{-1}) = [f(x)]^{-1}$

Isomorfismos de anéis

Um isomorfismo de um anel A em um anel B é uma função $f: A \to B$ que é um homomorfismo e bijetora.

Observações

⇒ Se existir um isomorfismo de anéis $f: A \to B$, então $f^{-1}: B \to A$ também é um isomorfismo.

⇒ Quando existir um isomorfismo de A em B, então dirá que A e B são isomorfos e denotamos isso por $A \simeq B$.

⇒ Se A e B forem anéis isomorfos, então eles têm as mesmas propriedades; a diferença entre eles é basicamente os nomes dos elementos.

6.4 Síntese da Unidade

Nesta Unidade, estudamos alguns aspectos do campo da Álgebra, tendo visitado especialmente a Teoria de Grupos e a Teoria de Anéis.

Um grupo é um conjunto com uma operação binária que satisfaz três condições básicas (associatividade, existência de um elemento neutro e existência de inversos). Em outras palavras, é um homomorfismo de grupos se preserva a operação entre quaisquer dois elementos dos grupos.

Depois de abordar esses conceitos, estudamos a estrutura algébrica, que é a estrutura de anel. Trata-se de uma estrutura importante, pois generaliza a aritmética dos conjuntos numéricos. Assim, os conjuntos dos números inteiros, dos racionais, dos reais ou dos complexos, são exemplos de anéis.

Vimos, ainda, que conjuntos de matrizes, de funções e de polinômios também formam anéis. Estudamos a definição de anel, vimos que corpos é um tipo especial de anel comutativo com unidade, e vimos também que todo corpo é domínio de integridade.

Além disso, tivemos a oportunidade de exibir alguns exemplos importantes de anéis e verificar a validade das propriedades básicas das operações de soma e de produto em um anel, decorrentes diretamente da definição.

Como sabemos, a Álgebra é um vasto campo da Matemática. Nesse sentido, é importante salientar que a Matemática é uma disciplina que se aprende “fazendo”, por isso a resolução de exercícios é parte fundamental desse aprendizado. Não deixe de praticar nos tópicos apresentados a seguir.

Esperamos que, ao chegar ao fim desta Unidade, você tenha avançado nesse aspecto e se torne cada vez mais independente em seus estudos.

6.5 Para saber mais

ENDLER, OTTO. **Teoria dos corpos.** Disponível em: http://www.impa.br/opencms/pt/biblioteca/pm/PM_19.pdf. Acessado em janeiro de 2021.
Neste site, você encontra, além de publicações do IMPA, muitos textos sobre as diversas áreas da Matemática que podem ser baixados para seu uso pessoal.

6.6 Aprendendo e praticando

1. **Seja $\otimes$ a operação sobre R definida por $x \otimes y = x + y + xy$. Verifique se essa operação é comutativa, se é associativa e se tem elemento neutro.**

   Solução
   Para quaisquer x, y ∈ R, $x \otimes y = x+y+xy = y+x+yx = y \otimes x$.
   Logo, a operação $\otimes$ é comutativa.

   Para quaisquer x, y,z ∈ R, temos: $x \otimes (y \otimes z) = x \otimes (y + z + yz) = x + (y + z + yz) + x(y + z + yz) = x + y + z + xy + xz + yz + xyz$; $(x \otimes y) \otimes z = (x + y + xy) \otimes z = (x + y + xy) + z + (x + y + xy)z = x + y + z + xy + xz + yz + xyz$.
   Logo, $x \otimes (y \otimes z) = (x \otimes y) \otimes z$, de onde concluímos que $\otimes$ é associativa.

   $0 \otimes x = x \otimes 0 = x + 0 + x \cdot 0 = x$, ∀x ∈ R.
   Logo, o 0 (zero) é o elemento neutro da operação.

2. **Consideremos o conjunto dos números reais R com a operação definida por $x*y = \sqrt[3]{x^3 + y^3}$. Mostre que G = (R, ∗) é um grupo abeliano.**

   Solução
   $x*y = \sqrt[3]{x^3 + y^3} = \sqrt[3]{y^3 + x^3} = y * x$, ∀x, y ∈ R.
   Logo, ∗ é comutativa.

   Sejam x, y, z ∈ R' três elementos genéricos. $x*(y * z) = x*\sqrt[3]{y^3 + z^3} = \sqrt[3]{x^3 + (\sqrt[3]{y^3 + z^3})^3} = \sqrt[3]{x^3 + y^3 + z^3}$. →$(x*y)*z = \sqrt[3]{x^3 + y^3} *z = \sqrt[3]{x^3 + y^3 + z^3}$.
   Logo, x∗(y∗z) = (x∗y)∗z, ou seja, a operação ∗ é associativa. • $0*x = x*0 = \sqrt[3]{x^3 + 0^3} = \sqrt[3]{x^3} =$ x, ∀x ∈ R, logo, 0 (zero) é o elemento neutro.

   Dado x ∈ R, y = −x é tal que $y*x = x*y = \sqrt[3]{x^3 + y^3} = \sqrt[3]{x^3 + (-x)^3} = \sqrt[3]{x^3 - x^3} =$ 0 elemento neutro.
   Logo, −x é o elemento inverso de x. Os quatro itens anteriores demonstram que (G, ∗) é um grupo abeliano.

3. **Verifique se H é subgrupo de G no seguinte caso: H = (R−Q, +), G = (R, +).**

Solução

O conjunto H é o conjunto dos números irracionais. Dados dois irracionais, por exemplo, $x = 2-\sqrt{3}$ e $y = 2+\sqrt{3}$, temos $x+y = (2-\sqrt{3})+(2+\sqrt{3}) = 4$ não pertence a H.

Logo, o conjunto dos irracionais não é fechado para a adição de números reais e, consequentemente, não forma um subgrupo de R.

4. **Sejam $A = Z\times Z$, $(a, b)\oplus(c, d) = (a+c, b+d)$, $(a, b)\otimes(c, d) = (ac-bd, ad+bc)$, onde $a, b, c, d \in Z$. Mostre que $(A, \oplus, \otimes)$ é um anel, verifique se é comutativo e se tem unidade.**

Solução

$(A, \oplus, \otimes)$ é um anel comutativo com unidade.

5. **Determine quais das seguintes operações são associativas:**
   (a) A operação o sobre Z definida por a o b = a – b.
   (b) A operação o sobre R definida por aob = a+ b + ab.

6. **Sejam $A = \{0, 1, 2, 3, 4\} \subset N$ e as operações $\oplus$ e $\odot$ definidas por**
   - $x \odot y$ = resto da divisão de xy por 5;
   - $x \oplus y$ = resto da divisão de x + y por 5. Construa a tábua dessas duas operações sobre o conjunto A.

Solução

Alguns exemplos: • $3 \odot 4$ = resto da divisão de 12 por 5 = 2.

• $2 \odot 3$ = resto da divisão de 6 por 5 = 1, • $4 \oplus 3$ = resto da divisão de 7 por 5 = 2, etc.

Prosseguindo dessa forma, obtemos as seguintes tabelas:

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\oplus$	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

7. **Considere a seguinte operação * definida sobre o conjunto dos números racionais $x*y=\frac{x+y}{2}$. Verifique se * é comutativa, se é associativa, se tem elemento neutro e se existem elementos invertíveis.**

Solução

Para quaisquer $x, y \in Q$, temos $x * y = x+y/2 = y+x/2 = y*x$, logo, a operação é comutativa.

$\Rightarrow 1*(2*3) = 1*(2+3)/2 = 1*5/2 = (1+ 5/2)/2 = 7/4$ e $(1*2)*3 = (1+2)/2 * 3 = 3/2*3 = 3/2 +3)/2 = 9/4$; logo, $1*(2* 3)\neq(1*2)*3$ e daí concluímos que a operação não é associativa.

$\Rightarrow$ Suponhamos que e seja o elemento neutro dessa operação. Então, por exemplo, $e*0 = 0$ e $e*1 = 1 \Rightarrow e+0/2 = 0$ e $e+1/2 = 1$, ou seja, $e = 0$ e $e = 1$, o que é impossível.
Logo, a operação não tem elemento neutro.
Se a operação não tem elemento neutro, então não faz sentido a definição de elemento invertível.

UNITAU digital

ISBN: 978-65-86914-56-6